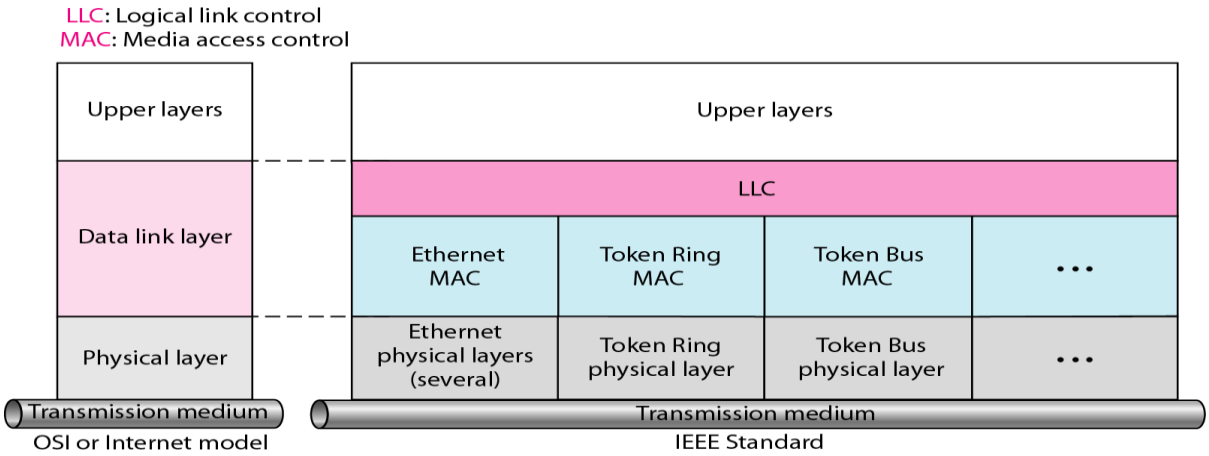
Ethernet

IEEE Standards

The relationship of the 802 Standard to the traditional OSI model is shown in the figure. The IEEE has subdivided the data link layer into two sublayers: logical link control (LLC) and media access control (MAC). IEEE has also created several physical layer standards for different LAN protocols.



Data Link Layer

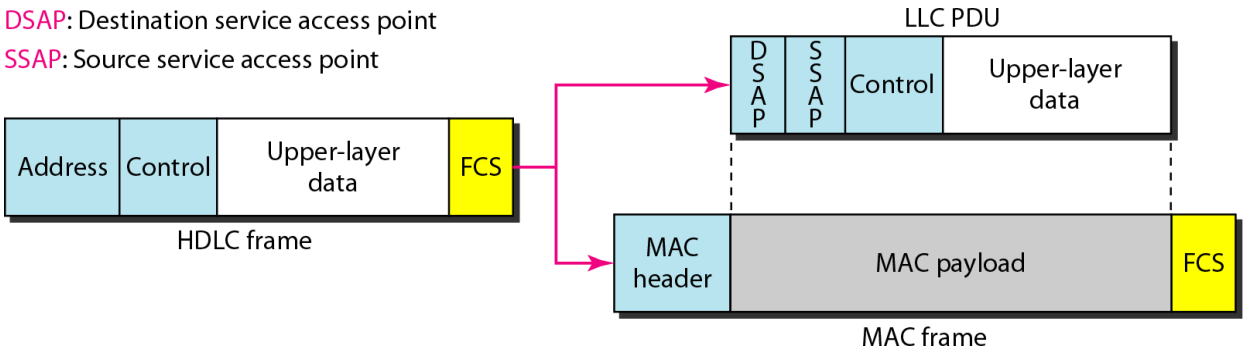
The data link layer in the IEEE standard is divided into two sublayers: LLC and MAC.

Logical Link Control (LLC) ***- flow control, error control, part of framing.*** *Provides one single data link control for all IEEE LANs*

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).
- 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.

FCS: Frame Check Sequence: Contains CRC-32 Error Detection sequence



Need for LLC The purpose of the LLC is to provide flow and error control for the upper-layer protocols that actually demand these services.

For example, if a LAN or several LANs are used in an isolated system, LLC may be needed to provide flow and error control for the application layer protocols.

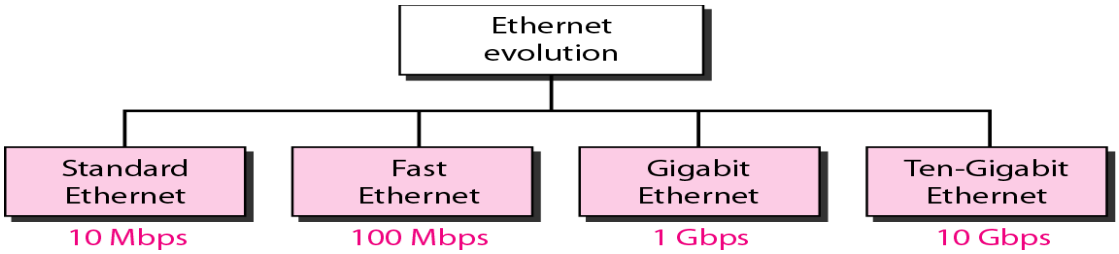
Media Access Control (MAC) *- Defines the specific access method for each type of LAN (Ethernet–CSMA/CD, Token Ring and Token Bus-Token Passing). Provides part of framing function.*

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.

4.1 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 (10 t Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps), and Ten-Gigabit Ethernet (10 Gbps), as shown in the figure:

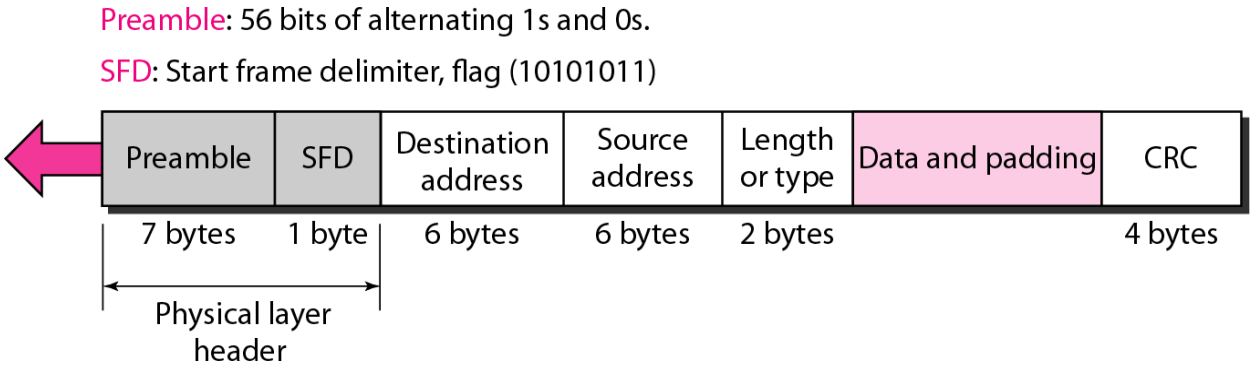


MAC Sublayer

In Standard Ethernet, the MAC sublayer governs the operation of the access method. It also frames data received from the upper layer and passes them to the physical layer.

Frame Format

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. The format of the MAC frame is shown in the figure.

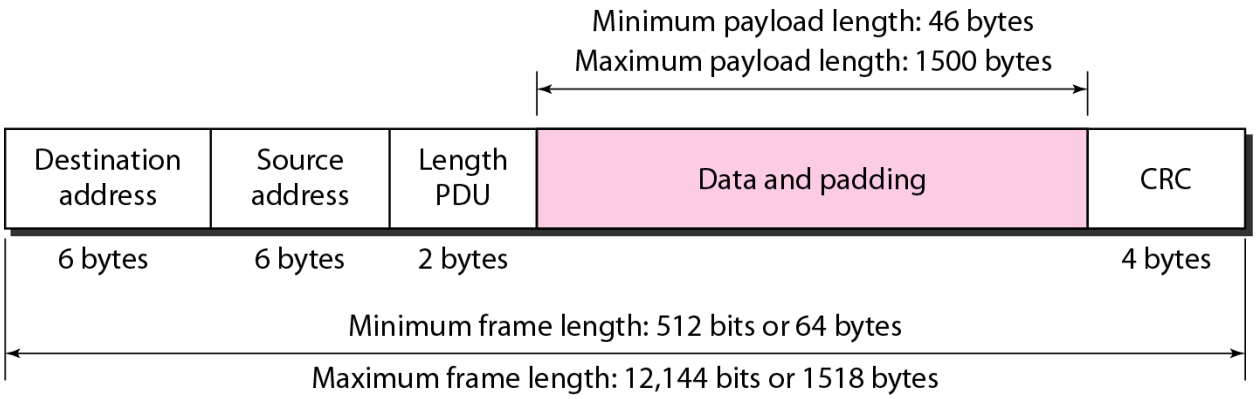


- **Preamble**. The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating 0s and 1s that alerts the receiving system to the coming frame and enables it to synchronize its input timing.
- **Start frame delimiter (SFD).** The second field (1 byte: 10101011) signals the beginning of the 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**. Define upper layer protocol, length: the number of bytes in data field Data. 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, as shown in figure.



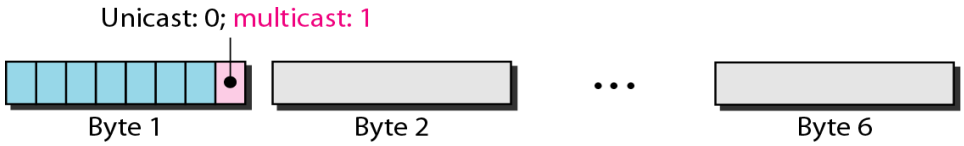
Addressing

- Each station on an Ethernet network (such as a PC, workstation, or printer) 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 the figure, the Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.

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.

The following 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 one4o-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 ls.

Access Method: CSMA/CD

Standard Ethernet uses 1-persistent CSMA/CD

Slot Time In an Ethernet network, the round-trip time required for a frame to travel from one end of a maximum-length network to the other plus the time needed to send the jam sequence is called the slot time.

Slot time = round-trip time + time required to send the jam sequence

The slot time in Ethernet is defined in bits. It is the time required for a station to send 512 bits. This means that the actual slot time depends on the data rate; for traditional 10-Mbps Ethernet it is 51.2µs.

Slot Time and Collision The choice of a 512-bit slot time was not accidental. It was chosen to allow the proper functioning of CSMA/CD.

Slot Time and Maximum Network Length There is a relationship between the slot time and the maximum length of the network (collision domain). It is dependent on the propagation speed of the signal in the particular medium.

In most transmission media, the signal propagates at 2x 10^8 m/s (two-thirds of the rate for propagation in air). For traditional Ethernet, we calculate

$$\text{MaxLength} = \text{PropagationSpeed} \times \frac{\text{SlotTime}}{2}$$

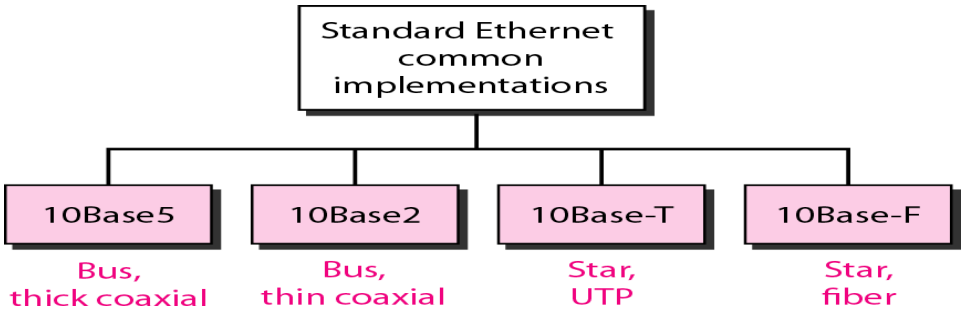
$$\text{MaxLength} = (2 \times 10^8) \times (51.2 \times 10^{-6} / 2) = 5120 \text{ m}$$

Of course, we need to consider the delay times in repeaters and interfaces, and the time required to send the jam sequence. These reduce the maximum-length of a traditional Ethernet network to 2500 m, just 48 percent of the theoretical calculation.

MaxLength = 2500 m

Physical Layer

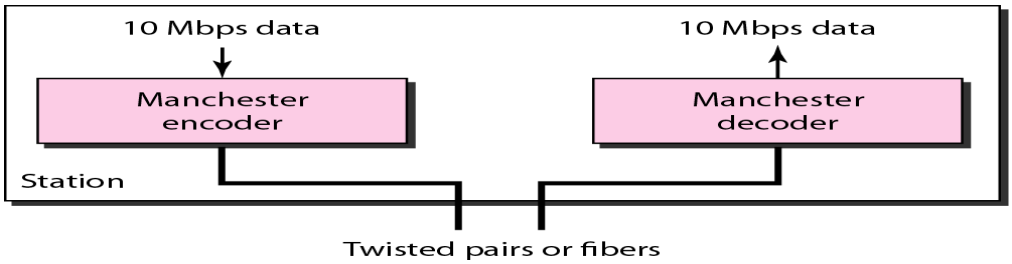
The Standard Ethernet defines several physical layer implementations; four of the most common, are shown in figure.



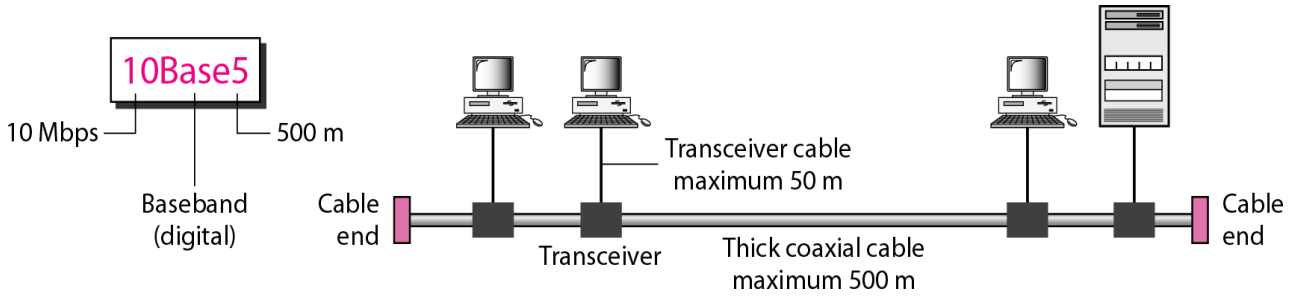
Encoding and Decoding

At the **sender,** data are converted to a digital signal using the Manchester scheme; at the **receiver**, the received signal is interpreted as Manchester and decoded into data.

The figure shows the encoding scheme for Standard Ethernet.



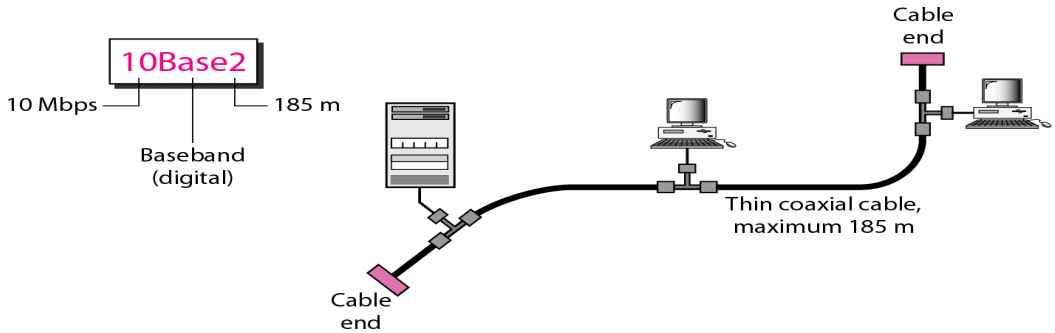
10Base5: Thick Ethernet



- Known as Thicknet
- Thick coaxial cable
- Uses bus topology with external transceiver: transceiver is responsible for transmitting, receiving, and detecting collisions.
- Max length of each segment 500m

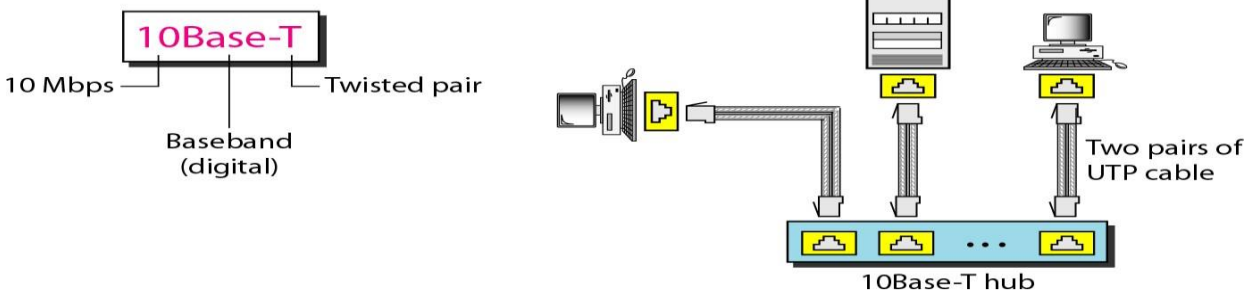
10Base2: Thin Ethernet

- Knows as Thin Ethernet
- Uses bus topology with thin and more flexible cable
- Uses internal Transceiver – part of NIC(network interface card) which is installed inside the station.
- Max length of each segment 185m due to the high level of attenuation in thin coaxial cable.
- This implementation is more cost effective than 10Base5 because thin coaxial cable is less expensive than thick coaxial and the tee connections are much cheaper than taps.



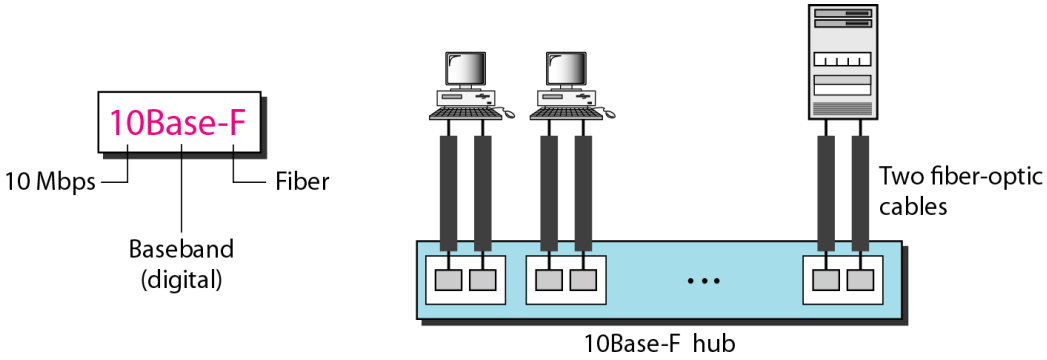
10Base- T: Twisted-Pair Ethernet

- Knows as twisted pair Ethernet
- Uses physical star topology
- Stations connected to hub via two pairs of twisted cable.
- Max length 100m
- Collision here happens in the hub.



10Base-F: Fiber Ethernet

- 10Base-F uses a star topology to connect stations to a hub.
- The stations are connected to the hub using two fiber-optic cables.



Summary of Standard Ethernet implementations

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

4.2 CHANGES IN THE STANDARD

Bridged Ethernet

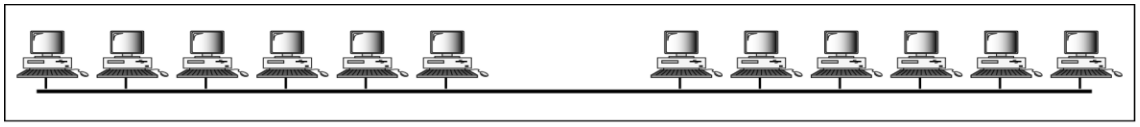
Bridges have two effects on an Ethernet LAN: They **raise the bandwidth** and they **separate collision domains**.

Raising the Bandwidth

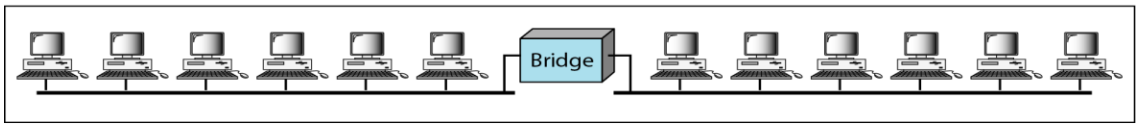
- In an unabridged Ethernet network, the total capacity (10 Mbps) is shared among all stations with a frame to send; the stations share the bandwidth of the network.
- If only one station has frames to send, it benefits from the total capacity (10 Mbps). But if more than one station needs to use the network, the capacity is shared.
- A **bridge** divides the network into two or more networks. Bandwidth-wise, each network is independent.

For example, in the figure below, a network with 12 stations is divided into two networks, each with 6 stations. Now each network has a capacity of 10 Mbps. The 10-Mbps capacity in each segment is now shared between 6 stations (actually 7 because the bridge acts as a station in each segment), not 12 stations.

- In a network with a heavy load, each station theoretically is offered 10/6 Mbps instead of 10/12 Mbps, assuming that the traffic is not going through the bridge.



a. Without bridging

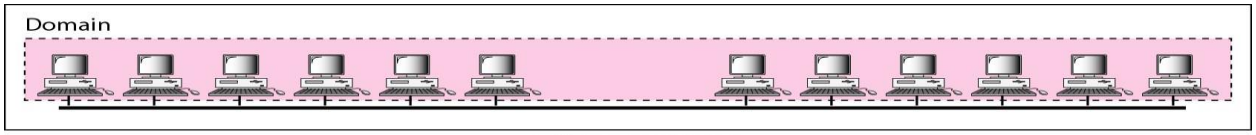


b. With bridging

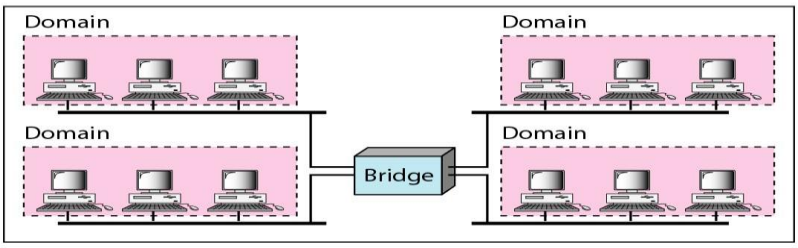
Separating Collision Domains

- Another advantage of a bridge is the separation of the collision domain.
- The figure below shows the collision domains for an unbridged and a bridged network.

- You can see that the collision domain becomes much smaller and the probability of collision is reduced tremendously. Without bridging, 12 stations contend for access to the medium; with bridging only 3 stations contend for access to the medium.



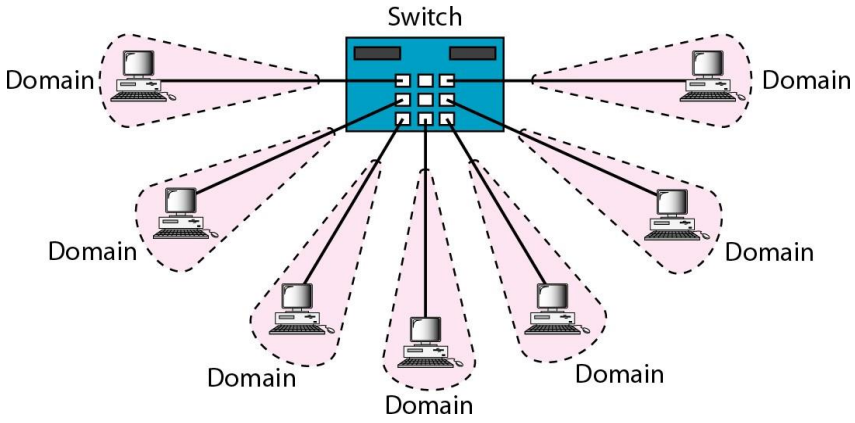
a. Without bridging



b. With bridging

Switched Ethernet

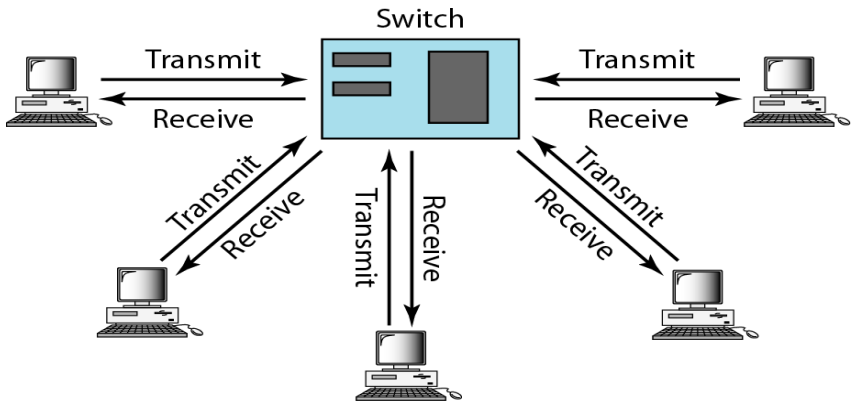
- The idea of a bridged LAN can be extended to a switched LAN.
- In other words, if we can have a multiple-port bridge, It has an N-port switch, In this way, the bandwidth is shared only between the station and the switch (5 Mbps each).



Full-Duplex Ethernet

- One of the limitations of 10Base5 and 10Base2 is that communication is half-duplex (10Base-T is always full-duplex); a station can either send or receive, but may not do both at the same time.
- The next step in the evolution was to move from switched Ethernet to full-duplex switched Ethernet. The full-duplex mode increases the capacity of each domain from 10 to 20 Mbps.

- The figure below shows a switched Ethernet in full-duplex mode. Note that instead of using one link between the station and the switch, the configuration uses two links: one to transmit and one to receive.



4.3 FAST ETHERNET

The goals of Fast Ethernet can be summarized as follows:

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

- For the star topology, there are two choices, as we saw before: half duplex and full duplex.
- In the half-duplex approach, the stations are connected via a hub; in the full-duplex approach, the connection is made via a switch with buffers at each port.
- The access method is the same (CSMA/CD) for the half-duplex approach;
- For full-duplex Fast Ethernet, there is no need for CSMA/CD.

Autonegotiation

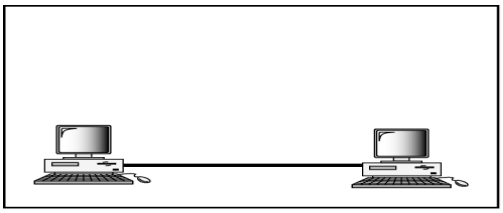
A new feature added to Fast Ethernet is called autonegotiation. It allows a station or a hub a range of capabilities. ***Autonegotiation allows two devices to negotiate the mode or data rate of operation***.

Physical Layer

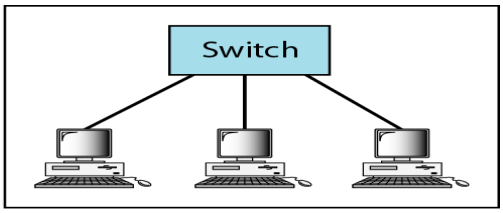
Topology

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

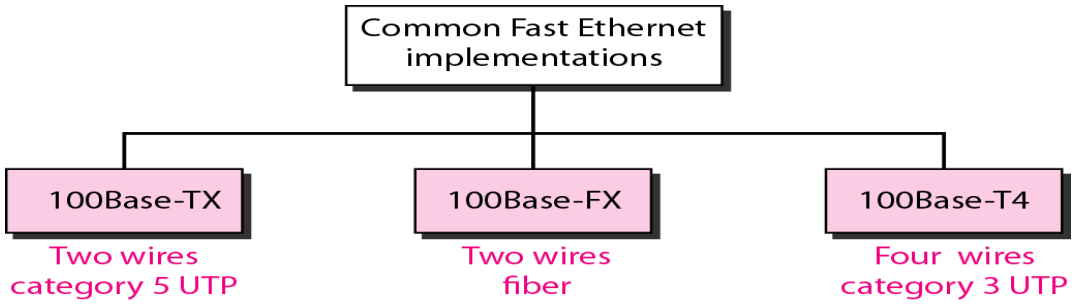


a. Point-to-point



b. Star

Implemetation



100Base-TX:

- Uses two pairs of twisted-pair cable (either category 5 UTP or STP).
- MLT-3 scheme was selected since it has good bandwidth performance.
- 4B/5B block coding is used to provide bit synchronization.
- 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.

- NRZ-I encoding scheme for this implementation. However, NRZ-I has a bit synchronization problem for long sequences of 0s (or 1s, based on the encoding).
- To overcome this problem, the designers used 4B/5B block encoding.
- The block encoding increases the bit rate from 100 to 125 Mbps, which can easily be handled by fiber-optic cable.

100Base-T4,

- Was designed to use category 3 or higher UTP. The implementation uses four pairs of UTP for transmitting 100 Mbps.
- Encoding/decoding in 100Base-T4 is more complicated. As this implementation uses category 3 UTP, each twisted-pair cannot easily handle more than 25 Mbaud.
- In this design, one pair switches between sending and receiving. Three pairs of UTP category 3, however, can handle only 75 Mbaud (25 Mbaud) each. We need to use an encoding scheme that converts 100 Mbps to a 75 Mbaud signal.
- 8B/6T satisfies this requirement. In 8B/6T, eight data elements are encoded as six signal elements. This means that 100 Mbps uses only (6/8) x 100 Mbps, or 75 Mbaud.

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

4.4 GIGABIT ETHERNET

The goals of the Gigabit Ethernet design can be summarized as follows:

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

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.

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. This means that CSMA/CD is not used.

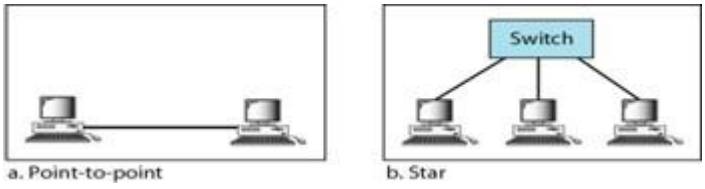
Half-Duplex Mode

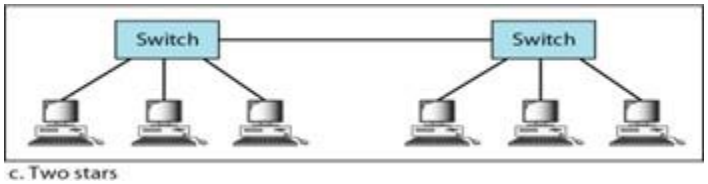
Gigabit Ethernet can also be used in half-duplex mode, although it is rare. In this case, a switch can be replaced by a hub, which acts as the common cable in which a collision might occur. The half-duplex approach uses CSMA/CD.

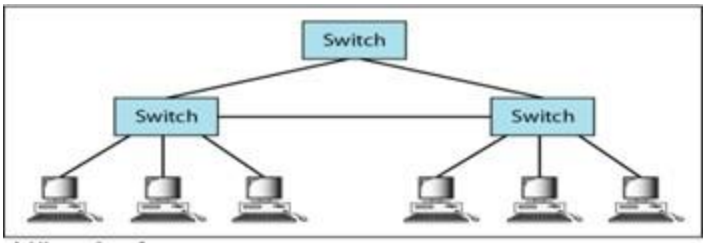
Physical Layer

Topology

- 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.

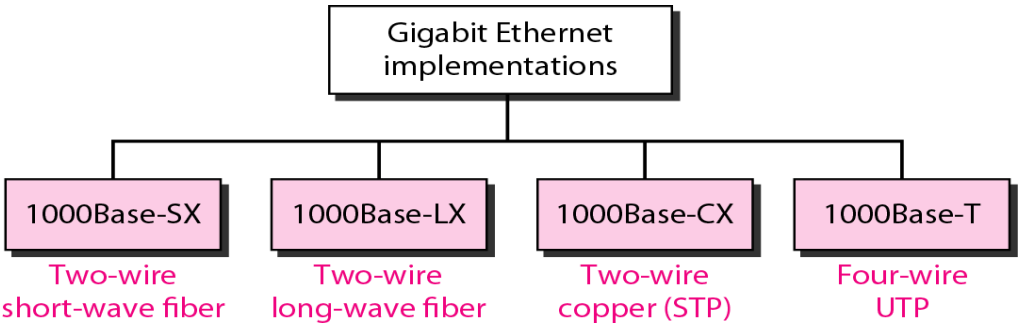






d. Hierarchy of stars

Implementation



Summary of Ten-Gigabit Ethernet implementations

Characteristics	*10GBase-S*	*10GBase-L*	*10GBase-E*
Media	Short-wave 850-nm multimode	Long-wave 1310-nm single mode	Extended 1550-mm single mode
Maximum length	300 m	10 km	40 km

4.5 Ten-Gigabit Ethernet

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: 10GBase-S, 10GBase-L, and 10GBase-E.

Summary of Ten-Gigabit Ethernet implementations

Characteristics	*10GBase-S*	*10GBase-L*	*10GBase-E*
Media	Short-wave 850-nm multimode	Long-wave 1310-nm single mode	Extended 1550-mm single mode
Maximum length	300 m	10 km	40 km

4.9 IEEE 802.11

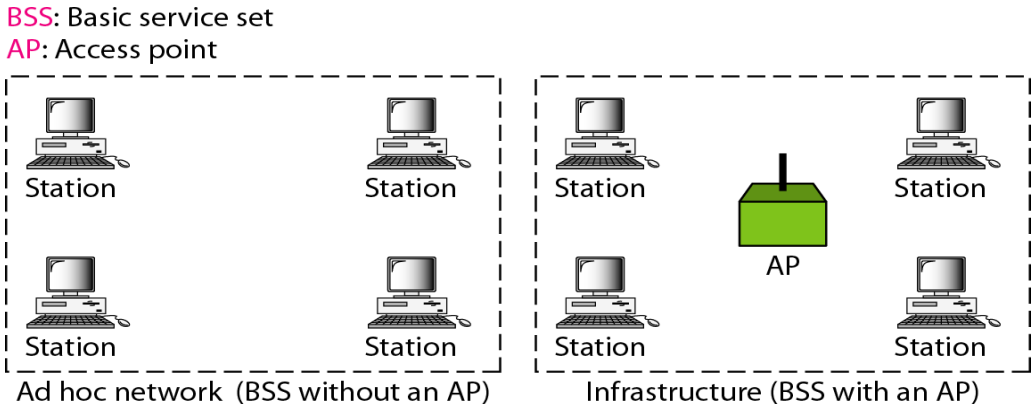
IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

Architecture

The standard defines two kinds of services: the Basic Service Set (BSS) and the Extended Service Set (ESS).

Basic Service Set

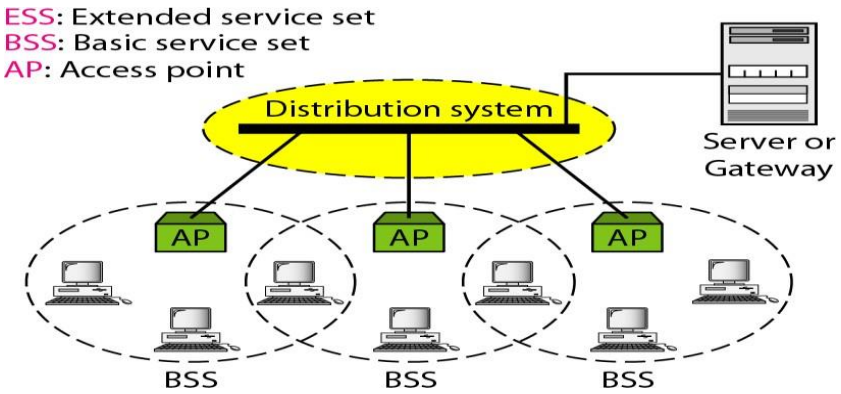
- IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN.
- A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).



- 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.

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.
- 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.

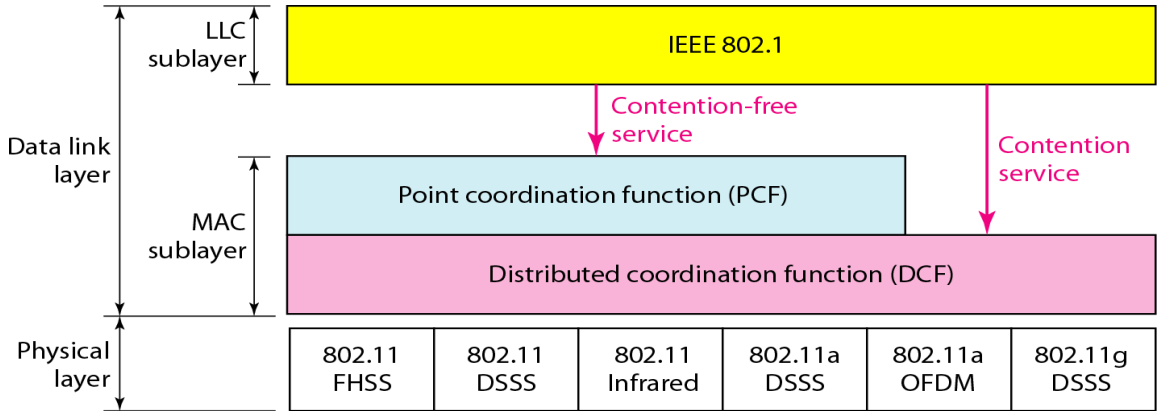


Station Types

- IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN: no-transition, BSS-transition, and 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).

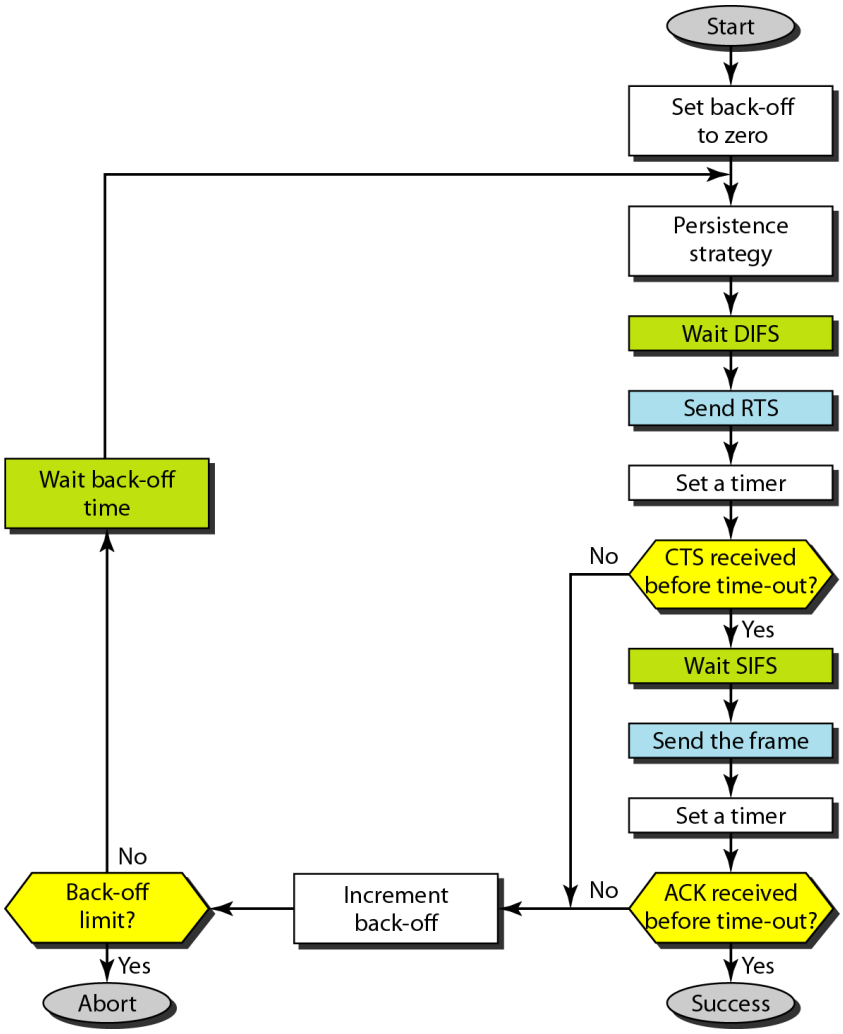


Distributed Coordination Function

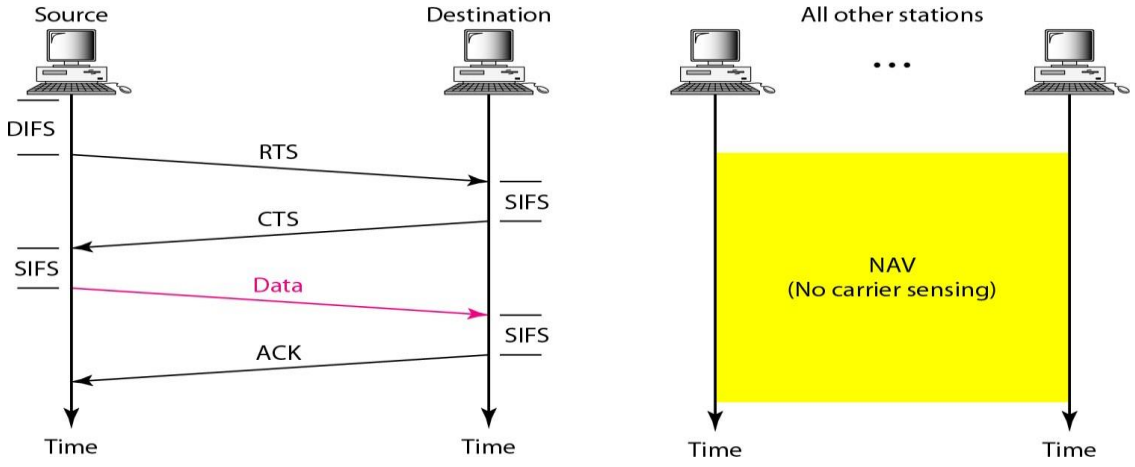
One of the two protocols defined by IEEE at the MAC sublayer is called the distributed coordination function (DCF). DCF uses *CSMA/CA* as the access method. Wireless LANs cannot implement *CSMA/CD* for three reasons:

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

Process Flowchart The figure shows the process flowchart for CSMA/CA as used in wireless LANs.



Frame Exchange Time Line The figure shows the exchange of data and control frames in time.



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 soume that data have arrived.

Network Allocation Vector:

- 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.

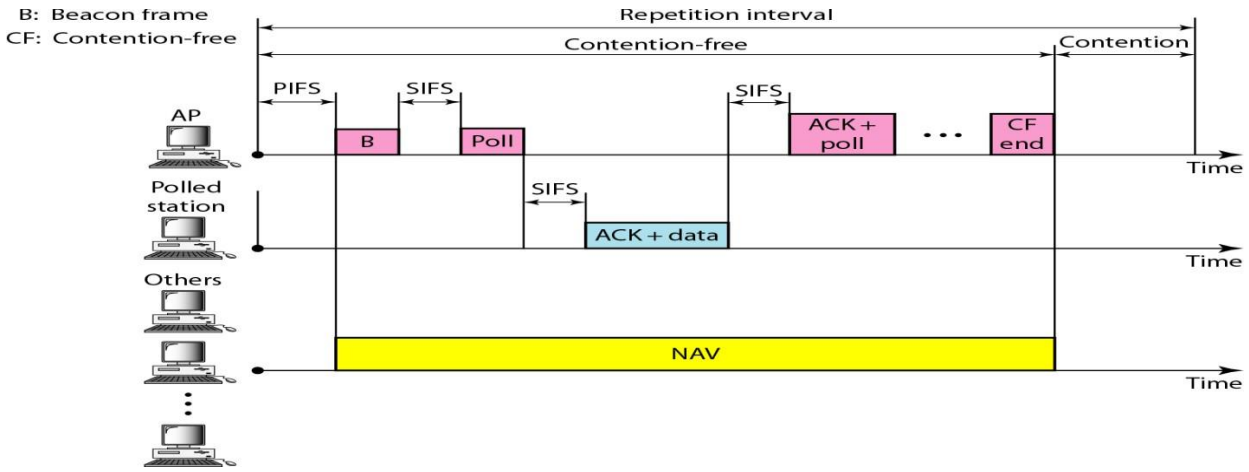
Collision during Handshaking

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 point coordination function (PCF) is an optional access method that can be implemented in an infrastructure network (not in an ad hoc 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. This means that if, at the same time, a station wants to use only DCF and an AP wants to use PCF, the AP has priority.
- 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. T
- he 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. The figure shows an example of a repetition interval.

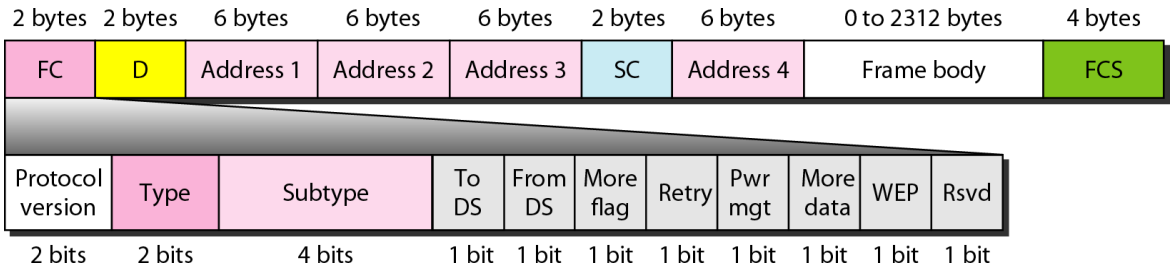


Fragmentation

The wireless environment is very noisy; a corrupt frame has to be retransmitted. The protocol, therefore, recommends fragmentation--the division of a large frame into smaller ones. It is more efficient to resend a small frame than a large one.

Frame Format

The MAC layer frame consists of nine fields, as shown.



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

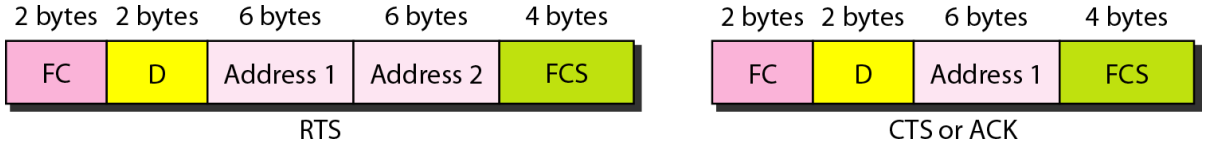
Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 14.2)
To DS	Defined later
From DS	Defined later
More flag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr 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

- **ID**. 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 and will be discussed later.
- **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** Management frames are used for the initial communication between stations and access points.
- **Control Frames** Control frames are used for accessing the channel and acknowledging frames. The figure shows the format.



For control frames the value of the type field is 01; the values of the subtype fields for frames we have discussed are shown in the table.

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

- **Data Frames** Data frames are used for carrying data and control information.

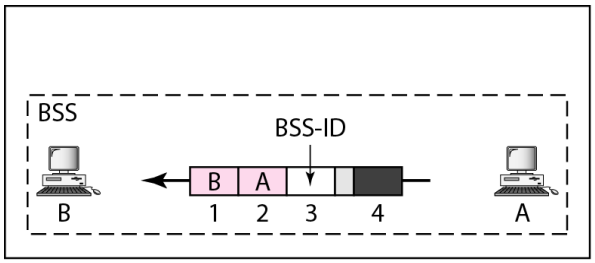
Addressing Mechanism

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, as shown in the table.

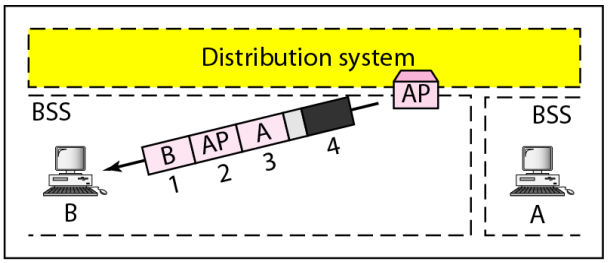
To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

Note that address 1 is always the address of the next device. Address 2 is always the address of the previous device. Address 3 is the address of the final destination station if it is not defined by address 1. Address 4 is the address of the original source station if it is not the same as address 2.

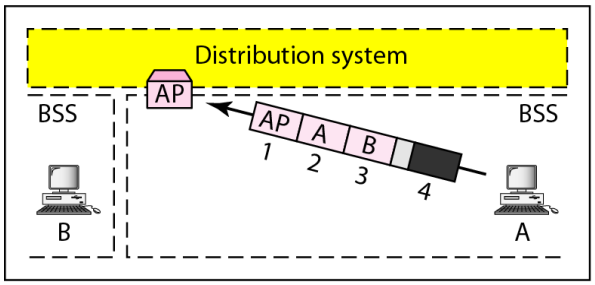
Case 1:00 In this case, To DS = 0 and From DS = 0. This means that the frame is not going to a distribution system (To DS = 0) and is not coming from a distribution system (From DS = 0). The frame is going from one station in a BSS to another without passing through the distribution system. The ACK frame should be sent to the original sender. The addresses are shown in figure.



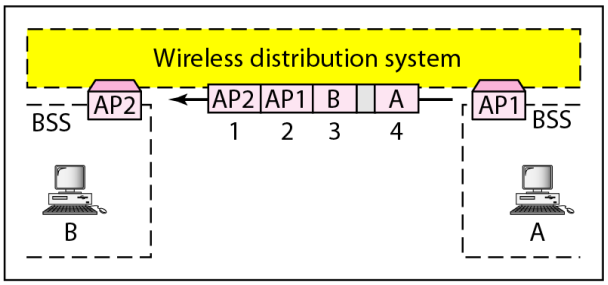
a. Case 1



b. Case 2



c. Case 3



d. Case 4

Case 2:01 In this case, To DS = 0 and From DS = 1. This means that the frame is coming from a distribution system (From DS = 1). The frame is coming from an AP and going to a station. The ACK should be sent to the AP. The addresses are as shown in Figure 14.9. Note that address 3 contains the original sender of the frame (in another BSS).

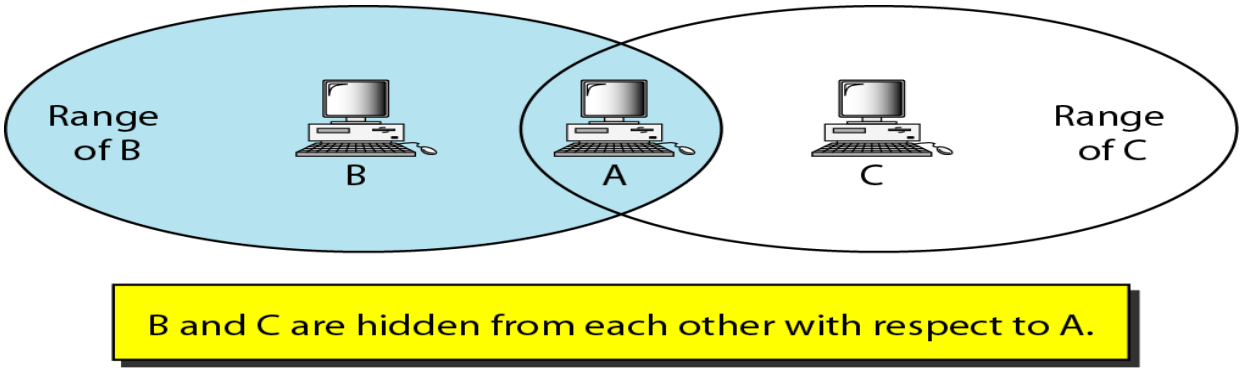
Case 3:10 In this case, To DS = 1 and From DS = 0. This means that the frame is going to a distribution system (To DS = 1). The frame is going from a station to an AP. The ACK is sent to the original station. The addresses are as shown in figure above. Note that address 3 contains the final destination of the frame (in another BSS).

Case 4:11 In this case, To DS = 1 and From DS = 1. This is the case in which the distribution system is also wireless. The frame is going from one AP to another AP in a wire-less distribution system. We do not need to define addresses if the distribution system is a wired LAN because the frame in these cases has the format of a wired LAN frame (Ethernet, for example). Here, we need four addresses to define the original sender, the final destination, and two intermediate APs. Figure above shows the situation.

Hidden and Exposed Station Problems

Hidden Station Problem

The figure below 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 B and C; it can hear any signal transmitted by B or C.

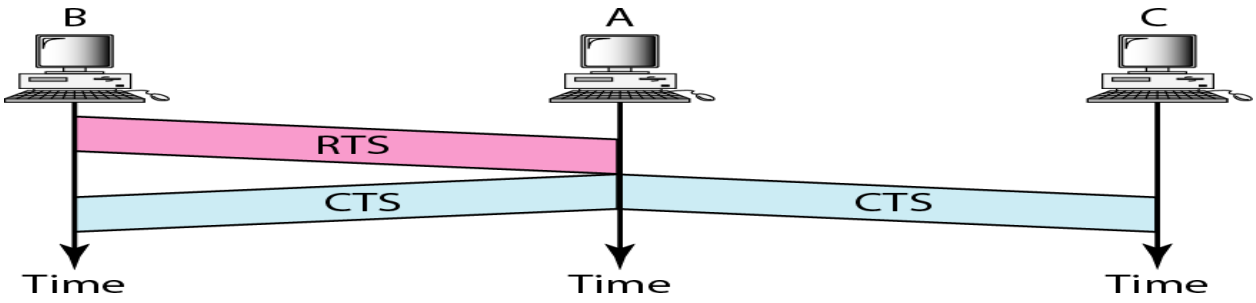
Assume that station B is sending data to station A. In the middle of this transmission, station C also has data to send to station A. However, station C is out of B's range and transmissions from B cannot reach C. Therefore C thinks the medium is free. Station C sends its data to A, which results in 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)

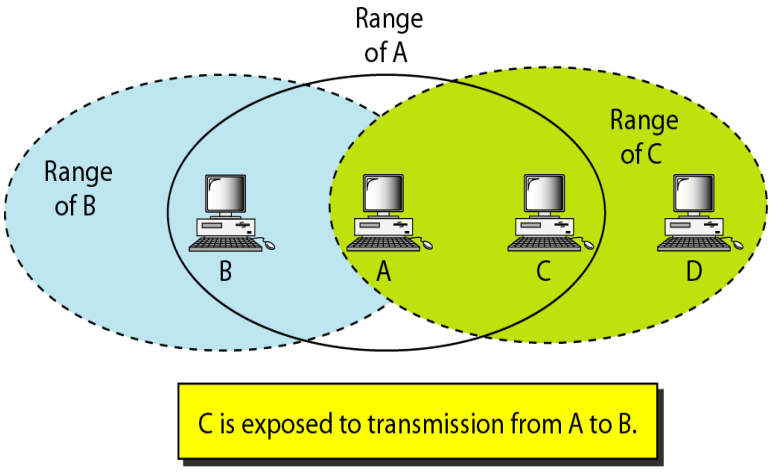
The figure shows that the RTS message from B reaches A, but not C. However, because both B and C are within the range of A, the CTS message, which contains the duration of data transmission from B to A reaches C.

Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

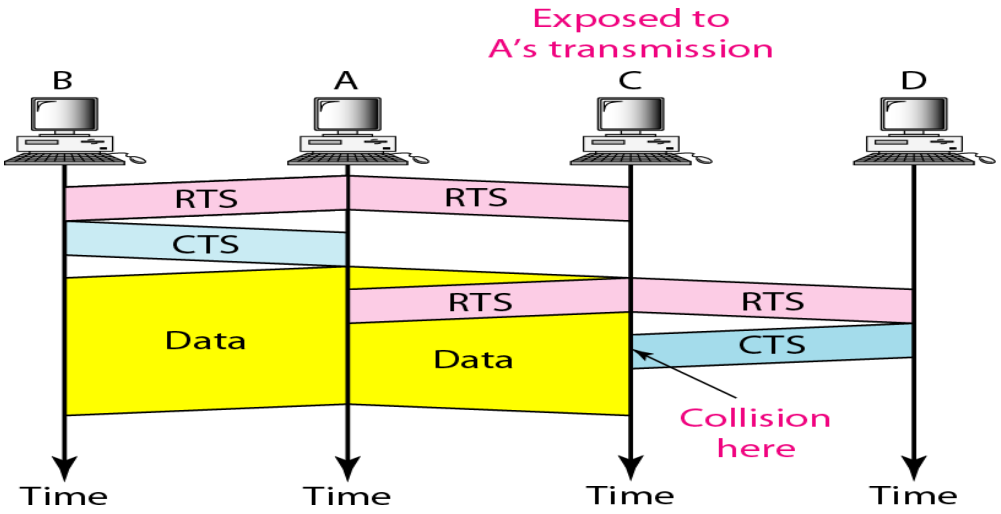


Exposed Station Problem Now consider a situation that is the inverse of the previous one: the exposed station problem. In this problem a station refrains from using a channel when it is, in fact, available. In the figure, station A is transmitting to station B. Station C has some data to send to station 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

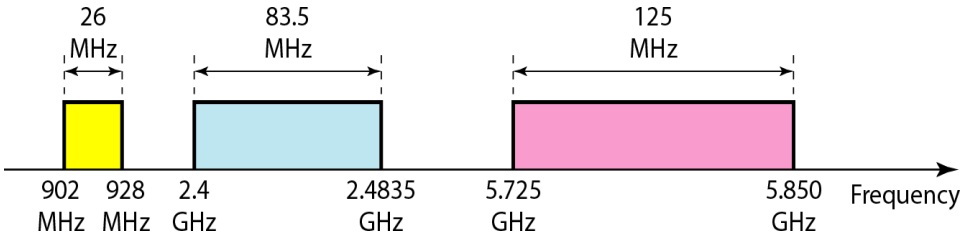


Physical layer:

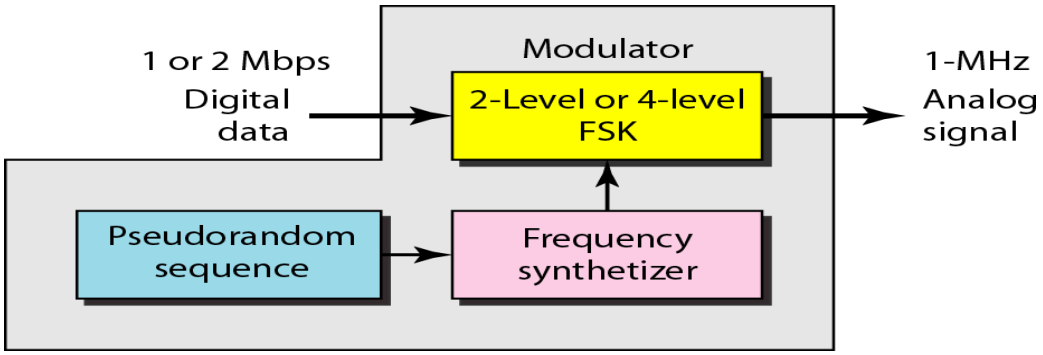
IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.4 GHz	FSK	1 and 2
	DSSS	2.4 GHz	PSK	1 and 2
		Infrared	PPM	1 and 2
802.11a	OFDM	5.725 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.4 GHz	PSK	5.5 and 11
802.11g	OFDM	2.4 GHz	Different	22 and 54

The 2.4GHz ISM band is divided into 79 bands of 1MHz

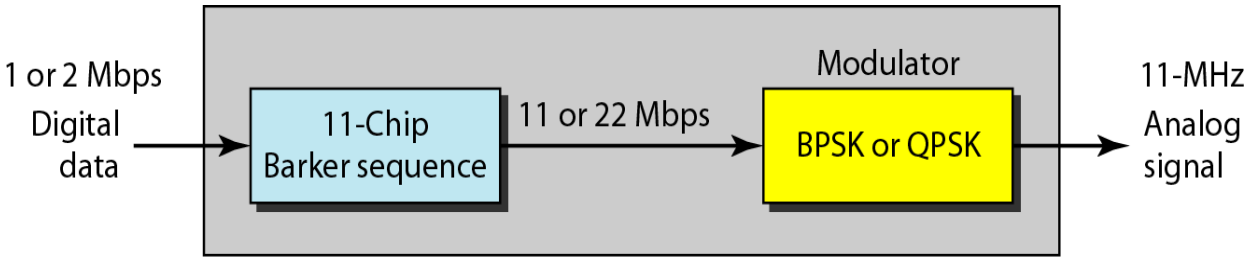
Industrial-Scientific-Medical (ISM) band



- In Frequency Hopping Spread Spectrum (FHSS) the sender sends on one carrier frequency for a short amount of time, then hops to another carrier frequency for the same amount of time, and so on. After N hop-pings, the cycle is repeated.
- Spreading makes it difficult for unauthorized persons to make sense of the transmitted data

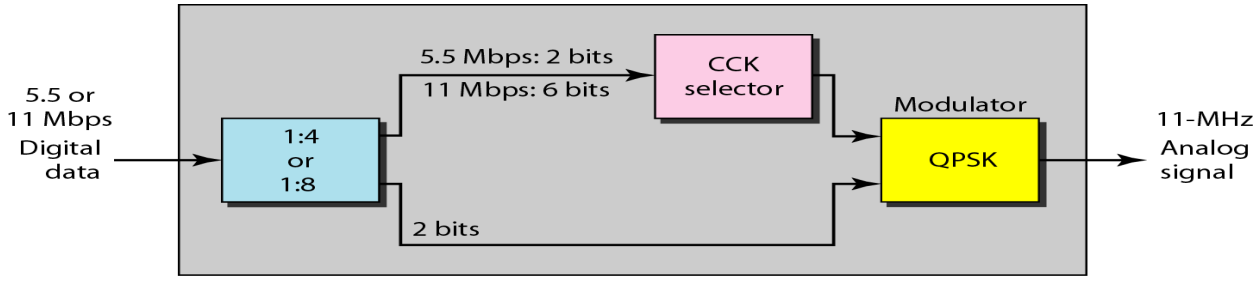


- In Direct Sequence Spread Spectrum (DSSS) each bit sent by the sender is replaced by a sequence of bits called a chip code.
- To avoid buffering, the time needed to send one chip code must be the same as the time needed to send one original bit.
- DSSS is implemented at the physical layer and uses a 2.4GHz ISM band



- IEEE 802.11a describes the orthogonal frequency-division multiplexing (OFDM) method for signal generation in the 5GHz ISM band
- OFDM is the same as FDM with one major difference:
    - All the subbands are used by one source at a given time
    - Sources conend with one another at the data link layer for access
- OFDM uses PSK (18Mbps) and QAM (54Mbps) for modulation

- IEEE 802.11b describes the high-rate DSSS method for signal generation at 2.4GHz ISM band.
- This 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



,

- ❖ IEEE 802.11 FHSS(Frequency-hopping spread spectrum)
  - Operating in 2.4 GHz ISM band
  - Lower cost, power consumption
  - Most tolerant to signal interference
- ❖ IEEE 802.11 DSSS (Direct-sequence spread spectrum)
  - Operating in 2.4 GHz ISM band
  - Supports higher data rates
  - More range than FH or IR physical layers
- ❖ IEEE 802.11 Infrared
  - Lowest cost
  - Lowest range compared to spread spectrum
  - Doesn't penetrate walls, so no eavesdropping
- ❖ IEEE 802.11a
  - Makes use of 5-GHz band
  - Provides rates of 6, 9 , 12, 18, 24, 36, 48, 54 Mbps
  - Uses orthogonal frequency division multiplexing (OFDM)
- ❖ IEEE 802.11b
  - 802.11b operates in 2.4 GHz band

- Provides data rates of 5.5 and 11 Mbps
- Complementary code keying (CCK) modulation scheme

❖ IEEE 802.11g

- 802.11g operates in 2.4 GHz band
- Provides data rates of 22 and 54 Mbps
- Uses orthogonal frequency division multiplexing (OFDM)

4.10 Bluetooth

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers, coffee makers, and so on. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously.

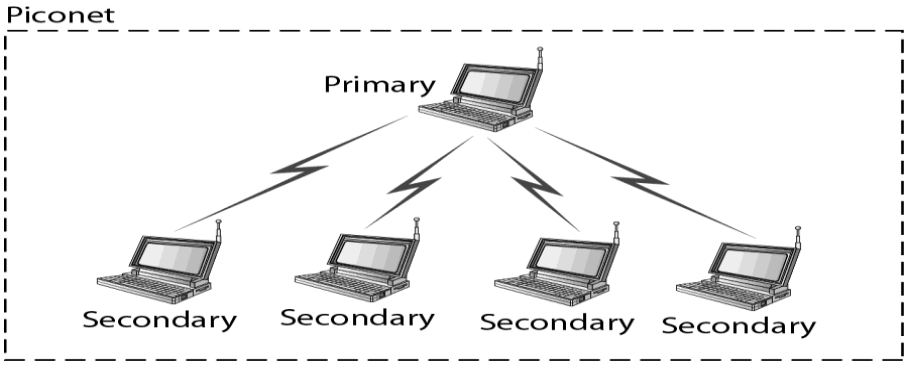
Architecture

Bluetooth defines two types of networks: piconet and scatternet.

Piconet:

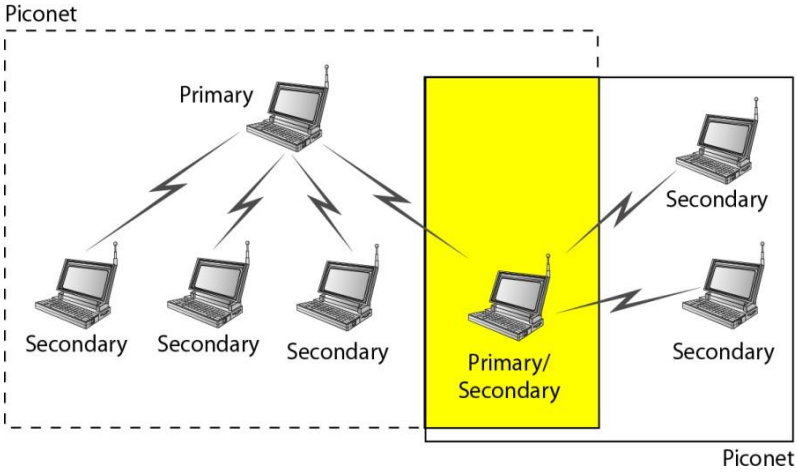
- A Bluetooth network is called a piconet, or a small net.
- It can have up to eight stations, one of which is called the master; the rest are called slaves.
- Maximum of seven slaves. Only one master.
- Slaves synchronize their clocks and hopping sequence with the master.

  But an additional eight slaves can stay in parked state, which means they can be synchronized with the master but cannot take part in communication until it is moved from the parked state



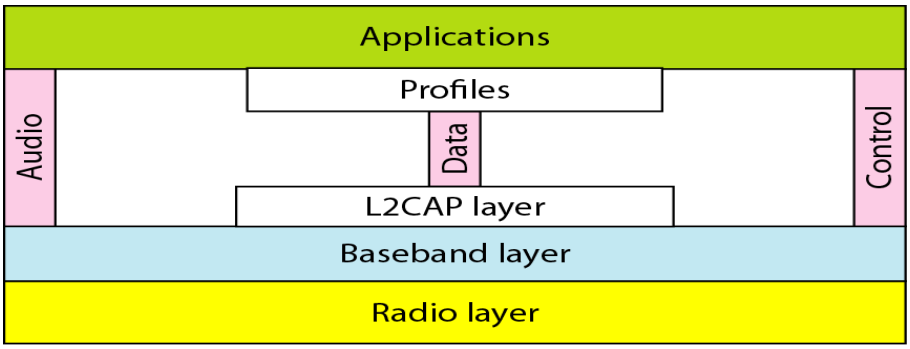
Scatternet

- Piconets can be combined to form what is called a scatternet.
- A slave station in one piconet can become the master in another piconet.
- Bluetooth devices has a built-in short-range radio transmitter.



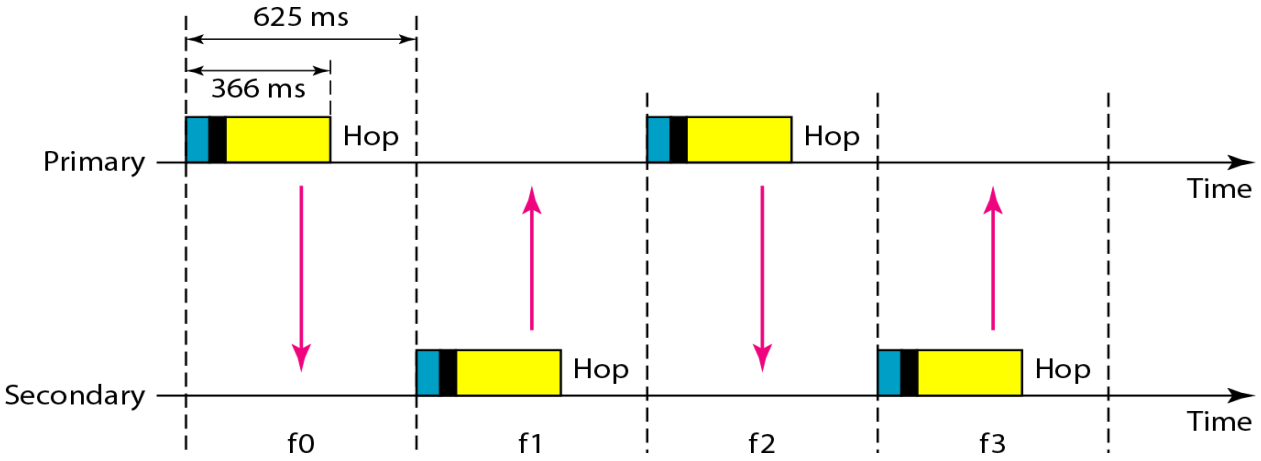
Bluetooth layers

- **Radio Layer:** Roughly equivalent to physical layer of the Internet model. Physical links can be synchronous or asynchronous.
    - Uses Frequency-hopping spread spectrum [Changing frequency of usage]. Changes it modulation frequency 1600 times per second.
    - Uses frequency shift keying (FSK)with Gaussian bandwidth filtering to transform bits to a signal.
- **Baseband layer:** Roughly equivalent to MAC sublayer in LANs. Access is using Time Division (Time slots).
    - Length of time slot = dwell time = 625 microsec. So, during one frequency, a sender sends a frame to a slave, or a slave sends a frame to the master.
    - Time division duplexing TDMA (TDD-TDMA) is a kind of half-duplex communication in which the slave and receiver send and receive data, but not at the same time (half-duplex). However, the communication for each direction uses different hops, like walkie-talkies.



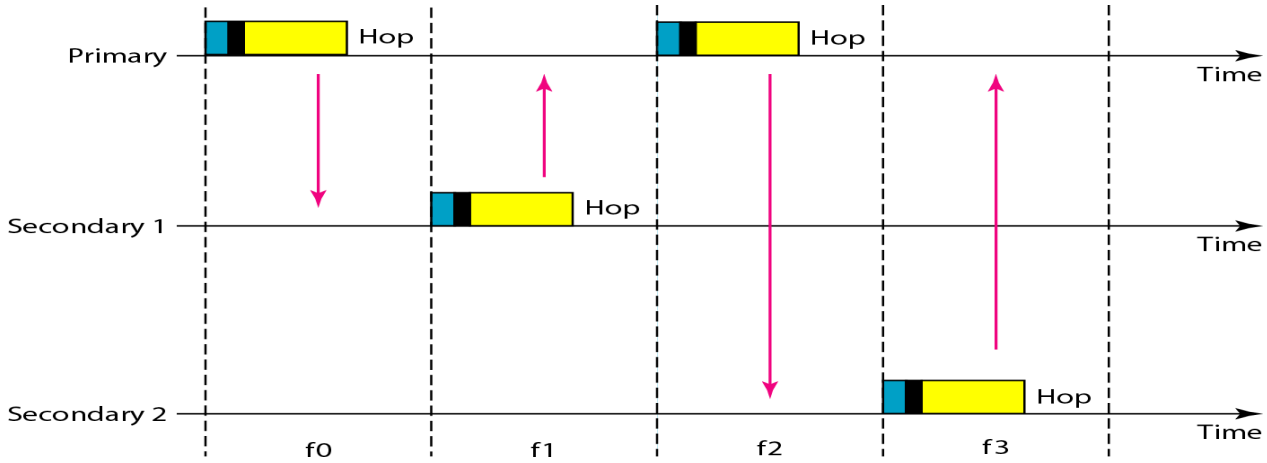
Single-secondary communication

- Master uses even-numbered slots
- Slave uses odd-numbered slots



Multiple-secondary communication also called Multiple-slave communication

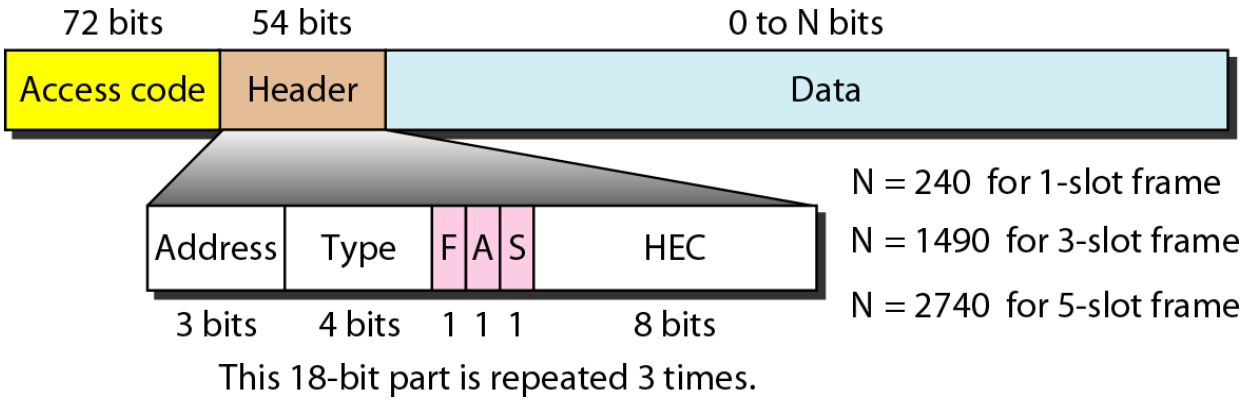
- Master uses even-numbered slots
- Slave sends in the next odd-numbered slot if the packet in the previous slot was addressed to it.



Physical Links

- Synchronous connection-oriented (SCO)
  - Latency is important than integrity.
  - Transmission using slots.
  - No retransmission.
- Asynchronous connectionless link (ACL)
  - Integrity is important than latency.
  - Does like multiple-slave communication.
  - Retransmission is done.

Frame format



- **Access code.** This 72-bit field normally contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from another.
- **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.
    3. F. This 1-bit subfield is for flow control. When set (I), it indicates that the device is unable to receive more frames (buffer is full).
        A. This 1-bit subfield is for acknowledgment. Bluetooth uses Stop-and-Wait ARQ; 1 bit is sufficient for acknowledgment.
    4. S. This 1-bit subfield holds a sequence number. Bluetooth uses Stop-and-Wait ARQ; 1 bit is sufficient for sequence numbering.
    5. 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.
- **Payload.** This subfield can be 0 to 2740 bits long. It contains data or control information corning from the upper layers.

L2CAP (Logical Link Control and Adaptation Protocol)

- Equivalent to LLC sublayer in LANs.
- Used for data exchange on ACL Link. SCO channels do not use L2CAP.
- Frame format has 16-bit length [Size of data coming from upper layer in bytes], channel ID, data and control.

- Can do Multiplexing, segmentation and Reassembly, QoS [with no QoS, best-effort delivery is provided] and Group mangement [Can do like multicast group, using some kind of logical addresses].

L2CAP data packet format