CHAPTER 2

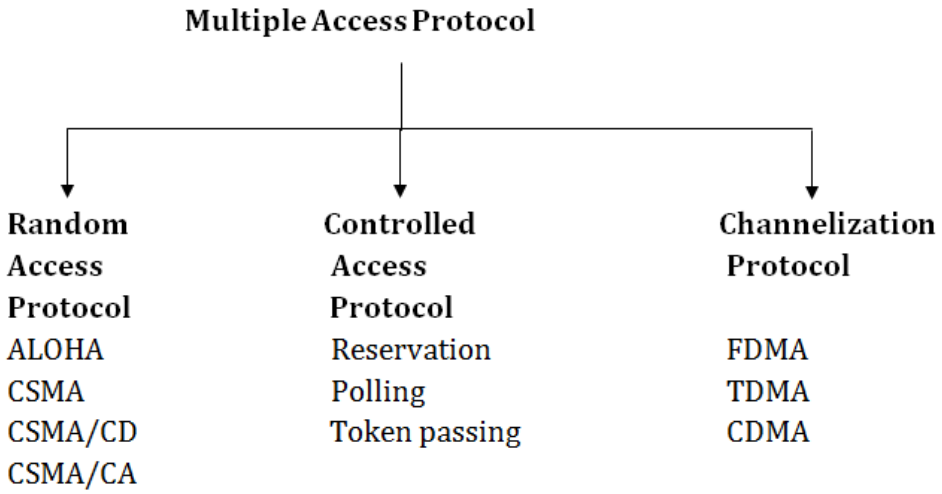
2. Media Access and Internet Working

Objectives

- To understand about Media Access Control and Internetworking.
- To explain wired and wireless networks.
- To know about switching and bridging.
- To explain about basic internetworking – IP, ARP, RARP, ICMP, BOOTP, DHCP.

2.1. Medium Access Control (MAC)

A multi-access medium based computer network needs a protocol for efficient media sharing. A Multipoint is formed when connecting more nodes or stations using a direct bond. It is otherwise called as broad cast connection. A protocol which can manage synchronized multiple access to the link is needed.



2.1.1. Random Access Control

All the stations are given equal priority or importance in any random-access system. There cannot be any station given authority over the next station in contention system. No node allows or hinders another node from sending data. A station with a data decides whether to send it using a protocol-defined procedure. This shows dependency on the environment, whether it stays idle otherwise it is busy. The protocol checks for the availability and each station will transmit when it wishes.

Features

- A station does not have a scheduled time to transmit. Between the stations, transmission is random, so it is called random access.
- No ruling stated to compete such as which station to send and which one to access the medium and it is called Contention method.
- In random method of access each station is entitled to the medium for better management.
- If more than one station attempts to submit a conflict of access and the frames are either lost or changed.

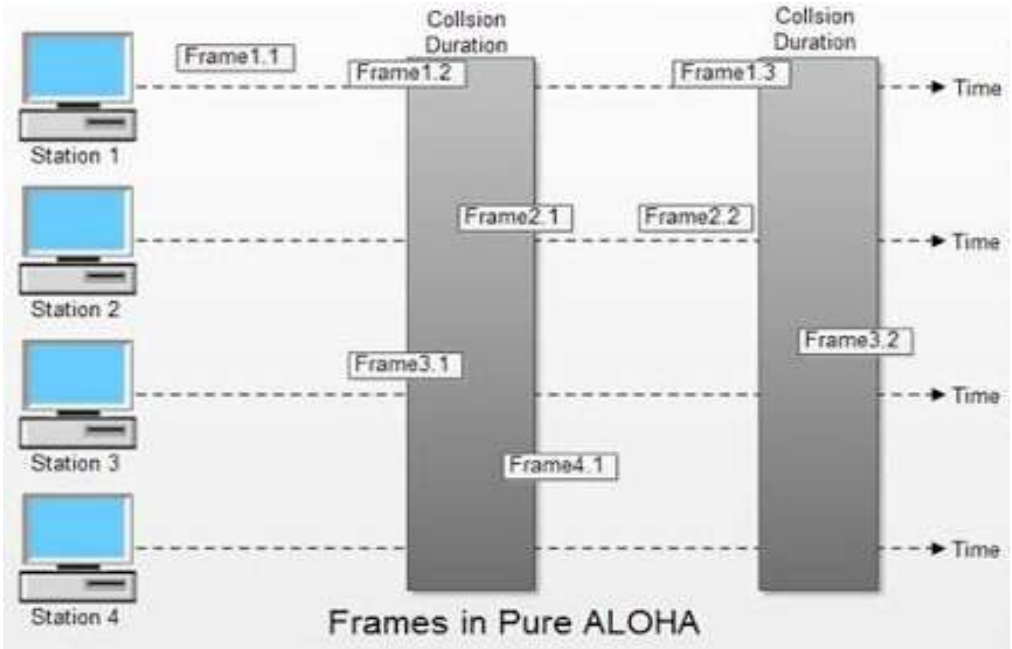
- Multiple Access is the methodology observed by ALOHA.
- The method approved with the addition of the method facing the station is called Carrier Sense Multiple Access (CSMA) that senses the medium prior to transmission.
- There are two parallel CSMA approaches that are Carrier Sense Multi Access with Collision Detection (CSMA / CD) and Carrier Sense Multi-Access with Collision Avoidance (CSMA / CA).
- Appropriate station is informed with the remedial action when collision has occurred by CSMA / CD and CSMA/CA avoids collision.

a) ALOHA

It is the initial of method for accessing the data randomly, established in 1970 at the University of Hawaii. Wireless radio LAN was its major target and also it worked out well with a medium in sharing with others too. When a station transmits information, a different station can simultaneously attempt to do just that. The two stations' data clash with each other.

Pure ALOHA

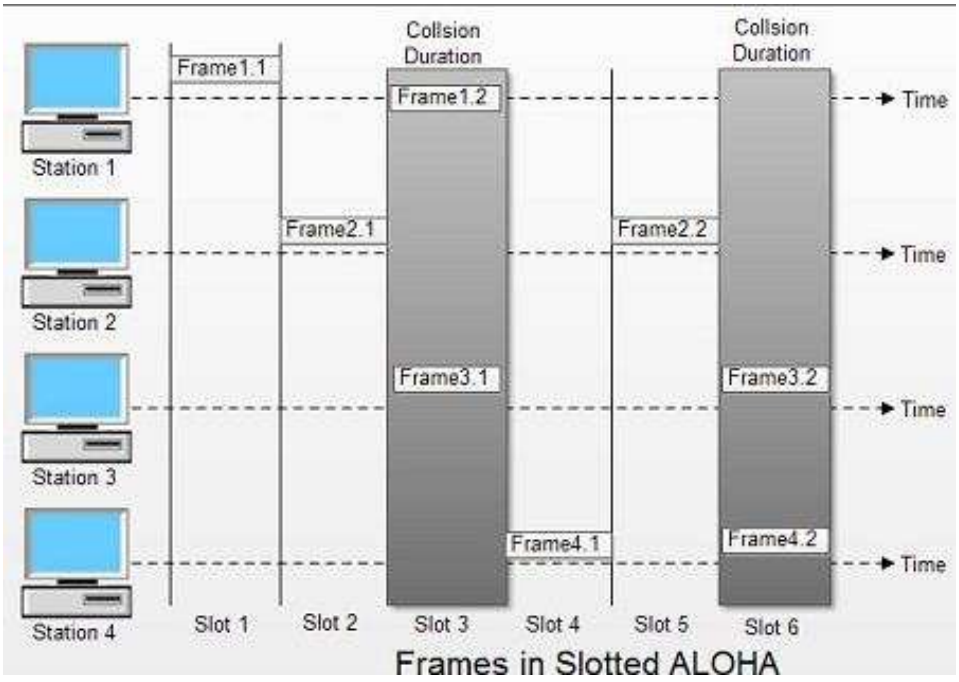
- It is the protocol which stands modest and effective.
- If it has data to send, each station transmits it as a frame through the single channel available that ends up in collision. It may involve more stations too.



- Collision happens when one bit of a frame collocates with another frame and the frames are lost.
- This protocol is based upon receiver acknowledgments.
- An acknowledgement is necessary, for a station that transmits a frame.
- On delay of receiving the acknowledgement, the sender retransmits the same frame, with the prediction that the previous one is missed on ten go.
- The frames would clash again while trafficking with resending of the same frames from these stations.
- Pure ALOHA dictates wait for the station for some duration and instructs to retransmit the data frames after the pause.
- The randomness helps prevent further collisions.

Slotted ALOHA

- The time in slotted ALOHA is divided as time force and force slots and instruct the node to submit by start of time slot.
- On this, channel is permitted to deliver at the start of the coordinated time slot, if a station fails that moment, it must wait until the start of the next time slot.
- The station that began to transmit by the start of time slot has completed frame transmission.



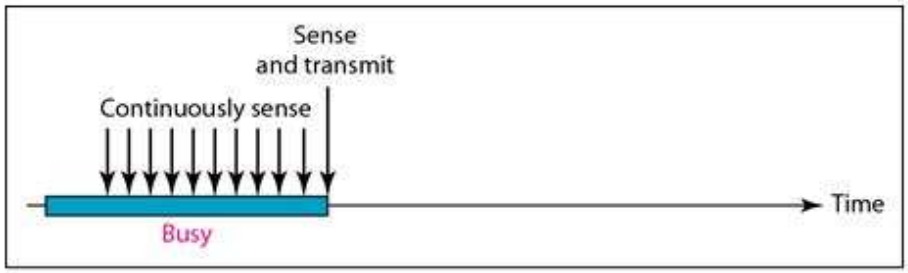
b) Carrier Sense Multiple Access (CSMA)

- This protocol operates on carrier sensing principles. A station listens to the nature of the transmission (carrier) on the cable in this protocol and intends to behave accordingly.
  - Non - Persistent CSMA.
  - I - Persistent CSMA.
  - P - Persistent CSMA.

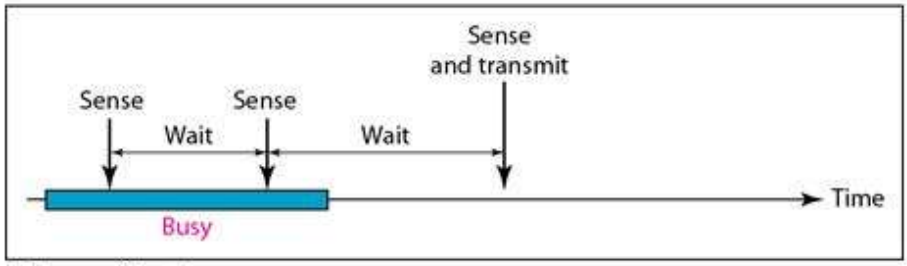
- **I-persistent CSMA**
  - A modest and straight forward method.
  - The frames are sent immediately after the station finds the line idle.
  - This approach leads to maximum collision, as two or more stations can idle the line and start sending their frames.

- **Non-persistent**
  - The transmission of data is done in this mode automatically, when the line stays passive.
  - For a predicted time duration it holds on and when the connection becomes active, further checks for medium's availability.
  - Decreases collision, since the nodes defer and then trace the path for submission concurrently.
  - Decreases network reliability, since the medium remains idle while there are several frame stations to transmit.

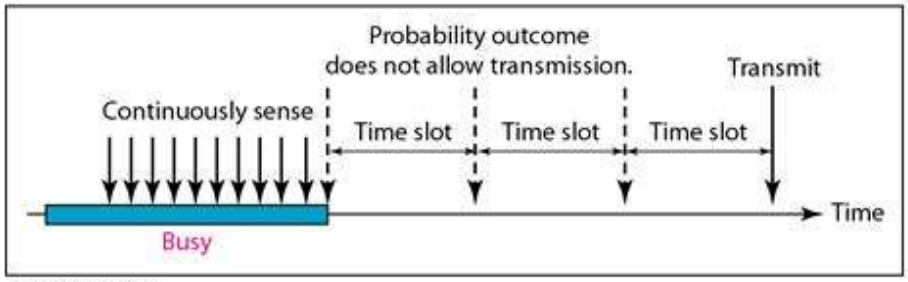
- **P-persistent**
  - This method works when the medium holds time slots of length same as or bigger one to the longest time of propagation.
  - P-persistent methods incorporate the benefits of those two other methods.
  - It decreases the risk of collision and proves efficiency.



a. 1-persistent



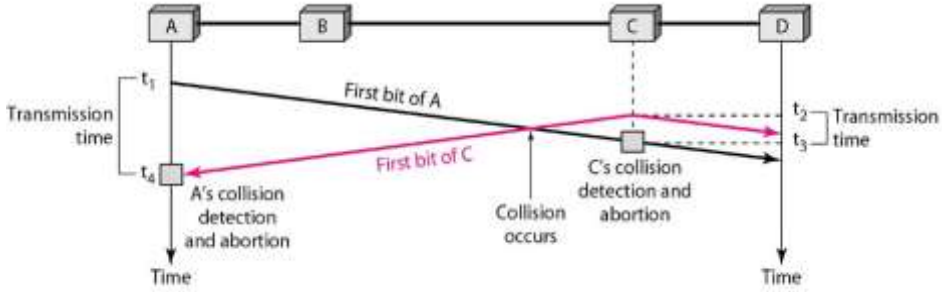
b. Nonpersistent



c. p-persistent

c) Carrier Sense Multiple Access with Collision Detection (CSMA\CD)

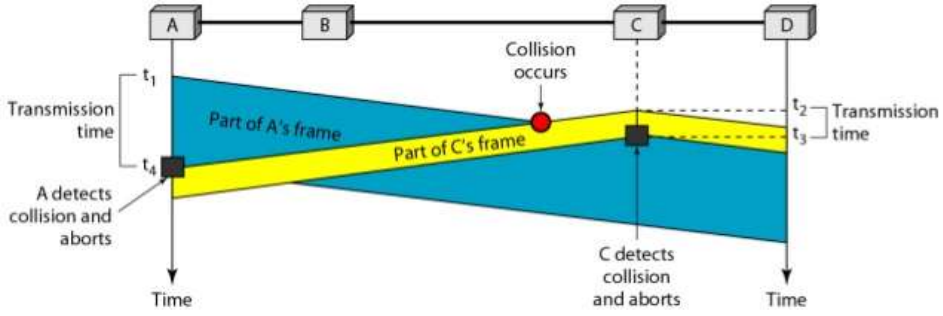
The clarity of an algorithm is not specified with this CSMA method, as how to resolve collision by employing its CSMA/CD arguments. A station tracks the medium in its system post the transmission of a frame to see if the transmission has been carried out properly. Then the work gets done or it resends the frame if collision occurs.



Time

- Using persistence procedure Node, A executes its procedure at time t1, and begins to submit frames.
- Node C is yet to receive the initial bit which was transmitted by A at t2.
- C performs the process of perseverance so that begins transmitting bits on both directions.
- After t2, collision occurs at t3 and it is identified by C as initial bit of frame A is delivered. So, C shall abort transmission.
- By t4, A understands that collision has occurred as the initial bit of C is received, and so it is instantly aborted.
- Finally the transmission is resolved as A during t4-t1 and C during t3-t2.

Restriction on frame size should be included in CSMA / CD. Collison should be detected and the transmitter must abort it before transmitting end bit of the data frame. On transmitting complete frame, no more back up is available, the monitoring goes to halt state. The transmission time of Tfr should be minimum twice the longest time of propagation Tp = 2Tp.

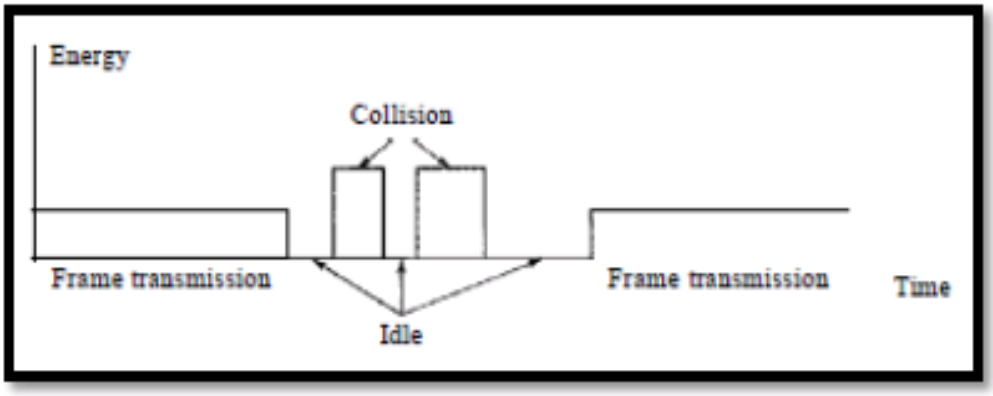


CSMA / CD is similar to the protocol for ALOHA. Until we begin sending the frame employing any of the persistence procedure, the persistence mechanism is used to sense the channel. Transmission is used to send the whole frame, and hold on to receive an acknowledgment and detect collision as well. In the event that other stations have not yet detected the collision, the jamming signal is being used to trigger the collision.

Energy level's of a channel has 3 values as: Zero, Normal, Abnormal.

- **Zero level** - the channel is idle.
- **Normal level –** the channel is acquired and has started transmitting the frame.
- **Abnormal level -** the normal energy level is doubled with collision.

A station with a frame to submit needs to track the energy level to decide if the channel is active, idle or in collision mode.



Energy level during transmission, idle and collision

CSMA/CD's throughput is max of ALOHA control or otherwise it is considered to be a slotted one. The max throughput occurs at a different value of G, which holds dependency caused by process of persistence while the value of p refers to p-persistence.

d) Carrier Sense Multiple Access/Collision Avoidance

As a collision is detected, the CSMA / CA station must be capable of receiving when transmitting. The transmission of its data occurs with a station when it receives a signal of non-collision and during collision, 2 signals are received, either its signal or a signal received from other station.

The obtained signal must be substantially different in these two situations. The signal of the second station has to append a considerable amount of energy to that provided by previous station.

The energy of the signal stays unchangeable to that of the energy preserved during transmission in **wired network**, since either cable duration seems low or repeaters to amplify the energy exists with sender and receiver. Most of the transmitted energy in **wireless network** is lost in transmission. There is very little energy in the received signal.

CSMA/CA is mainly invented for wireless network.

1. **Frame space**
2. **Contention window**
3. **Acknowledgements**

Inter Frame Space

- Even if the channel is found idle, collision is prevented by deferring transmission.
- The identification of a channel staying idle will not instantly mount the process.
- It awaits interframe space (IFS) for a period of time.
- The IFS time enables this station to be read from the pre-positioning of the signal from a station.
- The IFS variable may also be used to set the preferences for stations or frame styles.
- Continuing to be idle after the IFS time the station will give, but if it still has to wait the same time as the time of the contention.
- The IFS can also be used in CSMA / CA to describe a station or frame's priority.

Contention Window

- The slots are segregated to form the window of contention.
- A ready-to-send station selects any slot for its idle time.
- As per the binary exponential back-off technique, the slot's count in the window varies.
- For the first time it takes up one slot and doubles after the ifs duration every time the station does not identify an inactive stream.
- The station monitors the channel in contention window at the end of every time slot.
- If the station finds the channel busy, rather than restarting the process it just ends the timer and restarts it while the channel is noticed to be idle. This provides preference to longest waiting station.
- In CSMA / CA, if the station notices the channel busy, the contention window timer doesn't restart, the timer restarts when the channel becomes passive.

Acknowledgement

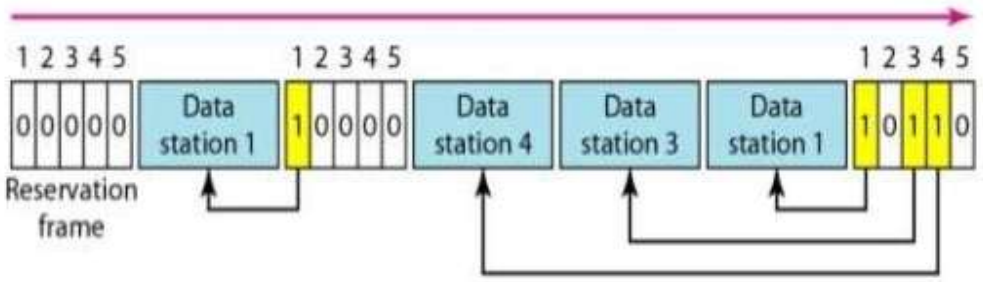
- Collision results in data loss.
- Data can be compromised during forwarding.
- As the recipient receives the data frame, a positive acknowledgment and time-out timer is initiated.

2.1.2. Controlled Access Control

In controlled access the station consults with each other in identifying the appropriate station to transmit. Any identified station doesn't be granted priority to send without authorization from connected stations.

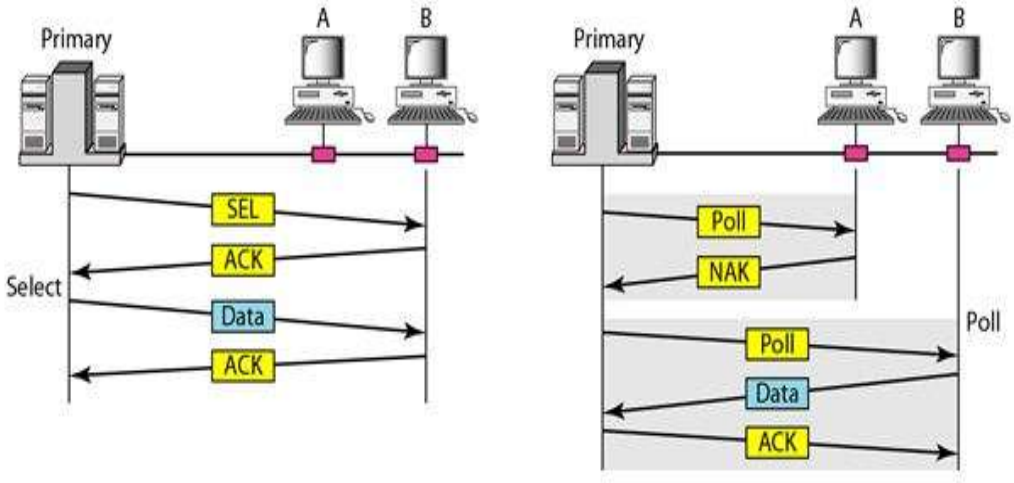
a) Reservation

During this process, reservation had been made by the station before sending data. Intervals are obtained by splitting the time and usually the data frames the reservation frame within that duration. Having the availability of N stations in the system, the reservation frame is exactly N reservation mini slots. Each mini slot is station owned. Therefore, whenever a data frame has to be sent by a station, its own mini slots are reserved. The stations with these reservations hold the authority to send the required data frame that is usually preceded by the reservation frame.



b) Polling

This methodology operates based on topology where each unit is chosen as either a primary or a secondary station. And when the ultimate destination is a secondary device, all data exchanges must be performed via the primary device. The first device manages the connection and it is followed by the secondary device. The primary computer is always session initiator.



- If primary wants to receive data, it tells the secondary to get ready to receive.

Select

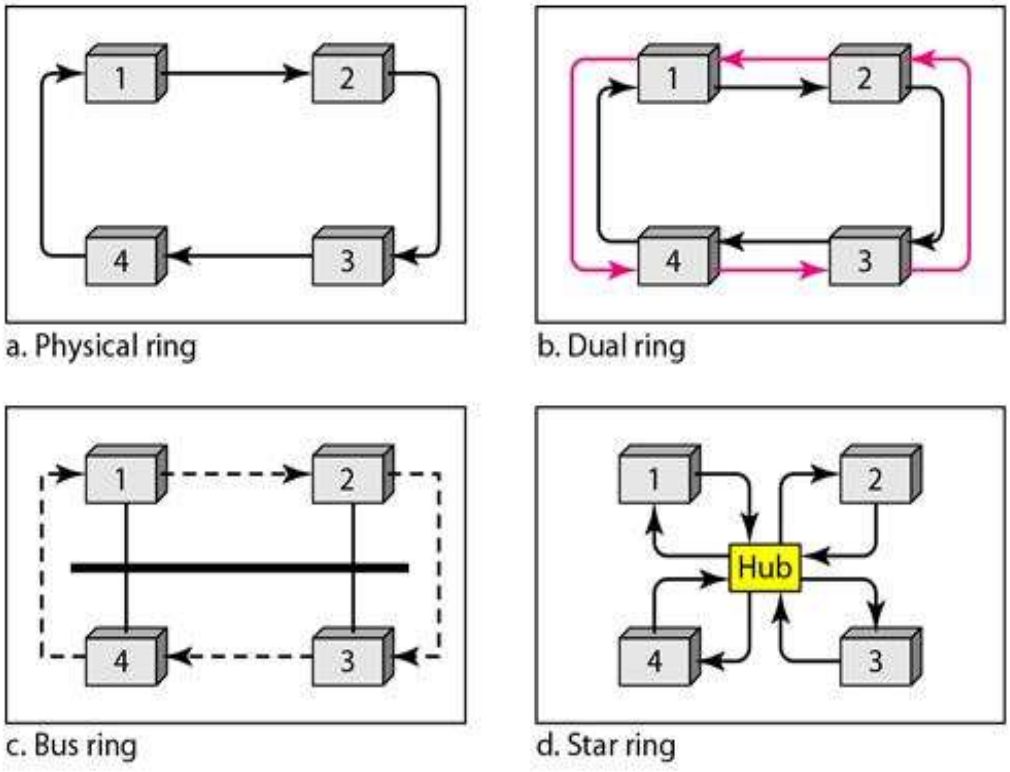
- If the main computer has anything to send, the select function is used.
- If it has anything to attach, attach it to the primary computer.
- The primary must alert the secondary to the upcoming transmission and wait for the secondary's ready state to be recognised.
- A select (SEL) frame is created and transmitted by the primary before sending the data, and address of the secondary is held by a field.

Poll

- Whenever a primary device attempts to invoke a transmission from any other secondary devices, this poll mechanism is utilized by the primary device.
- Each system must seek to POLL, if it needs to send, whenever the primary data is ready for receiving.
- When the first secondary is contacted, the response might be a NAK or any data frame.
- Assuming reflex is negative with NAK, the first one elects the next one similar to it, till it identifies the station with transmittable data.
- In case of a positive answer, the first one reads data frame and sends an acknowledgment (ACK) confirming its reception.

c) Token Passing

On a network connectivity, stations are arranged in such a way that it appears to be a logical ring. There exists a predecessor and successor stations for every station. The channel can be accessed at the current station. A special packet called a token, flows through the ring owning to token grants the station the might to view and transfer the data to the station. Therefore, a station had to wait before sending a data until its predecessor receives the token. The token is preserved till the results are sent and is released once it is left out with no more data. Unless the token is received in the next round, the station is unable to send data. When a station receives the token in this process and has no data to send, it only transfers the data to the next station. The token needs to be controlled to make sure it is not lost or ruined. Usually, the tokens are controlled by the token management and its primary role is to allocate the station priorities and the types of data for transmission. This token management is highly required for identifying high priority stations, where the token held by it is higher than the token held by other stations.



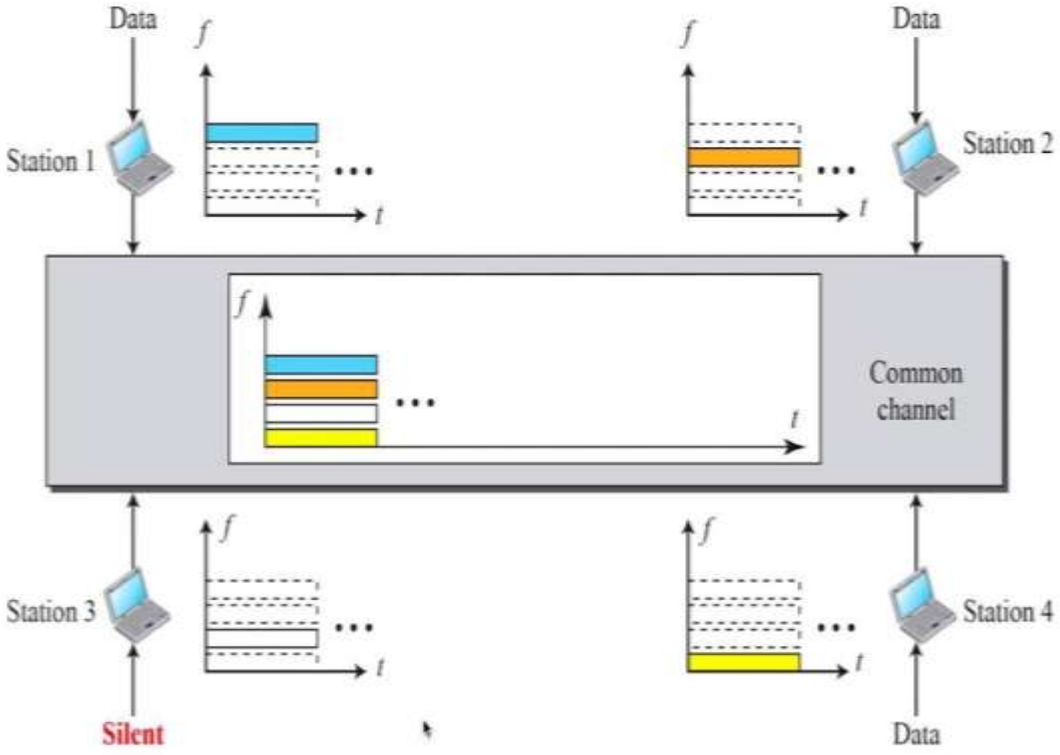
2.1.3. Channelization

It is a multiple access method where the bandwidth available for establishing a connectivity can be shared either by frequency or time or code.

a. FDMA → Frequency Division Multiple Access.
b. TDMA → Time Division Multiple Access.
c. CDMA → Code Division Multiple Access.

a) FDMA – Frequency Division Multiple Access

In FDMA, the accessible bandwidth is split as different bands of frequency and a band is reserved to each station for data transmission. The transmitter frequencies are confined by means of a band pass filter. To avoid station interfaces, tiny guard bands separate the assigned bands from each other. In FDMA, guard bands segregate the bandwidth of shared channel.



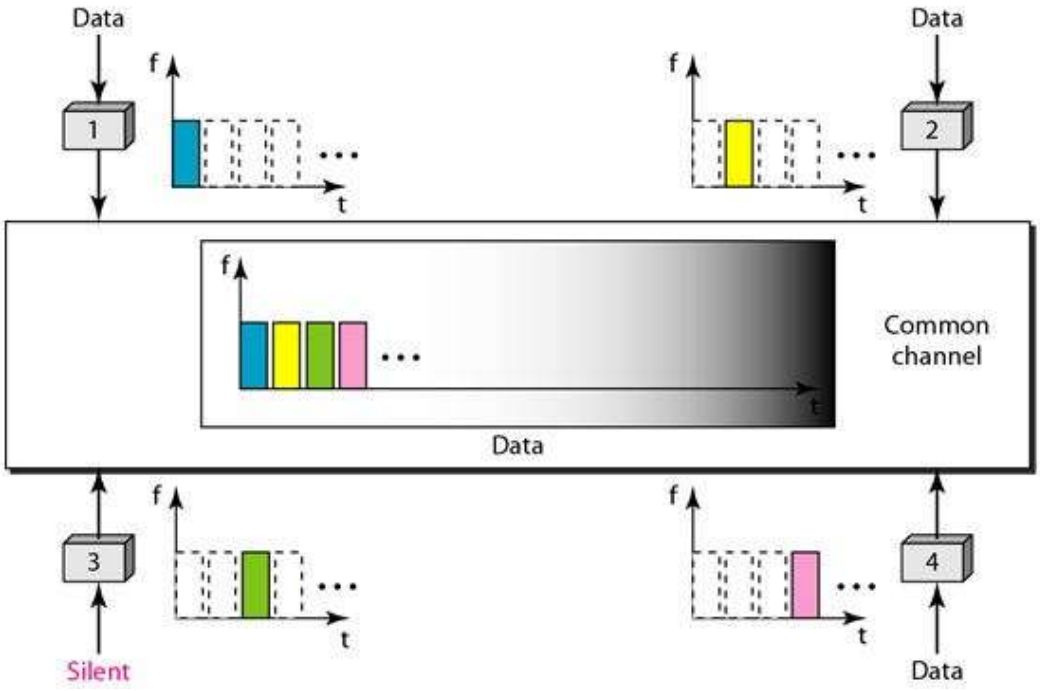
- FDMA specifies a predefined frequency bands or entire duration of and established connectivity. Eg: Cellular telephone systems.

Here, the physical layer techniques integrate low-bandwidth channel loads. Low-pass is the channels that are integrated. The multiplexer modulates, integrates and generates a band pass signal for the signals. Every channel's bandwidth is transferred by the multiplexer. The access method tells each station in its physical layer in the datalink layer to propagate a band pass signal out if data passed to it. In the allocated band, the signal must be generated. The physical layer does not contain a physical multiplexer. Automatically band pass-filter filters the signals produced at each station. When they are sent to a popular channel, they are mixed.

b) TDMA-time Division Multiple Access

The stations share the channel's bandwidth over time in this methodology. A time slot is assigned to each station during which it will be submitting data.

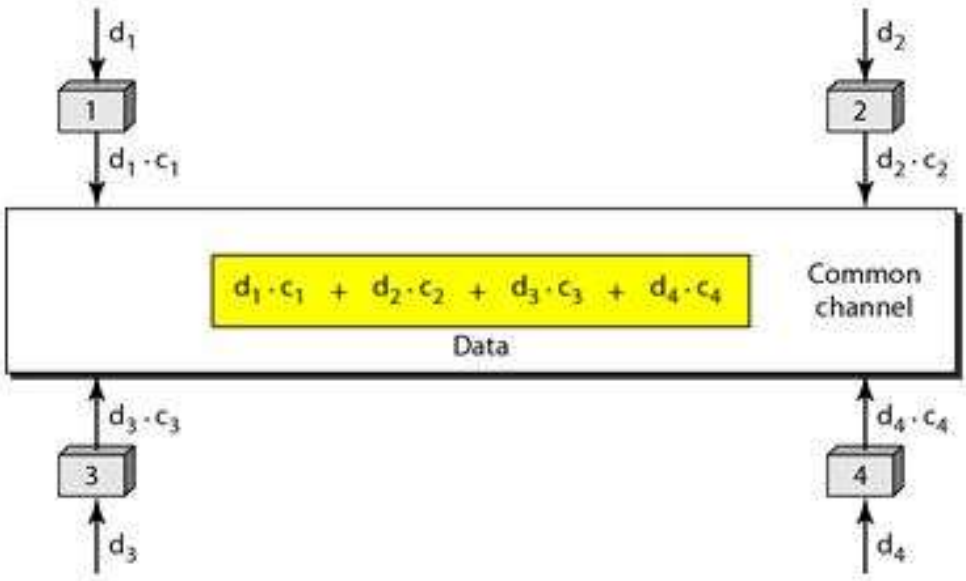
Every data is sent during the allotted slot of time duration.



The primary issue with TDMA is to achieve synchronisation between the various stations. The station must be alert about the start and end of the time durations along with its location. If the stations are scattered over a wide area of propagation delays, the delay guard times are added to compensate. Synchronization is typically done by providing some synchronisation bits by the start position. TDMA holds the bandwidth as a channel which shares among various stations over time. In the physical layer, the slower data is combined and transmitted using a faster source. The interleaving of data units are accomplished by using multiplexer. In the data link layer, TDMA is an access process and conveys the physical layer to occupy the designated slot of duration.

c) CDMA-code Division Multiple Access

In code division multiple access, it occupies only an allotted channel of bandwidth in the link. It sends all the data simultaneously in no time-sharing mode. In CDMA, a channel transmits all data concurrently.



For Example

Four stations 1,2,3,4 as d1, d2, d3, d4

Codes c1, c2, c3, c4

There are 2 properties

1. The multiplication of each code by another, results in 0
2. The multiplication of each code by itself, results in 4

   Message = d1.c1 + d2.c2 + d3.c3 + d4.c4

2.2. Ethernet (802.3) or Wired LAN

LAN - Local Area Network

The LAN has numerous connecting methodologies stated as Ethernet, token bus or ring, FDDI, ATM LAN etc. In 1985, IEEE developed 802 project and ANSI adopted in 1987. The physical standards are established by subdividing data link layer as two other layers by IEEE.

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

Physical Layer

It depends upon how it is implemented and the types of physical media used. The specifications for all LAN are detailly defined by IEEE.

Datalink Layer

As per the IEEE standard, data link layers can be divided as LCC and MAC.

1. LCC - Logical Link Control

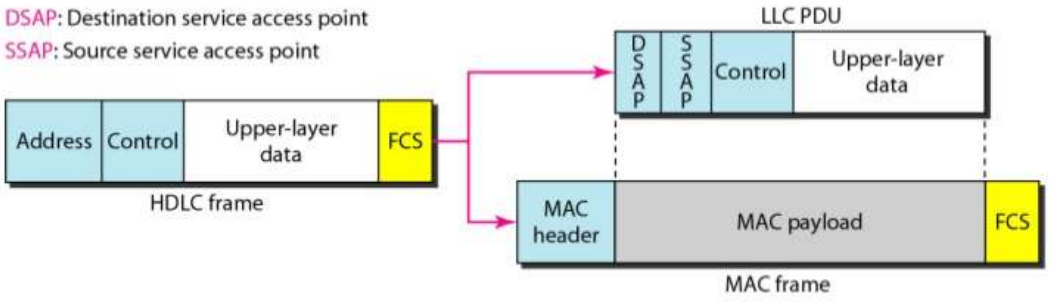
The framing, control over the data flow and errors are managed by data link control. In IEEE project 802, flow control, error control and certain framing duties are dealt in logical link control. In both LCC & MAC, framing is done. For all IEEE LANs, the LCC provides a single data link control protocol. Different LANs are provided with various protocols. One LCC Protocol offers interconnection between various LANs, as MAC sublayer performs the transport operation.

Framing

- LCC defines a Protocol Data Unit (PDU).
- The leader contains a control field of both error and flow control.
- The protocol of higher layer and LCC are defined at the source and destination respectively by the other two header files. These fields are called as Destination Service Access Point (DSAP) and Source Service Access Point (SSAP).

Need for LCC

The purpose of LCC is to provide flow and error control for the upper layer protocol that actually demand their service. LCC facilitates error control, flow control over protocols of application layer. IP is not used as the service provided by LCC in upper layers.

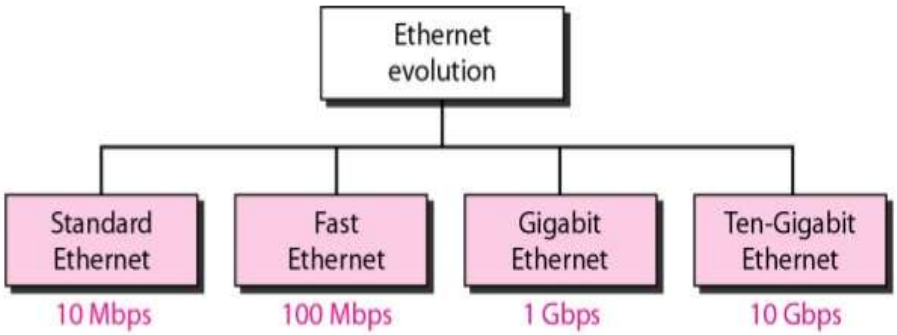


2. MAC - Media Access Control

- It includes random access, controlled access and channelization.
- A sub layer called MAC has been developed by IEEE project 802 with the unique access method which is specified for each LAN.

- It identifies CSMA / CD as the Ethernet LAN media access system and the LAN token ring and token bus system of token passing.
- A variety of distinct modules are included in the MAC layer. They are specifying the method of access and the unique format of framing in LAN.

2.2.1. Evolution of Ethernet



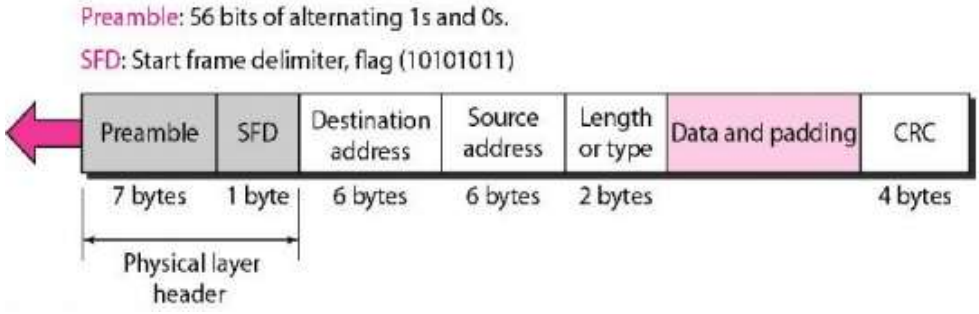
1. Standard Ethernet

MAC Sublayer

- All the operations of the methods are administrated by MAC sublayer.
- The data of the upper layer is framed and transferred to the physical layer.

Frame Format

- The frame of ethernet has 7 fields.



Preamble: 56 bits of 0's and 1's

SFD: start frame delimiter flag.

Preamble

The first frame field has 7 bytes of the 802.3 and are alerted by the receiving device and allows synchronise the timing of the input.

Start Frame Delimiter (SFD)

The next field that is obviously the second is of 1 byte and signals the frame's beginning.

The SFD frame alerts the station of synchronisation or lack of opportunity.

It also alerts the receiver that the next field is the destination address.

Destination Address (DA)

The DA field is (6 bytes) and includes the physical address of the packet receiving station or station.

Source Address (SA)

The SA field is (6 bytes) and includes the physical address of the packet sender.

Length Type

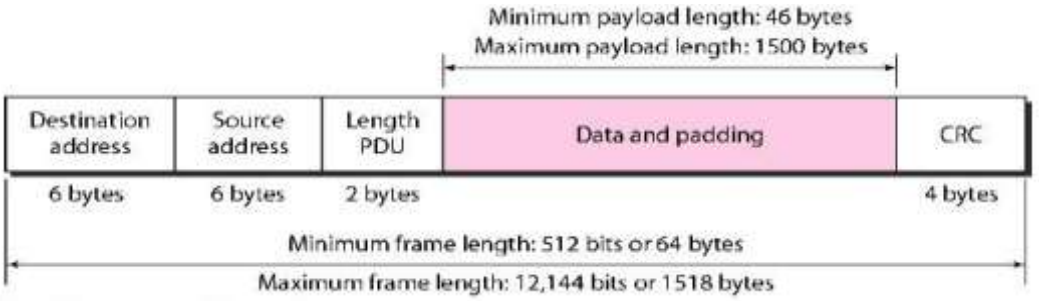
It defines the type field or length field.

Data

This area carries data encapsulated from protocols of the higher layers. 46 bytes minimum and -1500 bytes maximum.

CRC

This field includes knowledge about error detection.

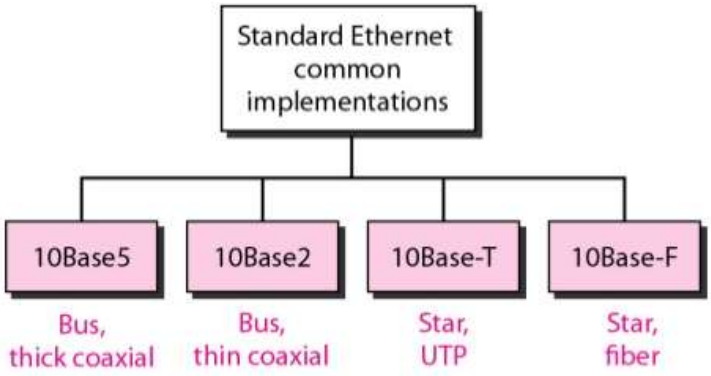


Addressing

Every station holds unique Network Interface Card (NIC) on Ethernet. Inside the station, NIC offers a physical address of about 6-bytes, to station. This is specified by the least significant bit of the first byte. For unicast the bit is 0 and multicast, otherwise. The link between the sender and the receiver, determines the destination address of the unicast that is available with one recipient. A multicast destination address identifies a collection of

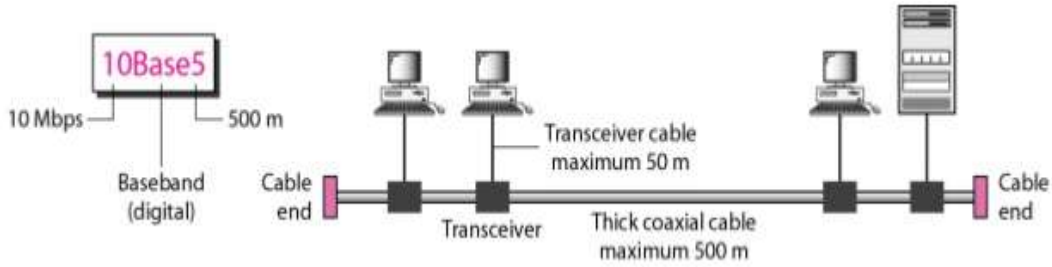
addresses, one to many are the links between the sender and receive. The destination address of the broadcast holds the bits as IS in a special sect of a multicast address.

2.2.2. Physical Layer



10 Base 5: Thick Ethernet

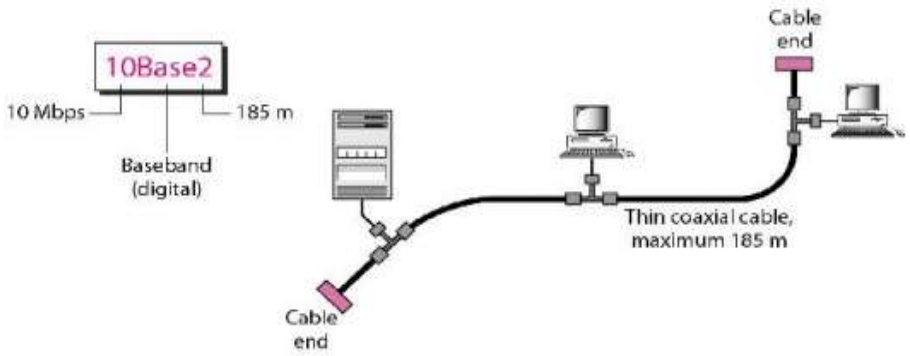
This is a thicknet → This name is formulated by referring to the size of the cable. Ethernet specification uses bus topology with transceiver connected to a cable with thick coaxial, through a tap.



The responsibilities of transceiver are transmitting, receiving and also collision detection. It is associated to the cable that provides path to send and receive data through coaxial cables.

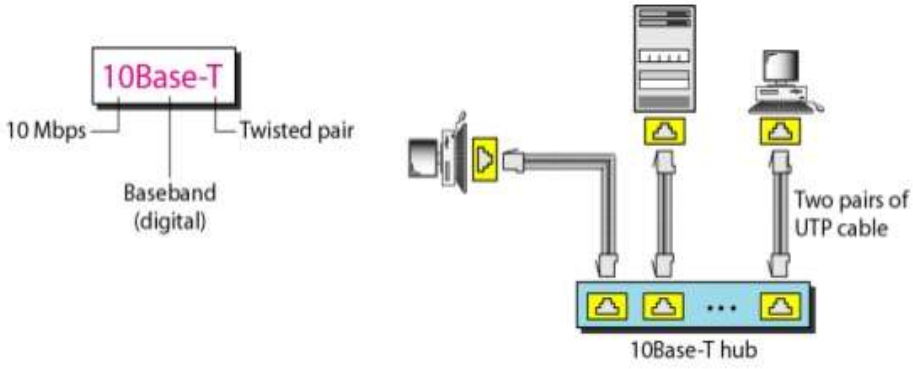
10 Base 2: Thin Ethernet

10 base 2, thin ethernet, cheaper net → It is connected through bus with thinner and supple cable. The cable will have the ability to bend to pass though the stations very close by. The transceiver is considered as a part of NIC installed in station. It is highly cost effective when compared to other 10 base.



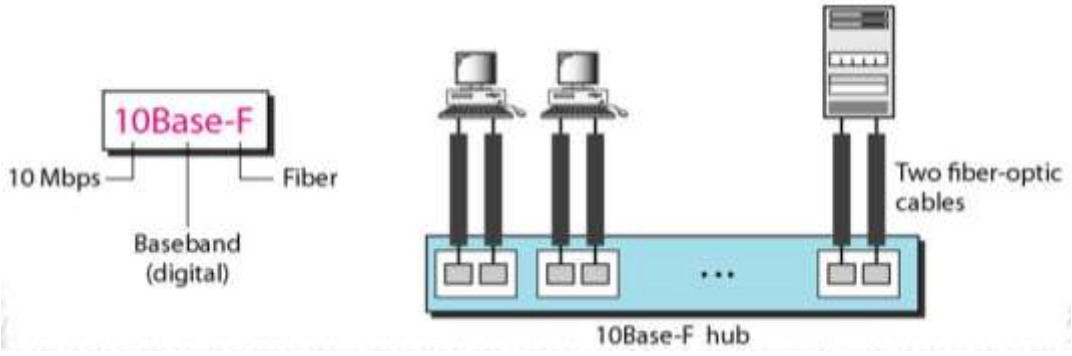
10 Base T: Twisted Pair Ethernet

Mostly through two pairs of twisted cables, these stations are linked to a hub. One path for sending and one path between the station and the centre for receiving. So if a collision is involved, the hub replaces the coaxial cable. The actual length of the pair being twisted is 100 M.



10 base F: Fiber Ethernet

For connecting stations to a hub, 10 base F uses a star topology. Using two fibre optic cables, the stations are connected to the hub.



2. Fast Ethernet

Fast ethernet was intended for LAN protocol through fiber channel. IEEE fast ethernet is named as 802.30. It works at 100mbps rate which is 10 times faster.

Goals of Fast Ethernet

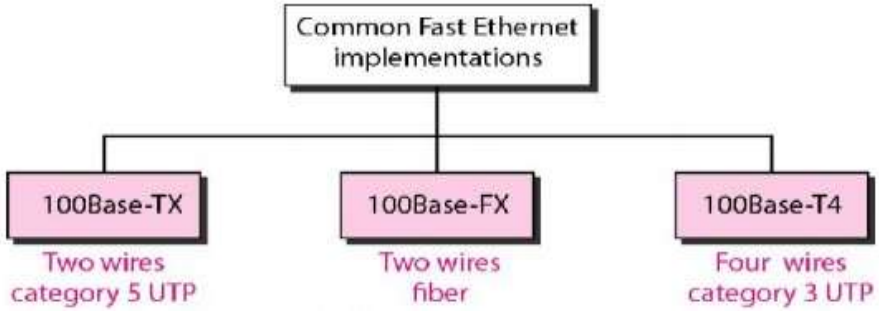
1. Elevation of information rate shoot up to 100 MBPS.
2. Making consistency with the ethernet standard.
3. Maintain a constant 48 bits of address.
4. Maintain a constant format for frame.
5. Maintain the constant length of the frame.

2.2.3. MAC Sublayer

Evolution of ethernet from 10 Mbps**.** Star topology is used to establish the connectivity by full duplex and half duplex. In full duplex, stations are connected via hub and in half duplex, the connections is made via a switch with buffer at each port.

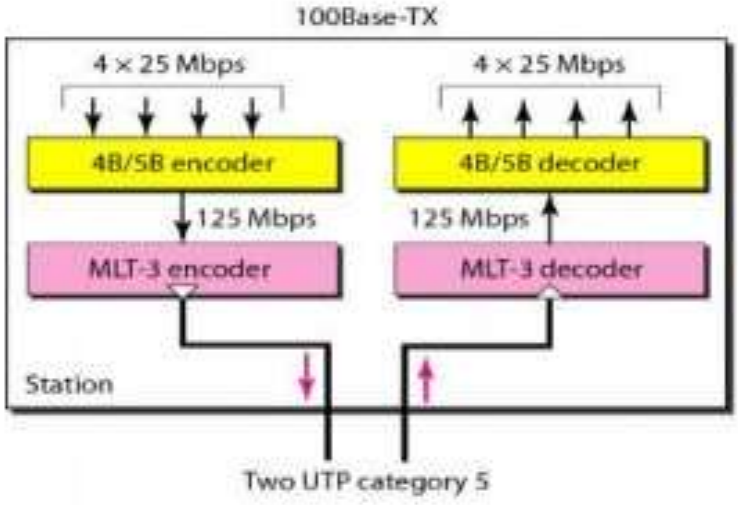
Uses of Fast Ethernet

- To allow incompatible devices to get connected with each other.
- To activate the multiple capabilities of one system.
- Allowing a station to verify the capabilities of a centre.



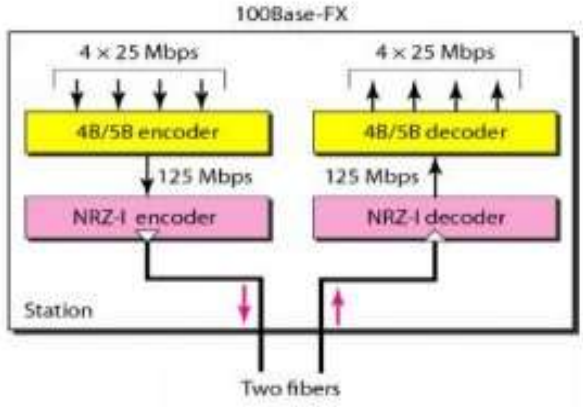
100 base -TX

- Two pairs of twisted-pair cables are used.
- Data rate 125Mbps.
- MLT3 scheme is used for good bandwidth.
- Block coding 4B15B is for bit synchronisation by preventing a long series of OS and LS from occurring.



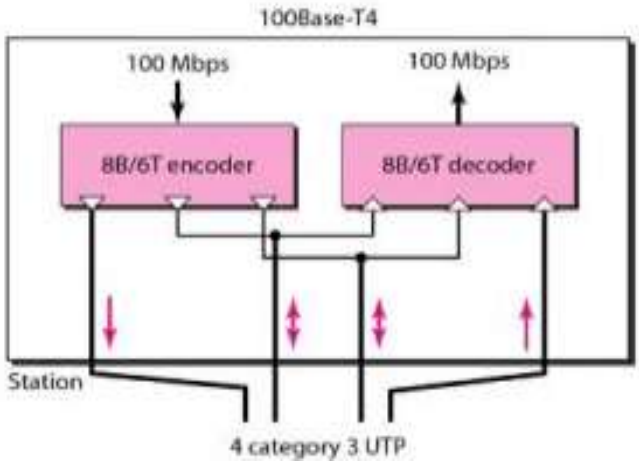
100 Base-FX

- It uses two fibre optic cables in pairs.
- By using simple encoding schemes, it can easily handle high bandwidth efficiently.
- NRZ-1 encoding scheme is used for bit synchronisation issue for long sequences of OS 100 to 125Mbps.



100 Base-T4

- It utilises UTP category 3 or higher.
- It uses 4 UTP pairs to relay 100Mbps.
- Each twisted pair cannot manage more than 25 M band easily.
- One pair switch between sending and receiving. It handles 75Mband (25Mband each).
- In 8B/6T, six-signal elements are obtained as a result of eight data elements.



3. Gigabit Ethernet

Gigabit Ethernet protocol has higher data rate of 1000Mbps. It is also known as standard 802.3z.

Goals of Gigabit Ethernet

- Upgrade the speed of data to 1Gbps.
- It must be made as a standard one or compatible for Fast Ethernet.
- The same address of 48-bits and similar format is used for frames.
- The frame lengths are maintained the same for all sizes.
- Promoting auto-negation to be described in Fast Ethernet.

MAC Sublayer

Gigabit Ethernet has two approaches as given below:

a. Half-duplex
b. Full-duplex

a) Full-Duplex

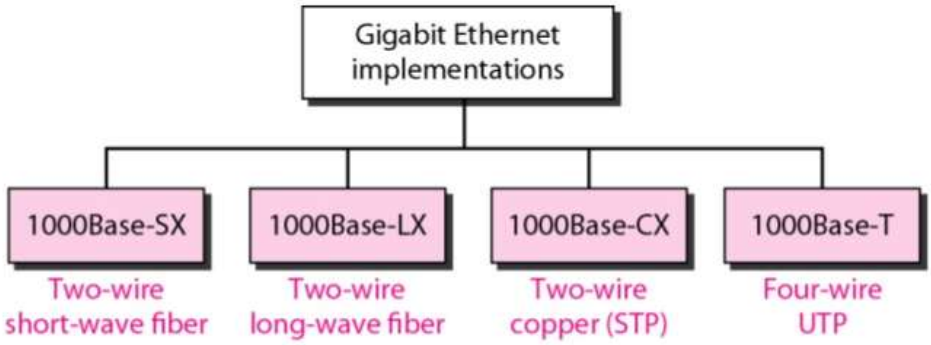
- There is no collision in the full-duplex Gigabit Ethernet mode; the attenuation of signal identifies the overall cable length.
- Each switch connected with buffers to store data until they are transmitted.

b) Half Duplex

- A switch may be alternated with a hub which serves as a common cable if there is a collision.
- It uses CSMA/CD, which depends on minimum frame size.

- Traditional - 512 bits
- Carrier extension - 4096 bits
- Frame bursting-multiple frames sent with frame padding

Gigabit Ethernet Implementation



4. Ten - Gigabit Ethernet

- 10 gigabit ethernet is also mentioned as standard 802.3 AE.
- The motive behind 10 Gigabit are given as follows.
  - Elevation of data speed to 10Gbps.
  - Assuring compatibility over standard, fast and gigabit Ethernet.
  - Using determined and relevant address with 48 bits.
  - Maintain the size of frame lengths.
  - Enable existing LANs to be interconnected to Metropolitan Area or Wide Area Network.
  - Frame relay & ATM.

2.3. Wireless LAN

2.3.1. IEEE 802.11 - WIFI

IEEE 802.11, a wireless LAN was designed by IEEE that conceals physical layer and data link layer.

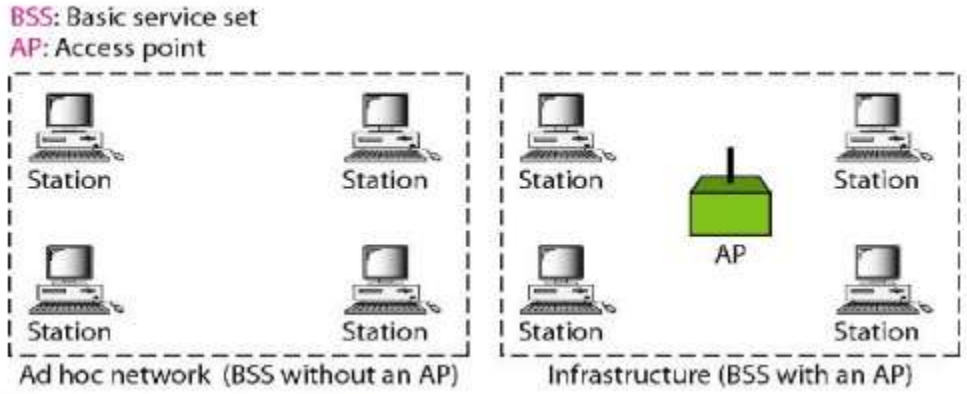
2.3.2. Architecture

The services are given below,

1. The Basic Service Set (BSS)
2. The Extended Service Set (ESS)

1. Basic Service Set (BSS)

A wireless LAN is the basic service set (BSS), made of stationary or mobile wireless stations and an optional central base station known as Access point (AP). It is a standalone network without an AP and does not transmit data to another BSS. It is referred to as ADHOC architecture. On the other hand, BSS with AP is deemed as infrastructure network.

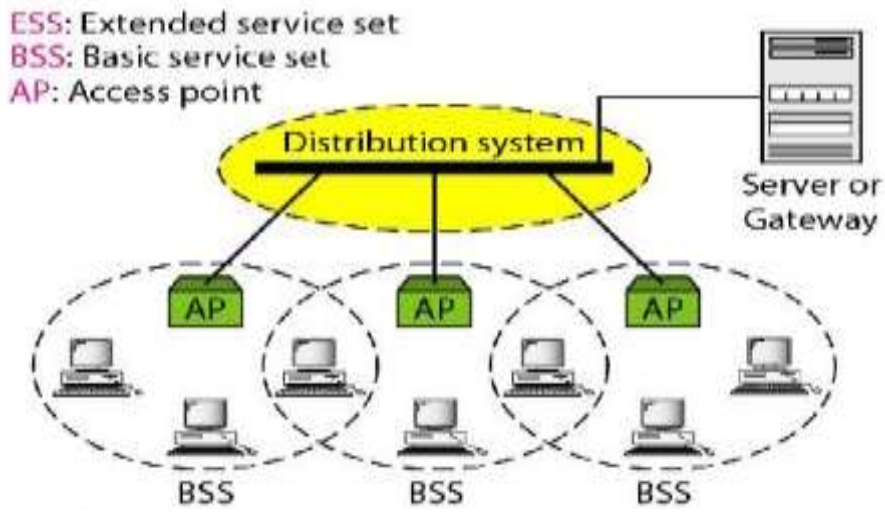


2. Extended Service Set (ESS)

Two or more BSS with AP forms an extended service set (ESS). BSS is connected over a distributed structure by wired LAN. Distributed system connects AP in the BSS.

There are two types of stations.

- Mobile-normal stations inside BSS.
- Stationary-AP stations using a LAN with wired connectivity.



Station Types

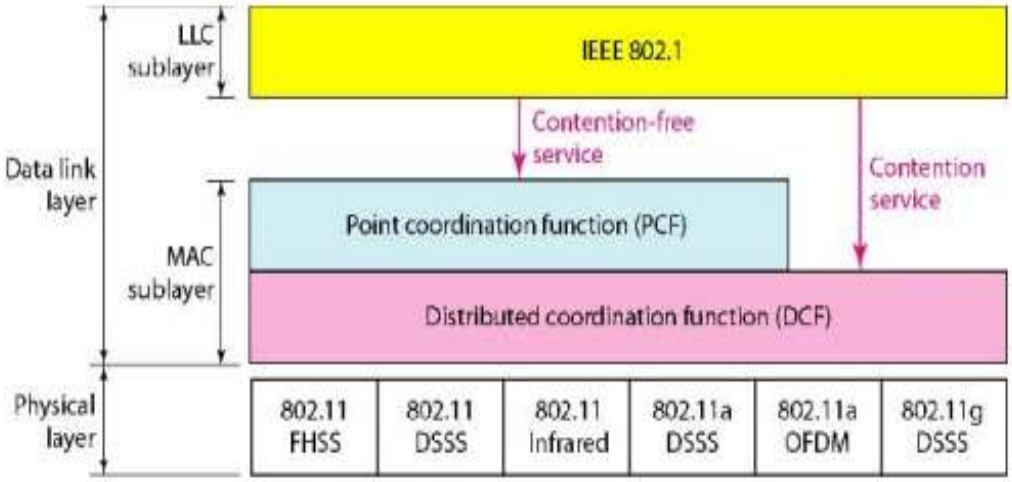
Three different stations depending upon their mobility in a wireless LAN are with no-transition, BSS-transition and ESS-transition in IEEE 802.11.

Location which has no – transmission movement is a stationary one or BSS that moves. BSS transfer mobility may make a station to switch between different BSS, while the communication is designed within a BSS. From one ESS to another, a station with ESS transfer mobility may switch from one another.

2.3.3. MAC Sublayer

IEEE 802.11 Expresses 2 MAC Sublayers

- **DCF**- Distributed Coordination Function
- **PCF**- Point Coordination Function



Distribution Coordination Function (DCF)

Access method used by **DCF** is CSMA/CA. **Wireless LAN** will not be possible to device CSMA/CD because of few points.

1. While detecting a collision, a station should send data and receive alert related to collision concurrently. Here it means expensive stations possess higher specifications of bandwidth.
2. The identification of collision will not be acknowledged due to the hidden station issue.
3. Great signal fading may be the distance between stations, which may prevent a station from hearing a collision at one end and at the other end.

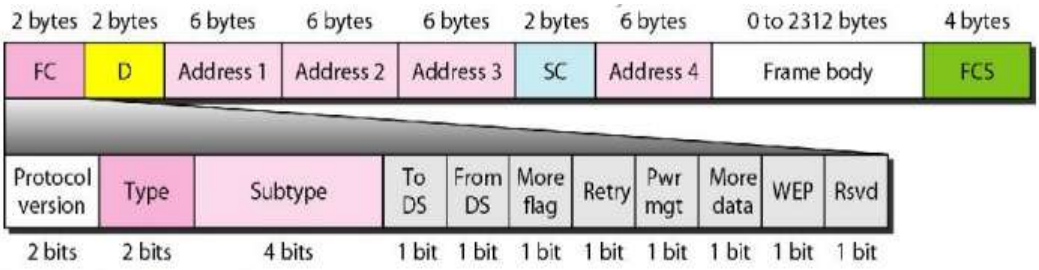
When a station sends an RTS frame it includes the duration of time that it needs to occupy the channel. The Network Allocation Vector (NAV) resembles a timer, that is produced on the nodes which impacts the transmission indicating how much time it takes. Two or more stations can attempt to simultaneously submit RTS frames. These control frames can collide. The non-reception of CTS frame from the receiver, states the sender that there has been a collision. The back off technique is used and the sender resends.

Point Coordination Function (PCF)

PCF is an optional form of connectivity that can be introduced in a network of infrastructures. It is a centralised method of contention-free polling access. The AP performs polling for stations that are capable of being polled. The stations are polled one after another, **sending** whatever data they have to the AP. The Point Controller (PC) will be able to transmit data to poll frame, send acknowledgement, receive acknowledgement, further use one of the combinations called as piggybacking.

2.3.4. Frame Format

The MAC layer comprises fields of nine, namely:



Frame control (FC) - The FC field has a length of 2 bytes and specifies the frame's type and some other additional information related to control.

D - This field defines the duration of transmission that is used to set the value of NAV

Address - They are four in number with each containing 6 bytes of length, Address fields depend on the value to DS and from DS subfield.

Sequence control (SC) - Number of the Sequence of frames are defined that is necessary for flow control.

Frame body - It ranges from 0 to 2312 bytes which holds data depending on the type and subtype specified.

FCS - It measures a length of 4 bytes and comprises of CRC-32 error detection sequence.

Sub Fields in FC Field

Version	current version 0
Type	management (00), control (00), and data (10)
Subtype	1011- request to Send (RTS)
	1100- Clear to Send (CTS)
	1101- Acknowledgement (ACK)
To DS	to Distributed System
From DS	from Distributed System
More flag	1 with more number of fragments
Retry	1 which retransmits data frame
Pwr mgt	1 when mode is on for power management
More data	1 when power to send data
WEP	wired equivalent privacy
RSRD	reserved

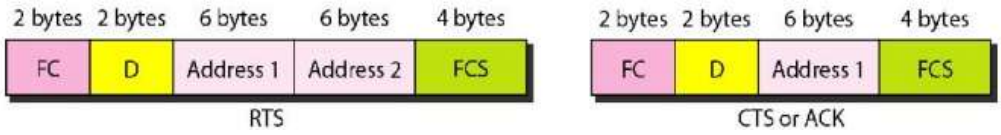
Frame Types

The frames are segregated as management frames, control frames and data frames

Management frames - Send early message with station and that of the access point.

Control frames - Responsibly acts towards retrieving the channel and recognizing it.

Data frames - Carries data and control information.



2.3.5. Physical Layer

IEEE 802.11 FHSS - IEEE 802.11 Frequency Hopping Spread Spectrum uses 2.4 GHZ ISM band. The band is divided in 79 sub bands of I MHZ.

IEEE 802.11 Infrared - It is also referred as Pulse Position Modulation (PPM) and uses Infrared light that ranges between 800 and 900 nm.

IEEE 802.11 DSSS - IEEE 80.11 Direct Sequence Spread Spectrum uses 2.4 GHZ ISM band.

IEEE 802.11 OFDM - IEEE 802.11a Orthogonal Frequency Division Multiplexing method for signal generation in 5 GHZ ISM band. This band is divided into 52 sub bands, where 48 sub bands for sending 48 groups of bits at a time and 4 sub bands for control information.

IEEE 802.11 DSSS - This describes the Direct Sequence method that is of higher rata and the signal is generated in 2.4GHZ ISM band.

IEEE 802.11g - It gives forward error correction and OFDM using the 2.4 GHZ ISM band. It is backward compatible with 802.11b.

2.4. Bluetooth

Bluetooth is a kind of wireless LAN technology that is designed for connecting various devices with different functionalities such as telephone, computers, cameras, printers, and so on. Bluetooth LAN (IEEE 802.15) is an ad hoc network, where the devices are connected impulsively referred as gadgets. Bluetooth was initiated by Ericsson Company. This is more suited for small area and defined as a wireless Personal Area Network (PAN).

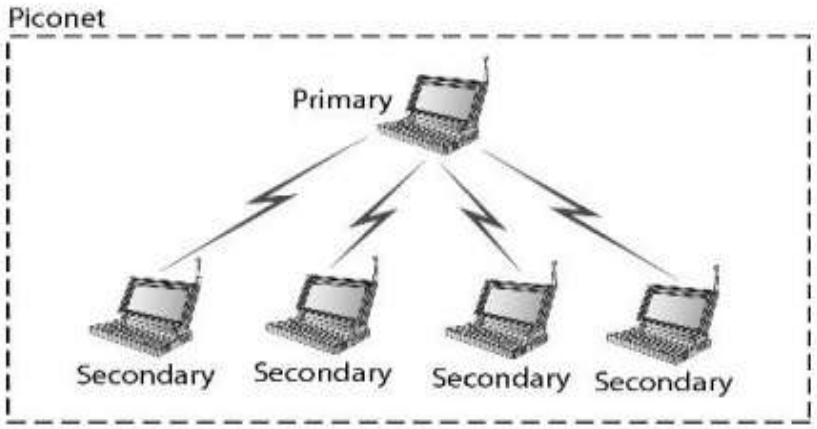
2.4.1. Architecture

Bluetooth defines two types of network.

- piconet
- scatternet

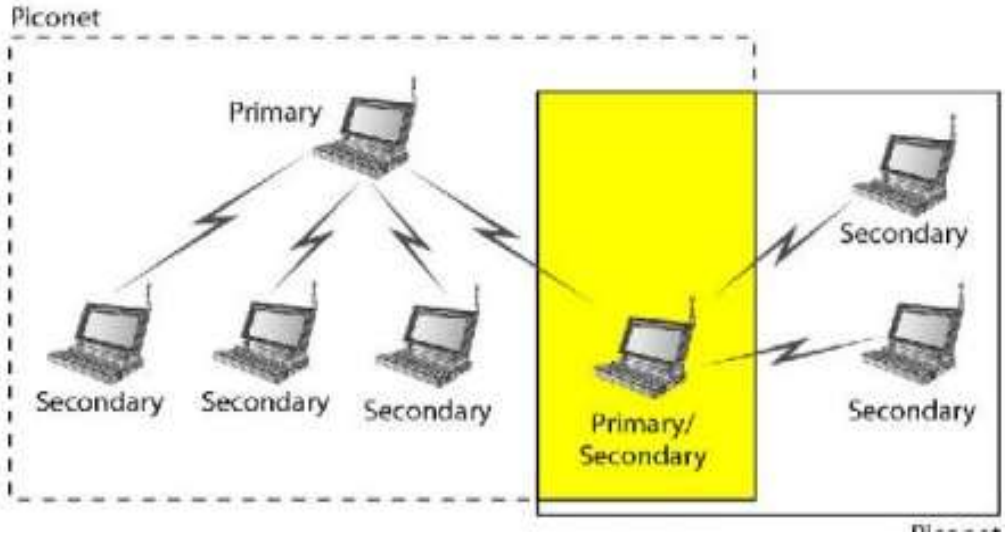
Piconet

A Bluetooth is network that can be called as a piconet or otherwise called as a small net. A piconet can have up to 8 primary stations and rest as secondary stations. All the secondary stations synchronise with the primary with their clocks and hopping sequence. A piconet may have only one primary station. One to one or one to many may be the contact between the main and secondary. A piconet has a maximum of 7 secondaries and 8th can be a parked state. A secondary is synchronised with the primary in a parked state.



Scatternet

Piconets are fused to create what is referred to as a scatternet. A secondary station in one piconet may be the main in another piconet. This station can receive messages from the main in the first piconet (secondary) and functions as a main, delivers them to secondary in the second piconet. Any station might take part in 2 piconets.



A built-in short-range radio transmitter is found in a Bluetooth system with 2.4 GHz bandwidth. It is the interface between IEEE 802.11b wireless LAN and Bluetooth LAN.

2.4.2. Bluetooth Layers

2.4.2.1. Radio Layer

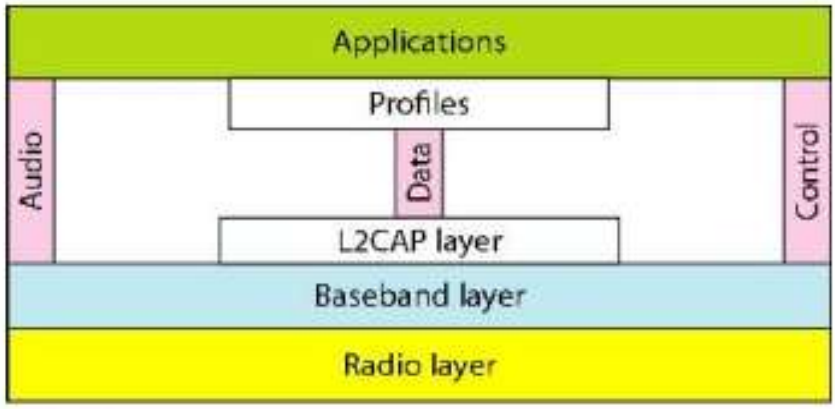
It is equivalent to the physical layer in internet model**.** A low power devices are Bluetooth with a range of 10m.

Band

The 2.4 GHz ISM band used by Bluetooth is segregated into 1 MHz each that contributes 79 channels.

Modulation

Sophisticated version of FSK called GFSK (Gaussian bandwidth filtering)**,** GFSK is a carrier frequency where bit 1 represents frequency over the carrier and bit 0 represents frequency below the carrier is used in Bluetooth.



FHSS - Frequency Hopping Spread Spectrum.

This methodology is used by physical layer that avoids interferences caused by different systems or networks. It is observed that bluetooth can hop upto 1600 times in a second i.e., frequency modulation of the devices can be varied to 1600 times in a second. The frequency of 625 micro seconds (1/1600 s) is utilised.

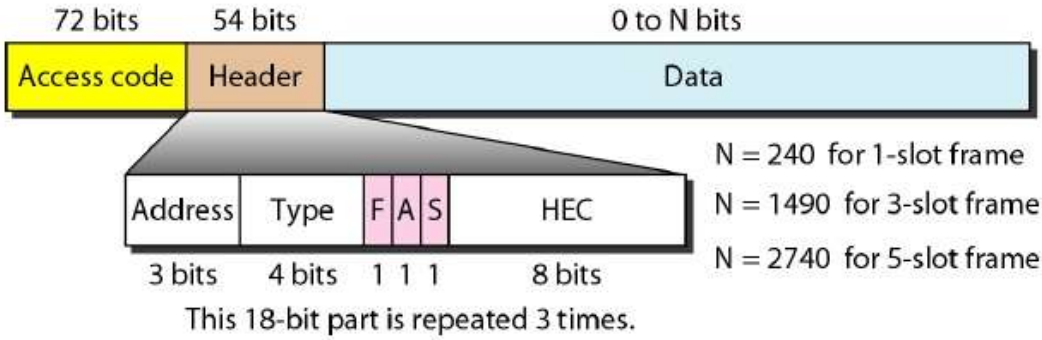
2.4.2.2. Base Band Layer

MAC sublayer in LAN resembles the baseband layer. The different nodes contact each other in the timing duration. The allotted slot is 625 micro seconds. TDMA is used as Time Division Duplex TDMA (TDD-TDMA) by the Bluetooth with half-duplex type of communication i.e., data is sent or received non-synchronously.

Physical Links

There are 2 types of links given as Synchronous Connection-Oriented link (SCO) which evades delay and integrity & Asynchronous Connection-Oriented link (ACL) which overrides latency avoidance by data integrity.

Frame Format



Access code - It consists of 72 bits for synchronization as well as for identifying the primary frame from one piconet to another.

Header - 18-bit pattern is used to repeat the 54 bits field.

Address - 3 bits address define up to 7 secondaries if address is 0 and it is used for broadcast.

Type - Type of data traversing through higher layers where,

F - Flow control

A - Acknowledgement

S - Sequence number

HEC - Header Error Correction

2.4.2.3. L2CAP

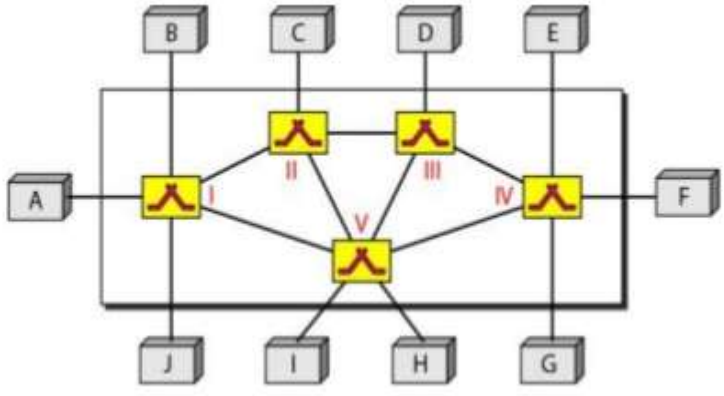
The Logical Link Control and Adaptation Protocol (L2CAP) resembles LLC sublayer. It is used for exchange of data, on an ACL link, while an SCO channel does not use L2CAP. The 16-**bit** length field defines the size of the data from upper layers. The L2CAP performs multiplexing, segmentation, reassembly, Quality Of Service (QOS) and group management.

2.4.2.4. Data Field

This field contains the data or control bits. It can be of length 0 to 2740 bits, which holds either data otherwise control bits traversing from upper layers.

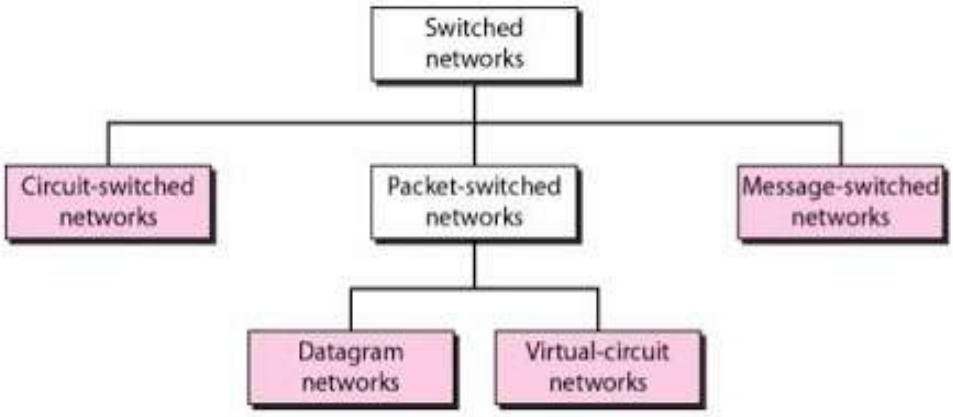
2.5. Switching

This network is made up of nodes named switches. These switches provide an adhoc link with many switch-linked devices. Few of them are linked with the end systems in the switched network.



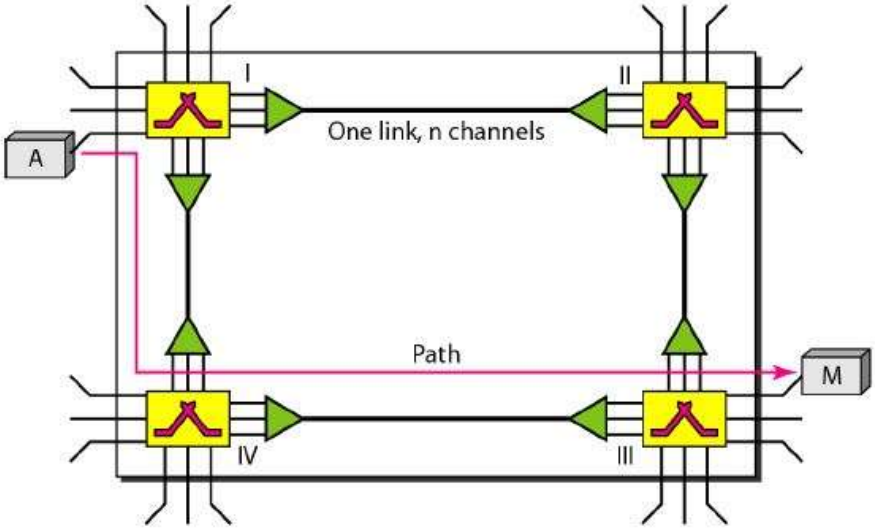
The end systems are A, B, C, D, E, F, G, H, I, J, and switches are 1,2,3,4,5.

2.5.1. Taxonomy of Switched Networks



2.5.1.1. Circuit Switched Networks

Series of continuous switches are linked through physical links in network switched circuit. A link connecting various nodes holds a separate path composed of many connectors. This network holds a constant flow of physical-connected switches where every connection is segregated as h-channels.

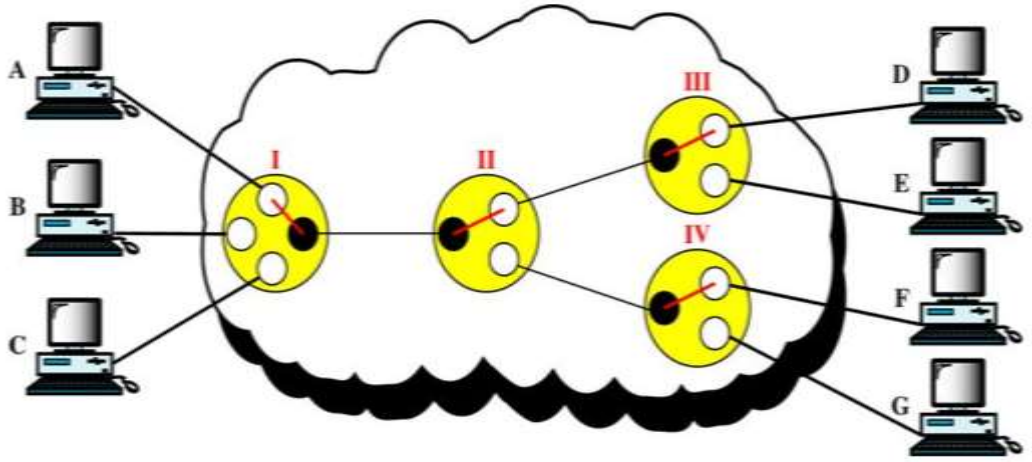


A switch is attached to the final device. In order to get connected with the system x, it is expected to appeal a link with x such as all switches and x agrees. The process is done in the setup phase. On each connection, a circuit (channel) is reserved and the dedicated path is specified by the combination of circuits or channels. At the physical stage, circuit switching

takes place. For the services to be used during the interaction, the station must make a reservation. Resources such as channels, switch buffers, switch processing time, input / output switch ports have to be preserved with confinement until the tear-down step for the overall cycle of message transfer. During data transfer, there is no source and addressing involved.

Three Phases

1. **Setup phase -** A connection between the two end systems are created with the address required for communication.
2. **Data transfer phase -** Two nodes (channels) can transfer data.
3. **Teardown phase -** When one of the parties needs to disconnect a signal is sent to each switch to release the resources.



The telephone network is connection oriented. It involves in the transfer through a network that has a dedicated connectivity and this is termed circuit switching.

Advantages

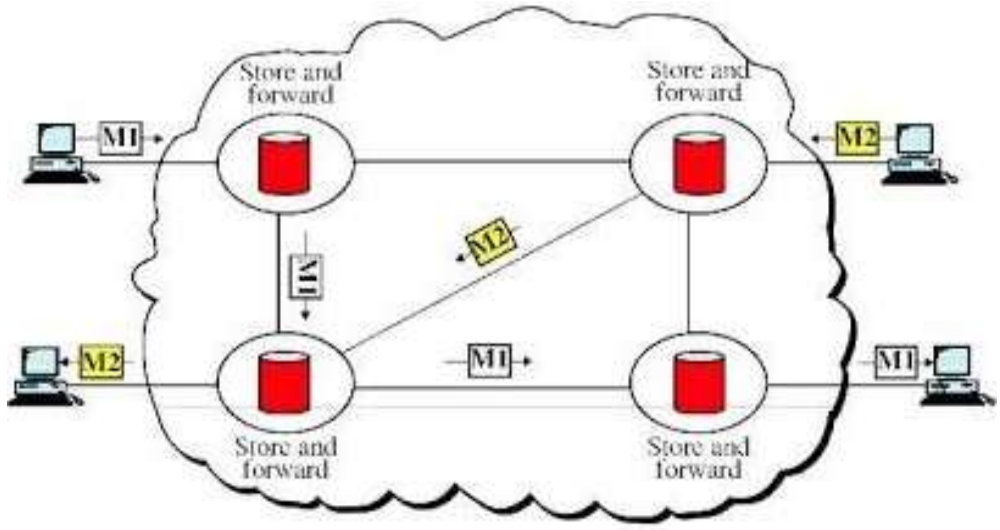
- Dedicated transmission channel establishment provides a guaranteed data rate of transmission.
- Time delay is not found in data flow.

Disadvantages

- Although the channel is idle, it cannot be used to transmit any other data.
- More Bandwidth is demanded by dedicated channels.
- It takes longer time to establish connection.

2.5.1.2. Message Switching (OR) Telegraph Network

Text message is encoded using different code to frame a sequence of data with dashes. The text message is sent from the telegraph office which is the source to the telegraph switching station. An operator takes the decision of routing the message based on the destination address information the operator will either forward the message is a connectivity to the destination is free or store the message till the communication line becomes free. Every message is considered as an independent unit and includes both the source and destination addresses. All complete messages are transmitted from a device to another device through the connectivity.



Each intermediate device receives the message, ensures the readiness of the connecting device and then forwards it to the next one. This is called as a store and forward network. The information is more efficient and other switches that can be used to forward messages to their ultimate destination.

Advantages

- Effective traffic management is offered by prioritizing messages that needs to be switched.
- Network traffic congestion is minimized.
- The network devices share the data channels.
- Asynchronous communication is provided across different time zones.

Disadvantages

- Storing and forwarding introduces delay.
- A large storing capacity is needed for intermediate devices in storing the messages.

2.5.1.3. Packet Switching

The message to be transmitted is fragmented into smaller packets and each packet contains information about the source and destination in a header along with the address details of the intermediate nodes. Each and every packet can take various routes in order to reach the destination. There are 2 advantages.

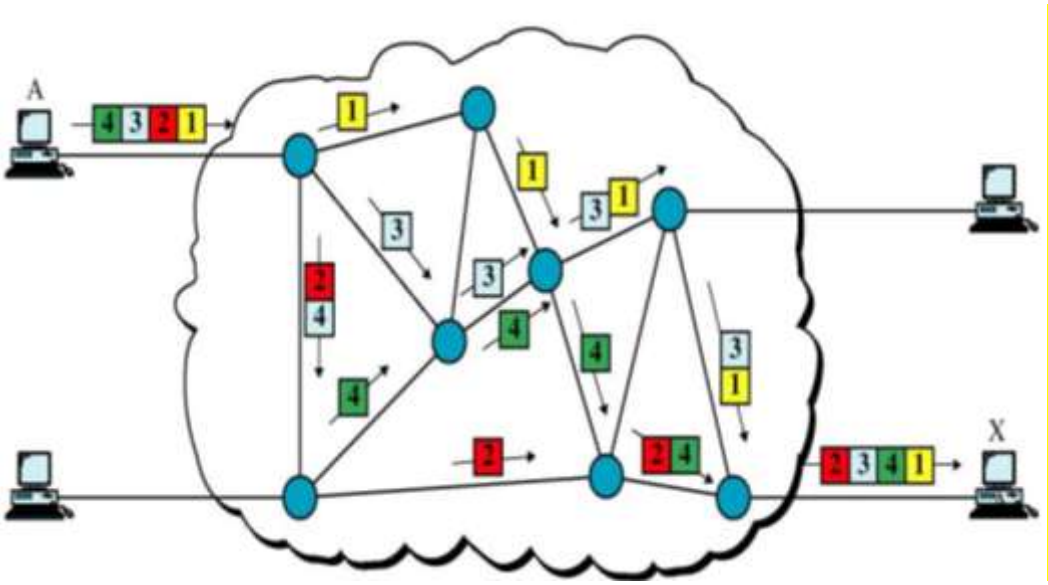
1. Bandwidth is reduced by splitting data into different routes in a busy circuit.
2. If a certain link in the network goes down during the transmission, the remaining packets can send through another route.
    - The packet length is restricted to a maximum length.
    - There are two methods of packet switching.
        - Datagram packet switching.
        - Virtual circuit packet switching.

a) Datagram Packet Switching

A stream of packets is obtained by dividing the message into packets and each packet has its own control instruction and acts an independent unit. Also, each packet is routed independently using the switching devices with individual intermediate node which helps in identifying the next route. Once it is ready for transmission, control information is exchanged in order to establish the packet sequence and destination.

b) Virtual Circuit Packet Switching

Virtual circuit is nothing but establishing a logical connection between the sender and receiver. Based on the agreement of the commination parameter with the receiving device, a communication is established with a conversation initiated by the sending device. The devices use it for the rest of the conversion. All the packet travel through the logical connection established between the sender and receiver.



Advantages

- The bandwidth of the network can be increased in order to communicate with numerous devices via the same network channel.
- A packet can be routed using a switching node based on its requirements.
- Time and transmission delay are reduced.

Disadvantages

- In Packet switching, the size of the RAM is proportional to the quantity of the packets.
- It requires more processing power.

2.5.2. Bridging

Bridge is used to connect two or more detached networks that are connected for exchanging data or resources. It utilizes addressing protocols and can affect the flow control of a single LAN. Bridges are more active at the data link layer. It receives the signal and it can check the physical (MAC) address of source and destination stored in the frame.

Generally 2 types of bridges exist namely,

- Transparent bridge
- Routing bridge

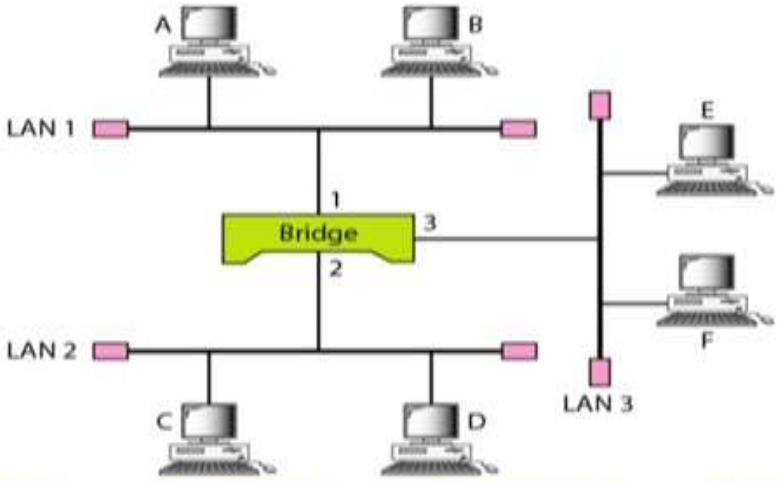
2.5.2.1. Transparent Bridge

In this bridge, the stations are unaware of bridge connectivity. Transparent bridges keep a table of address in memory to regulate the forwarding of data.

The duties of transparent bridge are:

1. Filtering flames
2. Forwarding
3. Blocking

Each packet traces the destination and source addresses. It checks the destination to decide where to send the packet. If it does not recognize the destination address it relays the packet to all of the stations on both segments. When a frame arrives at a bridge, it must choose to **either** discard or forward it and if the latter is true, then decide on which LAN to put the frame.



Address	Port

a. Original

Address	Port
A	1

b. After A sends a frame to D

Address	Port
A	1
E	3

c. After E sends a frame to A

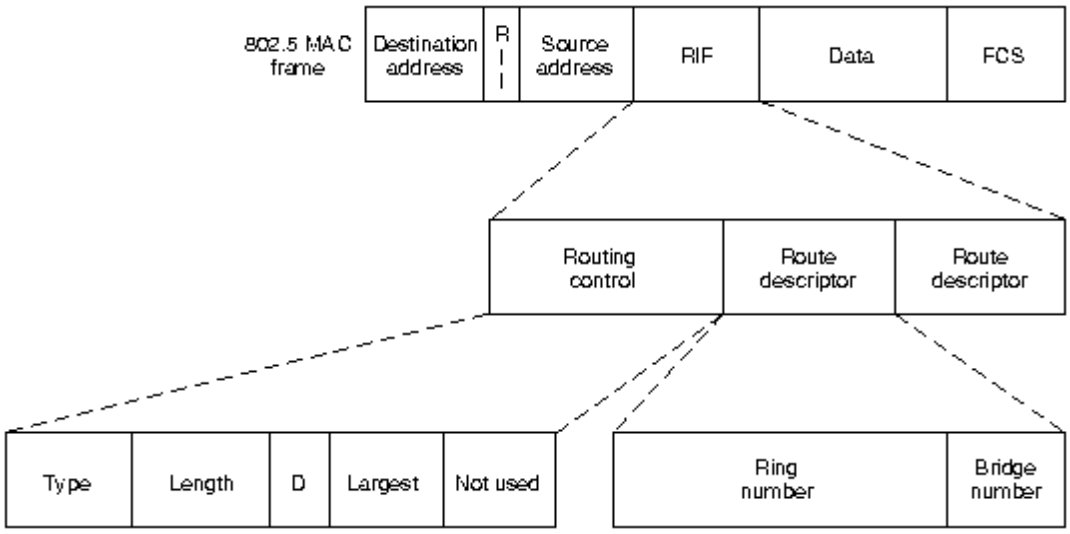
Address	Port
A	1
E	3
B	1

d. After B sends a frame to C

- A sends frame to D:**flooding**
- E sends a frame to A: **Forwarding**
- B sends a frame to C :**flooding**

2.5.2.2. Routing Bridge

The routing bridge is used to interconnect token ring networks. The header holds the route to destined node, during its travel. This information is present only if the communication is between varied LANs.



How to Discover a Route?

- The station who wants to discover a route first broadcasts a special frame.
- The frame visits every LAN exactly once and eventually reaches the destination.
- Next, a special frame named all routes special frame is responded from the destination station which produces all probable routes to the source station.
- Finally, the best route is chosen at the source from the all collected routes and is saved.

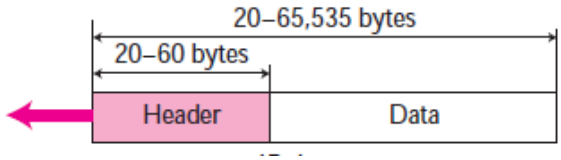
2.6. Basic Internetworking

2.6.1. Internet Protocol (IP)

IP is network layer protocol designed as connectionless delivery between hosts for the internet that guarantees least reliability. This is due to the fact that it supplies no error control or flow control. Also, the error alone will be detected and the corrupted packet will be discarded. Each IP packet is handled independently and it can follow a different route to the destination.

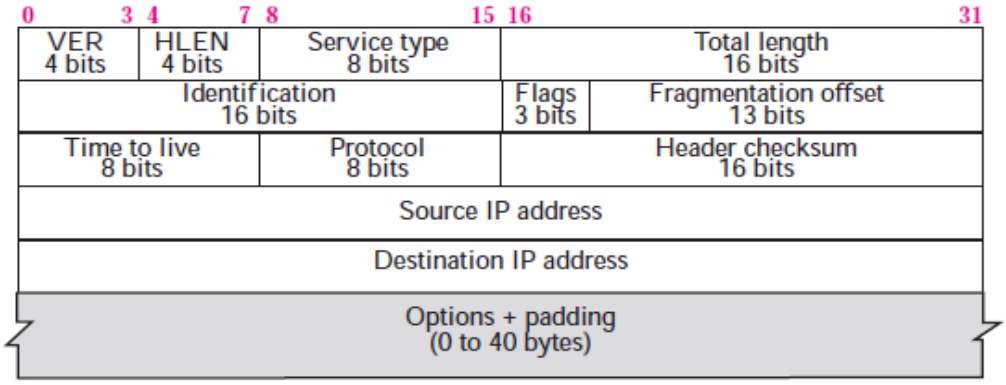
Datagram

- Packets in IP layer is called as datagrams.
- A datagram is a variable length with two parts; header and data.
- The header is 20 to 60 bytes in length it contains details for routing and delivery.
- The field width of the data is not of fixed length.



Structure of IP Frame Header

- The routing details are held at the IP frame header that is linked with diagram delivery.



Various Fields in IP Header

VER (Version)

- IP version is defined.
- IPV4 and IPV6 are the present versions.
- It is four-bit long field.

HLEN (Header Length)

- This field defines a 4-byte word as the length of the datagram header.
- The value is obtained by multiplying the length by 4 in bytes.

Differential Service (DS)

- The quality of service is shown by the class of the packet in this field.
- They accept traffic only above certain precedence at time of high load.
- The trade-off between low delay, high reliability and throughput.

Total Length

- The entire length of IP packet is defined as the complete length.
- The header and data field comprises the actual total length.
- The length of the field is 16 bits which equals 65535 bytes.

Identification; Flag; Offset

(i) Identification

- The identifying the datagram that originates from the source host is held in this field.
- The copier is held in all fragments, with its identification.
- The identification member helps destination in reassembling fragments of datagram.

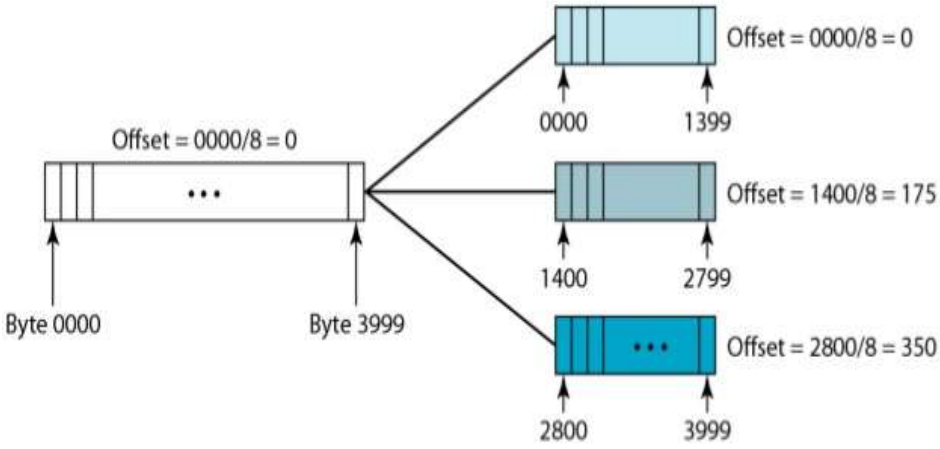
(ii) Flag

- The field has 3-bits.

- (0) is reserved at the first bit, whereas the second bit is referred by Do not fragment bit and finally, the third bit is called to be more fragment bit.

(iii) Fragmentation Offset

- A 13-bit field that indicates relative position of the fragmentation in the full datagram.
- An 8 bytes of offset is left in the datagram.
- 4000 bytes are held by IP packets ranging from 0 to 3999.
- It is segregated into 3.



Time to live

- The field has a length of eight bits and also holds a control over most of the routers which the datagram has made a visit.

Protocol

- Higher level protocol is defined by this field that uses various services provided by the IP layer.
- A protocol of higher level which summarizes data in IP datagram is done by TCP.

Header Checksum

- For an IP packet, the header alone is covered in this checksum.
- At each point, the field will be recomputed and verified, when the fields at the header attempts a change.

Source and Destination Address

- These are used in defining the IP addresses of source and destination fields.

Options

- They are used for network testing and debugging IP that provides several options of allowing a packets sender of requisites over the path which is followed on a network, identifies the route taken by packets which further label them with preserving attributes of secure transmission.

Services Provided

The following services are offered by IP:

a) Addressing

The header of IP comprehends 32-bit addresses to recognize the hosts of the sender and receiver. Intermediate routers employ the usage of these addresses in order to choose the path for a packet via a network.

b) Fragmentation

It splits larger packets into smaller fragments that helps networks that can handle only the smaller packets. These fragments are transparent as well.

c) Packet Timeout

Time to live (TTL) field is found in all IP packet that gets decremented whenever a router handles a packet and is discarded, when reaches zero.

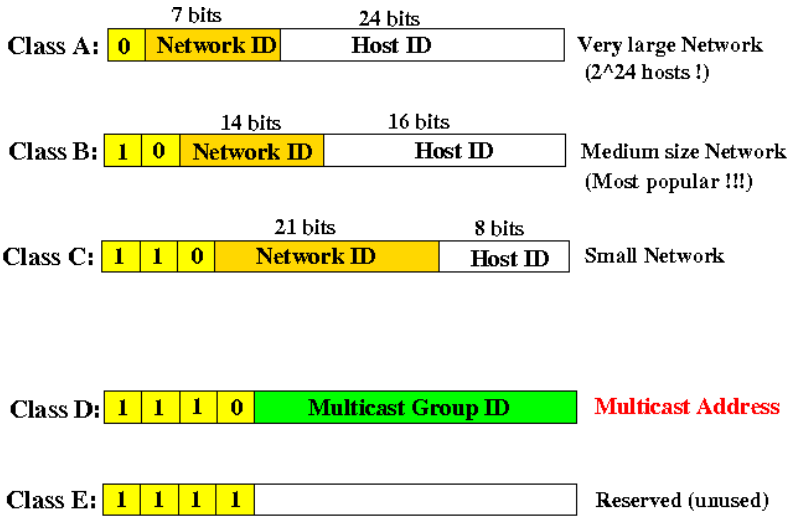
d) Types of Services

IP supports traffic **prioritization** by allowing packets to be labelled with an abstract type service.

IP Addresses

- The IP address for hosts is assigned by the network administrator.
- An IP address consist of two part.

1. **Address, called as network number which identifies a network.**
2. **Host ID, refers to each host of the network.**

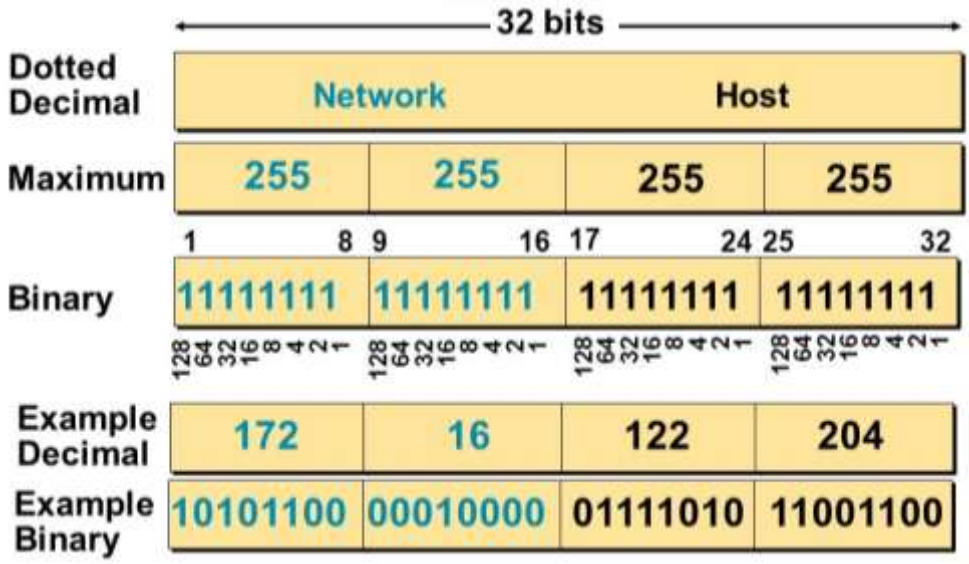


Network Address

- This address helps in defining the network and is not possible to be allotted to a host.

Class	Address range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or research and development purposes.

IP Address (Decimal and Binary Form)



Subnetting

Identical network number is provided to every hosts present in a network. IP addressing can be problematic as the network size increases. Subnetting allows an additional level of hierarchy in IP addressing. Network is split into several smaller networks internally but it acts like a single network. The smaller parts of a networks are called as subnets.

Subnet Mark

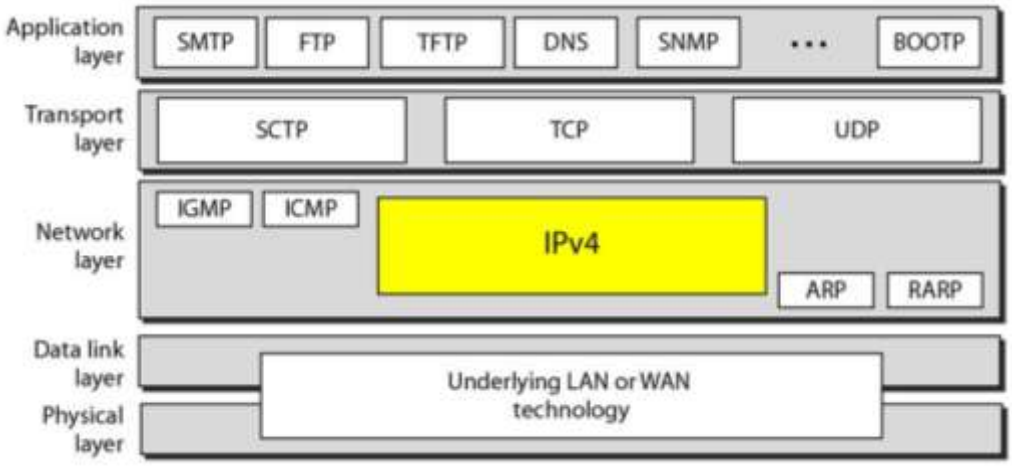
The number of 1s in the subnet mask is more than the number of 1s in the corresponding default mask. Leftmost 0s are default mask to make a subnet mask.

Super Netting

The addresses of class A and B are most depleted but class C addresses are marked until available. The prerequisite of the organisation is left unsatisfied by the C address as its size maximizes to 256 only. Therefore, it requires more addresses which is attained by combining several networks to form a super network.

2.6.1.1. IPV4

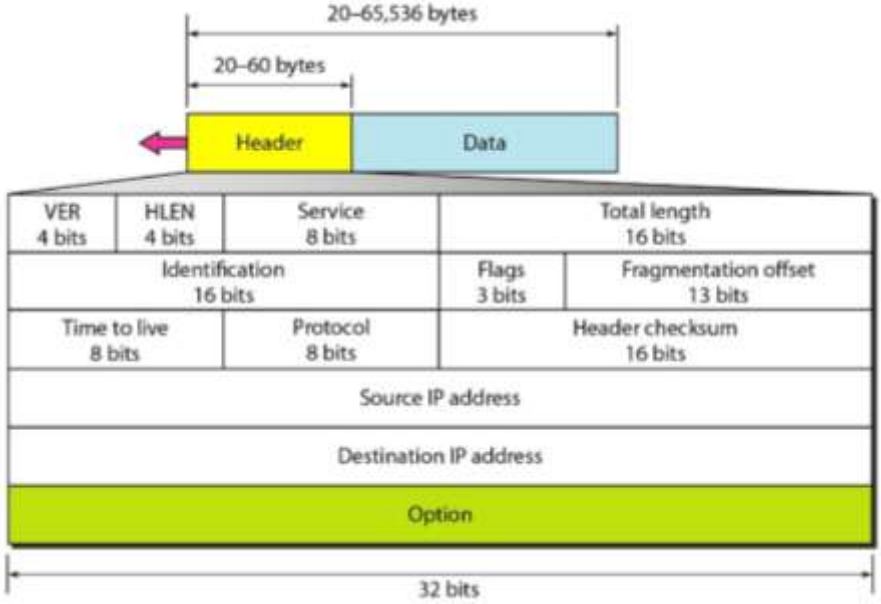
TCP/IP protocols uses internet protocol version 4 (IPV4) as the procedure to perform delivery of packets.



IPV4 is considered to be a datagram protocol which is unreliable and connectionless. It is a best effort delivery service. Best effort means IPV4 provides no error control or flow control. This protocol that utilizes packet switching technology follows the datagram approach. Each datagram is routed independently and different routes to the destination are followed through the network.

Datagram

- In IPV4 layer, a datagram is referred as the packets.
- Each datagram is of variable size and consist two parts, namely, the header and data. Each header is about 20 to 60 bytes long.



VER (Version)

The version of 4 is held in 4-bit field which states the version of the IP*4 protocol.

Header Length (HLEN)

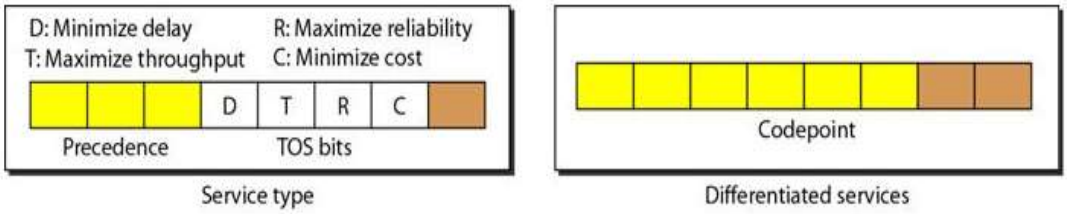
This 4-bit field defines the total length of the datagram header in 4-byte words.

Services

Service type is 8-bit field that offers differentiated services.

(a) Service Type

Precedence bits are the first three as shown in the figure and type of service (TOS) bits occupy the next 4 bits.



D **-** Minimize delay

T **-** Maximize throughput

R **-** Maximize reliability

C **-** Minimize cost

Precedence - The precedence gives a priority to the datagram during congestion, which is a 3-bit field.

TOS bits - It is a 4-bit field with each bit having a special meaning.

(b) Differentiated Services

The first 6 bits make up the code point subfield and last 2 bits are not used.

Total Length

This is a 16-bit field that defines the total length of the IPV4 datagram in bytes. Length of data = total length-header length.

Identification

This field is used in fragmentation.

Flags

This field is used in fragmentation offset and it has offset value. As a datagram travels across various networks, each network route decapsulates the frame it receives, processes the frame and then encapsulates it with another frame. The format and size of each frame is dependent on the protocols of the physical network.

Time to Live

The travel lifetime is limited for a datagram via internet. This field is designated for timestamp and gets decremented once a route is visited. Also, a datagram can travel without being delivered at its host for a relatively longer time. Therefore, this field helps in limiting the lifetime of a datagram as well as in limiting the journey of the **packet**.

Protocol

The functionalities of the IPv4 layer is given by a higher-level protocol and uses 8-bit field**.** It encapsulates data from different protocols of higher-levels namely TCP, UDP, ICMP, IGMP. It notifies the final destination protocol to which the IPV4 datagram is delivered.

Checksum

The concept of checksum and its calculations were checked for error detection.

Source Address

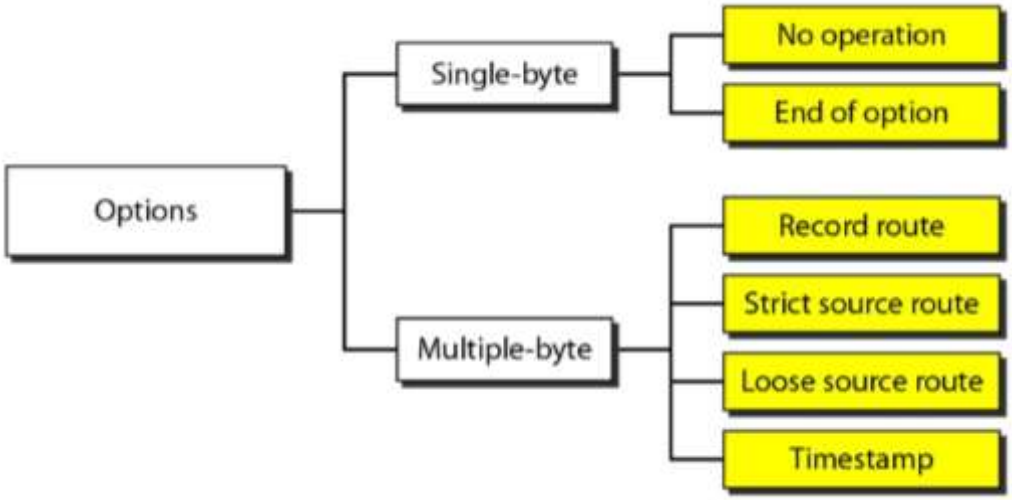
It is a field for the source that is used to define the address of IPV4 and contains 32 bits. It is expected to be the same without any chances to the datagram during the source to destination travel of the host.

Destination Address

The destination address of the IPV4 is defined by 32 bits and is expected to be the same without modifications.

Options

A fixed and a variable part is found at the IPv4 datagram's header, with 20 and 40 bytes of length respectively and utilized for the process of testing and debugging in a network.



No Operation

It is just a single-byte operation which is often utilized for filtering options.

End of Option

This is also a single-byte option utilized especially at the end of the option for padding.

Strict Source Route

In order to opt for a specific service, for e.g., the service can be a minimum delay or some other services like maximum throughput, the sender has got a privilege in selecting a route. This is offered by strict source route option that enables a predetermined datagram route that travels via internet.

Loose Source Route

Even though loose source route appears to be similar to the strict source route, nevertheless it's rigidity is less. Various routers can be visited by the datagram.

Timestamp

This option is utilized when datagram's time processed by routes needs to be recorded. The routing time of a datagram is given here.

2.6.2. Address Resolution Protocol (ARP)

The internet comprises of numerous networks and routers. In general, a packet visits various physical networks while beginning from the source host, reaching the destination host. At the network level, the addresses are used in recognising the hosts and routers.

1. IP Address

An IP address is a unique internetwork address and every protocol requires IP address for internetworking.

2. MAC Addresses

As discussed above, packets pass via physical network and at the physical level, the IP addresses alone are not sufficient but MAC addresses are required to recognize the hosts and routes. A MAC address is a unique local address and it is also passed through different physical network. The IP and MAC addresses are two different identifies and both are required to be available at the same time in the network layer. To deliver a packet to a host or a route, bi-level addressing is required as IP addressing and MAC addressing.

Mapping can be done by using static mapping or dynamic mapping.

1. Static Mapping

A table is maintained to associate IP address with MAC address. Whenever a machine wants to communicate with another machine knowing its IP address, then the MAC address can be found in the table. The table of the static mapping has to be updated periodically. The Address Resolution Protocol (ARP) associates an IP address with the physical address. On a typical physical network LAN, each device on a link is identified by a physical or station address usually imprinted on the Network Interface Card (NIC).

2. Dynamic Mapping

A protocol is set to discover the address of the other machine, given a known address in dynamic mapping. The performance of dynamic mapping is defined by the following two protocols,

- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)

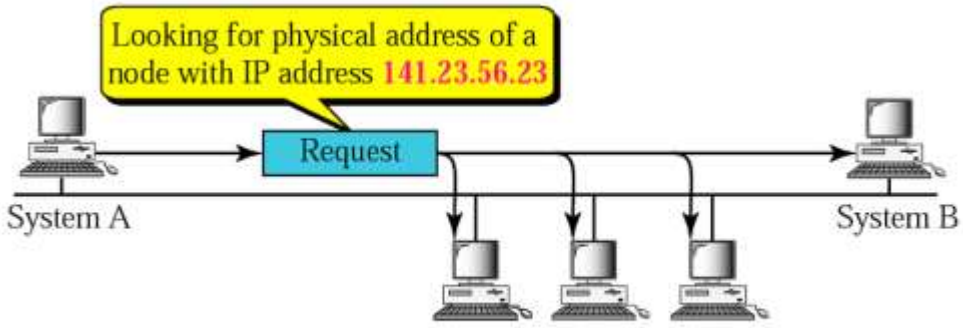
ARP Operation

The association of an IP address and the appropriate MAC address is done by ARP. Every LAN has its own physical or station address as its identification which is imprinted on the NIC.

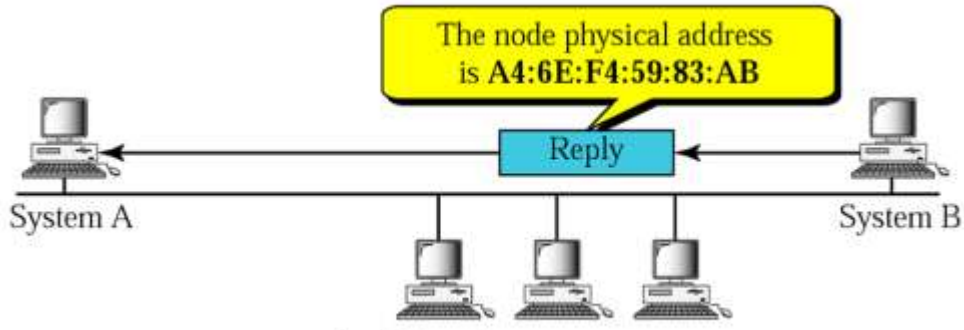
How to Find the MAC Address?

The discovery of MAC addresses of other hosts or network requires the following steps.

- An ARP request packet is sent when the router or host requests to discover the MAC address of another router.
- This packet includes both IP along with MAC address of transitter and the IP address of receiver.
- Although all router and host throughout the network receives and processes the ARP request packet, only specific receiver (B) recognizes its IP address in the request packet and reverts an ARP response packet containing IP and physical addresses of the receiver (B).
- This packet is delivered only to A (unicast) using A's physical address in the ARP request packet.



a. ARP request is broadcast

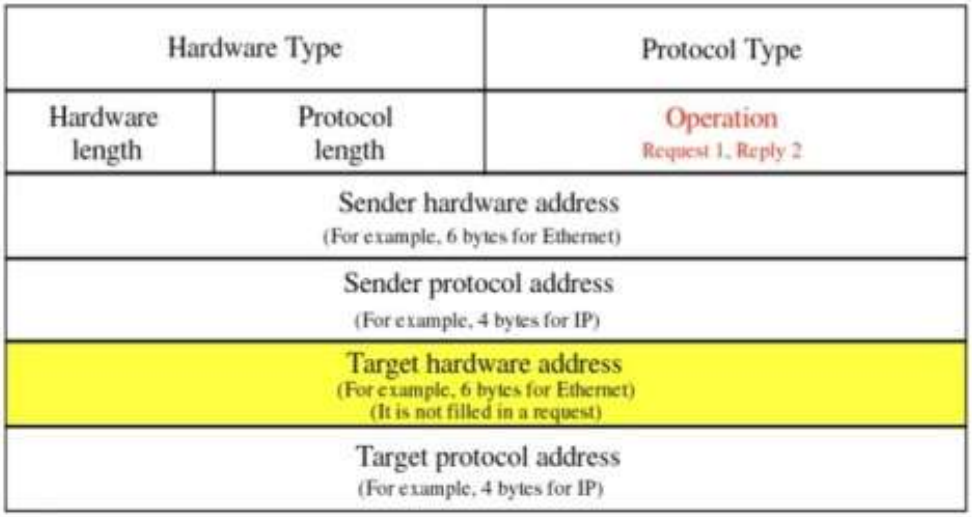


b. ARP reply is unicast

ARP Packet Format

The format of ARP packet that includes a variety of fields that are listed below:

- Having been aware of the internet address of any node, ARP can find the physical address.



1. Hardware Type (HTYPE)

ARP has the potential to run on any physical network and is given by a 16-bit field.

2. Protocol Type (PTYPE)

This is also a 16-bit field that can be used along with higher-level protocols namely IPV4.

3. Hardware Length (HLEN)

This is an 8-bit space and is designated in obtaining the physical addresses' length which is given in bytes.

4. Protocol Length (PLEN)

How long the IP address is stored in bytes is preserved in this 8-bit field.

5. Operation (OPER)

The category of packet is preserved in this 16-bit field. ARP request and ARP reply are the two types of packets.

6. Sender Hardware Address (SHA)

The sender's logical address is defined by SHA and its length is variable.

7. Target Hardware Length (THL)

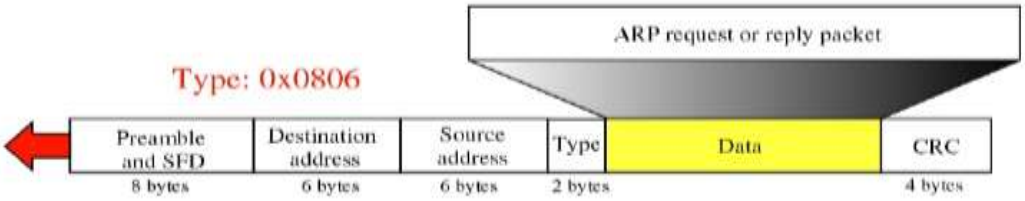
The target's physical address is defined by THL which is of variable length. At the time of ARP request packet, the field is set to zeros as the sender is unaware of the receiver's physical address.

8. Target Protocol Address (TPA)

It is another field with a length that varies and defines the target's logical address.

Encapsulation

The datalink layer holds the ARP packet (request or reply) condensed frame. The indication of the data is specified in the type field as for ARP request or reply packet.



ARP Operations

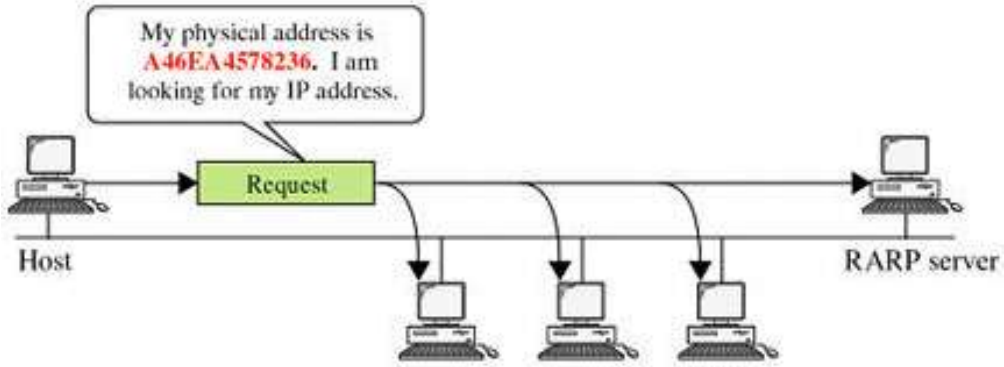
It can be used under the following conditions when it is being operated on internet.

1. Intra network transmission between hosts.
2. Inter network transmission between hosts.
3. Inter network transmission from a router to a host.
4. Inter network transmission received by a router destined to another host.

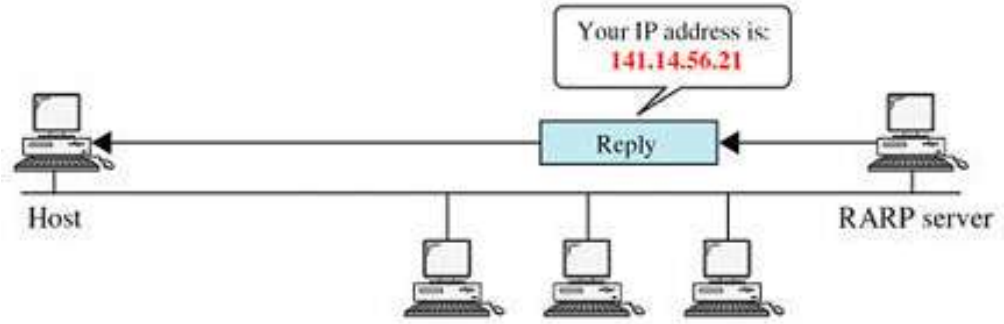
The address of the IP is known to the sender. IP address uses ARP to create an ARP request message. The request packet consists of physical and IP address of the sender along with IP address of the target. In DL layer, the ARP request packet is composed by frame and the broadcast of it is received by all routers and hosts, while the data packet is accessed only by the destined node. The destiny acknowledges with ARP reply holding the physical address of the target. This process is unicast. The frame containing IP datagram with data is sent as unicast to the destination.

2.6.3. Reverse Address Resolution Protocol (RARP)

A part of the TCP / IP protocol suite is RARP. This enables a machine or a diskless workstation, to obtain an IP address from a server. It broadcasts a RARP request packet on the network when a diskless TCP / IP workstation is enabled on a network. This address packet is transmitted for everyone to receive on the network since the workstation does not know the server's IP address which provides an address. The reply will be done using the physical network address or MAC address in request packet. The request pack in the server access the table content for a comparison with the IP address of MAC. Further it returns the IP address to the workstation that is diskless.



a. RARP request is broadcast



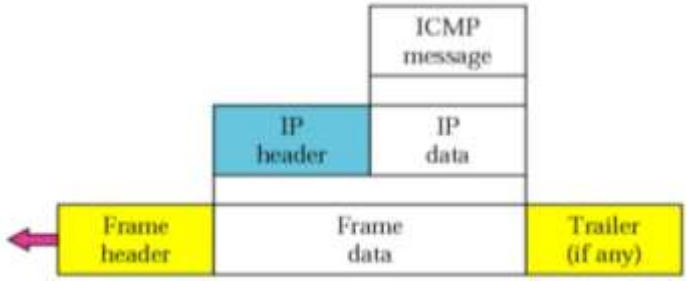
b. RARP reply is unicast

2.6.4. Internet Control Message Protocol (ICMP)

The ICMP intelligences error as well as control messages and they are sent to IP. ICMP never makes IP reliable instead reports error and a feedback is provided for certain conditions. ICMP designed to compensate these two deficiencies.

1. A host sometimes need to determine if a router host is alive.
2. Sometimes a network manager needs information from another host to router.

ICMP is a network layer protocol, its messages are not passed directly to the data link layer as expected.



The encapsulation of messages inside IP datagrams is done before travesring to the lower layer. The value of the protocol field in the IP datagram is 1 to indicate that the IP data is an ICMP message. The ping command is used to test whether station is reachable. Ping packages an ICMP echo request message in a datagram and sends it to a selected destination.

Ping 100.50.25.1

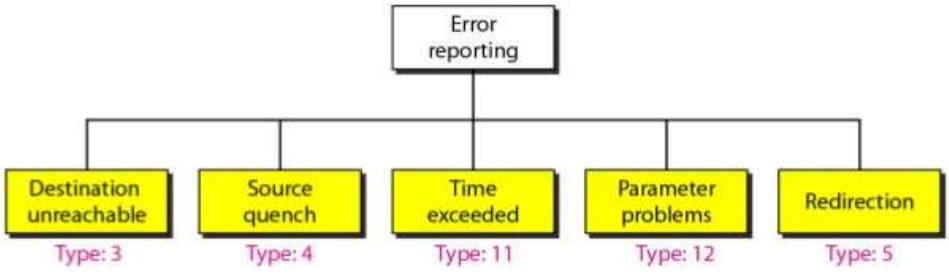
When the destination receives the echo request messages, it responds Y sending an ICMP echo reply messages. If a reply is not returned within a set time, ping resends the echo request several more times or it indicates destination is unreachable. ICMP traces routes which provide a list of all the routers along the path to the specified destination.

Types of Messages

The two types of ICMP messages are error repeating messages and query messages.

Error Repeating Messages

Error reporting has been the prime responsibility of ICMP. ICMP without correcting the errors it simply reports them and error correction is at the discretion to the higher-level protocols. ICMP sends the error reporting messages back to original source. It holds 5 types of errors.



1. Destination Unreachable

The not reachable destiny of IP packet crossing any router, signals the sender with this message.

2. Source Quench Message

A host or router uses source quench messages to report congestion to the original source and to request it to reduce its current state of packet transmission. IP does not support flow control or congestion control. There is no flow control or congestion control mechanism in IP. This type of message is ICMP which is defined to append the flow as well as congestion control

to IP. The source will be informed about the destruction of datagram. The source is further instructed to quench its flow, as a congestion is identified at some place.

3. Time Exceeded Message

Two different cases are discussed under this type of message.

(1) The datagram with TTL 0 is destroyed and acknowledges with message that intimates the source with exceed of time.

(2) The non-reception of fragments at the destiny in the stipulated time, sends a time exceeded message to the source.

4. Parameter Problem Message

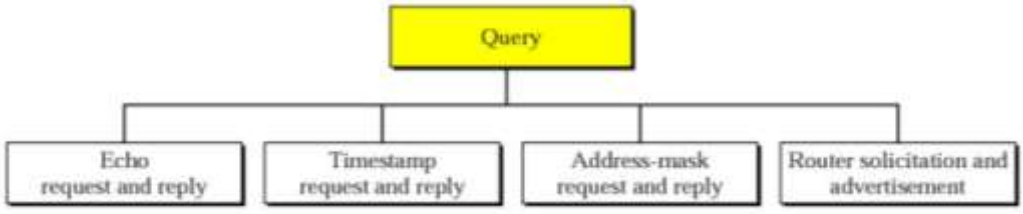
Header section of any datagram should be devoid of ambiguity. If any such indecision or lost value is identified by a router or destination host, further the message is discarded and intimated to sender.

5. Redirection Message

When a packet is transferred to another network, the next router's IP address should be known. In order to find the address of the next router, an entry in routing table has to be preserved in the router and also in the hosts, thereby routing table are continuously modified. For each update, a redirection message is sent back to its host by ICMP.

Query Messages

The ICMP message can diagnose some of the network problems and such a diagnosis is accomplished through the query messages. These messages are categorised as follows.



- **Echo Request and Reply**

The prime focus of this message is diagnosis. They determine if two systems (hosts or routers) communicates with one another.

- **Timestamp Request and Reply**

These IP datagram holds the control over the circuit of the message visiting nodes. Clock synchronization is also accomplished.

- **Address Mask Request and Reply**

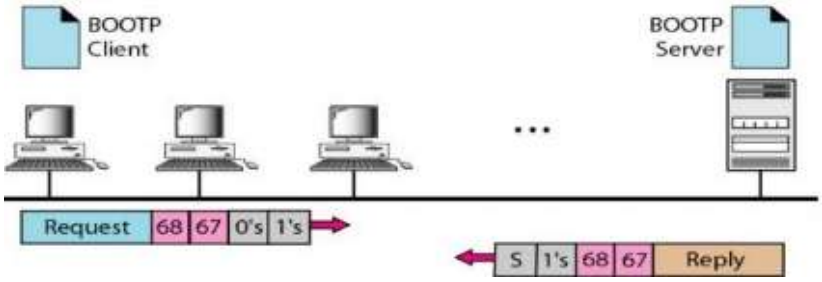
A network address, subnet address and host identifier are contained in an IP address. IP address can be held by host and cannot hold its bifurcation. Address mask reply message is transmitted further.

1. Router Solicitation and Advertisement

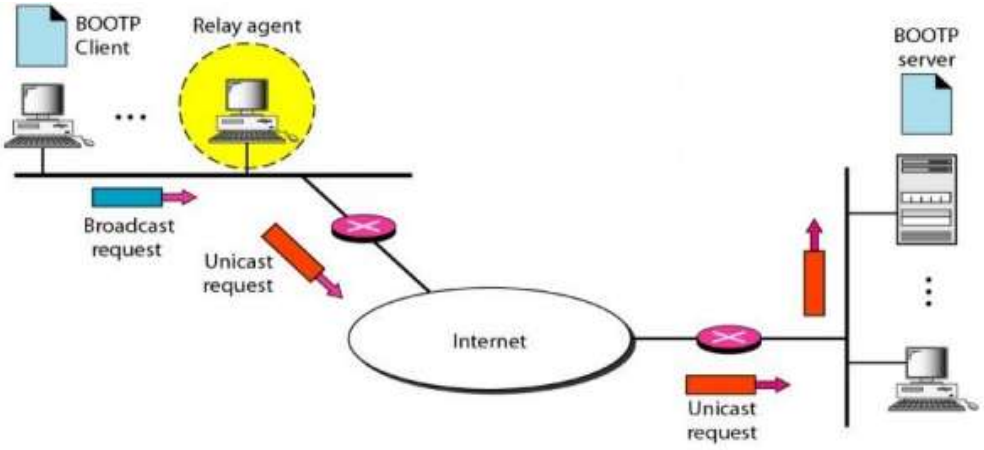
This message makes the routers to broadcast their routing information.

2.6.5. Bootstrap Protocol (BOOTP)

The mapping process of physical address with logical address mapping is facilitated by the client/server protocol called BOOTP. BOOTP is considered to be application layer protocol. The client and server may be available as intra or inter networking, as mentioned by administrator. UDP packet holds BOOTP messages encapsulated in an IP packet.



Without knowing the self-address or the server's IP address, it is possible for a client to transfer an IP datagram. BOOTP is client and server application process. The existence of client and server might be in different networks. Broadcasting from the client is initiated having been unaware of the server's IP address, but router does not allow an IP datagram which is broadcasted.



Relay agent is the host employed to know the unicast address of a BOOTP server. The packet received is encapsulated in unicast datagram and sent to the BOOTP server with request. The packet with unicast address reaches the BOOTP server. The BOOTP server knows the message coming from a relay agent because one of the fields in the request message defines the IP address of the relay agent. The reply is received from the relay agent and forwarded to BOOTP client.

2.6.6. Dynamic Host Configuration Protocol (DHCP)

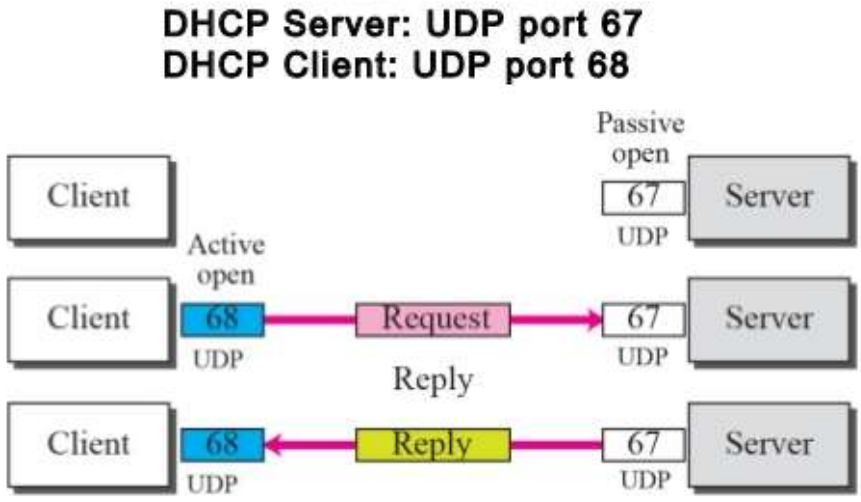
The dynamic address allocation and also static address allocation are devised by DHCP either manually or automatically.

Static Address Allocation

A host BOOTP client executing host requests for a static address from DHCP server, where both are backward compatible. The Physical address and IP address are bound statically in a database of DHCP server.

Dynamic Address Allocation

This DHCP client posts a request for temporary IP address, then the server checks with the unused IP addresses in the pool and allocates an appropriate IP address for a specified duration of time. When DHCP requests its server, it checks for static database. When the address requested is present in the static database, then it's permanent IP address is the response message or if one such address is not present, it selects any available IP address and assigns to client initially and appends this new notification in the dynamic database. The address assigned from the pool is temporary address.



Manual and Automatic Configuration

- Owing to change of physical address and IP address, manual configuration as well as automatic configuration are used.
- The manual config creates static address.
- The automatic config creates dynamic address.