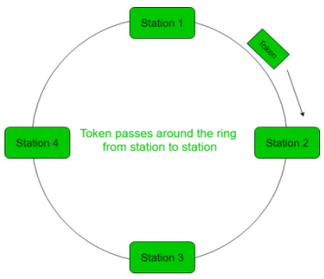
UNIT-III

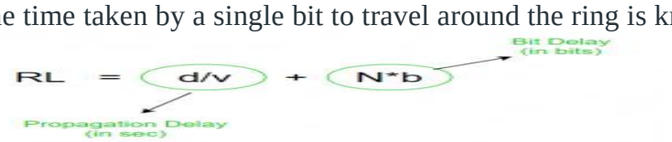
Local Area Network Technology: Token Ring. Error detection (Parity, CRC), Ethernet, Fast Ethernet, Gigabit Ethernet, Personal Area Network: Bluetooth and Wireless Communications Standard: Wi-Fi (802.11) and Wi-MAX

Token Ring

Token Ring protocol is a communication protocol used in Local Area Network (LAN). In a token ring protocol, the topology of the network is used to define the order in which stations send. The stations are connected to one another in a single ring. It uses a special three-byte frame called a **"token"** that travels around a ring. It makes use of Token Passing controlled access mechanism. Frames are also transmitted in the direction of the token. This way they will circulate around the ring and reach the station which is the destination.



Ring Latency –
The time taken by a single bit to travel around the ring is known as ring latency.



Where,
d = length of the ring
v = velocity of data in ring
N = no. of stations in ring
b = time taken by each station to hold the bit before transmitting it (bit delay)

Converting N*b into sec –

RL = d/v + (N*b)/B (B – bandwidth)

Converting d/v into bits –

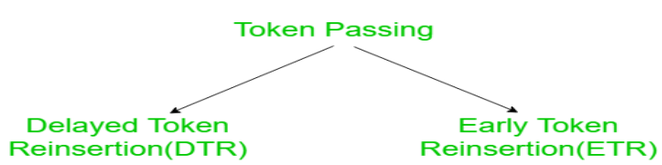
RL = (d/v)*B + N*b (B – bandwidth)

Cycle Time –
The time taken by the token to complete one revolution of the ring is known as cycle time.

Cycle time = T_p + (THT*N)
Where, THT - Token Holding Time
T_p - Propagation delay(d/v)

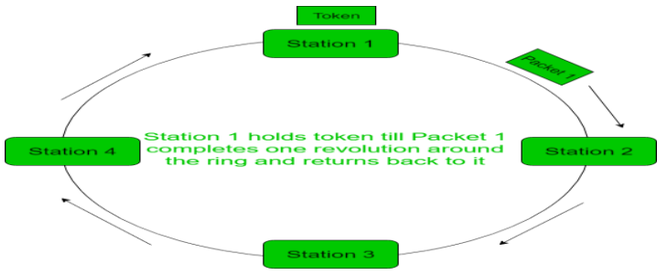
Token Holding Time (THT) –
The maximum time a token frame can be held by a station is known as THT, by default it is set to 10msec. No station can hold the token beyond THT.

Calculating THT:



1. Delayed token reinsertion (DTR) –

- In this, the sender transmit the data packet and waits till the time the whole packet takes the round trip of the ring and return to it. When the whole packet is received by the sender, then it releases the token
- There is only one packet in the ring at an instance
- More reliable than ETR

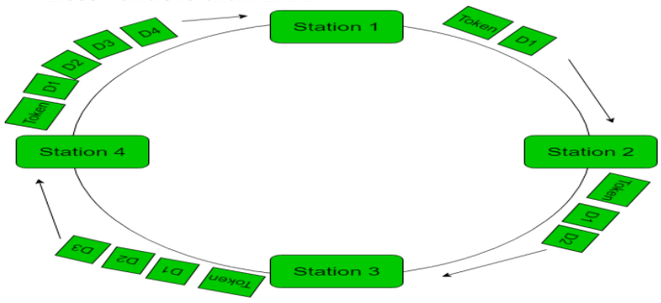


In this case,

THT = T_t + RL
= T_t + T_p + N*b (In most cases, bit delay is 0)
So, THT = T_t + T_p
where T_t = transmission delay
T_p = propagation delay

2. Early token reinsertion (ETR) –

- Sender does not wait for the data packet to complete revolution before releasing the token. Token is released as soon as the data is transmitted
- Multiple packets present in the ring
- Less reliable than DTR



Station 1: Receives the token and transmits data D1 and then, releases the token.
Station 2: Receives D1 (puts it onto the other end) and the token and then, transmits data D2 and releases the token.
Station 3: Receives D1 –> transmits D1
Receives D2 –> transmits D2
Receives token –> transmits D3
Releases token.
Station 4: Receives D1 –> transmits D1
Receives D2 –> transmits D2
Receives D3 –> transmits D3
Receives token –> transmits D4
Releases token.
Station 1: Receives D1 –> discards D1 as D1 has completed its journey
Receives D2 –> transmits D2
Receives D3 –> transmits D3
Receives D4 –> transmits D4
Receives token –> transmits D1(new)
Releases token.
(and the cycle continues so on…..)
In this case,

THT = T_t
where T_t = transmission delay
T_p = propagation delay

Efficiency –
Efficiency, e = useful time/ total time
useful time = N*T_t
total time = cycle time = T_p + (THT*N)
So, e = (N*T_t)/(T_p + (THT*N))

1. Delayed token reinsertion –
In this case, THT = T_t + T_p
So, cycle time = T_p + N*(T_t + T_p)
Efficiency, e = (N*T_t)/(Tp + N*(Tt + Tp))
= 1/(1 + a*((N+1)/N))
where a = Tp/Tt

2. Early token reinsertion –
In this case, THT = T_t
So, cycle time = $T_p + N*(T_t)$

Efficiency, e = $(N*T_t)/(Tp + N*(Tt))$

$= 1/(1 + a*(1/N))$

where a = Tp/Tt

Error detection (Parity, CRC)

Error

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

- Data can be corrupted during transmission. Some applications require that errors be detected and corrected.

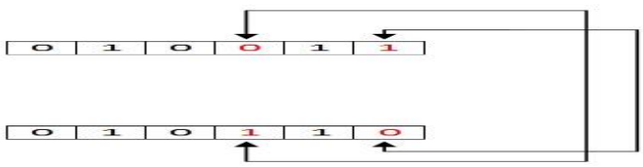
Types of Errors:

- **Single-Bit Error:** The term single-bit error means that only 1 bit of a given data unit is changed from 1 to 0 or from 0 to 1.

Figure: *Single-bit error*

- **Burst Error:**

Multiple Bit error



Error Detecting Codes

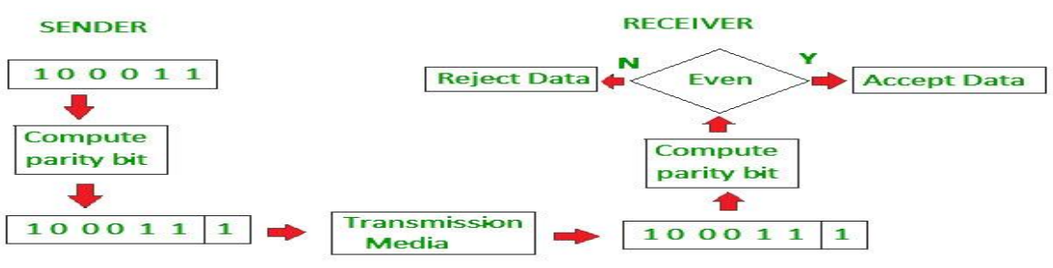
- Basic approach used for error detection is the use of redundancy, where additional bits are added to facilitate detection and correction of errors. Popular techniques are:
  1) Simple Parity check
  2) Two-dimensional Parity check
  3) Checksum
  4) Cyclic redundancy check

Simple Parity- Check Code:

Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of :

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

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



Two-dimensional parity check:

- A better approach is the two-dimensional parity check. In this method, the dataword is organized in a table (rows and columns). Following Figure, the data to be sent, five 7-bit bytes, are put in separate rows. For each row and each column, 1 parity-check bit is calculated. The whole table is then sent to the receiver, which finds the syndrome for each row and each column. As Following Figure shows, the two-dimensional parity check can detect up to three errors that occur anywhere in the table (arrows point to the locations of the created nonzero syndromes). However, errors affecting 4 bits may not be detected.

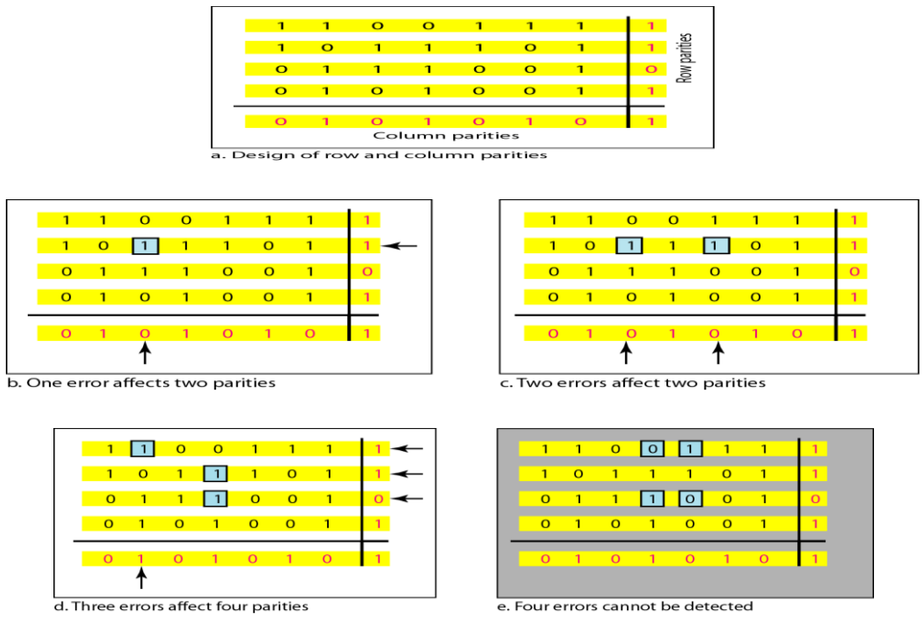


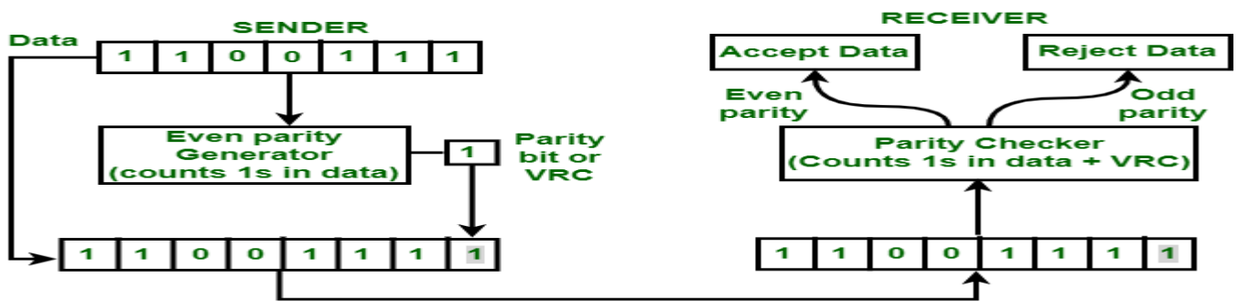
Figure: *Two-dimensional parity-check code*

Vertical Redundancy Check (VRC) or Parity Check

Vertical Redundancy Check is also known as Parity Check. In this method, a redundant bit also called parity bit is added to each data unit. This method includes even parity and odd parity. Even parity means the total number of 1s in data is to be even and odd parity means the total number of 1s in data is to be odd.

Example –

If the source wants to transmit data unit 1100111 using even parity to the destination. The source will have to pass through Even Parity Generator.



Even parity VRC

Data along with parity bit is then transmitted across the network. In this case, 11001111 will be transmitted. At the destination, This data is passed to parity checker at the destination. The number of 1s in data is counted by parity checker.

If the number of 1s count out to be odd, e.g. 5 or 7 then destination will come to know that there is some error in the data. The receiver then rejects such an erroneous data unit.

Advantages :

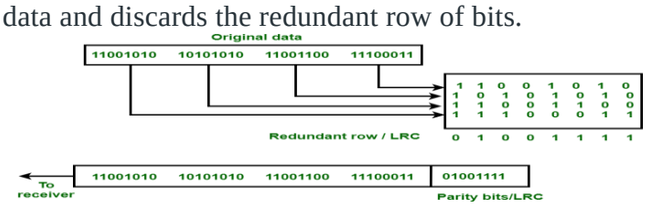
- VRC can detect all single bit error.
- It can also detect burst errors but only in those cases where number of bits changed is odd, i.e. 1, 3, 5, 7, …….etc.

Disadvantages :

The major disadvantage of using this method for error detection is that it is not able to detect burst error if the number of bits changed is even, i.e. 2, 4, 6, 8, …….etc.

Example –

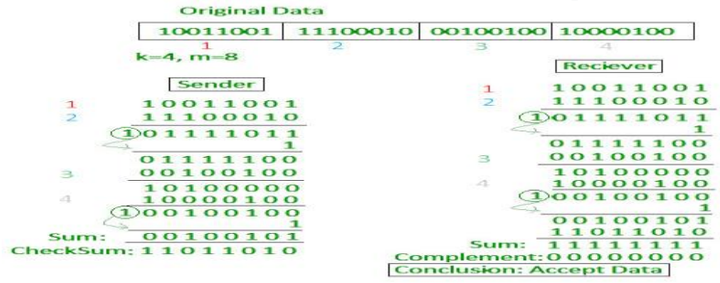
Longitudinal Redundancy Check (LRC) is also known as 2-D parity check. In this method, data which the user want to send is organised into tables of rows and columns. A block of bit is divided into table or matrix of rows and columns. In order to detect an error, a redundant bit is added to the whole block and this block is transmitted to receiver. The receiver uses this redundant row to detect error. After checking the data for errors, receiver accepts the data and discards the redundant row of bits.



Advantage :
LRC is used to detect burst errors.
Example :

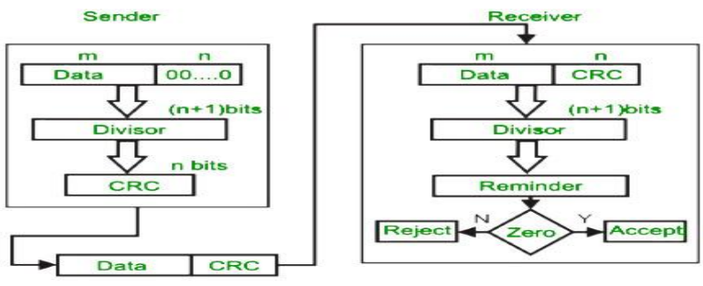
Disadvantage :
The main problem with LRC is that, it is not able to detect error if two bits in a data unit are damaged and two bits in exactly the same position in other data unit are also damaged.
Checksum

- In checksum error detection scheme, the data is divided into k segments each of m bits.
- In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.
- At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.



Cyclic Redundancy Check (CRC)

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



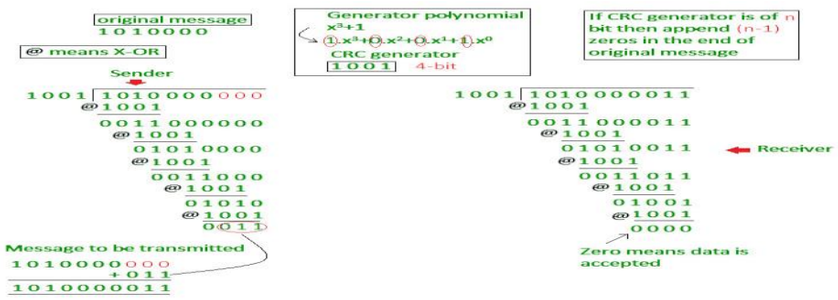
Requirements of CRC: A CRC will be valid if and only if it satisfies the following requirements:

1) It should have exactly one less bit than divisor.
2) Appending the CRC to the end of the data unit should result in the bit sequence which is exactly divisible by the divisor.

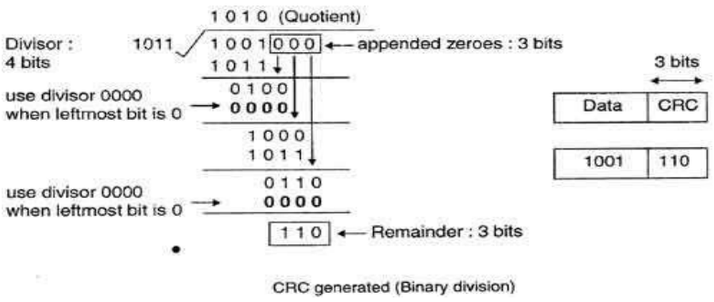
The various steps followed in the CRC method are

- A string of n as is appended to the data unit. The length of predetermined divisor is n+ 1.
- The newly formed data unit i.e. original data + string of n as are divided by the divisor using binary division and remainder is obtained. This remainder is called CRC.

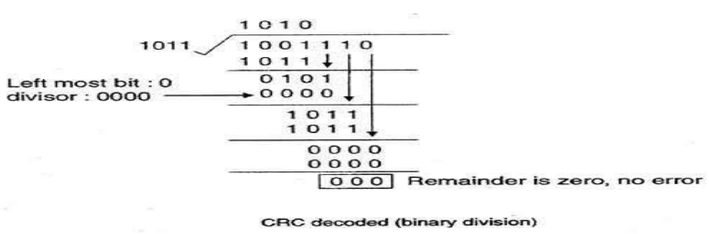
Example :



Data unit 1011000 is divided by 1011.



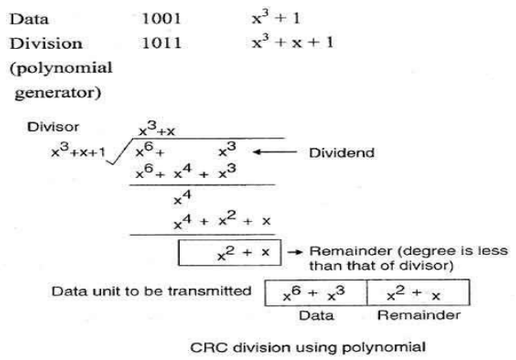
1) During this process of division, whenever the leftmost bit of dividend or remainder is 0, we use a string of Os of same length as divisor. Thus in this case divisor 1011 is replaced by 0000.
2) At the receiver side, data received is 1001110.
3) This data is again divided by a divisor 1011.
4) The remainder obtained is 000; it means there is no error.



- CRC can detect all the burst errors that affect an odd number of bits.
- The probability of error detection and the types of detectable errors depends on the choice of divisor.

CRC generator using polynomials

- If we consider the data unit 1001 and divisor or polynomial generator 1011their polynomial representation is:



CRC division using polynomial

- Now string of n 0s (one less than that of divisor) is appended to data. Now data is 1001000 and its corresponding polynomial representation is $x^6 + x^3$.
- The division of x^6+x^3 by x^3+x+1 is shown in fig
- The polynomial generator should have following properties:
    a. It should have at least two terms.
    b. The coefficient of the term x^0 should be 1.
    c. It should not be divisible by x.
    d. It should be divisible by x+ 1.
- There are several different standard polynomials used by popular protocols for CRC generation. These are:

Name	Polynomial	Application
CRC-8	$x^8 + x^2 + x + 1$	ATM header
CRC-10	$x^{10}+x^9+x^5+x^4+x^2+1$	ATM AAL
CRC-16	$x^{16}+x^{12}+x^5+1$	HDLC
CRC-32	$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$	LANs

Ethernet:-

STANDARD ETHERNET:

- The original Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC).
- Since then, it has gone through **four** generations: **Standard Ethernet (l0 Mbps), Fast Ethernet(100 Mbps), Gigabit Ethernet (l Gbps), and Ten-Gigabit Ethernet (l0 Gbps)**

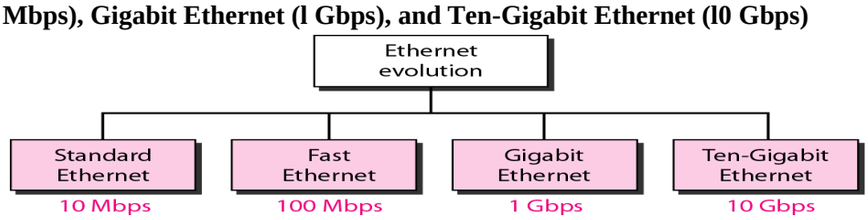


Figure: ***Ethernet evolution through four generations***

MAC Sublayer:

- MAC sublayer frames data received from the upper layer and passes them to the physical layer.

Frame Format:

- The Ethernet frame contains **seven fields.**
- Ethernet does not provide any mechanism for acknowledging received frames, making it what isknown as an unreliable medium. Acknowledgments must be implemented at the higher layers.

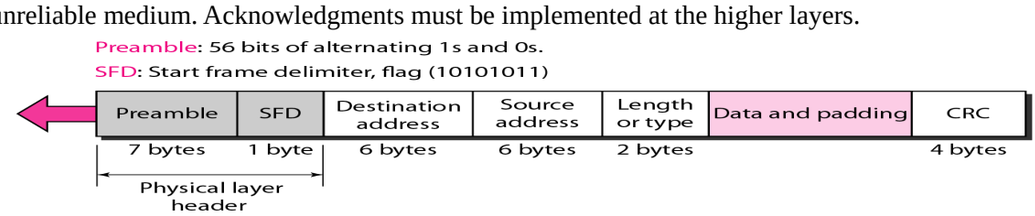


Figure: 802.3 MAC frame

- ***Preamble***. The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating Os and Is that alerts the receiving system to the coming frame and enables it to synchronize its input timing.

- ***Start frame delimiter (SFD).*** The second field (l byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization.
- ***Destination address (DA)***. The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet. We will discuss addressing shortly.
- ***Source address (SA).*** The SA field is also 6 bytes and contains the physical address of the sender of the packet. We will discuss addressing shortly.
- ***Length or type.*** This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame.
- ***Data***. This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes, as we will see later.***CRC.*** The last field contains error detection information, in this case a CRC-32.

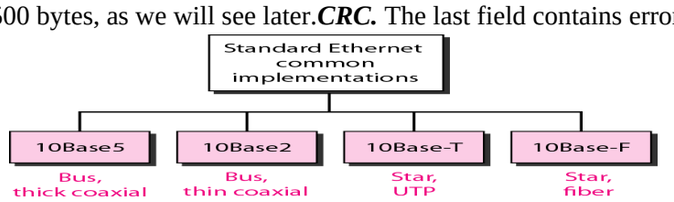
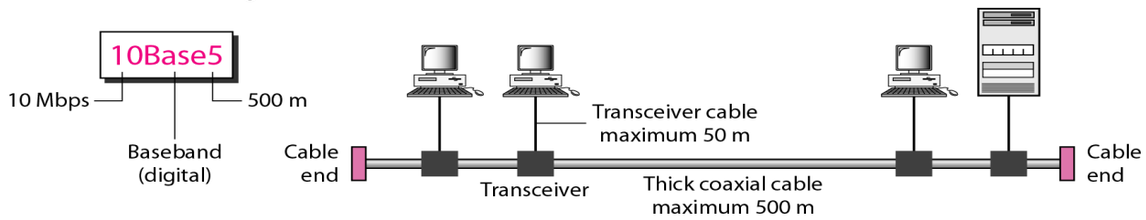


Figure: Categories of Standard Ethernet

10Base5: Thick Ethernet:

- The first implementation is called **10Base5, thick Ethernet, or Thicknet.**
- 10Base5 was the first Ethernet specification to use a bus topology with an external **transceiver (transmitter/receiver)** connected via a tap to a thick coaxial cable.
- The transceiver is responsible for transmitting, receiving, and detecting collisions.The transceiver is connected to the station via a transceiver cable that provides separate paths forsending and receiving
- This means that collision can only happen in the coaxial cable.
- The maximum length of the coaxial cable must not exceed *500 m*



10Base2:ThinEthernet

- The second implementation is called 10Base2, **thin Ethernet, or Cheapernet.**
- 10Base2 also uses a bus topology, but the cable is much thinner and more flexible.
- The cable can be bent to pass very close to the stations.
- In this case, the transceiver is normally part of the network interface card (NIC), which is installedinside the station.

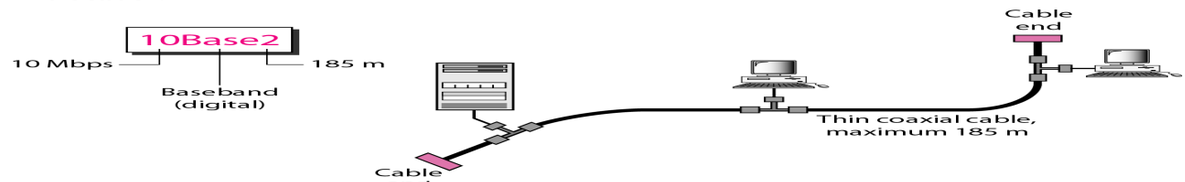
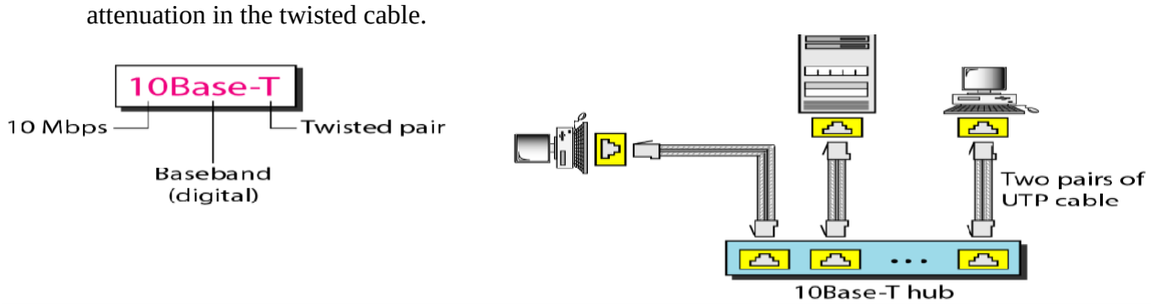


Figure: 10Base2 implementation

10Base-T: Twisted-Pair Ethernet:

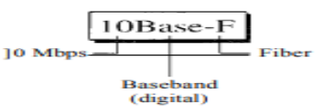
- 1OBase-T uses a physical star topology.
- Two pairs of twisted cable create two paths (one for sending and one for receiving) between thestation and the hub. Any collision here happens in the hub.
- Compared to 10Base5 or 10Base2, we can see that the hub actually replaces the coaxial cable as faras a collision is concerned.
- The maximum length of the twisted cable here is defined as 100 m, to minimize the effect of attenuation in the twisted cable.

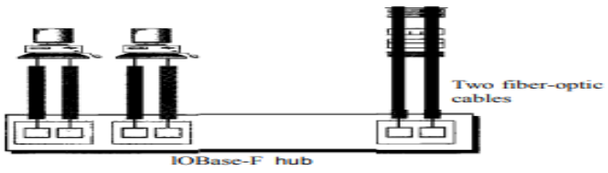


10Base-F: Fiber Ethernet:

- Although there are several types of optical fiber 10-Mbps Ethernet, the most common is called10Base-F.
- 10Base-F uses a star topology to connect stations to a hub.
- The stations are connected to the hub using two fiber-optic cables.

Characteristics	*10Base5*	*10Base2*	*10Base-T*	*10Base-F*
Media	Thick coaxial cable	Thin coaxial cable	2 UTP	2 Fiber
Maximum length	500 m	185 m	100 m	2000 m
Line encoding	Manchester	Manchester	Manchester	Manchester





FAST ETHERNET:-

- Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel.
- IEEE created Fast Ethernet under the name **802.3u**.
- Fast Ethernet is backward-compatible with Standard Ethernet, but it can transmit data 10 times fasterat a rate of 100 Mbps.

Goals of Fast Ethernet:

1. Upgrade the data rate to 100 Mbps.
2. Make it compatible with Standard Ethernet.
3. Keep the same 48-bit address.
4. Keep the same frame format.
5. Keep the same minimum and maximum frame lengths.

MAC Sublayer:

- Main consideration in the evolution of Ethernet from 10 to 100 Mbps was to keep the MAC sublayer untouched.
- **Drop bus topologies** and keep only the **star topology**.
- For the star topology, there are two choices, as we saw before: **half duplex** and **full duplex**.In Half-duplex approach:
- The stations are connected via a hub.
- The access method is CSMA/CD

Full-duplex approach

- The connection is made via a switch with buffers at each port.
- No need for CSMA/CD

Autonegotiation:

- A new feature added to Fast Ethernet is called autonegotiation.
- It allows a station or a hub a range of capabilities.
- Autonegotiation allows two devices to negotiate the mode or data rate of operation.
- It was designed particularly for the following purposes:
    1. To allow incompatible devices to connect to one another. For example, a device with a maximum capacity of 10 Mbps can communicate with a device with a 100 Mbps capacity (but can work at a lower rate).
    2. To allow one device to have multiple capabilities.
    3. To allow a station to check a hub's capabilities

Physical layer:

- The physical layer in Fast Ethernet is more complicated than the one in Standard Ethernet.

Topology:

- Fast Ethernet is designed to connect two or more stations together.
- If there are only two stations, they can be connected point-to-point.

- Three or more stations need to be connected in a star topology with a hub or a switch at the center.

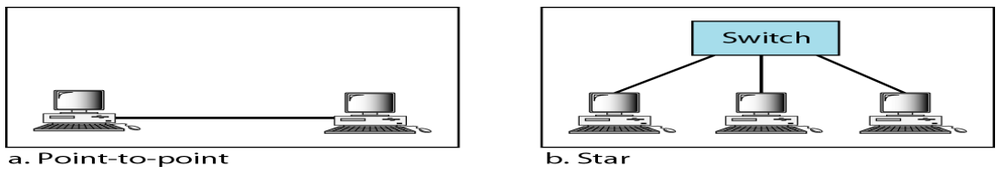


Figure: Fast Ethernet topology

Fast Ethernet implementations:

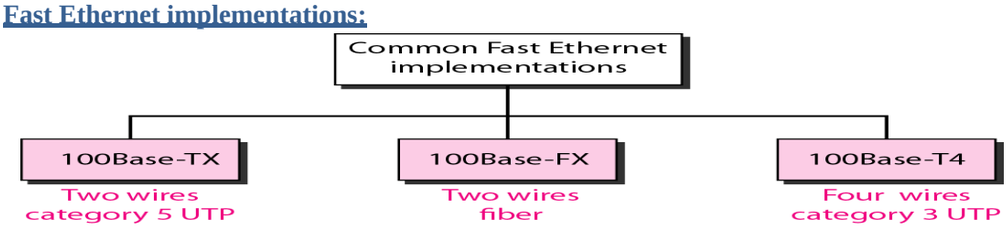


Figure: Fast Ethernet implementations

100Base-TX:

- It uses two pairs of twisted-pair cable (either category 5 UTP or STP(Shielded twisted pair).
- For this implementation, the MLT-3(Multi Level Transmit) scheme was selected since it has good bandwidth performance.
- 4B/5B block coding is used to provide bit synchronization by preventing the occurrence of a long sequence of 0s and 1s.
- This creates a data rate of 125 Mbps, which is fed into MLT-3 for encoding.

100Base-FX:

- Uses two pairs of fiber-optic cables.
- Optical fiber can easily handle high bandwidth requirements by using simple encoding schemes.
- Uses NRZ-I(Non-Return-to-Zero Inverted) encoding scheme (bit synchronization problem.)
- To overcome this problem, 4B/5B block coding is used.
- A 100Base-TX network can provide a data rate of 100 Mbps, but it requires the use of category 5UTP or STP cable. It is cost effective.

100Base-T4:

- Uses four pairs of category 3 or higher UTP.(not cost efficient compared to Category 5)
- Transmit 100 Mbps.
- Uses 8B/6T encoding

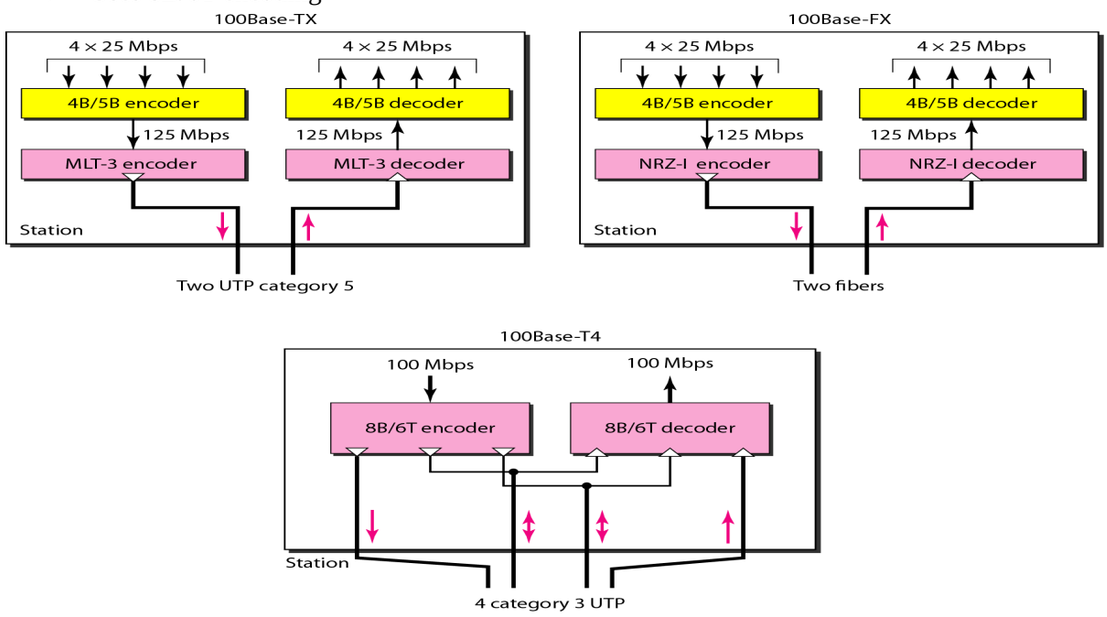


Figure: Encoding for Fast Ethernet implementation

Table 13.2 *Summary of Fast Ethernet implementations*

Characteristics	*lOOBase-TX*	*lOOBase-FX*	*100Base-T4*
Media	Cat 5 UTP or STP	Fiber	Cat 4 UTP
Number of wires	2	2	4
Maximum length	100m	100m	100m
Block encoding	4B/5B	4B/5B	
Line encoding	MLT-3	NRZ-I	8B/6T

GIGABIT ETHERNET

The need for an even higher data rate resulted in the design of the Gigabit Ethernet protocol (1000 Mbps). The IEEE committee calls the Standard 802.3z. The goals of the Gigabit Ethernet design can be summarized as follows:

Goals of gigabit Ethernet:

1. Upgrade the data rate to 1 Gbps.
2. Make it compatible with Standard or Fast Ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. To support autonegotiation as defined in Fast Ethernet.

MAC Sublayer:-

A main consideration in the evolution of Ethernet was to keep the MAC sublayer untouched. However, to achieve a data rate 1 Gbps, this was no longer possible.

Full-Duplex Mode

In full-duplex mode, there is a central switch connected to all computers or other switches. In this mode, each switch has buffers for each input port in which data are stored until they are transmitted. There is no collision in this mode, as we discussed before. This means that CSMAlCD is not used. Lack of collision implies that the maximum length of the cable is determined by the signal attenuation in the cable, not by the collision detection process.

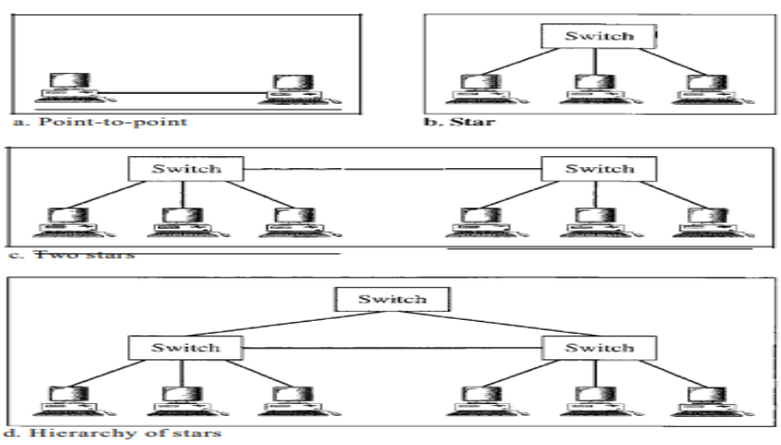
Half-Duplex Mode

Gigabit Ethernet can also be used in half-duplex mode, although it is rare. In this case, a switch can be replaced by a hub, which acts as the common cable in which a collision might occur. The half-duplex approach uses CSMAlCD. However, as we saw before, the maximum length of the network in this approach is totally dependent on the minimum frame size. Three methods have been defined: traditional, carrier extension, and frame bursting.

Physical Layer

The physical layer in Gigabit Ethernet is more complicated than that in Standard or Fast Ethernet. We briefly discuss some features of this layer.

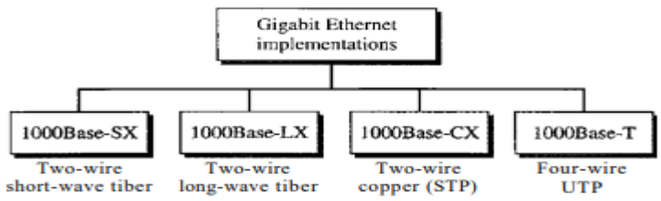
Topology:-Gigabit Ethernet is designed to connect two or more stations. *Topologies of Gigabit Ethernet*



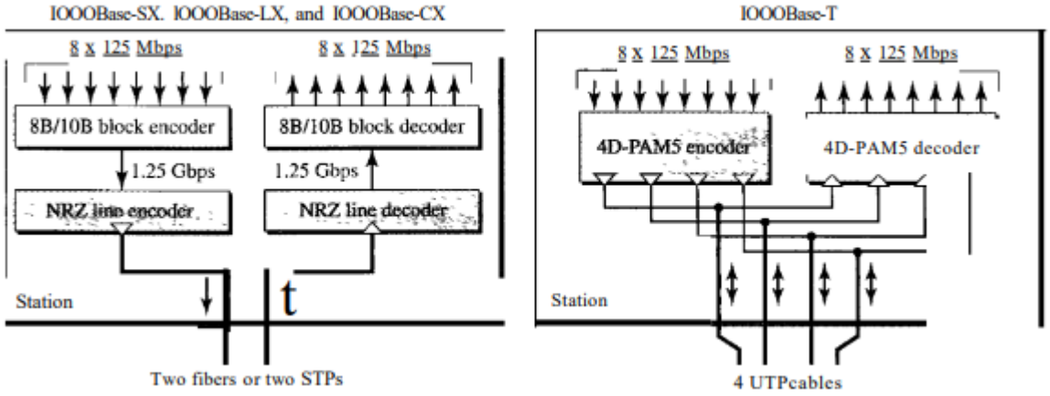
Implementation

Gigabit Ethernet can be categorized as either a two-wire or a four-wire implementation. The two-wire implementations use fiber-optic cable (1000Base-SX, short-wave, or lOOOBase-LX, long-wave), or STP (1000Base-CX). The four-wire version uses category 5 twisted-pair cable (lOOOBase-T). In other words, we have four implementations. lOOOBase-T was designed in response to those users who had already installed this wiring for other purposes such as Fast Ethernet or telephone services.

Gigabit Ethernet implementations



Encoding in Gigabit Ethernet implementations



Gigabit Ethernet cannot use the Manchester encoding scheme because it involves a very high bandwidth (2 GBaud). The two-wire implementations use an NRZ scheme, but NRZ does not self-synchronize properly. To synchronize bits, particularly at this high data rate, 8BIl OB block encoding, discussed in Chapter 4, is used. This block encoding prevents long sequences of Os or Is in the stream, because each wire would need to carry 500 Mbps, which exceeds the capacity for category 5 UTP. As a solution, 4D-PAM5 encoding, as discussed in Chapter 4, is used to reduce the bandwidth. Thus, all four wires are involved in both input and output; each wire carries 250 Mbps, which is in the range for category 5 UTP cable.

Summary

Characteristics	*lOOOBase-SX*	*lOOOBase-LX*	*lOOOBase-CX*	*lOOOBase-T*
Media	Fiber short-wave	Fiber long-wave	STP	Cat 5 UTP
Number of wires	2	2	2	4
Maximum length	550m	5000m	25m	100m
Block encoding	8B/lOB	*8B/lOB*	8B/lOB	
Line encoding	NRZ	NRZ	NRZ	4D-PAM5

Ten-Gigabit Ethernet :-

The IEEE committee created Ten-Gigabit Ethernet and called it Standard 802.3ae. The goals of the Ten-Gigabit Ethernet design can be summarized as follows:

1. Upgrade the data rate to 10 Gbps.
2. Make it compatible with Standard, Fast, and Gigabit Ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. Allow the interconnection of existing LANs into a metropolitan area network (MAN) or a wide area network (WAN).
7. Make Ethernet compatible with technologies such as Frame Relay and ATM .

MAC Sublayer

Ten-Gigabit Ethernet operates only in full duplex mode which means there is no need for contention; CSMA/CD is not used in Ten-Gigabit Ethernet.

Physical Layer

The physical layer in Ten-Gigabit Ethernet is designed for using fiber-optic cable over long distances. Three implementations are the most common: lOGBase-S, lOGBase-L, and lOGBase-E. Table 13.4 shows a summary ofthe Ten-Gigabit Ethernet implementaions.

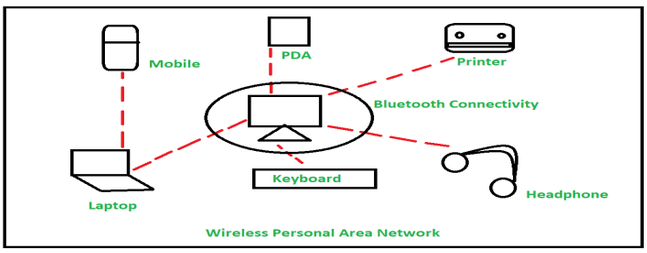
Characteristics	*lOGBase-S*	*lOGBase-L*	*lOGBase-E*
Media	Short-wave S50-nrn rnultimode	Long-wave 131O-nm single mode	Extended 1550-mrn single mode
Maximum length	300m	lOkm	40km

Personal Area Network (PAN)

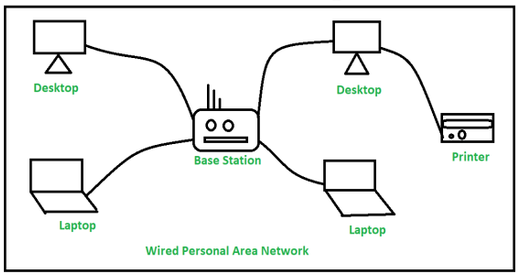
Personal Area Network (PAN) is a the computer network that connects computers/devices within the range of an individual person. As PAN provides a network range within a person's range typically within a range of 10 meters(33 feet) it is called as Personal Area Network. A Personal Area Network typically involves a computer, phone, tablet, printer, PDA (Personal Digital Assistant) and other and other entertainment devices like speakers, video game consoles etc.

Types of Personal Area Network (PAN) :
Personal Area Network can be of 2 types depending upon its connection i.e., Wireless PAN, and Wired PAN.

1. **Wireless PAN –**
   Wireless Personal Area Network (WPAN) is connected through signals sucinfrared, ZigBee, Bluetooth and ultrawideband etc.



2. **Wired PAN –**
   Wired PAN is connected through cables/wires such as Firwire or USB (Universal Serial Bus).



Examples of PAN :

- **Body Area Network –**
  It is a mobile network that moves with a persona range for example when person connects his smart phone to the Bluetooth headphone and moves in the market that refers to a body area network.
- **Offline Network –**
  In this multiple devices are connected through Bluetooth or Wi-Fi. The devices attached to your computer including printers, mouse, speakers, and other appliances are integrated using a Personal Area Network (PAN) and do not use internet. So a communication network is formed between the devices used in a small single space for example home.
- **Home Office –**
  In Home Office setup a separate smaller network is setup for work purpose which is separate from the network used by other home appliances. This network works as a separate body with multiple other devices connected for office work purpose.

Advantages and disadvantages of PAN –
These are some of the Advantages of PAN :

- Easy to use
- PAN is relatively flexible and provides high efficiency for short network range.
- It needs easy setup and relatively low cost.
- It does not require frequent installations and maintenance
- It is easy portable.
- It connect multiple devices.

These are some of the disadvantages of PAN :

- Low network coverage area/range.
- Data transmission is low
- Devices are not compatible with each other.
- Inbuilt WPAN devices are little bit costly.

Applications of PAN –

- Home and Offices
- Organizations and Business sector
- Medical and Hospital
- School and College Education
- Military and Defense

Bluetooth

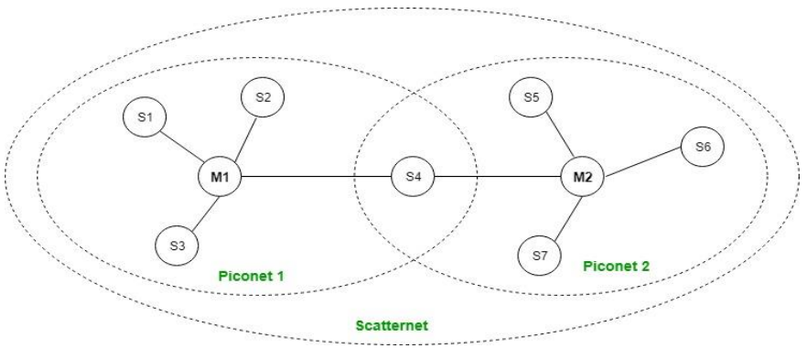
It is a Wireless Personal Area Network (WPAN) technology and is used for exchanging data over smaller distances. This technology was invented by Ericson in 1994. It operates in the unlicensed, industrial, scientific and medical (ISM) band at 2.4 GHz to 2.485 GHz. Maximum devices that can be connected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

Bluetooth Architecture:

The architecture of Bluetooth defines two types of networks:

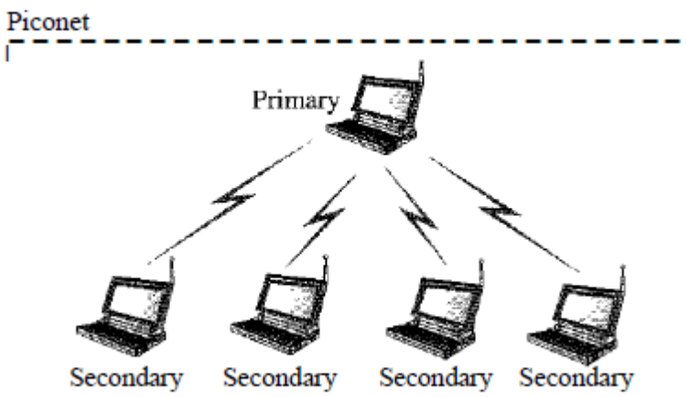
1. Piconet

2. Scatternet



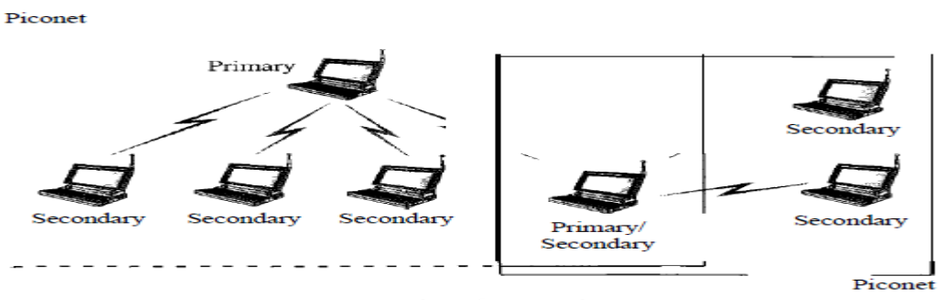
Piconet:

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

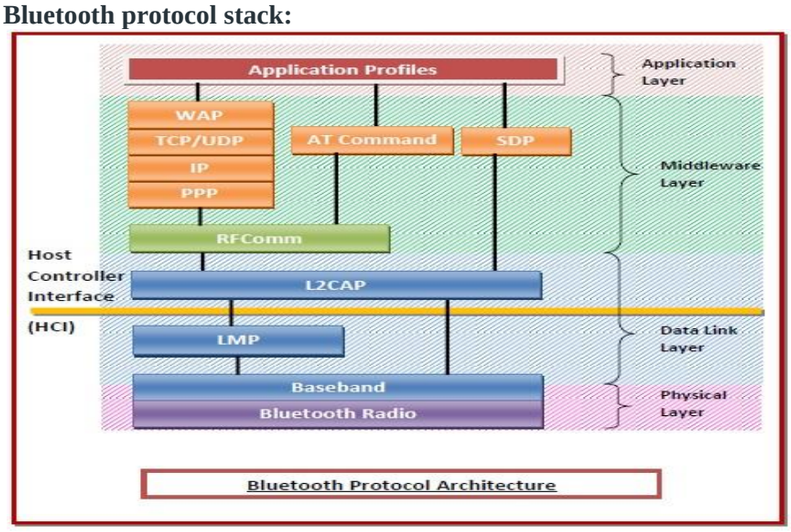


Scatternet:

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 message from master in one piconet and deliver the message to its slave into the other piconet where it is acting as a slave. This type of node is refer as bridge node. A station cannot be master in two piconets.



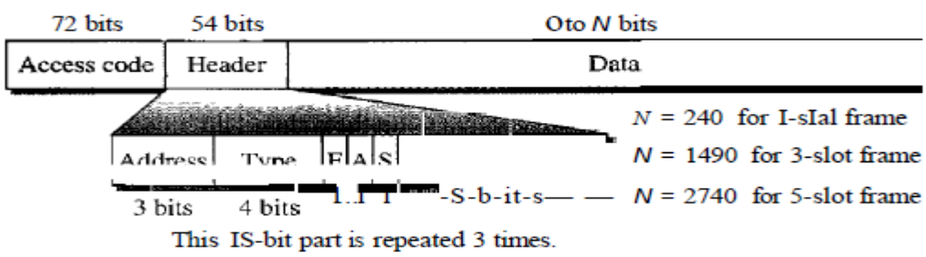
Bluetooth protocol stack:



Protocols in the Bluetooth Protocol Architecture

- **Physical Layer** − This includes Bluetooth radio and Baseband (also in the data link layer.
    - **Radio** − This is a physical layer equivalent protocol that lays down the physical structure and specifications for transmission of radio waves. It defines air interface, frequency bands, frequency hopping specifications, and modulation techniques.
    - **Baseband** − This protocol takes the services of radio protocol. It defines the addressing scheme, packet frame format, timing, and power control algorithms.
- **Data Link Layer** − This includes Baseband, Link Manager Protocol (LMP), and Logical Link Control and Adaptation Protocol (L2CAP).
    - **Link Manager Protocol (LMP)** − LMP establishes logical links between Bluetooth devices and maintains the links for enabling communications. The other main functions of LMP are device authentication, message encryption, and negotiation of packet sizes.
    - **Logical Link Control and Adaptation Protocol (L2CAP)** − L2CAP provides adaption between upper layer frame and baseband layer frame format. L2CAP provides support for both connection-oriented as well as connectionless services.
- **Middleware Layer** − This includes Radio Frequency Communications (RFComm) protocol, adopted protocols, SDP, and AT commands.
    - **RFComm** − It is short for Radio Frontend Component. It provides a serial interface with WAP.
    - **Adopted Protocols** − These are the protocols that are adopted from standard models. The commonly adopted protocols used in Bluetooth are Point-to-Point Protocol (PPP), Internet Protocol (IP), User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Wireless Application Protocol (WAP).
    - **Service Discovery Protocol (SDP)**− SDP takes care of service-related queries like device information so as to establish a connection between contending Bluetooth devices.
    - **AT Commands** − ATtention command set.
- **Applications Layer** − This includes the application profiles that allow the user to interact with the Bluetooth applications.

Frame Format



Header. This 54-bit field is a repeated I8-bit pattern. Each pattern has the following subfields:
1. **Address.** The 3-bit address subfield can define up to seven secondaries (l to 7). If the address is zero, it is used for broadcast communication from the primary to all secondaries.
2. **Type**. The 4-bit type subfield defines the type of data coming from the upper layers. We discuss these types later.

3**. F.** This I-bit subfield is for flow control. When set (I), it indicates that the device is unable to receive more frames (buffer is full).
4. **A.** This I-bit subfield is for acknowledgment. Bluetooth uses Stop-and-Wait ARQ; I bit is sufficient for acknowledgment.
5**. S.** This I-bit subfield holds a sequence number. Bluetooth uses Stop-and-Wait ARQ; I bit is sufficient for sequence numbering.
6. **HEC**. The 8-bit header error correction subfield is a checksum to detect errors in each 18-bit header section.
The header has three identical 18-bit sections. The receiver compares these three sections, bit by bit. If each of the corresponding bits is the same, the bit is accepted; if not, the majority opinion rules. This is a form of forward error correction (for the header only). This double error control is needed because the nature of the communication, via air, is very noisy. Note that there is no retransmission in this sublayer.
o **Payload.** This subfield can be 0 to 2740 bits long. It contains data or control information corning from the upper layers.

Applications

- *They are used in data transfer like images, videos, audio and information from one Bluetooth enable device to another.*
- *They are built in modern devices like laptops, mobile phones, printers and digital cameras.*
- *For better communications, they are also built-in mouse, keyboards and speakers.*
- *They are also used in security-enabled devices like CCTV cameras and car systems.*
- *They are wireless technology; therefore, communications are done without the use of wires and cables.*
- *They can connect to other devices without obstacles. Consequently, they can be used in small offices for data exchange.*

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

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

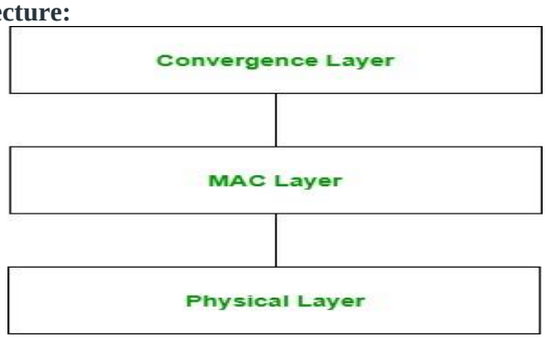
WIMAX

WiMax stands for **Worldwide Inter-operability for Microwave Access**. This technology is based on IEEE 802.16. It is used to provide higher data rates with increased coverage. It is based on MAN (Metropolitan Area Network) technology. Its range is upto 50 Km. It may provide speed upto 70 Mbps and it can operate in Non-Line-of-Sight. This technology is fast, convenient and cost effective. It is a broad band wireless acess.

Past of WIMAX

- In the mid 1990's cell phone companies and service providers started to work on wireless broadband connection technology.
- In 1999 the 802.16 standard was developed by the Institute of Electrical and Electronics Engineers, or the IEEE. This technology was released in 2001 but had a small range and was limited to line-of-sight transmissions. it was initially designed to provide 30 to 40 megabit-per-second data rates.

Architecture:



1. **Physical Layer:**
   This layer is responsible for encoding and decoding of signals and manages bit transmission and reception. It converts MAC layer frames into signals to be transmitted. Modulation schemes which are used on this layer includes: QPSK, QAM-16 and QAM-64.

2. **MAC Layer:**
   This layer provides and interface between convergence layer and physical layer of WiMax protocol stack. It provides point to multipoint communication and is based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

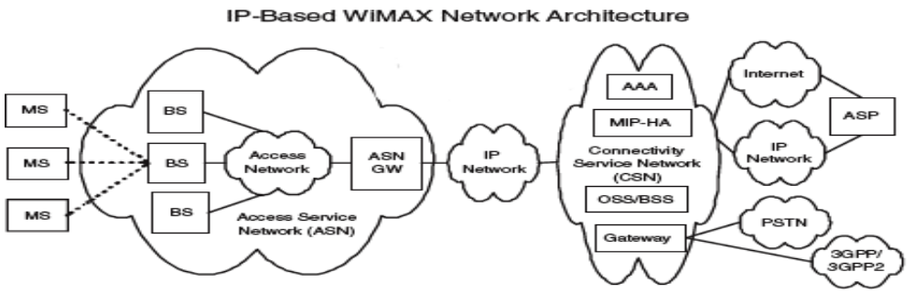
3. **Convergence Layer:**
   This layer provides the information of the external network. It accepts higher layer protocol data unit (PDU) and converts it to lower layer PDU. It provides functions depending upon the service being used.

Reference network model.

The network reference model envisions a unified network architecture for supporting fixed, nomadic, and mobile deployments and is based on an IP service model. Below is simplified illustration of an IP-based WiMAX network architecture. The overall network may be logically divided into three parts −

- Mobile Stations (MS) used by the end user to access the network.
- The access service network (ASN), which comprises one or more base stations and one or more ASN gateways that form the radio access network at the edge.
- Connectivity service network (CSN), which provides IP connectivity and all the IP core network functions.

The network reference model developed by the WiMAX Forum NWG defines a number of functional entities and interfaces between those entities. The following figure shows some of the more important functional entities.



- **Base station (BS)** − The BS is responsible for providing the air interface to the MS. Additional functions that may be part of the BS are micro mobility management functions, such as handoff triggering and tunnel establishment, radio resource management, QoS policy enforcement, traffic classification, DHCP (Dynamic Host Control Protocol) proxy, key management, session management, and multicast group management.
- **Access service network gateway (ASN-GW)** − The ASN gateway typically acts as a layer 2 traffic aggregation point within an ASN. Additional functions that may be part of the ASN gateway include intra-ASN location management and paging, radio resource management, and admission control, caching of subscriber profiles, and encryption keys, AAA client functionality, establishment, and management of mobility tunnel with base stations, QoS and policy enforcement, foreign agent functionality for mobile IP, and routing to the selected CSN.
- **Connectivity service network (CSN)** − The CSN provides connectivity to the Internet, ASP, other public networks, and corporate networks. The CSN is owned by the NSP and includes AAA servers that support authentication for the devices, users, and specific services. The CSN also provides per user policy management of QoS and security. The CSN is also responsible for IP address management, support for roaming between different NSPs, location management between ASNs, and mobility and roaming between ASNs.

APPLICATIONS

- VOIP(Voice over internet protocol)
- Video call
- Video conference
- E-learning

ADVANTAGES

- Single station can serve hundreds of users
- Much faster deployment of new users comparing to wired networks
- It is convient
- Low cost

DISADVANTAGES

- Line of site is needed for longer connections
- Weather conditions like rain could interrupt the signals.

Features

- Speed:46Mbps Downlink & 4Mbps uplink
- Bandwidth:3.5MHZ to 10 MHZ
- Range:up to 50km optimized to 1.5 km-5km
- Data transfer:120kmph
- Cell capacity:100-200 users
- Duplxing mode:TDD,FDD
- Legacy:IEEE802.16a,802.16 b,802.16c,802.16d.

Difference between WiFi and WiMax:

Following are the important differences between Wifi and WiMax.

Sr. No.	Key	Wifi	WiMax
1	Definition	Wifi stands for Wireless Fidelity.	WiMax stands for Wireless Inter-operability for Microwave Access.
2	Usage	WiFi uses Radio waves to create wireless high-speed internet and network connections. A wireless adapter is needed to create hotspots.	WiMax uses spectrum to deliver connection to network and handle a larger inter-operable network.
3	IEEE	Wifi is defined under IEEE 802.11x standards where x defines various WiFi versions.	WiMax is defined under IEEE 802.16y standards where y defines various WiMax versions.
4	Usage	Wifi is used in LAN applications.	WiMax is used in MAN applications.
5	QoS	Wifi does not gurrantee Quality of Service, QoS.	WiMax guarantees Quality of Service, QoS.
6	Network Range	Wifi network ranges at max 100 meters.	WiMax network ranges to max 90 kms.
7	Transmission speed	Wifi transmission speed can be upto 54 mbps.	WiMax transmission speed can be upto 70 mbps.

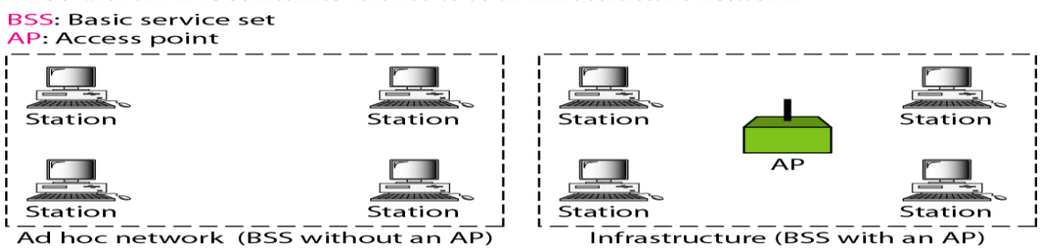
WIFI (OR) WIRELESS LAN

IEEE-802.11:

- IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers thephysical and data link layers.

Architecture:

- The standard defines two kinds of services:
  1. The basic service set (BSS)
  2. The extended service set (ESS)
- IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN.
- A basic service set is made of stationary or mobile wireless stations and an optional central basestation, known as the access point (AP).
- The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an **ad hoc architecture**.
- In this architecture, stations can form a network without the need of an AP; they can locate oneanother and agree to be part of a BSS.
- A BSS with an AP is sometimes referred to as an **infrastructure network**.



Extended Service Set:

- An extended service set (ESS) is made up of **two or more BSSs with APs**.
- In this case, the BSSs are connected through a distribution system, which is usually a wired LAN.
- The distribution system connects the APs in the BSSs.
- IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet.
- Note that the **extended service set uses two types of stations: mobile and stationary**.
- The mobile stations are normal stations inside a BSS.
- The stationary stations are AP stations that are part of a wired LAN.

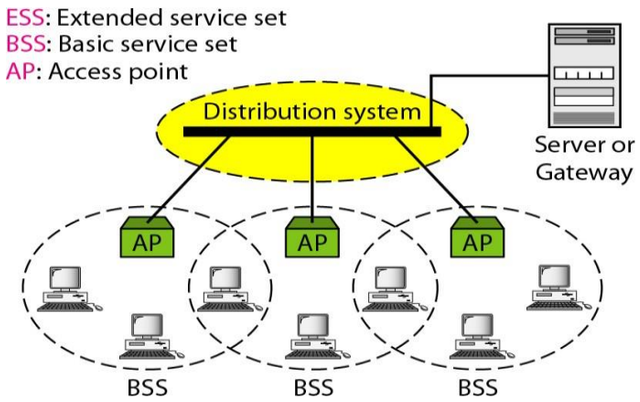


Figure: Extended service sets (ESSs)

- When BSSs are connected, the stations within reach of one another can communicate without the useof an AP.
- However, communication between two stations in two different BSSs usually occurs via two APs.

Station Types:

- IEEE 802.11 defines **three** types of **stations** based on their mobility in a wireless LAN:
  1. no-transition 2. BSS transition 3. ESS-transition mobility
- A station with no-transition mobility is either stationary (not moving) or moving only inside a BSS.
- A station with BSS-transition mobility can move from one BSS to another, but the movement isconfined inside one ESS.
- A station with ESS-transition mobility can move from one ESS to another.
- However, IEEE 802.11 does not guarantee that communication is continuous during the move.

MAC Sublayer:

- IEEE 802.11 defines **two** MAC sublayers: the distributed coordination function (DCF) and point coordination function (PCF).

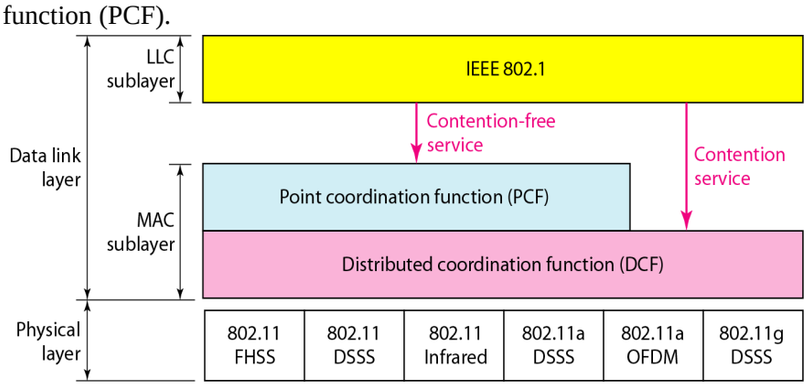
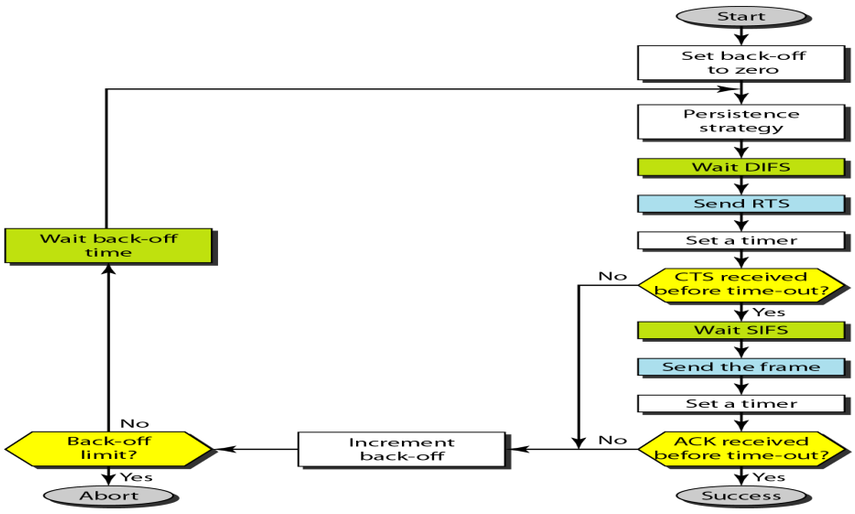


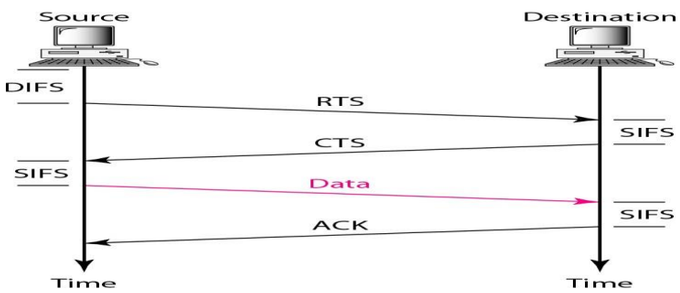
Figure: MAC layers in IEEE 802.11 standard

Distributed Coordination Function:

- DCF uses CSMA/CA as the access method.
- Wireless LANs cannot implement CSMA/CD for three reasons:
  1. For collision detection a station must be able to send data and receive collision signals atthe same time. This can mean costly stations and increased bandwidth requirements.
  2. Collision may not be detected because of the hidden station problem.
  3. The distance between stations can be great. Signal fading could prevent a station at oneend from hearing a collision at the other end.

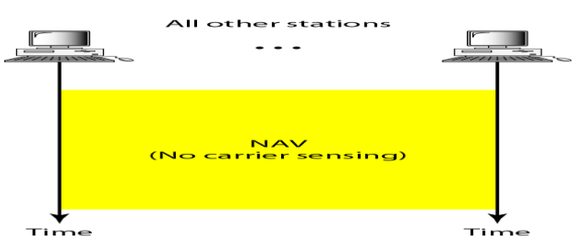


1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.
    a. The channel uses a persistence strategy with back-off until the channel is idle.
    b. After the station is found to be idle, the station waits for a period of time called the distributed interframe space (DIFS); then the station sends a control frame called the request to send (RTS).
2. After receiving the RTS and waiting a period of time called the short interframe space (SIFS), the destination station sends a control frame, called the clear to send (CTS)
3. The source station sends data after waiting an amount of time equal to SIFS.
4. The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received.
   Following figure shows the Frame Exchange Time line



Network Allocation Vector:

- How do other stations defer sending their data if one station acquires access?
- The key is a feature called **NAV**.
- When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel.
- The stations that are affected by this transmission create a timer called a network allocation vector (NAV) that
- Each time a station accesses the system and sends an RTS frame, other stations start their NAV.
- In other words, each station, before sensing the physical medium to see if it is idle, first checks its NAV to see if it has expired.



Collision During Handshaking:

- What happens if there is collision during the time when RTS or CTS control frames are in transition,often called the handshaking period?
- Two or more stations may try to send RTS frames at the same time.
- These control frames may collide.
- However, because there is no mechanism for collision detection, the sender assumes there has been acollision if it has not received a CTS frame from the receiver.
- The back-off strategy is employed, and the sender tries again.

Point Coordination Function (PCF):

- The PCF is an optional access method that can be implemented in an infrastructure network.
- It is implemented on top of the DCF and is used mostly for time-sensitive transmission.
- PCF has a centralized, contention-free polling access method.
- The AP performs polling for stations that are capable of being polled.
- The stations are polled one after another, sending any data they have to the AP.
- To give priority to PCF over DCF, another set of interframe spaces has been defined: PIFS and SIFS.
- The SIFS is the same as that in DCF, but the PIFS (PCF IFS) is shorter than the DIFS.
- Due to the priority of PCF over DCF, stations that only use DCF may not gain access to the medium.

To prevent this, a repetition interval has been designed to cover both contention-free (PCF) andcontention-based (DCF) traffic.

- The repetition interval, which is repeated continuously, starts with a special control frame, called a **beacon frame**.
- When the stations hear the beacon frame, they start their NAV for the duration of the contention-freeperiod of the repetition interval.

Frame Format:

- The MAC layer frame consists of nine fields

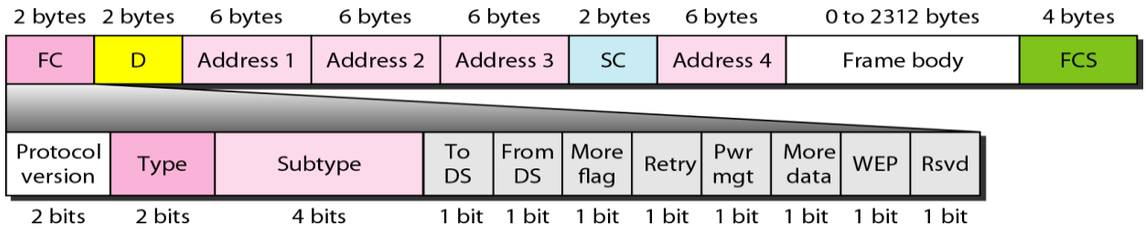


Figure: Frame format

✓ **Frame control (FC).** The FC field is 2 bytes long and defines the type of frame and some control information.

Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 14.2)
To DS	Defined later
From DS	Defined later
More flag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

✓ **D**. In all frame types except one, this field defines the duration of the transmission that is used to setthe value of NAV. In one control frame, this field defines the ID of the frame.

✓ **Addresses**. There are four address fields, each 6 bytes long. The meaning of each address fielddepends on the value of the To DS and From DS subfields

✓ **Sequence control**. This field defines the sequence number of the frame to be used in flow control.

✓ **Frame body**. This field, which can be between 0 and 2312 bytes, contains information based on thetype and the subtype defined in the FC field.

✓ **FCS**. The FCS field is 4 bytes long and contains a CRC-32 error detection sequence.

Frame Types:

- A wireless LAN defined by IEEE 802.11 has three categories of frames: **management frames**,**control frames**, and **data frames**.
- Management frames are used for the initial communication between stations and access points.
- Data frames are used for carrying data and control information.
- Control frames are used for accessing the channel and acknowledging frames.

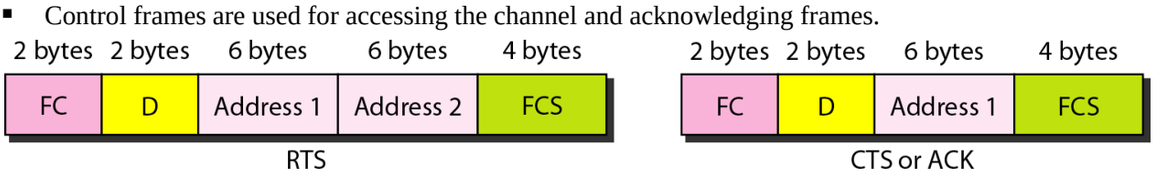


Figure: Control frames

- For control frames the value of the type field is 01; the values of the subtype fields for frames

Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

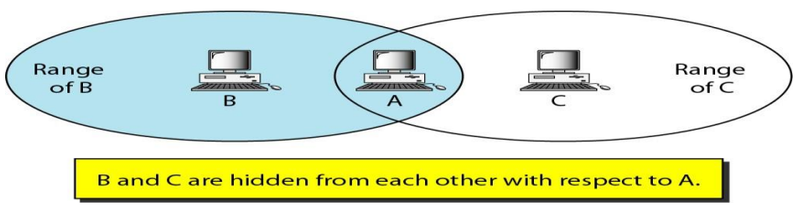
Table: Values of subfields in control frames

Addressing Mechanism:

- The IEEE 802.11 addressing mechanism specifies four cases, defined by the value of the two flags inthe FC field, To DS and From DS.
- Each flag can be either 0 or 1, resulting in four different situations.
- The interpretation of the four addresses (address 1 to address 4) in the MAC frame depends on thevalue of these flags

To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

Table: Addresses



Hidden and Exposed Station Problems:

Figure: Hidden station problem

Above Figure shows an example of the hidden station problem. Station B has a transmission range shown by the left oval (sphere in space); every station in this range can hear any signal transmitted by station B. Station C has a transmission range shown by the right oval (sphere in space); every station locatedin this range can hear any signal transmitted by C. Station C is outside the transmission range of B; likewise,station B is outside the transmission range of C. Station A, however, is in the area covered by both Band C;it can hear any signal transmitted by B or C.

Assume that station B is sending data to station A. In the middle of this transmission, station C also has data to send to station A. However, station C is out of B's range and transmissions from B cannot reach C. Therefore C thinks the medium is free. Station C sends its data to A, which results in a collision at A because this station is receiving data from both B and C. In this case, we say that stations B and C are hidden from each other with respect to A. Hidden stations can reduce the capacity of the network because ofthe possibility of collision.

The solution to the hidden station problem is the use of the handshake frames (RTS and CTS) that we discussed earlier. Following Figure shows that the RTS message from B reaches A, but not C. However, because both Band C are within the range of A, the CTS message, which contains the duration of data transmission from B to A reaches C. Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

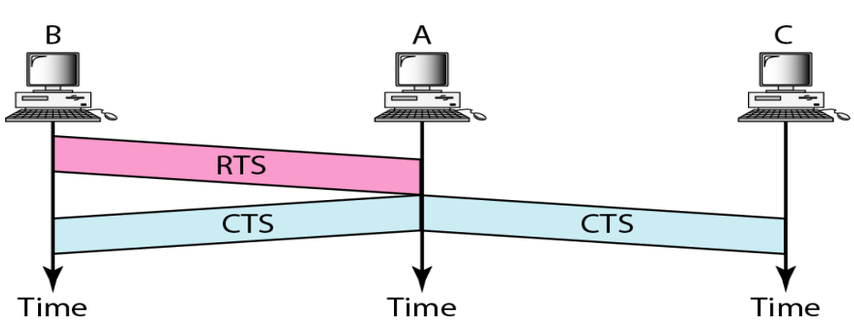
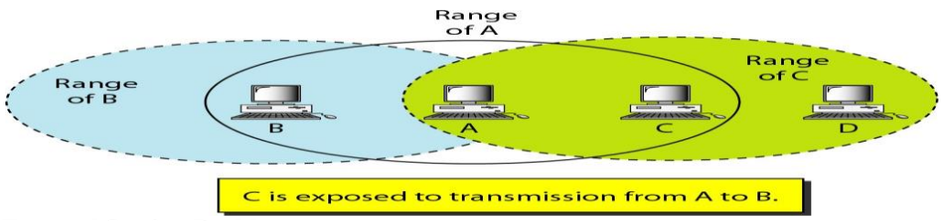


Figure: Use of handshaking to prevent hidden station problem



Exposed Station Problem:

In this problem a station refrains from using a channel when it is, in fact, available. In the above figure, station A is transmitting to station B. Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B. However, station C is exposed to transmission from A; it hears what A is sending and thus refrains from sending. In other words, C is too conservative and wastes the capacity of the channel.

The handshaking messages RTS and CTS cannot help in this case, despite what you might think. Station C hears the RTS from A, but does not hear the CTS from B. Station C, after hearing the RTS fromA, can wait for a time so that the CTS from B reaches A; it then sends an RTS to D to show that it needs to communicate with D. Both stations B and A may hear this RTS, but station A is in the sending state, not the receiving state. Station B, however, responds with a CTS. The problem is here. If station A has started sending its data, station C cannot hear the CTS from station D because of the collision; it cannot send itsdata to D. It remains exposed until A finishes sending its data as Following Figure shows.

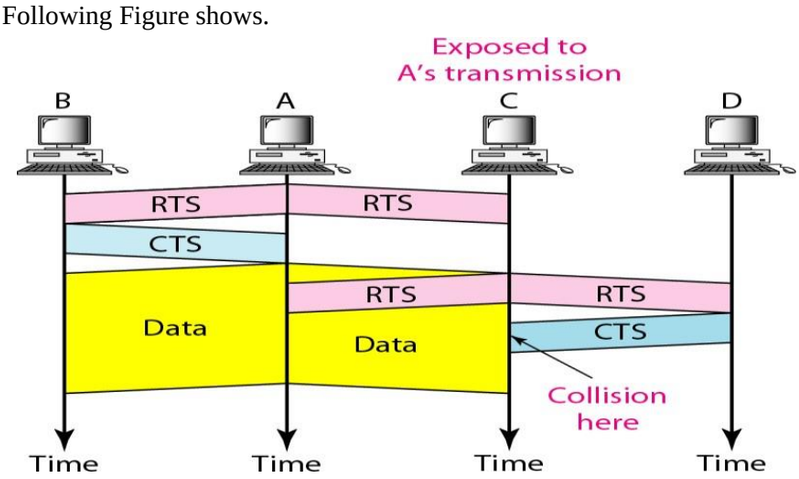


Figure: Use of handshaking in exposed station problem

Physical Layer:

All implementations, except the infrared, operate in the industrial, scientific, and medical (ISM) band, which defines three unlicensed bands in the three ranges 902-928 MHz, 2.400--4.835 GHz, and 5.725-5.850 GHz.

IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.4 GHz	FSK	1 and 2
	DSSS	2.4 GHz	PSK	1 and 2
		Infrared	PPM	1 and 2
802.11a	OFDM	5.725 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.4 GHz	PSK	5.5 and 11
802.11g	OFDM	2.4 GHz	Different	22 and 54

Table : *Physical layers*

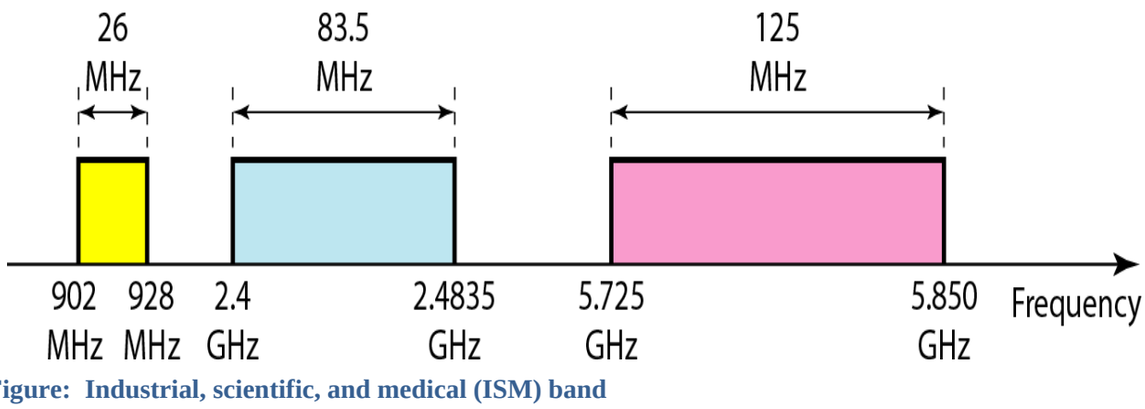


Figure: Industrial, scientific, and medical (ISM) band

IEEE 802.11 FHSS:

- IEEE 802.11 FHSS uses the frequency-hopping spread spectrum (FHSS) method.
- FHSS uses the 2.4-GHz ISM band.
- The band is divided into 79 subbands of 1 MHz (and some guard bands).
- A pseudorandom number generator selects the hopping sequence.
- The modulation technique in this specification is either two-level FSK or four-level FSK with 1 or 2 bits/baud, which results in a data rate of 1 or 2 Mbps.

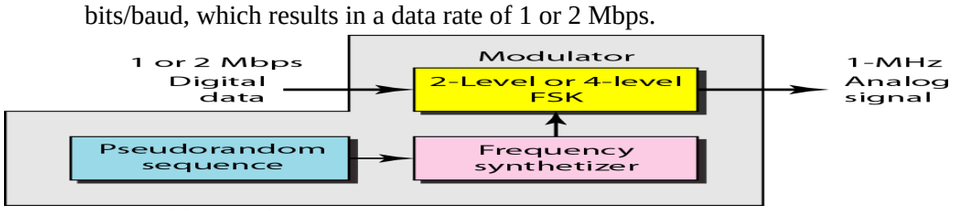


Figure: Physical layer of IEEE 802.11 FHSS

IEEE 802.11 DSSS:

- IEEE 802.11 DSSS uses the direct sequence spread spectrum (DSSS) method.
- DSSS uses the 2.4-GHz ISM band. The modulation technique in this specification is PSK at 1 Mbaud/s. The system allows 1 or 2 bits/baud (BPSK or QPSK), which results in a data rate of 1 or 2 Mbps, as shown in Figure.

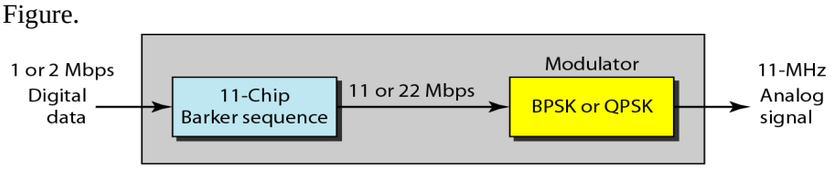
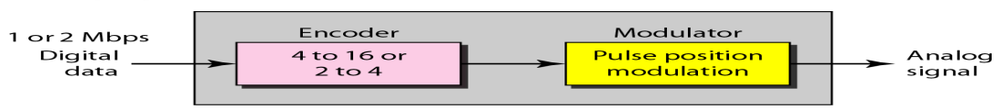


Figure: Physical layer of IEEE 802.11 DSSS

IEEE 802.11 Infrared:

- IEEE 802.11 infrared uses infrared light in the range of 800 to 950 nm.
- The modulation technique is called pulse position modulation (PPM).
- For a 1-Mbps data rate, a 4-bit sequence is first mapped into a 16-bit sequence in which only one bitis set to 1 and the rest are set to 0.
- For a 2-Mbps data rate, a 2-bit sequence is first mapped into a 4-bit sequence in which only one bitis set to 1 and the rest are set to 0.
- The mapped sequences are then converted to optical signals; the presence of light specifies 1, theabsence of light specifies 0.



IEEE 802.11A OFDM:

- IEEE 802.11a OFDM describes the orthogonal frequency-division multiplexing (OFDM) method forsignal generation in a 5-GHz ISM band.
- The band is divided into 52 subbands, with 48 subbands for sending 48 groups of bits at a time and 4 subbands for control information.
- OFDM uses PSK and QAM for modulation. The common data rates are 18 Mbps (PSK) and 54Mbps (QAM).

IEEE 802.11b DSSS:

- IEEE 802.11 b DSSS describes the high-rate direct sequence spread spectrum (HRDSSS) method forsignal generation in the 2.4-GHz ISM band.
- HR-DSSS is similar to DSSS except for the encoding method, which is called complementary codekeying (CCK).

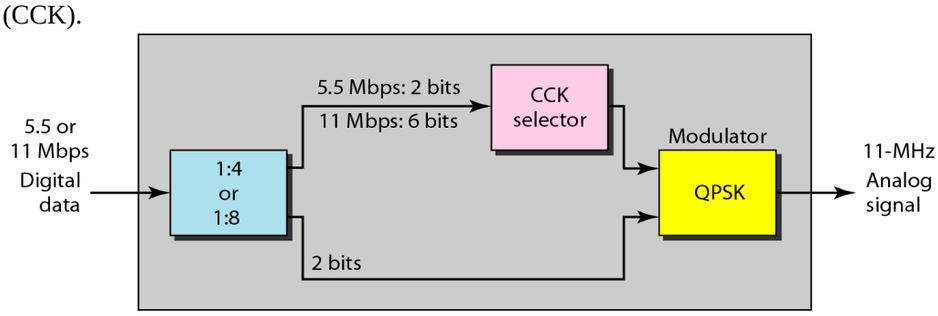


Figure: ***Physical layer of IEEE 802.11b***

IEEE 802.11g:

- This new specification defines forward error correction and OFDM using the 2.4-GHz ISM band.
- The modulation technique achieves a 22- or 54-Mbps data rate. It is backward compatible with802.11b, but the modulation technique is OFDM