MALLA REDDY INSTITUTE OF TECHNOLOGY & SCIENCE
(SPONSORED BY MALLA REDDY EDUCATIONAL SOCIETY)
Affiliated to JNTUH & Approved by AICTE, New Delhi
NAAC with 'A' Grade, NBA Accredited, ISO 9001:2015 Certified, Approved by UK Accrediation Centre
Granted Status of 2(f) & 12(b) under UGC Act, 1956, Govt. of India.

COMPUTER NETWORKS

FACULTY IN-CHARGE
M. MAMATHA & Harika
YEAR :III
SUBJECT CODE CS414PC
ACADEMIC YEAR 2022-2023
REGULATION R18

CS414PC: COMPUTER NETWORKS
III Year B. Tech. I SEM

Prerequisites

- A course on "Programming for problem solving".
- A course on "Data Structures".

Course Objectives:

- The objective of the course is to equip the students with a general overview of the concepts and fundamentals of computer networks.
- Familiarize the students with the standard models for the layered approach to communication between machines in a network and the protocols of the various layers.

Course Outcomes:

- Gain the knowledge of the basic computer network technology.
- Gain the knowledge of the functions of each layer in the OSI and TCP/IP reference model.
- Obtain the skills of sub-netting and routing mechanisms.
- Familiarity with the essential protocols of computer networks, and how they can be applied in network design and implementation.

UNIT – I

Network hardware, Network software, OSI, TCP/IP Reference models,
Example Networks: ARPANET, Internet.
Physical Layer: Guided Transmission media: twisted pairs, coaxial cable, fiber optics, Wireless transmission.

UNIT – II

Data link layer: Design issues, framing, Error detection and correction.
Elementary data link protocols: simplex protocol, a simplex stop and wait protocol for an error-free
Channel, A simplex stop and wait protocol for noisy channel.
Sliding Window protocols: A one-bit sliding window protocol, A protocol using Go-Back-N, A protocol Using Selective Repeat, Example data link protocols.
Medium Access sub layer: The channel allocation problem, Multiple access protocols: ALOHA,
Carrier sense multiple access protocols, collision free protocols. Wireless LANs, Data link layer
switching.

UNIT – III

Network Layer: Design issues, Routing algorithms: shortest path routing, Flooding, Hierarchical
Routing, Broadcast, Multicast, distance vector routing, Congestion Control Algorithms, Quality of
Service, Internetworking, the Network layer in the internet.

UNIT – IV

Transport Layer: Transport Services, Elements of Transport protocols, Connection management, TCP & UDP protocols.

UNIT – V

Application Layer –Domain name system, SNMP, Electronic Mail; the World WEB, HTTP, Streaming Audio and Video.

TEXT BOOK:

1. Computer Networks -- Andrew S Tanenbaum, David. j. Wetherall, 5th Edition. Pearson Education/PHI

REFERENCE BOOKS:

1. An Engineering Approach to Computer Networks-S. Keshav, 2nd Edition, Pearson Education
2. Data Communications and Networking – Behrouz A. Forouzan. 3rd Edition TMH.

UNIT – I

Network hardware, Network software, OSI, TCP/IP Reference models, Example Networks: ARPANET, Internet.
Physical Layer: Guided Transmission media: twisted pairs, coaxial cable, fiber optics, Wireless transmission.

Network hardware

Network hardware is a set of physical or network devices that are essential for interaction and communication between hardware units operational on a computer network.
These are dedicated hardware components that connect to each other and enable a network to function effectively and efficiently.
Network hardware plays a key role as industries grow as it supports scalability, enterprise's needs, effective mode of communication, improving the business standards.
It also promotes multiprocessing and enables sharing of resources, information, and software with ease.
Routers, hubs, switches, and bridges are some examples of network hardware.

1. **Modems:**

A modem enables a computer to connect to the internet via a telephone line.
The modem at one end converts the computer's digital signals into analog signals and sends them through a telephone line.
At the other end, it converts the analog signals to digital signals that are understandable for another computer.

2. **Routers:**

A router connects two or more networks.
One common use of the router is to connect a home or office network (LAN) to the internet (WAN).
It generally has a plugged-in internet cable along with cables that connect computers on the LAN.

Alternatively, a LAN connection can also be wireless (Wi-Fi-enabled), making the network device wireless.
These are also referred to as wireless access points (WAPs).

3. Hubs:

A hub broadcasts data to all devices on a network.
As a result, it consumes a lot of bandwidth as many computers might not need to receive the broadcasted data.
The hub could be useful in linking a few gaming consoles in a local multiplayer game via a wired or wireless LAN.

4. Bridges:

A bridge connects two separate LAN networks.
It scans for the receiving device before sending a message.
This implies that it avoids unnecessary data transfers if the receiving device is not there.
Moreover, it also checks to see whether the receiving device has already received the message.
These practices improve the overall performance of the network.

5. Switches:

A switch is more powerful than a hub or a bridge but performs a similar role.
It stores the MAC addresses of network devices and transfers data packets only to those devices that have requested.
Thus, when the demand is high; a switch becomes more efficient as it reduces the amount of latency.

6. Network interface cards:

A network interface card (NIC) is a hardware unit installed on a computer, which allows it to connect to a network.
It is typically in the form of a circuit board or chip.
In most modern machines, NICs are built into the motherboards, while in some computers; an extra expansion card in the form of a small circuit board is added externally.

7. Network cables:

Cables connect different devices on a network.
Today, most networks have cables over a wireless connection as they are more secure, i.e., less prone to attacks, and at the same time carry larger volumes of data per second.

8. Firewall:

A firewall is a hardware or software device between a computer and the rest of the network open to attackers or hackers.
Thus, a LAN can be protected from hackers by placing a firewall between the LAN and the internet connection.
A firewall allows authorized connections and data-like emails or web pages to pass through but blocks unauthorized connections made to a computer or LAN.

Network software

Network software is an umbrella term used to describe a wide range of software that streamlines the operations, design, monitoring, and implementation of computer networks.

Network software is a fundamental element for any networking system. It helps administrators and security personnel reduce network complexities, and manage, monitor, and better control network traffic.

Network software plays a crucial role in managing a network infrastructure and simplifying IT operations by facilitating communication, security, content, and data sharing.

Functions of network software

1. **User management**
   Allows administrators to add or remove users from the network.
   This is particularly useful when hiring or relieving

2. **File management**
   Lets administrators decide the location of data storage and control user access to that data.

3. **Access**
   Enables users to enjoy uninterrupted access to network resources.

4. **Network security systems**
   Assist administrators in looking after security and preventing data breaches.

   Key Components of Network Software

   Network software is an advanced, robust, and secure alternative to traditional networking, making the network easier to administer in terms of management, modifications, configuration, supply resources and troubleshooting.

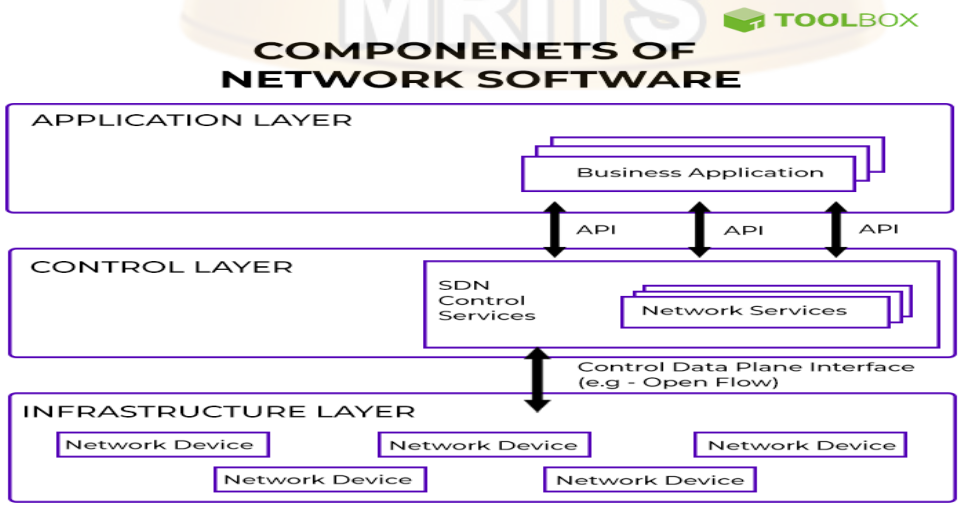


Fig: Components of Network Software

1. **Application layer**

The first component is the application layer or the application plane, which refers to the applications and services running on the network.

It is a program that conveys network information, the status of the network, and the network requirements for particular resource availability and application.

2. Control layer

The control layer lies at the center of the architecture and is one of the most important components of the three layers.

You could call it the brain of the whole system.

Also called the controller or the control plane, this layer also includes the network control software and the network operating system within it.

It is the entity in charge of receiving requirements from the applications and translating the same to the network components.

3. Infrastructure layer

The infrastructure layer, also called the data plane, consists of the actual network devices (both physical and virtual) that reside in this layer.

They are primarily responsible for moving or forwarding the data packets after receiving due instructions from the control layer.

In simple terms, the data plane in the network architecture components physically handles user traffic based on the commands received by the controller.

Network Software Types

There are numerous types of network software available, with most of them being categorized under the communications and security arena. The varieties of network software differ based on their key features and costs. The main role of network software is to eliminate the dependence on hardware by streamlining communications across multiple devices, locations, and systems. Not only are they extremely useful for end-user hardware (laptops, desktops), the addition of software is bound to have a positive effect on the organization's everyday functioning and operations.

Fig: Network Software Types

1. Network storage software

In many ways, data within networks is like a child. With time, it only grows, and as it does, it requires adequate attention. Soon enough, data needs to be stored spanning multiple locations and a wide range of devices. Network storage software allows businesses to utilize a standard

interface that manages countless databases between users or clients. It serves as a good manager of access between various departments or essential communities within an organization. This way, anybody having access can view or retrieve information with just a click, and at the same time, security concerns are also taken care of.

2. Data archiving software

In today's day and age of dynamic networks spread across various functioning corporate entities, data once misplaced is data lost. Hence, it is vital to take regular backups. As organizations grow and networks evolve in size, it gets especially tricky to save data appropriately. In addition to that, data that needs to be stored increases at a rapid pace, and its management gets costlier. In such a situation, data archiving software is a perfect choice.
Organizations have heaps of data that might not have to be utilized daily but is still essential to be stored for various purposes, one of them being for regular compliance. Data archiving software enables better management of such information and is an optimal solution to reduce costs while ensuring that the data is being protected. However, as a word of caution, archive software does not function the same way as regular standard backups. Hence, it is always recommended to ensure that the archived data doesn't need to be accessed soon.

3. Patch management software

It is a nightmare for IT employees to install updates on each device individually. Moreover, when a network consists of numerous devices, ensuring the timely installation of updates is not only expensive but often a cumbersome process as well. As the name suggests, patch management software aids in the smoother management of updates across numerous devices on the network through the installation of patches. This makes the process more seamless and enables each machine to download a patch managed by central software and run updates automatically. Patch management software is the more hassle-free and effective way to perform continuous updates across devices and systems in an organization.

4. Security surveillance software

A majority of network software focuses on data storage and linking devices. However, they do not incorporate protection for a network. This is where security surveillance software comes into the picture. It monitors and connects the various security solutions within a network. Specific software is ideal for large networks as it effortlessly links throughout locations and provides credible browser-based live and recorded footage to an organization. On the other hand, better-targeted software works well in protecting vulnerable units by building a network architecture that reduces attack surfaces, thereby keeping components hidden from any malicious parties. This happens through developing outbound-only connections with cloud services and providers.

5. Asset management software

One of the most challenging tasks in any organization is to keep the network up and running efficiently. Achieving this demands greater visibility of the network infrastructure as well as regular tracking and monitoring of essential metrics. That's where asset management software comes to the rescue. Compared to most of its counterparts, asset management software operates from a centralized server room or hub and is not connected to any hardware. This is good in terms of cost reduction and offers an excellent experience to the users and clients.

6. Deployment and migration software

Managing a network comes with regular upgrades or movement of assets, and this can sometimes become a herculean task. However, it doesn't have to be so. The use of deployment and migration software aids organizations in making processes such as upgrading systems hassle-free. The software provides an interface that enables easy monitoring of any deployment or data movement between the hardware and databases within the network. It also ensures mandatory checks on compatibility when any data is being moved between regular backups and archives, thereby significantly reducing the chances of data loss.

7. Printer and fax software

Printers and fax machines are indispensable equipment for any working organization. As an organization grows, so does the number of assets involved within its network. Standard options such as Wi-Fi printing might not always be the best choice, especially for big corporations or schools that span across many floors. This software provides an easy-to-use interface that enables the undertaking and maintenance of multiple tasks. That's not it! With this software, one can easily set IP printing across networks or even deploy updates. What's more? In some cases, it can also enable organizations to fax or print important documents and correspondence across different locations.

8. Network management software

In a sea of countless options, why should an organization opt for network management software? The reason is quite apparent. Their primary function is to monitor, manage, and troubleshoot any hurdles in network performance across the whole device infrastructure. While a network monitoring software might have some basic options plugged in to troubleshoot, network management software is equipped to manipulate and modify network performance for the better. These software applications are hosted by several industry-leading brands.

OSI/ ISO MODEL:

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

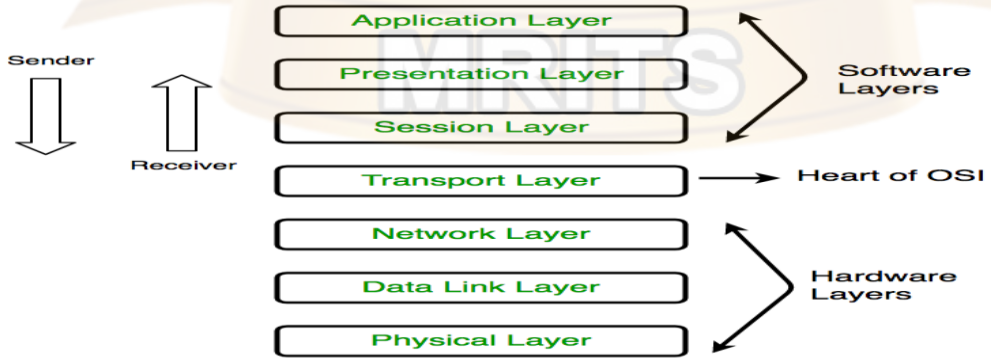
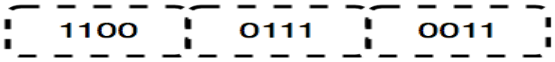


FIG: OSI/ ISO MODEL

1. **Physical Layer (Layer 1) :**

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



The functions of the physical layer are :

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

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

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

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

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

The packet received from the Network layer is further divided into frames depending on the frame size of NIC (Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.
The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.

The functions of the Data Link layer are :

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

** Packet in Data Link layer is referred to as **Frame**.*
*** Data Link layer is handled by the NIC (Network Interface Card) and device drivers of*

host machines.
**** Switch & Bridge are Data Link Layer devices.*

3. Network Layer (Layer 3):
The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP addresses are placed in the header by the network layer.
The functions of the Network layer are :

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

* *Segment* in Network layer is referred to as **Packet**.

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

4. Transport Layer (Layer 4):
The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

- **At sender's side:**

Transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.
Note: The sender needs to know the port number associated with the receiver's application.
Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.

- **At receiver's side:**

Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.
The functions of the transport layer are :

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

address, the transport layer makes sure that the message is delivered to the correct process.

The services provided by the transport layer :

1. **Connection-Oriented Service:**
   It is a three-phase process that includes
   – Connection Establishment
   – Data Transfer
   – Termination / disconnection
   In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.
2. **Connectionless service:**
   It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

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

5. Session Layer (Layer 5):

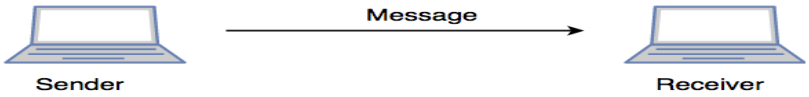
This layer is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensures security.
The functions of the session layer are:

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

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

SCENARIO:

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



6. Presentation Layer (Layer 6):

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

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

7. Application Layer (Layer 7):

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

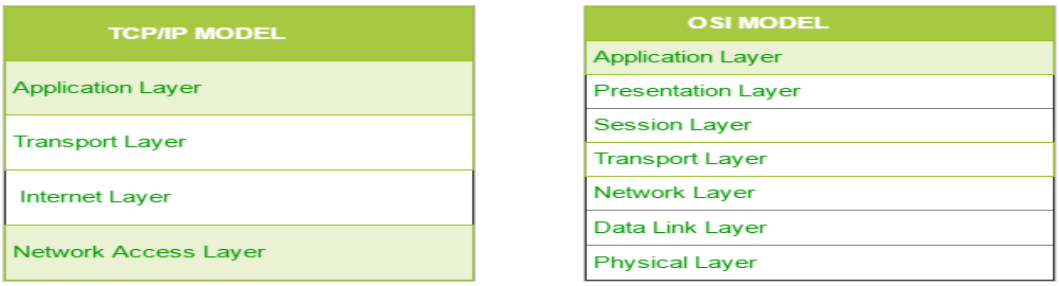
The functions of the Application layer are :

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

OSI model acts as a reference model and is not implemented on the Internet because of its late invention. The current model being used is the TCP/IP model.
TCP/ IP REFERENCE MODEL:
The **OSI Model** we just looked at is just a reference/logical model.
It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components.
But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols.
It stands for Transmission Control Protocol/Internet Protocol.
The **TCP/IP model** is a concise version of the OSI model.
It contains four layers, unlike seven layers in the OSI model.
The layers are:

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

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



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

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

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

1. **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:
   IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses is limited in number when compared to the number of users.
2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagram 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 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.

EXAMPLE NETWORKS:
ARPANET
ARPANET stands for **Advanced Research Projects Agency NET**. ARPANET was first network which consisted of distributed control.
It was first to Implement TCP/IP protocols.
It was basically beginning of Internet with use of these technologies.
It was designed with a basic idea in mind that was to communicate with scientific users among an institute or university.

History of ARPANET:

ARPANET was introduced in the year 1969 by Advanced Research Projects Agency (ARPA) of US Department of Defense.
It was established using a bunch of PCs at various colleges and sharing of information and messages was done.
It was for playing as long separation diversions and individuals were asked to share their perspectives.

In the year 1980, ARPANET was handed over to different military network, Defense Data Network.

Characteristics of ARPANET:

1. It is basically a type of WAN.
2. It used concept of Packet Switching Network.
3. It used Interface Message Processors (IMPs) for sub-netting.
4. ARPANETs software was split into two parts- a host and a subnet.

Advantages of ARPANET:

- ARPANET was designed to service even in a Nuclear Attack.
- It was used for collaborations through E-mails.
- It created advancement in transfer of important files and data of defense.

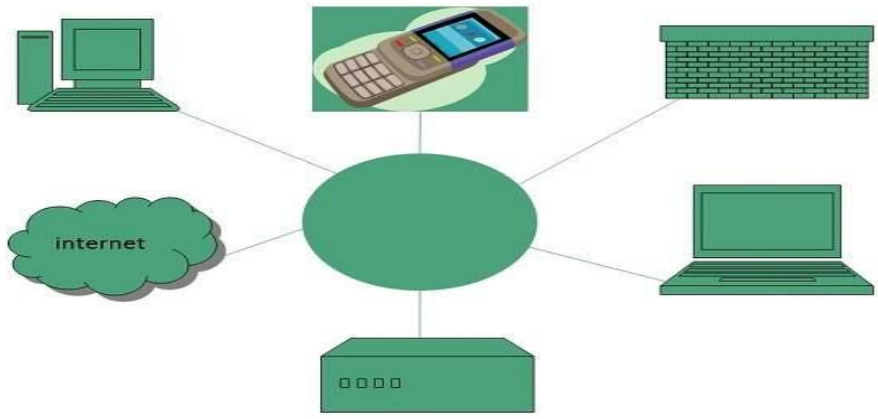
Limitations of ARPANET:

- Increased number of LAN connections resulted in difficulty handling.
- It was unable to cope-up with advancement in technology.

INTERNET
In simplest terms, the Internet is a global network comprised of smaller networks that are interconnected using **standardized** communication protocols.
The Internet standards describe a framework known as the Internet protocol suite.
This model divides methods into a *layered system of protocols.*
These layers are as follows:

1. **Application layer (highest) –**
   Concerned with the data (URL, type, etc.).
   This is where HTTP, HTTPS, etc., comes in.
2. **Transport layer –**
   Responsible for end – to - end communication over a network.
3. **Network layer –**
   Provides data route.

The Internet provides a variety of information and communication facilities; contains forums, databases, email, hypertext, etc.
It consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies.



Evolution

The concept of Internet was originated in 1969 and has undergone several technological & Infrastructural changes as discussed below:

- The origin of Internet devised from the concept of **Advanced Research Project Agency Network (ARPANET).**
- **ARPANET** was developed by United States Department of Defense.
- Basic purpose of ARPANET was to provide communication among the various bodies of government.
- Initially, there were only four nodes, formally called **Hosts.**
- In 1972, the **ARPANET** spread over the globe with 23 nodes located at different countries and thus became known as **Internet.**
- By the time, with invention of new technologies such as TCP/IP protocols, DNS, WWW, browsers, scripting languages etc., Internet provided a medium to publish and access information over the web.

Advantages

Internet covers almost every aspect of life, one can think of. Here, we will discuss some of the advantages of Internet:

- Internet allows us to communicate with the people sitting at remote locations. There are various apps available on the wed that uses Internet as a medium for communication. One can find various social networking sites such as:

Face book	Twitter	Yahoo	Google+	Flickr	Orkut

- One can surf for any kind of information over the internet. Information regarding various topics such as Technology, Health & Science, Social Studies, Geographical Information, Information Technology, Products etc can be surfed with help of a search engine.
- Apart from communication and source of information, internet also serves a medium for entertainment. Following are the various modes for entertainment over internet.

Online Television	Online Games	Songs	Videos	Social Networking Apps

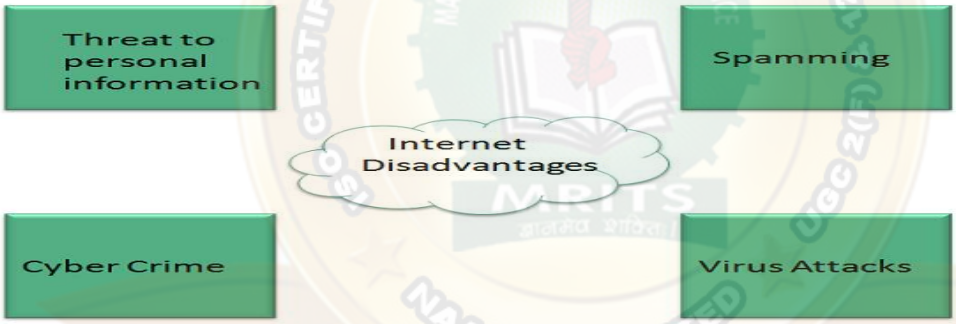
- Internet allows us to use many services like:

Internet Banking	Matrimonial Services	Online Shopping	Online Ticket Booking	Online Bill Payment	Data Sharing	E-mail

- Internet provides concept of **electronic commerce**, that allows the business deals to be conducted on electronic systems

Disadvantages

However, Internet has proved to be a powerful source of information in almost every field, yet there exists many disadvantages discussed below:



- There are always chances to loose personal information such as name, address, credit card number. Therefore, one should be very careful while sharing such information. One should use credit cards only through authenticated sites.
- Another disadvantage is the **Spamming**. Spamming corresponds to the unwanted e-mails in bulk. These e-mails serve no purpose and lead to obstruction of entire system.
- **Virus** can easily be spread to the computers connected to internet. Such virus attacks may cause your system to crash or your important data may get deleted.
- Also a biggest threat on internet is pornography. There are many pornographic sites that can be found, letting your children to use internet which indirectly affects the children healthy mental life.
- There are various websites that do not provide the authenticated information. This leads to misconception among many people.

PHYSICAL LAYER

Physical Layer is the bottom-most layer in the **Open System Interconnection (OSI) Model** which is a physical and electrical representation of the system.

It consists of various network components such as power plugs, connectors, receivers, cable types, etc.

Physical Layer sends data bits from one device(s) (like a computer) to another device(s).
Physical Layer defines the types of encoding (that is how the 0's and 1's are encoded in a signal).
Physical Layer is responsible for the communication of the unstructured raw data streams over a physical medium.

Functions Performed by Physical Layer:

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

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

Physical Topologies:

Physical Topology or Network Topology is the Geographical Representation of Linking devices. Following are the four types of physical topology-

1. **Mesh Topology:**

In a mesh topology, each and every device should have a dedicated point-to-point connection with each and every other device in the network. Here there is more security of data because there is a dedicated point-to-point connection between two devices. Mesh Topology is difficult to install because it is more complex.

2. **Star Topology:**

In star topology, the device should have a dedicated point-to-point connection with a central controller or hub. Star Topology is easy to install and reconnect as compared to Mesh Topology. Star Topology doesn't have Fault Tolerance Technique.

3. **Bus Topology:**

In a bus topology, multiple devices are connected through a single cable that is known as backbone cable with the help of tap and drop lines. It is less costly as compared to Mesh Topology and Star Topology. Re-connection and Re-installation are difficult.

4. **Ring Topology:**

In a ring topology, each device is connected with repeaters in a circle-like ring that's why it is called Ring Topology. In Ring topology, a device can send the data only when it has a token, without a token no device can send the data, and a token is placed by Monitor in Ring Topology.

Point to Point configuration:

In Point-to-Point configuration, there is a line (link) that is fully dedicated to carrying the data between two devices.

Multi-Point configuration:

In Multi-Point configuration, there is a line (link) through which multiple devices are connected.

Modes of Transmission Medium:

1. **Simplex mode:**

In this mode, out of two devices, only one device can transmit the data, the other device can only receive the data.
Example- Input from keyboards, monitors, TV broadcasting, Radio broadcasting, etc.

2. **Half Duplex mode:**

In this mode, out of two devices, both devices can send and receive the data but only one at a time not simultaneously. Example- Walkie -Talkie, Railway Track, etc.

3. **Full-Duplex mode:**

In this mode, both devices can send and receive the data simultaneously.
Example- Telephone System, Chatting applications, etc.

Guided Transmission Media

It is defined as the physical medium through which the signals are transmitted called as guided transmission Media.

It is also known as Bounded media.

Types of Guided media:

Twisted pair	Coaxial Cable	Fiber Optic

1. **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.

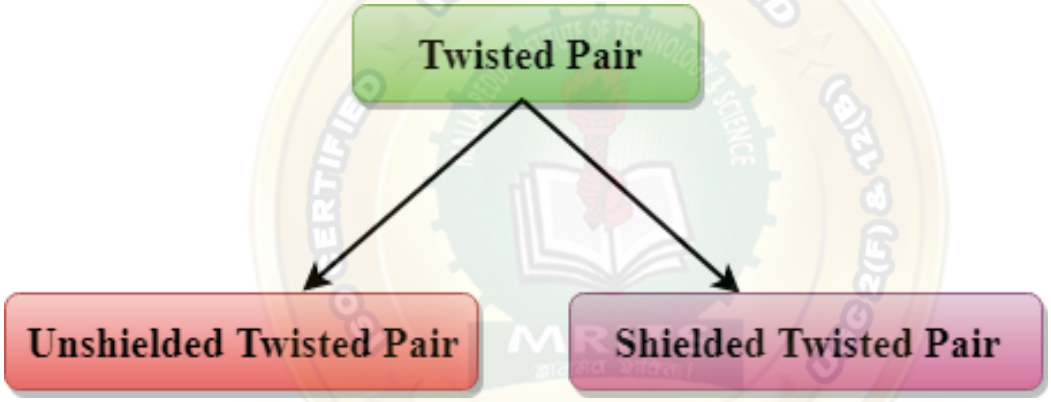
The frequency range for twisted pair cable is from 0 to 3.5 KHz.

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 up to 4Mbps.
- **Category 3:** It can support up to 16Mbps.
- **Category 4:** It can support up to 20Mbps. Therefore, it can be used for long-distance communication.
- **Category 5:** It can support up to 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.

2. 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.

Advantages of Coaxial cable:

- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

Disadvantages of Coaxial cable:

- It is more expensive as compared to twisted pair cable.

- If any fault occurs in the cable causes the failure in the entire network.

3. Fiber Optic

- Fiber optic cable is a cable that uses electrical signals for communication.
- Fiber optic is a cable that holds the optical fibers coated in plastic that are used to send the data by pulses of light.
- The plastic coating protects the optical fibers from heat, cold, electromagnetic interference from other types of wiring.
- Fiber optics provides faster data transmission than copper wires.

Diagrammatic representation of fiber optic cable:

Basic elements of Fiber optic cable:

- **Core:** The optical fiber consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fiber. The more the area of the core, the more lightly will be transmitted into the fiber.
- **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fiber.
- **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fiber strength, absorb shock and extra fiber protection.

Following are the advantages of fiber optic cable over copper:

- **Greater Bandwidth:** The fiber optic cable provides more bandwidth as compared copper. Therefore, the fiber optic carries more data as compared to copper cable.
- **Faster speed:** Fiber optic cable carries the data in the form of light. This allows the fiber optic cable to carry the signals at a higher speed.
- **Longer distances:** The fiber optic cable carries the data at a longer distance as compared to copper cable.
- **Better reliability:** The fiber optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
- **Thinner and Sturdier:** Fiber optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

Wireless Transmission (Un-Guided 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 omni-directional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3 KHz 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**.

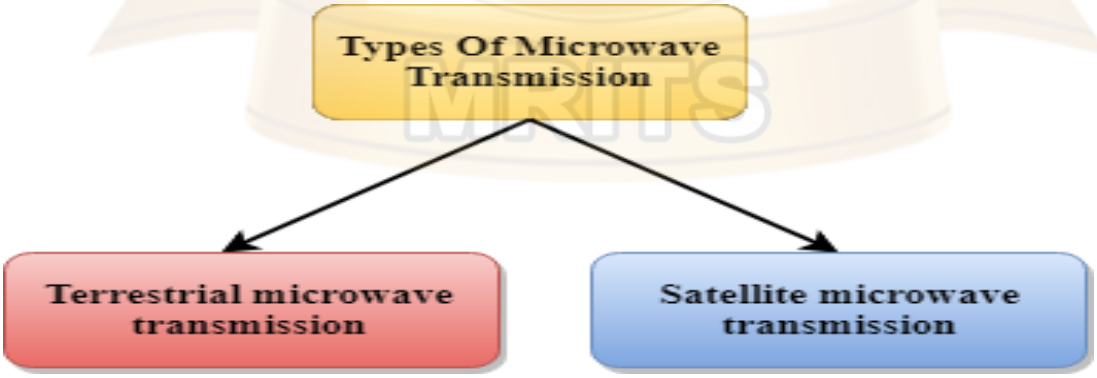
Applications of Radio waves:

- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.

Advantages of Radio transmission:

- Radio transmission is mainly used for wide area networks and mobile cellular phones.
- Radio waves cover a large area, and they can penetrate the walls.
- Radio transmission provides a higher transmission rate.

Microwaves



Microwaves are of two types:

- Terrestrial microwave
- Satellite microwave communication.

Terrestrial Microwave Transmission

- Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.

- Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
- Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focused.
- In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
- It works on the line of sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

Characteristics of Microwave:

- **Frequency range:** The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- **Bandwidth:** It supports the bandwidth from 1 to 10 Mbps.
- **Short distance:** It is inexpensive for short distance.
- **Long distance:** It is expensive as it requires a higher tower for a longer distance.
- **Attenuation:** Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

Advantages of Microwave:

- Microwave transmission is cheaper than using cables.
- It is free from land acquisition as it does not require any land for the installation of cables.
- Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
- Communication over oceans can be achieved by using microwave transmission.

Disadvantages of Microwave transmission:

- **Eavesdropping:** An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
- **Out of phase signal:** A signal can be moved out of phase by using microwave transmission.
- **Susceptible to weather condition:** A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.
- **Bandwidth limited:** Allocation of bandwidth is limited in the case of microwave transmission.

Satellite Microwave Communication

- A satellite is a physical object that revolves around the earth at a known height.
- Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.
- We can communicate with any point on the globe by using satellite communication.

How Does Satellite work?

The satellite accepts the signal that is transmitted from the earth station, and it amplifies the signal. The amplified signal is retransmitted to another earth station.

Advantages of Satellite Microwave Communication:

- The coverage area of a satellite microwave is more than the terrestrial microwave.
- The transmission cost of the satellite is independent of the distance from the centre of the coverage area.
- Satellite communication is used in mobile and wireless communication applications.
- It is easy to install.
- It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

Disadvantages Of Satellite Microwave Communication:

- Satellite designing and development requires more time and higher cost.
- The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
- The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

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

Data link layer: **D**esign issues, **f**raming, **E**rror detection and correction. **Elementary data link protocols:** Simplex protocol, a simplex stop and wait protocol for an error-free Channel, A simplex stop and wait protocol for noisy channel.
Sliding Window protocols: A one-bit sliding window protocol, A protocol using Go-Back-N, A protocol Using Selective Repeat, Example data link protocols.
Medium Access sub layer: The channel allocation problem, Multiple access protocols: ALOHA, Carrier sense multiple access protocols, collision free protocols. Wireless LANs, Data link layer Switching.

Data link layer

Design issues

Data-link layer is the second layer after the physical layer.
The data link layer is responsible for maintaining the data link between two hosts or nodes. Some of its sub-layers and their functions are as following below.
The data link layer is divided into two sub-layers:

1. **Logical Link Control Sub-layer (LLC)** – Provides the logic for the data link, thus it controls the synchronization, flow control, and error checking functions of the data link layer.
   Functions are –
   - **(i)** Error Recovery.
   - **(ii)** It performs the flow control operations.
   - **(iii)** User addressing.

2. **Media Access Control Sub-layer (MAC)** – It is the second sub-layer of data-link layer. It controls the flow and multiplexing for transmission medium. Transmission of data packets is controlled by this layer. This layer is responsible for sending the data over the network interface card. Functions are –
   - **(i)** To perform the control of access to media.
   - **(ii)** It performs the unique addressing to stations directly connected to LAN.
   - **(iii)** Detection of errors.

Design issues with data link layer are:

1. **Services provided to the network layer –** The data link layer act as a service interface to the network layer. The principle service is transferring data from network layer on sending machine to the network layer on destination machine. This transfer also takes place via DLL (Data link-layer).

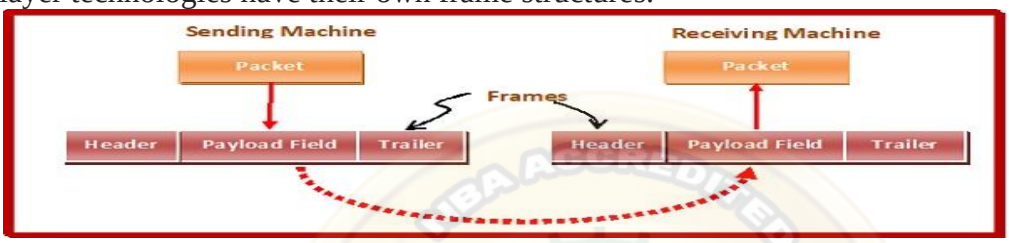
2. **Framing –**
   The source machine sends data in the form of blocks called frames to the destination machine. The starting and ending of each frame should be identified so that the frame can be recognized by the destination machine.
3. **Flow control –**
   Flow control is done to prevent the flow of data frame at the receiver end. The source

machine must not send data frames at a rate faster than the capacity of destination machine to accept them.

4. **Error control** – Error control is done to prevent duplication of frames. The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

Framing in Data Link Layer

Framing is **a function of the data link layer**. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. Ethernet, token ring, frame relay, and other data link layer technologies have their own frame structures.



In the physical layer, data transmission involves synchronized transmission of bits from the source to the destination. The data link layer packs these bits into frames.

Data-link layer takes the packets from the Network Layer and encapsulates them into frames.

If the frame size becomes too large, then the packet may be divided into small sized frames.

Smaller sized frames makes flow control and error control more efficient.

Then, it sends each frame bit-by-bit on the hardware. At receiver's end, data link layer picks up signals from hardware and assembles them into frames.

Parts of a Frame

A frame has the following parts −

- Frame Header − It contains the source and the destination addresses of the frame.
- Payload field − It contains the message to be delivered.
- Trailer − It contains the error detection and error correction bits.
- Flag − It marks the beginning and end of the frame.

Problems in Framing –

- **Detecting start of the frame:**
  When a frame is transmitted, every station must be able to detect it.
  Station detects frames by looking out for a special sequence of bits that marks the beginning of the frame
  i.e. SFD (Starting Frame Delimiter).

- **How does the station detect a frame:**
  Every station listens to link for SFD pattern through a sequential circuit.
  If SFD is detected, sequential circuit alerts station.
  Station checks destination address to accept or reject frame.

- **Detecting end of frame:**
  When to stop reading the frame.

Types of Framing

Framing can be of two types:

1. Fixed sized framing	**2.** Variable sized framing.

1. Fixed-sized Framing

Here the size of the frame is fixed and so the frame length acts as delimiter of the frame.

Consequently, it does not require additional boundary bits to identify the start and end of the frame.

Example: ATM cells.

- Drawback:
  It suffers from internal fragmentation if the data size is less than the frame size

- Solution: Padding

2. Variable – Sized Framing

Here, the size of each frame to be transmitted may be different. So additional mechanisms are kept to mark the end of one frame and the beginning of the next frame. It is used in local area networks.

Two ways to define frame delimiters in variable sized framing are –

- **Length Field** –

  Here, a length field is used that determines the size of the frame.

  It is used in Ethernet (IEEE 802.3).

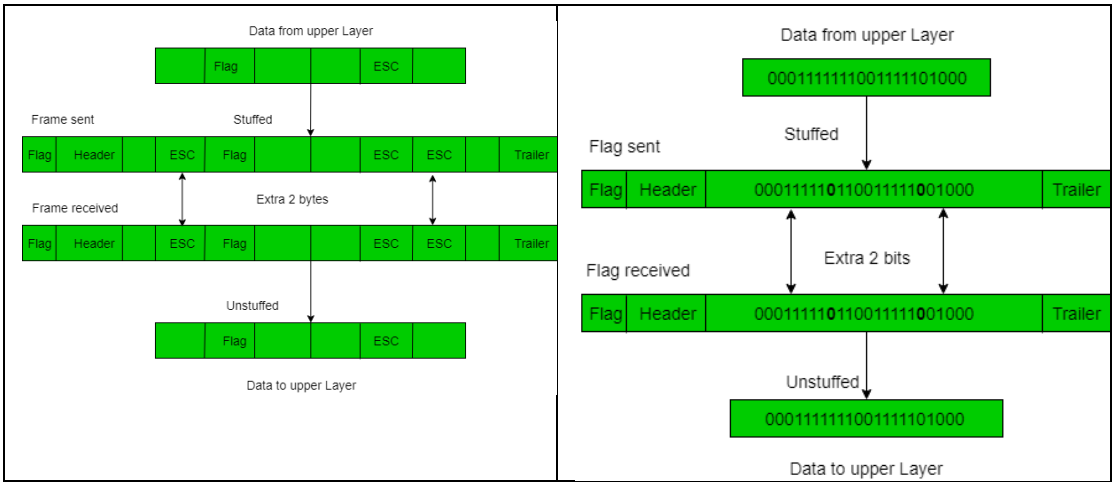
- **End Delimiter** –

  Here, a pattern is used as a delimiter to determine the size of frame.

  It is used in Token Rings.

  If the pattern occurs in the message, then two approaches are used to avoid the situation

(A)Byte/ Character – Stuffing –	**(B)Bit – Stuffing** –
A byte is stuffed in the message to differentiate from the delimiter. This is also called character-oriented framing. **Disadvantage –** It is very costly and obsolete method.	A pattern of bits of arbitrary length is stuffed in the message to differentiate from the delimiter. This is also called bit – oriented framing.



ERROR DETECTION

A condition when the receiver's information does not match with the sender's information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from sender to receiver.

That means a 0 bit may change to 1 or a 1 bit may change to 0.

Error Detecting Codes (Implemented either at Data link layer or Transport Layer of OSI Model)

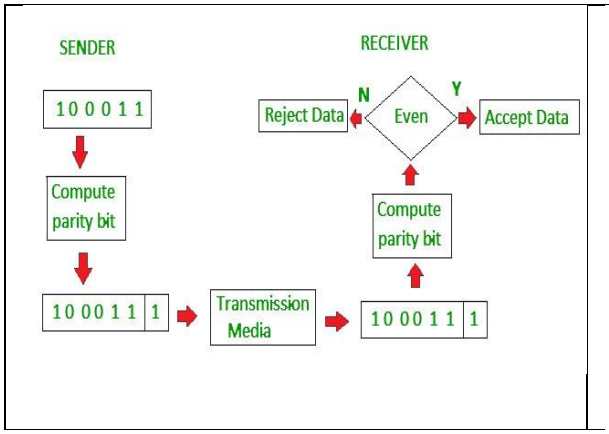
Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the message.

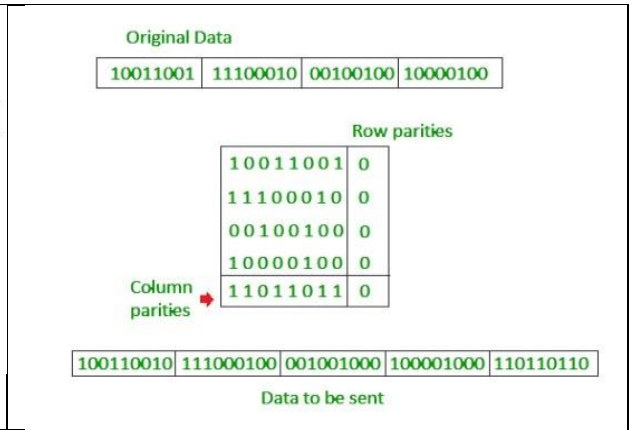
Basic approach used for error detection is the use of redundancy bits, where additional bits are added to facilitate detection of errors.

Some popular techniques for error detection are:

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

Simple Parity check	**Two-dimensional Parity check**
Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of : • 1 is added to the block if it contains odd number of 1's, and • 0 is added if it contains even number of 1's This scheme makes the total number of 1's even, that is why it is called even parity checking.	Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, and then both are sent along with the data. At the receiving end these are compared with the parity bits calculated on the received data.





Checksum

In checksum error detection scheme, IT IS BASED ON REDUNANCY

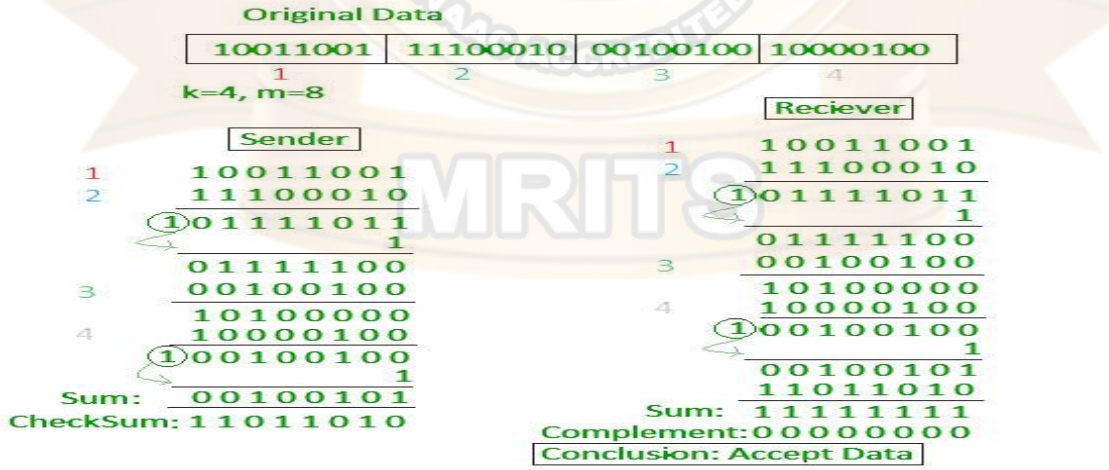
TYPES	
CHECK SUM GENERATOR	CHECKSUM CHECKER

A) Checksum generator

It can be done only on sender's side
The data is divided into k segments each of m bits.
In the sender's end the segments are added using 1's complement arithmetic to get the sum.
The sum is complemented to get the checksum.
The checksum segment is sent along with the data segments.

B) Checksum checker

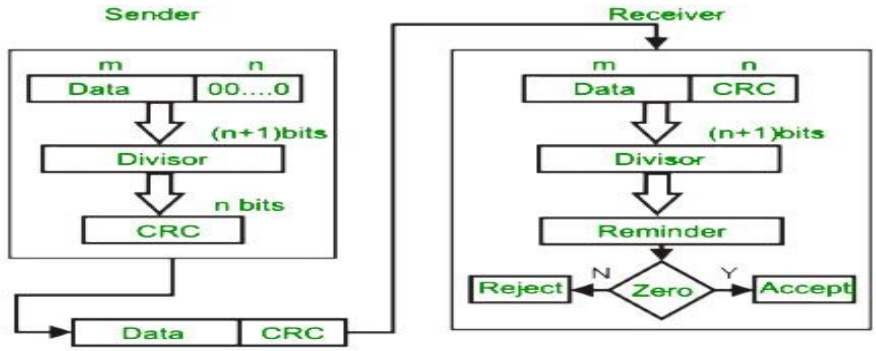
At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum.
The sum is complemented.
If the result is zero, the received data is accepted; otherwise discarded.



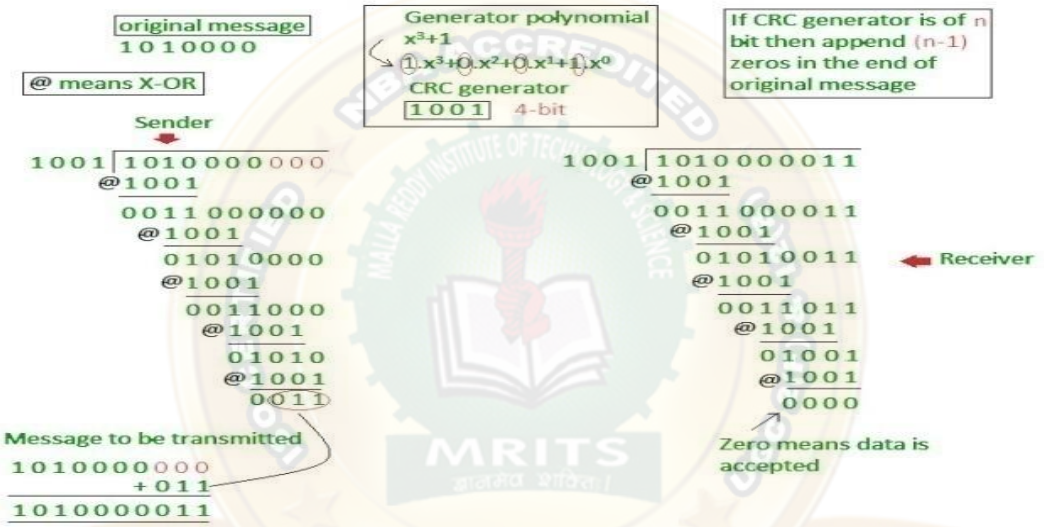
Cyclic redundancy check (CRC)

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

- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.



Example :



The remainder is 0 indicates the data is not corrupted

If the remainder is 1 indicates data is corrupted then data need to re-transmit again & again

ERROR CORRECTION

Error Correction codes are used to detect and repair mistakes that occur during data transmission from the transmitter to the receiver.

There are two approaches to error correction:

1. Backward Error Correction:

When a backward mistake is detected, the receiver requests that the sender retransmit the complete data unit.

2. Forward Error Correction:

In this scenario, the error-correcting code is used by the receiver, which automatically corrects the mistakes.

A single extra bit can identify but not repair the mistake.

To correct the mistakes, the specific location of the error must be known. If we wish to compute a single-bit mistake, for example, the error correcting algorithm will identify which one of seven bits is incorrect. We will need to add some more redundant bits to do this.

The number of redundant bits is calculated using the following formula:

$2^r >= d+r+1$

The above formula is used to compute the value of r. For example, if the value of d is 4, the least possible number that fulfils the above relation is 3.

Error Correction Techniques:

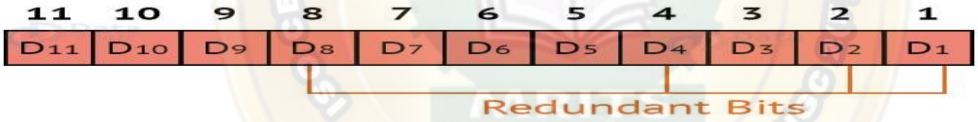
Hamming Code:

- **Parity bits:** A bit that is added to the original binary data to make sure the total number of 1s is even or odd (in case of even or odd parity respectively).

- **Even parity:** To check for even parity, if the total number of 1s is even, the parity bit value is 0. If the total number of occurrences of 1s is odd, the parity bit value is 1.
- **Odd Parity:** To test for odd parity, if the total number of 1s is even, the parity bit value is 1. If the total number of 1s is odd, the parity bit value is 0.

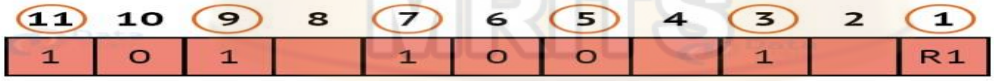
To produce d+r, an information of 'd' bits is added to the redundant bits 'r'.
Each (d+r) digit's position is assigned a decimal value.
The 'r' bits are assigned to locations 1, 2,….2k-1.
The parity bits are recalculated at the receiving end. The position of an error is determined by the decimal value of the parity bits.
Example: If the data to be transmitted is 1011001

Number of data bits = 7
Thus, number of redundancy bits = 4
Total bits = 7+4 = 11
Redundant bits are always placed at positions that correspond to the power of 2, so the redundant bits will be placed at positions: 1,2,4 and 8.
Redundant bits will be placed here:

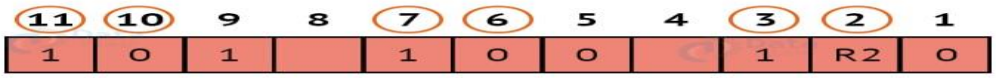


Thus now, all the 11 bits will look like this:

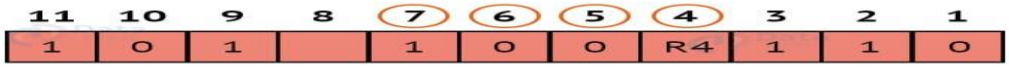
Here, R1, R2, R4 and R8 are the redundant bits.
Determining the parity bits:
R1:



We look at bits 1,3,5,7,9,11 to calculate R1. In this case, because the number of 1s in these bits together is even, we make the R1 bit equal to 0 to maintain even parity.
R2:

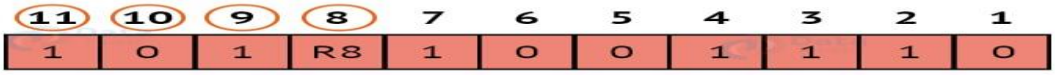


We look at bits 2,3,6,7,10,11 to calculate R2. In this case, because the number of 1s in these bits together is odd, we make the R2 bit equal to 1 to maintain even parity.
R4:

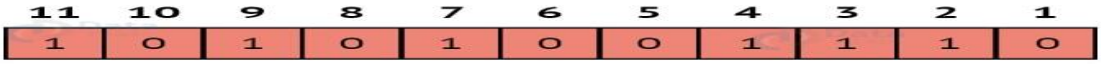


We look at bits 4,5,6,7 to calculate R4. In this case, because the number of 1s in these bits together is odd, we make the R4 bit equal to 1 to maintain even parity.

R8:



We look at bits 8,9,10,11 to calculate R8. In this case, because the number of 1s in these bits together is even, we make the R8 bit equal to 0 to maintain even parity.
Thus, the final block of data which is transferred looks like this:



Summary:
We looked at the concepts of error detection and error correction, and the various techniques used in both these concepts. We also looked at the detailed explanation of the Hamming Code method which is the most popular method for error correction, as well as some popular methods for error detection such as Cyclic Redundancy Check, Parity Check etc.

Elementary data link 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.

Types of Data Link Protocols

Data link protocols can be broadly divided into two categories, depending on whether the transmission channel is noiseless or noisy.

1) **Noise-less channel**

An idealistic channel, in which no frames are lost, corrupted or duplicated.
The protocol does not implement error control in this category.
There are two protocols for the noiseless channel as follows.

(A)Simplex protocol

The Simplex protocol is data link layer protocol for transmission of frames over computer network.

It is hypothetical protocol designed for unidirectional data transmission over an ideal channel, i.e. a channel through which transmission can never go wrong.

It is assumed that both the sender and the receiver are always ready for data processing and both of them have infinite buffer.

The sender simply sends all its data available onto the channel as soon as they are available its buffer.

The receiver is assumed to process all incoming data instantly.

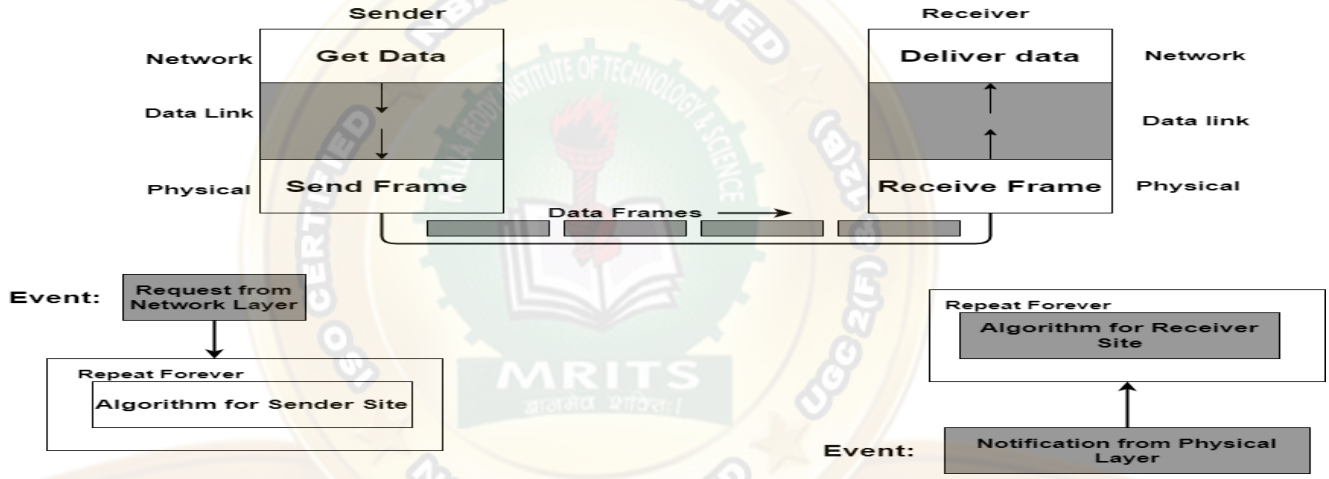
It is does not handle flow control or error control.

Since this protocol is totally unrealistic, it is often called Utopian Simplex protocol.

The significance of this protocol lies in the fact that it shows the basic structure on which the usable protocols are built upon.

Design

- **Sender Site**: The data link layer in the sender site waits for the network layer to send a data packet. On receiving the packet, it immediately processes it and sends it to the physical layer for transmission.
- **Receiver Site**: The data link layer in the receiver site waits for a frame to be available. When it is available, it immediately processes it and sends it to the network layer.



The procedure used by the data link layer

The procedure used by the data link layer at both sides (sender as well as the receiver).

- There is no frame send by the data link layer of the sender site until its network layer has a data packet to send.
- Similarly, the receiver site cannot deliver a data packet to its network layer until a frame arrives.
- The procedure at the sender site runs constantly; there is no action until there is a request from the network layer.
- Also, the procedure at the receiver site runs constantly; there is no action until there is a notification from the physical layer.
- Both the procedure runs continuously because either of them doesn't know when the corresponding events will occur.

Sender-site algorithm –	**Receiver's algorithm –**

while (true) //Repeat forever
{
Wait_For_Event();
// sleep until there is occurrence of an event
if(Event(Request_To_Send))
	while(true) //Repeat forever
	{
	waitForEvent(); //sleep until an event occur
	if(Event(ArrivalNotification)) //data frame arrived
	{

// means there is a packet to send
{
Get_Data();
Make_Frame();
Send_Frame(); // send the frame
}
}
	ReceiveFrame();
	ExtractData();
	DeliverData(); //Deliver data to network layer
	}
	}

Flow Diagram for Simplest Protocol

This Flow Diagram shows an example of communication using the simplest protocol. It is very straightforward. The sender sends a series of frames without further consideration about the receiver. Let's take an example, three frames will send from the sender, and three frames received by receivers. Bear in mind the data frames are shown by tilted boxes; the height of the box defines the transmission time difference between the first bit and the last bit in the frame.

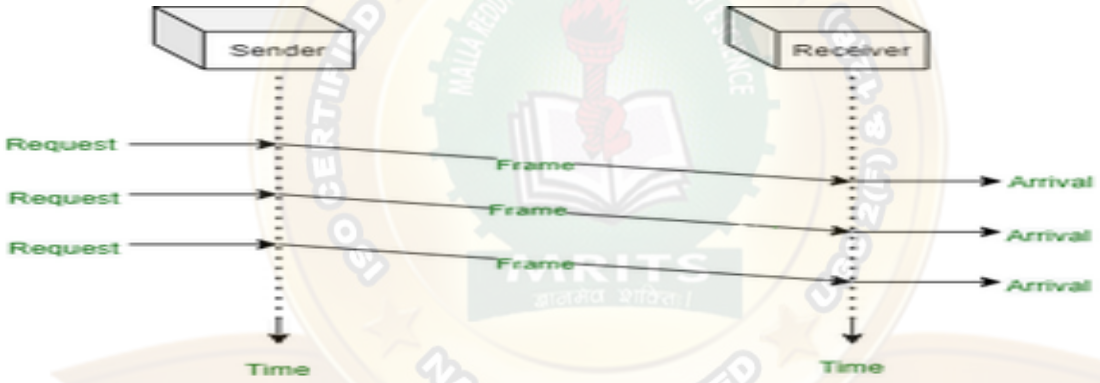


Fig: *Flow Diagram for Simplex Protocol*

(B)STOP - & - WAIT PROTOCOL

Here stop and wait means, whatever the data that sender wants to send, he sends the data to the receiver.

After sending the data, he stops and waits until he receives the acknowledgment from the receiver.

The stop and wait protocol is a flow control protocol where flow control is one of the services of the data link layer.

It is a data-link layer protocol which is used for transmitting the data over the noiseless channels.

It provides unidirectional data transmission which means that either sending or receiving of data will take place at a time.

It provides flow-control mechanism but does not provide any error control mechanism.

The idea behind the usage of this frame is that when the sender sends the frame then he waits for the acknowledgment before sending the next frame.

Primitives of Stop and Wait Protocol

Sender side

Rule 1: Sender sends one data packet at a time.

Rule 2: Sender sends the next packet only when it receives the acknowledgment of the previous packet.

Therefore, the idea of stop and wait protocol in the sender's side is very simple, i.e., send one packet at a time, and do not send another packet before receiving the acknowledgment.

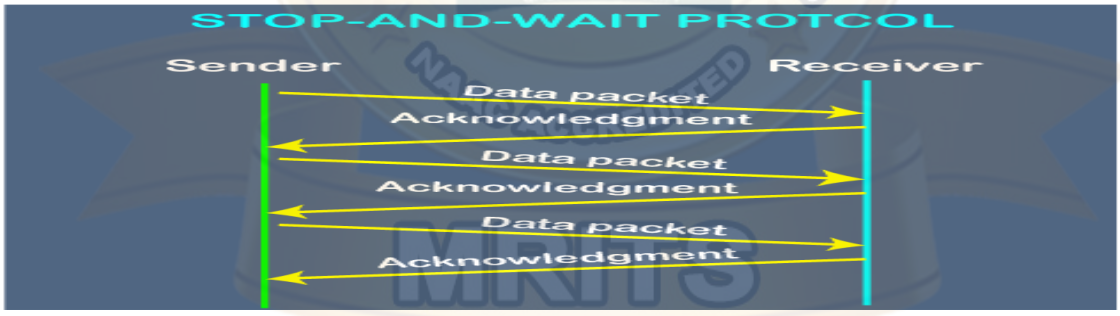
Receiver side

Rule 1: Receive and then consume the data packet.

Rule 2: When the data packet is consumed, receiver sends the acknowledgment to the sender.

Therefore, the idea of stop and wait protocol in the receiver's side is also very simple, i.e., consume the packet, and once the packet is consumed, the acknowledgment is sent. This is known as a flow control mechanism

Working of Stop and Wait protocol



If there is a sender and receiver, then sender sends the packet and that packet is known as a data packet.

The sender will not send the second packet without receiving the acknowledgment of the first packet.

The receiver sends the acknowledgment for the data packet that it has received. Once the acknowledgment is received, the sender sends the next packet.

This process continues until all the packet are not sent.

The main advantage of this protocol is its simplicity but it has some disadvantages also.

For example, if there are 1000 data packets to be sent, then all the 1000 packets cannot be sent at a time as in Stop and Wait protocol, one packet is sent at a time.

Design

- **Sender Site**:

  The data link layer in the sender site waits for the network layer for a data packet.

  It then checks whether it can send the frame. If it receives a positive notification from the physical layer, it makes frames out of the data and sends it.

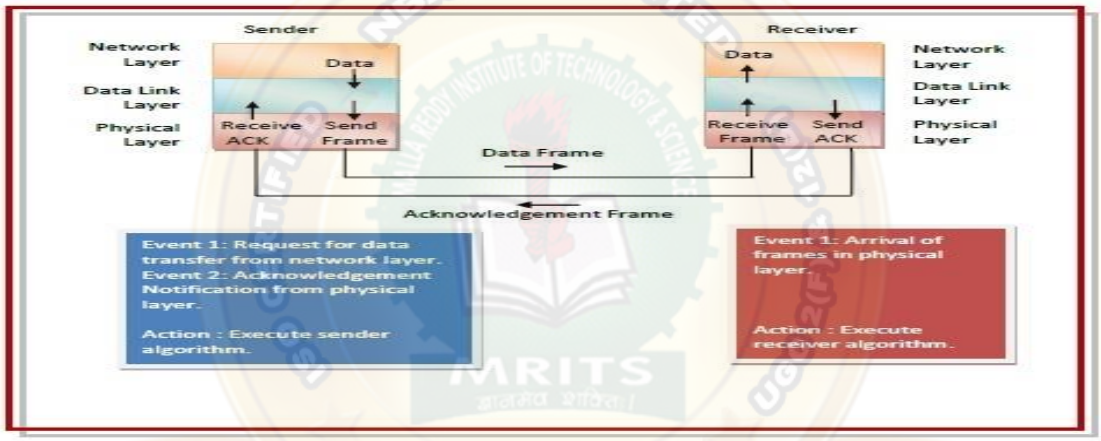
  It then waits for an acknowledgement before sending the next frame.

- **Receiver Site**:

  The data link layer in the receiver site waits for a frame to arrive.

  When it arrives, the receiver processes it and delivers it to the network layer.

  It then sends an acknowledgement back to the sender.



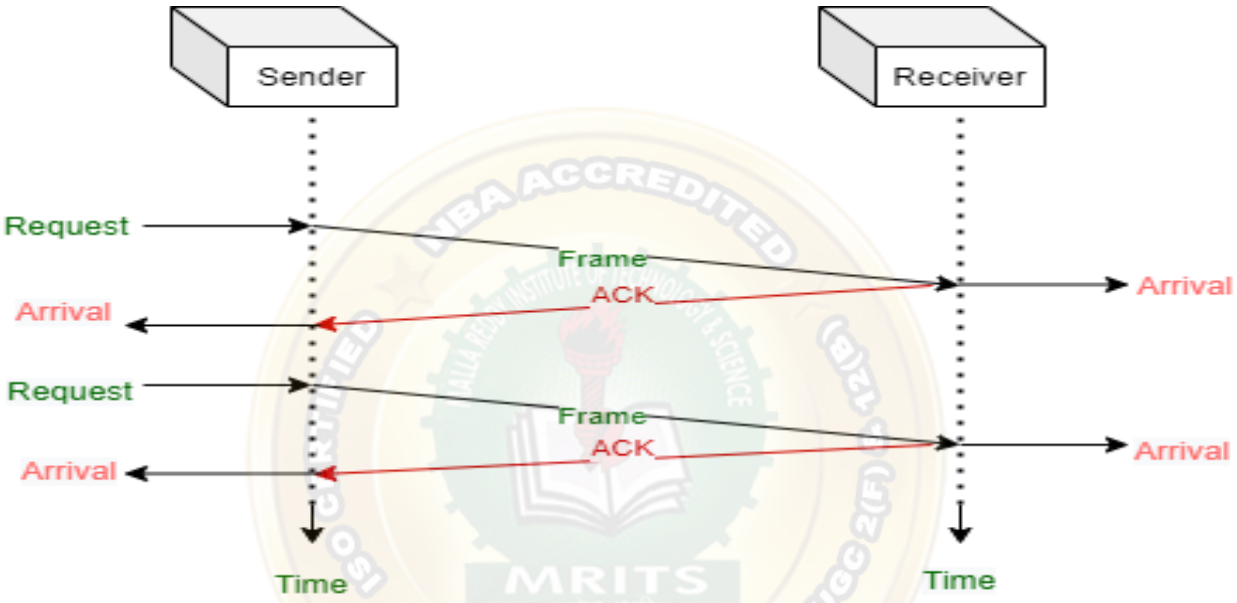
Sender-site and Receivers algorithms:

Sender-site algorithm	**Receiver's algorithm**

while(true)
//Repeat forever
canSend = true
// Allow the first frame to go
{
waitForEvent();
//sleep until an event occur
if (Event(RequestToSend)AND canSend)
//there is a packet to send
{
GetData();
MakeFrame();
SendFrame();
//send the data frame
canSend = false;
//cannot send until ACK arrives
}
WaitForEvent();
//sleep until an event occurs
if(Event(ArrivalNotification))
	while(true)
	//Repeat forever
	{
	waitForEvent();
	//sleep until an event occur
	if (Event(ArrivalNotification)
	//data frame arrives
	{
	ReceiveFrame();
	ExtractData();
	DeliverData();
	//Deliver data to network layer
	SendFrame();
	//Send an ACK frame
	}
	}

//An ACK has arrived
{
ReceiveFrame();
//Receive the ACK frame
CanSend = true;
}	

Flow Diagram



2) Noisy channel or Sliding window protocol

Sliding window protocol is also known as noisy channel are DLL for reliable and sequential delivery of data frames.

The sliding window is also used in Transmission Control Protocol.
In this protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgment from the receiver.
The term sliding window refers to the imaginary boxes to hold frames.
Sliding window method is also known as windowing.
(Or)

The sliding window is a technique for sending multiple frames at a time.

It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed.

It is also used in TCP (Transmission Control Protocol).

In this technique, each frame has sent from the sequence number.

The sequence numbers are used to find the missing data in the receiver end.

The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

Working Principle

In these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window.

The size of the sending window determines the sequence number of the outbound frames.

If the sequence number of the frames is an n-bit field, then the range of sequence numbers that can be assigned is 0 to 2^n-1.

Consequently, the size of the sending window is 2^n-1.

Thus in order to accommodate a sending window size of 2^n-1, a n-bit sequence number is chosen.

The sequence numbers are numbered as modulo-n.

For example, if the sending window size is 4, then the sequence numbers will be 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, and so on.

The number of bits in the sequence number is 2 to generate the binary sequence 00, 01, 10, 11.

The size of the receiving window is the maximum number of frames that the receiver can accept at a time.

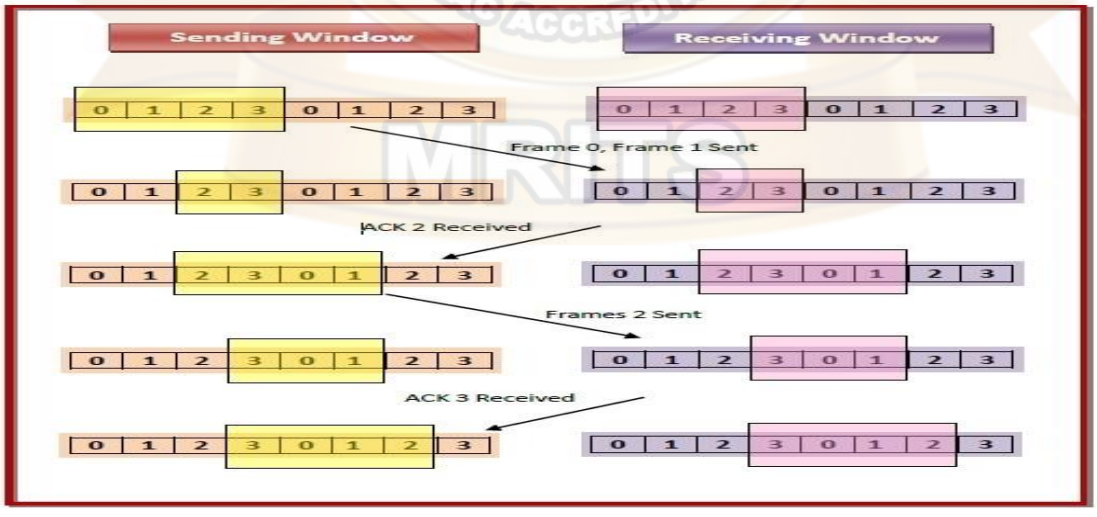
It determines the maximum number of frames that the sender can send before receiving acknowledgment.

Example

Suppose that we have sender window and receiver window each of size 4.

So the sequence numbering of both the windows will be 0,1,2,3,0,1,2 and so on.

The following diagram shows the positions of the windows after sending the frames and receiving acknowledgments.



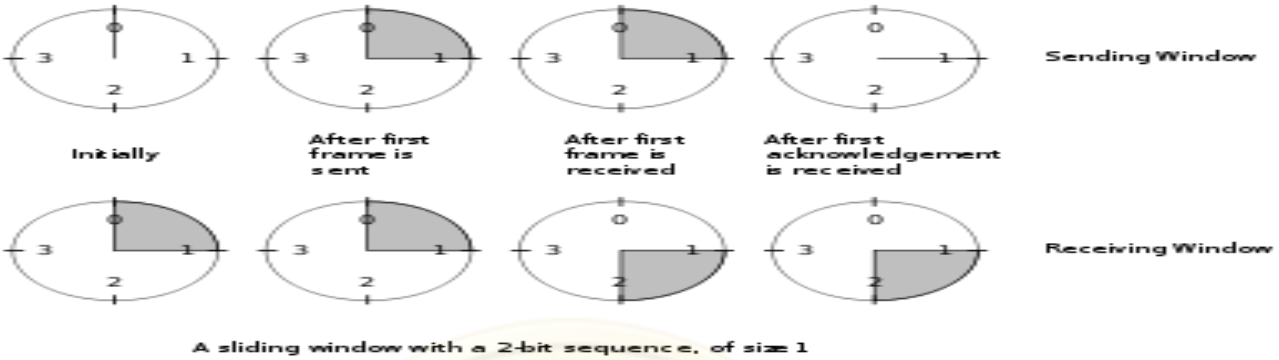
Types of Sliding Window Protocols

The Sliding Window ARQ (Automatic Repeat Request) protocols are of 3 categories –

SLIDING WINDOW PROTOCOL

STOP & WAIT ARQ	GO BACK N ARQ	SELECTIVE REPEAT ARQ

Fig; Types of sliding window protocol



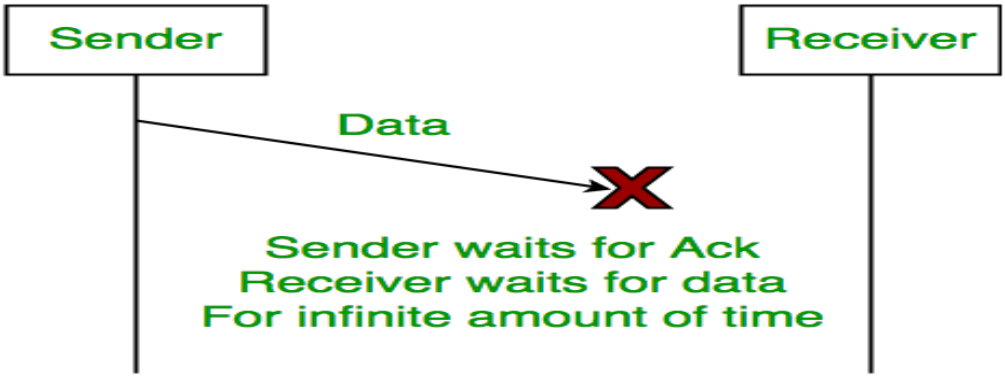
A Simplex Stop-and-Wait Protocol for a Noisy Channel

The Stop-and-Wait Automatic Repeat Request (Stop-and-Wait ARQ), adds a simple error control mechanism to the Stop-and-Wait Protocol.
To detect and correct corrupted frames, we need to add redundancy bits to our data frame.
When the frame arrives at the receiver site, it is checked and if it is corrupted, it is silently discarded.
The detection of errors in this protocol is manifested by the silence of the receiver.
FLOW CONTROL = It tells sender how much data should be sent to the receiver so that it is not lost. This mechanism makes the sender wait for an ACK before sending the next data
ERROR CONTROL = To ensure that the information received by receiver is exact information transmitted by sender
As we know that stop & wait protocol in noiseless channel:

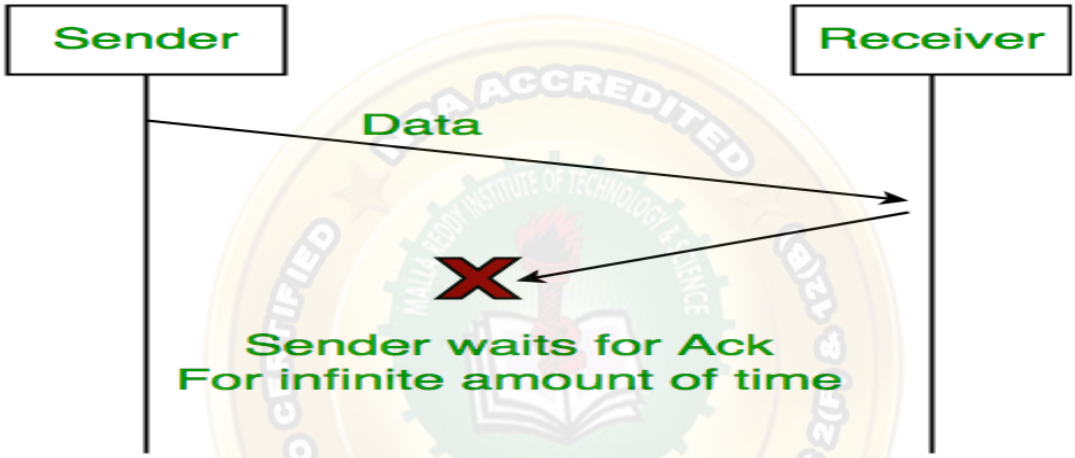
1) Sender sends packet 1 & then wait for Ack from receiver
2) After getting Ack from receiver then sender sends packet 2 to receiver & so on

Here problems facing stop & wait protocol are:

1. **Lost Data**



2. **Lost Acknowledgement:**



3. **Delayed Acknowledgement/Data:**

After a timeout on the sender side, a long-delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet.

Here we use atop & wait ARQ to solve all problems in stop & wait protocol:

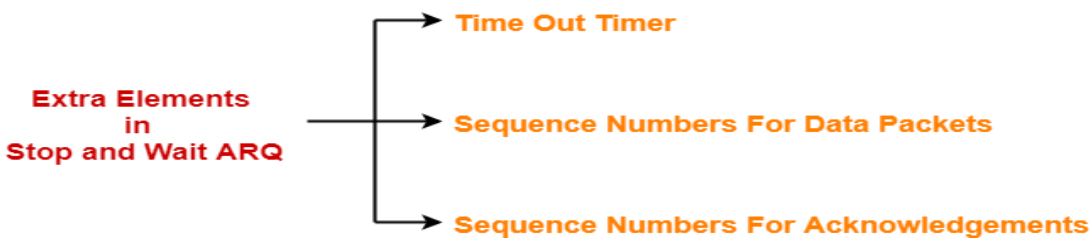
Stop & wait ARQ is an improved & modified version of stop & wait protocol

Stop and Wait ARQ assumes-

- The communication channel is noisy.
- Errors may get introduced in the data during the transmission.

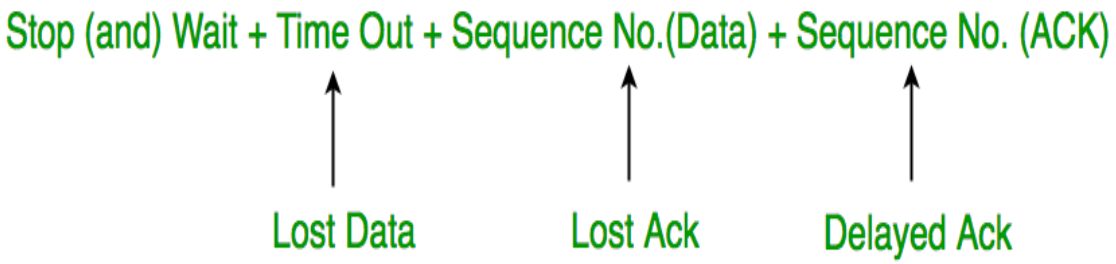
Working-

- Stop and wait ARQ works similar to stop and wait protocol.
- It provides a solution to all the limitations of stop and wait protocol.
- Stop and wait ARQ includes the following three extra elements.



Thus, we can say-

Stop and Wait ARQ
= Stop and Wait Protocol + Time Out Timer + Sequence Numbers for Data Packets and Acknowledgements



Number of Sequence Numbers Required-

NOTE
For any sliding window protocol to work without any problem,
the following condition must be satisfied-
Available Sequence Numbers >= Sender Window Size + Receiver Window Size

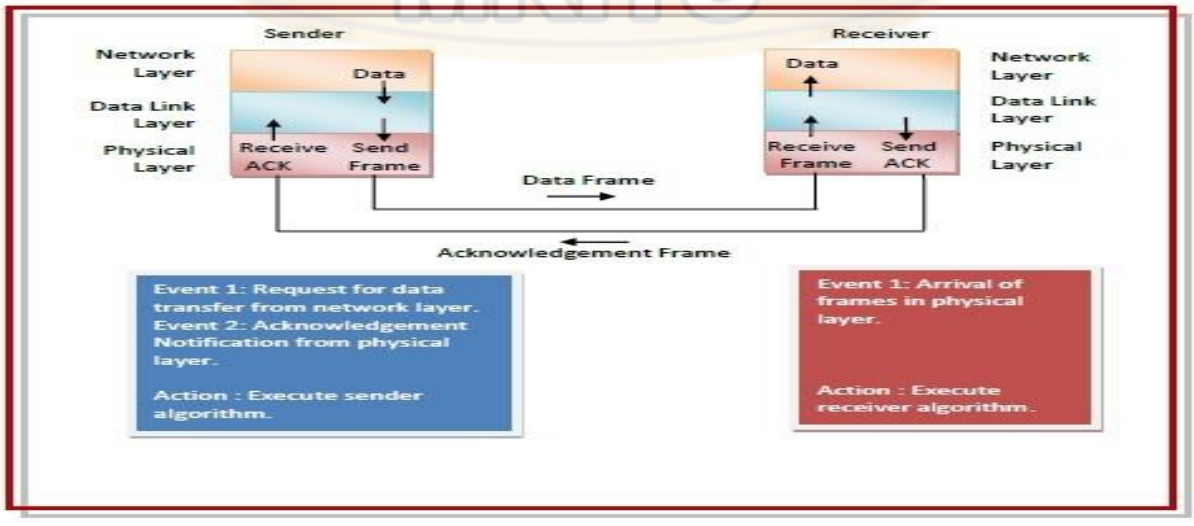
Stop and wait ARQ is a one bit sliding window protocol where-

- Sender window size = 1
- Receiver window size = 1

Thus, in stop and wait ARQ,
Minimum number of sequence numbers required
= Sender Window Size + Receiver Window Size
= 1 + 1
= 2
Thus,

- Minimum number of sequence numbers required in Stop and Wait ARQ = 2.
- The two sequence numbers used are 0 and 1.

Design:

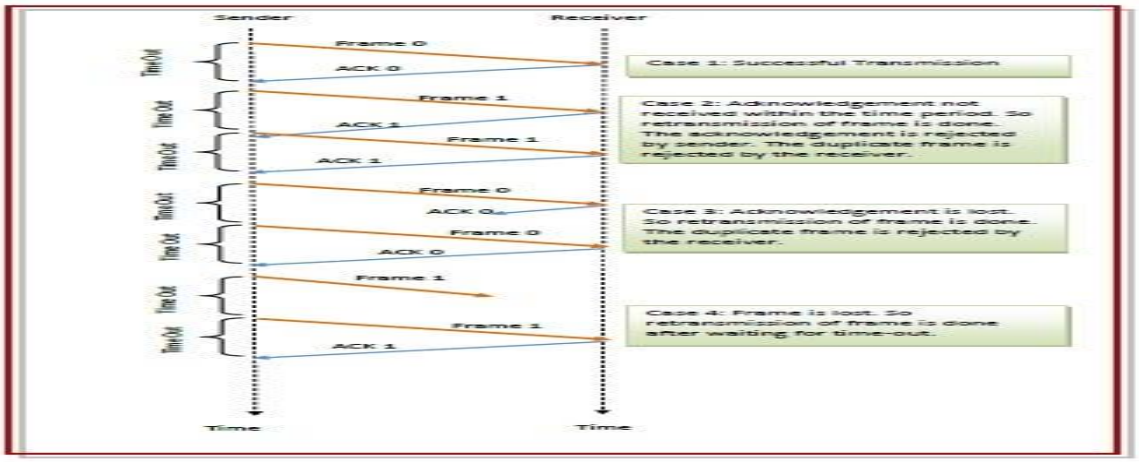


Algorithm for STOP & WAIT ARQ:

Sender site:	Receiver site:

begin
SeqNo = 0;
// Initialise sequence number of outbound frame
canSend = True;
//Allow the first frame to be sent
while (true)
//check repeatedly
do
Wait_For_Event();
//wait for availability of packet
if(Event(Request_For_Transfer) AND canSend) then
Get_Data_From_Network_Layer();
frame = Make_Frame(SeqNo);
Store_Copy_Frame(frame.SeqNo);
Send_Frame_To_Physical_Layer(frame.SeqNo);
Start_Timer(frame.SeqNo);
SeqNo = SeqNo + 1;
canSend = False;
else if (Event(Acknowledgement_Arrival)) then
Receive_ACK();
if (ACK_No = SeqNo) then
Stop_Timer (frame.SeqNo);
canSend = True;
end if
else if (Event(Timer > Max_time)) then
Resend_Frame_To_Physical_Layer(frame.SeqNo-1);
Start_Timer(frame.SeqNo-1);
end if
end while
end
	begin
	RSeqNo = 0;
	// Initialise sequence number of expected frame
	while (true)
	//check repeatedly
	do
	Wait_For_Event();
	//wait for arrival of frame
	if (Event(Frame_Arrival) then
	Receive_Frame_From_Physical_Layer();
	if (Corrupted (frame.SeqNo)
	doNothing();
	else if(frame.SeqNo = RSeqNo) then
	Extract_Data();
	Deliver_Data_To_Network_Layer();
	RSeqNo = RSeqNo + 1;
	end if
	Send_ACK(ACKframe[RSeqNo]);
	end if
	end while
	end

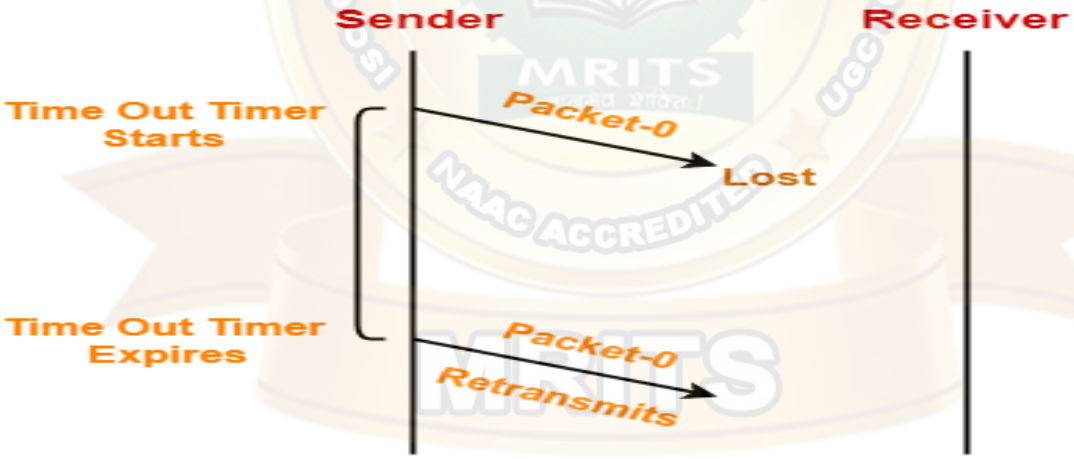
FLOW DIAGRAM:



How Stop and Wait ARQ Solves All Problems?

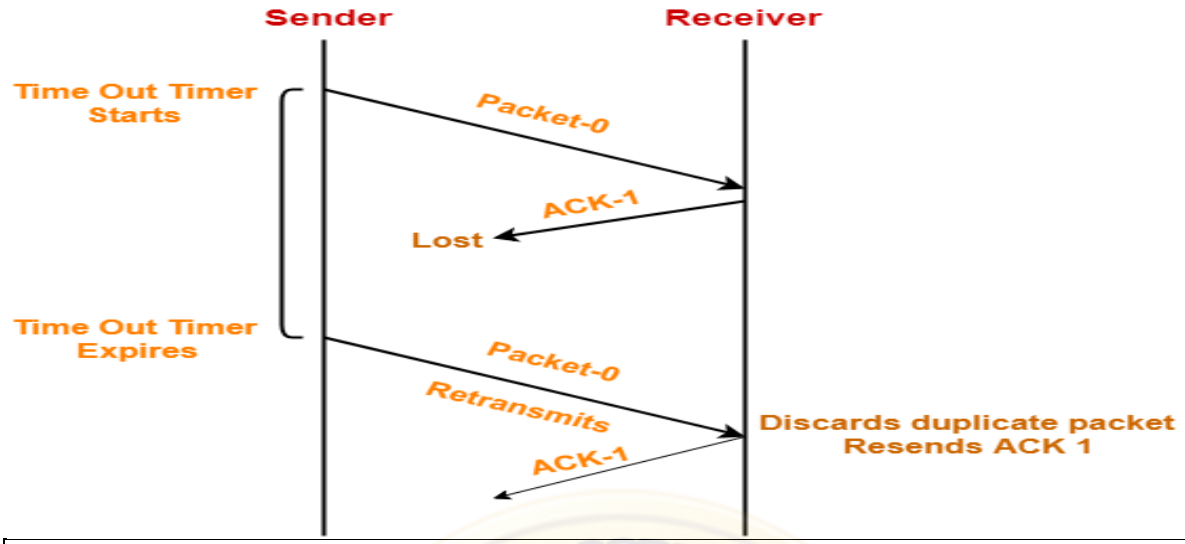
1. Problem of Lost Data Packet-

- Time out timer helps to solve the problem of lost data packet.
- After sending a data packet to the receiver, sender starts the time out timer.
- If the data packet gets acknowledged before the timer expires, sender stops the time out timer.
- If the timer goes off before receiving the acknowledgement, sender retransmits the same data packet.
- After retransmission, sender resets the timer.
- This prevents the occurrence of deadlock.



2. Problem of Lost Acknowledgement-

- Sequence number on data packets help to solve the problem of delayed acknowledgement.
- Consider the acknowledgement sent by the receiver gets lost.
- Then, sender retransmits the same data packet after its timer goes off.
- This prevents the occurrence of deadlock.
- The sequence number on the data packet helps the receiver to identify the duplicate data packet.
- Receiver discards the duplicate packet and re-sends the same acknowledgement.



Role of Sequence Number on Data Packets

Consider the above example-

Step-01:

Sender sends a data packet with sequence number-0 to the receiver.

Step-02:

Receiver receives the data packet correctly.

Receiver now expects data packet with sequence number-1.

Receiver sends the acknowledgement ACK-1.

Step-03:

Acknowledgement ACK-1 sent by the receiver gets lost on the way.

Step-04:

Sender receives no acknowledgement and time out occurs.

Sender retransmits the same data packet with sequence number-0.

This will be a duplicate packet for the receiver.

Step-05:

Receiver receives the data packet and discovers it is the duplicate packet.

It expects the data packet with sequence number-1 but receiving the data packet with sequence number-0.

It discards the duplicate data packet and re-sends acknowledgement ACK-1.

ACK-1 requests the sender to send a data packet with sequence number-1.

This avoids the inconsistency of data.

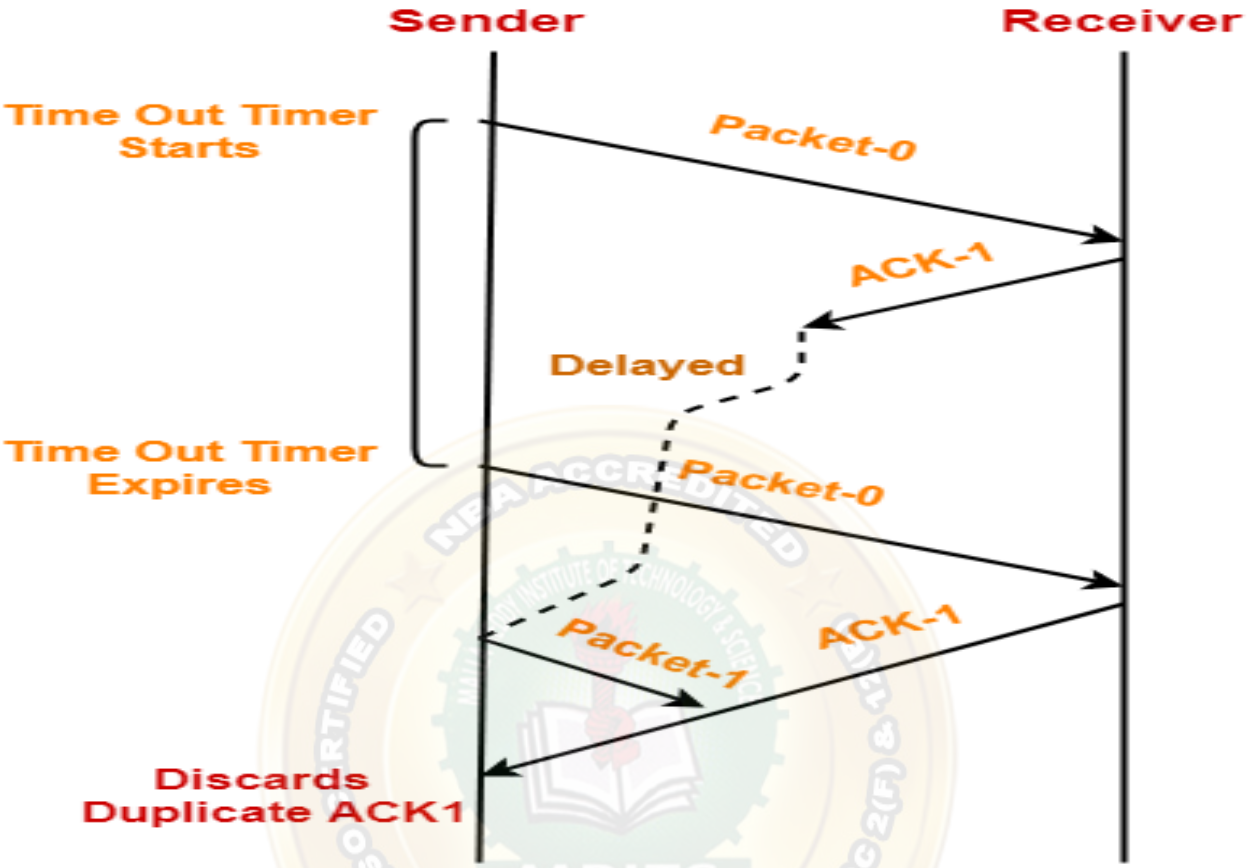
Conclusion-

Had the sequence numbers not been allotted to the data packets, receiver would have accepted the duplicate data packet thinking of it as the new data packet.

This is how sequence numbers allotted to the data packets prove to be useful for identifying the duplicate data packets and discarding them.

4. **Problem of Delayed Acknowledgement-**

Sequence number on acknowledgements help to solve the problem of delayed acknowledgement.



Role of Sequence Number on Acknowledgements

Consider the above example-

Step-01:

Sender sends a data packet with sequence number-0 to the receiver.

Step-02:

Receiver receives the data packet correctly.

Receiver now expects data packet with sequence number-1.

Receiver sends the acknowledgement ACK-1.

Step-03:

Acknowledgement ACK-1 sent by the receiver gets delayed in reaching the sender.

Step-04:

Sender receives no acknowledgement and time out occurs.

Sender retransmits the same data packet with sequence number-0.

This will be a duplicate packet for the receiver.

Step-05:

Receiver receives the data packet and discovers it is the duplicate packet.

It expects the data packet with sequence number-1 but receiving the data packet with sequence number-0.

It discards the duplicate data packet and re-sends acknowledgement ACK-1. ACK-1 requests the sender to send a data packet with sequence number-1.

Step-06:

Two acknowledgements ACK1 reaches the sender.

When first acknowledgement ACK1 reaches the sender, sender sends the next data packet with sequence number 1.

When second acknowledgement ACK1 reaches the sender, sender rejects the duplicate acknowledgement.

This is because it has already sent the data packet with sequence number-1 and now sender expects the acknowledgement with sequence number 0 from the receiver.

Conclusion-

Had the sequence numbers not been allotted to the acknowledgements, sender would have accepted the duplicate acknowledgement thinking of it as the new acknowledgement for the latest data packet sent by it.

This is how sequence numbers allotted to the acknowledgements prove to be useful for identifying duplicate acknowledgements and discarding them.

5. Problem of Damaged Packet-

- If receiver receives a corrupted data packet from the sender, it sends a negative acknowledgement (NAK) to the sender.
- NAK requests the sender to send the data packet again.

Limitation of Stop and Wait ARQ-

The major limitation of Stop and Wait ARQ is its very less efficiency.

To increase the efficiency, protocols like **Go back N** and **Selective Repeat** are used.

Characteristics

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

Useful Terms:

- **Propagation Delay:** Amount of time taken by a packet to make a physical journey from one router to another router.

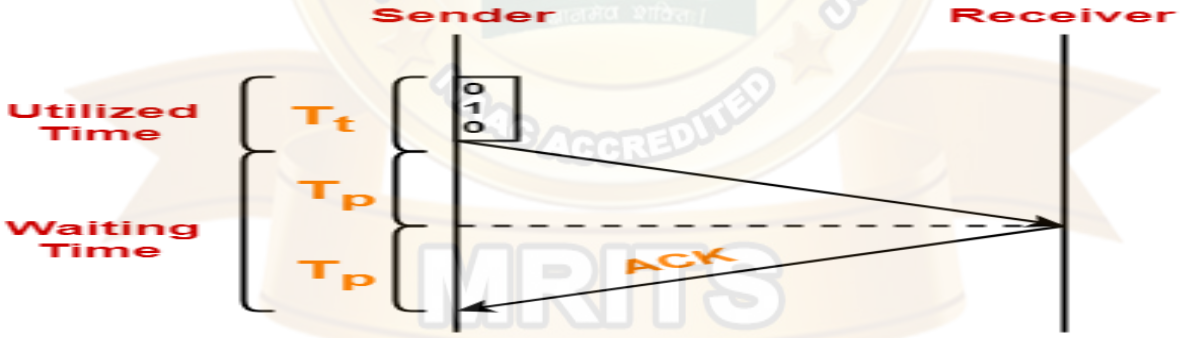
Propagation Delay = (Distance between routers) / (Velocity of propagation)

- **RoundTripTime** (**RTT**) = 2* Propagation Delay
- **TimeOut** (**TO**) = 2* RTT
- **Time To Live** (**TTL**) = 2* TimeOut. (Maximum TTL is 180 seconds)

Explanation-

In stop and wait ARQ,

- Sender window size is 1.
- This allows the sender to keep only one frame unacknowledged.
- So, sender sends one frame and then waits until the sent frame gets acknowledged.
- After receiving the acknowledgement from the receiver, sender sends the next frame.



Here,

- Sender uses T_t time for transmitting the packet over the link.
- Then, sender waits for 2 x T_p time.
- After 2 x T_p time, sender receives the acknowledgement for the sent frame from the receiver.
- Then, sender sends the next frame.
- This 2 x T_p waiting time is the actual cause of less efficiency.

Efficiency Improvement-

- The efficiency of stop and wait ARQ can be improved by increasing the window size.
- This allows the sender to keep more than one unacknowledged frame in its window.
- Thus, sender can send frames in the waiting time too.

One bit sliding window protocol

In previous, we have discussed about sliding window protocol

One bit sliding window protocol is based on the concept of sliding window protocol.

But here the window size is of 1 bit.

1. One bit sliding window protocol is used for delivery of data frames.
2. Sender has sending window.
3. Receiver has receiving window.
4. Sending and receiving windows act as buffer storage.
5. Here size of windows size is 1.
6. One bit sliding window protocol uses Stop and Wait.
7. Sender transmits a frame with sequence number.
8. Than sender wait for acknowledgment from the receiver.
9. Receiver sends back an acknowledgement with sequence number.
10. If sequence number of acknowledgement matches with sequence number of frame.
11. Sender transmits the next frame.
12. Else sender re-transmits the previous frame.
13. Its bidirectional protocol.

Algorithm of One-bit sliding window protocol is as follows:

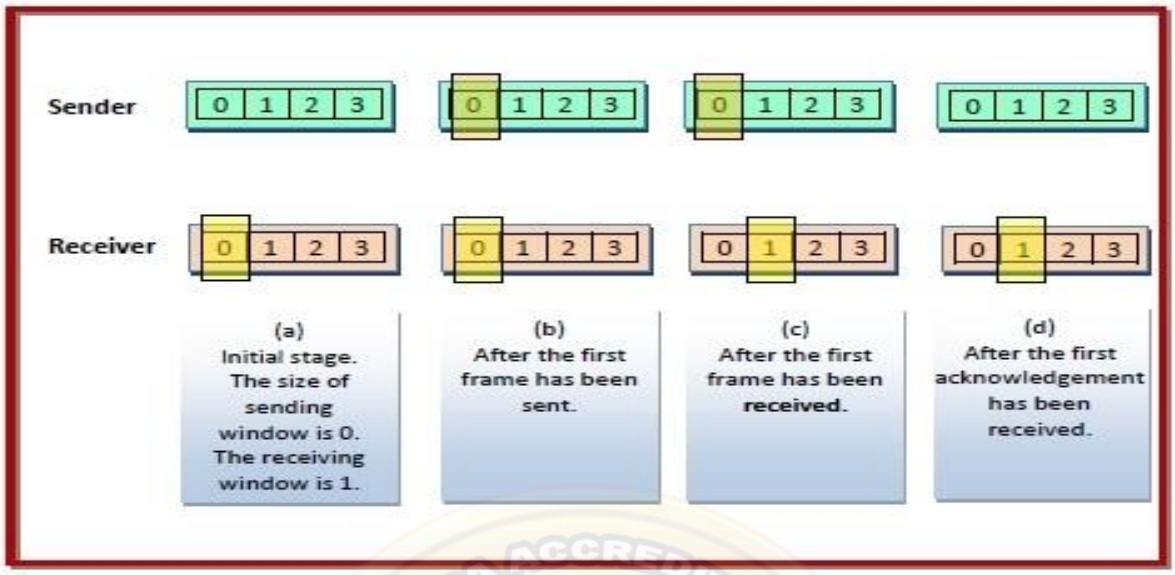
Algorithm:

```
begin
frame s, r;
//s and r denotes frames to be sent and received
SeqNo = 0;
// Initialise sequence number of outbound frame
RSeqNo = 0;
// Initialise sequence number of expected frame
while (true)
//check repeatedly
do
Wait_For_Event();
//wait for availability of packet
if ( Event(Request_For_Transfer) AND canSend) then
Get_Data_From_Network_Layer();
```

```
s = Make_Frame(SeqNo);
Store_Copy_Frame(s);
Start_Timer(s);
SeqNo = SeqNo + 1;
end if;
Wait_For_Event();
//wait for arrival of frame
if ( Event(Frame_Arrival) then
r = Receive_Frame_From_Physical_Layer();
if ( r.SeqNo = RSeqNo ) then
Extract_Data(r);
Deliver_Data_To_Network_Layer(r);
Stop_Timer(r);
RSeqNo = RSeqNo + 1;
end if
end if
s.ack = r.SeqNo;
Send_Frame_To_Physical_Layer(s);
Start_Timer(s);
SeqNo = SeqNo + 1;
end while
end
```

Illustrative Example

The following diagram depicts a scenario with sequence numbers 0, 1, 2, 3, 0, 1, 2 and so on. It depicts the sliding windows in the sending and the receiving stations during frame transmission.



A Protocol Using Go-Back-N

Go-Back-N protocol, also called Go-Back-N Automatic Repeat Request.

It is a data link layer protocol that uses a sliding window method for reliable and sequential delivery of data frames.

It is a case of sliding window protocol having to send window size of N and receiving window size of 1.

GO-BACK-N ARQ employs the protocol pipelining idea, in which numerous frames can be delivered before getting acknowledgment of the first frame.

For example - If we have 5 frames and the window size is 3, then frame 1, frame 2, and frame 3 can be sent before anticipating the acknowledgment of frame

Sender Site Algorithm	**Receiver Site Algorithm**

begin
frame s;
//s denotes frame to be sent
frame t;
//t is temporary frame
S_window = power(2,m) – 1;
//Assign maximum window size
SeqFirst = 0;
// Sequence number of first frame in window
SeqN = 0;
// Sequence number of Nth frame window
	Begin
	frame f;
	RSeqNo = 0;
	// Initialise sequence number of expected frame
	while (true) //check repeatedly
	do
	Wait_For_Event(); //wait for arrival of frame
	if (Event(Frame_Arrival) then
	Receive_Frame_From_Physical_Layer();
	if (Corrupted (f.SeqNo)
	doNothing();

```
while(true)
//check repeatedly
do
Wait_For_Event();
//wait for availability of packet
if( Event(Request_For_Transfer)) then
//check if window is full
if(SeqN–SeqFirst>=S_window) then
doNothing();
end if;
Get_Data_From_Network_Layer();
s = Make_Frame();
s.seq = SeqN;
Store_Copy_Frame(s);
Send_Frame(s);
Start_Timer(s);
SeqN = SeqN + 1;
end if;
if(Event(Frame_Arrival) then
r = Receive_Acknowledgement();
if(AckNo > SeqFirst && AckNo < SeqN )
then
while(SeqFirst <= AckNo )
Remove_copy_frame(s.seq(SeqFirst));
SeqFirst = SeqFirst + 1;
end while
Stop_Timer(s);
end if
end if
// Resend all frames if acknowledgement havn't been received
if(Event(Time_Out)) then
TempSeq = SeqFirst;
while(TempSeq < SeqN)
t = Retrieve_Copy_Frame(s.seq(SeqFirst));
```

```
else if ( f.SeqNo = RSeqNo ) then
Extract_Data();
Deliver_Data_To_Network_Layer();
RSeqNo = RSeqNo + 1;
Send_ACK(RSeqNo);
end if
end if
end while
end
```

```
Send_Frame(t);
Start_Timer(t);
TempSeq = TempSeq + 1;
end while
end if
end
```

Working Principle

Go – Back – N ARQ provides for sending multiple frames before receiving the acknowledgment for the first frame.

The frames are sequentially numbered and a finite number of frames.

The maximum number of frames that can be sent depends upon the size of the sending window.

If the acknowledgment of a frame is not received within an agreed upon time period, all frames starting from that frame are retransmitted.

Suppose there are a sender and a receiver, and let's assume that there are 11 frames to be sent.

These frames are represented as 0,1,2,3,4,5,6,7,8,9,10, and these are the sequence numbers of the frames.

Mainly, the sequence number is decided by the sender's window size.

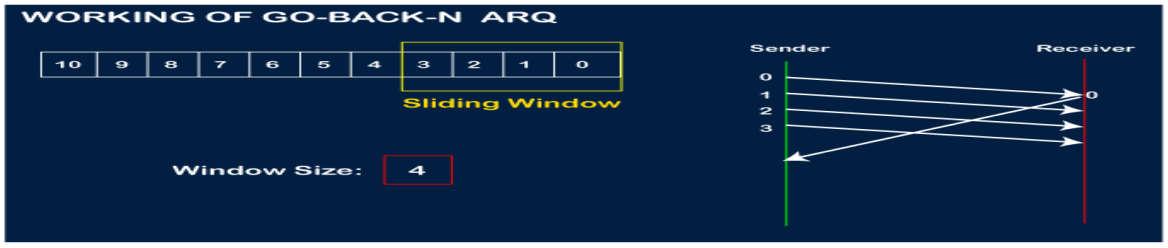
But, for the better understanding, we took the running sequence numbers, i.e., 0,1,2,3,4,5,6,7,8,9,10.

Let's consider the window size as 4, which mean that the four frames can be sent at a time before expecting the acknowledgment of the first frame.

Step 1:

Firstly, the sender will send the first four frames to the receiver, i.e., 0,1,2,3, and now the sender is expected to receive the acknowledgment of the 0^{th} frame.

Let's assume that the receiver has sent the acknowledgment for the 0 frame, and the receiver has successfully received it.



The sender will then send the next frame, i.e., 4, and the window slides containing four frames (1,2,3,4).

The receiver will then send the acknowledgment for the frame no 1.

After receiving the acknowledgment, the sender will send the next frame, i.e., frame no 5, and the window will slide having four frames (2,3,4,5).

Now, let's assume that the receiver is not acknowledging the frame no 2, either the frame is lost, or the acknowledgment is lost.

Instead of sending the frame no 6, the sender Go-Back to 2, which is the first frame of the current window, retransmits all the frames in the current window, i.e., 2,3,4,5.

Important points related to Go-Back-N ARQ:

- In Go-Back-N, N determines the sender's window size, and the size of the receiver's window is always 1.
- It does not consider the corrupted frames and simply discards them.
- It does not accept the frames which are out of order and discards them.
- If the sender does not receive the acknowledgment, it leads to the retransmission of all the current window frames.

Example for Go-Back-N ARQ is as follows:

Let's understand the Go-Back-N ARQ through an example.

Example 1: In GB4, if every 6th packet being transmitted is lost and if we have to spend 10 packets then how many transmissions are required?

Solution: Here, GB4 means that N is equal to 4. The size of the sender's window is 4.

Step 1:

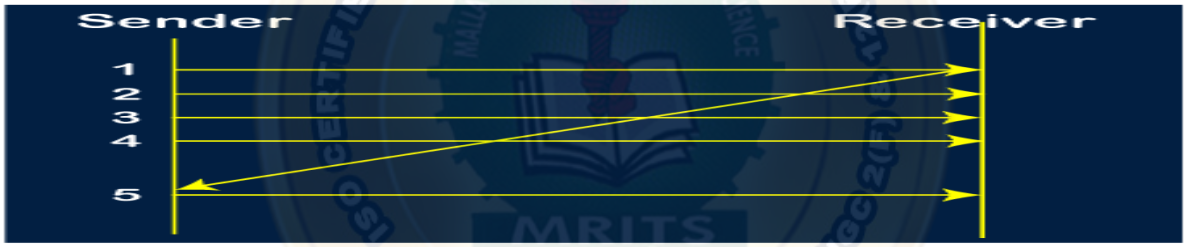
As the window size is 4, so four packets are transferred at a time, i.e., packet no 1, packet no 2, packet no 3, and packet no 4.

Step 2:

Once the transfer of window size is completed, the sender receives the acknowledgment of the first frame, i.e., packet no1.

As the acknowledgment receives, the sender sends the next packet, i.e., packet no 5.

In this case, the window slides having four packets, i.e., 2,3,4,5 and excluded the packet 1 as the acknowledgment of the packet 1 has been received successfully.

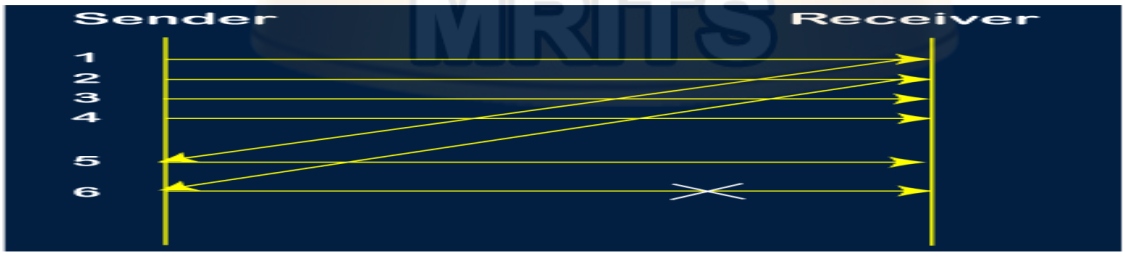


Step 3:

Now, the sender receives the acknowledgment of packet 2.

After receiving the acknowledgment for packet 2, the sender sends the next packet, i.e., packet no 6.

As mentioned in the question that every 6th is being lost, so this 6th packet is lost, but the sender does not know that the 6th packet has been lost.

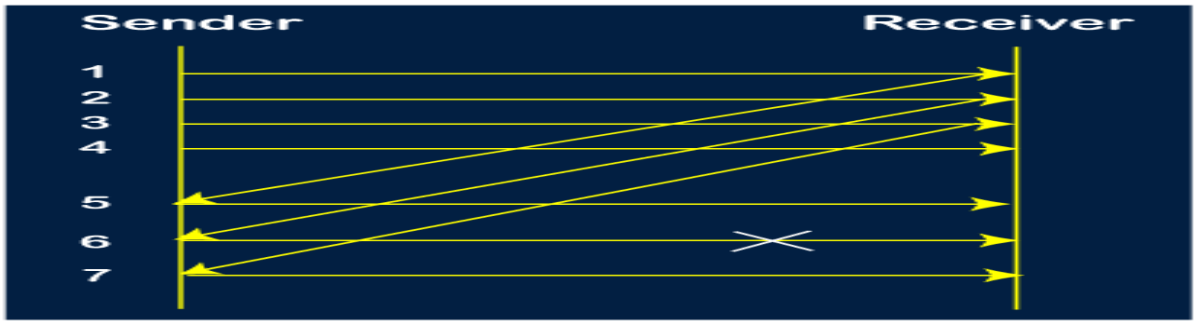


Step 4:

The sender receives the acknowledgment for the packet no 3.

After receiving the acknowledgment of 3rd packet, the sender sends the next packet, i.e., 7th packet.

The window will slide having four packets, i.e., 4, 5, 6, 7.

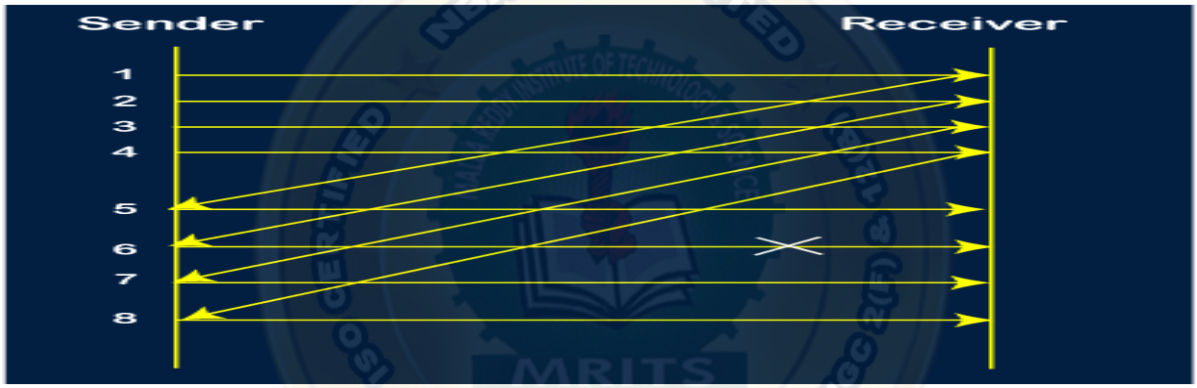


Step 5:

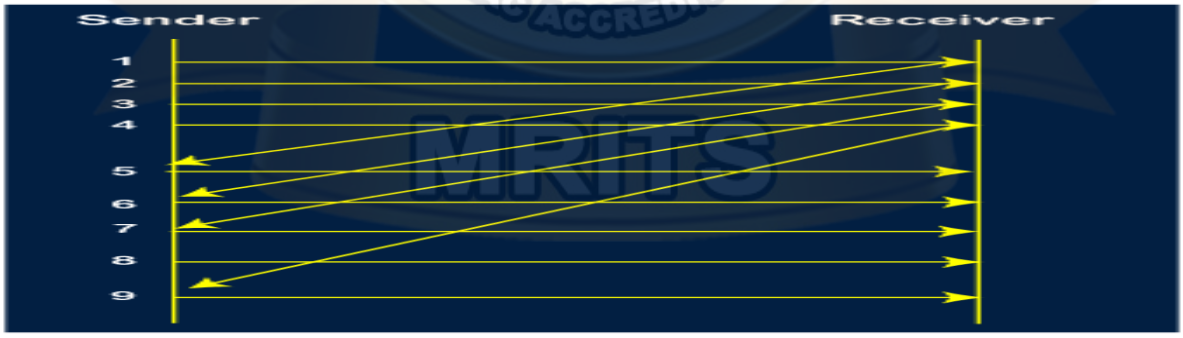
When the packet 7 has been sent, then the sender receives the acknowledgment for the packet no 4.

When the sender has received the acknowledgment, then the sender sends the next packet, i.e., the 8^{th} packet.

The window will slide having four packets, i.e., 5, 6, 7, 8.



Step 6: When the packet 8 is sent, then the sender receives the acknowledgment of packet 5. On receiving the acknowledgment of packet 5, the sender sends the next packet, i.e., 9^{th} packet. The window will slide having four packets, i.e., 6, 7, 8, 9.



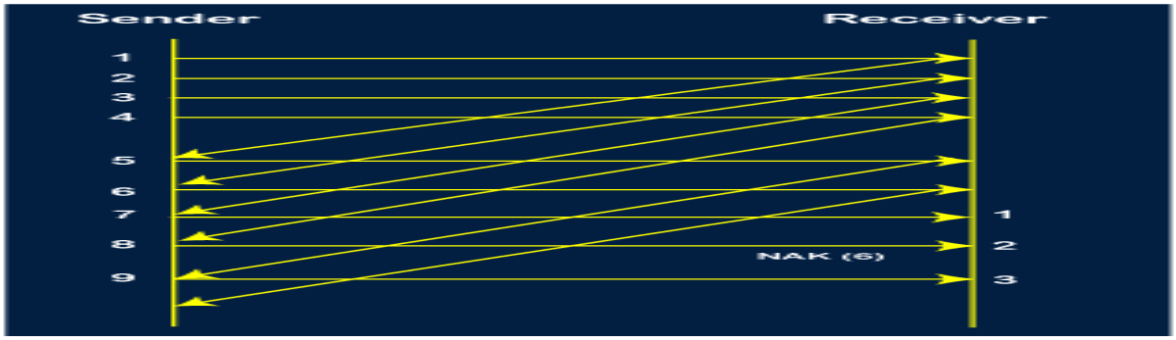
Step 7:

The current window is holding four packets, i.e., 6, 7, 8, 9, where the 6^{th} packet is the first packet in the window.

As we know, the 6^{th} packet has been lost, so the sender receives the negative acknowledgment NAK(6).

As we know that every 6^{th} packet is being lost, so the counter will be restarted from 1.

So, the counter values 1, 2, 3 are given to the 7^{th} packet, 8^{th} packet, 9^{th} packet respectively.

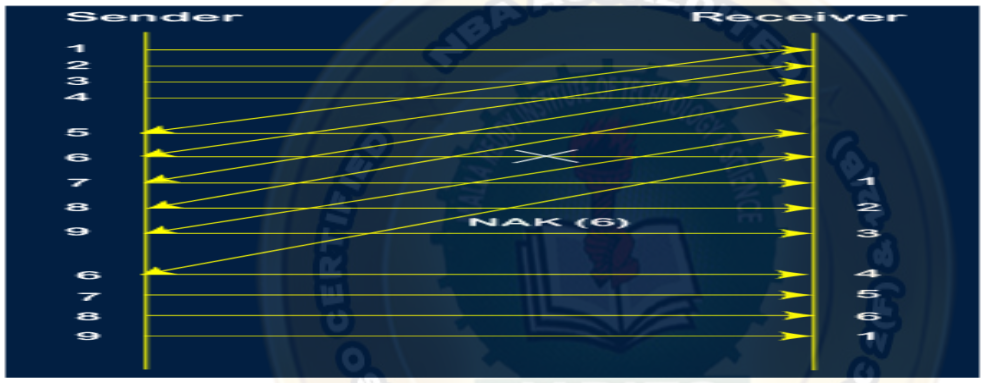


Step 8:

As it is Go-BACK, so it retransmits all the packets of the current window.

It will resend 6, 7, 8, 9. The counter values of 6, 7, 8, 9 are 4, 5, 6, 1, respectively.

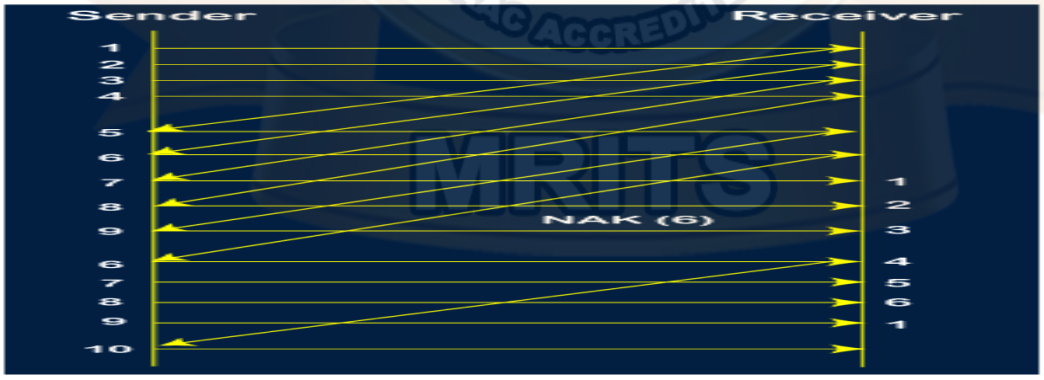
In this case, the 8th packet is lost as it has a 6-counter value, so the counter variable will again be restarted from 1.



Step 9: After the retransmission, the sender receives the acknowledgment of packet 6.

On receiving the acknowledgment of packet 6, the sender sends the 10th packet.

Now, the current window is holding four packets, i.e., 7, 8, 9, 10.

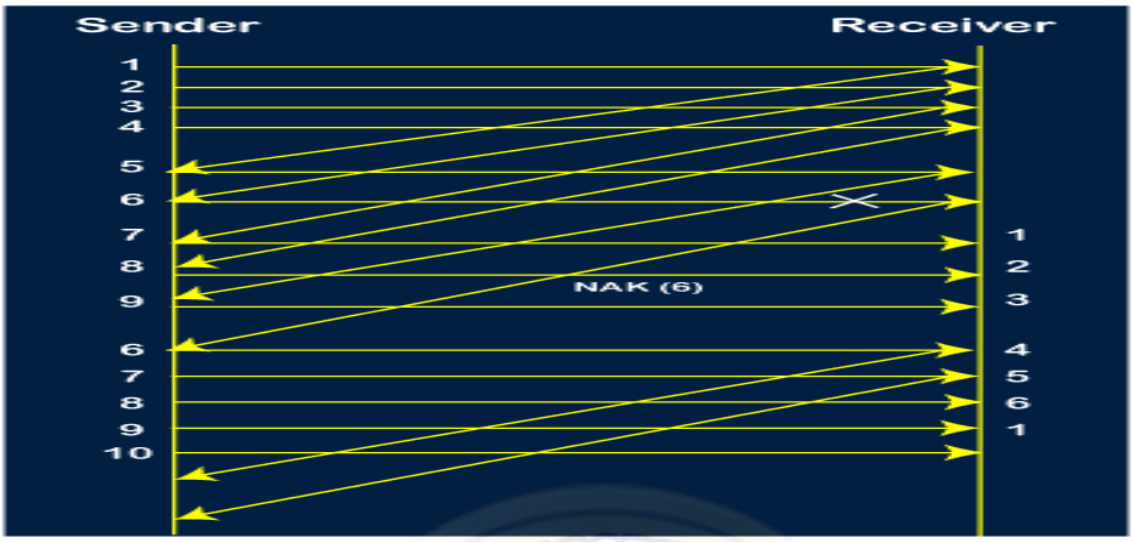


Step 10:

When the 10th packet is sent, the sender receives the acknowledgment of packet 7.

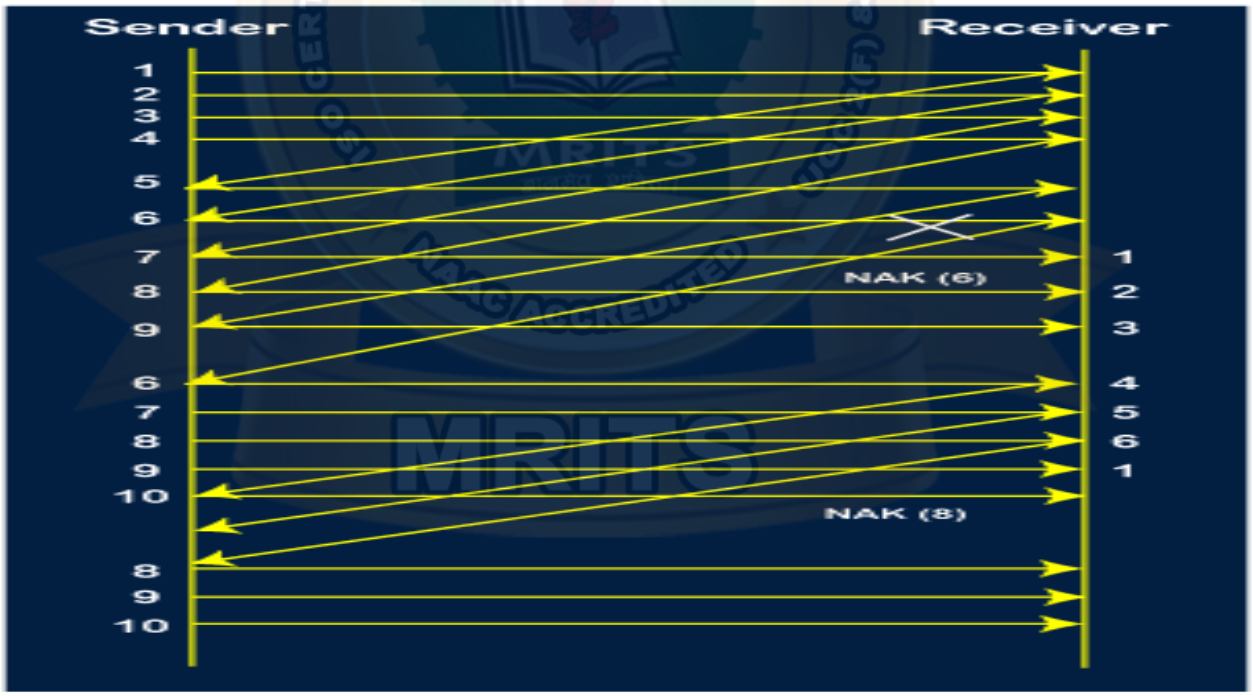
Now the current window is holding three packets, 8, 9 and 10.

The counter values of 8, 9, 10 are 6, 1, 2.



Step 11: As the 8th packet has 6 counter values which means that 8th packet has been lost, and the sender receives NAK (8).

Step 12: Since the sender has received the negative acknowledgment for the 8th packet, it resends all the packets of the current window, i.e., 8, 9, 10.



Step 13:

The counter values of 8, 9, 10 are 3, 4, 5, respectively, so their acknowledgments have been received successfully.

We conclude from the above figure that total 17 transmissions are required.

A Protocol Using Selective Repeat

Selective repeat protocol, also called Selective Repeat ARQ (Automatic Repeat Request).

Selective-repeat ARQ is one of the techniques where a data link layer may deploy to control errors.

Requirements for Error Control

Some requirements for error control mechanisms as follows −

- **Error detection** –

  The sender and receiver, or any must ascertain that there is some error in the transit.

- **Positive ACK** –

  Whenever a receiver receives a correct frame, it should acknowledge it.

- **Negative ACK** –

  Whenever the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and sender must retransmit the correct frame.

- **Retransmission** –

  The sender always maintains a clock and sets a timeout period. If an ACK of data-frame previously transmitted does not arrive before the timeout, the sender retransmits the frame, thinking that the frame or it's ACK is lost in transit

Sender Site Algorithm

```
begin
frame s;
//s denotes frame to be sent
frame t; //t is temporary frame
S_window = power(2,m-1); //Assign maximum window size
SeqFirst = 0; / Sequence no. of first frame in window
SeqN = 0;
// Sequence no. of Nth frame window
while(true) //check repeatedly
do
Wait_For_Event(); //wait for availability of packet
if(Event(Request_For_Transfer)) then //check if window is full
if(SeqN–SeqFirst >= S_window) then
doNothing();
end if;
Get_Data_From_Network_Layer();
s = Make_Frame();
s.seq = SeqN;
Store_Copy_Frame(s);
Send_Frame(s);
Start_Timer(s);
```

```
SeqN = SeqN + 1;
end if;
if ( Event(Frame_Arrival) then
r = Receive_Acknowledgement();
//Resend frame whose sequence number is with ACK
if ( r.type = NAK) then
if ( NAK_No > SeqFirst && NAK_No < SeqN ) then
Retransmit( s.seq(NAK_No));
Start_Timer(s);
end if //Remove frames from sending window with positive ACK
else if ( r.type = ACK ) then
Remove_Frame(s.seq(SeqFirst));
Stop_Timer(s);
SeqFirst = SeqFirst + 1;
end if
end if // Resend frame if acknowledgement haven't been received
if ( Event(Time_Out)) then
Start_Timer(s);
Retransmit_Frame(s);
end if
end
```

Receiver Site Algorithm

```
Begin
frame f;
RSeqNo = 0;
// Initialise sequence number of expected frame
NAKsent = false;
ACK = false;
For each slot in receive_window
Mark(slot)=false;
while (true) //check repeatedly
do
Wait_For_Event();
//wait for arrival of frame
if ( Event(Frame_Arrival) then
```

```
Receive_Frame_From_Physical_Layer();
if ( Corrupted ( f.SeqNo ) AND NAKsent = false) then
SendNAK(f.SeqNo);
NAKsent = true;
end if
if ( f.SeqNo != RSeqNo AND NAKsent = false ) then
SendNAK(f.SeqNo);
NAKsent = true;
if ( f.SeqNo is in receive_window ) then
if ( Mark(RSeqNo) = false ) then
Store_frame(f.SeqNo);
Mark(RSeqNo) = true;
end if
end if
else
while ( Mark(RSeqNo))
Extract_Data(RSeqNo);
Deliver_Data_To_Network_Layer();
RSeqNo = RSeqNo + 1;
Send_ACK(RSeqNo);
end while
end if
end if
end while
end
```

Working Principle:

It is also known as Sliding Window Protocol and used for error detection and control in the data link layer.

In the selective repeat, the sender sends several frames specified by a window size even without the need to wait for individual acknowledgement from the receiver as in Go-Back-N ARQ.

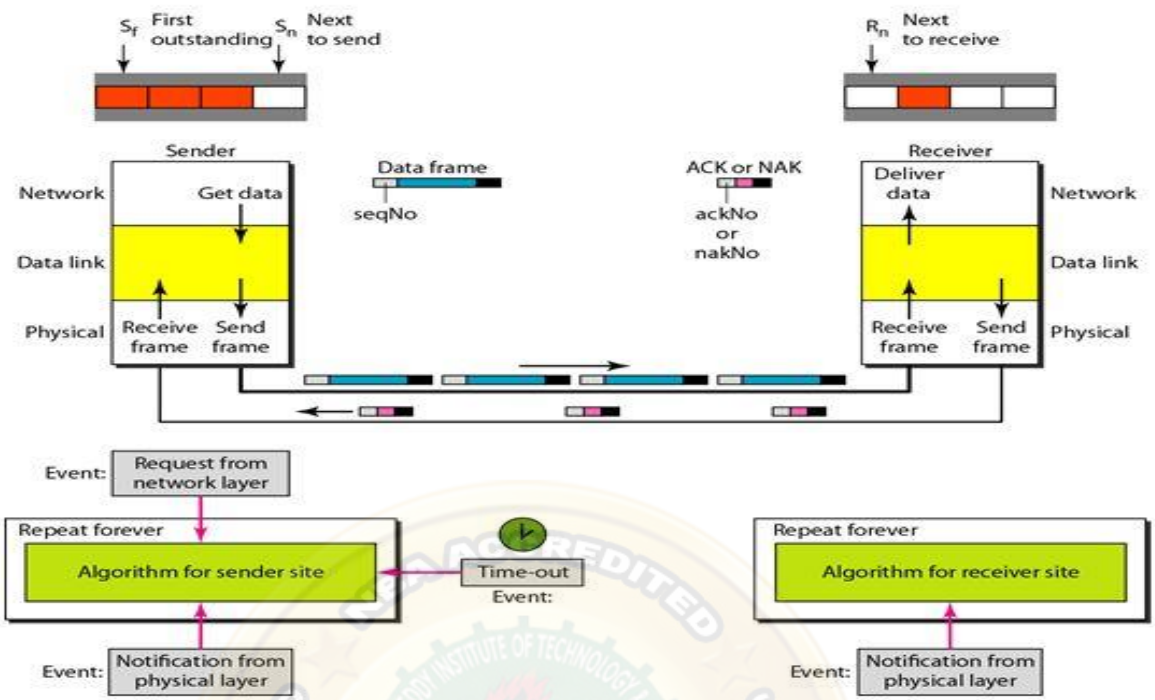
In selective repeat protocol, the retransmitted frame is received out of sequence.

In Selective Repeat ARQ only the lost or error frames are retransmitted, whereas correct frames are received and buffered.

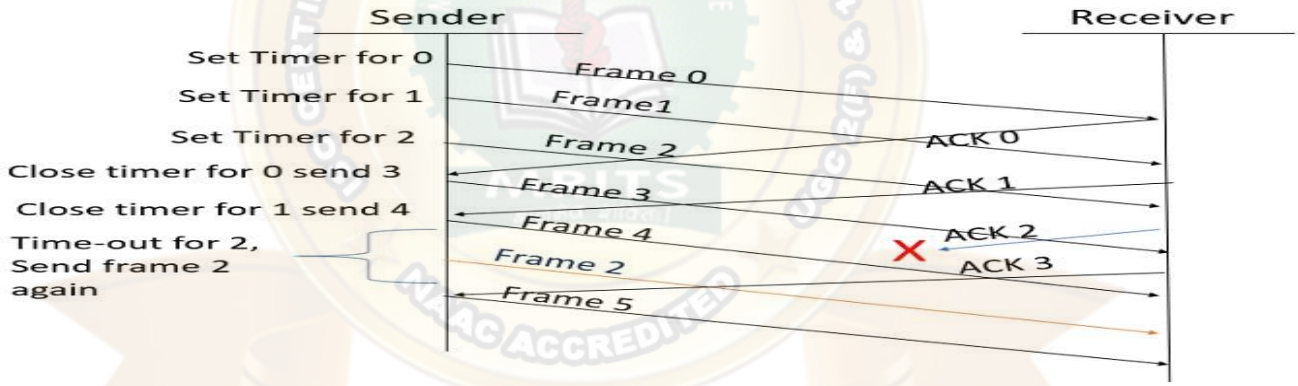
The receiver while keeping track of sequence numbers buffers the frames in memory and sends NACK for only frames which are missing or damaged.

The sender will send/retransmit a packet for which NACK is received.

Design issues:



Example: Given below is an example of the Selective Repeat ARQ −



Explanation

Step 1 – Frame 0 sends from sender to receiver and set timer.

Step 2 – Without waiting for acknowledgement from the receiver another frame, Frame1 is sent by sender by setting the timer for it.

Step 3 – In the same way frame2 is also sent to the receiver by setting the timer without waiting for previous acknowledgement.

Step 4 – Whenever sender receives the ACK0 from receiver, within the frame 0 timer then it is closed and sent to the next frame, frame 3.

Step 5 − whenever the sender receives the ACK1 from the receiver, within the frame 1 timer then it is closed and sent to the next frame, frame 4.

Step 6 – If the sender doesn't receive the ACK2 from the receiver within the time slot, it declares timeout for frame 2 and resends the frame 2 again, because it thought the frame2 may be lost or damaged.

Medium Access sub layer

The medium access control (MAC) is a sub-layer of the data link layer of OSI/ISO reference model for data transmission.

It is responsible for flow control and multiplexing for transmission medium.

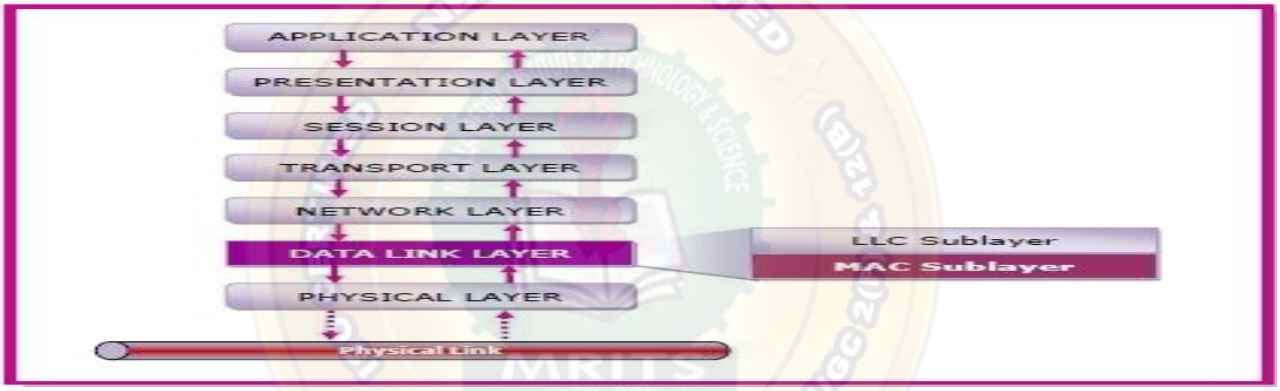
It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.

MAC Layer in the OSI Model

The Open System Interconnections (OSI) model is a layered networking framework that conceptualizes how communications should be done between heterogeneous systems. The data link layer is the second lowest layer. It is divided into two sub-layers −

- The logical link control (LLC) sub-layer
- The medium access control (MAC) sub-layer

The following diagram depicts the position of the MAC layer -



Functions of MAC Layer

- It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.
- It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.
- It resolves the addressing of source station as well as the destination station, or groups of destination stations.
- It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.
- It also performs collision resolution and initiating retransmission in case of collisions.
- It generates the frame check sequences and thus contributes to protection against transmission errors.

MAC Addresses

MAC address or media access control address is a unique identifier allotted to a network interface controller (NIC) of a device. It is used as a network address for data transmission within a network segment like Ethernet, Wi-Fi, and Bluetooth.

MAC address is assigned to a network adapter at the time of manufacturing. It is hardwired or hard-coded in the network interface card (NIC). A MAC address comprises of six groups of two hexadecimal digits, separated by hyphens, colons, or no separators. An example of a MAC address is 00:0A:89:5B:F0:11.

(or)

``Data Link Layer for LANs''

Can divide networks into point-to-point and broadcast. Look at broadcast networks and their protocols.

When many stations compete for a channel (e.g., broadcast channel such as an Ethernet), an algorithm must arbitrate access to the shared channel.

Need a way of insuring that when two or more stations wish to transmit, they all wait until doing so won't interfere with other transmitters. Broadcast links include LANs, satellites (WAN), etc.

LAN's:

- diameter not more than a few kilometers
- data rate of at least several Mbps.
- complete ownership by a single organization.

MANs cover a city-wide area with LAN technology. For example, cable TV.

Can have higher speed, lower error rate lines with LANs than WANs.

The channel allocation problem
In a broadcast network, the single broadcast channel is to be allocated to one transmitting user at a time.
When multiple users use a shared network and want to access the same network. Then channel allocation problem in computer networks occurs.
So, to allocate the same channel between multiple users, techniques are used, which are called channel allocation techniques in computer networks.

Channel Allocation Techniques

For the efficient use of frequencies, time-slots and bandwidth channel allocation techniques are used.
There are three types of channel allocation techniques that you can use to resolve channel allocation problem in computer networks as follows:

- Static channel allocation **in LANs and MANs**
- Dynamic channel allocation
- Hybrid channel allocation.

Channel Allocation Techniques		
Static channel allocation **in LANs and MANs**	Dynamic channel allocation	Hybrid channel allocation

Fig: Channel Allocation Techniques

- **Static Channel Allocation**

The traditional way of allocating a single channel between multiple users is called static channel allocation.
Static channel allocation is also called fixed channel allocation.

Real-life example of static channel allocation such as a telephone channel
The frequency division multiplexing (FDM) and time-division multiplexing (TDM) are two examples of static channel allocation.
In these methods, FDM fixed frequency is assigned to each user & TDM fixed time slot is assigned to each user

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

- **Dynamic channel allocation**

The technique in which channels are not permanently allocated to the users is called dynamic channel allocation.

In this technique, no fixed frequency or fixed time slot is allotted to the user.
Dynamic channel allocation is further categorized into two parts as follows:

- Centralized dynamic channel allocation
- Distributed dynamic channel allocation

The following are the assumptions in dynamic channel allocation:
Station Model: Assumes that each of N stations independently produce frames.
Single Channel Assumption: In this allocation all stations are equivalent and can send and receive on that channel.
Collision Assumption: If frames are transmitted at the same time by two or more stations, then the collision occurs.
Time can be divided into Slotted or Continuous
Stations can sense a channel is busy before they try it. .

Hybrid Channel Allocation: The mixture of fixed channel allocation and dynamic channel allocation is called hybrid channel allocation. The total channels are divided into two sets, fixed and dynamic sets.
First, a fixed set of channels is used when the user makes a call. If all fixed sets are busy, then dynamic sets are used. When there is heavy traffic in a network, then hybrid channel allocation is used.

Multiple access protocols: ALOHA

Multiple access protocols are a set of protocols operating in the Medium Access Control sub-layer (MAC sub-layer) of the Open Systems Interconnection (OSI) model.

These protocols allow a number of nodes or users to access a shared network channel. Several data streams originating from several nodes are transferred through the multi-point transmission channel.

The objectives of multiple access protocols are optimization of transmission time, minimization of collisions and avoidance of cross-talks.
Categories of Multiple Access Protocols

Multiple access protocols can be broadly classified into three categories - random access protocols, controlled access protocols and channelization protocol

Fig: Categories of Multiple Access Protocols

1. Random Access Protocols

Random access protocols assign uniform priority to all connected nodes.

Any node can send data if the transmission channel is idle.

No fixed time or fixed sequence is given for data transmission.

The four random access protocols are−

- ALOHA
- Carrier sense multiple access (CMSA)
- Carrier sense multiple access with collision detection (CMSA/CD)
- Carrier sense multiple access with collision avoidance (CMSA/CA)

ALOHA:

ALOHA is a multiple access protocol for transmission of data via a shared network channel. It operates in the medium access control sub-layer (MAC sub-layer) of the open systems interconnection (OSI) model. In ALOHA, each node or station transmits a frame without trying to detect whether the transmission channel is idle or busy. If the channel is idle, then the frames will be successfully transmitted. If the channel is busy, then the frames will be frames collision of frames will occur and the frames will be discarded. These stations may choose to retransmit the corrupted frames repeatedly until successful transmission occurs.

Versions of ALOHA Protocols

Pure ALOHA

In pure ALOHA, the time of transmission is continuous. Whenever a station has an available frame, it sends the frame. If there is collision and the frame is destroyed, the sender waits for a random amount of time before retransmitting it.

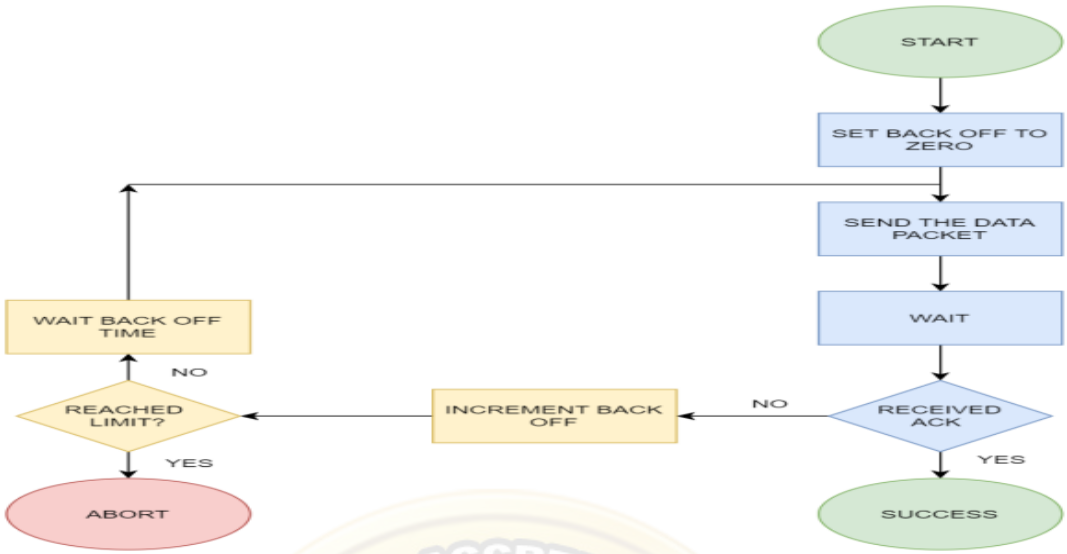


FIG: FLOW CHART OF PURE ALOHA

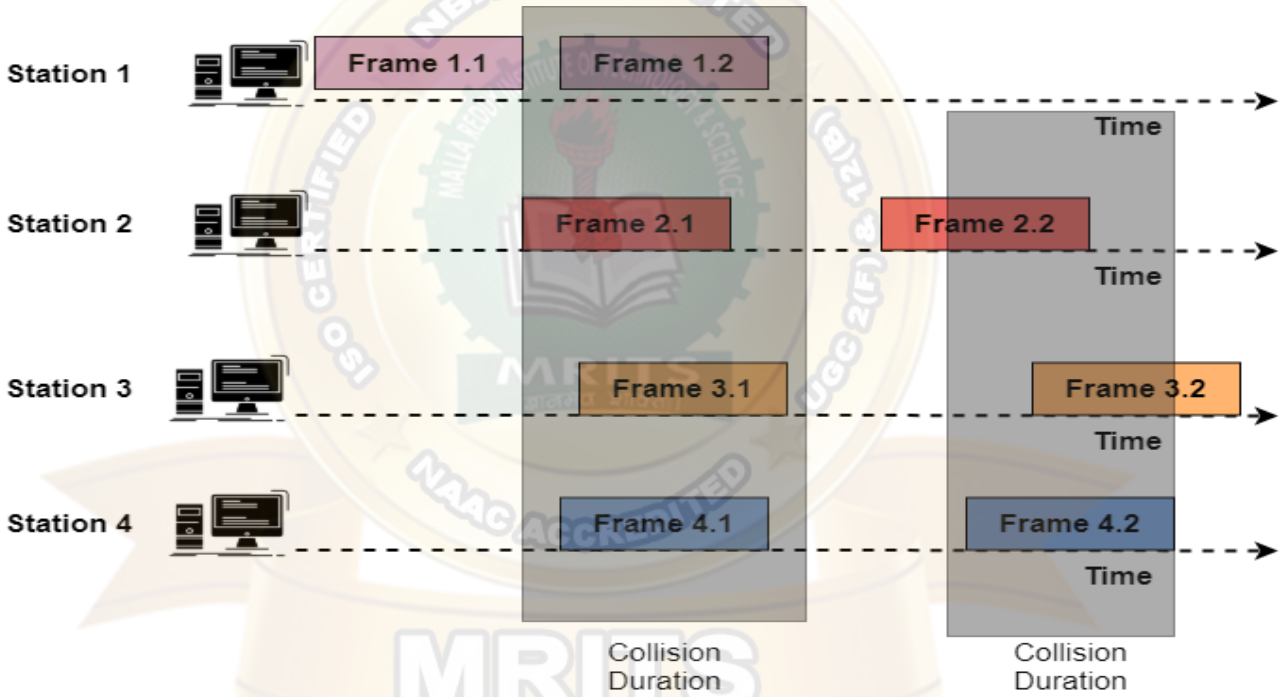


FIG: PURE ALOHA NETWORK

Data transmission: Stations can transmit the data randomly i.e. any number of stations can transmit data at any time.

Time status: Here, the time is continuous and is not globally synchronized with any other station.

Vulnerable time = 2 x T fr

Probability of successful transmission of a data packet

G*e-2G

where,

G = no. of stations willing to transmit data

Maximum efficiency = 18.4%

Collision status: It does not reduce the total number of collisions to half

Slotted ALOHA

Slotted ALOHA reduces the number of collisions and doubles the capacity of pure ALOHA.

The shared channel is divided into a number of discrete time intervals called slots.

A station can transmit only at the beginning of each slot.

However, there can still be collisions if more than one station tries to transmit at the beginning of the same time slot.

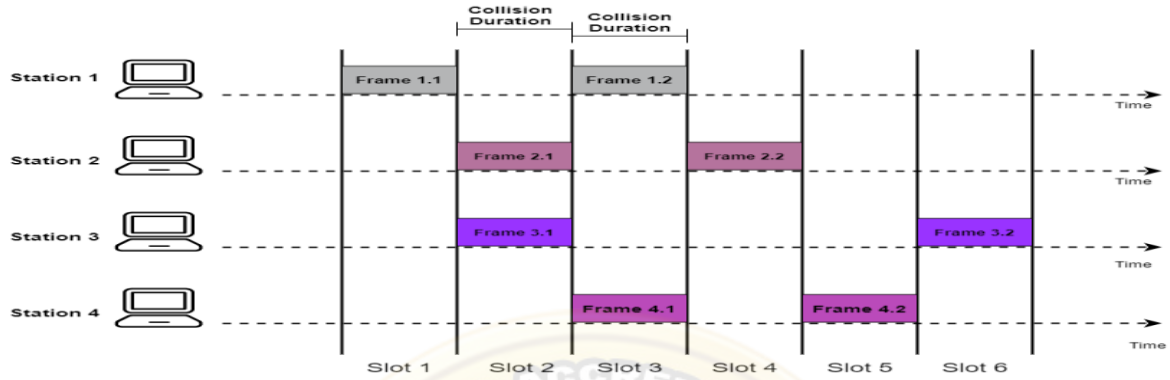


FIG: SLOTTED ALOHA NETWORK

Data transmission: Here, any random station can transmit the data at the beginning of any random time slot

Time status: Here, the time is discrete unlike pure ALOHA and is also globally synchronized

Vulnerable time = Tfr.

Probability of successful transmission of a data packet

G*e-G where,

G = no. of stations willing to transmit data

Maximum efficiency = 36.8%

Collision status: Here, it reduces the total number of collisions to half and doubles the efficiency of pure ALOHA

CSMA

CSMA stands for **Carrier Sense Multiple Access**.

When 2 or more stations start sending data at same time, then a collision occurs.

So this CSMA method was developed to decrease the chances of collisions when 2 or more stations start sending their signals over the data link layer.

The CSMA makes each station to first check channel whether channel idle or busy before sending any data packet.

Vulnerable time = Propagation time (Tp)

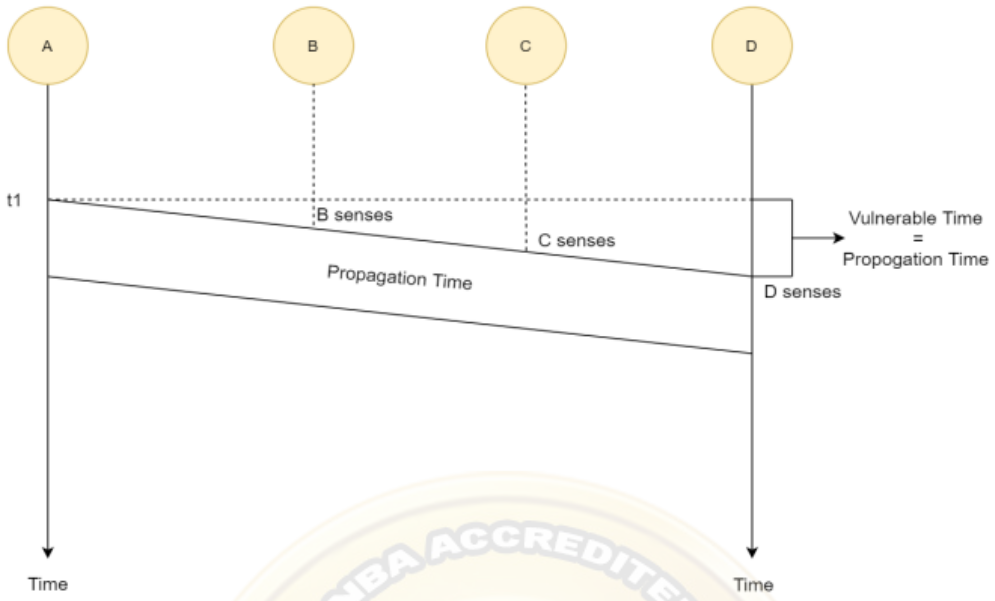


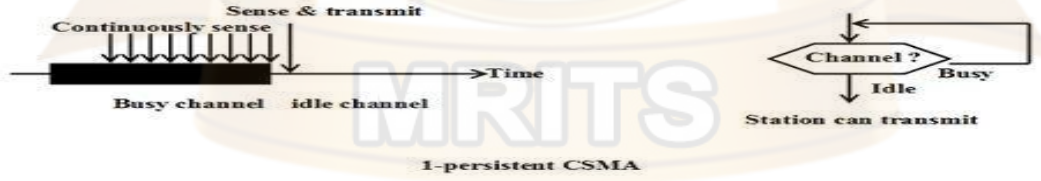
FIG: Vulnerable time of CSMA

But if the channels are busy, here the persistence methods can be applied to help the station act when the channel is busy or idle.

TYPES OF CSMA

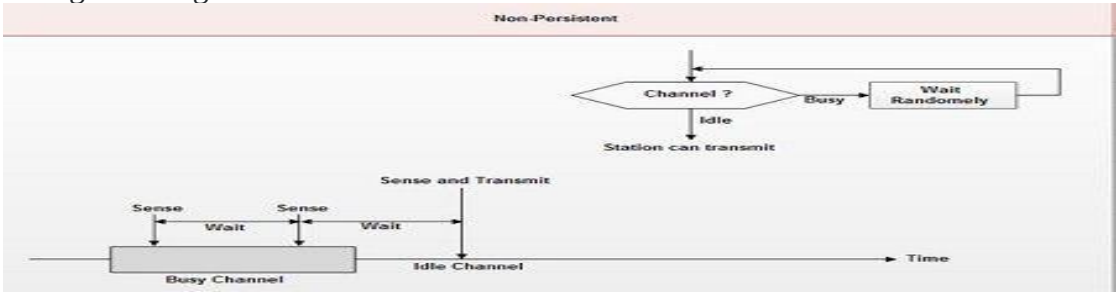
- **1-persistent mode**:

The station continuously senses the channel to check its state ie., idle or busy so that it can transfer data or not. In case when channel is busy, the station will wait for the channel to become idle. When station found idle channel, it transmits the frame to the channel without any delay. It transmits the frame with probability 1 is called 1-persistent CSMA



- **Non-persistent mode**:

Non- persistent CSMA is a non- aggressive version of CSMA protocol that operates MAC (Medium Access Control) layer. When a transmitting station has a frame to send & it senses a busy channel, it waits for random period of time without sensing the channel & repeats the algorithm again.



- **P-persistent mode**:

This method is used, when channel has time – slots & time slot duration >= maximum propagation delay time. When station is ready to send the frames, it will sense channel.

If channel found by sy, channel wait for next slot.

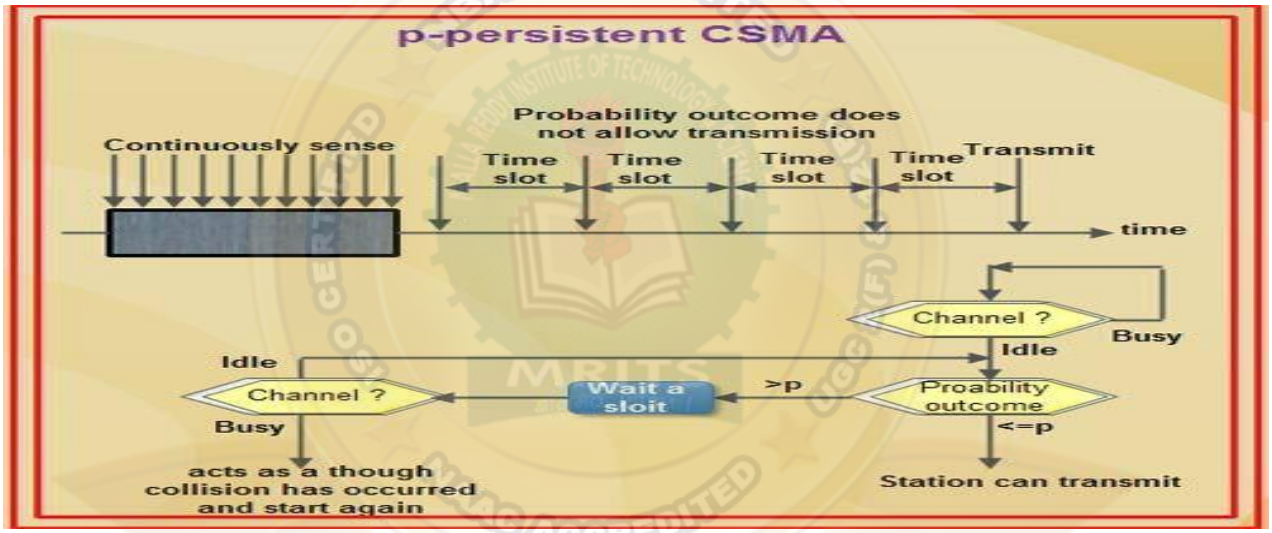
If channel is idle transmits frame with probability P

q=1-p

so, station will wait for beginning of next time slot

If next slot also found idle transmit or wait again with probabilities p & q

This process is repeated until either frame gets transmitted or another station has started transmitting.



CSMA/CD

CSMA/CD means **CSMA with Collision Detection**.

In this, whenever station transmits data-frame it then monitors the channel or the medium to acknowledge the state of the transmission i.e. successfully transmitted or failed.

If the transmission succeeds, then it prepares for the next frame otherwise it resends the previously failed data-frame.

The point to remember here is, that the frame transmission time should be at least twice the maximum propagation time, which can be deduced when the distance between the two stations involved in a collision is maximum.

CSMA/CA

CSMA/CA means **CSMA with collision avoidance**.

To detect the possible collisions, the sender receives the acknowledgement and if there is only one acknowledgment present (it's own) then this means that the data-frame has been sent successfully.

But, if there are 2 or more acknowledgment signals then this indicates that the collision has occurred.

2. Controlled Access Protocols

Controlled access protocols allow only one node to send data at a given time. Before initiating transmission, a node seeks information from other nodes to determine which station has the right to send. This avoids collision of messages on the shared channel.

The station can be assigned the right to send by the following three methods−

- Reservation
- Polling
- Token Passing

3. Channelization

Channelizations are a set of methods by which the available bandwidth is divided among the different nodes for simultaneous data transfer.

The three channelization methods are−

- Frequency division multiple access (FDMA)
- Time division multiple access (TDMA)
- Code division multiple access (CDMA)

Collision free protocols

When more than one station tries to transmit simultaneously via a shared channel, the transmitted data is garbled called collision.

The Medium Access Control (MAC) layer of the OSI model is responsible for handling collision of frames.

Collision – free protocols are devised so that collisions do not occur. Protocols like CSMA/CD and CSMA/CA nullifies the possibility of collisions once the transmission channel is acquired by any station.

However, collision can still occur during the contention period if more than one stations starts to transmit at the same time.

Collision – free protocols resolves collision in the contention period and so the possibilities of collisions are eliminated.

Types of Collision – free Protocols

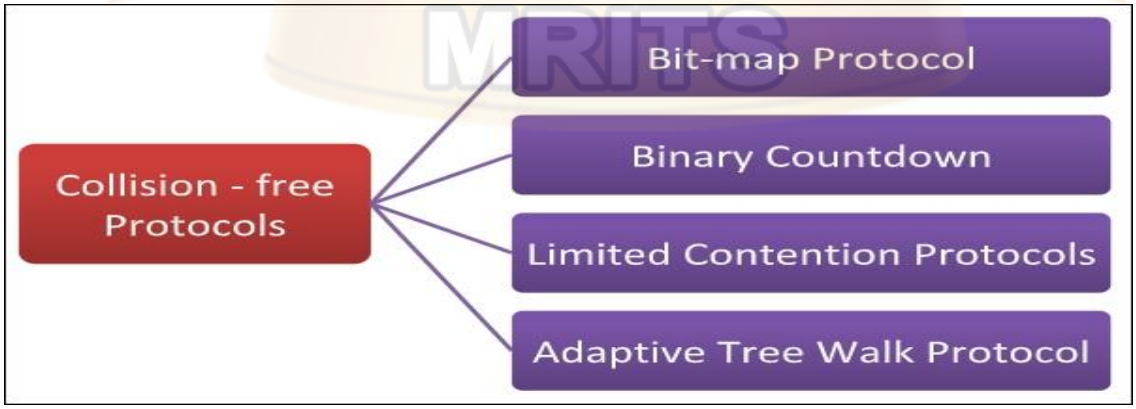


Fig: **Types of Collision – free Protocols**

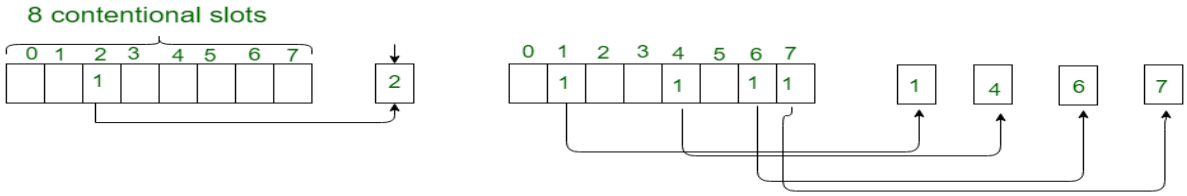
BIT – MAP PROTOCOL

In bit map protocol, the contention period is divided into N slots, where N is the total number of stations sharing the channel.

If a station has a frame to send, it sets the corresponding bit in the slot.

So, before transmission, each station knows whether the other stations want to transmit.

Collisions are avoided by mutual agreement among the contending stations on who gets the channel.



A Bit-map Protocol.

BINARY COUNT DOWN

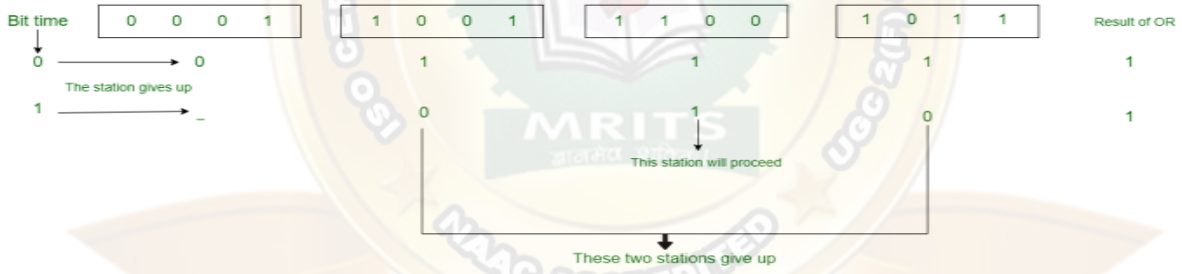
This protocol overcomes the overhead of 1 bit per station of the bit – map protocol.

Here, binary addresses of equal lengths are assigned to each station.

For example, if there are 6 stations, they may be assigned the binary addresses 001, 010, 011, 100, 101 and 110.

All stations wanting to communicate broadcast their addresses.

The station with higher address gets the higher priority for transmitting.



Binary countdown

LIMITED CONTENTION PERIOD

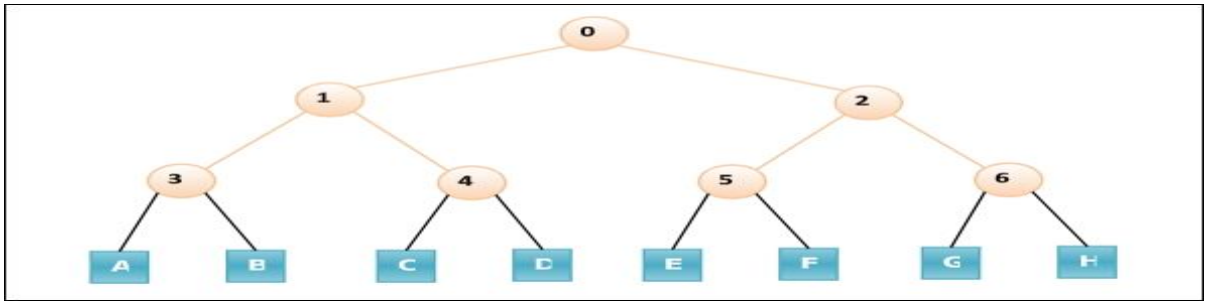
Collision based protocols (pure and slotted ALOHA, CSMA/CD) are good when the network load is low.

Collision free protocols (bitmap, binary Countdown) are good when load is high.
How about combining their advantages –

1. Behave like the ALOHA scheme under light load
2. Behave like the bitmap scheme under heavy load.

ADAPTIVE TREE – WALK PROTOCOLS

In adaptive tree walk protocol, the stations or nodes are arranged in the form of a binary tree as follows –



Initially all nodes (A, B ……. G, H) are permitted to compete for the channel. If a node is successful in acquiring the channel, it transmits its frame. In case of collision, the nodes are divided into two groups (A, B, C, D in one group and E, F, G, H in another group). A node belonging to only one of them is permitted for competing. This process continues until successful transmission occurs.

WIRELESS LAN's (WLAN)

WLAN stands for Wire-less Local Area Network.

WLAN is a LAN that uses radio communication to provide mobility to n/w users while maintaining connectivity to wired network.

A WLAN extends wired LAN

WLAN's built attaching a device called access points (AP) to edge of wired network

Clients communicate AP using wireless network adapter similar function to Ethernet adapter

WLAN also called as a LAWN

LAWN stands for Local Area Wireless Network

Performance:	High compared to other Wireless Networks
Coverage:	Within Campus or building or Tech Parks
Uses:	Mobile Propagation Of Wired Networks
Standards:	Hiper LAN, Wi-Fi, & IEEE 802.11
Offers:	Service to desktop laptop, Mobile application & all devices works in Internet

Example:

College WI-FI, Company WI-FI, Industry WI-FI

WLAN affordable method & can setup in 24 hrs

WLAN gives users mobility to move around within a local coverage area & still be connected to network

Latest Brands in WLAN based on IEE 802.11 standards, which are WI-FI Brand name

HISTORY:

A professor University Of Hawaii whose name was "Norman Abramson", developed world's first wireless computer communication network.

In 1979, G. Feller & U. Bapst published a paper in IEE proceeding reporting an experimental WLAN using diffused infrared communications.

First of IEEE workshops ON WLAN held in 1991

Components of WLANs

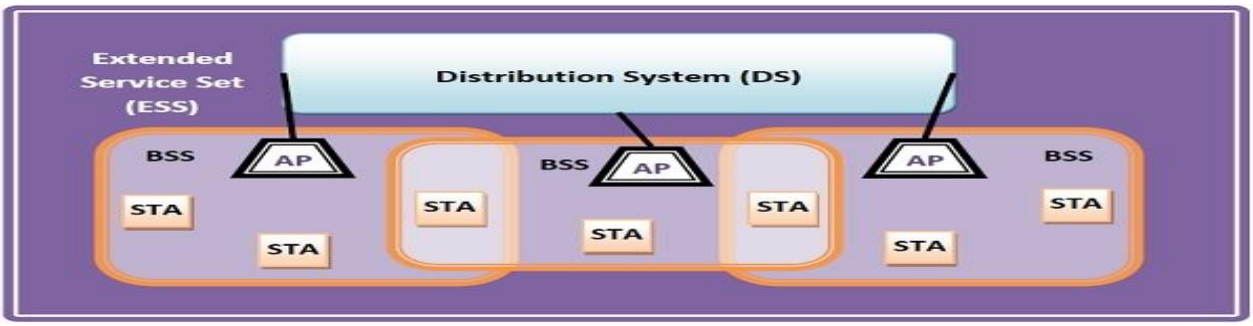


Fig: components of wireless LANs

Stations (STA) – Stations of all devices and equipment that are connected to the wireless LAN. Each station has a wireless network interface controller.

A station can be of two types –

Wireless Access Point (WAP or AP)	Client

Basic Service Set (BSS) – A group of stations communicating at the physical layer level.

BSS can be of two categories –

Infrastructure BSS	Independent BSS

Extended Service Set (ESS) – It is a set of all connected BSS.

Distribution System (DS) – It connects access points in ESS.

Types of WLANS

WLANS	
Infrastructure Mode	**Ad Hoc Mode**

Fig: types of WLANs

- **Infrastructure Mode** – Mobile devices or clients connect to an access point (AP) i.e., connects via a bridge to the LAN or Internet. The client transmits frames to other clients via the AP.
- **Ad Hoc Mode** – Clients transmit frames directly to each other in a peer-to-peer fashion.

CHARACTERISTICS:

- Seamless operation.
- Low power for battery use.
- Simple management, easy to use for everyone.
- Protection of investment in wired networks.
- Robust transmission technology

ADVANTAGES:

- Installation speed and simplicity.
- Installation flexibility.
- Reduced cost of ownership.
- Reliability.
- Mobility.

- Robustness.

DIS - ADVANTAGES:

- Slower bandwidth.
- Security for wireless LAN's is the prime concern.
- Less capacity.
- Wireless networks cost four times more than wired network cards.
- Wireless devices emit low levels of RF which can be harmful to our health.

Data Link Layer Switching

Network switching is the process of forwarding data frames or packets from one port to another leading to data transmission from source to destination.

Data link layer is the second layer of the Open System Interconnections (OSI) model whose function is to divide the stream of bits from physical layer into data frames and transmit the frames according to switching requirements.

Switching in data link layer is done by network devices called **bridges**.

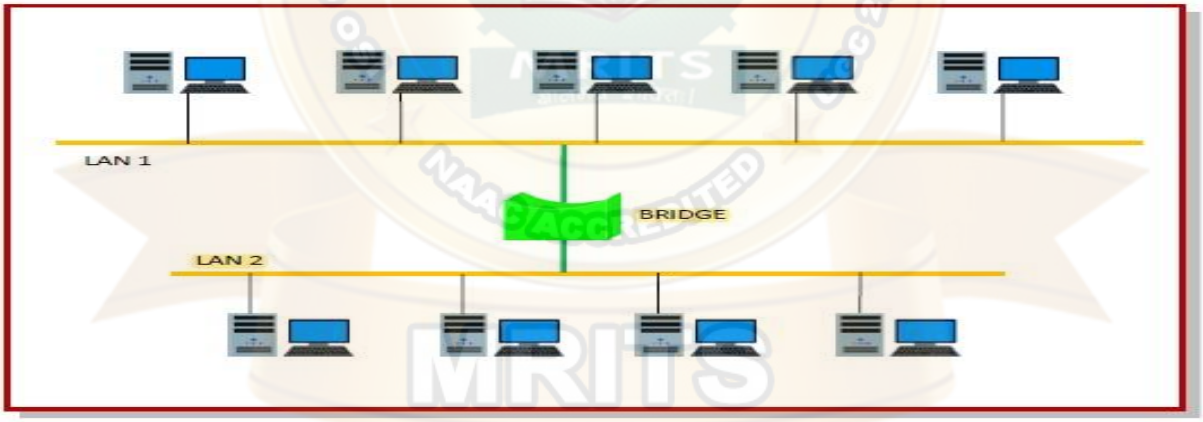
Bridges

A data link layer bridge connects multiple LANs (local area networks) together to form a larger LAN.

This process of aggregating networks is called network bridging.

A bridge connects the different components so that they appear as parts of a single network.

The following diagram shows connection by a bridge –



Switching by Bridges

When a data frame arrives at a particular port of a bridge, the bridge examines the frame's data link address, or more specifically, the MAC address. If the destination address as well as the required switching is valid, the bridge sends the frame to the destined port. Otherwise, the frame is discarded.

The bridge is not responsible for end to end data transfer. It is concerned with transmitting the data frame from one hop to the next. Hence, they do not examine the payload field of the frame. Due to this, they can help in switching any kind of packets from the network layer above.

Bridges also connect virtual LANs (VLANs) to make a larger VLAN.

If any segment of the bridged network is wireless, a wireless bridge is used to perform the switching.

There are three main ways for bridging −

- simple bridging
- multi-port bridging
- learning or transparent bridging

ADVANTAGES

Switches divide a network into several isolated channel or collision domains

Possibility of collision reduced

1. Collision only occurs when 2 devices try to get access to 1 channel
2. Can be solved by buffering one of them for later access

Each channel has its own network capacity

- Suitable for real-time applications
  Example: Video Conferencing

LIMITATIONS

When buffer is full, device can't detect collision

Some higher level protocols do not detect error ie., for example: UDP

CSMA / CD scheme will not work since data channels are isolated, not in case as in Ethernet

Contains buffers to accommodate bursts of traffic can become overwhelmed by heavy traffic

Data Link Layer Switch supports Layer – 2 switches, Layer – 3 switches, Layer – 4 switches

LAYER – 2 SWITCH

Layer – 2 switches performs Physical Layer & Data Link Layer. It is the bridge with many ports & design that allows better performance. It operates physical network addresses, identify individual devices. Most hardware devices permanently assigned during manufacturing process. Switching operates layer – 2 are very fast because sorting physical address & they aren't smart

LAYER – 3 SWITCH

Layer – 3 Switches uses network or IP addresses ie., identifying locations on network or more closer to Layer – 2 switch. They identify network locations as well as physical device. It is smarter than Layer – 2 devices & calculate best way to send a packet from source to destination. It is smarter, may not fast as their algorithm, fabric & processor don't support high speeds

LAYER – 4 SWITCH

LAYER – 4 SWITCH is ISO/ OSI model co-ordinates communication between systems

LAYER – 4 SWITCH are capable of identifying application protocols ie., HTTP, SNTP, FTP are included with each packet

LAYER – 4 SWITCH use information to hand-off packet to high layer software

It provides effective wire-speed security shield for your network because any company or industry can be authorized switched ports or users

UNIT – III : Network Layer
Design issues, Routing algorithms: shortest path routing, Flooding, Hierarchical Routing, Broadcast, Multicast, distance vector routing, Congestion Control Algorithms, Quality of Service, Internetworking, the Network layer in the internet

INTRODUCTION TO NETWORK LAYER

- The Network Layer is the third layer of the OSI model.
- It handles the service requests from the transport layer and further forwards the service request to the data link layer.
- The network layer translates the logical addresses into physical addresses
- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
- The main role of the network layer is to move the packets from sending host to the receiving host.

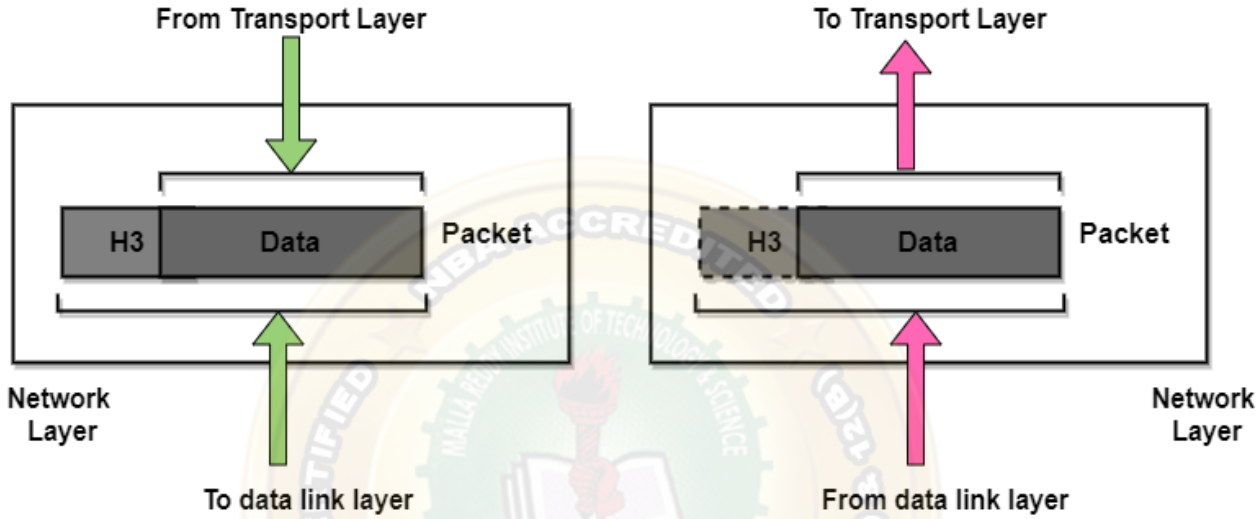


FIG: NETWORK LAYER

Functionalities

Routing:
When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2

Logical Addressing:
The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.

Internetworking:
This is the main role of the network layer that it provides the logical connection between different types of networks.

Fragmentation:
The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.

NETWORK LAYER SERVICES

Guaranteed delivery of Packets :

The network layer guarantees that the packet will reach its destination.

Guaranteed delivery with the bounded delay:

It is another service provided by the network layer and it guarantees that the packet will surely be delivered within a specified host-to-host delay bound.

Transfer of packets in Order:

According to this service, it is ensured that packets arrive at the destination in the same order in which they are sent by the sender.

Security:

Security is provided by the network layer by using a session key between the source host and the destination host.

ADVANTAGES

By forwarding service of the network layer, the data packets are transferred from one place to another in the network.

In order to reduce the traffic, the routers in the network layer create collisions and broadcast the domains.

Failure in the data communication system gets eliminated by packetization.

DIS - ADVANTAGES

In the design of the network layer, there is a lack of flow control

In the network layer, there is a lack of proper error control mechanisms; due to the presence of fragmented data packets the implementation of error control mechanism becomes difficult.

Due to the presence of too many data-grams there happens occurrence of congestion.

DESIGN ISSUES IN NETWORK LAYER

Definition:

N/w layer is majorly focused on getting packets from source to destination, routing error handling & congestion ctrl

N/w layer is well known model is OSI/ ISO approach with 7 layers

Before learning about design issues in n/w layer we will learn its functions:

1. ADDRESSING

2. PACKETING
3. ROUTING
4. INTER - NETWORKING

1. **ADDRESSING -** Maintain address at frame header of both source & destination & performs addressing detect various devices in network

2. **PACKETING -** This is performed by Internet protocol. The Network layer converts packets from its upper layer

3. **ROUTING -** It is most important functionality. This layer chooses most & best path for data transmission from source to destination

4. **INTER - NETWORKING -** It works to deliver a logical connection across multiple devices

NETWORK LAYER DESIGN ISSUES

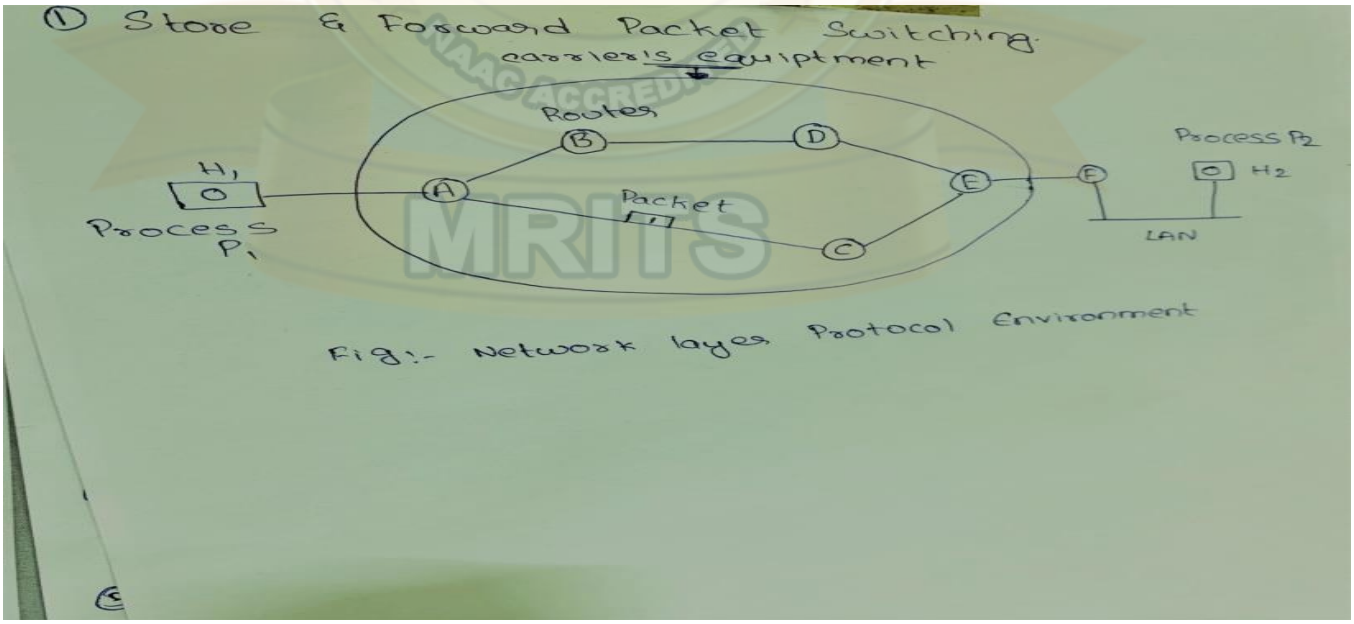
The Network layer design issues are as follows:

1. STORE & FORWARD PACKET SWITCHING
2. SERVICES PROVIDED TO THE TRANSPORT LAYER

3. IMPLEMENTATION OF CONNECTION – LESS SERVICE

4. IMPLEMENTATION OF CONNECTION ORIENTED SERVICE

1. STORE & FORWARD PACKET SWITCHING



Host H1 is connected to carrier's routers A by leased line.

Host h2 is LAN with router F, owned & operated by customer. This router F is connected by leased line to carrier's equipment.

A host with a packet to send transmits its nearest router, either its own LAN or a point - to – point link to carrier.
The packet is stored there until it has fully arrived so the checksum can be verified. Then packets are forwarded to next router along the path until it reaches the destination host. This is also called as STORE & FORWARD PACKET SWITCHING

2. SERVICES PROVIDED TO THE TRANSPORT LAYER

Network Layer provides services to transport layer at network layer / transport layer interface Following requirements are:

- Service should be Independent of Network Topology
- Network addresses should be made available to transport with a uniform numbering plan
- Transport layer should be shielded from number, type & topology of routers present

3. IMPLEMENTATION OF CONNECTION – LESS SERVICE

Connection – less network services called "Datagram's". Packets are termed as "Datagram's" & corresponding subnet as " Datagram subnets". When the message size that has to be transmitted is 4 times that size of packet, then network layer divides into 4 packets & transmits each packet to router via a few protocols. Each data packet has destination address & is routed independently irrespective of the packets.

4. IMPLEMENTATION OF CONNECTION ORIENTED SERVICE

Connection oriented network called as "Virtual circuit ". To use a connection oriented service, first we establishes a connection, use it & then release it. In connection – oriented service, the data packets are delivered to receiver in same order in which they have been sent by sender. It can be done either 2 ways are:

- **Circuit Switched Connection -** A dedicated physical path or a circuit is established between communicating nodes & 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 user that there is a dedicated path from sender to receiver. A virtual path is established here. While, other connections may also be using the same path

ROUTING ALGORITHM

DEFINATION: An algorithm is a procedure that lays down the route or path to transfer data packets from source to destination called Routing algorithm.

CLASSIFICATION: There are 2 categories in routing algorithm are as follows:

ROUTING ALGORITHM	
ADAPTIVE ROUTING ALGORITHM	**NON – ADAPTIVE ROUTING ALGOTITHM**

1. **Adaptive Routing Algorithm**

Definition: It is an algorithm that constructs the routing table based on network conditions called Adaptive Routing Algorithm
Uses: Dynamic Routing
Complexity: More difficult
Routing decision: Based on topology & network traffic

Types: There are 3 types in Adaptive Routing Algorithm are as follows:

- Centralized Algorithm
- Isolation Algorithm
- Distributed Algorithm

- **Centralized Algorithm -** It also called as Global routing algorithm. It computes "least – cost path" between source & destination using complete & global knowledge about network. Link State Algorithm is referred as Centralized Algorithm i.e., aware of cost of each link in network

- **Isolation Algorithm -** An algorithm that obtains routing information by using local information rather than gatherings information from other nodes.

- **Distributed Algorithm -** It also known as De-centralized Algorithm. It computes Least – cost path between source & destination in iterative & distributed manner. A distance vector is a de-centralized algorithm i.e., it known direction through which packet is to be forwarded along with Least – cost path.

2. **Non - Adaptive Routing Algorithm**

Definition: An algorithm that constructs static table to determine which node to send packet is called Non – adaptive Routing Algorithm
Uses: Static Routing
Complexity: More simple
Routing decisions: Static tables

Types: There are 2 types in Non – adaptive Routing algorithms are as follows:

- Flooding
- Random Walks

- **Flooding**

Every incoming packet is sent to all outgoing links except 1 from it has been reached.

Dis – advantage is Node may contain several copies of a particular packet

- **Random Walks**

A packet sent by node to 1 of its neighbors' randomly

Advantage is uses of alternative routes very efficiently

SHORTEST PATH ROUTING

In shortest path Routine, path length between each node is measured as a function of distance, bandwidth, average traffic, communication cost, queue length, measured delay etc.

By changing weighing function, algorithm then computes shortest path measured accordingly to any 1 of a no. of criteria or combination of criteria.

Types:

There are 2 types in Shortest Path Routing are as follows:

1. DIJKSTRA's Algorithm
2. BELLMAN – FORD Algorithm

1. DIJKSTRA's Algorithm

Each node is labeled with its distance from source node along with best known path

Initially no paths are known, so all nodes are labeled with infinity

As algorithm proceeds, paths are found, labels are changed, reflecting better paths

Following algorithm steps in DIJKSTRA's Algorithm are as follows:

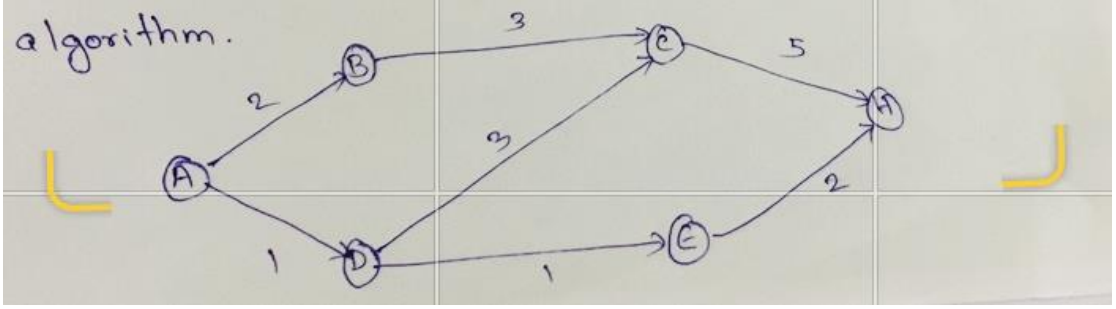
STEP 1: Source node is initialized & can be indicated as a filled circle

STEP 2: Initial path cost to neighboring nodes i.e., adjacent nodes / link nodes is computed & these nodes are re-labeled considering source node

STEP 3: Examine all adjacent nodes & find smallest label, make it permanent

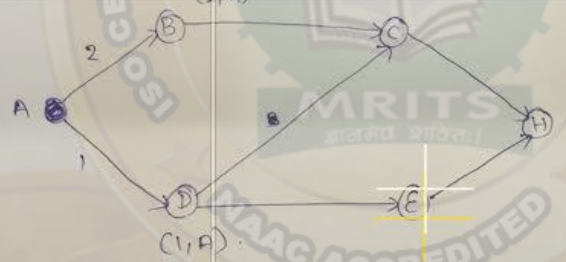
STEP 4: Smallest label is now working node, then step 2 & step 3 are repeated till destination node reaches

Ex → Find the shortest path node A & node H for the following. by applying Dijkstra's algorithm.

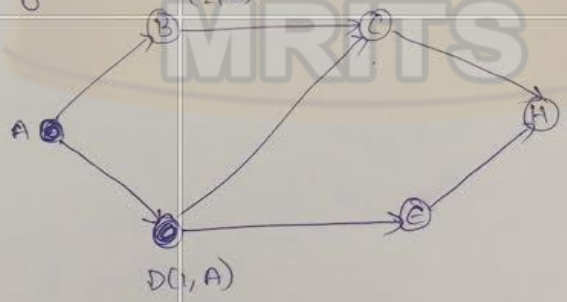


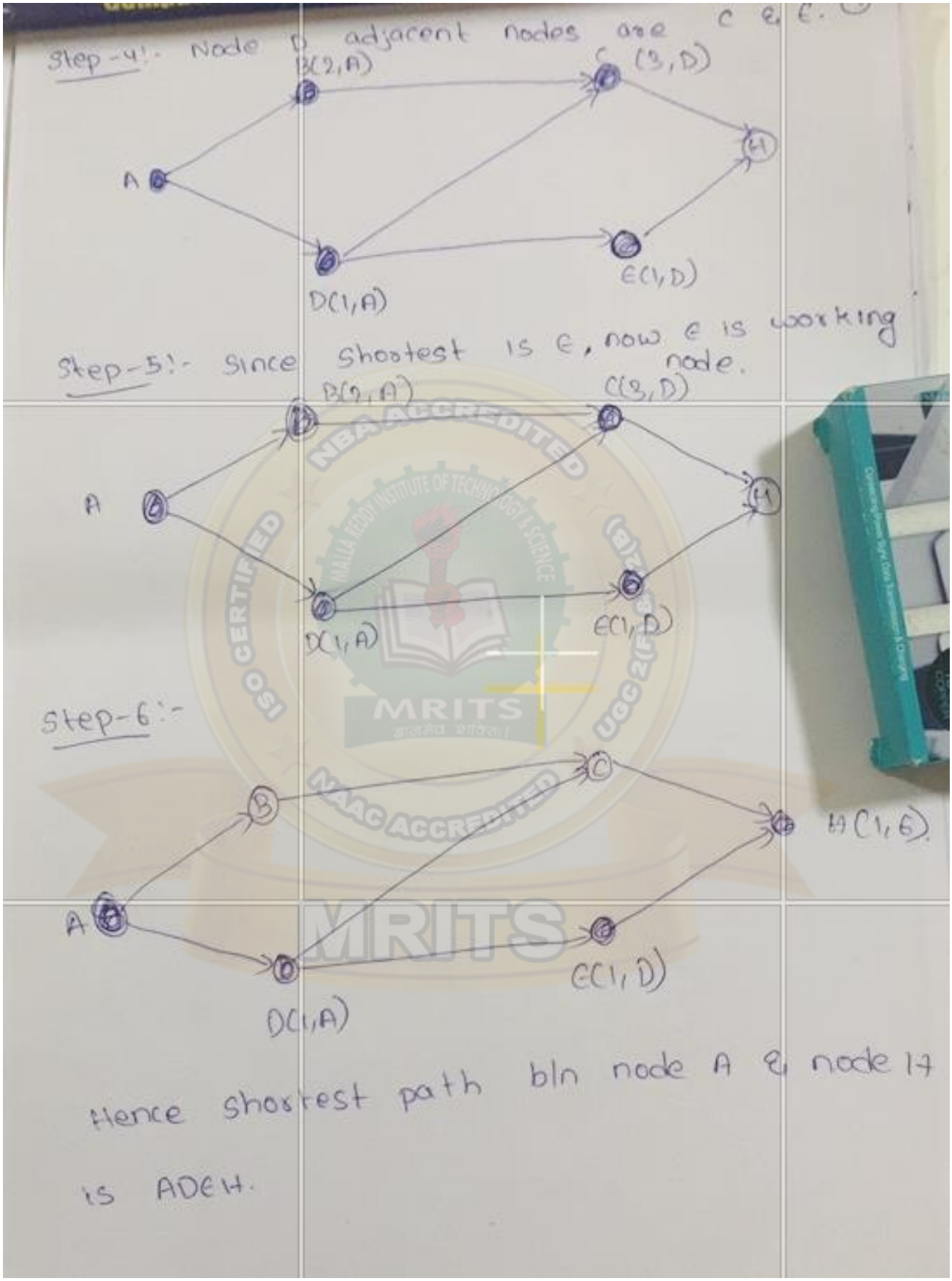
Step-1:-
Node A is intialized as source node.

Step-2:- Link cost is computed for the adjacent node. (1,A)



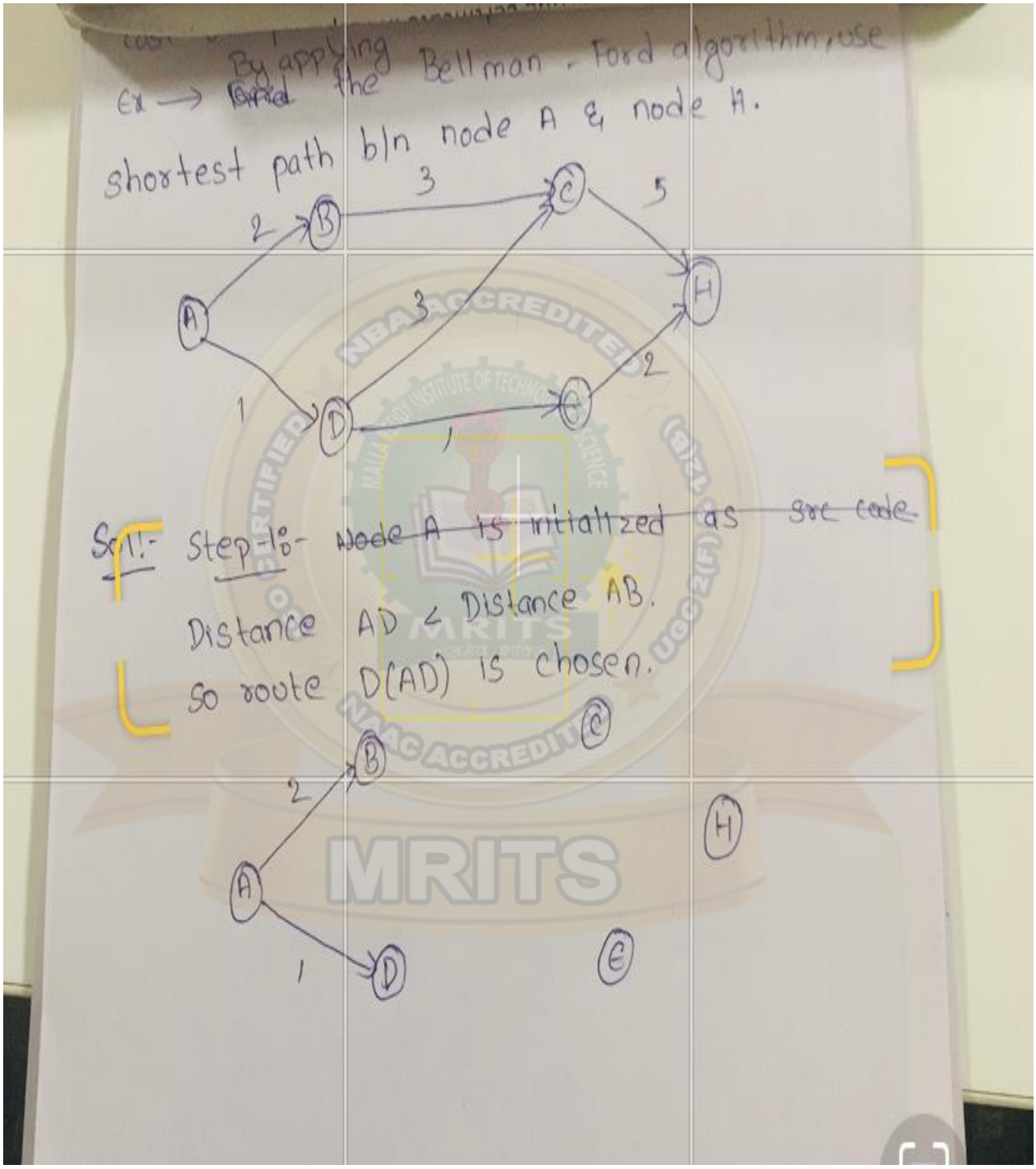
Step-3:- Since AD is smallest path, now D is working node. (2,A)

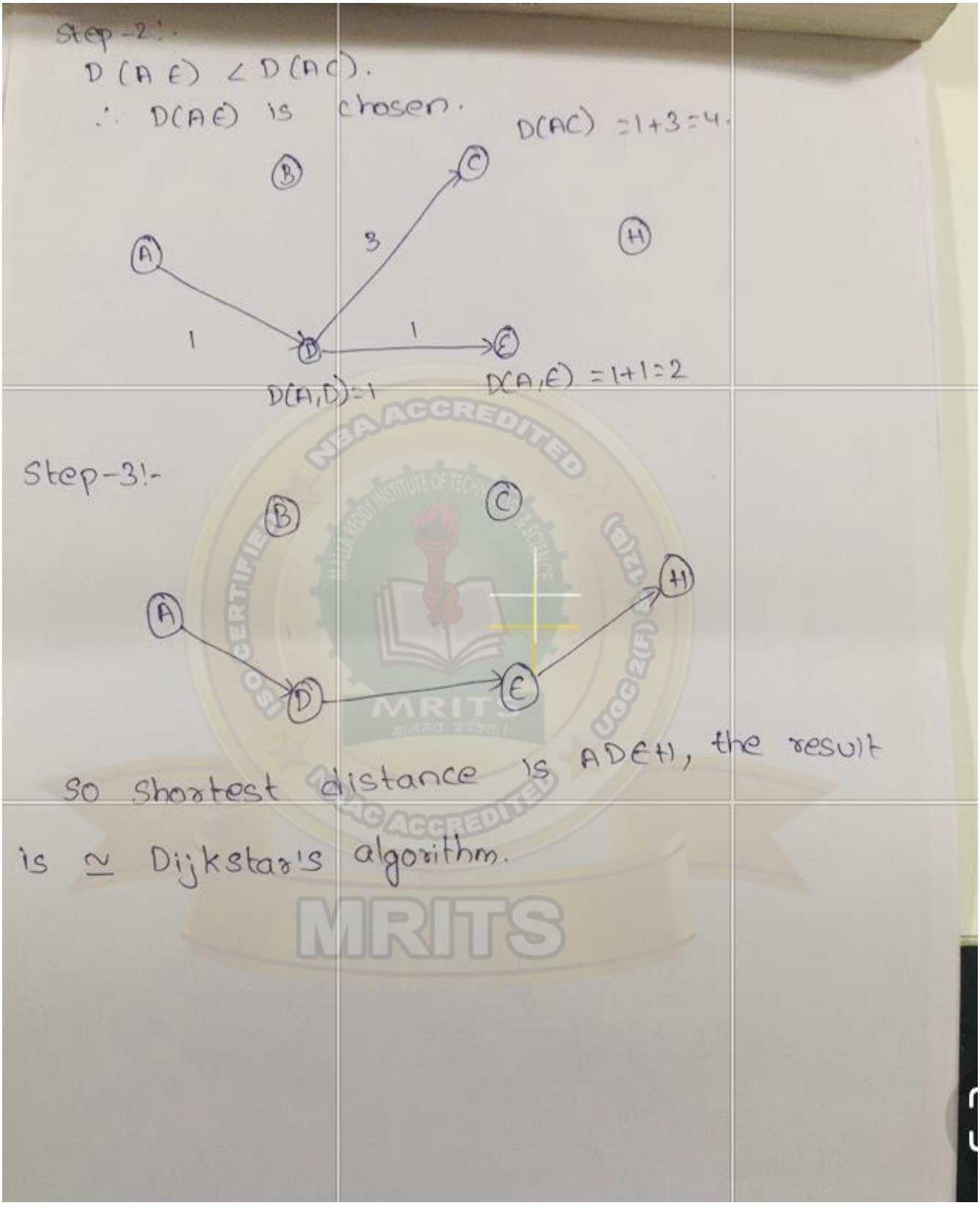




2. **BELLMAN FORD ALGORITHM**

Bellman Ford algorithm is similar to DIJKSTRA's algorithm but here shortest paths from a given source node is computed subject to constraint that path contain at most 1 link i.e., from source node, at each step Least – cost path with maximum no. of links are found. Finally Least – cost path to each node & cost of path is computed.



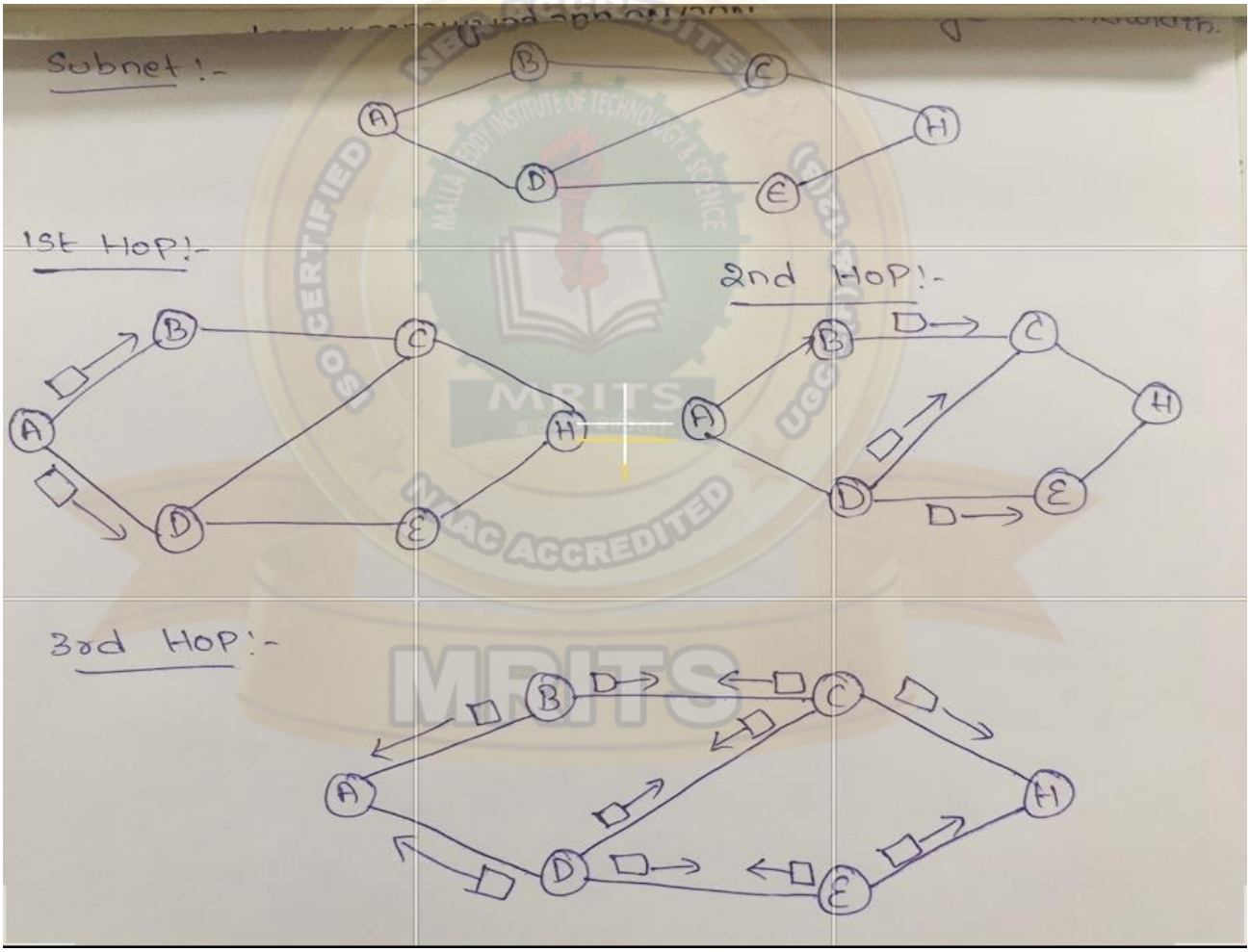


FLOODING

This technique requires no network information. A packet is sent by a source node to all its adjacent nodes.
At each node is retransmitted on every outgoing links, except link that it arrived from.

Flooding generates large no. of duplicate packets 1 way to prevent this for each node to renumber identify of those packets it has already sent.
When a duplicate packet arrives they are deleted.
One such measure is to have a hop counter contained in header of each packet is each hop.
When count reaches zero, packet is deleted.
If counter is set to maximum i.e., diameter of subnet

Selective flooding: The routers don't re-transmit every incoming packet on all links but only on those links that are in right direction.
Advantage: It is highly robust. This property finds application in military network i.e., subjected to extensive damage & distributed database applications where it is necessary to update DB concurrently
Disadvantage: Total traffic load. It generates directly proportional to connectivity of network. Also Flooding requires much large bandwidth



BROADCAST ROUTING

Transmitting data to the multi – destinations simultaneously called Broadcasting

Various methods of broadcast are as follows:

1. Flooding

2. Multi-destination Routing
3. Reverse path forwarding

1. Flooding

This technique requires no network information.
A packet is sent by a source node to all its adjacent nodes.

At each node is retransmitted on every outgoing links, except link that it arrived from.

Flooding generates large no. of duplicate packets 1 way to prevent this for each node to renumber identify of those packets it has already sent.

When a duplicate packet arrives they are deleted.

One such measure is to have a hop counter contained in header of each packet is each hop.

When count reaches zero, packet is deleted. If counter is set to maximum i.e., diameter of subnet

Selective flooding:

The routers don't re-transmit every incoming packet on all links but only on those links that are in right direction.

2. Multi-destination Routing

In this technique, each packet contains entire destination addresses.
When a packet arrives at a router, router checks addresses & select proper links for transmission

Router generates new copy of packets for each links with selected destination addresses. After few hops each packet will carry only one destination addresses & it is just as a normal packet

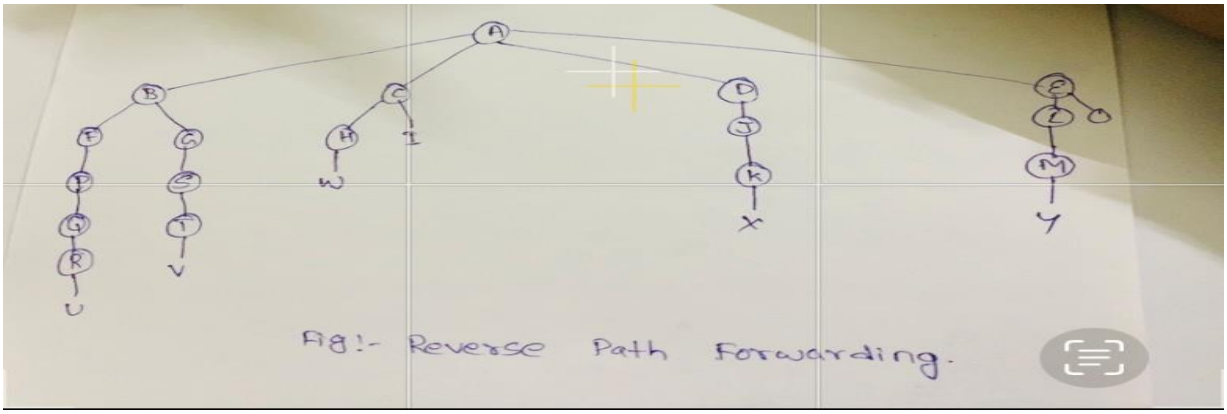
This process is just like separately addresses packets.

3. Reverse path forwarding

The broadcast packet is transmitted by a source information if arrives at a router, router checks a packet whether it is from preferred path & router sends it on best route path.

A tree like structure is forwarded by reverse path forwarding. The main advantage is:

a) Efficient & simple to implement
b) To maintain destination address by router is not required



First Hop:

During the first hop, A send packets to B, C, D, E as indicated.

Each packet arrived on preferred path to A, so indicated by a circle around the letter

Second Hop:

On second hop, seven packets are generated, two from routers B, C, E & one from D

The packets arrived on preferred paths are then generates further packets

Packets received on F, G, H, J are on preferred paths

Third Hop:

In third hop, 13 packets are generated, packet W not preferred path, so it is rejected. This process continues & after specific numbers of hops broadcasting terminates.

HIERARCHICAL ROUTING

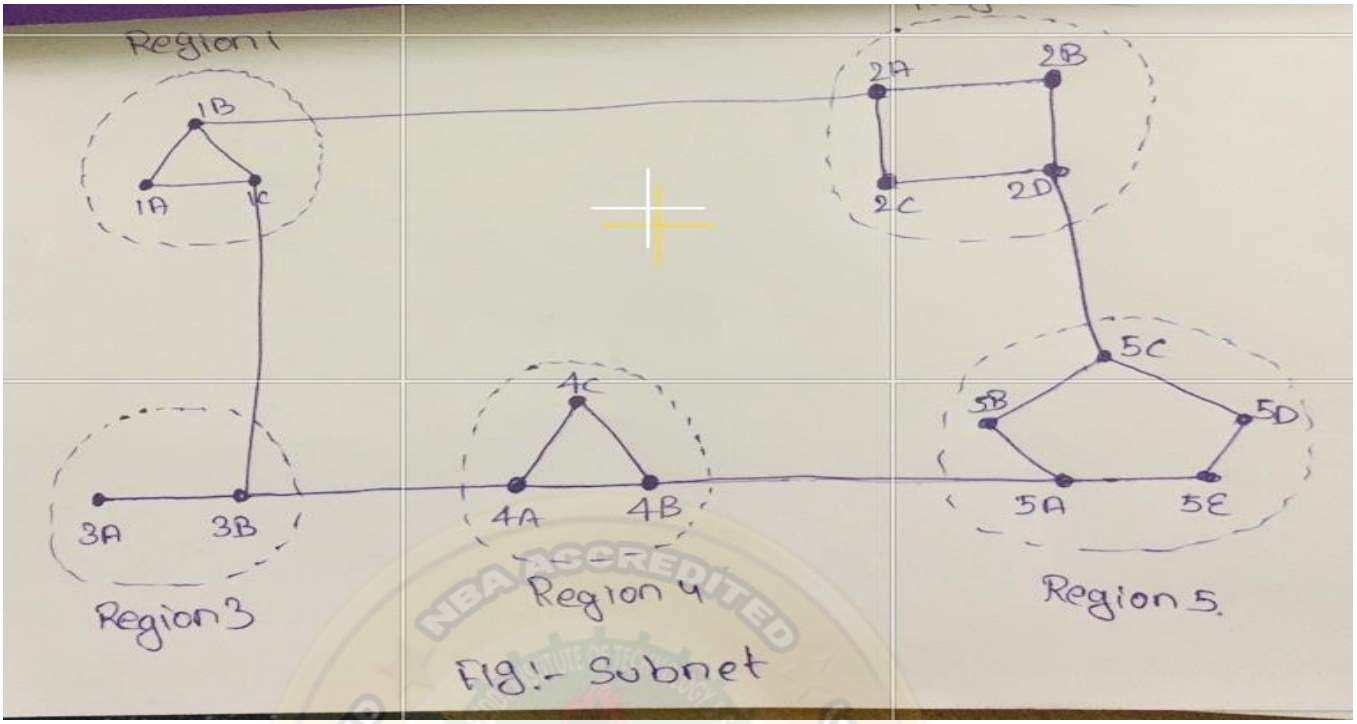
At certain point network may grow to the point where it is no longer feasible for every router to have an entry for other router, so the routing will have to be done hierarchically.

When this routing is used, the routers are divided into regions.

It contains all details about how to route packets to destination within its own region.

Some time, two – level hierarchy may be insufficient.

It is necessary to group regions into clusters, clusters into zones, zones into groups & so on.



Hierarchical table for 1A

Destination	**Line**	**Hops**
1A	-	-
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	5

FULL TABLE FOR 1A

Destination	**Line**	**Hops**
1A	-	-
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4

4C	1C	4
5A	1C	5
5B	1C	6
5C	1B	5
5D	1C	7
5E	1C	6

For router 1A has 17 entries in full routing table.

When hierarchical routing is used, only 7 entries valid for 1A.

There are entries for local routers but all other regions have been condensed into a single router.

Hierarchical routing increases the saving the table space.

MULTICAST ROUTING

To send messages to well defined groups that are numerically large is size but small compared to network as a whole.

Sending message to such a group is called multicasting & its routing algorithm called multicast routing

Multicasting requires group management.
Some way is needed to create & destroy groups & to allow processes to join & leave groups

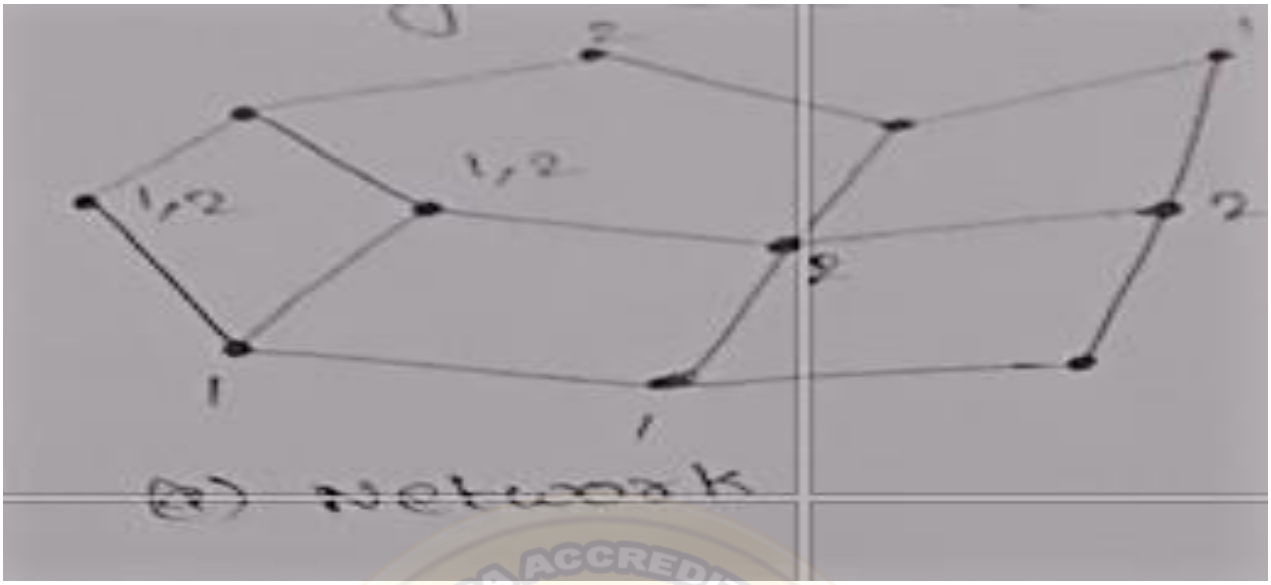
To do multicasting routing, each router computes a spanning tree occurring all other routers.

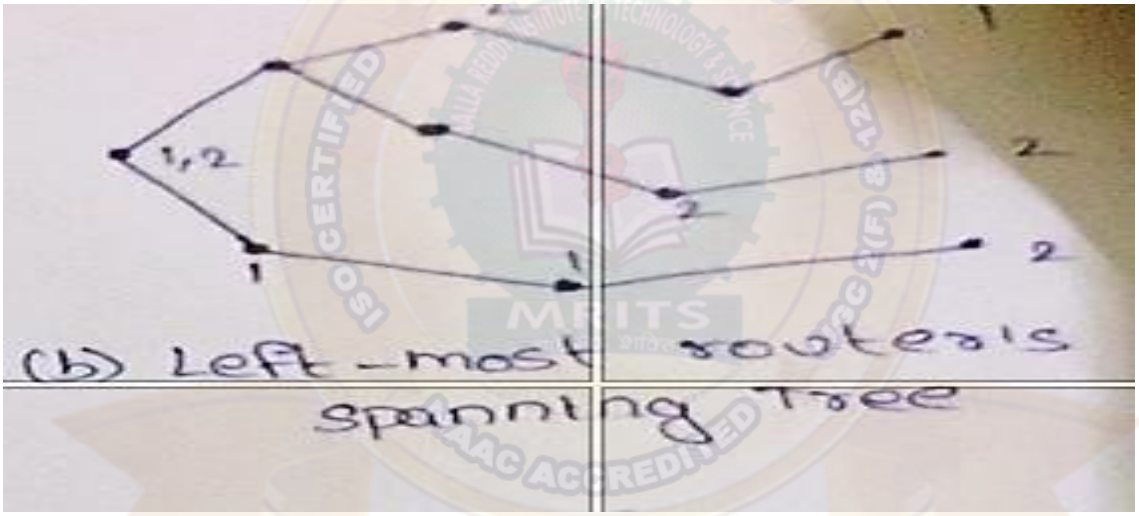
Various ways of constructing spanning tree are possible

The simplest one can be used, if link state routing is used & each router is aware of complete topology, including which hosts belong which groups.

It is important that routers know which of their hosts belong to which groups. Either hosts must inform their routers about changes in group membership or routers must query their host periodically.

Either way, routers learn about which of their hosts are in which groups. Routers tell their neighbors, so information propagates through subnet


1,2
1,2
2
2
1
1
(a) network


1,2
2
2
2
1
1
(b) Left-most routers is
spanning tree


1
1
1
1
) Group 1 multicast tree

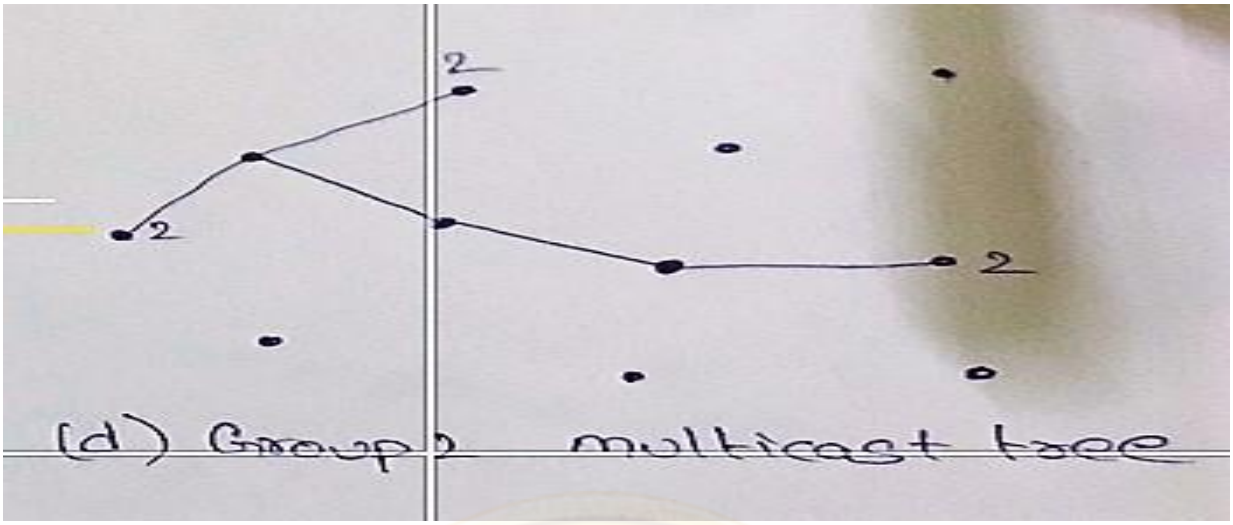


Fig – a, b, c & d: Multicast Routing

DISTANCE VECTOR ROUTING

Distance Vector Routing is a dynamic routing algorithm

This algorithm mainly used in ARPANET

Each router maintains a distance table known as Vector

It is also known as BELLMAN – FORD algorithm

Types:

There are three types in Distance vector Routing are as follows:

1. Iterative
2. Asynchronous
3. Distributed

1. **Iterative**: This process continues until no more information is available to be exchanged between neighbors

2. **Asynchronous:** This does not require that all of its nodes operate in lock step with each other

3. **Distributed**: Each node receives information from one or more of its directly attached neighbors performs calculation & then distributes result back to its neighbors

Working:

The distance vector routing algorithm working conditions are as follows:

a. Knowledge about whole network
b. Routing only to neighbors

c. Information sharing at regular intervals

a. **Knowledge about whole network:** Each router shares its knowledge through entire network.

The router sends its collected knowledge about network to its neighbors.

b. **Routing only to neighbors:** Router sends its knowledge about network to only these routers which have direct links.

The router sends whatever it has about the network through ports.

The information is received by router & uses information to update its own routing table

c. **Information sharing at regular intervals:** Within 30 seconds, router sends information to neighbors' routers.

Algorithm:

Step 1:

Each router prepares its routing table, by their local knowledge.

Each router knows about:

1. All routers present in network
2. Distance to its neighboring routers.

Step 2:

Each router exchanges its distance vector with its neighboring routers

Each router prepares a new routing table using distance vectors it has obtained from its neighbors.

This step is repeater for (n-2) times, if there are n routers in network

After this routing tables converge/ become stable

ADVANTAGES:

SIMPLICITY OF THIS ALGORITHM

DISADVANTAGES:

Doesn't take into account link bandwidth

Vulnerability to "Count – to – Infinity" problem

Takes longer time for convergence as network size grows

EXAMPLE:

- ✓ Consider an example, in which the delay is used as metric and the router knows the delay to each of its neighbours. Once every T msec each router send to each neighbour a list of its estimated delays to each destination. It also receives a similar list from each neighbour. Let xi being x's estimate of how long it takes to get router 'i'. If the router knows that the delay to x is 'm' m sec. To get router i via x is (xi +m) m sec. By performing this

calculation for each neighbour, a router can find out which estimate is the best and use that estimate and the corresponding line in its new routing table.

Fig: Input from A,I,H, K and new routing table for J

Fig.(a) shows the subnet and fig.(b) shows the vectors of J for its neighbours. Fig.(c) shows the new routing table for J. Let JA delay is 8, JI delay is 10, JH is 12, JK is 6.

The new route to G from J can be calculated as follows.

J can get A in 8 m sec.

A can get G in 18 m sec(from table)

∴ J can get G in (8+18) 26 m sec.

Similarly the delay to G via I, H and K is (31 +10) 41, (6+12)18, (31+6)37 m sec.

The best of these values is 18, so it makes an entry in its routing table that the delay to G is 18 m sec and that route is via H.

CONGESTION CONTROL ALGORITHM

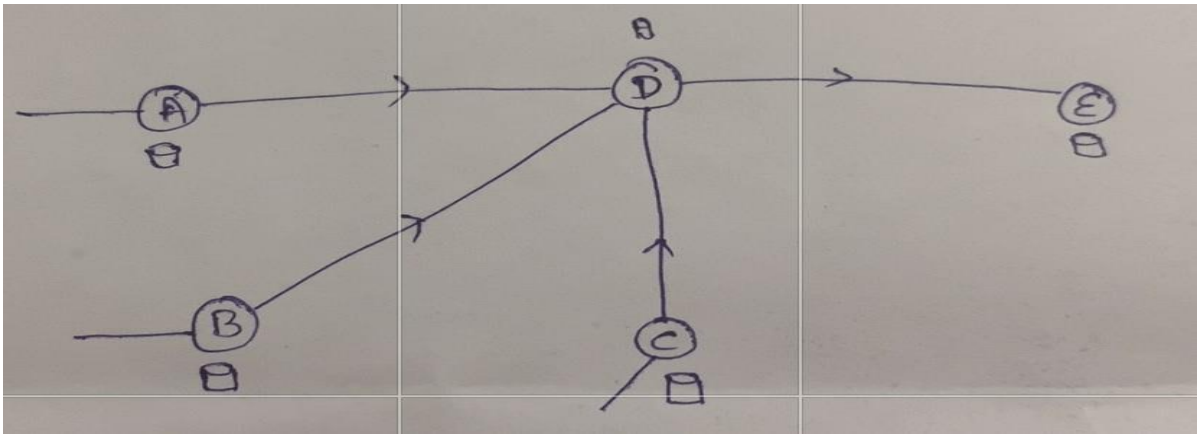
Congestion in a network may occur if load on network greater than capacity of network

load on network > capacity of network

Congestion control refers to mechanism & techniques to control the congestion

When too many packets arrive a part of packet switched network then performance degrades called congestion

For example,



Consider routers sending packets in same time i.e., A, B, C to router D & router D transmits packets to router E, then router D occurs for buffering mode that is congestion state/ not ready state

When next packets from routers A, B, C send again in same time to router D & router D will not transmit packets to router E also because router D occurs for buffering mode that is congestion state/ not ready state.

METHODS:

There are two methods in congestion control algorithm. They are:

1. Open loop congestion control
2. Closed loop congestion control

1. Open loop congestion control:

- Here a protocol to prevent or avoid congestion is called open loop congestion control. For example – flow control, acknowledgement, routing, retransmission, caching, packet discarding

- Traffic stopping:
  a. Leaky bucket algorithm
  b. Token bucket algorithm

Types of open loop congestion control are as follows:

i) SOURCE = We instructs in source packets need to be share time to transmit

ii) DESTINATION = Traffic control

2. Closed loop congestion control:

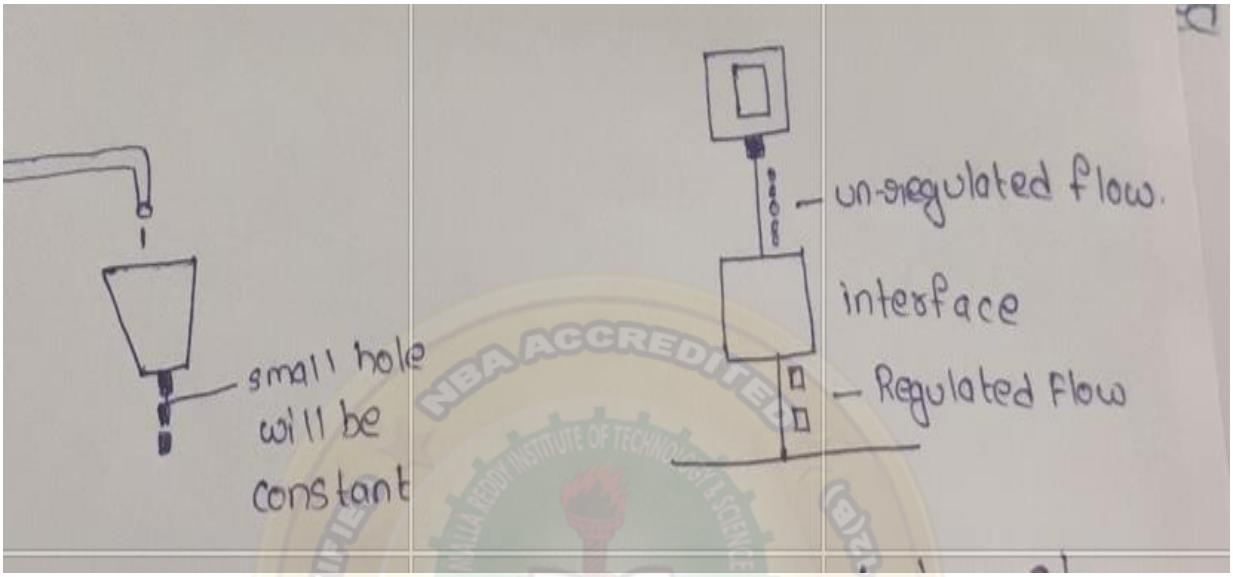
Protocols that allows system to enter congestion state i.e., detect it or remove it

Types of closed loop congestion control are as follows:

i) Explicit feedback = Network monitor status of network

ii) Implicit feedback = based upon fact

LEAKY BUCKET ALGORITHM



Consider a bucket with a small hole at bottom, whatever may be the rate of the water pouring on the bucket the rate at which water comes out the small hole is constant

Host computer will send packets from whatever space but it will be stored at interface ie., un-regulated flow then interface will send packets at regulated flow at constant rate.

Algorithm:

Step 1: When host has sent packet, the packet is thrown into bucket

Step 2: Bucket leaks at a constant rate

Step 3: Busty traffic is converted to a uniform traffic by leaky bucket

Step 4: In practice, the bucket is finite queue that outburst at a finite route

Drawbacks:

It enforces a rigid pattern at output stream irrespective of the Patten of input

TOKEN BUCKET ALGORITHM

If ‘n’ no. of packets received in speed then it transmits packets at same speed

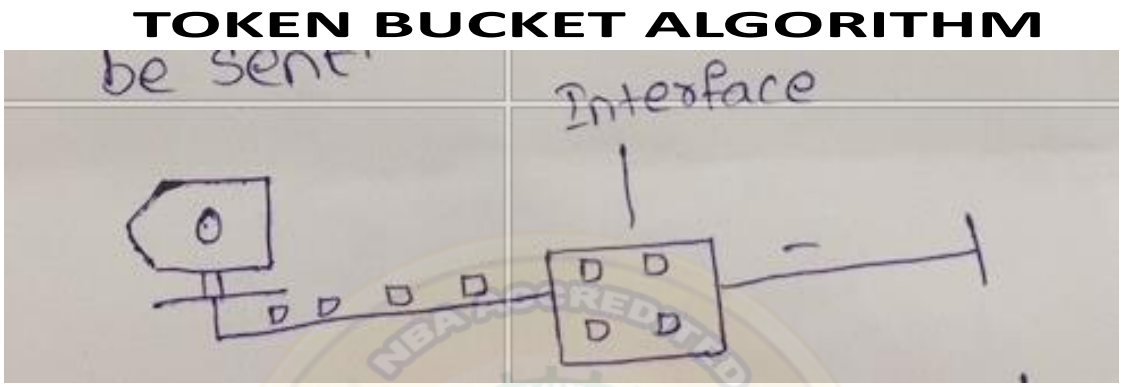
Algorithm:

Step 1: In regular intervals tokens are thrown into bucket

Step 2: Bucket has maximum capacity

Step 3: If there is a ready packet, a token is removed from bucket & packet is send

Step 4: If there is no token in bucket, packet can't be sent.



Implementation of token bucket algorithm is variable used just count the tokens

This counter is just incremented every T second & decremented is when packet is sent**.**

QUALITY OF SERVICES (QOS)

What is QoS in Networking?

Quality of service (QoS) is the use of mechanisms or technologies that work on a network to control traffic and ensure the performance of critical applications with limited network capacity.

It enables organizations to adjust their overall network traffic by prioritizing specific high-performance applications.

QoS is typically applied to networks that carry traffic for resource-intensive systems.

Common services for which it is required include internet protocol television (IPTV), online gaming, streaming media, videoconferencing, video on demand (VOD), and Voice over IP (VoIP).

Working:

QoS networking technology works by marking packets to identify service types, then configuring routers to create separate virtual queues for each application, based on their priority.

QoS technologies provide capacity and handling allocation to specific flows in network traffic.

Types: There are types of QOS are as follows:

1. RELIABILITY
2. DELAY
3. JITTER
4. BANDWIDTH

1. **RELIABILITY**

Reliability is something that a flow needs. Lack of reliability means losing a packet an acknowledgement, which extends re-transmission. However, the sensitivity of application program to reliability is not the same

For example, Video call & Email.

2. **DELAY**

Source & destination is another flow characteristics. Again application can tolerate delay in different degree

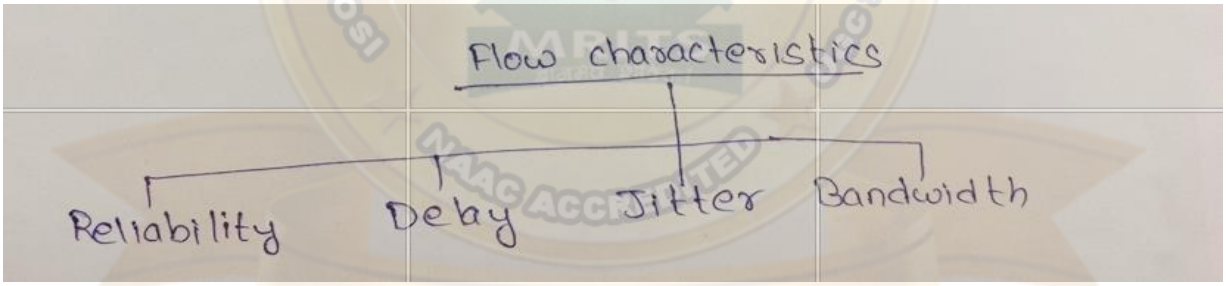
3. **JITTER**

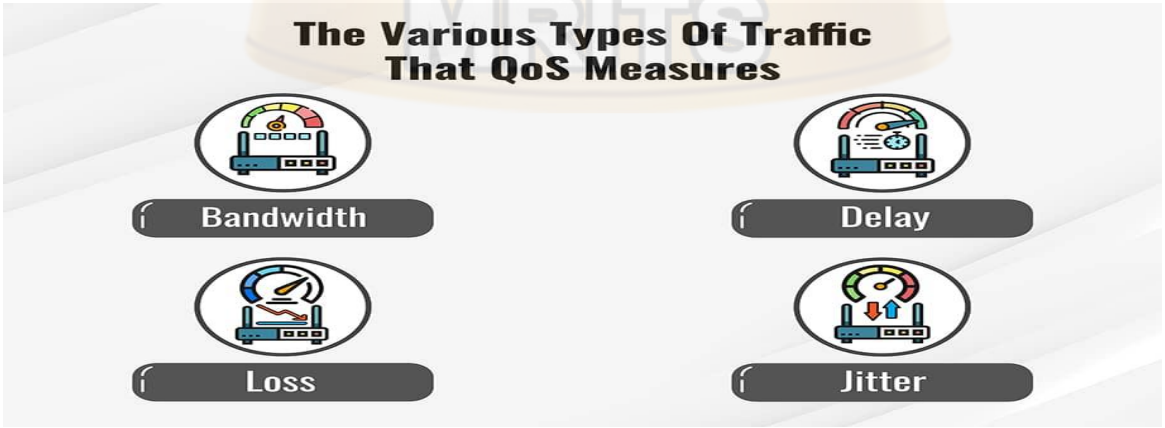
Jitter is variation in delay for packets belonging to same flow. Jitter is defined as variation in packet delay

So, High Jitter means difference between delay is large as same as Low Jitter means variation is small

4. **BANDWIDTH**

The speed of a link. QoS can tell a router how to use bandwidth.





TECHNIQUES

There are several techniques that businesses can use to guarantee the high performance of their most critical applications. These include:

1. Prioritization of delay-sensitive VoIP traffic via routers and switches
2. **Resource reservation**
3. **Queuing**
4. **Traffic marking**

1. Prioritization of delay-sensitive VoIP traffic via routers and switches

Many enterprise networks can become overly congested, which sees routers and switches start dropping packets as they come in and out faster than they can be processed. As a result, streaming applications suffer. Prioritization enables traffic to be classified and receive different priorities depending on its type and destination. This is particularly useful in a situation of high congestion, as packets with higher priority can be sent ahead of other traffic.

2. Resource reservation

The Resource Reservation Protocol (RSVP) is a transport layer protocol that reserves resources across a network and can be used to deliver specific levels of QoS for application data streams. Resource reservation enables businesses to divide network resources by traffic of different types and origins, define limits, and guarantee bandwidth.

3. Queuing:

Queuing is the process of creating policies that provide preferential treatment to certain data streams over others. Queues are high-performance memory buffers in routers and switches, in which packets passing through are held in dedicated memory areas. When a packet is assigned higher priority, it is moved to a dedicated queue that pushes data at a faster rate, which reduces the chances of it being dropped. For example, businesses can assign a policy to give voice traffic priority over the majority of network bandwidth. The routing or switching device will then move this traffic's packets and frames to the front of the queue and immediately transmit them.

4. Traffic marking:

When applications that require priority over other bandwidth on a network have been identified, the traffic needs to be marked. This is possible through processes like Class of Service (CoS), which marks a data stream in the Layer 2 frame header, and Differentiated Services Code Point (DSCP), which marks a data stream in the Layer 3 packet header.

Advantages of QoS:

Major advantages of deploying QoS include:

a. Unlimited application prioritization
b. Better resource management
c. Enhanced user experience
d. Point-to-point traffic management
e. Packet loss prevention
f. Latency reduction

a. Unlimited application prioritization

QoS guarantees that businesses' most mission-critical applications will always have priority and the necessary resources to achieve high performance

b. Better resource management

QoS enables administrators to better manage the organization's internet resources. This also reduces costs and the need for investments in link expansions

c. Enhanced user experience

The end goal of QoS is to guarantee the high performance of critical applications, which boils down to delivering optimal user experience. Employees enjoy high performance on their high-bandwidth applications, which enables them to be more effective and get their job done more quickly.

d. **Point-to-point traffic management:**

Managing a network is vital however traffic is delivered, be it end to end, node to node, or point to point. The latter enables organizations to deliver customer packets in order from one point to the next over the internet without suffering any packet loss.

e. **Packet loss prevention:**

Packet loss can occur when packets of data are dropped in transit between networks. This can often be caused by a failure or inefficiency, network congestion, a faulty router, loose connection, or poor signal. QoS avoids the potential of packet loss by prioritizing bandwidth of high-performance applications.

f. **Latency reduction:**

Latency is the time it takes for a network request to go from the sender to the receiver and for the receiver to process it. This is typically affected by routers taking longer to analyze information and storage delays caused by intermediate switches and bridges. QoS enables organizations to reduce latency, or speed up the process of a network request, by prioritizing their critical application.

INTERNETWORKING

Internetworking is process or technique of connecting different networks by using intermediary devices such as routers or gateways devices.

Internetworking ensures data communication among networks owned & operated by different entities using a common data communication & internet routing protocol

Internetworking is a term used by CISCO. Any inter-connection among or between public, private or commercial, industrial or government. Computer may also defined as Internetwork or Internetworking

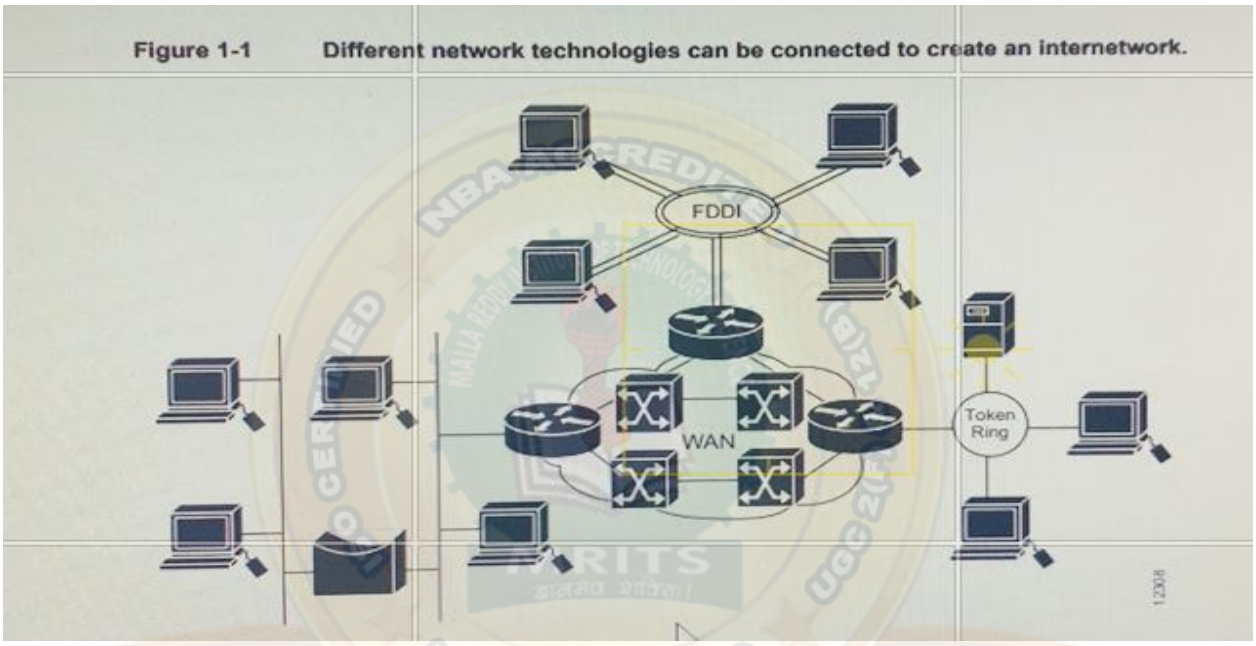
The standard reference model for Internetworking is Osi/ ISO model

Two architectural models are commonly used to describe protocols & methods used in Internetworking

An internetwork is a collection of individual networks, connected by intermediate networking devices, that functions as a single large network.

Internetworking refers other industry, products and procedures that meet the challenge of creating and administering internetworks.

Architecture:



(or)

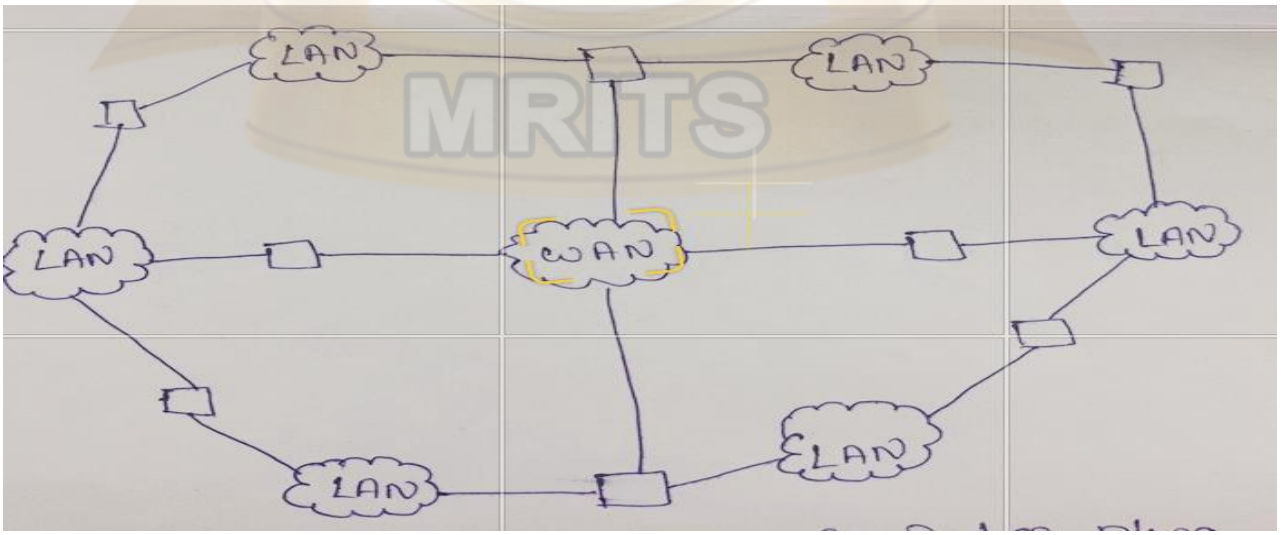


Fig: Architecture of Internetworking

History of Internetworking

The first networks were time-sharing networks that used mainframes and attached terminals. Such environments were implemented by both IBM's System Network Architecture (SNA) and Digital's network architecture.

Local area networks (LANs) evolved around the PC revolution. LANs enabled multiple users in a relatively small geographical area to exchange files and messages, as well as access shared resources such as file servers.

Wide area networks (WANs) interconnect LANs across normal telephone lines (and other media), thereby interconnecting geographically dispersed users.

Today, high-speed LANs and switched internetworks are becoming widely used, largely because they operate at very high speeds and support such high-bandwidth applications as voice and video conferencing.

Internetworking evolved as a solution to three key problems: isolated LANs, duplication of resources, and a lack of network management. Isolated LANS made electronic communication between different offices or departments impossible. Duplication of resources meant that the same hardware and software had to be supplied to each office or department, as did a separate support staff. This lack of network management meant that no centralized method of managing and troubleshooting networks existed.

Types

Internetworking is implemented in layer – 3 (network layer) of this model. The example of Internetworking is internet.

There are three types in internetworking are as follows:

1. Extranet
2. Intranet
3. Internet

Intranet & Extranet may or may not have connections to the internet

If internet is connected then Intranet & Extranet is normally protected from being accessed without authorization

1. Extranet

An Extranet is a network of internetwork or internetworking that is limited in scope to a single organization or entity but has limited connections to networks of one or more other. Usually, but not necessarily, trusted organization or entities. Extranet may also be categorized as a MAN, Wan or other type network

2. Intranet

An intranet is a set of interconnected networks or internetworking using internet protocol & uses IP-based tools such as web browser & FTP tools that is under control of single administrative entity.

A large Intranet will have its own web – server to provide users with information

3. Internet

A specific internetworking consists of a worldwide inter-connection of government, academic, public & private networks based upon ARPANET (**Advanced Research Projects Agency Network**) developed by ARPA of U.S. department of defense also home to WWW (World wide Web) & referred as ' Internet'.

Internetworking Challenges

Implementing a functional internetwork is no simple task. Many challenges must be faced, especially in the areas of connectivity, reliability, network management, and flexibility. Each area is key in establishing an efficient and effective internetwork.

The challenge when connecting various systems is to support communication between disparate technologies. Different sites, for example, may use different types of media, or they might operate at varying speeds.

Another essential consideration, reliable service, must be maintained in any internetwork. Individual users and entire organizations depend on consistent, reliable access to network resources.

Furthermore, network management must provide centralized support and troubleshooting capabilities in an internetwork. Configuration, security, performance, and other issues must be adequately addressed for the internetwork to function smoothly.

Flexibility, the final concern, is necessary for network expansion and new applications and services, among other factors.

The Network Layer in the Internet

Internet

The Internet layer, also known as the **network layer** or **IP layer**, accepts and delivers packets for the network. This layer includes the powerful Internet Protocol (IP), the Address Resolution Protocol (ARP), and the Internet Control Message Protocol (ICMP).

Network layer

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.

Why Network Layer in the Internet

The Internet can be viewed as a collection of sub-networks or Autonomous Systems (AS).
IP (Internet Protocol) hosts the whole Internet together.
Communication in the Internet works as follows:

- The transport layer takes data streams and breaks them up into datagram's.
- Each datagram is transmitted through the Internet.
- When all the pieces finally get to the destination machine, they are reassembled by the network layer, which inserts it into the receiving process' input stream.

IP Protocol

The IP protocol and its associated routing protocols are possibly the most significant of the entire TCP/IP suite.

IP is responsible for the following:

1. **IP addressing**
2. **Host-to-host communications**
3. **Packet formatting**
4. **Fragmentation**

1. IP addressing

The IP addressing conventions are part of the IP protocol. Designing an IPv4 Addressing Scheme introduces IPv4 addressing and IPv6 Addressing Overview introduces IPv6 addressing.

2. Host-to-host communications –

IP determines the path a packet must take, based on the receiving system's IP address.

3. Packet formatting –

IP assembles packets into units that are known as **datagram's**. Datagram's are fully described in Internet Layer: Where Packets Are Prepared for Delivery.

4. Fragmentation –

If a packet is too large for transmission over the network media, IP on the sending system breaks the packet into smaller fragments. IP on the receiving system then reconstructs the fragments into the original packet. Oracle Solaris supports both IPv4 and IPv6 addressing formats, which are described in this book. To avoid confusion when addressing the Internet Protocol, one of the following conventions is used:

a. When the term "IP" is used in a description, the description applies to both IPv4 and IPv6.

b. When the term "IPv4" is used in a description, the description applies only to IPv4.

c. When the term "IPv6" is used in a description, the description applies only to IPv6.

ICMP Protocol

The Internet Control Message Protocol (ICMP) detects and reports network error conditions. ICMP reports on the following:

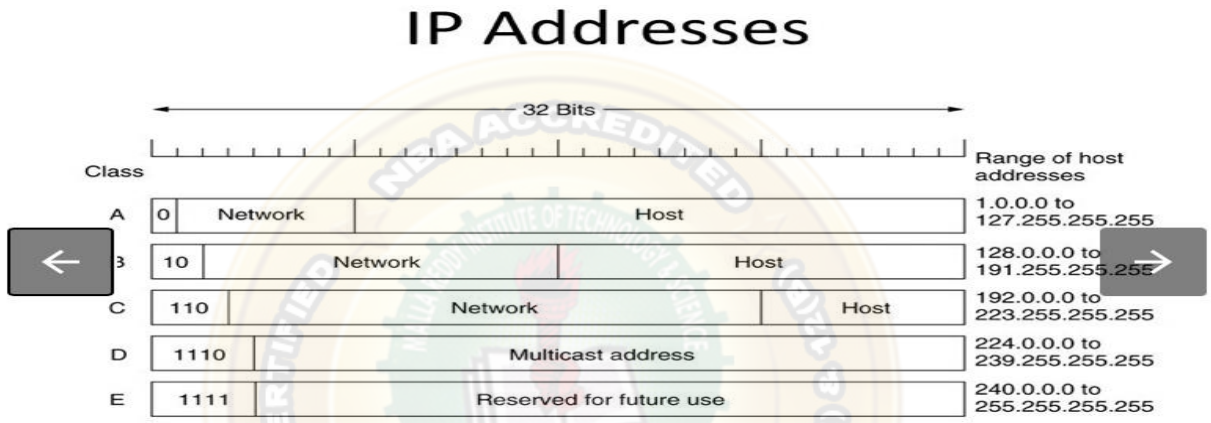
1. **Dropped packets** – Packets that arrive too fast to be processed

2. **Connectivity failure** – A destination system cannot be reached

3. **Redirection** – Redirecting a sending system to use another router

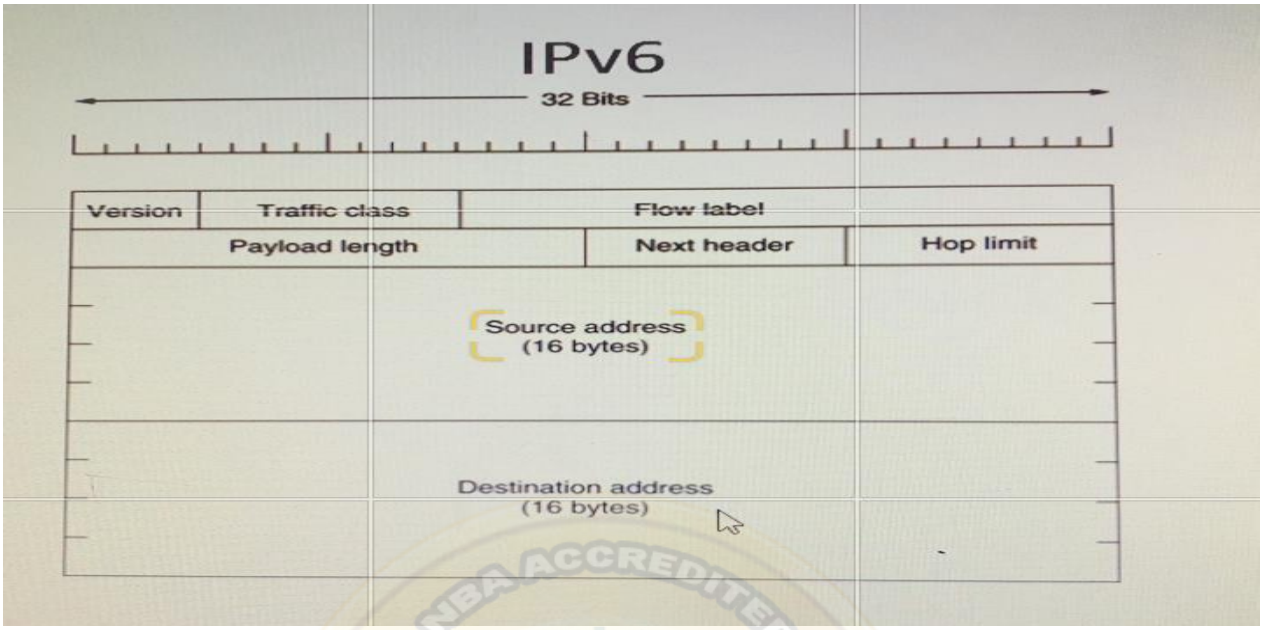
IP Addresses

Traditionally, IP addresses were divided into the five categories: A, B, C, D, E. Network numbers are managed by a nonprofit corporation called ICANN (Internet Corporation for Assigned Names and Numbers) to avoid conflicts. Network address, which are 32-bit numbers, are usually written in dotted decimal notation.



1. IPV6

- The newest version of IP (version 6, or IPng) uses 128 bits, yielding
- 2^128 unique combinations
- IPv6 is slowly be integrated in the existing Internet.
- IPv4's 32 bits continues to be the dominant form of IP addressing



- **VERSION**. 4 BITS – IPV6 VERSION NUMBER

- **Traffic Class**. 8 bits. - Internet traffic priority delivery value.

- **Flow Label**. 20 bits. - Used for specifying special router handling from source to destination(s) for a sequence of packets.

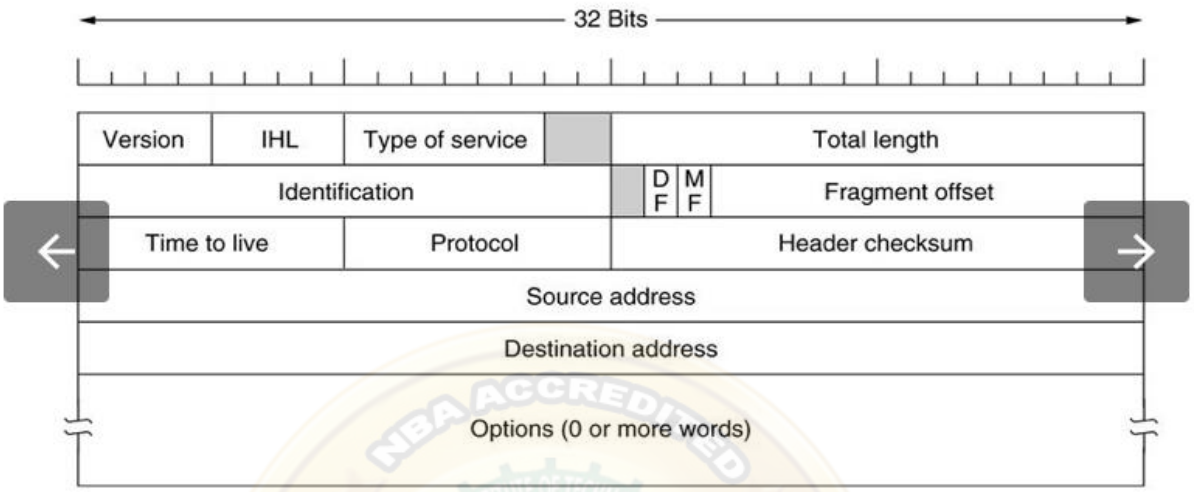
- **Payload Length**. 16 bits, unsigned. - Specifies the length of the data in the packet. When set to zero, the option is a hop-by-hop Jumbo payload.
- **Next Header**. 8 bits. - Specifies the next encapsulated protocol. The values are compatible with those specified for the IPv4 protocol field.

- **Hop Limit**. 8 bits, unsigned. -For each router that forwards the packet, the hop limit is decremented by 1. When the hop limit field reaches zero, the packet is discarded. This replaces the TTL field in the IPv4 header that was originally intended to be used as a time based hop limit.
- **Source address**. 16 bytes. - The IPv6 address of the sending node.
- **Destination address**. 16 bytes. -The IPv6 address of the destination node.

2. IpV4

The newest version of IP (version 6, or IPng) uses 128 bits, yielding
2^128 unique combinations
IPv6 is slowly be integrated in the existing Internet.
IPv4's 32 bits continues to be the dominant form of IP addressing

The IP Header -V4



- **Header length** – The length of the datagram header in 32-bit words.

- **Type of service** – Contains five subfields that specify the precedence (priority 0-7), delay, throughput, reliability, and cost desired for a packet.

- **Total length** – The length of the datagram in bytes including the header, options, and the appended transport protocol segment or packet. The maximum length is bytes.

- **Identification** – An integer that identifies the datagram.
- **DF** – Don't fragment
- **MF** – More Fragments. All fragments except the last one have this bit set.
- **Fragment offset** – The relative position of this fragment measured from the beginning of the original datagram in units of 8 bytes.

- **Time to live** – How many routers a datagram can pass through. Each router decrements this value by 1 until it reaches 0 when the datagram is discarded. This keeps misrouted datagram's from remaining on the Internet forever.

- **Protocol** – The high-level protocol type.

- **Header checksum** – A number that is computed to ensure the integrity of the header values.

- **Source address** – The 32-bit IPv4 address of the sending host.

- **Destination address** – The 32-bit IPv4 address of the receiving host.

- **Options** – A list of optional specifications for security restrictions, route recording, and source routing. Not every datagram specifies an options field.

- **Padding** – Null bytes which are added to make the header length an integral multiple of 32 bytes as required by the header length field.

UNIT – IV

Transport Layer**:**
Transport Services, Elements of Transport protocols, Connection management, TCP & UDP protocols.

UNIT – IV

Transport Layer

The transport layer is the fourth layer in the OSI layered architecture.
The transport layer is responsible for reliable data recovery.
The upper – layer protocols depends heavily on the transport layer protocol.
A high level of recovery is also provided in this layer.
This layer ensures, that packets are delivered error free, in sequence & with no losses & duplication.

Duties of transport layer:

This layer breaks messages into packets
It performs error recovery if the lower layers are not adequately error free.
Function of flow control if not done adequately at the network layer.
Functions of multiplexing & de-multiplexing sessions together.
This layer can be responsible for setting up & releasing connections across the network
Data Link Layer is responsible for delivery of frames between 2 neighboring nodes over a link called Node – to – Node delivery
Network layer is responsible for Host – to – Host delivery i.e., delivery of datagram's between 2 hosts.
Transport layer is responsible for Process – to – Process delivery i.e. delivery of a packet, part of a message from one process to another.
Client – Server paradigm is used for process – to – Process communication. A process on the local machine (hot) called a client needs services from a process usually on the remote host called Server.
Now a days, operating system support multi-user & multi-programming environments. A remote computer can run several server programs at the same time. Following parameters are used for communication

Local host	Local process	Remote host	Remote process

The services that a transport protocol can provide are often constrained by the service model of the underlying network layer protocol. If network layer protocol cannot provide delay or bandwidth guarantee for 4 PDU's sent between hosts, then the transport layer protocol cannot provide delay or bandwidth guarantees for messages sent between processes.
Some of the services offered by the transport protocol even when the underlying network protocol does not offer the corresponding service at the network layer.
A Transport protocol can offer reliable data transfer service to an application even when the underlying network protocol is unreliable, even when the network protocol loses, garbles & duplicate packets.

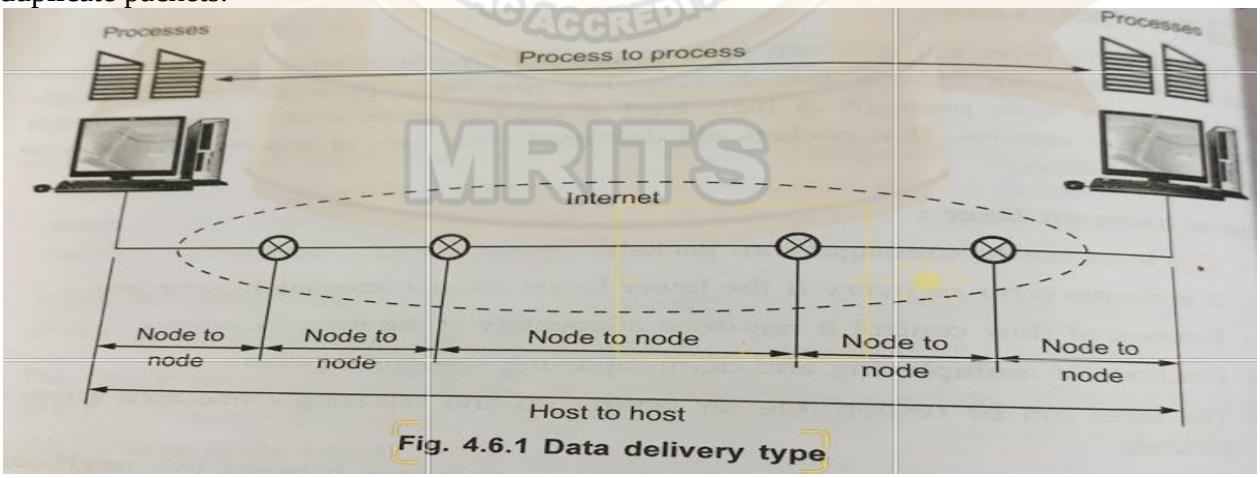


Fig. 4.6.1 Data delivery type

ADDRESSING METHOD

We need a address where to deliver something to one specific destination among may. All the layers uses different addressing methods
Data link Layer uses MAC address to choose one node among several nodes, if the connection is not point to point

Network layer uses IP address to choose one host among millions of host. In network layer, datagram needs a destination IP address for delivery & a source Ip address for a destination reply

Transport layer requires transport layer address called a port number for selecting among multiple processes running on the destination host. Source port number is used for reply & destination port number for delivery.

Port numbers from 0 to 65535 are used in Internet. It is the 16 – bits integer so the range is 0 to 65535. The client program defines itself with a port number, chosen randomly by the transport layer software running on the client host. This is the EPHEMERAL PORT NUMBER.

Server also defines a port number but not randomly. Internet has decided to use universal port numbers for servers; these are called well known port numbers. The port numbers ranging from 0 to 1023 are called well known port numbers & are restricted, which means that they are reserved for use by well known application protocols such as HTTP.

IANA RANGES

The IANA (Internet Assigned Number Authority) has divided the port number into 3 ranges are as follows:

Well known ports	Registered port	Dynamic ports

S. No.	Port Type	Range	Remark
1.	Well known ports	0 to 1023	Assigned & controlled by IANA
2.	Registered port	1024 to 49151	Not assigned & controlled by IANA. Only registered to prevent duplication
3.	Dynamic port	49152 to 65535	Neither controlled nor registered. Used by any process. These are ephemeral ports

Transport Services

1. Services provided to the upper layer

The transport protocol should provide to higher-level protocols. The transport entity that provides services to transport service users, which might be an application process. The hardware & software within the transport layer that does the work called the transport entity. It can be in the operating system kernel, in a separate user process or on the network interface card, the relation of the network, transport & application layers.

Categories of service are useful for describing the transport services are as follows

a) Type of service
b) Quality of service
c) Data transfer
d) User interface
e) Connection management
f) Expedited delivery
g) Status reporting
h) Security

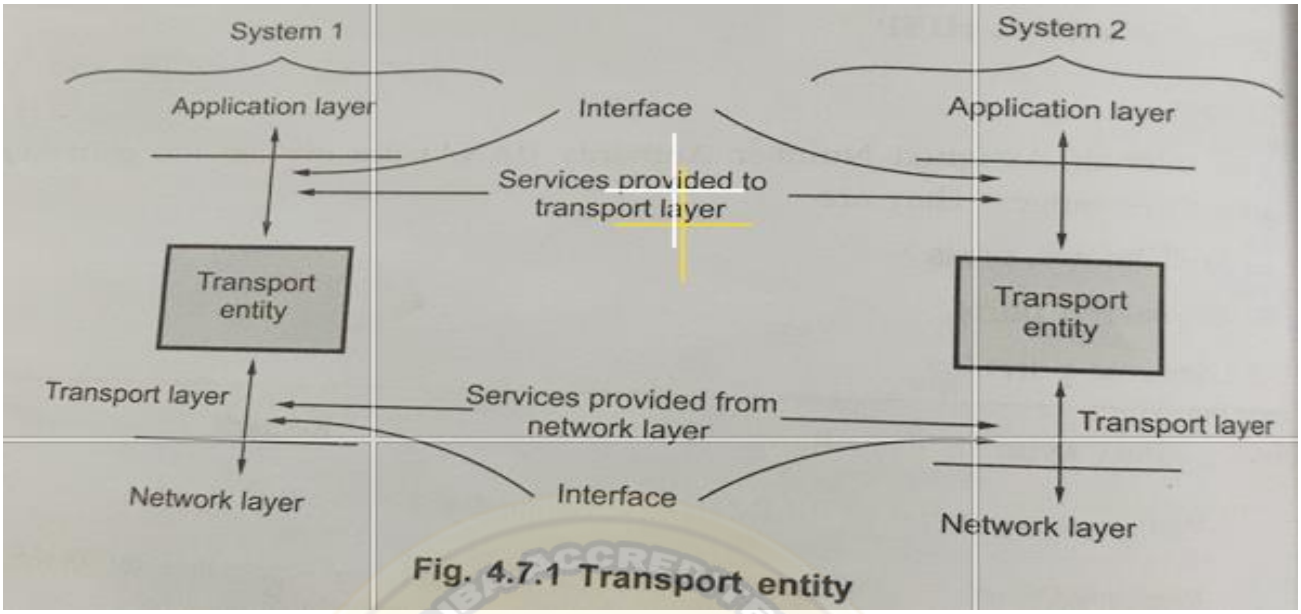


Fig. 4.7.1 Transport entity

a) Type of service

It provides 2 types of services connection – oriented & connection – less or datagram service. A connection – oriented service provides for the establishment, maintenance & termination of a logical connection between transport service users. The connection – oriented service generally implies that the service is reliable. The connection – oriented service allows for connection – related features such as flow control, error control & sequenced delivery.

b) Quality of service

The transport protocol entity should allow the transport service user to specify the quality of transmission service to be provided. Following are the transport layer quality of service parameters

- Error & loss levels
- Desired average & maximum delay
- Throughput
- Priority level
- Resilience

The error & loss level measures the no. of lost or garbled messages as a fraction of the total sent.

The desired average & maximum delay measures the time between messages is being sent by the transport user on the source machine & it's being received by the transport user in the destination machine.

The throughput parameter measures the number of bytes of user data transferred per second, measured over some time interval.

The priority level parameter provides a way for a transport user to indicate that some of its connection is more important than other ones.

The higher priority connections get serviced before the low priority ones.

Examples of applications that might request particular qualities of service are as follows:

i) A FTP might require high throughput
ii) A transaction protocol may require low delay.
iii) An E-mail protocol may require multiple priority protocols

c) Data transfer

It transfers data between 2 transport entities. Both user data & control data must be transferred. Full duplex service must be provided. Half - duplex & simplex modes may also be offered

d) User interface

There is not clear mechanism of the user interface to the transport protocol should be standardized.

e) Connection management

If connection – oriented service is provided, the transport entity is responsible for establishing & terminating connections. Symmetric connection procedure should be provided, which allows either TS user to initiate connection establishment.

f) Expedited delivery

It performs fast delivery of data packets

g) Status reporting

It gives the following information:

(i) Addresses
(ii) Performance characteristics of a connection
(iii)Class of protocol in use
(iv)Current timer values

h) Security

The transport entity may provide a variety of security services. It provides encryption & decryption of data. The transport entity may be capable of routing through secure links or nodes if such a service is available from the transmission facility.

2. TRANSPORT SERVICE PRIMITIVES

To allow users to access the transport service, the transport layer must provide some operations to application programs. Real networks can lose packets, so the network service is generally unreliable. The transport service is reliable. Network service is used only by the transport entities. The transport service must be convenient & easy to use

At the transport layer, even a simple unidirectional data exchange is more complicated than at the network layer. Every data packet sent will also be acknowledged. These acknowledgements are managed by the transport entities using the network layer protocol & are not visible to transport user.

TPDU (Transport Protocol Data Unit) for messages sent from transport entity to transport entity. TPDU are contained in packets. Packets are contained in frames. When a frame Arrives, the data link layer processes the frame header & passes the contents of the frame payload field up to the network entity. The network entity processes the packet header & passes the contents of the packet payload up to the transport entity.

PRIMITIVE	PACKET SENT	MEANING
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ	Actively attempt to establish a connection
SEND	DATA	Send information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ	This side wants to release the connection

FIG: **PRIMITIVES USED FOR A SIMPLE TRANSPORT SERVICE**

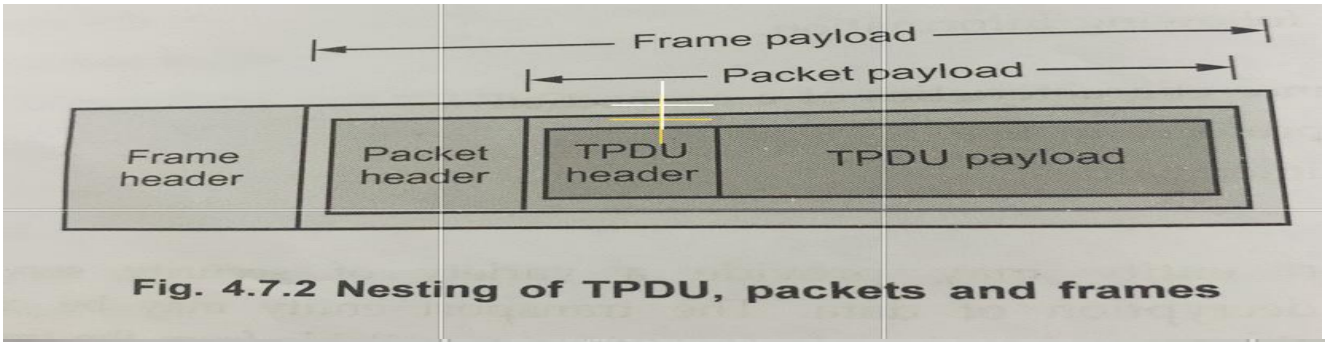


Fig. 4.7.2 Nesting of TPDU, packets and frames

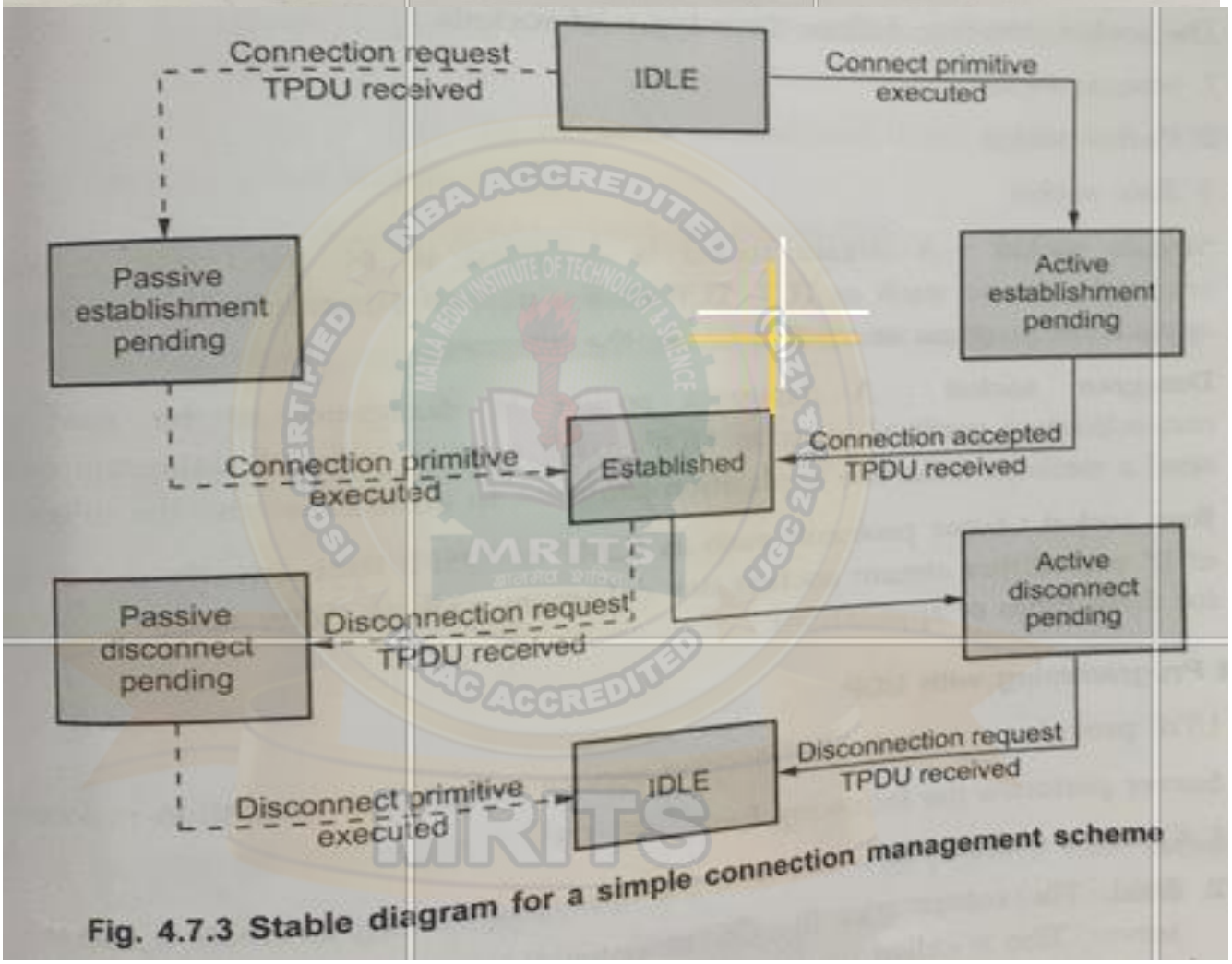


Fig. 4.7.3 Stable diagram for a simple connection management scheme

3. SOCKET

A socket acts as end point. 2 processes need a socket at each end to communicate with each other. A socket is to defined in the operating system as a structure.

Socket structures with 5 fields are as follows:

(i) Family: This field defines the protocol group: IPV4, IPV6unix domain protocols and so on

(ii) **Type:** This field defines the type of socket: stream socket, pocket socket or raw socket.

(iii)Protocol: This field is usually set to zero for TCP & UDP

(iv)**Local Socket addresses:** This field defines the local socket address, a combination of the local Ip address & the port address of the local application program.

(v) **Remote Socket address**: This field defines the remote socket address, a combination of the remote IP address & the port address of the application program.

Socket types:

The socket interface defines 3 types of sockets:

Stream socket	Packet Socket	Raw Socket

1. Stream socket: A stream socket is designed to be used with a connection oriented protocol such as TCP. TCP uses a pair of stream sockets to connect one application program to another across the internet.
2. Datagram Socket: A datagram socket is designed to be used with a connectionless protocol such as UDP. UDP uses a pair of datagram sockets for send a message from one application program to another across the internet.
3. Raw Socket: Some protocols such as ICMP or OSPF that directly use the services of IP use neither stream sockets nor datagram sockets. Raw sockets are designed for these types of applications

Socket programming with udp

UDP provides an unreliable transport service to its communication processes

Server performs the following functions:

i) Create a Socket: The server asks the operating system to create a socket

ii) Bind: The server asks the OS to enter the information in the socket related to server is called binding the server socket

iii) Receive a request: The server asks the OS to wait for a request destined for this socket & to receive it

iv) Process the request: The request is processed by the server

v) Send the result: The response is sent to the circuit

Client performs the following functions:

a) **Create a socket:** The client asks the OS a create a socket. There is no need for binding here.
b) **Sent the request:** The client asks the OS to send a request
c) **Receive:** The client asks the OS to wait for the response & deliver it when it has arrived.
d) **Destroy the Socket:** When the client has no more requests, it asks the OS to destroy the socket.

Socket programming with TCP

Server performs the following functions:

a) **Create a socket:** The server asks the OS to create a socket
b) **Bind:** The server asks the OS to enter information in the socket created in the previous step
c) **Listen:** The server asks the OS to be passive & listen to the client that needs to be connected to this server
d) **Read:** Read a stream of bytes from the connection
e) **Process:** Processes the stream of bytes
f) **Write:** Writes the results as a stream of bytes to the connection
g) Destroy socket

Client performs the following functions:

a) Create a Socket
b) Connect
c) Write
d) Read
e) Destroy

To establish a reliable service between two machines on a network, transport protocols are implemented, which somehow resembles the data link protocols implemented at layer 2. The major difference lies in the fact that the data link layer uses a physical channel between two routers while the transport layer uses a subnet.

Following are the issues for implementing transport protocols−

Types of Service

The transport layer also determines the type of service provided to the users from the session layer. An error-free point-to-point communication to deliver messages in the order in which they were transmitted is one of the key functions of the transport layer.

Error Control

Error detection and error recovery are an integral part of reliable service, and therefore they are necessary to perform error control mechanisms on an end-to-end basis. To control errors from lost or duplicate segments, the transport layer enables unique segment sequence numbers to the different packets of the message, creating virtual circuits, allowing only one virtual circuit per session.

Flow Control

The underlying rule of flow control is to maintain a synergy between a fast process and a slow process. The transport layer enables a fast process to keep pace with a slow one. Acknowledgements are sent back to manage end-to-end flow control. Go back N algorithms are used to request retransmission of packets starting with packet number N. Selective Repeat is used to request specific packets to be retransmitted.

Connection Establishment/Release

The transport layer creates and releases the connection across the network. This includes a naming mechanism so that a process on one machine can indicate with whom it wishes to communicate. The transport layer enables us to establish and delete connections across the network to multiplex several message streams onto one communication channel.

Multiplexing/De multiplexing

The transport layer establishes a separate network connection for each transport connection required by the session layer. To improve throughput, the transport layer establishes multiple network connections. When the issue of throughput is not important, it multiplexes several transport connections onto the same network connection, thus reducing the cost of establishing and maintaining the network connections.

When several connections are multiplexed, they call for demultiplexing at the receiving end. In the case of the transport layer, the communication takes place only between two processes and not between two machines. Hence, communication at the transport layer is also known as peer-to-peer or process-to-process communication.

Fragmentation and re-assembly

When the transport layer receives a large message from the session layer, it breaks the message into smaller units depending upon the requirement. This process is called fragmentation.

Thereafter, it is passed to the network layer. Conversely, when the transport layer acts as the receiving process, it reorders the pieces of a message before reassembling them into a message.

Addressing

Transport Layer deals with addressing or labeling a frame. It also differentiates between a connection and a transaction. Connection identifiers are ports or sockets that label each frame, so the receiving device knows which process it has been sent from. This helps in keeping track of multiple-message conversations. Ports or sockets address multiple conservations in the same location.

TCP CONNECTION MANAGEMENT

TCP stands for **Transmission Control Protocol**. It is a transport layer protocol that facilitates the transmission of packets from source to destination. It is a connection-oriented protocol that means it establishes the connection prior to the communication that occurs between the computing devices in a network. This protocol is used with an IP protocol, so together, they are referred to as a TCP/IP.

The main functionality of the TCP is to take the data from the application layer. Then it divides the data into a several packets, provides numbering to these packets, and finally transmits these packets to the destination. The TCP, on the other side, will reassemble the packets and transmits them to the application layer. As we know that TCP is a connection-oriented protocol, so the connection will remain established until the communication is not completed between the sender and the receiver.

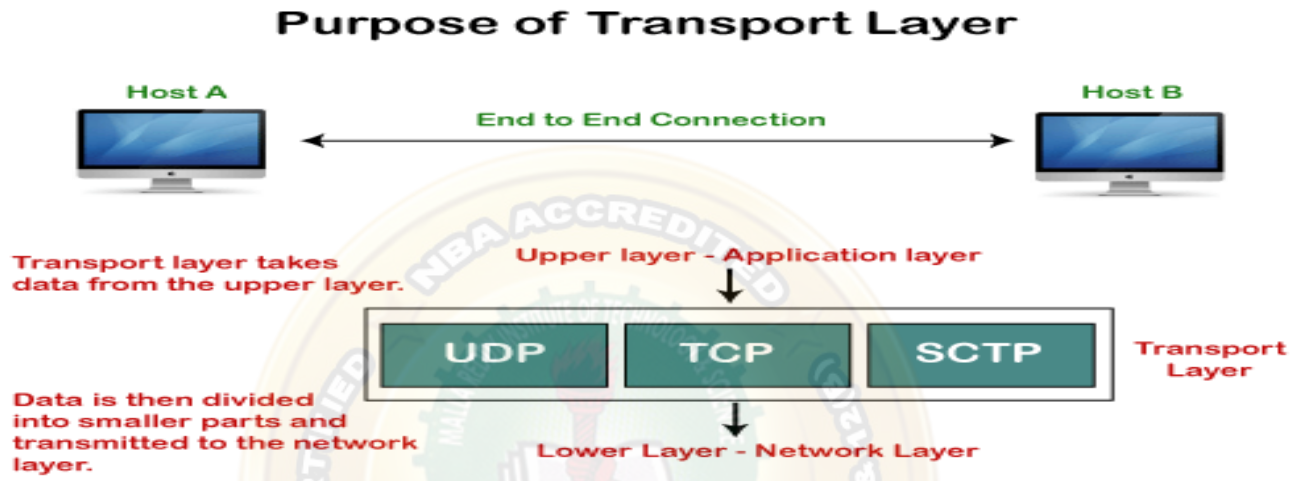
Features of TCP protocol

The following are the features of a TCP protocol:

- **Transport Layer Protocol -** TCP is a transport layer protocol as it is used in transmitting the data from the sender to the receiver.
- **Reliable -** TCP is a reliable protocol as it follows the flow and error control mechanism. It also supports the acknowledgment mechanism, which checks the state and sound arrival of the data. In the acknowledgment mechanism, the receiver sends either positive or negative acknowledgment to the sender so that the sender can get to know whether the data packet has been received or needs to resend.
- **Order of the data is maintained -** This protocol ensures that the data reaches the intended receiver in the same order in which it is sent. It orders and numbers each segment so that the TCP layer on the destination side can reassemble them based on their ordering.
- **Connection-oriented -** It is a connection-oriented service that means the data exchange occurs only after the connection establishment. When the data transfer is completed, then the connection will get terminated.
- **Full duplex -** It is a full-duplex means that the data can transfer in both directions at the same time.
- **Stream-oriented -** TCP is a stream-oriented protocol as it allows the sender to send the data in the form of a stream of bytes and also allows the receiver to accept the data in the form of a stream of bytes. TCP creates an environment in which both the sender and receiver are connected by an imaginary tube known as a virtual circuit. This virtual circuit carries the stream of bytes across the internet.

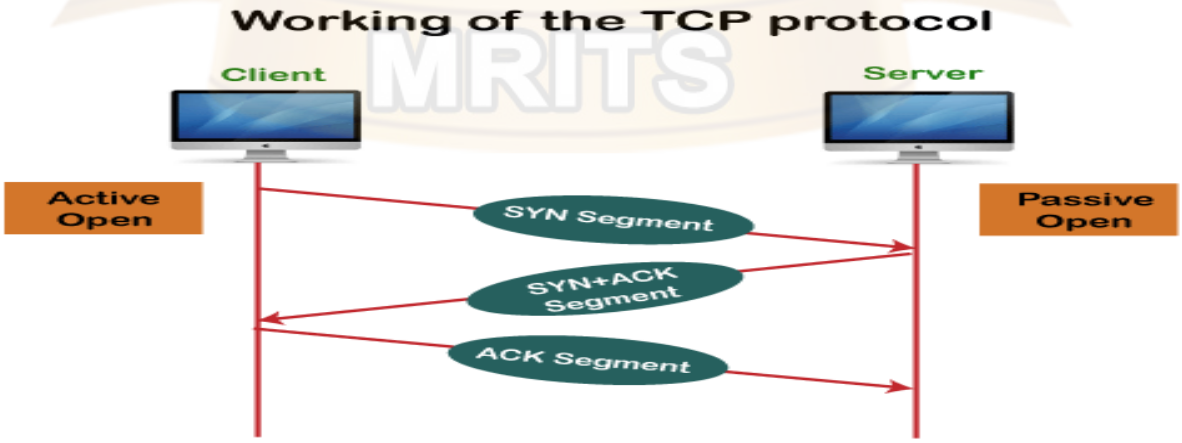
Need of Transport Control Protocol

In the layered architecture of a network model, the whole task is divided into smaller tasks. Each task is assigned to a particular layer that processes the task. In the TCP/IP model, five layers are application layer, transport layer, network layer, data link layer, and physical layer. The transport layer has a critical role in providing end-to-end communication to the directly application processes. It creates 65,000 ports so that the multiple applications can be accessed at the same time. It takes the data from the upper layer, and it divides the data into smaller packets and then transmits them to the network layer.



Working of TCP

In TCP, the connection is established by using three-way handshaking. The client sends the segment with its sequence number. The server, in return, sends its segment with its own sequence number as well as the acknowledgement sequence, which is one more than the client sequence number. When the client receives the acknowledgment of its segment, then it sends the acknowledgment to the server. In this way, the connection is established between the client and the server.



Advantages of TCP

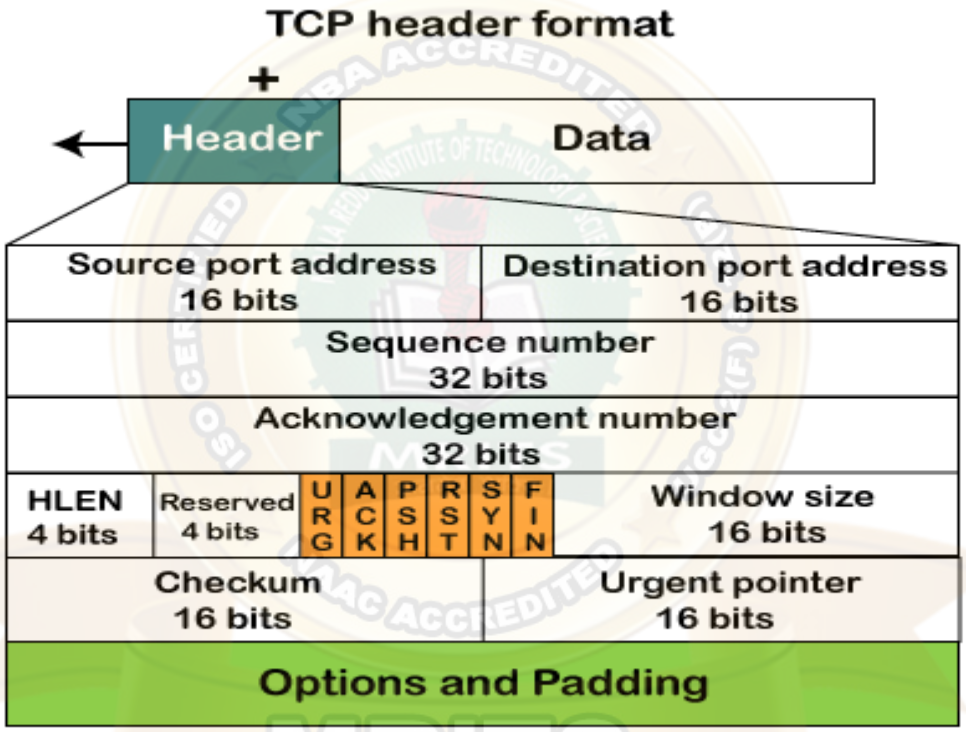
- It provides a connection-oriented reliable service, which means that it guarantees the delivery of data packets. If the data packet is lost across the network, then the TCP will resend the lost packets.

- It provides a flow control mechanism using a sliding window protocol.
- It provides error detection by using checksum and error control by using Go Back or ARP protocol.
- It eliminates the congestion by using a network congestion avoidance algorithm that includes various schemes such as additive increase/multiplicative decrease (AIMD), slow start, and congestion window.

Disadvantage of TCP

It increases a large amount of overhead as each segment gets its own TCP header, so fragmentation by the router increases the overhead.

TCP Header format



- **Source port:** It defines the port of the application, which is sending the data. So, this field contains the source port address, which is 16 bits.
- **Destination port:** It defines the port of the application on the receiving side. So, this field contains the destination port address, which is 16 bits.
- **Sequence number:** This field contains the sequence number of data bytes in a particular session.
- **Acknowledgment number:** When the ACK flag is set, then this contains the next sequence number of the data byte and works as an acknowledgment for the previous data received. For example, if the receiver receives the segment number 'x', then it responds 'x+1' as an acknowledgment number.
- **HLEN:** It specifies the length of the header indicated by the 4-byte words in the header. The size of the header lies between 20 and 60 bytes. Therefore, the value of this field would lie between 5 and 15.
- **Reserved:** It is a 4-bit field reserved for future use, and by default, all are set to zero.

- **Flags**
  There are six control bits or flags:
  1. **URG:** It represents an urgent pointer. If it is set, then the data is processed urgently.
  2. **ACK:** If the ACK is set to 0, then it means that the data packet does not contain an acknowledgment.
  3. **PSH:** If this field is set, then it requests the receiving device to push the data to the receiving application without buffering it.
  4. **RST:** If it is set, then it requests to restart a connection.
  5. **SYN:** It is used to establish a connection between the hosts.
  6. **FIN:** It is used to release a connection, and no further data exchange will happen.
- **Window size**
  It is a 16-bit field. It contains the size of data that the receiver can accept. This field is used for the flow control between the sender and receiver and also determines the amount of buffer allocated by the receiver for a segment. The value of this field is determined by the receiver.
- **Checksum**
  It is a 16-bit field. This field is optional in UDP, but in the case of TCP/IP, this field is mandatory.
- **Urgent pointer**
  It is a pointer that points to the urgent data byte if the URG flag is set to 1. It defines a value that will be added to the sequence number to get the sequence number of the last urgent byte.
- **Options**
  It provides additional options. The optional field is represented in 32-bits. If this field contains the data less than 32-bit, then padding is required to obtain the remaining bits.

TCP and UDP in Transport Layer

Layer 3 or the Network layer uses IP or Internet Protocol which being a connection less protocol treats every packet individually and separately leading to lack of reliability during a transmission. For example, when data is sent from one host to another, each packet may take a different path even if it belongs to the same session. This means the packets may/may not arrive in the right order. Therefore, IP relies on the higher layer protocols to provide reliability.

TCP (Transmission Control Protocol):

TCP is a layer 4 protocol which provides acknowledgement of the received packets and is also reliable as it resends the lost packets. It is better than UDP but due to these features it has an additional overhead. It is used by application protocols like HTTP and FTP.

UDP (User Datagram Protocol):

UDP is also a layer 4 protocol but unlike TCP it doesn't provide acknowledgement of the sent packets. Therefore, it isn't reliable and depends on the higher layer protocols for the same. But on the other hand it is simple, scalable and comes with lesser overhead as compared to TCP. It is used in video and voice streaming.

TCP Vs UDP –

1. **Session Multiplexing:**
   A single host with a single IP address is able to communicate with multiple servers. While using TCP, first a connection must be established between the server and the receiver and

the connection is closed when the transfer is completed. TCP also maintains reliability while the transfer is taking place.

UDP on the other hand sends no acknowledgement of receiving the packets. Therefore, provides no reliability.

2. **Segmentation:**

Information sent is first broken into smaller chunks for transmission.

Maximum Transmission Unit or MTU of a Fast Ethernet is 1500 bytes whereas the theoretical value of TCP is 65495 bytes. Therefore, data has to be broken into smaller chunks before being sent to the lower layers. MSS or Maximum Segment Size should be set small enough to avoid fragmentation. TCP supports MSS and Path MTU discovery with which the sender and the receiver can automatically determine the maximum transmission capability.

UDP doesn't support this; therefore it depends on the higher layer protocols for data segmentation.

3. **Flow Control:**

If sender sends data faster than what receiver can process then the receiver will drop the data and then request for a retransmission, leading to wastage of time and resources. TCP provides end-to-end flow control which is realized using a sliding window. The sliding window sends an acknowledgement from receiver's end regarding the data that the receiver can receive at a time.

UDP doesn't implement flow control and depends on the higher layer protocols for the same.

4. **Connection Oriented:**

TCP is connection oriented, i.e., it creates a connection for the transmission to take place, and once the transfer is over that connection is terminated.

UDP on the other hand is connectionless just like IP (Internet Protocol).

5. **Reliability:**

TCP sends an acknowledgement when it receives a packet. It requests a retransmission in case a packet is lost.

UDP relies on the higher layer protocols for the same.

6. **Headers:**

The size of TCP header is 20-bytes (16-bits for source port, 16-bits for the destination port, 32-bits for seq number, 32-bits for ack number, 4-bits header length)

The size of the UDP header is 8-bytes (16-bits for source port, 16-bits for destination port, 16-bits for length, 16-bits for checksum); it's significantly smaller than the TCP header.

Both UDP and TCP header is comprised of 16-bit Source port(these are used for identifying the port number of the source) fields and 16-bits destination port (these are used for specifying the offered application) fields.

UNIT – V

Application Layer –Domain name system, SNMP, Electronic Mail;
the World WEB, HTTP, Streaming Audio and Video.

Application Layer

The application layer in the OSI model is the closest layer to the end user which means that the application layer and end user can interact directly with the software application. The application layer programs are based on client and servers.

The Application layer includes the following functions:

- **Identifying communication partners:** The application layer identifies the availability of communication partners for an application with data to transmit.
- **Determining resource availability:** The application layer determines whether sufficient network resources are available for the requested communication.
- **Synchronizing communication:** All the communications occur between the applications requires cooperation which is managed by an application layer.

Services of Application Layers

- **Network Virtual terminal:** An application layer allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal, which in turn, talks to the host. The remote host thinks that it is communicating with one of its own terminals, so it allows the user to log on.
- **File Transfer, Access, and Management (FTAM):** An application allows a user to access files in a remote computer, to retrieve files from a computer and to manage files in a remote computer. FTAM defines a hierarchical virtual file in terms of file structure, file attributes and the kind of operations performed on the files and their attributes.
- **Addressing:** To obtain communication between client and server, there is a need for addressing. When a client made a request to the server, the request contains the server address and its own address. The server response to the client request, the request contains the destination address, i.e., client address. To achieve this kind of addressing, DNS is used.
- **Mail Services:** An application layer provides Email forwarding and storage.
- **Directory Services:** An application contains a distributed database that provides access for global information about various objects and services.
- **Authentication:** It authenticates the sender or receiver's message or both.

Network Application Architecture

Application architecture is different from the network architecture. The network architecture is fixed and provides a set of services to applications. The application architecture, on the other hand, is designed by the application developer and defines how the application should be structured over the various end systems.

Application architecture is of two types:

- **Client-server architecture:** An application program running on the local machine sends a request to another application program is known as a client, and a program that serves a request is known as a server. For example, when a web server receives a request from the client host, it responds to the request to the client host.

Characteristics of Client-server architecture:

- In Client-server architecture, clients do not directly communicate with each other. For example, in a web application, two browsers do not directly communicate with each other.
- A server is fixed, well-known address known as IP address because the server is always on while the client can always contact the server by sending a packet to the sender's IP address.

Disadvantage of Client-server architecture:

It is a single-server based architecture which is incapable of holding all the requests from the clients. For example, a social networking site can become overwhelmed when there is only one server exists.

- **P2P (peer-to-peer) architecture:** It has no dedicated server in a data center. The peers are the computers which are not owned by the service provider. Most of the peers reside in the homes, offices, schools, and universities. The peers communicate with each other without passing the information through a dedicated server; this architecture is known as peer-to-peer architecture. The applications based on P2P architecture includes file sharing and internet telephony.

Features of P2P architecture

- **Self scalability:** In a file sharing system, although each peer generates a workload by requesting the files, each peer also adds a service capacity by distributing the files to the peer.
- **Cost-effective:** It is cost-effective as it does not require significant server infrastructure and server bandwidth.

Client and Server processes

- A network application consists of a pair of processes that send the messages to each other over a network.
- In P2P file-sharing system, a file is transferred from a process in one peer to a process in another peer. We label one of the two processes as the client and another process as the server.
- With P2P file sharing, the peer which is downloading the file is known as a client, and the peer which is uploading the file is known as a server. However, we have observed in some applications such as P2P file sharing; a process can be both as a client and server. Therefore, we can say that a process can both download and upload the files.

Domain Name System (DNS) in Application Layer

DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

Requirement

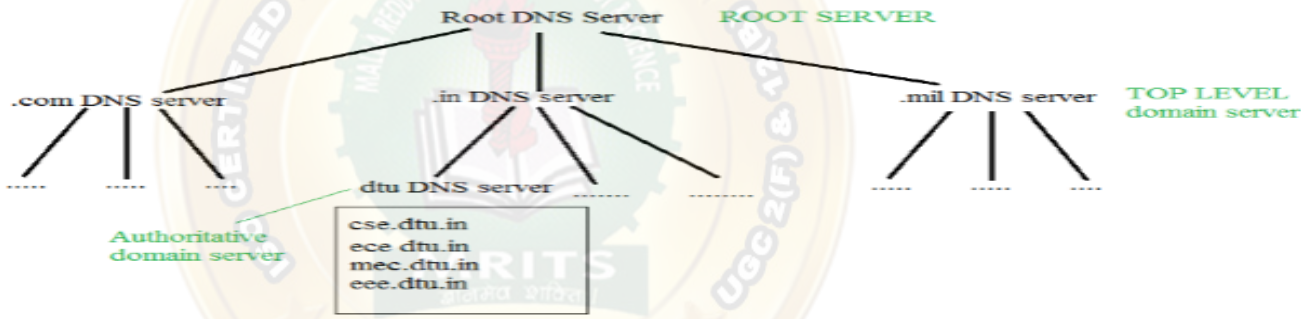
Every host is identified by the IP address but remembering numbers is very difficult for the people and also the IP addresses are not static therefore a mapping is required to change the domain name to IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

Domain:

There are various kinds of DOMAIN :

1. **Generic domain:** .com (commercial) .edu (educational) .mil(military) .org (non-profit organization) .net(similar to commercial) all these are generic domain.
2. **Country domain**: .in (India) .us .uk
3. Inverse domain if we want to know what is the domain name of the website. Ip to domain name mapping. So DNS can provide both the mapping for example to find the ip addresses of geeksforgeeks.org then we have to type nslookup www.geeksforgeeks.org.

Organization of Domain



It is Very difficult to find out the ip address associated to a website because there are millions of websites and with all those websites we should be able to generate the ip address immediately,

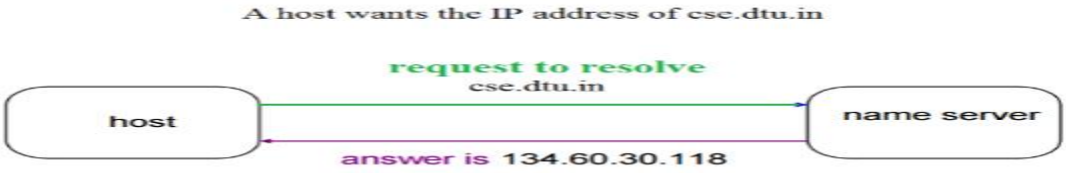
there should not be a lot of delay for that to happen organization of database is very important.

DNS record – Domain name, ip address what is the validity?? what is the time to live ?? and all the information related to that domain name. These records are stored in tree like structure.

Namespace – Set of possible names, flat or hierarchical . Naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value –

Name server – It is an implementation of the resolution mechanism.. DNS (Domain Name System) = Name service in Internet – Zone is an administrative unit, domain is a sub-tree.

Name to Address Resolution



The host request the DNS name server to resolve the domain name. And the name server

returns the IP address corresponding to that domain name to the host so that the host can future connect to that IP address.

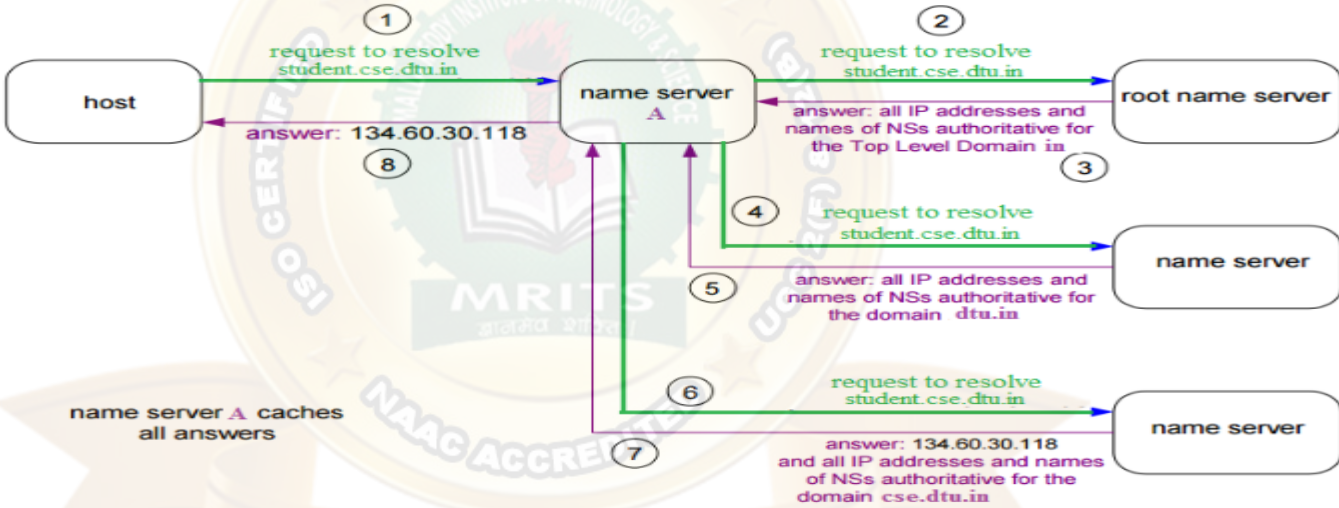
Hierarchy of Name Servers

Root name servers – It is contacted by name servers that can not resolve the name. It contacts authoritative name server if name mapping is not known. It then gets the mapping and return the IP address to the host.

Top level server – It is responsible for com, org, edu etc and all top level country domains like uk, fr, ca, in etc. They have info about authoritative domain servers and know names and IP addresses of each authoritative name server for the second level domains.

Authoritative name servers This is organization's DNS server, providing authoritative host Name to IP mapping for organization servers. It can be maintained by organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top level domain server and then to authoritative domain name server which actually contains the IP address. So the authoritative domain server will return the associative ip address.

Domain Name Server



The client machine sends a request to the local name server, which , if root does not find the address in its database, sends a request to the root name server , which in turn, will route the query to an intermediate or authoritative name server. The root name server can also contain some host Name to IP address mappings. The intermediate name server always knows who the authoritative name server is. So finally the IP address is returned to the local name server which in turn returns the IP address to the host.

Simple Network Management Protocol (SNMP)

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

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

SNMP components – There are 3 components of SNMP:

1. **SNMP Manager** – It is a centralized system used to monitor network. It is also known as Network Management Station (NMS)

2. **SNMP agent** – It is a software management software module installed on a managed device. Managed devices can be network devices like PC, routers, switches, servers, etc.

3. **Management Information Base** – MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables.

SNMP messages – Different variables are:

1. **Get_Request** – SNMP manager sends this message to request data from the SNMP agent. It is simply used to retrieve data from SNMP agents. In response to this, the SNMP agent responds with the requested value through a response message.

2. **Get_Next_Request** – This message can be sent to discover what data is available on an SNMP agent. The SNMP manager can request data continuously until no more data is left. In this way, the SNMP manager can take knowledge of all the available data on SNMP agents.

3. **Get_Bulk_Request** – This message is used to retrieve large data at once by the SNMP manager from the SNMP agent. It is introduced in SNMPv2c.

4. **Set_Request** – It is used by the SNMP manager to set the value of an object instance on the SNMP agent.

5. **Response** – It is a message sent from the agent upon a request from the manager. When sent in response to Get messages, it will contain the data requested. When sent in response to the Set message, it will contain the newly set value as confirmation that the value has been set.

6. **Trap** – These are the message sent by the agent without being requested by the manager. It is sent when a fault has occurred.

7. **Inform_Request** – It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to set trap continuously until it receives an Inform message. It is the same as a trap but adds an acknowledgement that the trap doesn't provide.

SNMP security levels – It defines the type of security algorithm performed on SNMP packets. These are used in only

SNMPv3. There are 3 security levels namely:

1. **No_Auth_No_Priv** – This (no authentication, no privacy) security level uses a community string for authentication and no encryption for privacy.

2. **Auth_No_priv –** This security level (authentication, no privacy) uses HMAC with Md5 for authentication and no encryption is used for privacy.

3. **Auth_Priv –** This security level (authentication, privacy) uses HMAC with Md5 or SHA for authentication and encryption uses the DES-56 algorithm.

SNMP versions –
There are 3 versions of SNMP:

1. **SNMPv1** – It uses community strings for authentication and uses UDP only.

2. **SNMPv2c** – It uses community strings for authentication. It uses UDP but can be configured to use TCP.

3. **SNMPv3** – It uses Hash-based MAC with MD5 or SHA for authentication and DES-56 for privacy. This version uses TCP. Therefore, the conclusion is the higher the version of SNMP, the more secure it will be.

E-mail Protocols

E-mail Protocols are set of rules that help the client to properly transmit the information to or from the mail server. Here in this tutorial, we will discuss various protocols such as **SMTP, POP,** and **IMAP.**

SMPTP

SMTP stands for **Simple Mail Transfer Protocol**. It was first proposed in 1982. It is a standard protocol used for sending e-mail efficiently and reliably over the internet.

Key Points:

- SMTP is application level protocol.
- SMTP is connection oriented protocol.
- SMTP is text based protocol.
- It handles exchange of messages between e-mail servers over TCP/IP network.
- Apart from transferring e-mail, SMPT also provides notification regarding incoming mail.
- When you send e-mail, your e-mail client sends it to your e-mail server which further contacts the recipient mail server using SMTP client.
- These SMTP commands specify the sender's and receiver's e-mail address, along with the message to be send.

- The exchange of commands between servers is carried out without intervention of any user.
- In case, message cannot be delivered, an error report is sent to the sender which makes SMTP a reliable protocol.

SMTP Commands

The following table describes some of the SMTP commands:

S.N.	Command Description
1	**HELLO:** This command initiates the SMTP conversation.
2	**EHELLO:** This is an alternative command to initiate the conversation. ESMTP indicates that the sender server wants to use extended SMTP protocol.
3	**MAIL FROM:** This indicates the sender's address.
4	**RCPT TO:** It identifies the recipient of the mail. In order to deliver similar message to multiple users this command can be repeated multiple times.
5	**SIZE:** This command let the server know the size of attached message in bytes.
6	**DATA:** The **DATA** command signifies that a stream of data will follow. Here stream of data refers to the body of the message.
7	**QUIT:** This commands is used to terminate the SMTP connection.
8	**VERFY:** This command is used by the receiving server in order to verify whether the given username is valid or not.
9	**EXPN:** It is same as VRFY, except it will list all the users name when it used with a distribution list.

IMAP

IMAP stands for **Internet Message Access Protocol.** It was first proposed in 1986. There exist five versions of IMAP as follows:

1. Original IMAP
2. IMAP2
3. IMAP3
4. IMAP2bis
5. IMAP4

Key Points:

- IMAP allows the client program to manipulate the e-mail message on the server without downloading them on the local computer.
- The e-mail is hold and maintained by the remote server.
- It enables us to take any action such as downloading, delete the mail without reading the mail. It enables us to create, manipulate and delete remote message folders called mail boxes.
- IMAP enables the users to search the e-mails.

- It allows concurrent access to multiple mailboxes on multiple mail servers.

IMAP Commands

The following table describes some of the IMAP commands:

S.N.	Command Description
1	**IMAP_LOGIN:** This command opens the connection.
2	**CAPABILITY:** This command requests for listing the capabilities that the server supports.
3	**NOOP:** This command is used as a periodic poll for new messages or message status updates during a period of inactivity.
4	**SELECT:** This command helps to select a mailbox to access the messages.
5	**EXAMINE:** It is same as SELECT command except no change to the mailbox is permitted.
6	**CREATE:** It is used to create mailbox with a specified name.
7	**DELETE:** It is used to permanently delete a mailbox with a given name.
8	**RENAME:** It is used to change the name of a mailbox.
9	**LOGOUT:** This command informs the server that client is done with the session. The server must send BYE untagged response before the OK response and then close the network connection.

POP

POP stands for Post Office Protocol. It is generally used to support a single client. There are several versions of POP but the POP 3 is the current standard.

Key Points

- POP is an application layer internet standard protocol.
- Since POP supports offline access to the messages, thus requires less internet usage time.
- POP does not allow search facility.
- In order to access the messaged, it is necessary to download them.
- It allows only one mailbox to be created on server.
- It is not suitable for accessing non mail data.
- POP commands are generally abbreviated into codes of three or four letters. Eg. STAT.

POP Commands

The following table describes some of the POP commands:

S.N.	Command Description
1	**LOGIN:** This command opens the connection.
2	**STAT:** It is used to display number of messages currently in the mailbox.
3	**LIST:** It is used to get the summary of messages where each message summary is shown.

4	**RETR:** This command helps to select a mailbox to access the messages.
5	**DELE:** It is used to delete a message.
6	**RSET:** It is used to reset the session to its initial state.
7	**QUIT:** It is used to log off the session.

Comparison between POP and IMAP

S.N.	POP	IMAP
1	Generally used to support single client.	Designed to handle multiple clients.
2	Messages are accessed offline.	Messages are accessed online although it also supports offline mode.
3	POP does not allow search facility.	It offers ability to search emails.
4	All the messages have to be downloaded.	It allows selective transfer of messages to the client.
5	Only one mailbox can be created on the server.	Multiple mailboxes can be created on the server.
6	Not suitable for accessing non-mail data.	Suitable for accessing non-mail data i.e. attachment.
7	POP commands are generally abbreviated into codes of three or four letters. Eg. STAT.	IMAP commands are not abbreviated, they are full. Eg. STATUS.
8	It requires minimum use of server resources.	Clients are totally dependent on server.
9	Mails once downloaded cannot be accessed from some other location.	Allows mails to be accessed from multiple locations.
10	The e-mails are not downloaded automatically.	Users can view the headings and sender of e-mails and then decide to download.
10	POP requires less internet usage time.	IMAP requires more internet usage time.

E-mail System

E-mail system comprises of the following three components:

- Mailer
- Mail Server
- Mailbox

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

Mail Server: **The function of mail server is to receive, store and deliver the email. It is must for mail servers to be running all the time because if it crashes or is down, email can be lost.**
Mailboxes: **Mailbox is generally a folder that contains emails and information about them.**

Working of E-mail

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

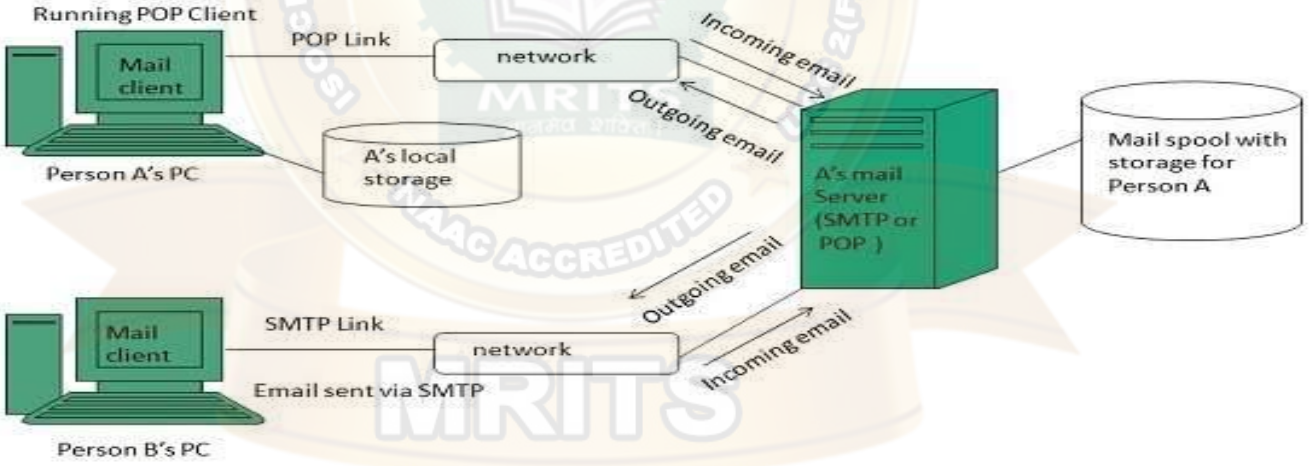
Following example will take you through the basic steps involved in sending and receiving emails and will give you a better understanding of working of email system:

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

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

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

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

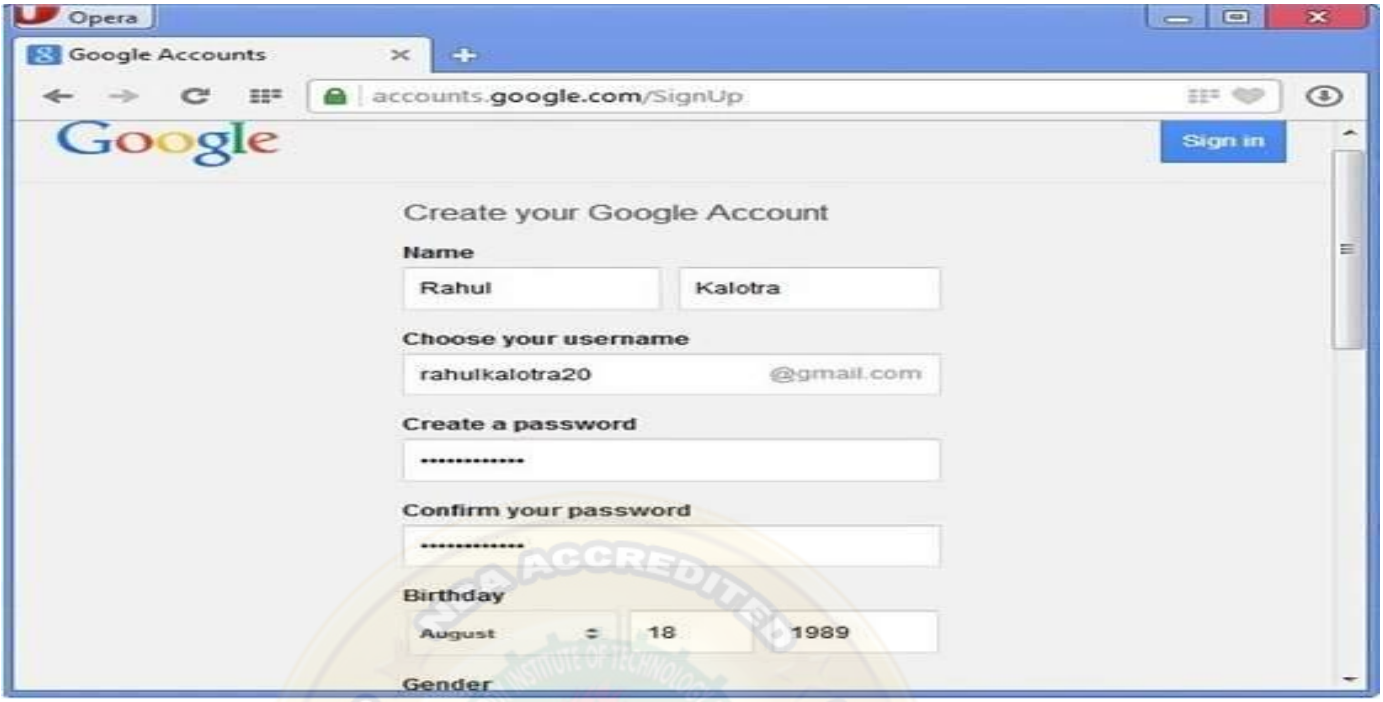


Here we will discuss the operations that can be performed on an e-mail. But first of all we will learn how to create an email account.

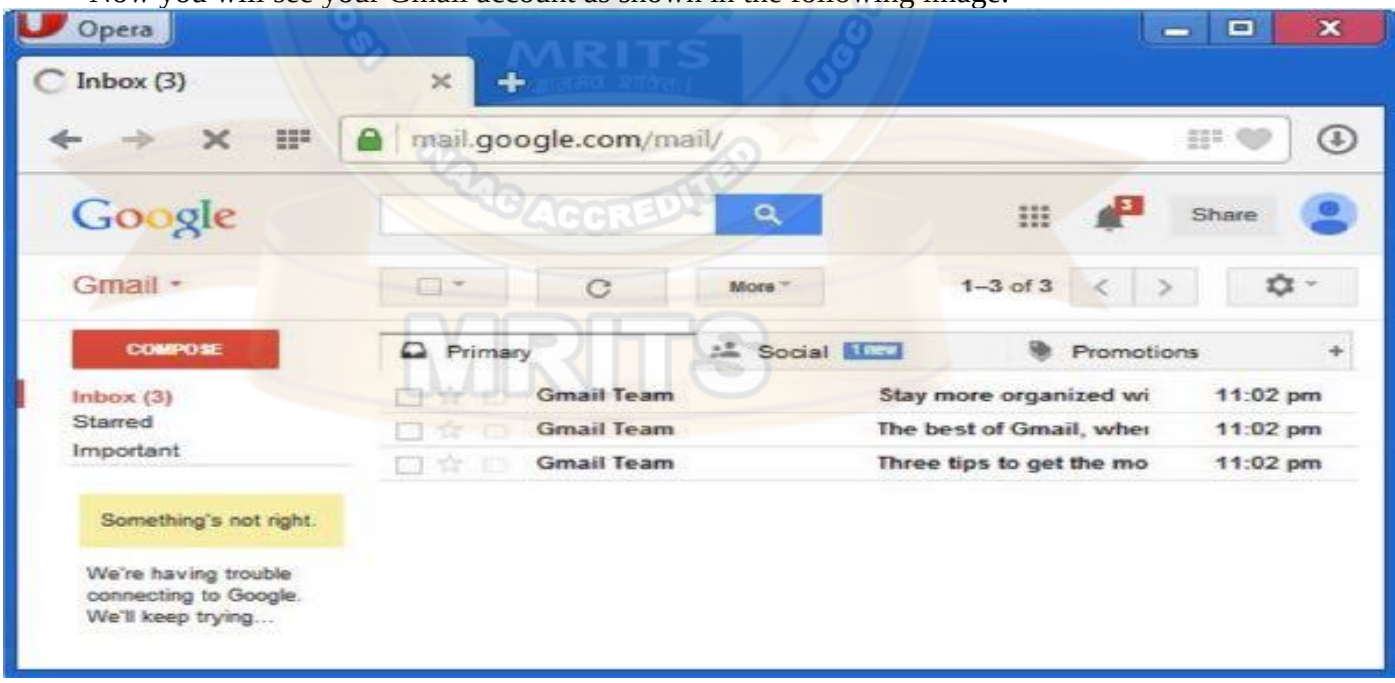
Creating Email Account

There are various email service provider available such as **Gmail, hotmail, ymail, rediff mail** etc. Here we will learn how to create an account using Gmail.

- Open gmail.com and click **create an account.**
- Now a form will appear. Fill your details here and click **Next Step.**



- This step allows you to add your picture. If you don't want to upload now, you can do it later. Click **Next Step.**
- Now a welcome window appears. Click **Continue to Gmail.**
- Wow!! You are done with creating your email account with Gmail. It's that easy. Isn't it?
- Now you will see your Gmail account as shown in the following image:



Key Points:

- Gmail manages the mail into three categories namely **Primary, Social** and **Promotions.**
- **Compose** option is given at the right to compose an email message.
- **Inbox, Starred, Sent mail, Drafts** options are available on the left pane which allows you to keep track of your emails.

Composing and Sending Email

Before sending an email, we need to compose a message. When we are composing an email message, we specify the following things:

- Sender's address in To field
- Cc (if required)
- Bcc (if required)
- Subject of email message
- Text
- Signature

You should specify the correct email address; otherwise it will send an error back to the sender.

Once you have specified all the above parameters, It's time to send the email. The mailer program provides a Send button to send email, when you click Send, it is sent to the mail server and a message **mail sent successfully** is shown at the above.

Reading Email

Every email program offers you an interface to access email messages. Like in Gmail, emails are stored under different tabs such as primary, social, and promotion. When you click one of tab, it displays a list of emails under that tab.

In order to read an email, you just have to click on that email. Once you click a particular email, it gets opened.

The opened email may have some file attached with it. The attachments are shown at the bottom of the opened email with an option called **download attachment.**

Replying Email

After reading an email, you may have to reply that email. To reply an email, click **Reply** option shown at the bottom of the opened email.

Once you click on Reply, it will automatically copy the sender's address in to the To field. Below the To field, there is a text box where you can type the message.

Once you are done with entering message, click Send button. It's that easy. Your email is sent.

Forwarding Email

It is also possible to send a copy of the message that you have received along with your own comments if you want. This can be done using **forward** button available in mail client software.

The difference between replying and forwarding an email is that when you reply a message to a person who has send the mail but while forwarding you can send it to anyone.

When you receive a forwarded message, the message is marked with a > character in front of each line and **Subject:** field is prefixed with **Fw.**

Deleting Email

If you don't want to keep email into your inbox, you can delete it by simply selecting the message from the message list and clicking **delete** or pressing the appropriate command.

Some mail clients offers the deleted mails to be stored in a folder called deleted items or trash from where you can recover a deleted email.

Now a day, the mail client comes with enhanced features such as attachment, address book, and MIME support. Here in this chapter we will discuss all of these features which will give you a better understanding of added feature of a mail client program.

Attachment

Ability to attach file(s) along with the message is one of the most useful features of email. The attachment may be a **word document, PowerPoint presentation, audio/video files,** or **images.**

- In order to attach file(s) to an email, click the attach button. As a result, a dialog box appears asking for specifying the name and location of the file you want to attach.
- Once you have selected the appropriate file, it is attached to the mail.
- Usually a paper clip icon appears in the email which indicates that it has an attachment.
- When adding an attachment it is better to compress the attached files so as to reduce the file size and save transmission time as sending and downloading large files consumes a lot of space and time.

Address Book

Address book feature of a mail program allows the users to store information about the people whom they communicate regularly by sending emails. Here are some of the key features of an Address book:

- Address book includes the nick names, email addresses, phone number etc. of the people.
- Using address book allows us not to memorize email of address of a person, you just have to select recipient name from the list.
- When you select a particular name from the list, the corresponding email address link automatically get inserted in to the **To:** field.
- Address book also allows creating a group so that you can send a email to very member of the group at once instead of giving each person email address one by one.

MIME Types

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

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

The following table describes commonly used MIME Types:

1.	Type	Subtype	Description	File extension(s)
2.	Application	postscript tex troff	Printable postscript document TEX document Printable troff document	.eps, .ps .tex .t, .tr, .roff
3.	Audio	aiff au	Apple sound Sun Microsystems sound	.aif, .aiff,.aifc .au, .snd

		midi real audio	Musical Instrument Digital Interface Progressive Network sound	.midi, .mid .ra, .ram
4.	image	gif jpeg png triff	Graphics Interchange Format Joint Photographic Experts Group Portable Network Graphics Tagged Image Modeling Language	.gif .jpeg, .jpg, .jpe .png .tiff, .tif
5.	Model	vrml	Virual reality Modelling Language	.wrl
6.	Text plain sgml	html	Hyper Text Markup Language Unformatted text Standard Generalized Markup language	.html, .htm .txt .sgml
7.	Video	avi mpeg quicktime sgi-movie	Microsoft Audio Video Interleaved Moving Pictures Expert Group Apple QuickTime movie silicon graphic movie	.avi .mpeg, .mpg .qt, .mov .movie

security

E-mail Hacking

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

- Spam
- Virus
- Phishing

Spam

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

Virus

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

Phishing

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

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

E-mail Spamming and Junk Mails

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

Spams may cause the following problems:

- It floods your e-mail account with unwanted e-mails, which may result in loss of important e-mails if inbox is full.
- Time and energy is wasted in reviewing and deleting junk emails or spams.

- It consumes the bandwidth that slows the speed with which mails are delivered.
- Some unsolicited email may contain virus that can cause harm to your computer.

Blocking Spams

Following ways will help you to reduce spams:

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

E-mail Cleanup and Archiving

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

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

The World WEB

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

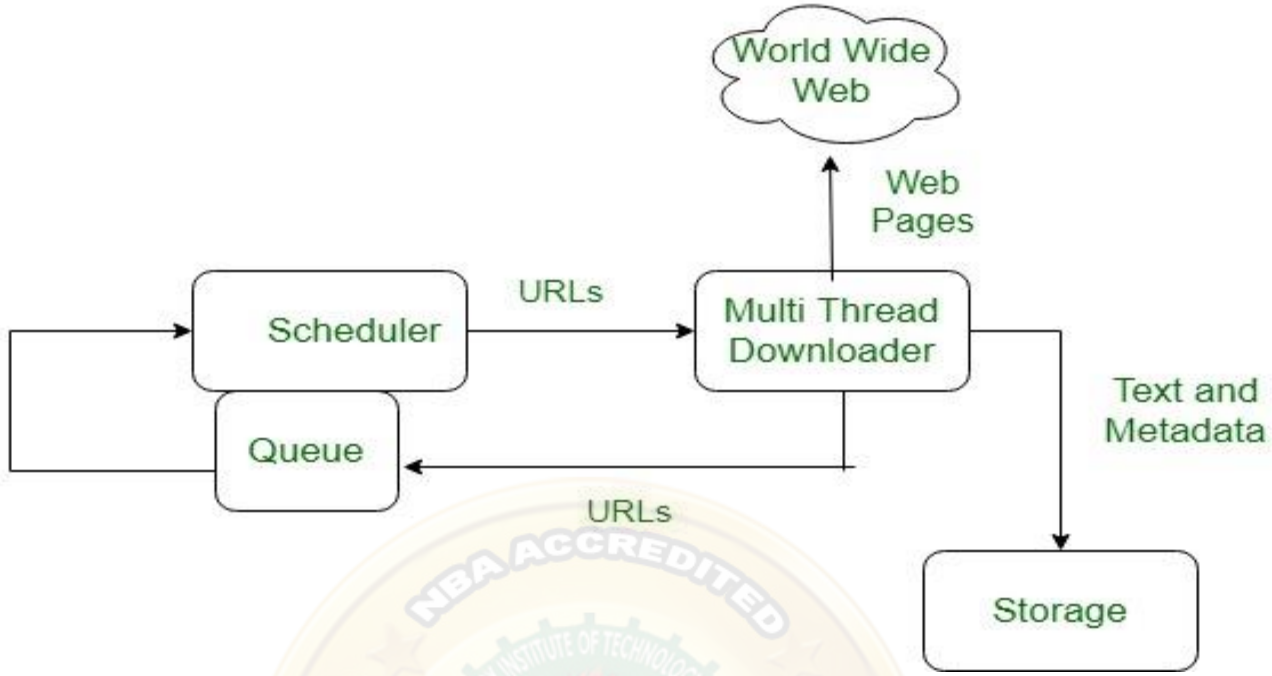
History:

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

System Architecture:

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

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



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

Working of WWW:

The World Wide Web is based on several different technologies: Web browsers, Hypertext Markup Language (HTML) and Hypertext Transfer Protocol (HTTP).

A Web browser is used to access webpages. Web browsers can be defined as programs which display text, data, pictures, animation and video on the Internet. Hyperlinked resources on the World Wide Web can be accessed using software interface provided by Web browsers. Initially Web browsers were used only for surfing the Web but now they have become more universal. Web browsers can be used for several tasks including conducting searches, mailing, transferring files, and much more. Some of the commonly used browsers are Internet Explorer, Opera Mini, Google Chrome.

Features of WWW:

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

Components of Web: There are 3 components of web:

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

HTTP

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

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

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

How it works ?

First of all, whenever we want to open any website then first we open web browser after that we will type URL of that website (e.g., www.facebook.com). This URL is now sent to Domain Name Server (DNS). Then DNS first check records for this URL in their database, then DNS will return IP address to web browser corresponding to this URL. Now browser is able to sent request to actual server.

After server sends data to client, connection will be closed. If we want something else from server we should have to re-establish connection between client and server.

History ::

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

HTTP version 0.9 – This was first version of HTTP which was introduced in 1991.

HTTP version 1.0 – In 1996, RFC 1945 (Request For Comments) was introduced in HTTP version 1.0.

HTTP version 1.1 – In January 1997, RFC 2068 was introduced in HTTP version 1.1. Improvements and updates to HTTP version 1.1 standards were released under RFC 2616 in June 1999.

HTTP version 2.0 – The HTTP version 2.0 specifications was published as RFC 7540 on May 14, 2015.

HTTP version 3.0 – HTTP version 3.0 is based on previous RFC draft. It is renamed as HyperText Transfer Protocol QUIC which is a transport layer network protocol developed by Google.

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

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

Advantages:

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

Disadvantages:

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

Streaming Audio and Video

When the internet first caught on with consumers in the mid-to-late 1990s, people had to buy a modem, hook it up to their computer and a phone line and dial the phone number for their local internet service provider (ISP). Connections were miserably slow.

The web was not designed to stream audio or video when it was first created in the 1960s, but enterprising developers found a way to help customers listen to real-live audio and the first live audio streaming event was broadcast on Sept. 5, 1995, for a game between the Seattle Mariners and New York Yankees. It was novel at first, and there wasn't a lot of long-form content. Between maddeningly slow connections and glitchy software no one was going to sit down to watch a movie on their home computer.

In just a few short years, technologies improved to make streaming video and audio more of an everyday occurrence. Companies like Netflix and Hulu delivered live movies and television. Content creators such as Paramount and Disney started their own video streaming networks, and tech giants like Apple and Amazon joined in. You can watch old classic TV shows or the latest movies on demand.

Streaming audio has matured as well. You can listen to live sports around the world, or turn your computer or smartphone into a custom radio channel with music providers like Deezer, Pandora, and Spotify. People commute to work or the grocery store listening to true-crime podcasts or the latest audiobooks.

In the last decade, audio and video streaming became popular enough to encourage cable and satellite TV providers to "cut the cord" and canceled their cable or satellite TV subscriptions for cheaper streaming options. In June 2021, media research company Nielsen revealed that streaming video has become more popular than over-the-air TV in the United States. Streamers' share of the market was 26 percent to over-the-air TV's 25 percent. That may not seem like much, especially when cable TV still had 39 percent of the market, but streaming media is likely to continue to grow, and cable subscriptions likely to decline.

You may have participated in a live streaming broadcast yourself. During the COVID-19 pandemic many people tuned in for remote meetings or online classes. Tools like Zoom, Microsoft Teams or Google Meet can handle live audio and video streaming simultaneously in one broadcast. It's a little like when the telephone companies promised us videophones in the mid-20th century, only better.

Contents

Finding and Playing Streaming Video and Audio

A sample of the channels you can access through Roku. TIFFANY HAGLER-GEARD/BLOOMBERG VIA GETTY IMAGES

If you're brand-new to streaming, you'll need a high-speed internet connection. You'll also need a device to enjoy the video or audio content on — that could be a smartphone, a computer, a tablet or a TV. Computers may be the easiest to set up for streaming. You can access the websites for many streaming video and audio providers and enjoy the media right in your browser window. You may also find a dedicated desktop application for a streaming service.

Although smartphones and tablets have web browsers, you're far more likely to use an app developed specifically for that particular service. If you wanted to watch or listen to a live game in progress, you might open the ESPN app. To hear the news, you might listen to TuneIn Radio, which offers live and recorded broadcasts from all over the world. Many services require paid subscriptions, but many others are ad-supported or completely free. For streaming audio, most people rely either on go to the website of the program in question or to a podcast platform which has a host of programs, like Apple Podcasts, Google Podcasts, Spotify or Stitcher. These can be found on your smartphone.

TVs require hardware to make live streaming connections. Often this is a device you plug into a port on the television such as Roku, Amazon FireStick or Google Chromecast — these are the devices that allow your TV to access the apps for streaming live content. If you have a smart TV, this hardware is already built in. Just turn on your TV, go to the "Apps" section and you'll see an operating system designed to run streaming apps for Netflix, Amazon Prime Video, PlutoTV, YouTube and many more. The most popular apps are usually pre-installed but your device or TV will let you download new apps as well. (If you still subscribe to a cable service, the newer cable boxes allow you to stream videos and apps through them, too.)

Once you've selected the app you want, you'll see an array of programs, along with descriptions and ratings. You just click on the show you want to get started. If it is a paid app (like Netflix,

Hulu or Amazon) you'll have to create an account or sign in if you already created an account and paid for the service online. The good news is once you've signed in, the streaming app will save that information so you don't have to do it again.

Most apps have an interface that lets you choose your favorite shows and browse others. With on-demand streaming you can watch one at a time, or "binge-watch" several in a row. You can pause the show to get something from the kitchen, usually even for live events like sports. Streaming media's flexibility is one of the key reasons it has become so popular.

Encoding Streaming Media

Demi Lovato performs during the Celebrating America Primetime Special on Jan. 20, 2021. The livestreamed event hosted by Tom Hanks featured remarks by president-elect Joe Biden and vice president-elect Kamala Harris and performances representing diverse American talent. HANDOUT/BIDEN INAUGURAL COMMITTEE VIA GETTY IMAGES

Streaming providers must determine the best way to get their content to your device in a way that's easy for you to use.

High-quality images, audio and video files often start out very large. Although still imagines aren't streaming, as an easy-to-imagine example let's say your smartphone has a 12-megapixel camera. A still photo you take with that camera has a print size of 9.7 by 14.5 inches (17.8 by 36.8 centimeters). That's larger than you need for a quick social media snapshot, but the larger file size means you can use the photo for other things, in this case perhaps a poster. Our phones create bigger sound, video and image files because it's generally a better idea to create a large file and shrink it down. It's harder to enlarge a smaller media file with a high-quality result.

Streaming providers use file formats that maximize quality over typical internet speeds. Compressing them is done using **codecs**, instructions for coding and decoding visual and audio information in a standard file format. Lossless formats capture more of the original file's fidelity

but have larger file sizes. Many formats, however, are lossy — they remove some of the information in the file but attempt to keep as much of the original as possible.

To compress audio and video files, a lossy-format codec may identify parts of the video that it can copy and apply later in the show. It deletes the redundant information to keep the file size down. Codecs may also reduce the number of colors in the video, lower the resolution of the video or reduce its frame rate. Lossy audio codecs may remove frequencies from the original recording that most people can't hear, around 20 Hz to 20,000 Hz.

While that may help save on streaming bandwidth, it can cause problems, too. You may have experienced some side effects of file compression while you watch a show if images seem washed out or pixilated. If you're running with your earbuds in, you may not hear a heavily compressed music file, but with nice headphones, you just might.

Streaming Infrastructure

Streaming providers want to make sure their service is as fast and reliable as possible, which means developing specialized systems to handle the traffic.

In 2016 researchers at Queen Mary University of London published a report on the content delivery network (CDN) used by Netflix. At the time, the streaming video company had just become a global service with 4,669 servers in 243 locations around the world. It had been developing its own CDN since 2011 to get the service ready for global traffic. Netflix Open Connect, as it's called, requires the assistance of internet service providers (ISPs) all over the world.

Netflix encourages these ISPs to join the system by giving them its proprietary streaming devices, called Open Connect Appliances (OCAs), for free. Their ISP partners embed the equipment in their networks. Netflix then uses the devices to connect customers to the closest service point in the network. It speeds up the service and prevents the network architecture from being stretched too thin.

Streaming a live conference call works a little differently. Each participant is streaming live audio and video to and from their device at the same time as each other participant. Providers prioritize connection over video quality and offer telephone-based options for those who need to attend but can't use the internet.

Business computer network security presents another hurdle. Part of Zoom's streaming software, called the Intelligent Transport Layer, determines the best communication protocol to connect multiple callers over different networks. Zoom uses a distributed network and its own proprietary codec to encode and share information during its calls. The company says it keeps 50 percent excess capacity available to accommodate increasing traffic.

Video and Audio Streaming Customers

This detail of a TV remote control shows various streaming platform buttons on Dec. 16, 2020 in Krakow, Poland. BEATA ZAWRZEL/NURPHOTO VIA GETTY IMAGES

What happens to the streaming video and audio at your end? On smartphones and tablets, we're often using a proprietary application designed by the streamer that takes care of the business for us. If you tune in to a Disney+ stream on your phone, you don't have to worry about whether you'll be able to watch it.

In a web browser, however, streaming works a little differently. Your computer and internet connection affect how well the media stream works on your machine. With the release of HTML 5 — the language webpages are written in — streaming providers can embed audio and video files in their webpages without forcing you to rely on browser plugins.

Smart TVs and devices that plug in to TVs, such as a Roku or Apple TV, have their own operating systems and dedicated apps for streaming services. It's a lot like the experience on a smartphone or tablet. Your experience may vary on the deals streamers and hardware manufacturers work out — or don't — among themselves. In 2021 Roku removed YouTube TV from its channel store in a contract dispute.

Some content providers use their corporate structure to offer deals to potential subscribers of multiple services. At the time of writing in June 2021, AT&T offers the HBO Max streaming service free to anyone subscribing to its highest-end video, internet or wireless plans. HBO Max is part of WarnerMedia, owned by AT&T. Similarly, Comcast's Xfinity service customers get Peacock Premium for no extra charge (Comcast owns NBCUniversal and its library of content). The device you own and the internet service you subscribe to may affect which content you can access, for good or bad.