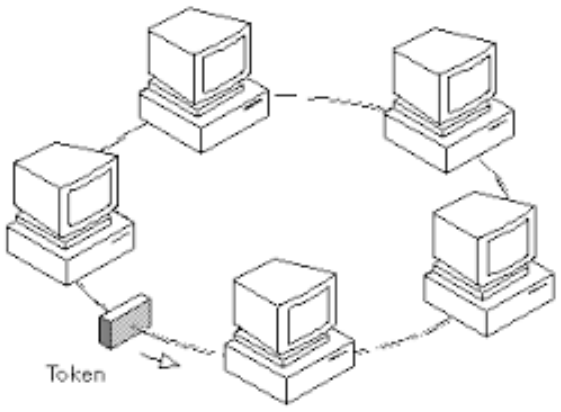
UNIT III

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 Network

- Token Ring is formed by the nodes connected in ring format as shown in the diagram below. The principle used in the token ring network is that a token is circulating in the ring and whichever node grabs that token will have right to transmit the data.
- Whenever a station wants to transmit a frame it inverts a single bit of the 3-byte token which instantaneously changes it into a normal data packet. Because there is only one token, there can atmost be one transmission at a time.
- Since the token rotates in the ring it is guarenteed that every node gets the token with in some specified time. So there is an upper bound on the time of waiting to grab the token so that starvation is avoided.
- There is also an upper limit of 250 on the number of nodes in the network.
- To distinguish the normal data packets from token (control packet) a special sequence is assigned to the token packet. When any node gets the token it first sends the data it wants to send, then recirculates the token.



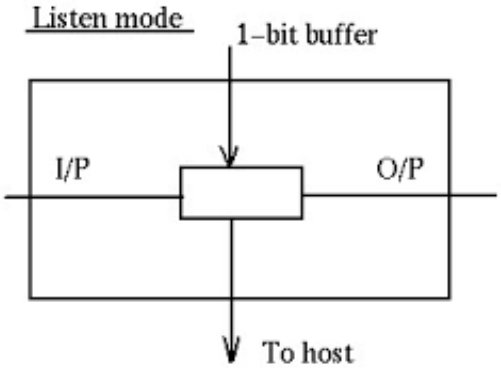
If a node transmits the token and nobody wants to send the data the token comes back to the sender. If the first bit of the token reaches the sender before the transmission of the last bit, then error situation araises. So to avoid this we should have:

propogation delay + transmission of n-bits (1-bit delay in each node) > transmission of the token time

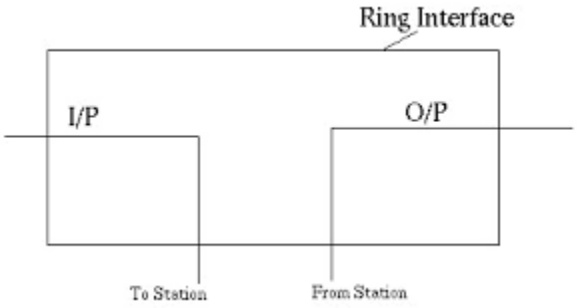
A station may hold the token for the token-holding time. which is 10 ms unless the installation sets a different value. If there is enough time left after the first frame has been transmitted to send more frames, then these frames may be sent as well. After all pending frames have been transmitted or the transmission frame would exceed the token-holding time, the station regenerates the 3-byte token frame and puts it back on the ring.

Modes of Operation

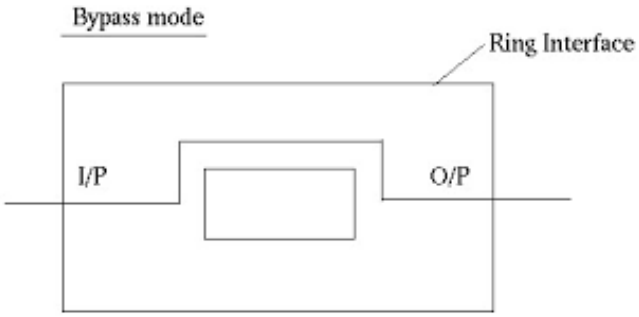
1. **Listen Mode:** In this mode the node listens to the data and transmits the data to the next node. In this mode there is a one-bit delay associated with the transmission.



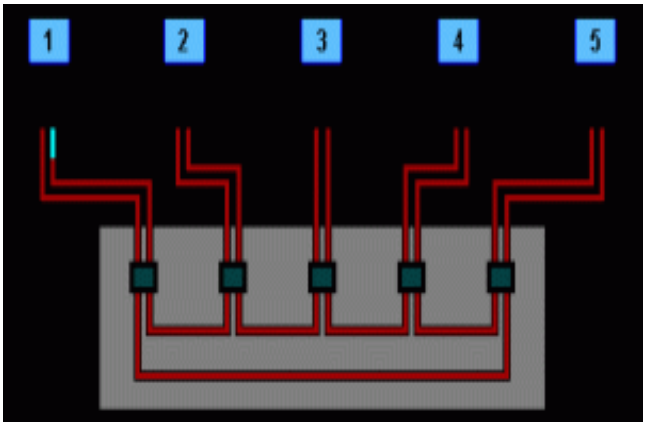
2. **Transmit Mode:** In this mode the node just discards the any data and puts the data onto the network.



3. **By-pass Mode:** In this mode reached when the node is down. Any data is just bypassed. There is no one-bit delay in this mode.



Token Ring Using Ring Concentrator



One problem with a ring network is that if the cable breaks somewhere, the ring dies. This problem is elegantly addressed by using a ring concentrator. A Token Ring concentrator simply changes the topology from a physical ring to a star wired ring. But the network still remains a ring logically. Physically, each station is connected to the ring concentrator (wire center) by a cable containing at least two twisted pairs, one for data to the station and one for data from the station. The Token still circulates around the network and is still controlled in the same manner, however, using a hub or a switch greatly improves reliability because the hub can automatically bypass any ports that are disconnected or have a cabling fault. This is done by having bypass relays inside the concentrator that are energized by current from the stations. If the ring breaks or station goes down, loss of the drive current will release the relay and bypass the station. The ring can then continue operation with the bad segment bypassed.

Who should remove the packet from the ring ?

There are 3 possibilities-

1. **The source itself removes the packet after one full round in the ring**.
2. **The destination removes it after accepting it**: This has two potential problems. Firstly, the solution won't work for broadcast or multicast, and secondly, there would be no way to acknowledge the sender about the receipt of the packet.
3. **Have a specialized node only to discard packets**: This is a bad solution as the specialized node would know that the packet has been received by the destination only when it receives the packet the second time and by that time the packet may have actually made about one and half (or almost two in the worst case) rounds in the ring.

Thus the first solution is adopted with the source itself removing the packet from the ring after a full one round. With this scheme, broadcasting and multicasting can be handled as well as the destination can acknowledge the source about the receipt of the packet (or can tell the source about some error).

Error Detection

Error

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

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

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

Basic approach used for error detection is the use of redundancy bits, whereadditional bits are added to facilitate detection of errors. Some popular

techniques for error detection are:

1. Simple Parity check

2. Two-dimensional Parity check

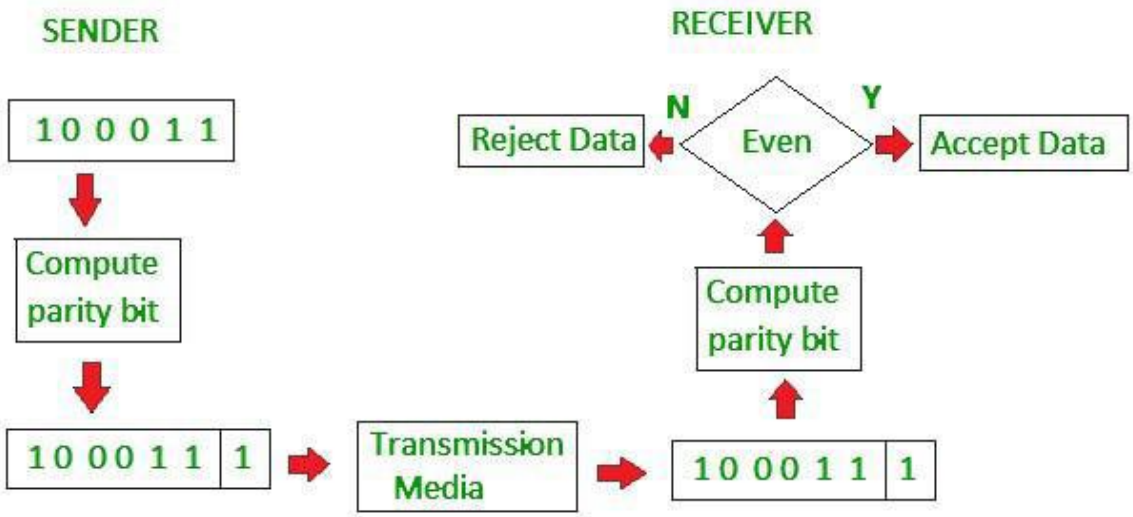
3. Checksum

4. Cyclic redundancy check

Simple Parity check

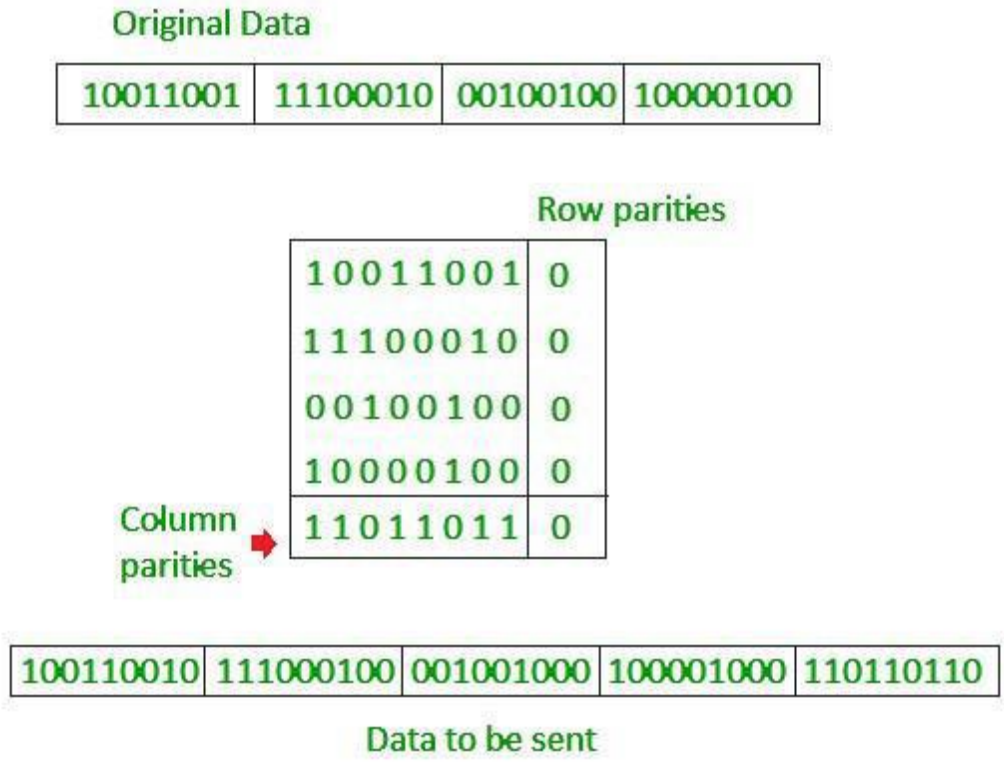
Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of : 1 is added to the block if it contains odd number of 1's, and 0 is added if it contains even

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

Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end these are compared with the parity bits calculated on the received data.



Checksum

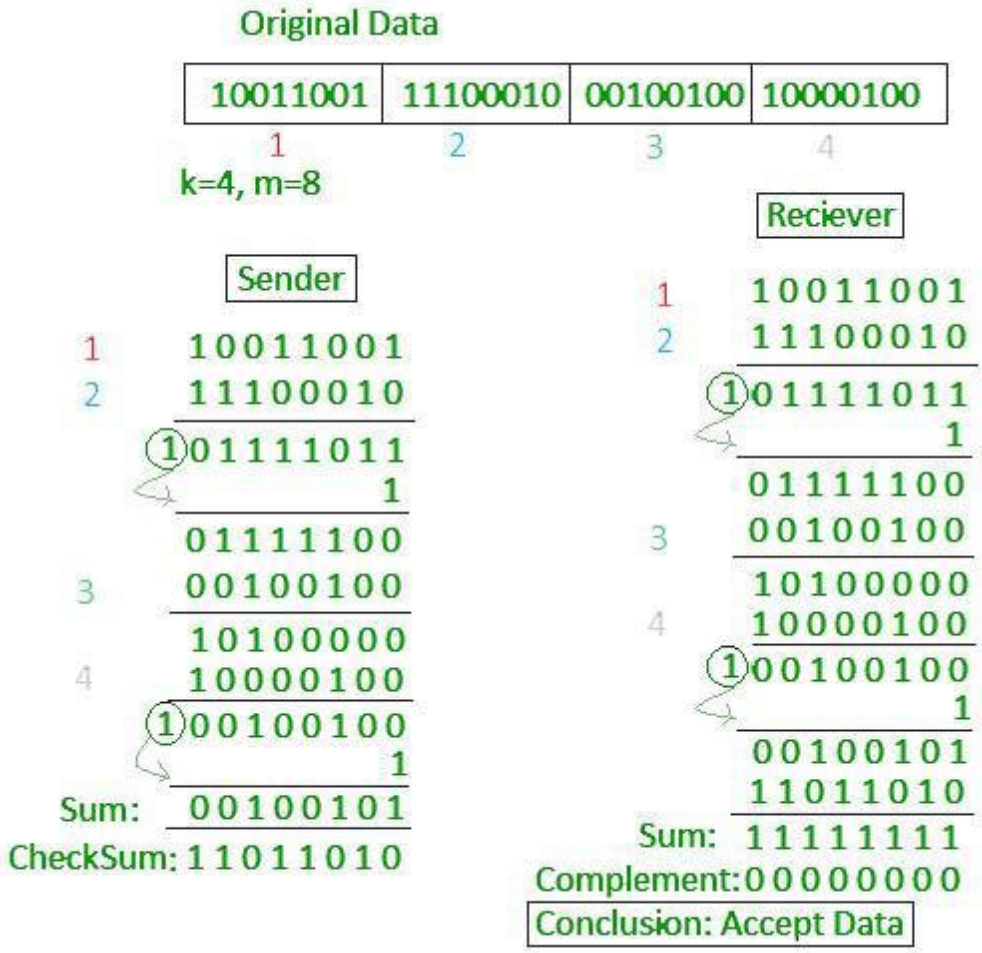
 In checksum error detection scheme, the data is divided into k segments each of m bits.

 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.

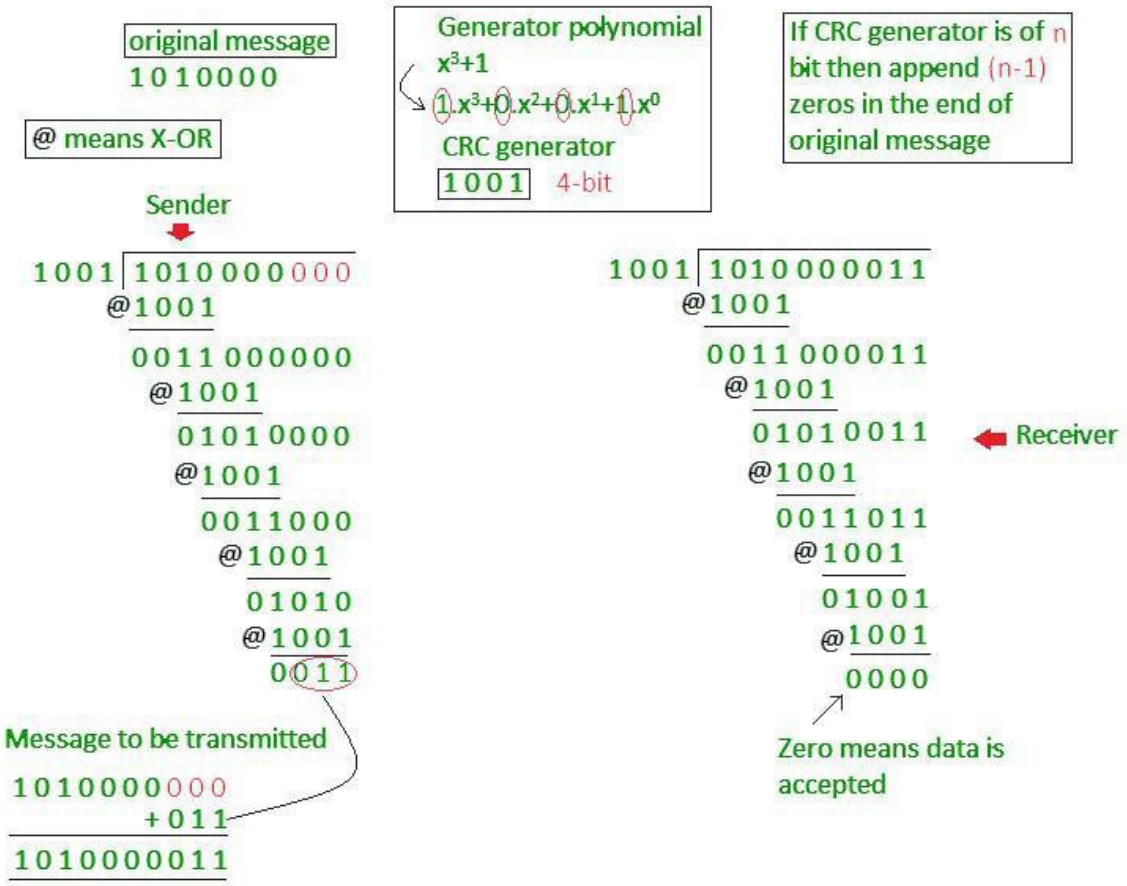
 The checksum segment is sent along with the data segments.

 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)



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

1. INTRODUCTION

A local area network (LAN) is a computer network that is designed for a limited geographic area such as a building or a campus. Although a LAN can be used as an isolated network to connect computers in an organization for the sole purpose of sharing resources, most LANs today are also linked to a wide area network (WAN) or the Internet. The LAN market has seen several technologies such as Ethernet, Token Ring, Token Bus, FDDI, and ATM LAN. Some of these technologies survived for a while, but Ethernet is by far the dominant technology.

2. IEEE STANDARDS

In **1985**, the Computer Society of the **IEEE** started a **project**, called **Project 802**, to set standards to enable intercommunication among equipment from a variety of manufacturers. Project 802 does not seek to replace any part of the OSI or the Internet model. Instead, it is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.

The original Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC). Since then, it has gone through four generations:

a. Standard Ethernet (10 Mbps),
b. Fast Ethernet (100 Mbps),
c. Gigabit Ethernet (1 Gbps), and
d. Ten-Gigabit Ethernet (10 Gbps), as shown in Figure 13.1.

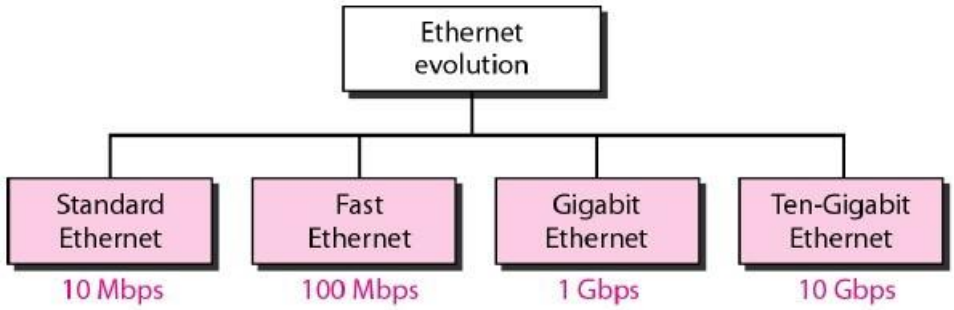


Figure 13.1 Ethernet evolution through four generations

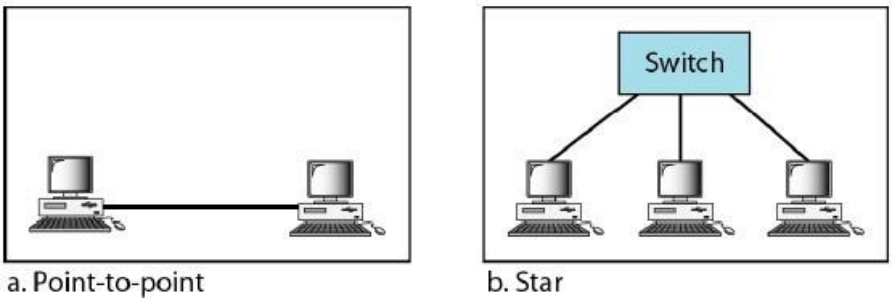
Fast Ethernet(IEEE 802.3u)

Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel (or Fibre Channel, as it is sometimes spelled). IEEE created Fast Ethernet under the name 802.3u. Fast Ethernet is backward-compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps. The goals of Fast Ethernet can be summarized as follows:

a. Upgrade the data rate to 100 Mbps.
b. Make it compatible with Standard Ethernet.
c. Keep the same 48-bit address.
d. Keep the same frame format.
e. Keep the same minimum and maximum frame lengths.

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, as shown in Figure 13.13.



Implementation

Fast Ethernet implementation at the physical layer can be categorized as either two-wire or four-wire. The two-wire implementation can be either category 5 UTP (100Base-TX) or fiber- optic cable (100Base-FX). The four-wire implementation is designed only for category 3 UTP (100Base-T4). See Figure 13.14.

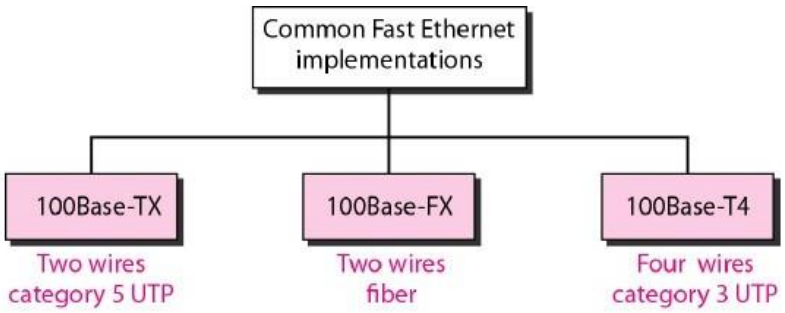


Figure 13.14 Fast Ethernet implementations

Table 13.2 Summary of Fast Ethernet implementations

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

Gigabit Ethernet(IEEE 802.3z)

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:

a. Upgrade the data rate to 1 Gbps.

b. Make it compatible with Standard or Fast Ethernet.

c. Use the same 48-bit address.

d. Use the same frame format.

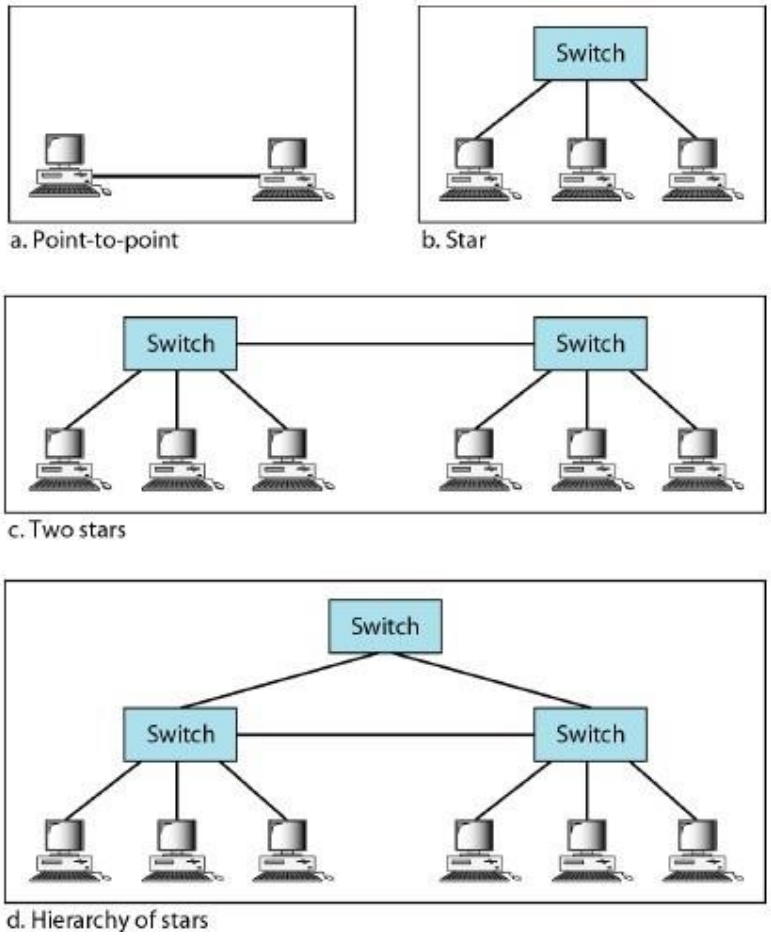
e. Keep the same minimum and maximum frame lengths.

f. To support autonegotiation as defined in Fast Ethernet

Gigabit Ethernet has two distinctive approaches for medium access: half-duplex and full-duplex. Almost all implementations of Gigabit Ethernet follow the full-duplex approach.

Topology

Gigabit Ethernet is designed to connect two or more stations. 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. Another possible configuration is to connect several star topologies or let a star topology be part of another as shown in Figure 13.15



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 1000Base-LX, long-wave), or STP (1000Base-CX). The four-wire version uses category 5 twisted-pair cable (1000Base-T). In other words, we have four implementations, as shown in Figure 13.16

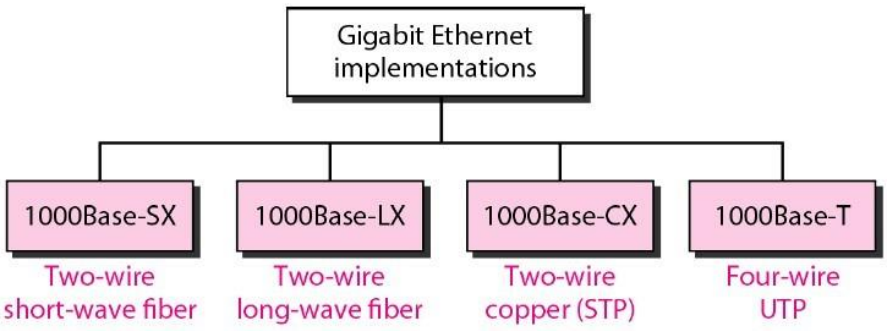


Figure 13.16 Gigabit Ethernet implementations

Summary

Table 13.3 is a summary of the Gigabit Ethernet implementations.

Table 13.3 Summary of Gigabit Ethernet implementations

Characteristics	**1000Base-SX**	**1000Base-LX**	**1000Base-CX**	**1000Base-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
Line encoding	NRZ	NRZ	NRZ	4D-PAM5

Bluetooth

• Bluetooth is, with the infrared, one of the major wireless technologies developed to achieve WPAN. Bluetooth is a wireless LAN technology used to connect devices of different functions such as telephones, computers (laptop or desktop), notebooks, cameras, printers and so on. Bluetooth is an example of personal area network.

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

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

• Nowadays, Bluetooth technology is used for several computer and non computer application:

1. It is used for providing communication between peripheral devices like wireless mouse or keyboard with the computer.

2. It is used by modern healthcare devices to send signals to monitors.

3. It is used by modern communicating devices like mobile phone, PDAs, palmtops etc to transfer data rapidly.

4. It is used for dial up networking. Thus allowing a notebook computer to call via a mobile phone.

5. It is used for cordless telephoning to connect a handset and its local base station.
6. It also allows hands-free voice comml1nication with headset.

7. It also enables a mobile computer to connect to a fixed LAN.

8. It can also be used for file transfer operations from one mobile phone to another.

9. Bluetooth uses omni directional radio waves that can through walls or other non-metal barriers.

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

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

We'll be covering the following topics in this tutorial:

- Bluetooth Architecture
- Bluetooth layers and Protocol Stack

Bluetooth Architecture

Bluetooth architecture defines two types of networks:

1. Piconet

2. Scattemet

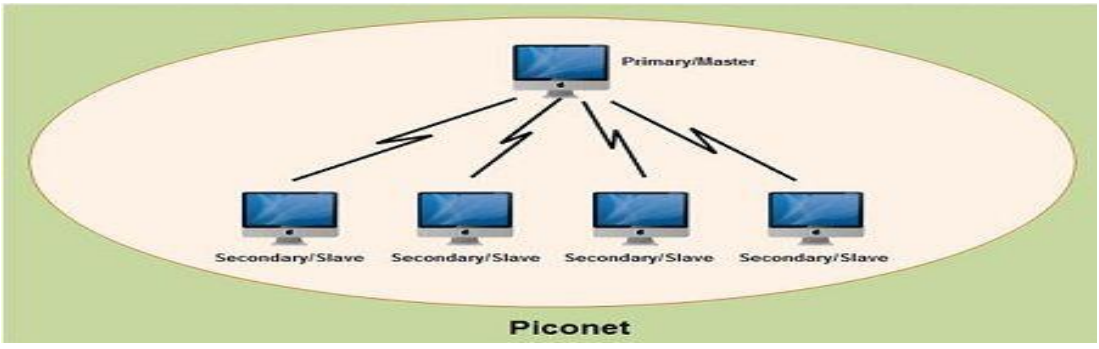
1. Piconet

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

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

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

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



• All communication is between master and a slave. Salve-slave communication is not possible.

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

2. Scatternet

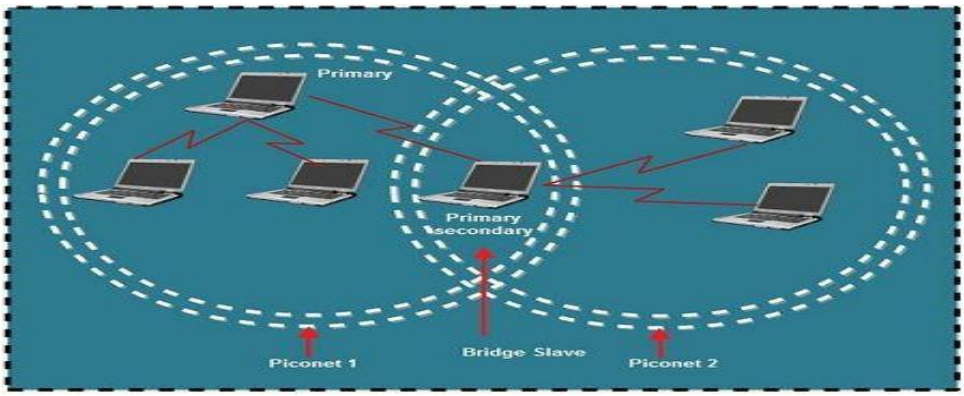
• Scattemet is formed by combining various piconets.

• A slave in one piconet can act as a master or primary in other piconet.

• Such a station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master. This node is also called bridge slave.

• Thus a station can be a member of two piconets.

• A station cannot be a master in two piconets.

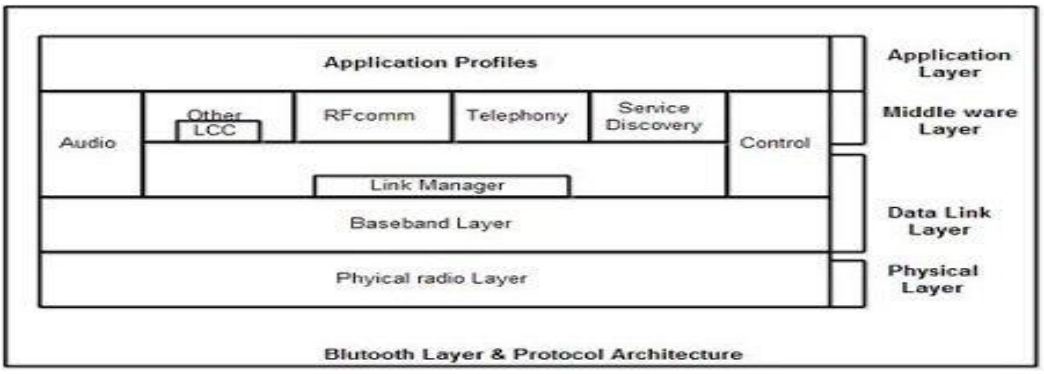


Bluetooth layers and Protocol Stack

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

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

• The different layers and Bluetooth protocol architecture.



Radio Layer

• The Bluetooth radio layer corresponds to the physical layer of OSI model.

• It deals with ratio transmission and modulation.

• The radio layer moves data from master to slave or vice versa.

• It is a low power system that uses 2.4 GHz ISM band in a range of 10 meters.

• This band is divided into 79 channels of 1MHz each. Bluetooth uses the Frequency Hopping Spread Spectrum (FHSS) method in the physical layer to avoid interference from other devices or networks.

• Bluetooth hops 1600 times per second, *i.e.* each device changes its modulation frequency 1600 times per second.

• In order to change bits into a signal, it uses a version of FSK called GFSK *i.e.* FSK with Gaussian bandwidth filtering.

Baseband Layer

• Baseband layer is equivalent to the MAC sublayer in LANs.

• Bluetooth uses a form of TDMA called TDD-TDMA (time division duplex TDMA).

• Master and slave stations communicate with each other using time slots.

• The master in each piconet defines the time slot of 625 μsec.

• In TDD- TDMA, communication is half duplex in which receiver can send and receive data but not at the same time.

• If the piconet has only no slave; the master uses even numbered slots (0, 2, 4, …) and the slave uses odd-numbered slots (1, 3, 5, ….). Both master and slave communicate in half duplex mode. In slot 0, master sends & secondary receives; in slot 1, secondary sends and primary receives.

• If piconet has more than one slave, the master uses even numbered slots. The slave sends in the next odd-numbered slot if the packet in the previous slot was addressed to it.

• In Base-band layer, two types of links can be created between a master and slave. These are:

1. Asynchronous Connection-less (ACL)

• It is used for packet switched data that is available at irregular intervals.

• ACL delivers traffic on a best effort basis. Frames can be lost & may have to be re-transmitted.

• A slave can have only one ACL link to its master.

• Thus ACL link is used where correct delivery is preferred over fast delivery.

• The ACL can achieve a maximum data rate of 721 kbps by using one, three or more slots.

2. Synchronous Connection Oriented (SCO)

• sco is used for real time data such as sound. It is used where fast delivery is preferred over accurate delivery.

• In an sco link, a physical link is created between the master and slave by reserving specific slots at regular intervals.

• Damaged packet; are not re-transmitted over sco links.

• A slave can have three sco links with the master and can send data at 64 Kbps.

Logical Link, Control Adaptation Protocol Layer (L2CAP)

• The logical unit link control adaptation protocol is equivalent to logical link control sub-layer of LAN.

• The ACL link uses L2CAP for data exchange but sco channel does not use it.

• The various function of L2CAP is:

1. Segmentation and reassembly

• L2CAP receives the packets of up to 64 KB from upper layers and divides them into frames for transmission.

• It adds extra information to define the location of frame in the original packet.

• The L2CAP reassembles the frame into packets again at the destination.

2. Multiplexing

• L2CAP performs multiplexing at sender side and de-multiplexing at receiver side.

• At the sender site, it accepts data from one of the upper layer protocols frames them and deliver them to the Base-band layer.

• At the receiver site, it accepts a frame from the base-band layer, extracts the data, and delivers them to the appropriate protocol1ayer.

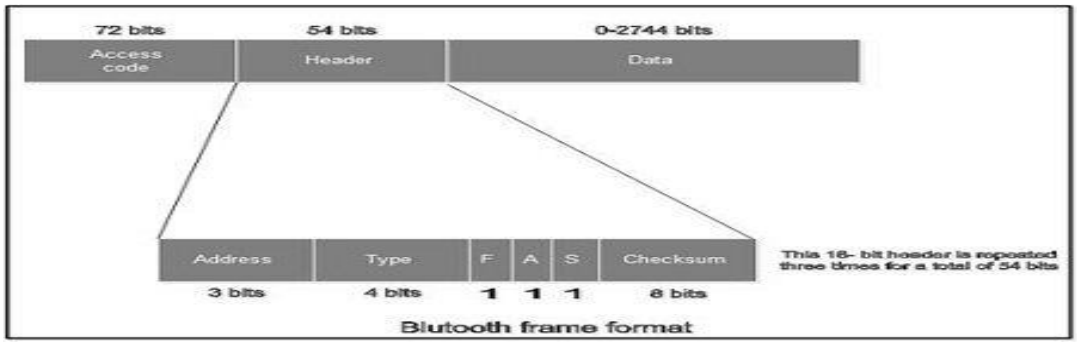
3. Quality of Service (QOS)

• L2CAP handles quality of service requirements, both when links are established and during normal operation.

• It also enables the devices to negotiate the maximum payload size during connection establishment.

Bluetooth Frame Format

The various fields of blue tooth frame format are:



1. **Access Code**: It is 72 bit field that contains synchronization bits. It identifies the master.

2. **Header**: This is 54-bit field. It contain 18 bit pattern that is repeated for 3 time.

The header field contains following sub-fields:

(i) **Address**: This 3 bit field can define up to seven slaves (1 to 7). If the address is zero, it is used for broadcast communication from primary to all secondaries.

(ii)Type: This 4 bit field identifies the type of data coming from upper layers.

(iii) **F**: This flow bit is used for flow control. When set to 1, it means the device is unable to receive more frames.

(iv) **A**: This bit is used for acknowledgement.

(v) **S**: This bit contains a sequence number of the frame to detect re-transmission. As stop and wait protocol is used, one bit is sufficient.

(vi) **Checksum**: This 8 bit field contains checksum to detect errors in header.

3. **Data**: This field can be 0 to 2744 bits long. It contains data or control information coming from upper layers

WiFi:

Any of the above wireless LAN standards are referred to by the brand name **"WiFi"**. It essentially denotes a set of Wireless LAN standards developed by the working group 11 of the
IEEE LAN/MAN Standards Committee (IEEE 802).

IEEE-802.11:

 IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical 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 base station, 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 one another and agree to be part of a BSS.

 A BSS with an AP is sometimes referred to as an **infrastructure network**.

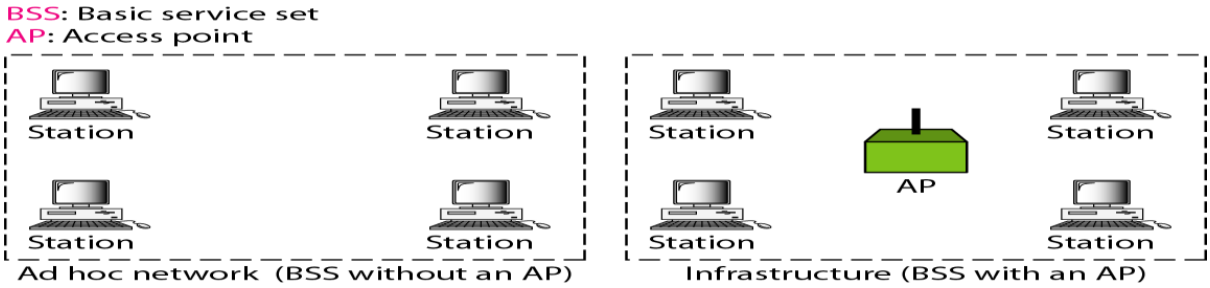
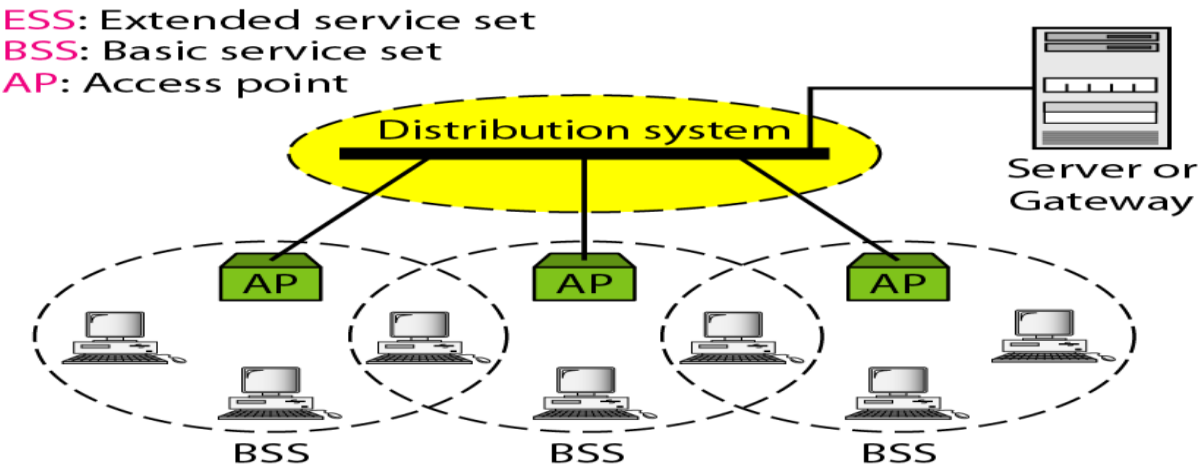


FIGURE: BASIC SERVICE SETS (BSSS)

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.



 When BSSs are connected, the stations within reach of one another can communicate without the use of 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:
- no-transition2. BSS transition3. ESS-transition mobility
- A station with no-transition mobility is either stationary (not moving) or moving only inside a BSS.
- A station with BSS-transitionmobility can move from one BSS to another, but the movement is confined 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).

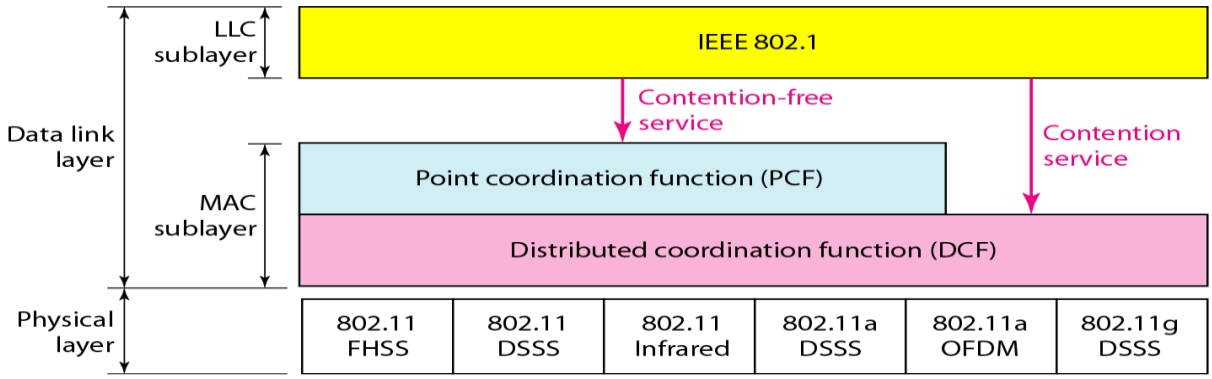


Figure: MAC layers in IEEE 802.11 standard

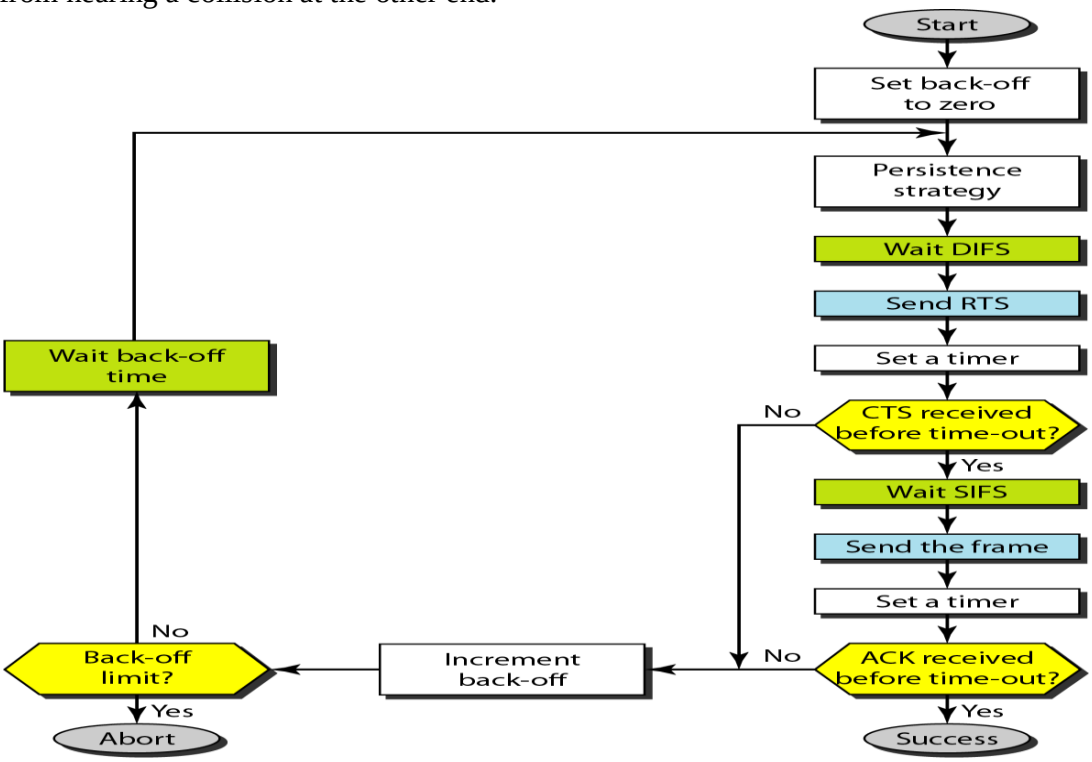
Distributed Coordination Function:

- 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 at the 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 one end 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.

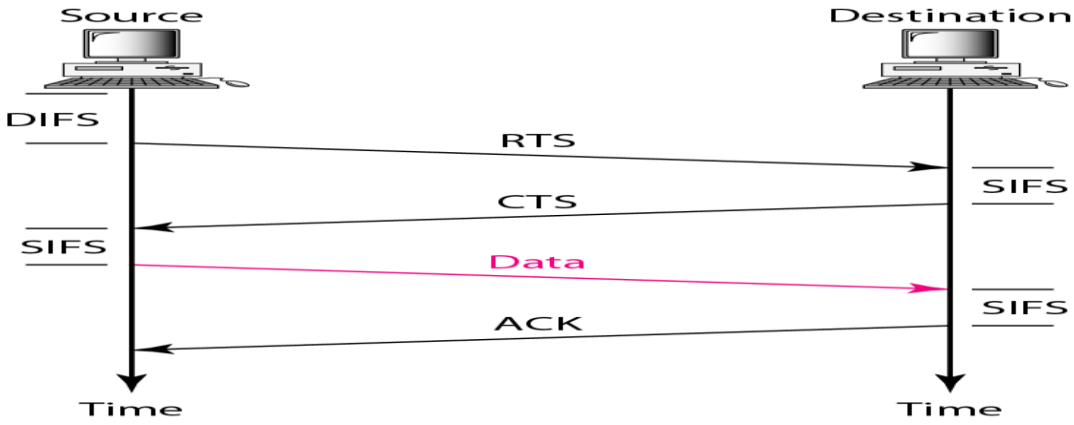
b. After the station is found to be idle, the station waits for a period of time called the distributed interframe space (DIFS); then the station sends a control frame called the request to send (RTS).

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), to the source station. This control frame indicates that the destination station is ready to receive data.

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. Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination. On the other hand, the lack of collision in *CSMA/CD* is a kind of indication to the source that data have arrived.

Following figure shows the Frame Exchange Time line



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.

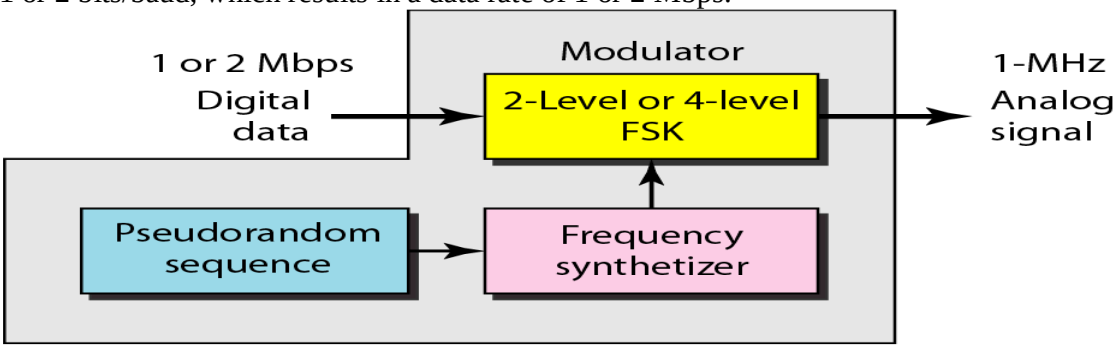


Figure: Physical layer of IEEE 802.11 FHSS

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.

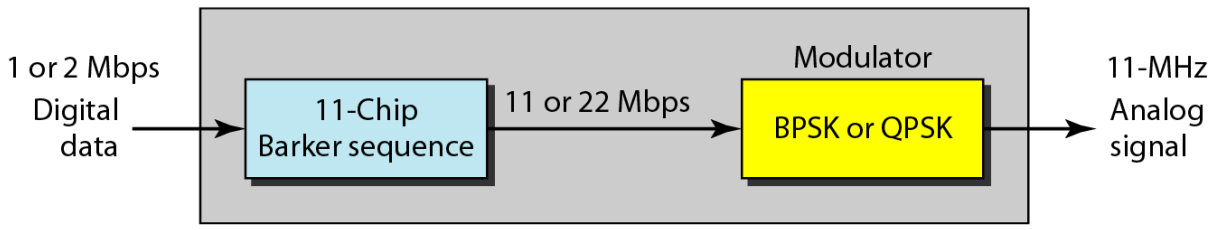
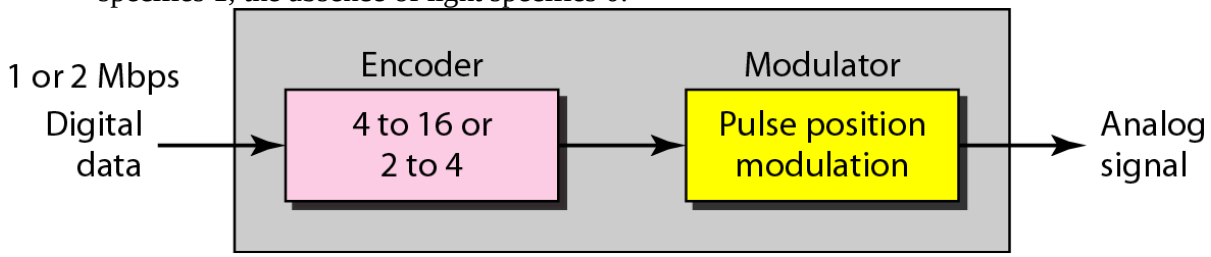


Figure: Physical layer of IEEE 802.11 DSSS

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 bit is 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 bit is 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, the absence of light specifies 0.



.

Figure: Physical layer of IEEE 802.11 infrared

IEEE 802.11A OFDM:

- IEEE 802.11a OFDM describes the orthogonal frequency-division multiplexing (OFDM) method for signal 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.
- Dividing the band into subbands diminishes the effects of interference.
- If the subbands are used randomly, security can also be increased.
- OFDM uses PSK and QAM for modulation. The common data rates are 18 Mbps (PSK) and 54 Mbps (QAM).

IEEE 802.11b DSSS:

- IEEE 802.11 b DSSS describes the high-rate direct sequence spread spectrum (HRDSSS) method for signal generation in the 2.4-GHz ISM band.
- HR-DSSS is similar to DSSS except for the encoding method, which is called complementary code keying (CCK).
- CCK encodes 4 or 8 bits to one CCK symbol. To be backward compatible with DSSS, HR-DSSS defines four data rates: 1,2, 5.5, and 11 Mbps.
- The first two use the same modulation techniques as DSSS. The 5.5-Mbps version uses BPSK and transmits at 1.375 Mbaud/s with 4-bit CCK encoding. The II-Mbps version uses QPSK and transmits at 1.375 Mbps with 8-bit CCK encoding.

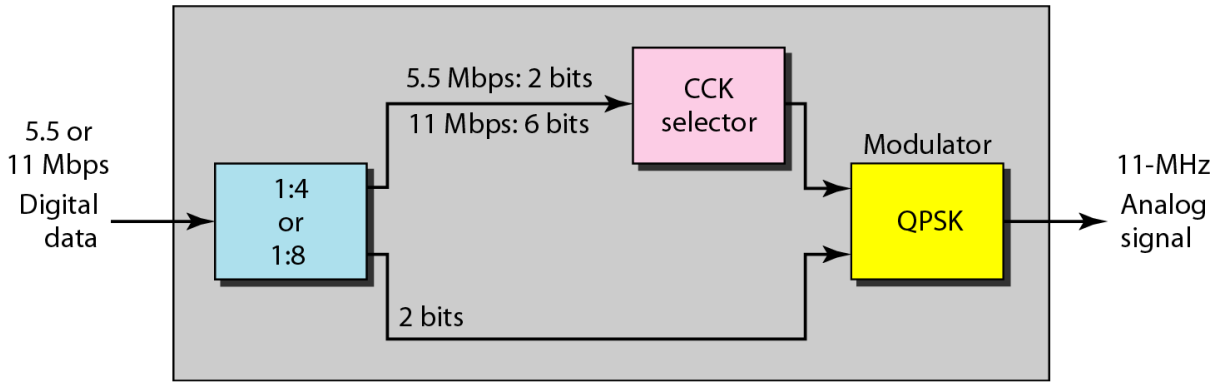


Figure: ***Physical layer of IEEE 802.11b***

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 with 802.11b, but the modulation technique is OFDM.

Frame Structure

The 802.11 standard defines three different classes of frames on the wire: data, control, and management. Each of these has a header with a variety of fields used within the MAC sublayer.
The format of the data frame is shown in Fig. First comes the Frame Control field. It itself has 11 subfields. The first of these is the Protocol version, which allows two versions of the protocol to operate at the same time in the same cell. Then come the Type (data, control, or management) and Subtype fields (e.g., RTS or CTS). The To DS and From DS bits indicate the frame is going to or coming from the intercell distribution system (e.g., Ethernet). The MF bit means that more fragments will follow. The Retry bit marks a retransmission of a frame sent earlier. The Power management bit is used by the base station to put the receiver into sleep state or take it out of sleep state. The More bit indicates that the sender has additional frames for the receiver. The W bit specifies that the frame body has been encrypted using the WEP (Wired Equivalent Privacy) algorithm. Finally, the O bit tells the receiver that a sequence of frames with this bit on must be processed strictly in order.

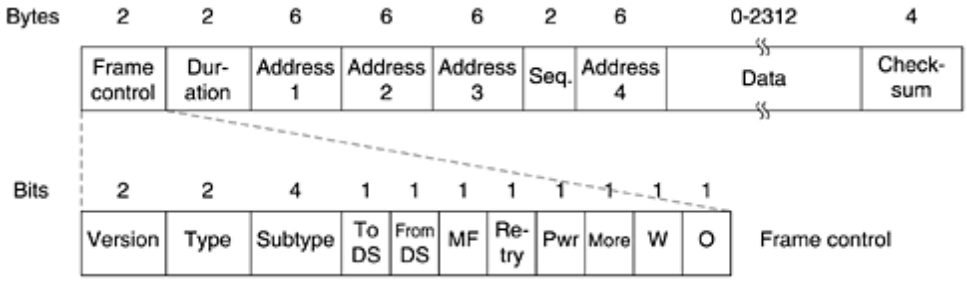


Figure The 802.11 data frame.

The second field of the data frame, the Duration field, tells how long the frame and its acknowledgement will occupy the channel. This field is also present in the control frames and is how other stations manage the NAV mechanism. The frame header contains four addresses, all in standard IEEE 802 format. The source and destination are obviously needed, but what are the other two for? Remember that frames may enter or leave a cell via a base station. The other two addresses are used for the source and destination base stations for intercell traffic.
The **Sequence** field allows fragments to be numbered. Of the 16 bits available, 12 identify the frame and 4 identify the fragment. The Data field contains the payload, up to 2312 bytes, followed by the usual Checksum.

Management frames have a format similar to that of data frames, except without one of the base station addresses, because management frames are restricted to a single cell. Control frames are shorter still, having only one or two addresses, no Data field, and no Sequence field. The key information here is in the Subtype field, usually RTS, CTS, or ACK.

WiMAX:

The story of wireless LAN cannot be complete without the mention of WiMAX, which stands for **W**orldwide **I**nteroperability for **M**icrowave **Acc**ess by the WiMAX Forum. The forum was formed in June 2001 to promote conformance and interoperability of the IEEE 802.16 standard, officially known as Wireless (Metropoliton Area Network) MAN. The Forum describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL". It supports point to multi-point (PMP) broadband wireless access. WiMAX can deliver a maximum of 70 Mbit/s, over a maximum distance of 70 miles (112.6 kilometers). It has some similarities to DSL in this respect, where one can either have high bandwidth or long range, but not both simultaneously. The other feature to consider with WiMAX is that available bandwidth is shared between users in a given radio sector, so if there are many active users in a single sector, each will get reduced bandwidth.