# CN MID 2

## 1. BLUETOOTH

**Bluetooth** is defined as the wireless standard for interconnecting, computing &, communicating devices and accessories using short range, low power and, inexpensive wireless radios.

It is mainly used as an alternative to wire connections, to exchange files between nearby portable devices and connect cell phones and music players with wireless headphones. In the most widely used mode, transmission power is limited to 2.5 mill watts, giving it a very short range of up to 10 metres (33 ft).

The project was named **BLUETOOTH** after Harald Blåtand.

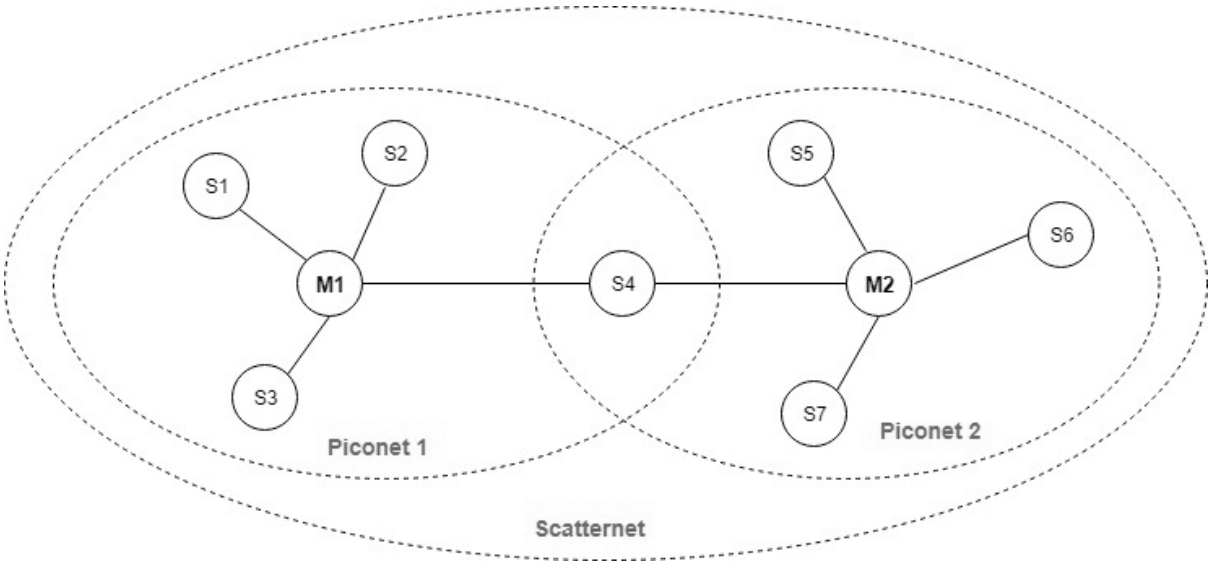
**Pairing:** The Bluetooth protocol lets devices find and connect with each other for transferring the data over short ranges, known as pairing

**Architecture of Bluetooth:**

The architecture of Bluetooth defines two types of networks:

1. Piconet

2. Scatternet



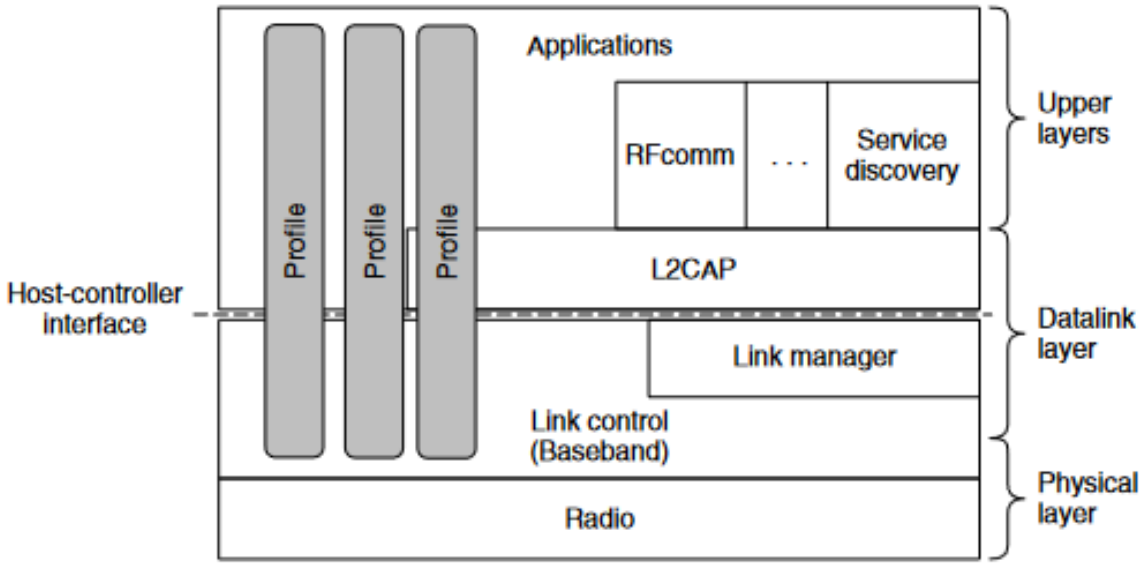

**Piconet:**

Piconet is a type of Bluetooth network that contains one primary node called the master node and seven active secondary nodes called slave nodes. Thus, we can say that there is a total of 8 active nodes which are present at a distance of 10 meters. The communication between the primary and secondary nodes can be one-to-one or one-to-many.

**Scatternet:**

It is formed by using various piconets. A slave that is present in one piconet can act as master or we can say primary in another piconet. This kind of node can receive a message from a master in one piconet and deliver the message

**Protocol Stack:**




Bluetooth architecture doesn't use OSI reference model but uses TCP/IP or other models instead.

•The bottom layer is **physical radio layer** which deals with radio transmissions and modulation

•The link control layer or the base band layer includes elements of physical layer and deals with time slots and frames

•The line management protocol handles the establishment of logical channels between devices including panel management, pairing, decryption and, quality of services.

**L2CAP**: The link protocol above the line is L2CAP (Logical Link Control Adapta- tion Protocol). It frames variable-length messages and provides reliability if needed. Many protocols use L2CAP, such as the two utility protocols that are shown.

**RF comm layer:** It is short for Radio Frontend Component. It provides a serial interface with WAP and OBEX. It also provides emulation of serial ports over the logical link control and adaption protocol(L2CAP). The protocol is based on the ETSI standard TS 07.10.

**SDP layer:** It is short for Service Discovery Protocol. It allows discovering the services available on another Bluetooth-enabled device.

## 2. IEE 802.11

IEEE 802.11 standard, popularly known as WiFi, lays down the architecture and specifications of wireless LANs (WLANs). WiFi or WLAN uses high-frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage.

The components of an IEEE 802.11 architecture are as follows −

802.11 networks can be used in two modes :

•Infrastructure Mode

•Ad hoc mode

**Infrastructure mode:** In infrastructure mode, each client is associated with an AP (Access Point) that is in turn connected to the other network. The client sends and receives its packets via the AP. Several access points may be connected together, typically by a wired network called a distribution system, to form an extended 802.11 network

**Ad hoc mode**: his mode is a collection of computers that are associated so that they can directly send frames to each other. There is no access point. Since Internet access is the killer application for wireless, ad hoc networks are not very popular

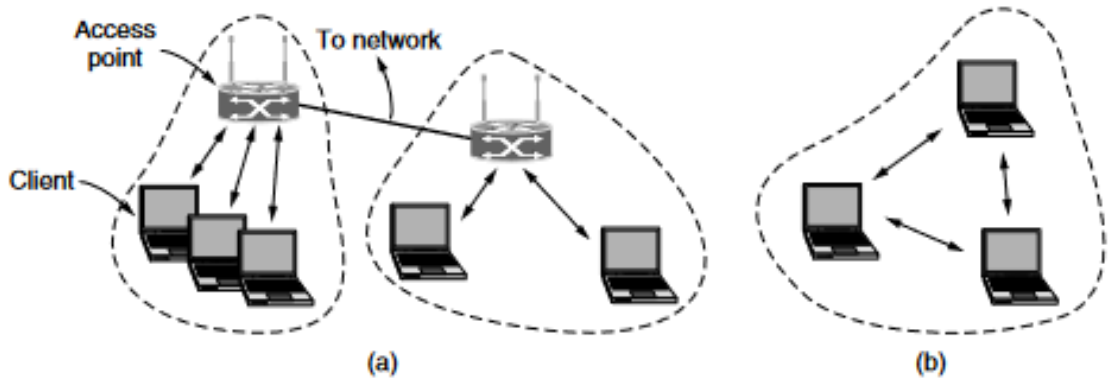
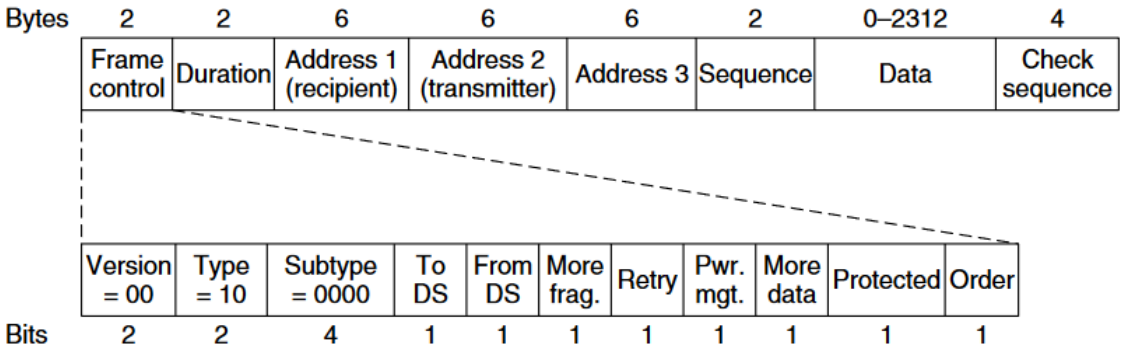



**Figure 4-23.** 802.11 architecture. (a) Infrastructure mode. (b) Ad-hoc mode.

**Frame Format of 802.11:**




- **Frame Control** −It is a 2 bytes starting field composed of 11 subfields. It contains control information of the frame. The 11 subfields are −
- **Protocol version** − The first sub-field is a two – bit field set to 00. It has been included to allow future versions of IEE 802.11 to operate simultaneously.
- **Type** − It is a two-bit subfield that specifies whether the frame is a data frame, control frame or a management frame.
- **Subtype** − it is a four – bit subfield states whether the field is a Request to Send (RTS) or a Clear to Send (CTS) control frame. For a regular data frame, the value is set to 0000.
- **To DS** − A single bit subfield indicating whether the frame is going to the access point (AC), which coordinates the communications in centralised wireless systems.
- **From DS** − A single bit subfield indicating whether the frame is coming from the AC.
- **More Fragments** − A single bit subfield which when set to 1 indicates that more fragments would follow.
- **Retry** − A single bit subfield which when set to 1 specifies a retransmission of a previous frame.
- **Power Management** − A single bit subfield indicating that the sender is adopting power-save mode.
- **More Data** − A single bit subfield showing that sender has further data frames for the receiver.
- **Protected Frame** − A single bit subfield indicating that this is an encrypted frame.
- **Order** − The last subfield, of one – bit, informs the receiver that to the higher layers the frames should be in an ordered sequence.
- **Duration** − It is a 2-byte field that specifies the time period for which the frame and its acknowledgement occupy the channel.

- Address fields: There are three 6-byte address fields containing addresses of source, immediate destination and final endpoint respectively.
- **Sequence** − It a 2 bytes field that stores the frame numbers. It detects duplicate frames and determines the order of frames for higher layers. Among the 16 bits, the first 4 bits provides identification to the fragment and the rest 12 bits contain the sequence number that increments with each transmission.
- **Data** − This is a variable sized field that carries the payload from the upper layers. The maximum size of data field is 2312 bytes.
- **Frame Check Sequence (FCS)** − It is a 4-byte field containing error detection information.

## 3. CONGESTION CONTROL ALGORITHM

**Congestion**:

A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

**Effects** of Congestion

- As delay increases, performance decreases.
- If delay increases, retransmission occurs, making situation worse.

**Congestion control algorithms**

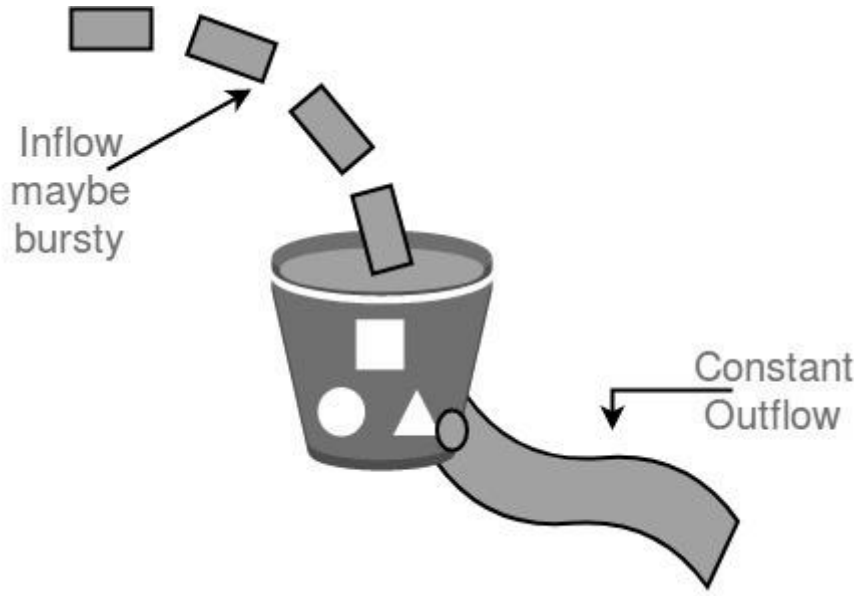
- Congestion Control is a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse.
- Congestive-Avoidance Algorithms (CAA) are implemented at the TCP layer as the mechanism to avoid congestive collapse in a network.
- There are two congestion control algorithm which are as follows:

- **Leaky Bucket Algorithm**
- The leaky bucket algorithm discovers its use in the context of network traffic shaping or rate-limiting.
- A leaky bucket execution and a token bucket execution are predominantly used for traffic shaping algorithms.

- This algorithm is used to control the rate at which traffic is sent to the network and shape the burst traffic to a steady traffic stream.
- The disadvantages compared with the leaky-bucket algorithm are the inefficient use of available network resources.
- The large area of network resources such as bandwidth is not being used effectively.

Let us consider an example to understand

Imagine a bucket with a small hole in the bottom.No matter at what rate water enters the bucket, the outflow is at constant rate.When the bucket is full with water additional water entering spills over the sides and is lost.




Similarly, each network interface contains a leaky bucket and the following **steps** are involved in leaky bucket algorithm:

1. When host wants to send packet, packet is thrown into the bucket.
2. The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
3. Bursty traffic is converted to a uniform traffic by the leaky bucket.
4. In practice the bucket is a finite queue that outputs at a finite rate.

- **Token bucket Algorithm**
- The leaky bucket algorithm has a rigid output design at an average rate independent of the bursty traffic.
- In some applications, when large bursts arrive, the output is allowed to speed up. This calls for a more flexible algorithm, preferably one that never loses information. Therefore, a token bucket algorithm finds its uses in network traffic shaping or rate-limiting.
- It is a control algorithm that indicates when traffic should be sent. This order comes based on the display of tokens in the bucket.
- The bucket contains tokens. Each of the tokens defines a packet of predetermined size. Tokens in the bucket are deleted for the ability to share a packet.
- When tokens are shown, a flow to transmit traffic appears in the display of tokens.
- No token means no flow sends its packets. Hence, a flow transfers traffic up to its peak burst rate in good tokens in the bucket.

**Need** of token bucket Algorithm:-

The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

**Steps** of this algorithm can be described as follows:

1. In regular intervals tokens are thrown into the bucket. ƒ
2. The bucket has a maximum capacity. ƒ
3. If there is a ready packet, a token is removed from the bucket, and the packet is sent.
4. If there is no token in the bucket, the packet cannot be sent.

Let’s understand with an example,

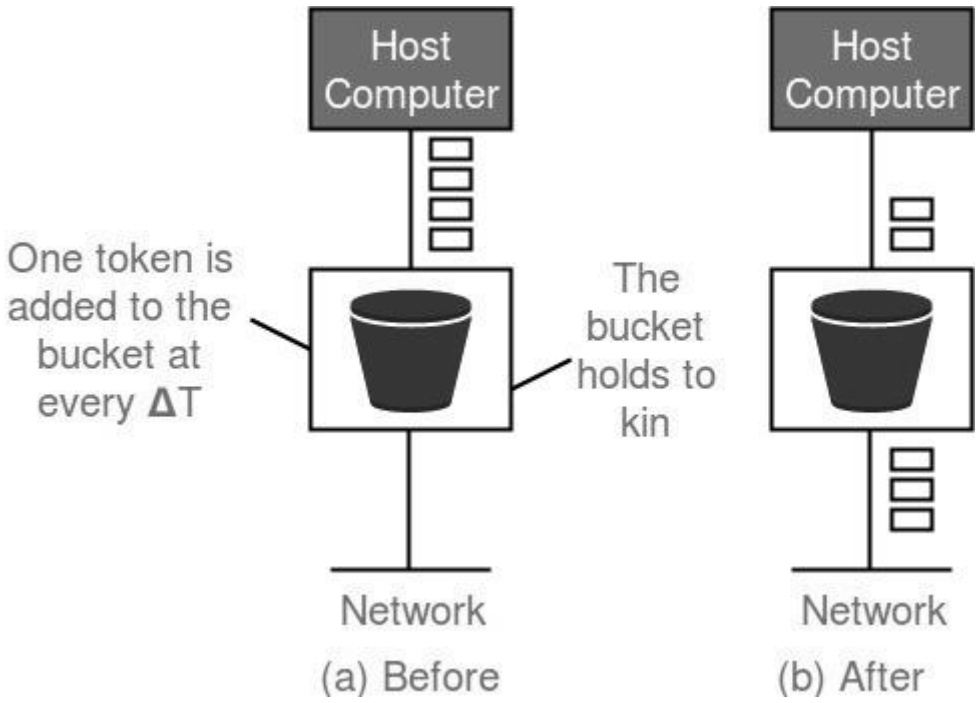
In figure (A) we see a bucket holding three tokens, with five packets waiting to be transmitted. For a packet to be transmitted, it must capture and destroy one token. In figure (B) We see that three of

the five packets have gotten through, but the other two are stuck waiting for more tokens to be generated.

**Ways in which token bucket is superior to leaky bucket:** The leaky bucket algorithm controls the rate at which the packets are introduced in the network, but it is very conservative in nature. Some flexibility is introduced in the token bucket algorithm. In the token bucket, algorithm tokens are generated at each tick (up to a certain limit). For an incoming packet to be transmitted, it must capture a token and the transmission takes place at the same rate. Hence some of the busty packets are transmitted at the same rate if tokens are available and thus introduces some amount of flexibility in the system.

**Formula:** M * s = C + ρ * s where S – is time taken M – Maximum output rate ρ – Token arrival rate C – Capacity of the token bucket in byte

Let's understand with an example,



## 4. STATIC ROUTING

Static routing is a type of network routing technique. Static routing is not a routing protocol; instead, it is the manual configuration and selection of a network route, usually managed by the network administrator. It is employed in scenarios where the network parameters and environment are expected to remain constant.

Static routing is only optimal in a few situations. Network degradation, latency and congestion are inevitable consequences of the non-flexible nature of static routing because there is no adjustment when the primary route is unavailable.

NO IDEA ABOUT THE EXAMPLE

## 5. ADAPTIVE ROUTING ALGORITHMS

Adaptive routing algorithms, also known as **dynamic routing algorithms**, makes routing decisions dynamically while transferring data packets from the source to the destination. These algorithms constructs routing tables depending on the network conditions like network traffic and topology. They try to compute computes the best path, i.e. "least – cost path", depending upon the hop count, transit time and distance.

Types of Adaptive routing algorithms:

- **Centralized**
- **Isolated**
- **Distributed**

- **Centralized algorithm** − In centralized routing, one centralized node has the total network information and takes the routing decisions. It finds the least-cost path between source and destination nodes by using global knowledge about the network. So, it is also known as global routing algorithm. The advantage of this routing is that only the central node is required to store network information and so the resource requirement of the other nodes may be less. However, routing performance is too much dependent upon the central node. An example of centralized routing is link state routing algorithm.
- **Isolated algorithm** − In this algorithm, the nodes make the routing decisions based upon local information available to them instead of gathering information from other nodes. They do not have information regarding the link status. While this helps in fast decision making, the nodes may transmit data packets along congested network resulting in delay. The examples of isolated routing are hot potato routing and backward learning.
- **Distributed algorithm** − This is a decentralized algorithm where each node receives information from its neighbouring nodes and takes the decision based upon the received information. The least-cost path between source and destination is computed iteratively in a distributed manner. An advantage is that each node can dynamically change routing decisions based upon the changes in the network. However, on the flip side, delays may be introduced due to time required to gather information. Example of distributed algorithm is distance vector routing algorithm.

## 6. IP ADDRESS

IP address stands **for "Internet Protocol address**." The Internet Protocol is a set of rules for communication over the internet, such as sending mail, streaming video, or connecting to a website. An IP address identifies a network or device on the internet.

The internet protocols manage the process of assigning each unique device its own IP address. (Internet protocols do other things as well, such as routing internet traffic.) This way, it's easy to see which devices on the internet are sending, requesting, and receiving what information.

IP addresses are like telephone numbers, and they serve the same purpose. When you contact someone, your phone number identifies who you are, and it assures the person who answers the phone that you are who you say you are. IP addresses do the exact same thing when you're online — that's why every single device that is connected to the internet has an IP address.

There are two types of IP addresses:

IPv4 and IPv6.

It's easy to recognize the difference if you count the numbers**. IPv4 addresses** contain a series of four numbers, ranging from 0 (except the first one) to 255, each separated from the next by a period — such as 5.62.42.77.

**IPv6 addresses** are represented as eight groups of four hexadecimal digits, with the groups separated by colons. A typical IPv6 address might look like this: 2620:0aba2:0d01:2042:0100:8c4d:d370:72b4.

An IP address has two parts:

**the network ID**, comprising the first three numbers of the address, and a **host ID**, the fourth number in the address. So on your home network — 192.168.1.1, for example – 192.168.1 is the network ID, and the final number is the host ID.

The Network ID indicates which network the device is on. The Host ID refers to the specific device on that network. (Usually your router is .1, and each subsequent device gets assigned .2, .3, and so on.)

**Types of IP address**

There are mainly four types of IP addresses:

- Public,
- Private,
- Static
- Dynamic.

Among them, public and private addresses are based on their location of the network private, which should be used inside a network while the public IP is used outside of a network.

Let us see all these types of IP address in detail.

**Public IP Addresses**

A public IP address is an address where one primary address is associated with your whole network. In this type of IP address, each of the connected devices has the same IP address.

This type of public IP address is provided to your router by your ISP.

**Private IP Addresses**

A private IP address is a unique IP number assigned to every device that connects to your home internet network, which includes devices like computers, tablets, smartphones, which is used in your household.

**Dynamic IP address:**

Dynamic IP addresses always keep changing. It is temporary and are allocated to a device every time it connects to the web. Dynamic IPs can trace their origin to a collection of IP addresses that are shared across many computers.

Dynamic IP addresses are another important type of internet protocol addresses. It is active for a specific amount of time; after that, it will expire.

**Static IP Addresses**

A static IP address is an IP address that cannot be changed. In contrast, a dynamic IP address will be assigned by a Dynamic Host Configuration Protocol (DHCP) server, which is subject to change. Static IP address never changes, but it can be altered as part of routine network administration.

## 7. SUB NETTING AND SUPER NETTING

**Subnetting:**

- Subnetting is a technique that is used to divide the individual physical network into a smaller size called sub-networks. These sub-networks are called a subnet. An internal address is made up of a combination of the small networks segment and host segment. A subnetwork is designed by accepting the bits from the IP address host portion; then, they are uses to assign a number of small-sized sub-networks in the original network.
- In the subnetting process, network bits are converted into host bits. Subnetting process is performed to slow down the depletion of the IP addresses. It allows the administrator to divide the single class A, class B and class C into small segments. Subnetting makes use of VLSM (Variable Length Subnet Mask) and FLSM (Fixed Length Subnet Mask).

**Advantages:**

- Subnetting increases the number of allowed hosts in the local area network.
- Subnetting decreases the volume of broadcast, hence minimize the number of network traffic.
- Sub networks are easy to maintain and manage.
- Subnetting increases the flexibility of address.
- Network security can be readily employed between sub networks rather than employing it in the whole network.

**Disadvantages:**

- The process of subnetting is quite expensive.
- To perform subnetting process, we need a trained administrator.

**Supernetting:**

Supernetting is the process that is used to combine several sub networks into a single network. Its process is inverse of the subnetting process. In supernetting, mask bits are moved towards the left of the default mask; network bits are converted into hosts bits. Supernetting is also called router summarization and aggregation.

It creates a more number of host addresses at the expense of network addresses. The Internet service provider performs the supernetting process to achieve the most efficient IP address allocation.It uses the CIDR method, i.e. Classless inter-domain routing method, to route the network

traffic across the internet. CIDR combines several sub networks and combined them together for routing network traffic. In other words, we can say that CIDR organizes the IP Addresses in the sub networks independent of the value of the Addresses.

**Advantages:**

- Supernetting reduces the traffic of the network over the internet.
- Supernetting increases the speed of routing table lookup.
- As it is summarized the number of routing information entries into a single entry, the size of the router's memory table decreased, hence saving the memory space.
- Provision for the router to isolate the topology changes from the other routers.

**Disadvantages:**

- The combination of blocks should be made in power 2 alternatively; if the three blocks are required, then there must be assigned four blocks.
- While merging several entries into one, it lacks covering different areas.
- The whole network must exist in the same class.

**Difference Between Subnetting and Supernetting**

- Subnetting divides the whole network into sub networks while supernetting combines the sub network and merge it as a whole network.
- Subnetting converts the bits of a host to bits of network hence increase the number of network bits, while supernetting converts the bits of a network to bits of the host, hence increase the number of host bits.
- Subnetting reduces the depletion of address, while supernetting increases the routing process.
- Subnetting uses VLSM and FL techniques, while supernetting uses CIDR.
- In subnetting, mask bits are moved towards the right of the default mask, whereas in supernetting, the mask bits are moved towards the left of the default mask.

## 8. HAND SHAKE IN TCP

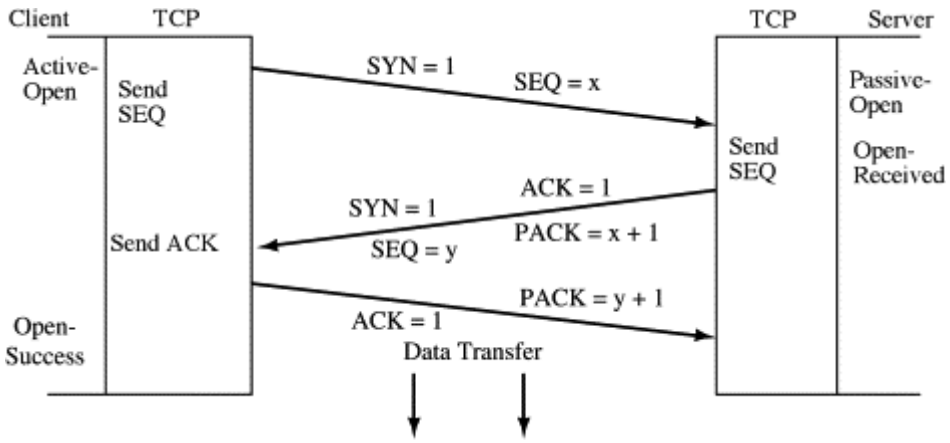
**Three-Way HandShake** or a TCP 3-way handshake is a process which is used in a TCP/IP network to make a connection between the server and client. It is a three-step process that requires both the client and server to exchange synchronization and acknowledgment packets before the real data communication process starts.

Three-way handshake process is designed in such a way that both ends help you to initiate, negotiate, and separate TCP socket connections at the same time. It allows you to transfer multiple TCP socket connections in both directions at the same time.

| Message | Description |
|---|---|
| Syn | Used to initiate and establish a connection. It also helps you to synchronize sequence numbers between devices. |
| ACK | Helps to confirm to the other side that it has received the SYN. |
| SYN-ACK | SYN message from local device and ACK of the earlier packet. |
| FIN | Used to terminate a connection. |

**TCP Three-Way Handshake Process**

TCP traffic begins with a three-way handshake. In this TCP handshake process, a client needs to initiate the conversation by requesting a communication session with the Server:




**3 way Handshake Diagram**

- Step 1: In the first step, the client establishes a connection with a server. It sends a segment with SYN and informs the server about the client should start communication, and with what should be its sequence number.
- Step 2: In this step server responds to the client request with SYN-ACK signal set. ACK helps you to signify the response of segment that is received and SYN signifies what sequence number it should able to start with the segments.
- Step 3: In this final step, the client acknowledges the response of the Server, and they both create a stable connection will begin the actual data transfer process.

## 9. DIFFERENCE BETWEEN TCP AND UDP

| Basis | Transmission control protocol (TCP) | User datagram protocol (UDP) |
|---|---|---|
| **Type of Service** | TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data. | UDP is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast types of network transmission. |
| **Reliability** | TCP is reliable as it guarantees the delivery of data to the destination router. | The delivery of data to the destination cannot be guaranteed in UDP. |
| **Error checking mechanism** | TCP provides extensive error-checking mechanisms. It is because it provides flow control and acknowledgment of data. | UDP has only the basic error checking mechanism using checksums. |
| **Acknowledgment** | An acknowledgment segment is present. | No acknowledgment segment. |
| **Sequence** | Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in order at the receiver. | There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer. |
| **Speed** | TCP is comparatively slower than UDP. | UDP is faster, simpler, and more efficient than TCP. |
| **Retransmission** | Retransmission of lost packets is possible in TCP, but not in UDP. | There is no retransmission of lost packets in the User Datagram Protocol (UDP). |
| **Header Length** | TCP has a (20-60) bytes variable length header. | UDP has an 8 bytes fixed-length header. |
| **Weight** | TCP is heavy-weight. | UDP is lightweight. |
| **Handshaking Techniques** | Uses handshakes such as SYN, ACK, SYN-ACK | It's a connectionless protocol i.e. No handshake |
| **Broadcasting** | TCP doesn't support Broadcasting. | UDP supports Broadcasting. |
| **Protocols** | TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet. | UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP. |
| **Stream Type** | The TCP connection is a byte stream. | UDP connection is message stream. |
| **Overhead** | Low but higher than UDP. | Very low. |

## 10. HTTP AND FTP

**HTTP:**

**HTTP** represents "**Hypertext Transfer Protocol**." HTTP is the protocol that can transfer information over the network. It is the Internet protocol suite method and defines commands and functions used for sharing web page data.

HTTP uses **a server-client model**. A client, for example, maybe a laptop or telephone device. The HTTP server is frequently a web host running web server software, such as Apache or IIS.

HTTP also represents commands such as GET and POST, which are used to handle submissions on websites. The CONNECT command can act as a fast connection that is encrypted using a secure socket layer (SSL).

HTTP is equivalent to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in how the messages are sent from the client to the server and from the server to the client. SMTP messages are saved and advanced, while HTTP messages are delivered directly.

**Features**

The features of HTTP are as follows −

**•Connectionless protocol**

HTTP is a connectionless protocol. HTTP user initiates a request and waits for a response from the server. When the server gets the request, the server processes the request and sends back the response to the HTTP user, after which the client disconnects the connection.

**•Media independent**

HTTP protocol is media independent as data can be transmitted as long as both the user and server know how to manage the data content. It is necessary for both the user and server to specify the content type in the MIME-type header.

**•Stateless**

It is a stateless protocol as both the client and server learn each other only during the current request. In HTTP every client connection opens a new session that sends its request the stateless nature keeps the protocol very simple and straightforward. This consumes very few resources on the server and can support more simultaneous users since there are no client information overheads to be maintained throughout the sessions.

**FTP:**

FTP represents **File transfer protocol** and it is a standard internet protocol supported by TCP/IP used for transmitting the files from one host to another. FTP needs TCP as a transport protocol to help the reliable end to end connections and executes two types of connections in managing data transfers.

The FTP clients initiate the first connection, referred to as the control connection, to wellknown port 21 (the clients port is typically ephemeral). It is on this part that an FTP server listens for it and accepts new connections. The control connection is issued for all of the control commands a client user uses to log on to the server, manipulate files, and terminate a session. This is also the relationship across which the FTP server will transmit messages to the client in response to their control commands.

The second connection used by FTP is defined as the data connection. Typically, the data connection is established on the server port 20. It depends on how the data connection is established; both the client and server can use ephemeral ports. It is across the connection that FTP shares the information.

**Advantages of FTP**

The advantages of FTP are as follows −

- Speed − The FTP is one of the quickest ways to transfer documents from one device to another.
- Security − It can create the FTP server. We need to log in with the username and password.
- Efficient − It is higher efficient as we do not require all the services to obtain the whole file.
- Back & forth movement − FTP enables us to send the files back and forth.

Disadvantages of FTP

- FTP serves two operations, such as sending and receiving huge files on a network. The size limit of the file is 2GB that can transmit.
- Passwords and file text are sent in clear text that enables unwanted eavesdropping. Therefore, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
- It is not compatible with every system

## 12. ARCHITECTURE OF WWW

WWW stands for World Wide Web. A technical definition of the World Wide Web is : all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP).

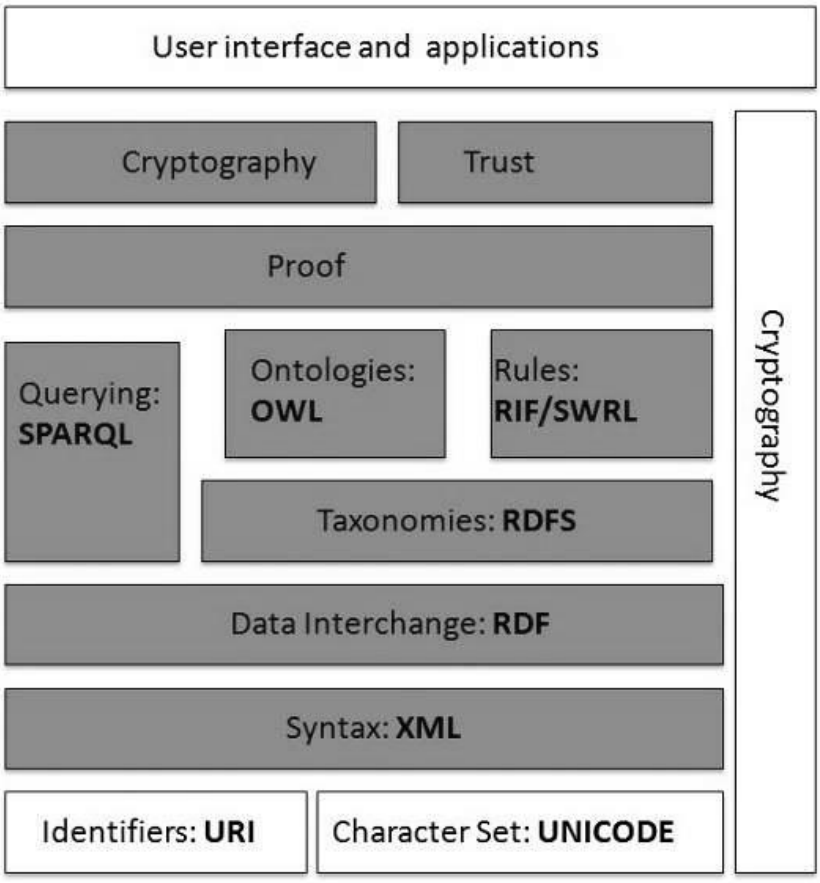
A broader definition comes from the organization that Web inventor Tim Berners-Lee helped found, the World Wide Web Consortium (W3C).

The World Wide Web is the universe of network-accessible information, an embodiment of human knowledge.

In simple terms, The World Wide Web is a way of exchanging information between computers on the Internet, tying them together into a vast collection of interactive multimedia resources.

### WWW Architecture

WWW architecture is divided into several layers as shown in the following diagram:




### Identifiers and Character Set

**Uniform Resource Identifier (URI)** is used to uniquely identify resources on the web and **UNICODE** makes it possible to built web pages that can be read and write in human languages.

**Syntax**

**XML (Extensible Markup Language)** helps to define common syntax in semantic web.

**Data Interchange**

**Resource Description Framework (RDF)** framework helps in defining core representation of data for web. RDF represents data about resource in graph form.

**Taxonomies**

**RDF Schema (RDFS)** allows more standardized description of **taxonomies** and other **ontological** constructs.

**Ontologies**

**Web Ontology Language (OWL)** offers more constructs over RDFS. It comes in following three versions:

- OWL Lite for taxonomies and simple constraints.
- OWL DL for full description logic support.
- OWL for more syntactic freedom of RDF

**Rules**

**RIF** and **SWRL** offers rules beyond the constructs that are available from **RDFs** and **OWL.** Simple Protocol and **RDF Query Language (SPARQL)** is SQL like language used for querying RDF data and OWL Ontologies.

**Proof**

All semantic and rules that are executed at layers below Proof and their result will be used to prove deductions.

**Cryptography**

**Cryptography** means such as digital signature for verification of the origin of sources is used.

User Interface and Applications

## 13. IEEE 802.3 MAC SUB LAYER

IEEE 802.3 is a working group and a collection standards defining the physical layer and data link layer's media access control (MAC) of wired Ethernet. The standards are produced by the working group of Institute of Electrical and Electronics Engineers (IEEE). This is generally a local area network (LAN) technology with some wide area network (WAN) applications. Physical connections are made between nodes and/or infrastructure devices (hubs, switches, routers) by various types of copper or fibre cable.

802.3 is a technology that supports the IEEE 802.1 network architecture.

802.3 also define LAN access method using CSMA/CD.

**802.3 MAC Sub Layer:**

The IEEE 802.3 Sub Layer is another name for Classic Ethernet MAC Sub layer Protocol.

**Classic Ethernet** is the original form of Ethernet used primarily in LANs. It provides data rates between 3 to 10 Mbps.It operates both in the physical layer and in the MAC sublayer of the OSI model. In the physical layer, the features of the cables and networks are considered. In MAC sublayer, the frame formats for the Ethernet data frame are laid down.

Classic Ethernet was first standardized in 1980s as IEEE 802.3 standard.

**Frame Format of Classic Ethernet**

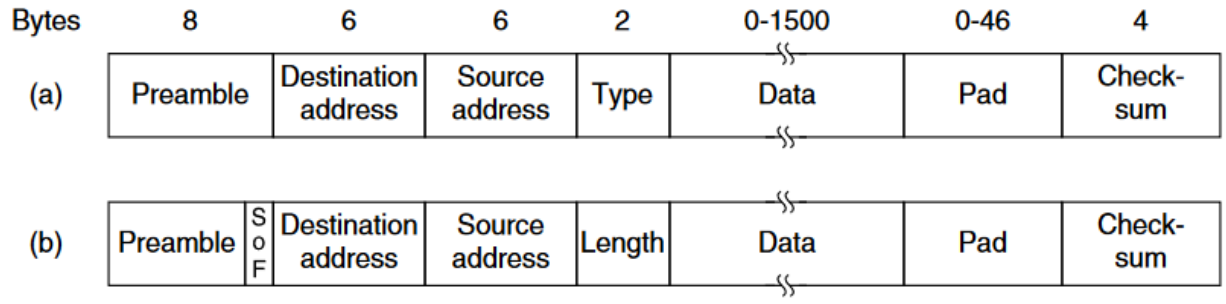



**Figure 4-14.** Frame formats. (a) Ethernet (DIX). (b) IEEE 802.3.

Classic Ethernet frames can be either of Ethernet (DIX) or of IEEE 802.3 standard. The frames of the two standards are very similar except for one field. The main fields of a frame of classic Ethernet are –

- **Preamble** − It is the starting field that provides alert and timing pulse for transmission. In case of Ethernet (DIX) it is an 8 byte field and in case of IEEE 802.3 it is of 7 bytes.
- **Start of Frame Delimiter (SOF)** − It is a 1 byte field in an IEEE 802.3 frame that contains an alternating pattern of ones and zeros ending with two ones.
- **Destination Address** − It is a 6 byte field containing physical address of destination stations.
- **Source Address** − It is a 6 byte field containing the physical address of the sending station.
- **Type/Length** − This is a 2 byte field. In case of Ethernet (DIX), the field is type that instructs the receiver which process to give the frame to. In case of IEEE 802.3, the field is length that stores the number of bytes in the data field.
- **Data** − This is a variable sized field carries the data from the upper layers. The maximum size of data field is 1500 bytes.
- **Padding** − This is added to the data to bring its length to the minimum requirement of 46 bytes.
- **CRC** − CRC stands for cyclic redundancy check. It contains the error detection information.

## 14. COMPONENTS OF EMAIL AND COMPANION PROTOCOLS

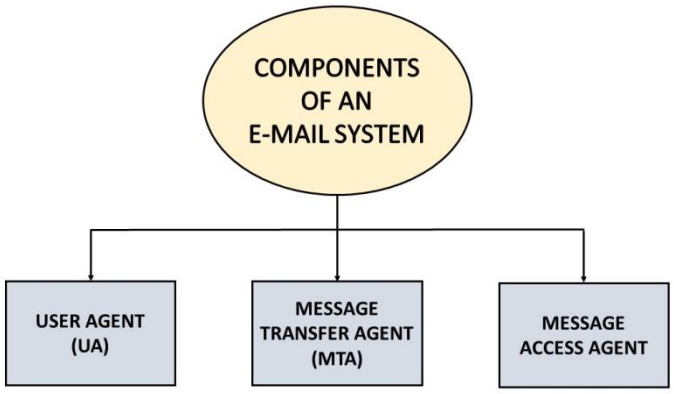
**Electronic mail (e-mail)** is a computer-based program that allows users to send and receive messages. E-mail is the electronic version of a letter, but with time and flexibility advantages. While a letter can take anywhere from a week to a couple of months to reach its intended destination, an e-mail is sent virtually almost instantly.

Messages in the mail contain not just text but also photos, audio, and video data. A person sending an e-mail is a sender, and the person receiving it is the recipient.

### Components Of Electronic Mail

The following are the essential components of an e-mail system:

1. User Agent (UA)
2. Message Transfer Agent (MTA)
3. Message Access Agent




### User Agent (UA)

The User-Agent is a simple software that sends and receives mail. It is also known as a mail reader. It supports a wide range of instructions for sending, receiving, and replying to messages and manipulating mailboxes.

Some of the services supplied by the User-Agent are listed below:

- Reading a Message
- Sending a reply to a Message
- Message Composition
- Forwarding a Message

**Message Transfer Agent**

The Message Transfer Agent manages the actual e-mail transfer operation (MTA). Simple Mail Transfer Protocol sends messages from one MTA to another. A system must have a client MTA and a system MTA to send an e-mail. If the recipients are connected to the same computer, it sends mail to their mailboxes. If the destination mailbox is on another computer, it sends mail to the receiver's MTA.

**Message Access Agent**

The Simple Mail Transfer Protocol is used for the first and second stages of e-mail delivery.

The pull protocol is mainly required at the third stage of e-mail delivery, and the message access agent is used at this point.

POP and IMAP4 are the two protocols used to access messages.

**Companion 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.

- 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.

**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

- 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.

**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.

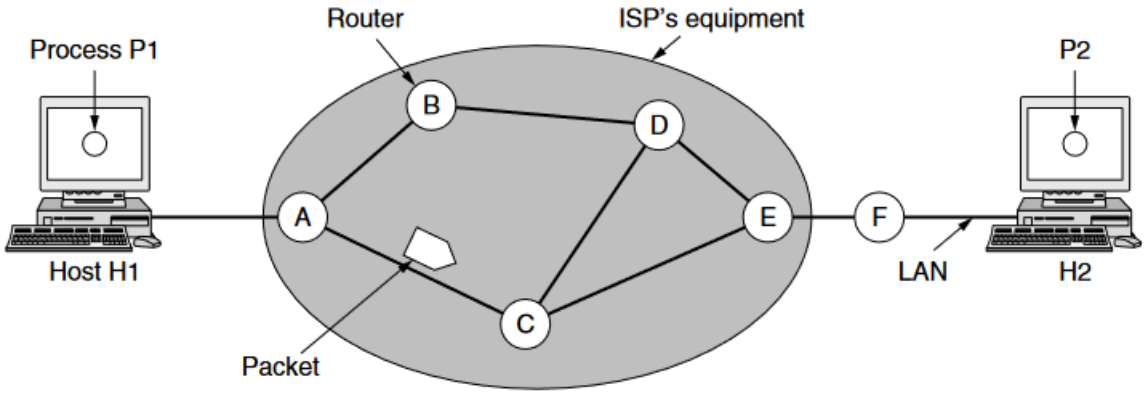
- POP is an application layer internet standard protocol.
- Since POP supports offline access to the messages, thus requires less internet usage time.
- POP does not allow search facility.
- In order to access the messaged, it is necessary to download them.
- It allows only one mailbox to be created 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.

## 15. DESIGN ISSUES OF NETWORK LAYER

Network layer comes up with certain design issues and they can be described as below:

### 1). Store-and-Forward Packet Switching

Here, the foremost elements are the carrier's equipment (the connection between routers through transmission lines) and the customer's equipment.




- H1 has a direct connection with carrier router 'A', while H2 is connected to carrier router 'F' on a LAN connection.
- One of the carrier router 'F', is pointed outside the carrier's equipment as it does not come under the carrier, whereas considered as protocols, software, and construction.
- This switching network performs as Transmission of data happens when the host (H1) with a packet transfers it to the nearby router through LAN (or) point-to-point connection to the carrier. The carrier stores the packet until it completely arrives thus confirms the checksum.
- Then after, the packet is transmitted over the path until H2 is reached.

### 2). Services Provided to the Transport Layer

Through the network/transport layer interface, the network layer delivers its services to the transport layer. One might come across the question of what type of services does the network layer provides?

So, we shall move with the same query and find out the services offered.

Services offered by the network layer are outlined considering few objectives. Those are:

- Offering services must not depend on router technology
- The transport layer needs to be protected from type, number and the topology of the available routers.

- Network addressing the transport layer needs to follow a consistent numbering scenario also at LAN and WAN connections.

Note: Next comes the scenario of connection-Oriented or connectionless

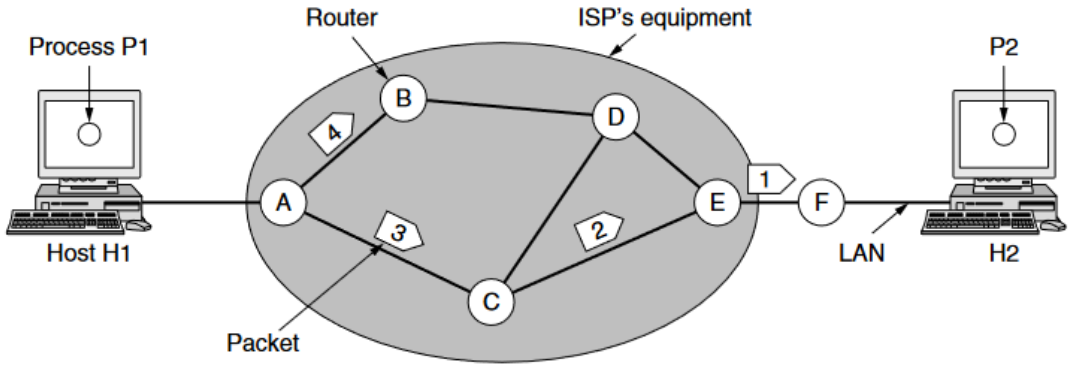
Here, two groupings are possible based on the offered services.

Connectionless – Here, routing and insertion of packets into subnet is accomplished individually. No additional setup is necessary

Connection-Oriented – Subnet must offer reliable service and all the packets are transmitted over a single route.

**3). Implementation of Connectionless Service**

In this scenario, packets are termed as datagrams and the corresponding subnet is termed as datagram subnet. Routing in datagram subnet is as follows:




A's table (initially)

| Dest. | Line |
|---|---|
| A | – |
| B | B |
| C | C |
| D | B |
| E | C |
| F | C |

A's table (later)

| | |
|---|---|
| A | – |
| B | B |
| C | C |
| D | B |
| E | B |
| F | B |

C's table

| | |
|---|---|
| A | A |
| B | A |
| C | – |
| D | E |
| E | E |
| F | E |

E's table

| | |
|---|---|
| A | C |
| B | D |
| C | C |
| D | D |
| E | – |
| F | F |

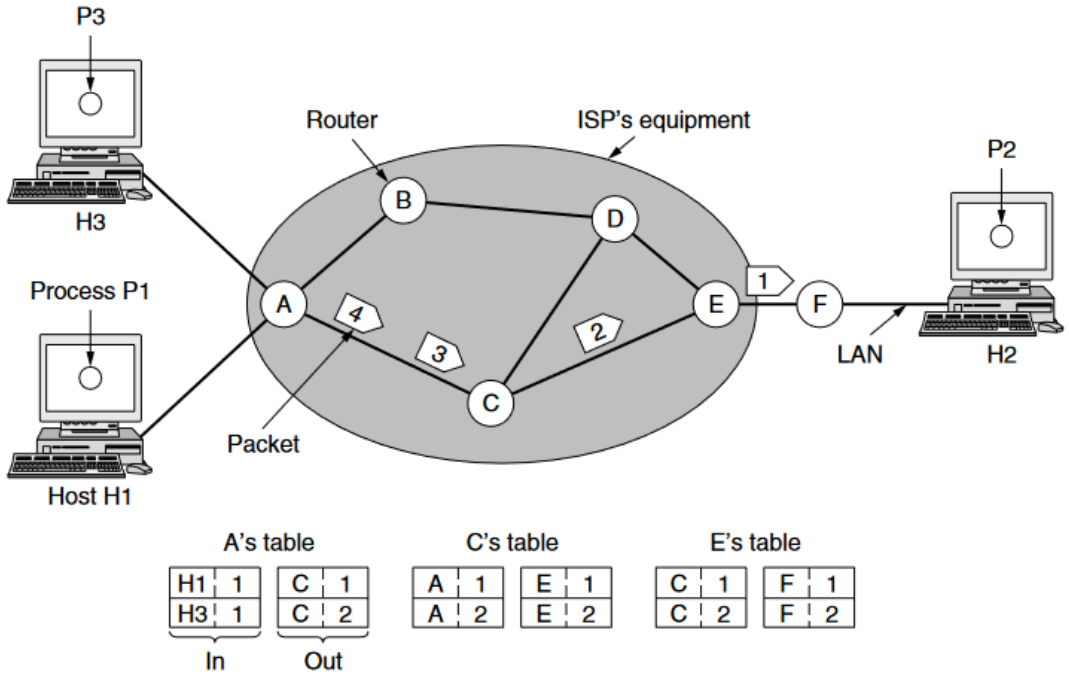
When the message size that has to be transmitted is 4 times the size of the packet, then the network layer divides into 4 packets and then transmits each packet to router 'A' through a few protocols. Each router is provided with a routing table where it decides the destination points.
In the above figure, it is clear that packets from 'A' need to be transmitted either to B or C even when the destination is 'F'. The routing table of 'A' is clearly outlined above.

Whereas in the case of packet 4, the packet from ‘A’ is routed to ‘B’, even the destination node is ‘F’. Packet ‘A’ chooses to transmit packet 4 through a different path than the initial three paths. This might happen because of traffic congestion along the path ACE.

**4). Implementation of Connection-Oriented Service**

Here, the functionality of connection-oriented service works on the virtual subnet. A virtual subnet performs the operation of avoiding a new path for each packet transmission. As a substitute for this, when there forms a connection, a route from a source node to a destination node is selected and maintained in tables. This route performs its action at the time of traffic congestion.

At the time when the connection is released, the virtual subnet also gets dismissed. In this service, every packet carries its own identifier that states the exact address of the virtual circuit. The below diagram shows the routing algorithm in the virtual subnet.



## 16. ALOHA

**ALOHA** is a multiple access protocol for transmission of data via a shared network channel. It operates in the medium access control sublayer (MAC sublayer) of the open systems interconnection (OSI) model. Using this protocol, several data streams originating from multiple nodes are transferred through a multi-point transmission channel.

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 two frames attempt to occupy the channel simultaneously, 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.

There are two types of ALOHA:

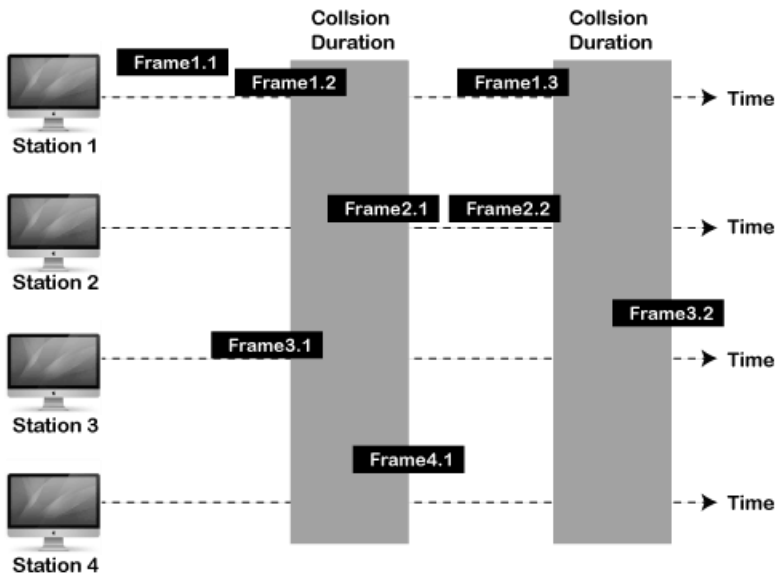
1.Pure ALOHA

2.Slotted ALOHA

**PURE ALOHA :**

Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

1. The total vulnerable time of pure Aloha is 2 * Tfr.
2. Maximum throughput occurs when G = 1/ 2 that is 18.4%.
3. Successful transmission of data frame is S = G * e ^ - 2 G.

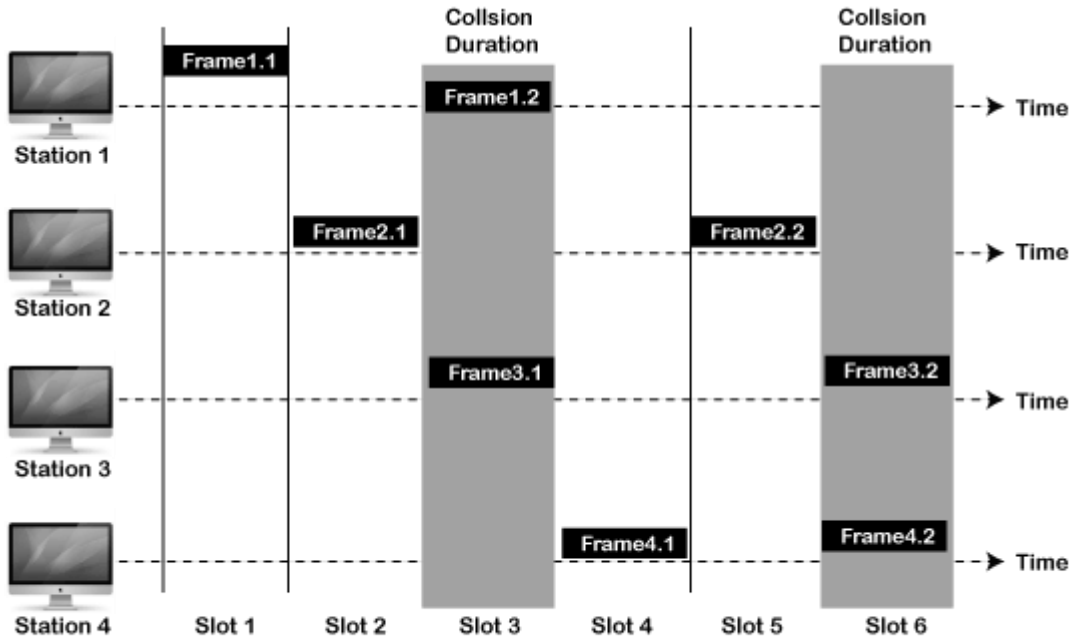



Frames in Pure ALOHA

**Slotted Aloha:**

The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.

1. Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.
2. The probability of successfully transmitting the data frame in the slotted Aloha is S = G * e ^ - 2 G.
3. The total vulnerable time required in slotted Aloha is Tfr.




Frames in Slotted ALOHA

**NOTE: A LOT OF DATA IS UNFILTERED...SO MAKE IT PRECISE AND SHORT...AND SOME DATA MIGHT BE INCONSISTENT AND UNCERTAIN...LOOK IT OUT**


**IN ASSOCIATION WITH CYBERPUNK 2077**