Unit-V

COMPUTER NETWORKS

Syllabus: **IEEE Standards:** data link layer, physical layer, Manchester encoding, **Standard Ethernet**: MAC Sub Layer, physical layer, **Fast Ethernet**: MAC Sub Layer, physical layer, **IEE-802.11:** Architecture, MAC sub layer, addressing mechanism, frame structure.

IEEE STANDARDS:

- The institute of electrical and electronic Engineers (IEEE) publishes several widely accepted LAN-recommended standards. These standards, collectively known as IEEE 802.
- Various IEEE 802 standards are as
  - IEEE 802.1 High Level Interface
  - IEEE 802.2 Logical Link Control(LLC)
  - IEEE 802.3 Ethernet
  - IEEE 802.4 Token Bus
  - IEEE 802.5 Token Ring
  - IEEE 802.6 Metropolitan Area Networks
  - IEEE 802.7 Broadband LANs
  - IEEE 802.8 Fiber Optic LANS
  - IEEE 802.9 Integrated Data and Voice Network
  - IEEE 802.10 Security
  - IEEE 802.11 Wireless Network

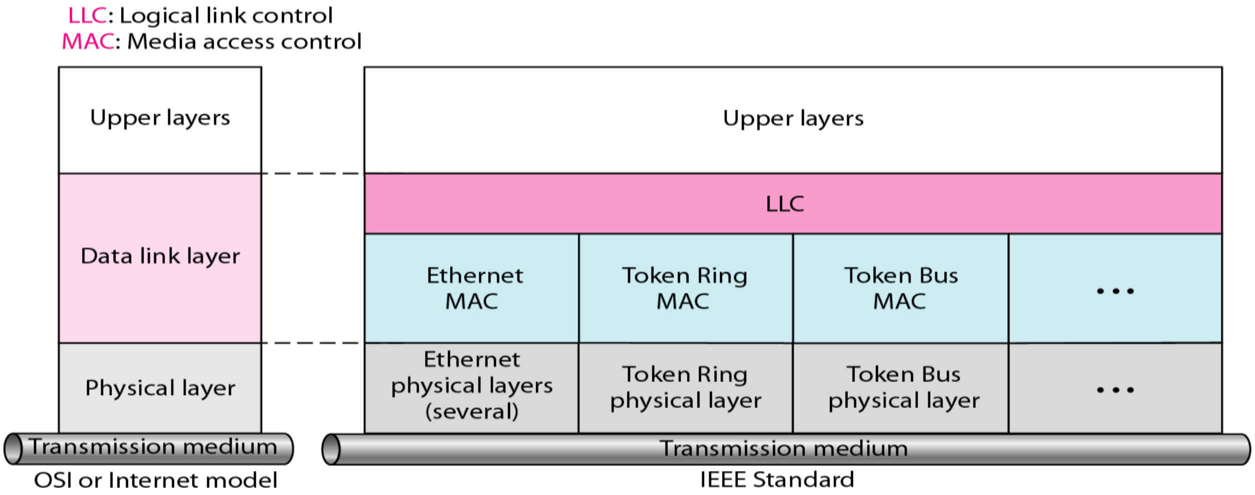


Figure: IEEE standard for LANs

Data Link Layer:

- The data link layer in the IEEE standard is divided into two sublayers: LLC and MAC.

Logical Link Control (LLC)

- Data link control handles framing, flow control, and error control.
- In IEEE Project 802, flow control, error control, and part of the framing duties are collected into one sublayer called the logical link control.
- Framing is handled in both the LLC sublayer and the MAC sublayer.
- The LLC provides one single data link control protocol for all IEEE LANs.
- A single LLC protocol can provide interconnectivity between different LANs because it makes the MAC sublayer transparent.

Framing:

- LLC defines a protocol data unit (PDU) that is somewhat similar to that of HDLC.
- The header contains a control field like the one in HDLC; this field is used for flow and error control.
- The two other header fields define the upper-layer protocol at the source and destination that uses LLC.
- These fields are called the destination service access point (DSAP) and the source service access point (SSAP).
- The other fields defined in a typical data link control protocol such as HDLC are moved to the MAC sublayer.
- In other words, a frame defined in HDLC is divided into a PDU at the LLC sublayer and a frame at the MAC sublayer, as shown in Figure.

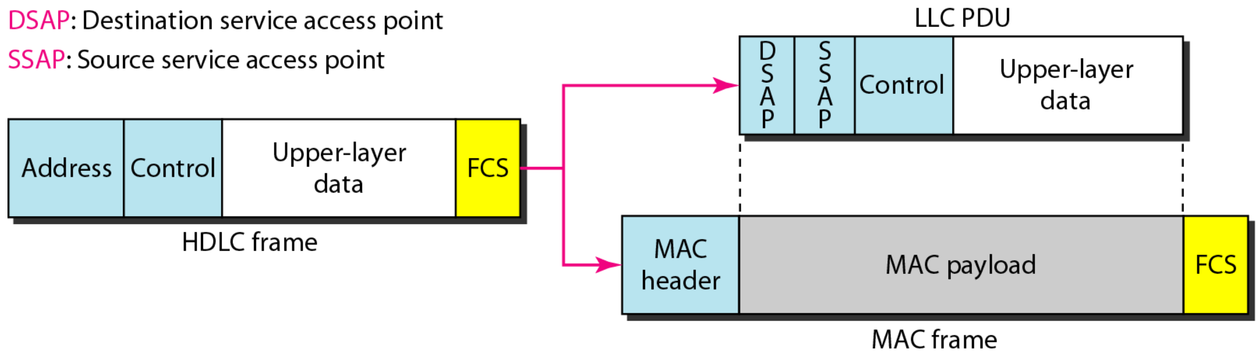


Figure: ***HDLC frame compared with LLC and MAC frames***

Media Access Control (MAC):

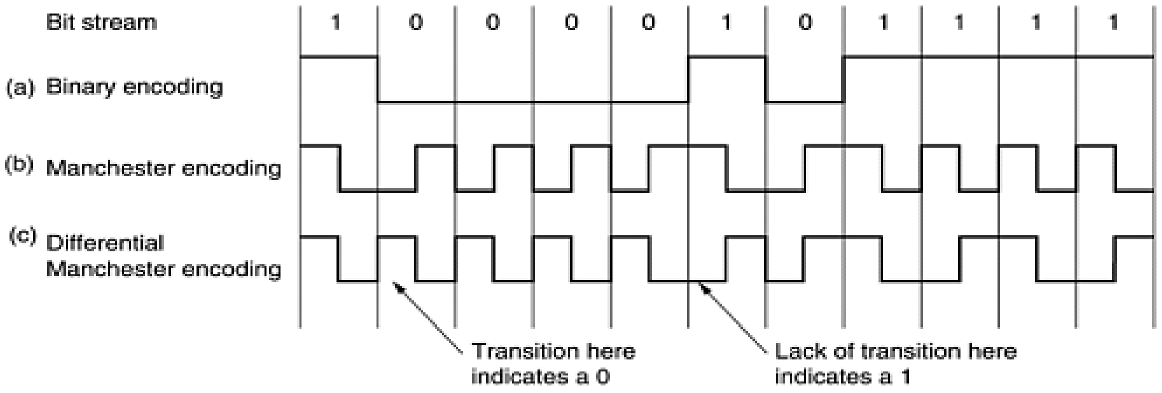
- IEEE Project 802 has created a sublayer called media access control that defines the specific access method for each LAN.
- For example, it defines CSMA/CD as the media access method for Ethernet LANs and the token passing method for Token Ring and Token Bus LANs.
- In contrast to the LLC sublayer, the MAC sublayer contains a number of distinct modules; each defines the access method and the framing format specific to the corresponding LAN protocol.

Physical Layer:

- The physical layer is dependent on the implementation and type of physical media used.
- IEEE defines detailed specifications for each LAN implementation.
- For example, although there is only one MAC sublayer for Standard Ethernet, there is a different physical layer specification for each Ethernet implementations.

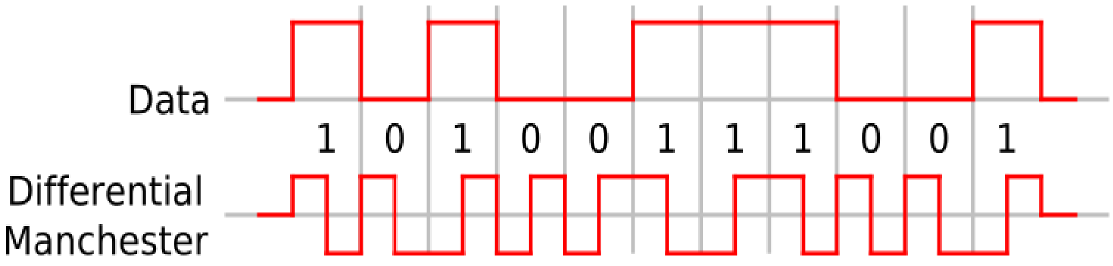
MANCHESTER ENCODING:

- Each bit period is divided into two equal intervals.
- A binary 1 bit is sent by having the voltage set high during the first interval and low in the second one.
- A binary 0 is just the reverse: first low and then high.
- This scheme ensures that every bit period has a transition in the middle, making it easy for the receiver to synchronize with the sender.
- A disadvantage of Manchester encoding is that it requires twice as much bandwidth as straight binary encoding because the pulses are half the width.
- For example, to send data at 10 Mbps, the signal has to change 20 million times/sec.


Bit stream
1 0 0 0 0 1 0 1 1 1 1
(a) Binary encoding
(b) Manchester encoding
(c) Differential Manchester encoding
Transition here indicates a 0
Lack of transition here indicates a 1

DIFFERENTIAL MANCHESTER ENCODING:

- In it, a 1 bit is indicated by the absence of a transition at the start of the interval.
- A 0 bit is indicated by the presence of a transition at the start of the interval.
- The differential scheme requires more complex equipment but offers better noise immunity. All Ethernet systems use Manchester encoding due to its simplicity.
- Ethernet does not use differential Manchester encoding, but other LANs (e.g., the 802.5 token ring) do use it.



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)**

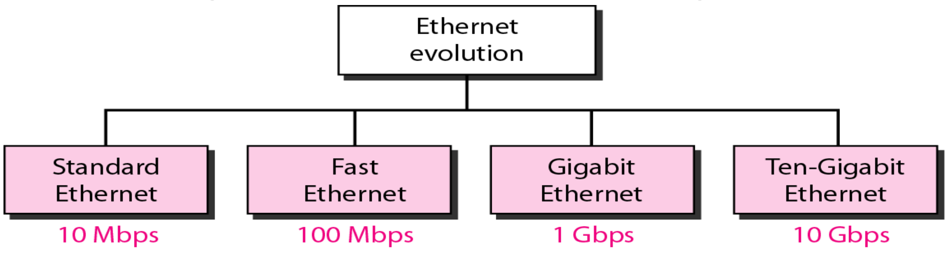


Figure: *Ethernet evolution through four generations*

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 is known as an unreliable medium. Acknowledgments must be implemented at the higher layers.

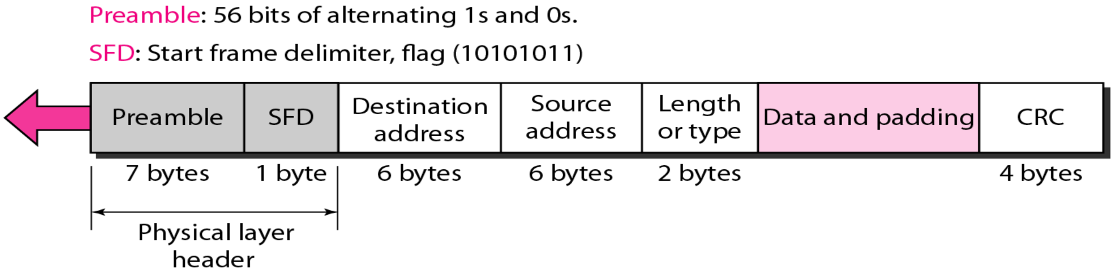


Figure: 802.3 MAC frame

- **Preamble**. The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating 0s and 1s that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The pattern provides only an alert and a timing pulse. The preamble is actually added at the physical layer and is not (formally) part of the frame.
- **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. The last 2 bits is 11 and alerts the receiver that the next field is the destination address.
- **Destination address (DA**). The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet.
- **Source address (SA).** The SA field is also 6 bytes and contains the physical address of the sender of the packet.
- **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. The IEEE standard used it as the length field to define the number of bytes in the data field. Both uses are common today.
- **Data.** This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.
- **CRC**. The last field contains error detection information, in this case a CRC-32.

Frame Length:

- Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame.

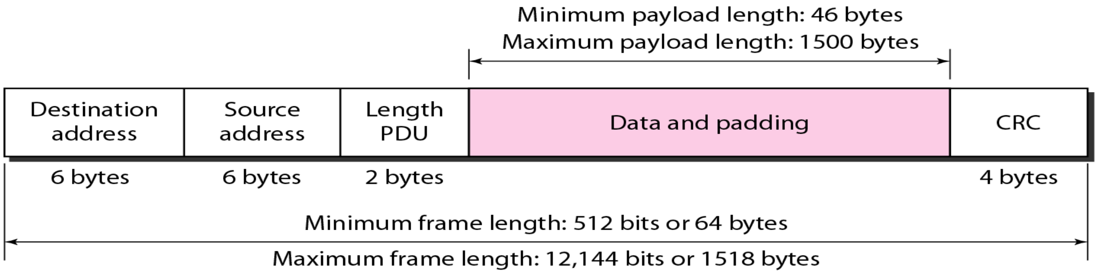

Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Destination address
Source address
Length PDU
Data and padding
CRC
6 bytes
6 bytes
2 bytes
4 bytes
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

Figure: Minimum and maximum lengths

- The minimum length restriction is required for the correct operation of *CSMA/CD*.
- An Ethernet frame needs to have a minimum length of 512 bits or 64 bytes.
- Part of this length is the header and the trailer.

- If we count 18 bytes of header and trailer (6 bytes of source address, 6 bytes of destination address, 2 bytes of length or type, and 4 bytes of CRC), then the minimum length of data from the upper layer is 64 - 18 = 46 bytes.
- If the upper-layer packet is less than 46 bytes, padding is added to make up the difference.
- The standard defines the maximum length of a frame 1518 bytes.
- If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes.

Note: Frame length: Minimum: 64 bytes (512 bits) Maximum: 1518 bytes (12,144 bits)

Addressing:

- Each station on an Ethernet network has its own network interface card (NIC).
- The NIC fits inside the station and provides the station with a 6-byte physical address. As shown in Figure, the Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.

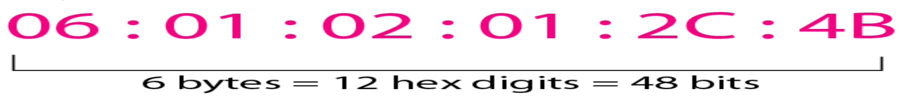

06 : 01 : 02 : 01 : 2C : 4B
6 bytes = 12 hex digits = 48 bits

Figure. Example of an Ethernet address in hexadecimal notation

Unicast, Multicast, and Broadcast Addresses:

- A source address is always a unicast address-the frame comes from only one station.
- The destination address, however, can be unicast, multicast, or broadcast.
- Figure shows how to distinguish a unicast address from a multicast address.
- If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise, it is multicast.
- A unicast destination address defines only one recipient; the relationship between the sender and the receiver is one-to-one.
- A multicast destination address defines a group of addresses; the relationship between the sender and the receivers is one-to-many.
- The broadcast address is a special case of the multicast address; the recipients are all the stations on the LAN.
- A broadcast destination address is forty-eight 1s.

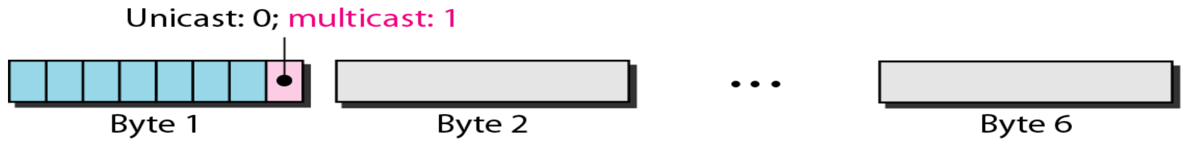


Figure: Unicast and multicast addresses

Access Method: CSMA/CD:

- Standard Ethernet uses 1-persistent CSMA/CD.
  1. Slot time = round-trip time + time required to send jam sequence
  2. Maximum length= propagation speed x slot time/2

Physical Layer:

- The Standard Ethernet defines several physical layer implementations; four of the most common, are shown in Figure

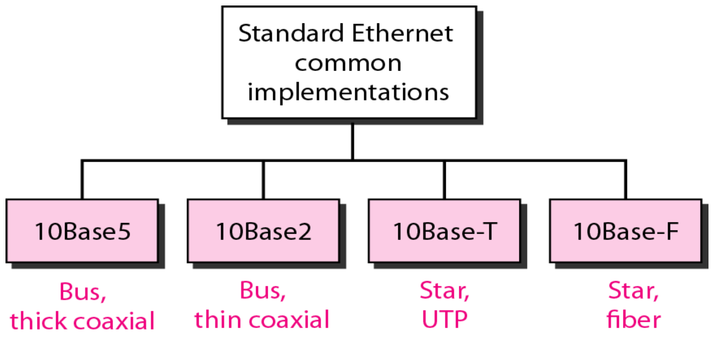


Figure: Categories of Standard Ethernet

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 for sending 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*

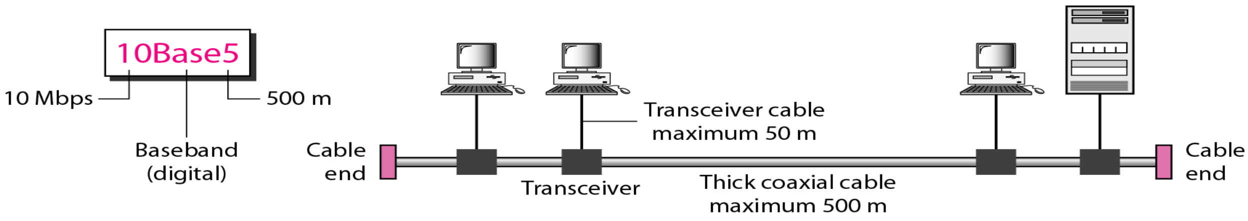


Figure: 10Base5 implementation

10Base2: Thin Ethernet:

- 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 installed inside the station.

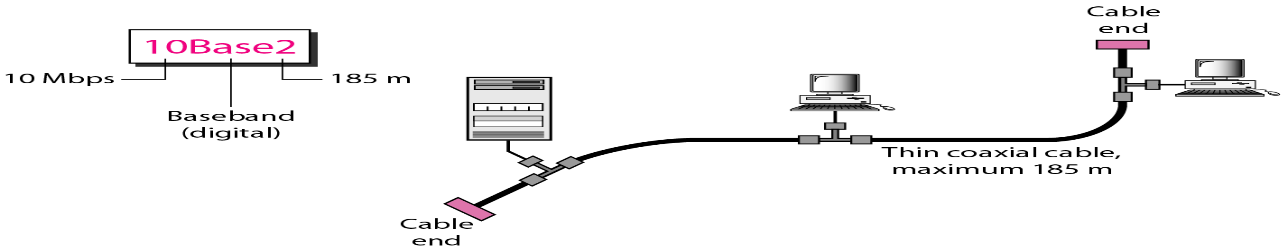


Figure: 10Base2 implementation

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 the station 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 far as 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.

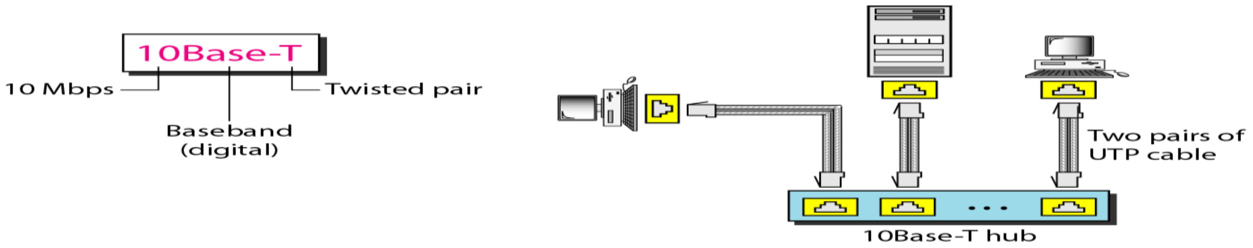


Figure: 10Base-T implementation

10Base-F: Fiber Ethernet:

- Although there are several types of optical fiber 10-Mbps Ethernet, the most common is called 10Base-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

Table: Summary of Standard Ethernet implementations

CHANGES IN THE STANDARD:

Bridged Ethernet:

- The first step in the Ethernet evolution was the division of a LAN by bridges.
- Bridges have two effects on an Ethernet LAN:
  1. They raise the bandwidth
  2. They separate collision domains.
- Without bridges, all the stations share the bandwidth of the network.

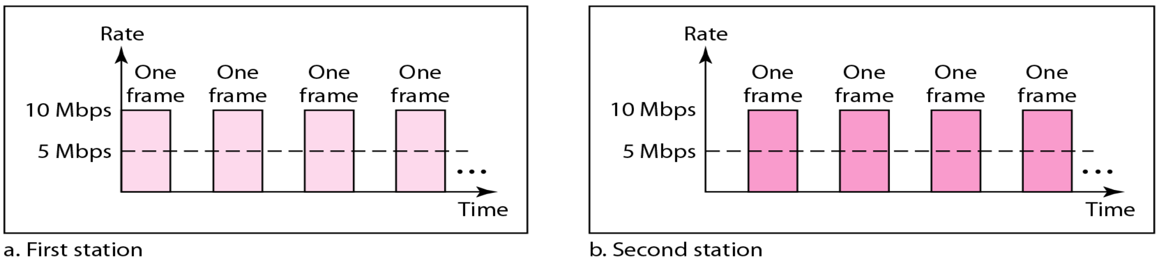


Figure: Sharing bandwidth

Bridged Ethernet: Raising the Bandwidth

- Bridges divide the network into two.
- Each network is independent.
- With bridges, 10 Mbps network is shared only by 6 [actually 7 as bridge acts as one station] stations.

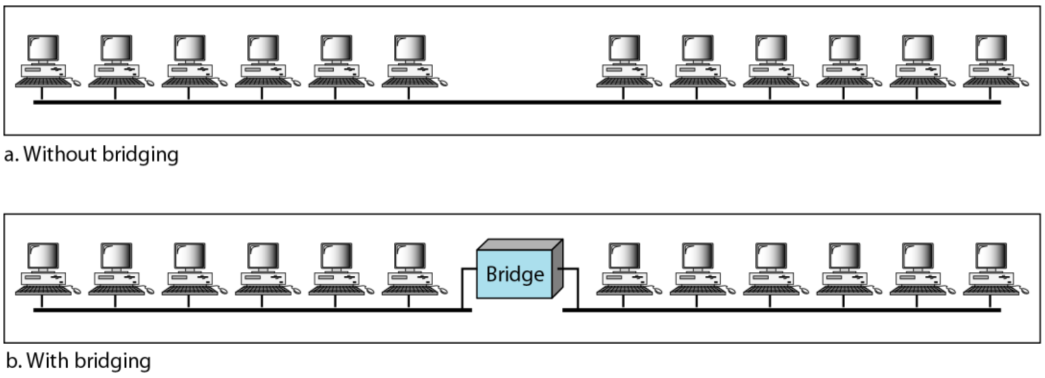


Figure: A network with and without a bridge

Bridged Ethernet: Separate Collision domains

- Collision domain becomes much smaller and the probability of collision is reduced.

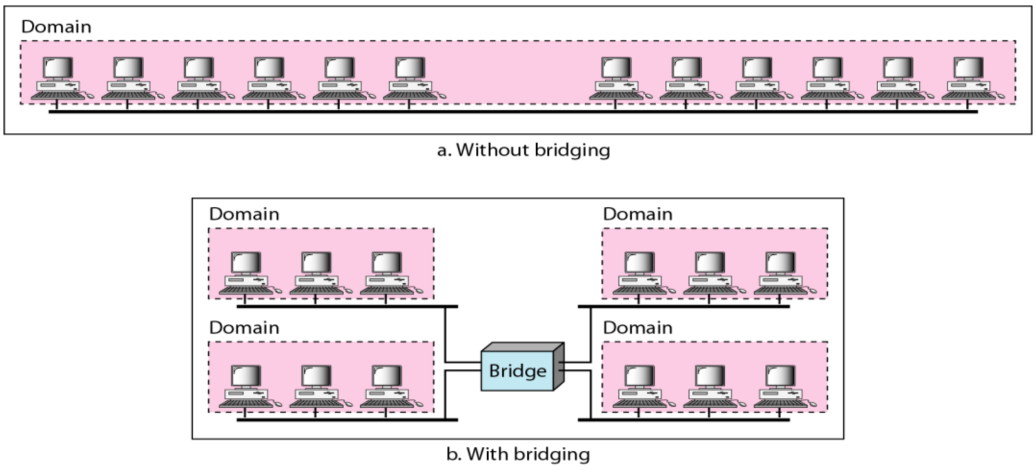


Figure: Collision domains in an unbridged network and a bridged network

Switched Ethernet:

- A network switch is a small hardware device that joins multiple computers together within one local area network.

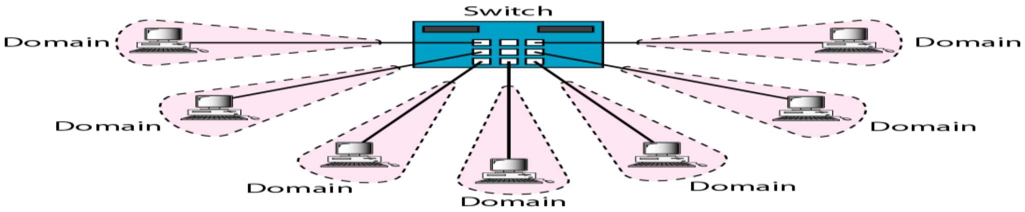


Figure: Switched Ethernet

Full-Duplex Ethernet:

- In full duplex switch there are two links, one for sending and one for receiving,
- We don't need CSMA/CD here (no collision).
- Increases the capacity of each domain from 10 to 20 Mbps.

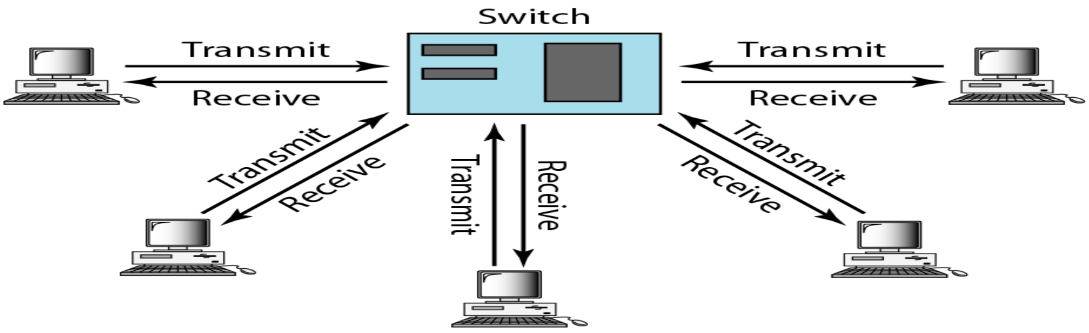


Figure: Full-duplex switched Ethernet

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 faster at 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:

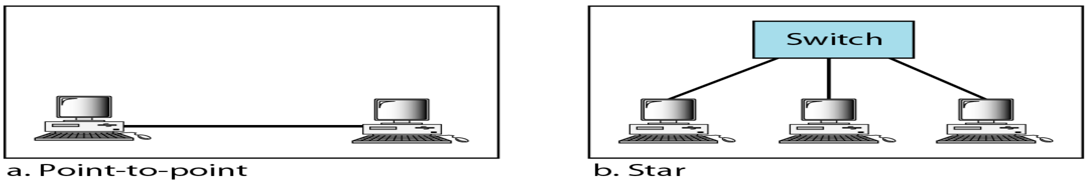
- A new feature added to Fast Ethernet is called autonegotiation.
- It allows a station or a hub a range of capabilities.
- Autonegotiation allows two devices to negotiate the mode or data rate of operation.
- It was designed particularly for the following purposes:
  1. To allow incompatible devices 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.



a. Point-to-point

b. Star

Figure: Fast Ethernet topology

Fast Ethernet implementations:

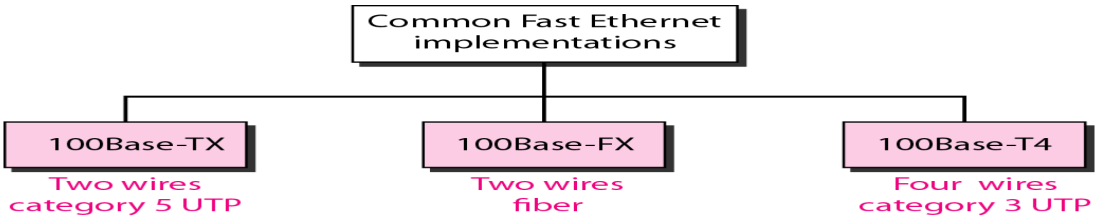


Figure: Fast Ethernet implementations

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.

<u>100Base-FX:</u>

- ➢ 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 5 UTP or STP cable. It is cost effective.

<u>100Base-T4:</u>

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

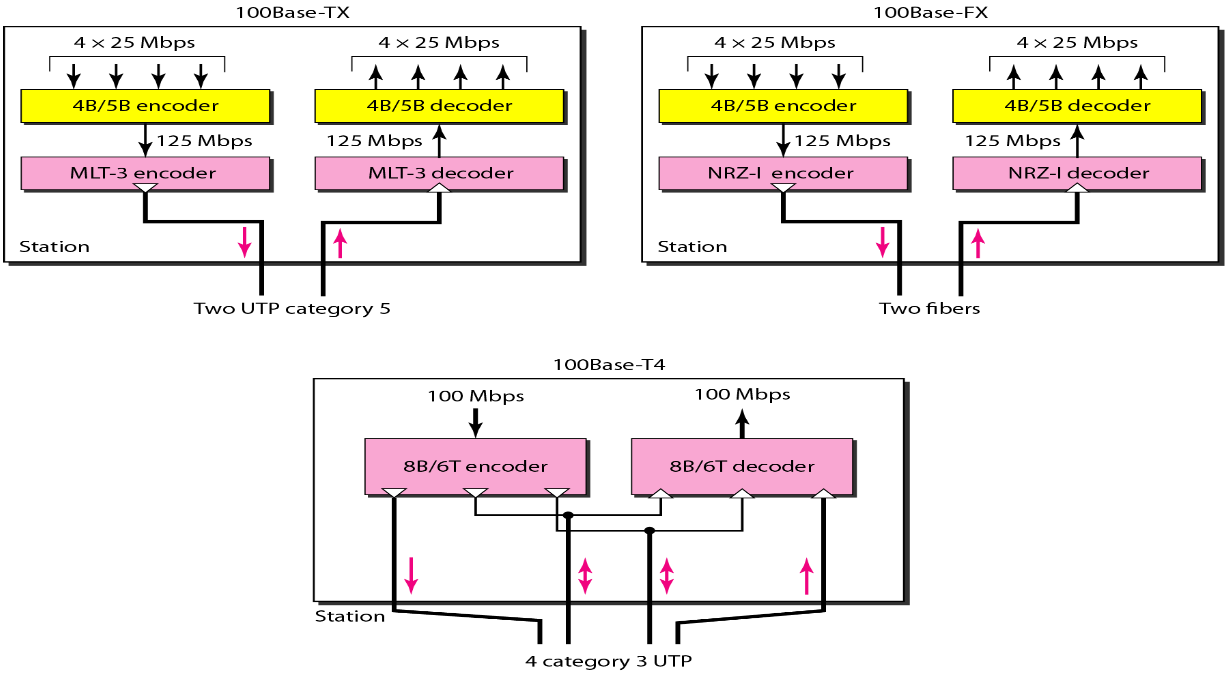
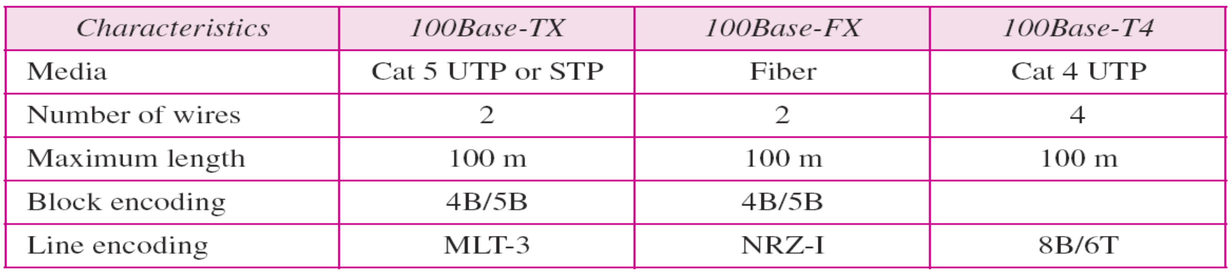


Figure: Encoding for Fast Ethernet implementation



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	100 m	100 m	100 m
Block encoding	4B/5B	4B/5B	
Line encoding	MLT-3	NRZ-I	8B/6T

Table: ***Summary of Fast Ethernet implementations***

<u>GIGABIT ETHERNET:</u>

- ➢ 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.

<u>The goals of the Gigabit Ethernet</u>

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

<u>Ten-Gigabit Ethernet:</u>

- ➢ The IEEE committee created Ten-Gigabit Ethernet and called it Standard 802.3ae.

<u>The goals of the Ten-Gigabit Ethernet</u>

- Upgrade the data rate to 10 Gbps.
- Make it compatible with Standard, Fast, and Gigabit Ethernet.
- Use the same 48-bit address.
- Use the same frame format.
- Keep the same minimum and maximum frame lengths.

- Allow the interconnection of existing LANs into a metropolitan area network (MAN) or a wide area network (WAN).
- Make Ethernet compatible with technologies such as Frame Relay and ATM.

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**.

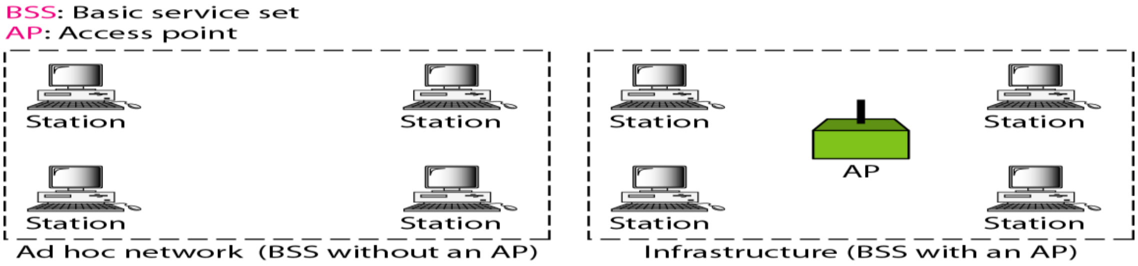


FIGURE: BASIC SERVICE SETS (BSSS)

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.

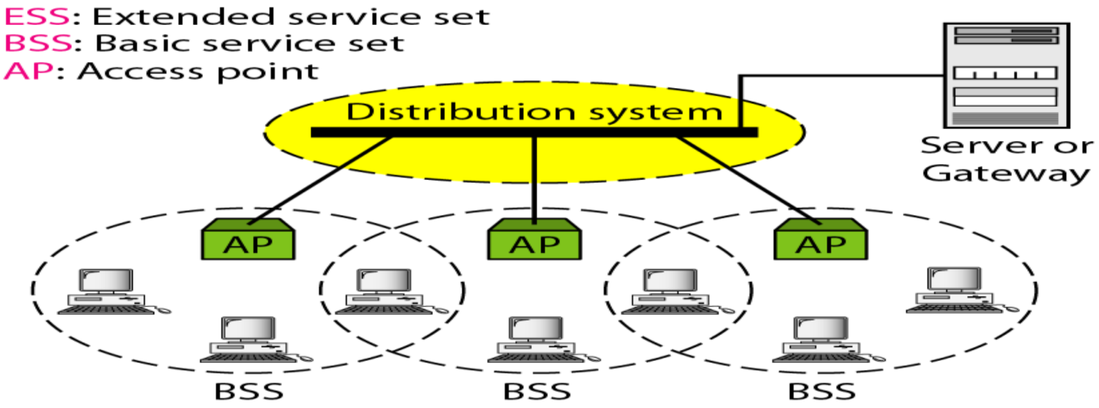


Figure: Extended service sets (ESSs)

- 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:
    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 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).

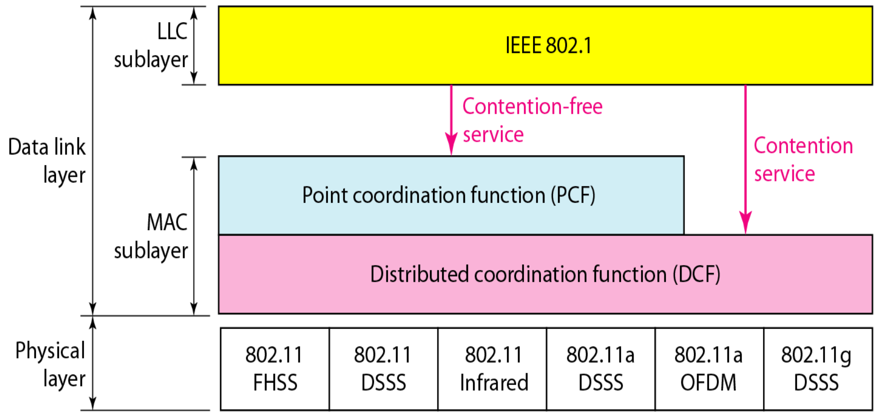
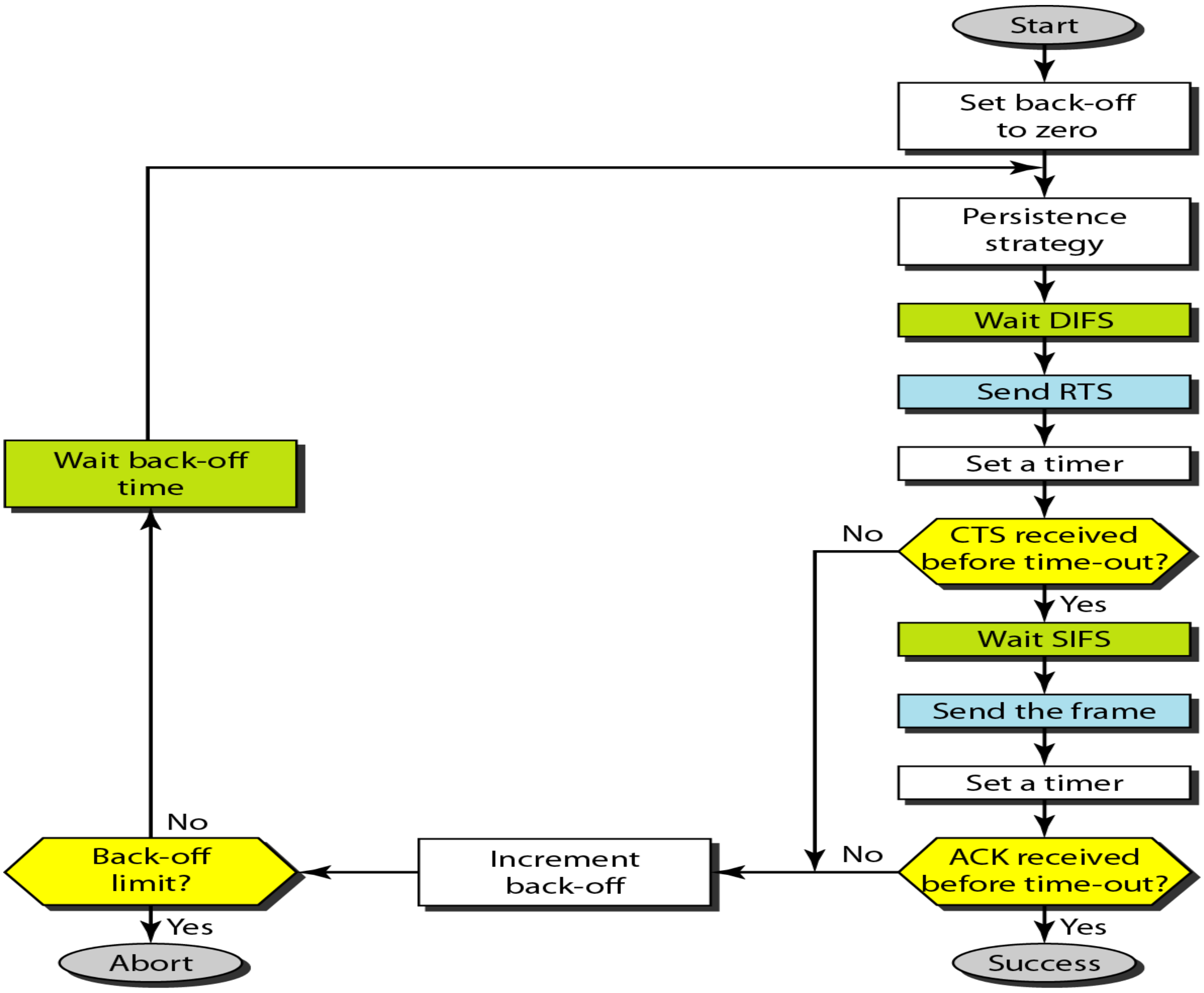


Figure: MAC layers in IEEE 802.11 standard

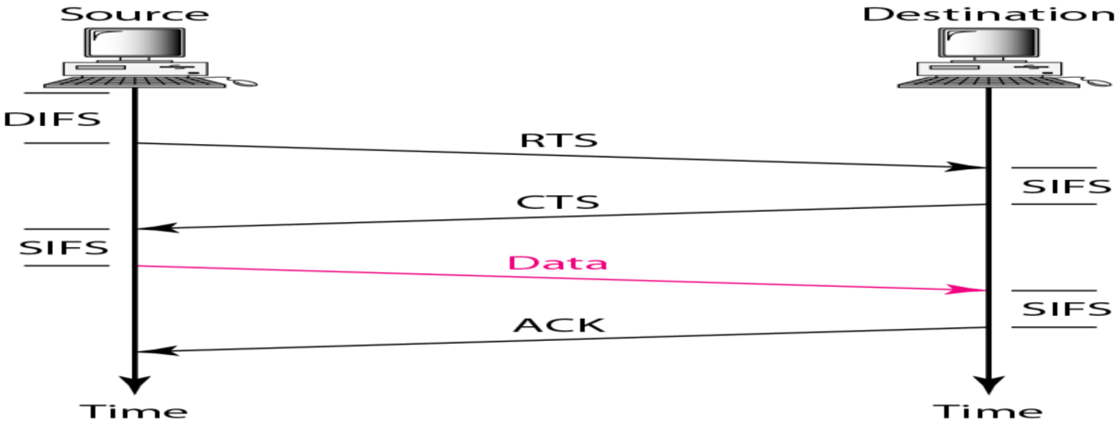
Distributed Coordination Function:

- 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.



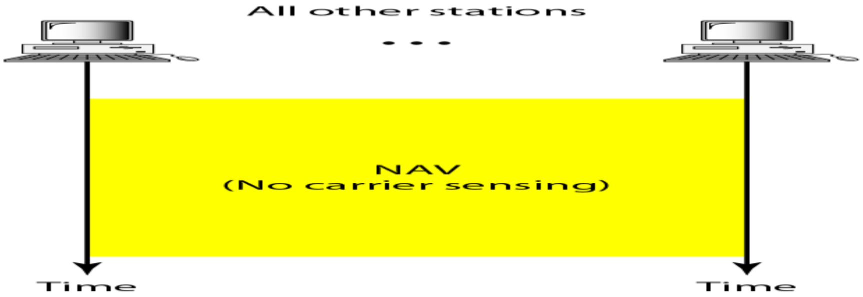
1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.
   a. The channel uses a persistence strategy with back-off until the channel is idle.
   b. After the station is found to be idle, the station waits for a period of time called the 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



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 shows how much time must pass before these stations are allowed to check the channel for idleness.
- 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 a collision 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) and contention-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-free period of the repetition interval.

Frame Format:

- The MAC layer frame consists of nine fields

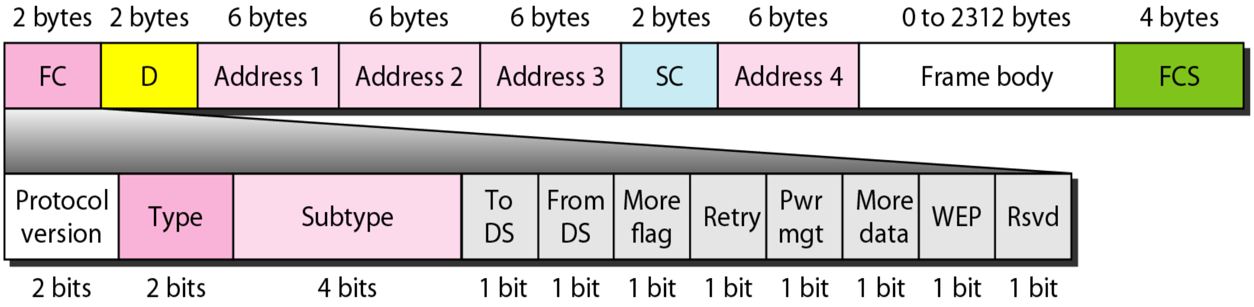
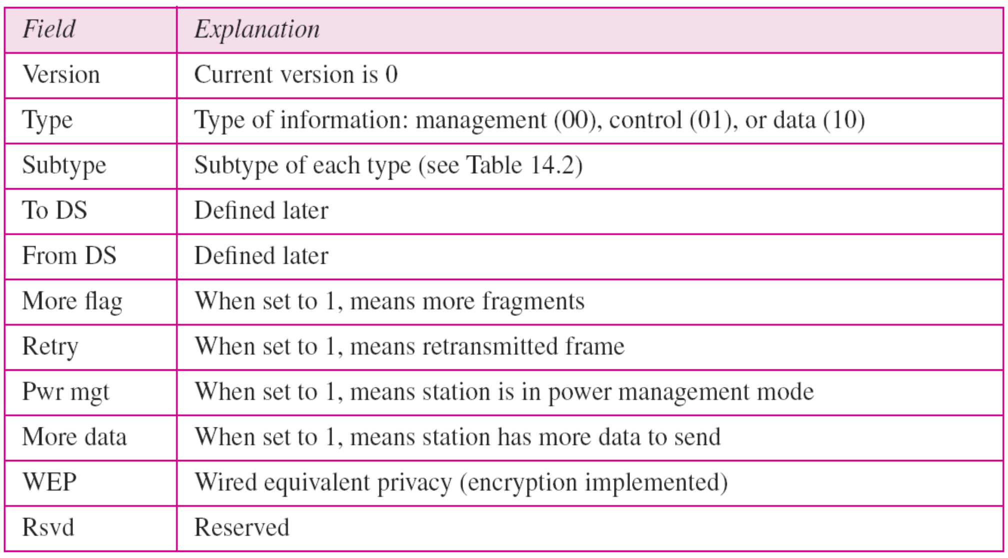


Figure: Frame format

- ✓ **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 set the 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 field depends 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 the type 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.

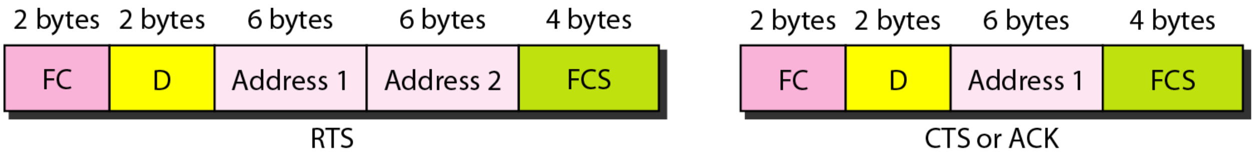
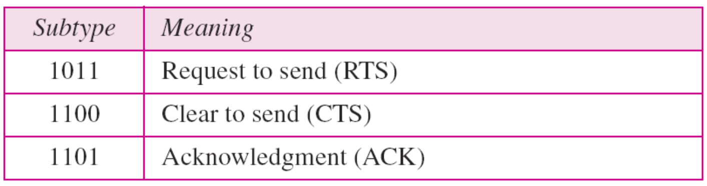


Figure: Control frames

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

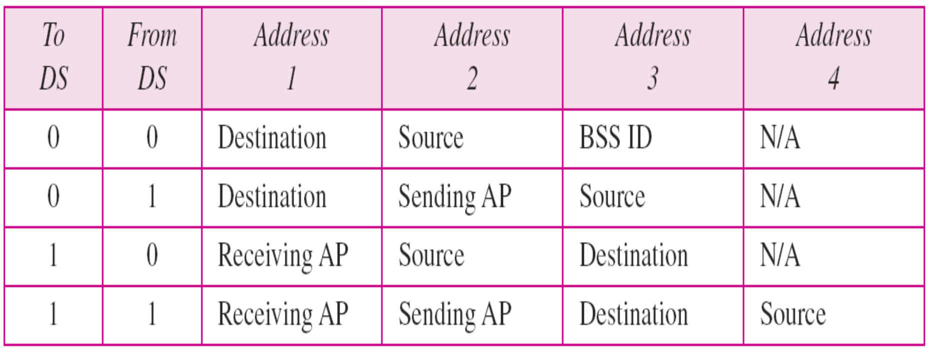


Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

Table: Values of subfields in control frames

Addressing Mechanism:

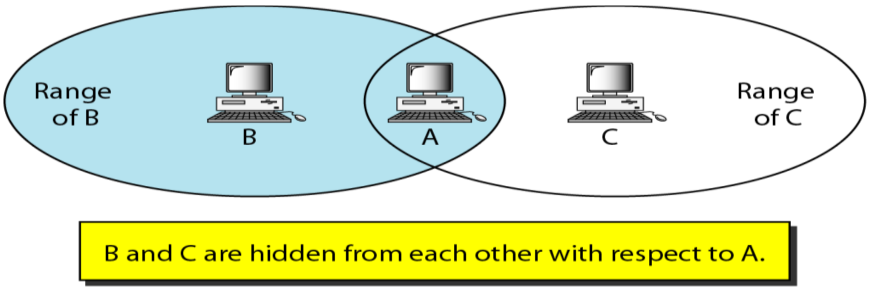
- The IEEE 802.11 addressing mechanism specifies four cases, defined by the value of the two flags in the FC field, To DS and From DS.
- Each flag can be either 0 or 1, resulting in four different situations.
- The interpretation of the four addresses (address 1 to address 4) in the MAC frame depends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



B and C are hidden from each other with respect to A.

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 located in 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 of the 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.

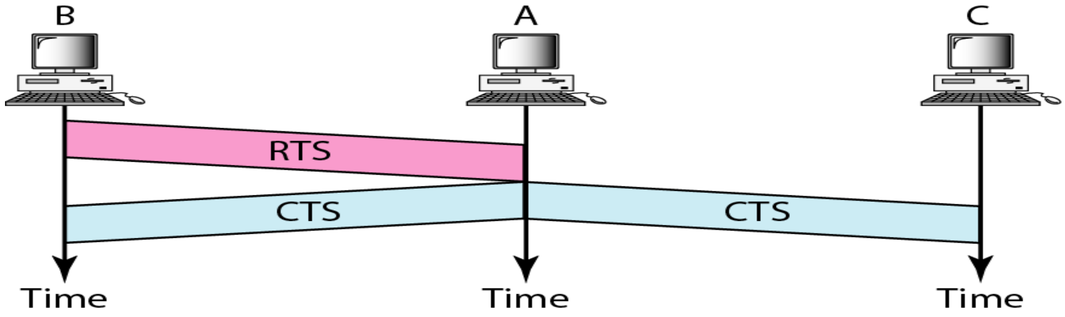


Figure: Use of handshaking to prevent hidden station problem

Exposed Station Problem:

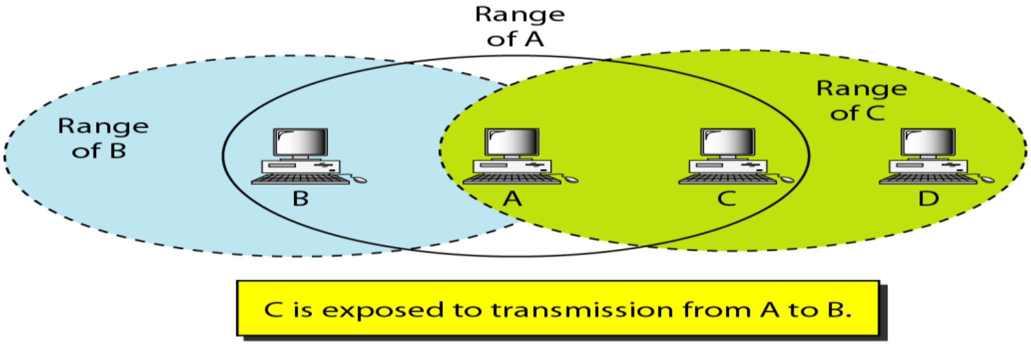


Figure: Exposed station problem

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 from A, 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 its data to D. It remains exposed until A finishes sending its data as Following Figure shows.

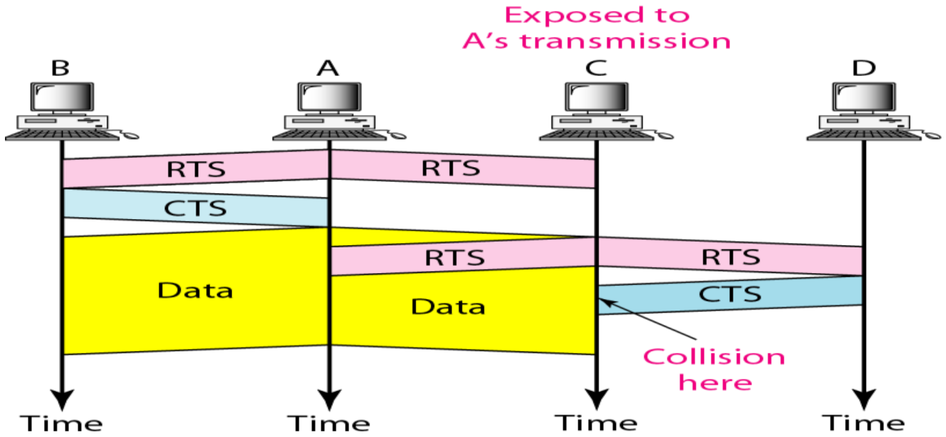


Figure: Use of handshaking in exposed station problem

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*

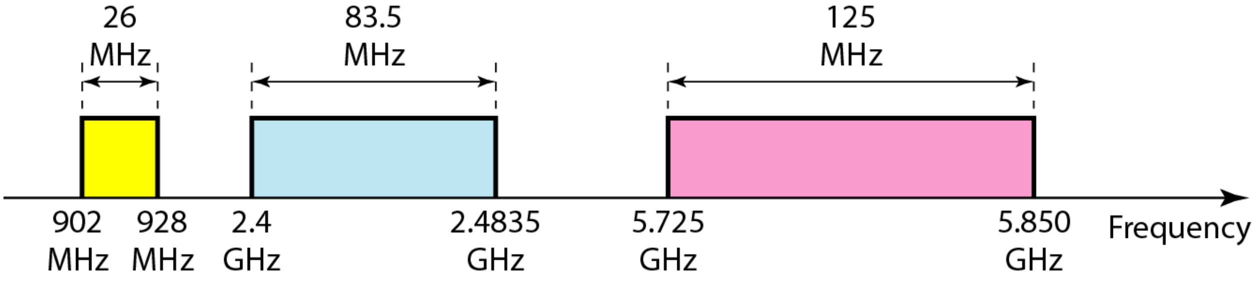


Figure: Industrial, scientific, and medical (ISM) band

<u>IEEE 802.11 FHSS:</u>

- 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.

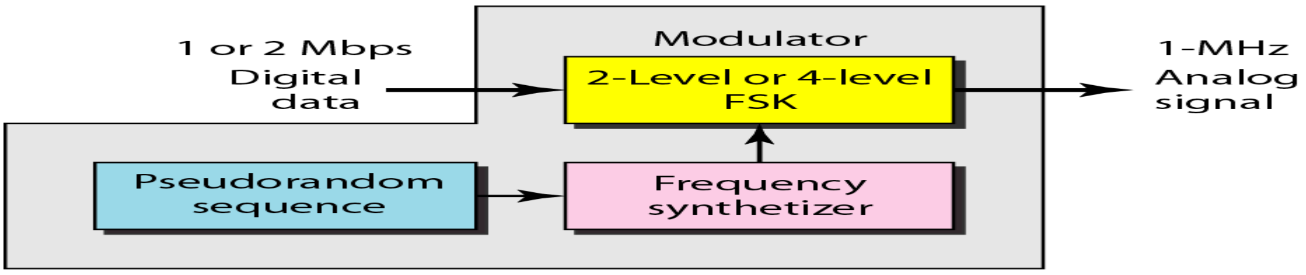


Figure: Physical layer of IEEE 802.11 FHSS

<u>IEEE 802.11 DSSS:</u>

- 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.

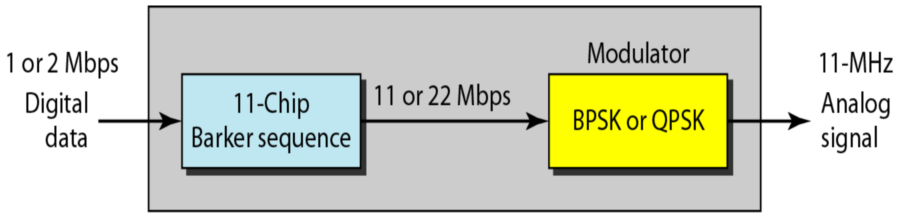


Figure: Physical layer of IEEE 802.11 DSSS

<u>IEEE 802.11 Infrared:</u>

- 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.

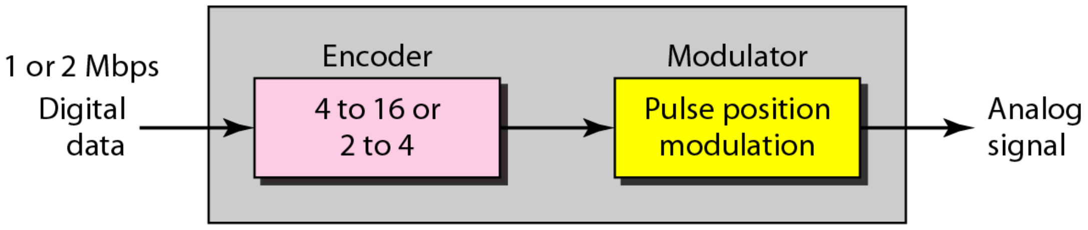


Figure: Physical layer of IEEE 802.11 infrared

<u>IEEE 802.11A OFDM:</u>

- 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).

<u>IEEE 802.11b DSSS:</u>

- 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.

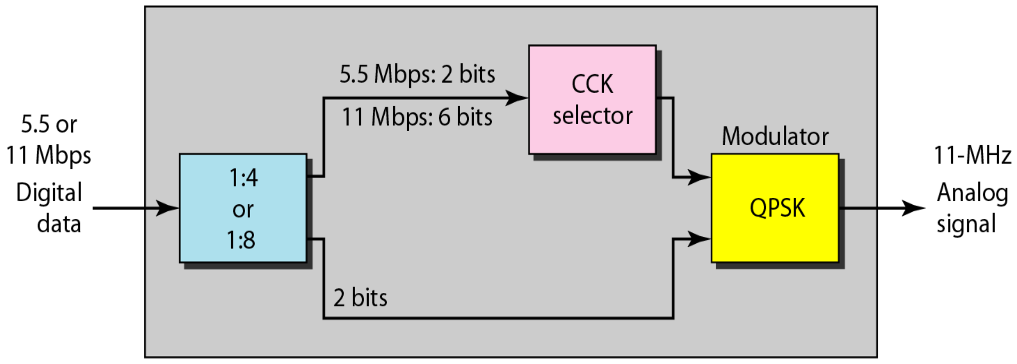


Figure: ***Physical layer of IEEE 802.11b***

IEEE 802.11g:

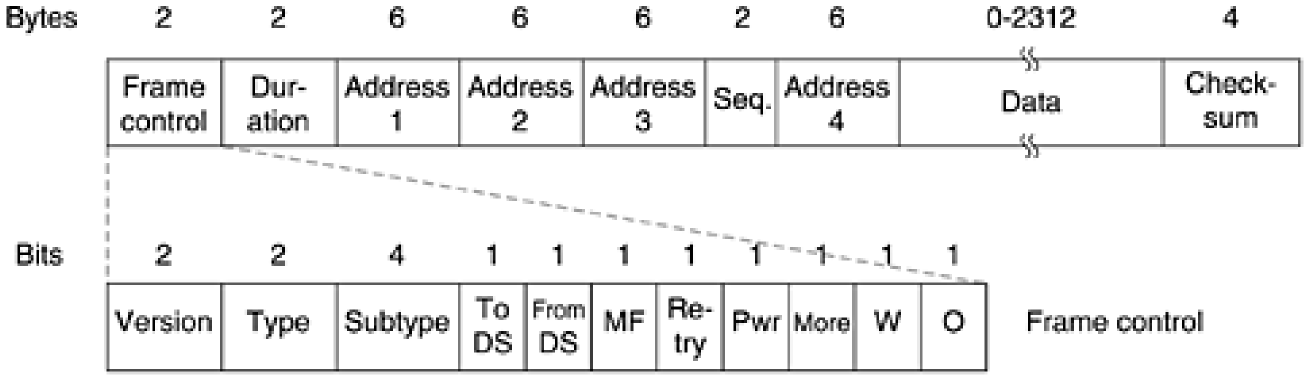
- This new specification defines forward error correction and OFDM using the 2.4-GHz ISM band.
- The modulation technique achieves a 22- or 54-Mbps data rate. It is backward compatible with 802.11b, but the modulation technique is OFDM.

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.



Bytes	2	2	6	6	6	2	6	0-2312	4
	Frame control	Dur-ation	Address 1	Address 2	Address 3	Seq.	Address 4	Data	Check-sum

Bits	2	2	4	1	1	1	1	1	1	1	1	
	Version	Type	Subtype	To DS	From DS	MF	Re-try	Pwr	More	W	O	Frame control

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.