6) Wired and Wireless LAN

6.1 Wired LAN : Ethernet, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, Ethernet IEEE standard 802.3, Bridged Ethernet, Switched Ethernet , Full Duplex Ethernet.

Ethernet:

1. Ethernet is a family of computer networking technologies for local area networks (LANs) and metropolitan area networks (MANs). It is the most popular LAN technology in the world. It is an easy, relatively inexpensive way to provide high-performance networking to all different types of computer equipment.
2. Ethernet was invented at Xerox PARC and developed jointly by Digital Equipment Corporation, Intel and Xerox. Ethernet has largely replaced competing wired LAN technologies such as token ring, FDDI, and ARCNET.
3. The Ethernet standards comprise several wiring and signaling variants of the OSI physical layer in use with Ethernet. Over time Ethernet data transfer rates have been increased from the original three megabits per second (Mbit/s) to the latest 100 gigabits per second (Gbit/s)
4. Systems communicating over Ethernet divide a stream of data into shorter pieces called frames. Each frame contains source and destination addresses and error-checking data so that damaged data can be detected and re-transmitted. As per the OSI model, Ethernet provides services up to and including the data link layer.
5. The CSMA/CD approach is used by any form of Ethernet operating in half-duplex mode-that is, the mode in which transmit (Tx) and receive (Rx) signals can be sent on the same wire or data path. In full-duplex mode, transmit and receive signals are separated onto dedicated, one-way channels. This eliminates the need for CSMA/CD, as all the transmissions on a single data path will be coming from a single device. Half-duplex mode is seldom used in versions of Ethernet running on fiber, and is not supported at all in the 10 Gbps standards.
6. 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 (lot Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (l Gbps), and Ten-Gigabit Ethernet (l0 Gbps), as shown in Figure.

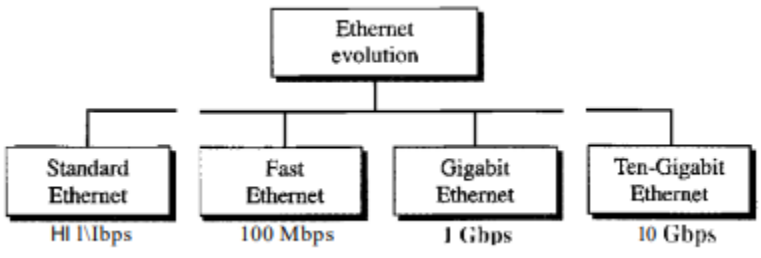


Figure: Ethernet evolution through four generations

Ethernet IEEE standard 802.3/ STANDARD ETHERNET

1. STANDARD ETHERNET uses MAC Sublayer & Physical Layer.
2. The speed of STANDARD ETHERNET is 10 Mbps.
3. Standard Ethernet uses I-persistent CSMAICD.

#MAC Sublayer

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

Frame Format

1. The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of protocol data unit (PDU), upper-layer data, and the CRe.
2. 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.
3. The format of the MAC frame is shown in Figure.

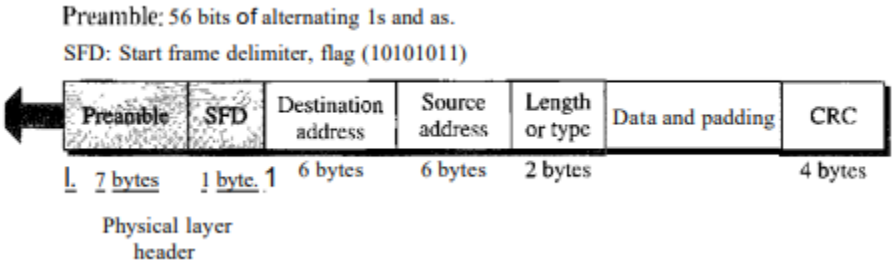


Figure:802.3 MAC frame

4. **From Figure,**
   - **Preamble:** The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating Os and Is that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The pattern provides only an alert and a timing pulse. The 56-bit pattern allows the stations to miss some bits at the beginning of the frame. The preamble is actually added at the physical layer and is not (formally) part of the frame.
   - **Start frame delimiter (SFD):** The second field (I 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. We will discuss addressing shortly.
   - **Source address (SA):** The SA field is also 6 bytes and contains the physical address of the sender of the packet. We will discuss addressing shortly.
   - **Length or type:** This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. 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, as we will see later. o 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.

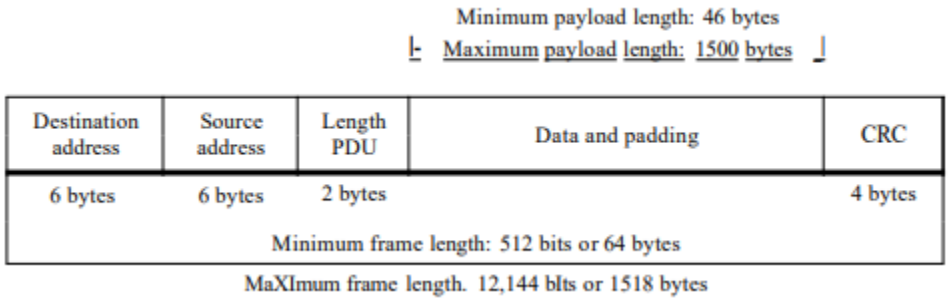


Figure: Minimum and maximum lengths

Addressing

1. Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC).
2. 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), nonnally written in hexadecimal notation, with a colon between the bytes.

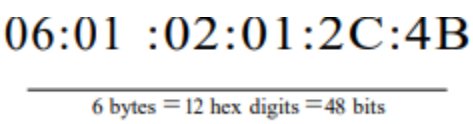


Figure: Example ofan Ethernet address in hexadecimal notation

Access Method: CSMA / CD

1. Standard Ethernet uses I-persistent CSMAICD.
2. 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

3. The slot time in Ethernet is defined in bits. It is the time required for a station to send 512 bits.
4. This means that the actual slot time depends on the data rate; for traditional 10-Mbps Ethernet it is 51.2 I1s.

#Physical Layer

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

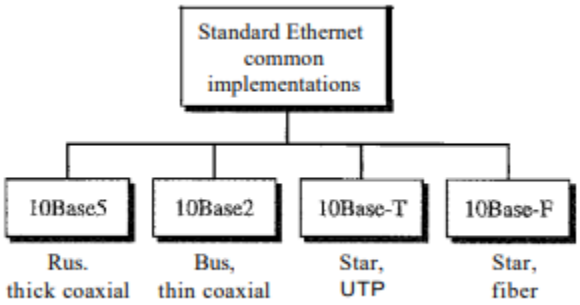


Figure: Categories of Standard Ethernet

Encoding and Decoding

1. All standard implementations use digital signaling (baseband) at 10 Mbps.
2. At the sender, data are converted to a digital signal using the Manchester scheme;
3. at the receiver, the received signal is interpreted as Manchester and decoded into data.
4. Manchester encoding is self-synchronous, providing a transition at each bit interval. Figure shows the encoding scheme for Standard Ethernet.

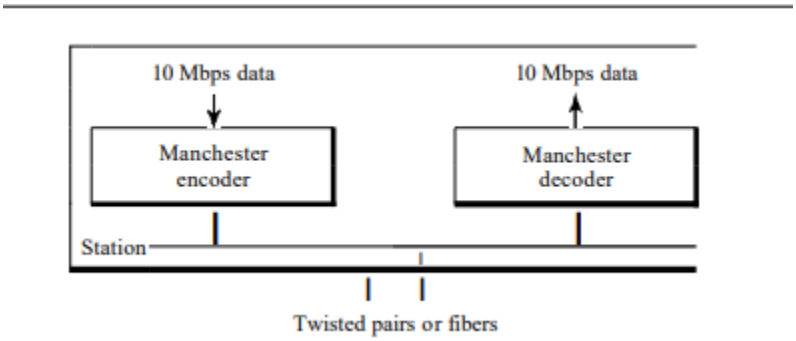


Figure : Encoding in a Standard Ethernet implementation

Summary

Table shows a summary of Standard Ethernet implementations.

Characteristics	*lOBase5*	*lOBase2*	*lOBase-T*	*IOBase-F*
Media	Thick coaxial cable	Thin coaxial cable	2UTP	2 Fiber
Maximum length	500m	185 m	100m	2000m
Line encoding	Manchester	Manchester	Manchester	Manchester

Figure: Summary ofStandard Ethernet implementations

Fast Ethernet

1. Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel (or Fibre Channel, as it is sometimes spelled).
2. 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.
3. 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

1. A main consideration in the evolution of Ethernet from 10 to 100 Mbps was to keep the MAC sublayer untouched. However, a decision was made to drop the bus topologies and keep only the star topology. F
2. or 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.
3. The access method is the same (CSMAICD) for the half-duplex approach; for fullduplex Fast Ethernet, there is no need for CSMAICD. However, the implementations keep CSMA/CD for backward compatibility with Standard Ethernet.

Auto Negotiation

1. A new feature added to Fast Ethernet is called autonegotiation.
2. It allows a station or a hub a range of capabilities.
3. Autonegotiation allows two devices to negotiate the mode or data rate of operation. It was designed particularly for the following purposes:
    - 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).
    - To allow one device to have multiple capabilities.
    - 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. We briefly discuss some features of this layer.

Topology

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

2. Three or more stations need to be connected in a star topology with a hub or a switch at the center, as shown in Figure.

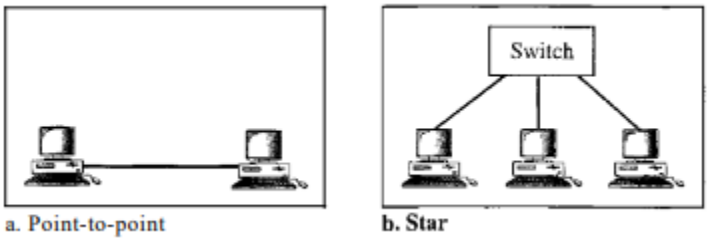


Figure:Fast Ethernet topology

Implementation

1. Fast Ethernet implementation at the physical layer can be categorized as either two-wire or four-wire.
2. The two-wire implementation can be either category 5 UTP (lOOBase-TX) or fiber-optic cable (lOOBase-FX). The four-wire implementation is designed only for category 3 UTP (l00Base-T4). See Figure.

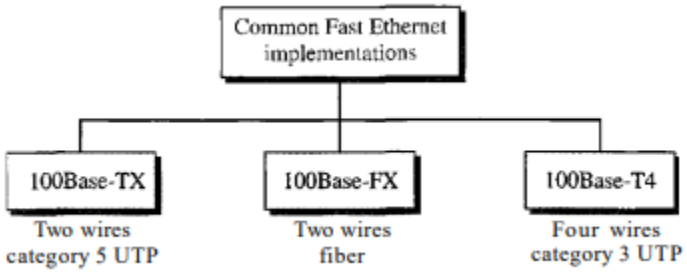


Figure: Fast Ethernet implementations

Encoding

1. Manchester encoding needs a 200-Mbaud bandwidth for a data rate of 100 Mbps, which makes it unsuitable for a medium such as twisted-pair cable.
2. For this reason, the Fast Ethernet designers sought some alternative encoding/decoding scheme. However, it was found that one scheme would not perform equally well for all three implementations. Therefore, three different encoding schemes were chosen.

#Summary Table is a summary of the Fast Ethernet implementations.

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

Table: Summary ofFast Ethernet implementations

GIGABIT ETHERNET

1. The need for an even higher data rate resulted in the design of the Gigabit Ethernet protocol (1000 Mbps).
2. The IEEE committee calls the Standard 802.3z.
3. The goals of the Gigabit Ethernet design can be summarized as follows:
    I. Upgrade the data rate to 1 Gbps.
    II. Make it compatible with Standard or Fast Ethernet.
    III. Use the same 48-bit address.
    IV. Use the same frame format.
    V. Keep the same minimum and maximum frame lengths.
    VI. To support auto negotiation as defined in Fast Ethernet.

#MAC Sublayer

1. A main consideration in the evolution of Ethernet was to keep the MAC sublayer untouched. However, to achieve a data rate of 1 Gbps, this was no longer possible.
2. Gigabit Ethernet has two distinctive approaches for medium access: half-duplex and full-duplex.
3. Almost all implementations of Gigabit Ethernet follow the full-duplex approach.

Full-Duplex Mode

1. 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.
2. There is no collision in this mode, as we discussed before. This means that CSMAICD is not used.
3. Lack of collision implies that the maximum length of the cable is determined by the signal attenuation in the cable, not by the collision detection process.
4. In the full-duplex mode of Gigabit Ethernet, there is no collision; the maximum length of the cable is determined by the signal attenuation in the cable.

Half-Duplex Mode:

1. 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.
2. The half-duplex approach uses CSMAICD. However, as we saw before, the maximum length of the network in this approach is totally dependent on the minimum frame size.
3. Three methods have been defined: traditional, carrier extension, and frame bursting.

#Physical Layer

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

Topology

Gigabit Ethernet is designed to connect two or more stations. If there are only two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the center.

Another possible configuration is to connect several star topologies or let a star topology be part of another as shown in Figure.

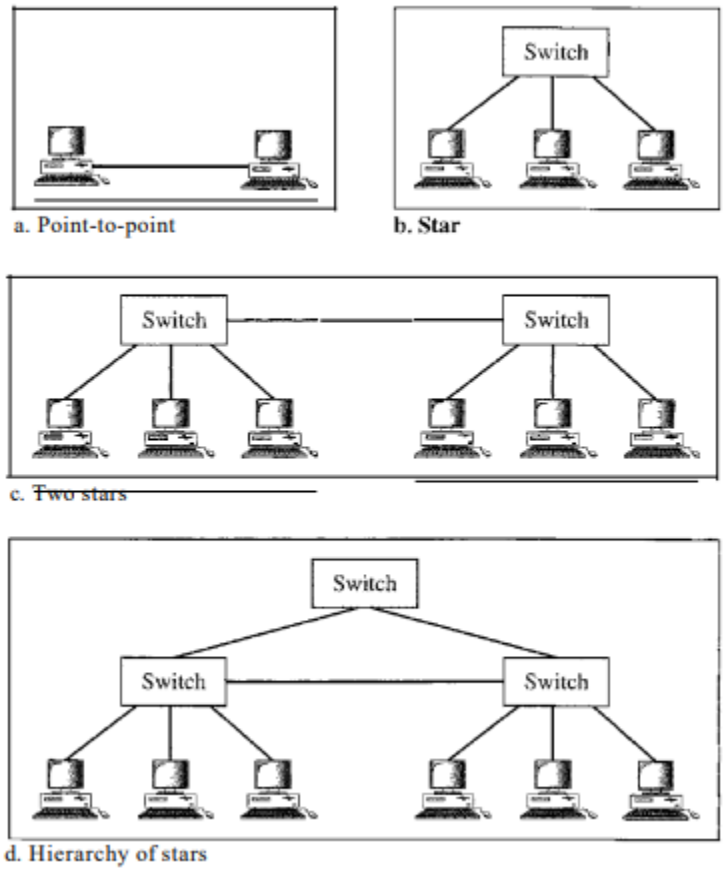


Figure: Topologies ofGigabit Ethernet

Implementation

1. Gigabit Ethernet can be categorized as either a two-wire or a four-wire implementation. The two-wire implementations use fiber-optic cable (1000Base-SX, short-wave, or lOOOBase-LX, long-wave), or STP (1000Base-CX).
2. The four-wire version uses category 5 twisted-pair cable (lOOOBase-T). In other words, we have four implementations, as shown in Figure.
3. GIGABIT ETHERNET 415 had already installed this wiring for other purposes such as Fast Ethernet or telephone serVIces.

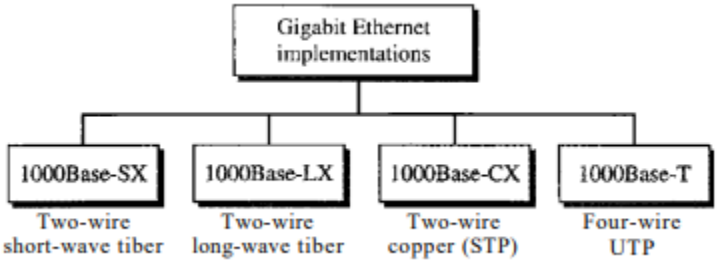


Figure: Gigabit Ethernet implementations

Encoding

1.Figure shows the encoding/decoding schemes for the four implementations.

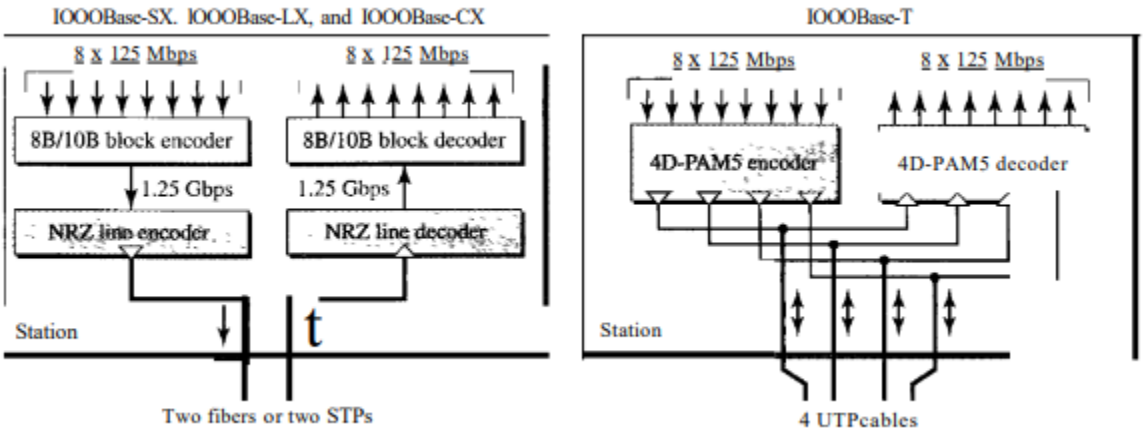


Figure: Encoding in Gigabit Ethernet implementations

2. Gigabit Ethernet cannot use the Manchester encoding scheme because it involves a very high bandwidth (2 GBaud). The two-wire implementations use an NRZ scheme, but NRZ does not self-synchronize properly.

#Summary

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

Figure: Summary ofGigabit Ethernet implementations

Ten-Gigabit Ethernet

1. The IEEE committee created Ten-Gigabit Ethernet and called it Standard 802.3ae.
2. 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.
   S. 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

1. The physical layer in Ten-Gigabit Ethernet is designed for using fiber-optic cable over long distances.
2. Three implementations are the most common: lOGBase-S, lOGBase-L, and lOGBase-E.

#Summary

1. Table shows a summary of the Ten-Gigabit Ethernet implementations.

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

Bridged Ethernet

1. The first step in the Ethernet evolution was the division of a LAN by bridges.
2. Bridges have two effects on an Ethernet LAN: They raise the bandwidth and they separate collision domains.

Raising the Bandwidth

1. In an un-bridged 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.
2. 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.
3. For example, if two stations have a lot of frames to send, they probably alternate in usage. When one station is sending, the other one refrains from sending. We can say that, in this case, each station on average, sends at a rate of 5 Mbps. Figure shows the situation.

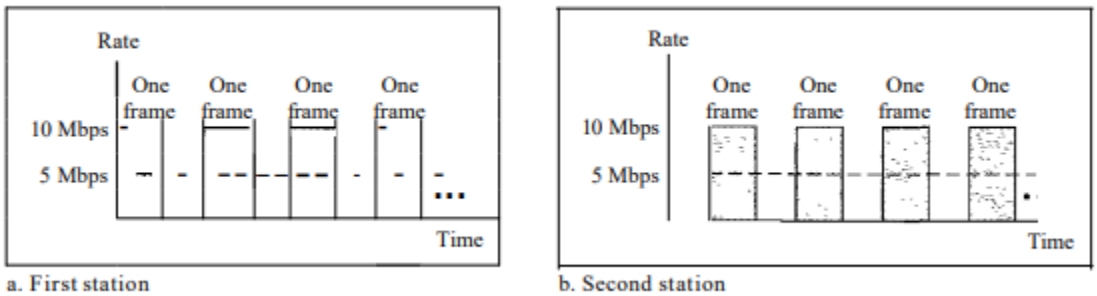


Figure: Sharing bandwidth

Separating Collision Domains

1. Another advantage of a bridge is the separation of the collision domain. Figure 13.16 shows the collision domains for an unbridged and a bridged network.
2. You can see that the collision domain becomes much smaller and the probability of collision is reduced tremendously.
3. Without bridging, 12 stations contend for access to the medium; with bridging only 3 stations contend for access to the medium.

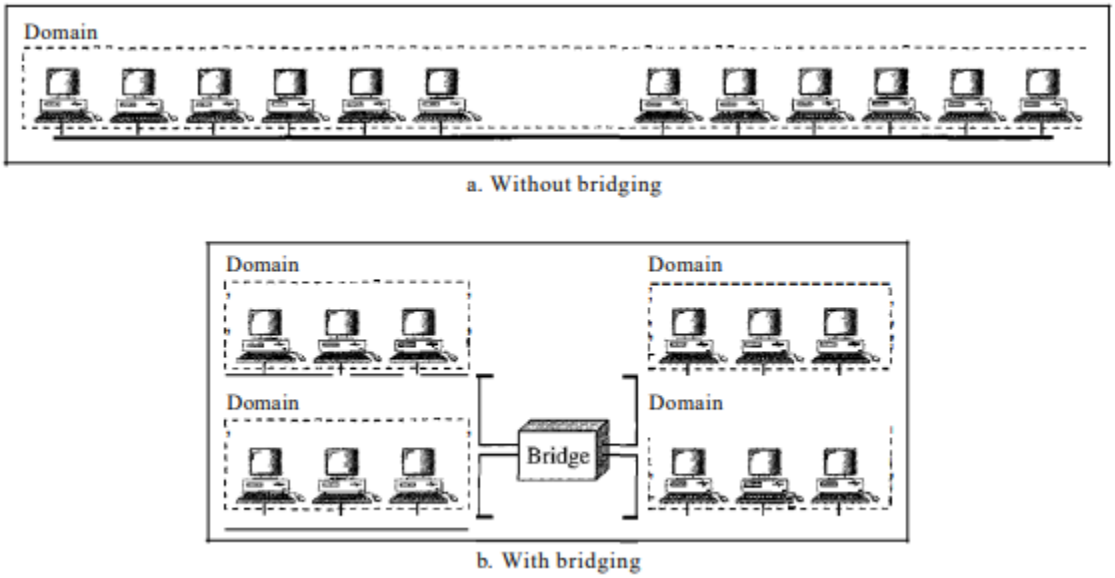


Figure: Collision domains in an unbridged network and a bridged network

Switched Ethernet

1. The idea of a bridged LAN can be extended to a switched LAN. Instead of having two to four networks, why not have N networks, where N is the number of stations on the LAN?
2. In other words, if we can have a multiple-port bridge, why not have an N-port switch? In this way, the bandwidth is shared only between the station and the switch (5 Mbps each).
3. In addition, the collision domain is divided into N domains. A layer 2 switch is an N-port bridge with additional sophistication that allows faster handling of the packets.
4. Evolution from a bridged Ethernet to a switched Ethernet was a big step that opened the way to an even faster Ethernet, as we will see.
5. Figure shows a switched LAN.

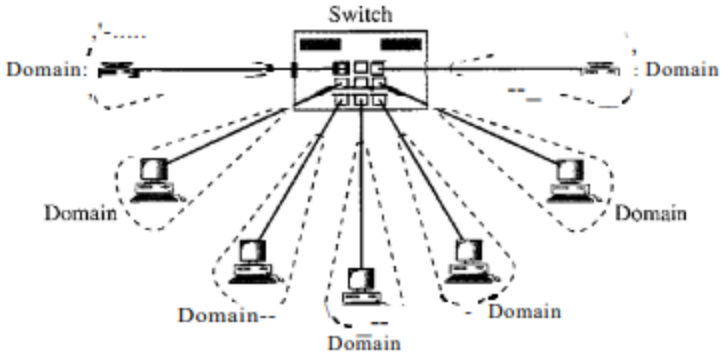


Figure: Switched Ethernet

Full-Duplex Ethernet

1. One of the limitations of 10Base5 and lOBase2 is that communication is half-duplex (lOBase-T is always full-duplex); a station can either send or receive, but may not do both at the same time.
2. 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.
3. Figure shows a switched Ethernet in full-duplex mode.
4. 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.

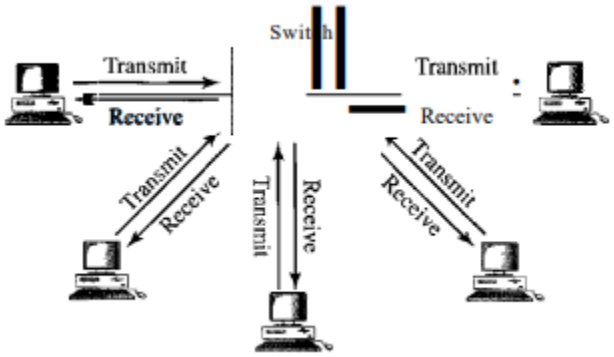


Figure: Full-duplex switched Ethernet

6.2 Multiple Access Random Access : ALOHA, CSMA, CSMA/CD, CSMA/CA

ALOHA

1. ALOHA, the earliest random access method, was developed at the University of Hawaii in early 1970. It was designed for a radio (wireless) LAN, but it can be used on any shared medium. It is obvious that there are potential collisions in this arrangement.
2. The medium is shared between the stations. When a station sends data, another station may attempt to do so at the same time. The data from the two stations collide and become garbled.

Pure ALOHA

1. The original ALOHA protocol is called pure ALOHA. This is a simple, but elegant protocol. The idea is that each station sends a frame whenever it has a frame to send.
2. However, since there is only one channel to share, there is the possibility of collision between frames from different stations. Figure shows an example of frame collisions in pure ALOHA.

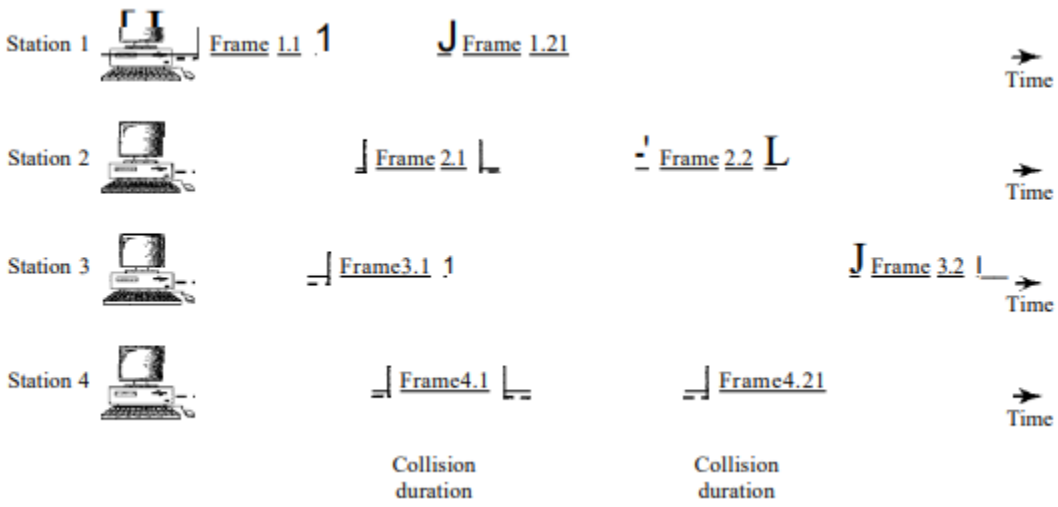


Figure: Frames in a pure ALOHA network

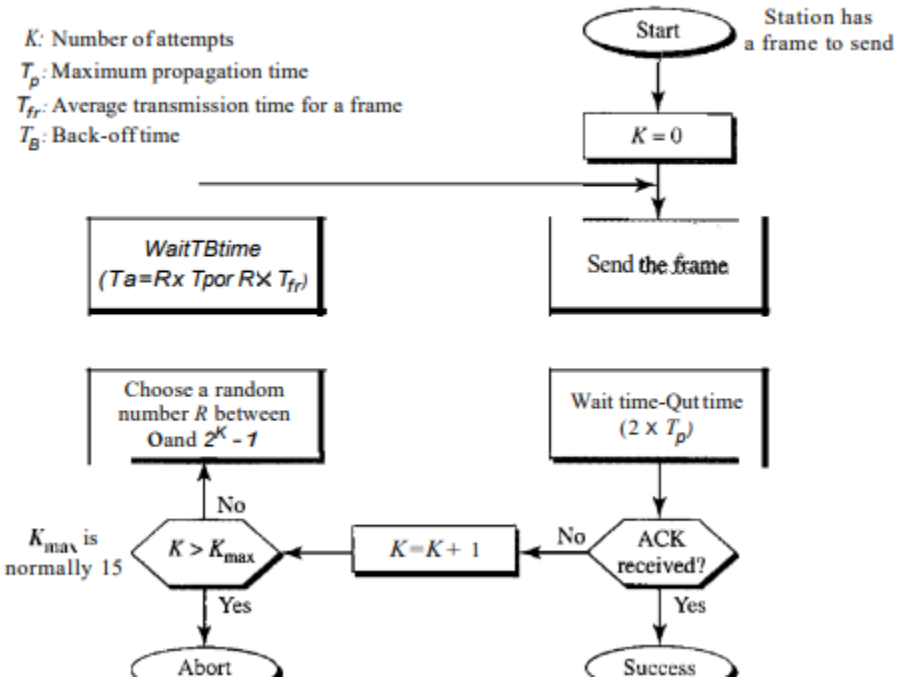
3. There are four stations (unrealistic assumption) that contend with one another for access to the shared channel.
4. The figure shows that each station sends two frames; there are a total of eight frames on the shared medium. Some of these frames collide because multiple frames are in contention for the shared channel.
5. Figure shows that only two frames survive: frame 1.1 from station 1 and frame 3.2 from station 3. We need to mention that even if one bit of a frame coexists on the channel with one bit from another frame, there is a collision and both will be destroyed.
6. It is obvious that we need to resend the frames that have been destroyed during transmission. The pure ALOHA protocol relies on acknowledgments from the receiver. When a station sends a frame, it expects the receiver to send an acknowledgment.
7. If The acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame. A collision involves two or more stations. If all these stations try to resend their frames after the time-out, the frames will collide again. Pure ALOHA

dictates that when the time-out period passes, each station waits a random amount of time before resending its frame.

8. The randomness will help avoid more collisions. We call this time the back-off time TB. Pure ALOHA has a second method to prevent congesting the channel with retransmitted frames. After a maximum number of retransmission attempts Kmax' a station must give up and try later.

#Procedure for pure ALOHA

Figure shows the procedure for pure ALOHA based on the above strategy.



1. The time-out period is equal to the maximum possible round-trip propagation delay, which is twice the amount of time required to send a frame between the two most widely separated stations (2 x Tp)'
2. The back-off time TB is a random value that normally depends on K (the number of attempted unsuccessful transmissions). The formula for TB depends on the implementation. One common formula is the binary exponential back-off.
3. In this method, for each retransmission, a multiplier in the range 0 to 2K - 1 is randomly chosen and multiplied by Tp (maximum propagation time) or Trr (the average time required to send out a frame) to find TB' Note that in this procedure, the range of the random numbers increases after each collision. The value ofKmax is usually chosen as 15.

 # Vulnerable time:

1. Let us find the length of time, the vulnerable time, in which there is a possibility of collision.
2. We assume that the stations send fixed-length frames with each frame taking Tfr S to send.
3. Pure ALOHA vulnerable time = 2 x Tfr

#Throughput:

1. Let us call G the average number of frames generated by the system during one frame transmission time.

2. Then it can be proved that the average number of successful transmissions for pure ALOHA is S = G x e-2G. The maximum throughput Smax is 0.184, for G = 1. I
3. The throughput for pure ALOHA is S =G x e-2G.
4. The maximum throughput Smax =0.184 when G =(1/2).

Slotted ALOHA

1. Pure ALOHA has a vulnerable time of 2 x Tfr. This is so because there is no rule that defines when the station can send.
2. A station may send soon after another station has started or soon before another station has finished.
3. Slotted ALOHA was invented to improve the efficiency of pure ALOHA. In slotted ALOHA we divide the time into slots of Tfr s and force the station to send only at the beginning of the time slot.
4. Figure shows an example of frame collisions in slotted ALOHA.
5. Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot.

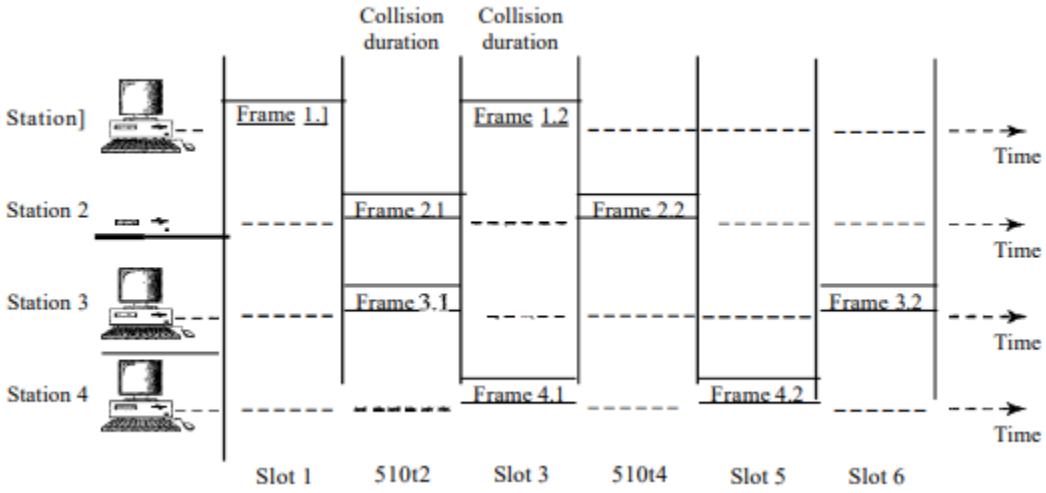


Figure: Frames in a slotted ALOHA network

#vulnerable time

1. However, the vulnerable time is now reduced to one-half, equal to Tfr
2. Figure shows that the vulnerable time for slotted ALOHA is one-half that of pure ALOHA.
3. Slotted ALOHA vulnerable time = Tfr

#Throughput

1. It can be proved that the average number of successful transmissions for slotted ALOHA is S = G x e-G. The maximum throughput Smax is 0.368, when G = 1.
2. In other words, if a frame is generated during one frame transmission time, then 36.8 percent of these frames reach their destination successfully.
3. The throughput for slotted ALOHA is S =: G x e-G. The maximum throughput Smax == 0.368 when G =1.

Carrier Sense Multiple Access (CSMA)

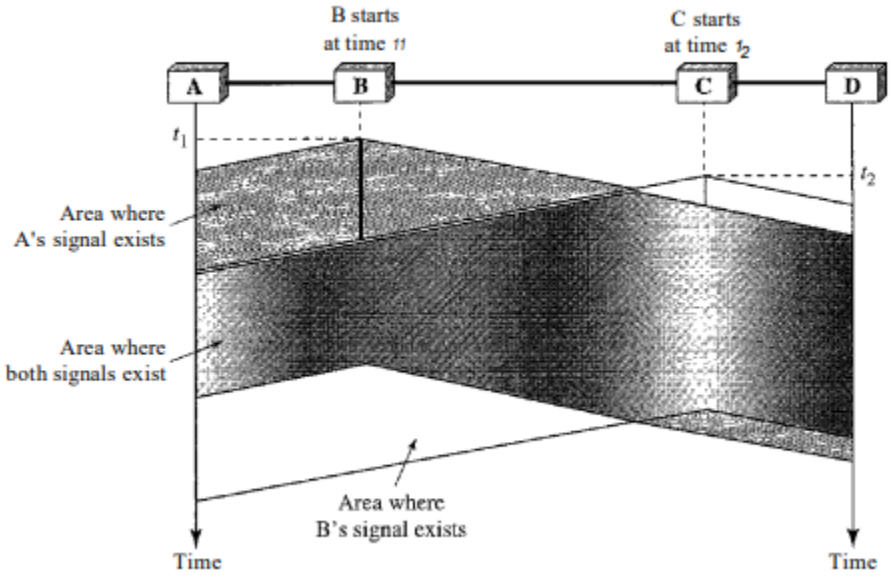


Figure: Space/time model of the collision in CSMA

1. To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The chance of collision can be reduced if a station senses the medium before trying to use it.
2. Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending. In other words, CSMA is based on the principle "sense before transmit" or "listen before talk."
3. CSMA can reduce the possibility of collision, but it cannot eliminate it. The reason for this is shown in Figure 12.8, a space and time model of a CSMA network. Stations are connected to a shared channel (usually a dedicated medium).
4. The possibility of collision still exists because of propagation delay; when a station sends a frame, it still takes time (although very short) for the first bit to reach every station and for every station to sense it.
5. In other words, a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received.
6. At time tl' station B senses the medium and finds it idle, so it sends a frame. At time t2 (t2> tl)' station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C. Station C also sends a frame. The two signals collide and both frames are destroyed.

 # Vulnerable Time

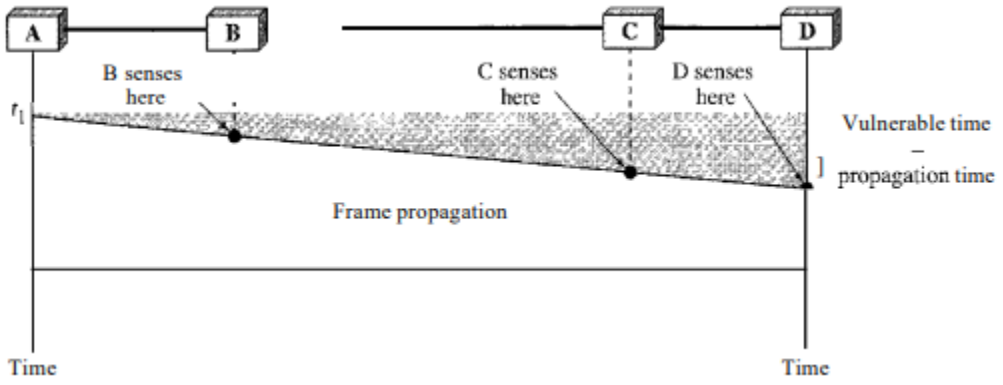


Figure: Vulnerable time in CSMA

1. The vulnerable time for CSMA is the propagation time Tp . This is the time needed for a signal to propagate from one end of the medium to the other.
2. When a station sends a frame, and any other station tries to send a frame during this time, a collision will result.
3. But if the first bit of the frame reaches the end of the medium, every station will already have heard the bit and will refrain from sending.
4. Figure shows the worst case. The leftmost station A sends a frame at time tl' which reaches the rightmost station D at time tl + Tp . The gray area shows the vulnerable area in time and space.

#Persistence Methods

I-Persistent :

1. The I-persistent method is simple and straightforward. In this method, after the station finds the line idle, it sends its frame immediately (with probability I).
2. This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

Non persistent:

1. In the non persistent method, a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again.
2. The non persistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.
3. However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

p-Persistent:

1. The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time.
2. The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency.

3. In this method, after the station finds the line idle it follows these steps:
    - With probability p, the station sends its frame.
    - With probability q = 1 - p, the station waits for the beginning of the next time slot and checks the line again.

      a. If the line is idle, it goes to step 1.

      b. If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

1. The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.
2. In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.
3. To better understand CSMA/CD, let us look at the first bits transmitted by the two stations involved in the collision. Although each station continues to send bits in the frame until it detects the collision, we show what happens as the first bits collide.
4. In Figure, stations A and C are involved in the collision.

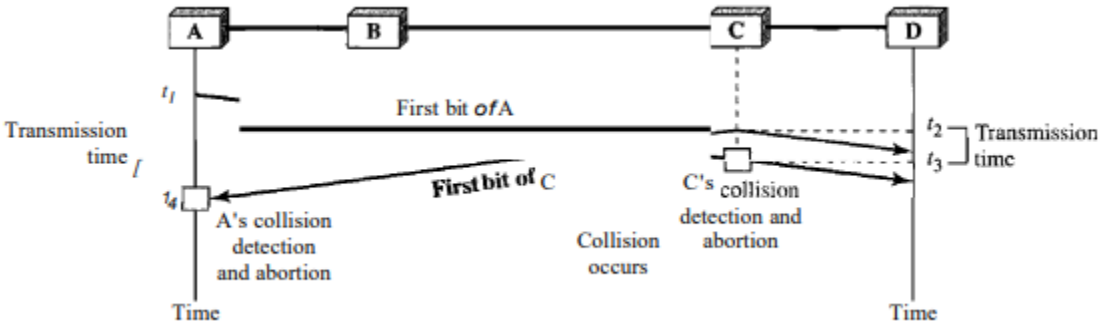


Figure: Collision of the first bit in CSMA / CD

5. At time t 1, station A has executed its persistence procedure and starts sending the bits of its frame. At time t2, station C has not yet sensed the first bit sent by A. Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right.
6. The collision occurs sometime after time t2' Station C detects a collision at time t3 when it receives the first bit ofA's frame. Station C immediately (or after a short time, but we assume immediately) aborts transmission.
7. Station A detects collision at time t4 when it receives the first bit of C's frame; it also immediately aborts transmission. Looking at the figure, we see that A transmits for the duration t4 - tl; C transmits for the duration t3 - t2' Later we show that, for the protocol to work, the length of any frame divided by the bit rate in this protocol must be more than either of these durations.
8. At time t4, the transmission of A:s frame, though incomplete, is aborted; at time t 3, the transmission of B's frame, though incomplete, is aborted.

#Minimum Frame Size:

1. For CSMAICD to work, we need a restriction on the frame size. Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission. This is so because the station, once the entire frame is sent, does not keep a copy of the frame and does not monitor the line for collision detection.
2. Therefore, the frame transmission time Tfr must be at least two times the maximum propagation time Tp. To understand the reason, let us think about the worst-case scenario.
3. If The two stations involved in a collision are the maximum distance apart, the signal from the first takes time Tp to reach the second, and the effect of the collision takes another time Tp to reach the first. So the requirement is that the first station must still be transmitting after 2Tp .

#Flow diagram for the CSMA/CD:

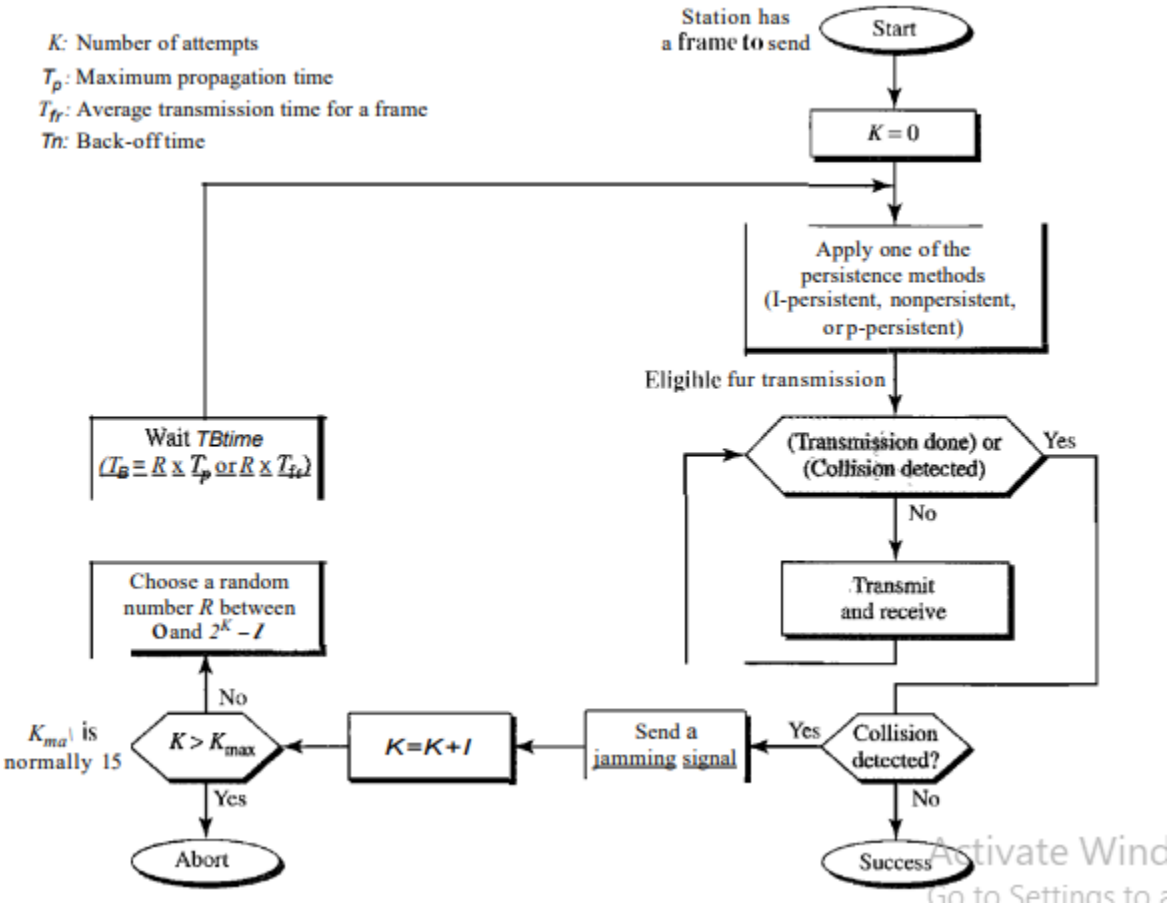


Figure: Flow diagram for the CSMA/CD

#Throughput

1. The throughput of CSMAICD is greater than that of pure or slotted ALOHA. The maximum throughput occurs at a different value of G and is based on the persistence method and the value of p in the p-persistent approach.
2. For I-persistent method the maximum throughput is around 50 percent when G =1. For nonpersistent method, the maximum throughput can go up to 90 percent when G is between 3 and 8.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

1. The basic idea behind CSMA/CD is that a station needs to be able to receive while transmitting to detect a collision. When there is no collision, the station receives one signal: its own signal. When there is a collision, the station receives two signals: its own signal and the signal transmitted by a second station.
2. To distinguish between these two cases, the received signals in these two cases must be significantly different. In other words, the signal from the second station needs to add a significant amount of energy to the one created by the first station.
3. In a wired network, the received signal has almost the same energy as the sent signal because either the length of the cable is short or there are repeaters that amplify the energy between the sender and the receiver. This means that in a collision, the detected energy almost doubles.
4. However, in a wireless network, much of the sent energy is lost in transmission. The received signal has very little energy. Therefore, a collision may add only 5 to 10 percent additional energy. This is not useful for effective collision detection.
5. We need to avoid collisions on wireless networks because they cannot be detected. Carrier sense multiple access with collision avoidance (CSMAICA) was invented for this network. Collisions are avoided through the use ofCSMAICA's three strategies: the interframe space, the contention window, and acknowledgments, as shown in Figure.

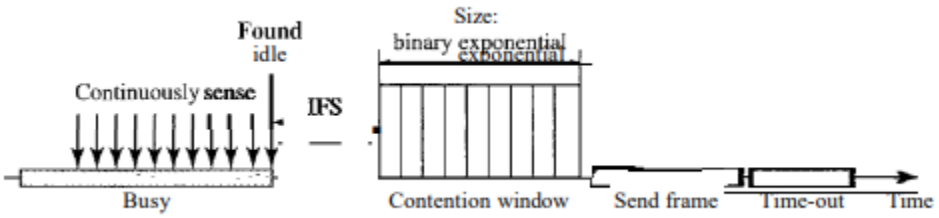


Figure: Timing in CSMA/CA

#Interframe Space (IFS)

1. First, collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period of time called the interframe space or IFS.
2. In CSMAICA, the IFS can also be used to define the priority of a station or a frame.

#Contention Window

3. The contention window is an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time. The number of slots in the window changes according to the binary exponential back-off strategy.
4. In CSMAICA, if the station finds the channel busy, it does not restart the timer of the contention window; it stops the timer and restarts it when the channel becomes idle.

#Procedure

Figure shows the procedure. Note that the channel needs to be sensed before and after the IFS. The channel also needs to be sensed during the contention time. For each time slot of the contention window, the channel is sensed. If it is found idle, the timer continues; if the channel is found busy, the timer is stopped and continues after the timer becomes idle again.

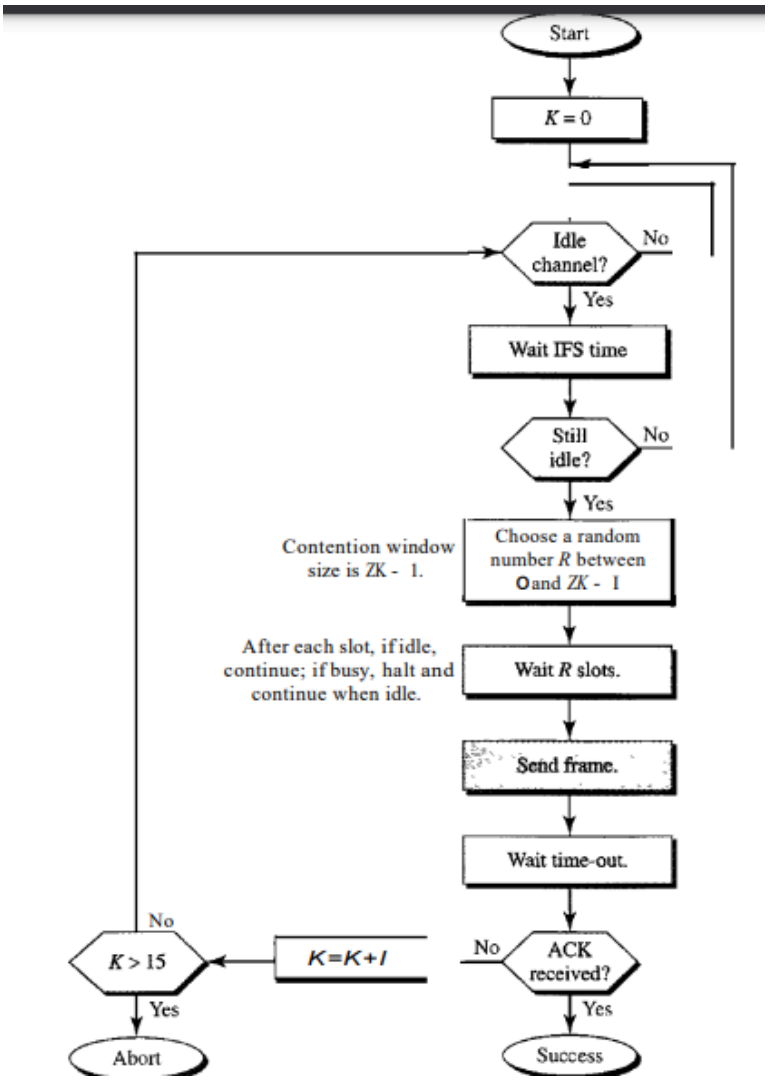


Figure: Flow diagram for CSMA/CA

#Acknowledgment

With all these precautions, there still may be a collision resulting in destroyed data. In addition, the data may be corrupted during the transmission. The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.

#CSMAICA and Wireless Networks

CSMAICA was mostly intended for use in wireless networks. The procedure described above, however, is not sophisticated enough to handle some particular issues related to wireless networks, such as hidden terminals or exposed terminals. We will see how these issues are solved by augmenting the above protocol with hand-shaking features.

6.3 Wireless LANs : Wireless communication system, Bluetooth Architecture, Bluetooth layers connecting LANs , Wi-Fi Architecture ,Wi-Fi connecting LAN, Introduction to Li-Fi.

Wireless communication system

1. Wireless communication systems use radio-frequency, infrared, microwave or other types of electromagnetic or acoustic waves in place of wires, cables or fibre optics to transmit signals or data.
2. Wireless communications, System using radio-frequency, infrared, microwave, or other types of electromagnetic or acoustic waves in place of wires, cables, or fibre optics to transmit signals or data.
3. Wireless devices include cell phones, two-way radios, remote garage-door openers, television remote controls, and GPS receivers (*see* Global Positioning System).
4. Wireless modems, microwave transmitters, and satellites make it possible to access the Internet from anywhere in the world.

What is Wireless Communication

- Wireless communication is a method of transmitting information from one point to another without using any connection like wires, cables or any physical medium.

- Wireless communication doesn't require any physical medium but propagates the signal through space.

Why Wireless Communication

- The primary and important benefit of wireless communication is mobility.

- Wireless communication also offers flexibility and ease of use, which makes it increasingly popular day by day.

Basic Elements of a Wireless Communication System

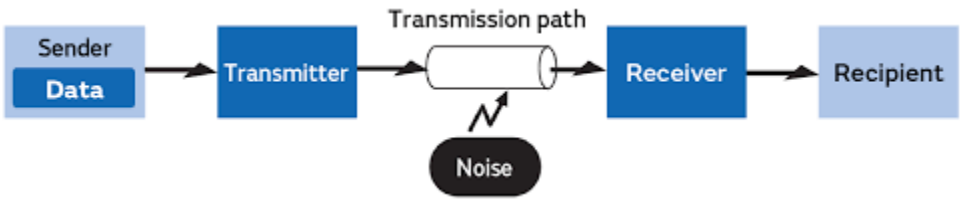


Figure: Wireless Communication System

- The Transmitter

A transmitter is a crucial component in a wireless communication system, responsible for sending information over the airwaves.

Here are some uses of a transmitter:

1. Converting information into signals: The transmitter converts the original information (e.g., sound, image, or data) into a suitable format for transmission over the airwaves.

2. Modulating the signal: The transmitter modulates the signal to encode the information onto a carrier wave, making it possible to transmit multiple signals simultaneously.

3. Amplifying the signal: The transmitter amplifies the modulated signal to increase its strength and range.

4. Transmitting the signal: The transmitter sends the amplified signal into the airwaves through an antenna.

5. Wireless communication: Transmitters are used in various wireless communication systems.

- The Channel

In wireless communication, a channel refers to the medium through which information is transmitted between a transmitter and a receiver.

Here are some uses of a channel:

1. Transmission medium: The channel acts as a transmission medium, allowing signals to propagate from the transmitter to the receiver.

2. Signal propagation: The channel enables signals to travel through the airwaves, wirelessly connecting devices.

3. Frequency allocation: Channels are allocated specific frequency bands to minimize interference and ensure efficient use of the spectrum.

4. Bandwidth allocation: Channels are assigned bandwidth, determining the amount of data that can be transmitted simultaneously.

5. Multiplexing: Channels can be multiplexed, allowing multiple signals to share the same frequency band, increasing transmission efficiency.

6. Error correction: Channels can use error correction techniques to detect and correct errors that occur during transmission.

7. Security: Channels can be encrypted to ensure secure transmission and prevent unauthorized access.

8. Interference management: Channels can use techniques like frequency hopping and spread spectrum to mitigate interference.

9. Channel sharing: Channels can be shared among multiple devices, enabling wireless networking and communication.

- The Receiver

A receiver is a device or component that detects and decodes signals transmitted through a communication channel.

Here are some uses of a receiver:

1. Signal detection: Receivers detect signals transmitted through the airwaves, wirelessly or through a physical medium.

2. Decoding and demodulation: Receivers decode and demodulate the received signals to extract the original information.

3. Amplification: Receivers amplify the weak signals to increase their strength and quality.

4. Noise reduction: Receivers use techniques like filtering and amplification to reduce noise and interference.

5. Error correction: Receivers use error correction techniques to detect and correct errors that occur during transmission.

6. Data extraction: Receivers extract the original data or information from the received signals.

7. Wireless communication: Receivers are used in various wireless communication systems, such as:

- Radio broadcasting
- Mobile phones
- Wi-Fi
- Bluetooth
- Satellite communication

Advantages of Wireless Communication

- Cost
- Mobility
- Ease of Installation
- Reliability
- Disaster Recovery

Disadvantages of Wireless Communication

- Interference
- Security
- Health Concerns

BLUETOOTH

1. Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, and so on.
2. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet. A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability. A Bluetooth LAN, by nature, cannot be large.
3. If There are many gadgets that try to connect, there is chaos. Bluetooth technology has several applications. Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology. Monitoring devices can communicate with sensor devices in a small health care center.
4. Home security devices can use this technology to connect different sensors to the main security controller. Conference attendees can synchronize their laptop computers at a conference.
5. Bluetooth was originally started as a project by the Ericsson Company. It is named for Harald Blaatand, the king of Denmark (940-981) who united Denmark and Norway. Blaatand translates to Bluetooth in English.
6. Today, Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard. The standard defines a wireless personal-area network (PAN) operable in an area the size of a room or a hall.

Bluetooth Architecture,

Bluetooth defines two types of networks: piconet and scatternet.

Piconets:

1. A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries.
2. All the secondary stations synchronize their clocks and hopping sequence with the primary. Note that a piconet can have only one primary station.
3. The communication between the primary and the secondary can be one-to-one or one-to-many. Figure shows a piconet.

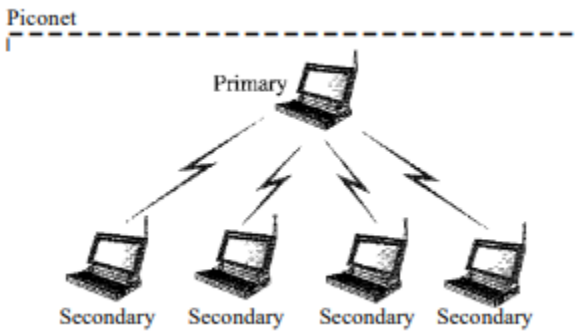


Figure: Piconet

4. Although a piconet can have a maximum of seven secondaries, an additional eight secondaries can be in the parked state.

5. A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state.
6. Because only eight stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

Scatternet:

1. Piconets can be combined to form what is called a scatternet. A secondary station in one piconet can be the primary in another piconet.
2. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets.
3. Figure Illustrates a scatternet.

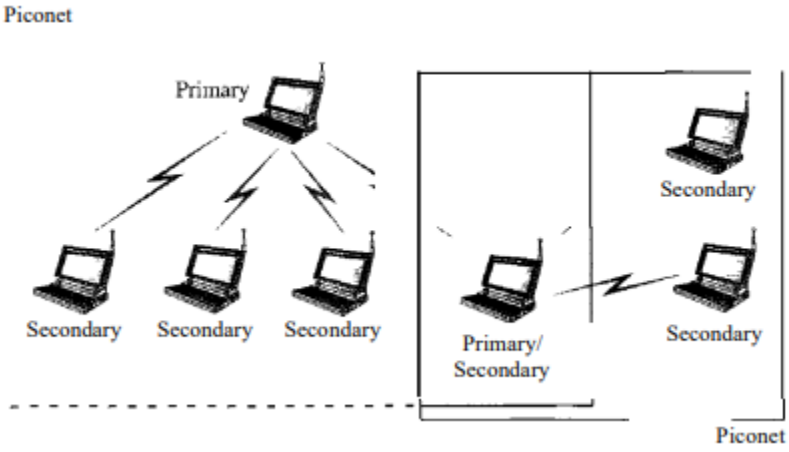


Figure: Scatternet

Bluetooth Devices

1. A Bluetooth device has a built-in short-range radio transmitter. The current data rate is 1 Mbps with a 2.4-GHz bandwidth.
2. This means that there is a possibility of interference between the IEEE 802.11b wireless LANs and Bluetooth LANs.

Bluetooth layers connecting LANs

Bluetooth uses several layers that do not exactly match those of the Internet model we have defined in this book. Figure shows these layers.

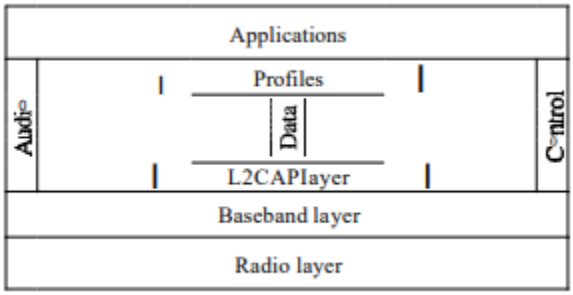


Figure: Bluetooth layers

#Radio Layer

The radio layer is roughly equivalent to the physical layer of the Internet model. Bluetooth devices are low-power and have a range of 10 m.

Band

Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.

FHSS

Bluetooth uses the frequency-hopping spread spectrum (FHSS) method in the physical layer to avoid interference from other devices or other networks. Bluetooth hops 1600 times per second, which means that each device changes its modulation frequency 1600 times per second. A device uses a frequency for only 625 Ils (1/1600 s) before it hops to another frequency; the dwell time is 625 Ils.

Modulation

To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK (FSK with Gaussian bandwidth filtering; a discussion of this topic is beyond the scope of this book). GFSK has a can'ier frequency. Bit 1 is represented by a frequency deviation above the carrier; bit ais represented by a frequency deviation below the carrier. The frequencies, in megahertz, are defined according to the following formula for each channel:

fc=2402+n n =0, 1,2,3, ..., 78

For example, the first channel uses carrier frequency 2402 MHz (2.402 GHz), and the second channel uses carrier frequency 2403 MHz (2.403 GHz).

#Baseband Layer

1. The baseband layer is roughly equivalent to the MAC sublayer in LANs. The access method is TDMA. The primary and secondary communicate with each other using time slots. The length of a time slot is exactly the same as the dwell time, 625 Ils.
2. This means that during the time that one frequency is used, a sender sends a frame to a secondary, or a secondary sends a frame to the primary. Note that the communication is only between the primary and a secondary; secondaries cannot communicate directly with one another.

#L2CAP

1. The Logical Link Control and Adaptation Protocol, or L2CAP (L2 here means LL), is roughly equivalent to the LLC sublayer in LANs.
2. It is used for data exchange on an ACL link; SCQ channels do not use L2CAP. Figure 14.25 shows the format of the data packet at this level.
3. The I6-bit length field defines the size of the data, in bytes, coming from the upper layers. Data can be up to 65,535 bytes. The channel ID (CID) defines a unique identifier for the virtual channel created at this level.

4. The L2CAP has specific duties: multiplexing, segmentation and reassembly, quality of service (QoS), and group management.

Profile

- Controller Layers (Physical, Link Manager, L2CAP): Manage the connection and data transmission.

- Host Layers (SDP, RFCOMM, TCS, AVCTP, AVDTP, OBEX, DMP): Provide services and applications for device interaction.

Application

The Application Layer of Bluetooth is responsible for providing services and interfaces for applications to use the Bluetooth connectivity. This layer is divided into several protocols that enable various applications to communicate over Bluetooth.

Some of the key protocols in the Application Layer of Bluetooth are:

1. Serial Port Profile (SPP): Emulates a serial cable connection over Bluetooth, enabling applications to use Bluetooth as a wireless replacement for serial cables.

2. Object Push Profile (OPP): Enables the exchange of objects, such as files, between devices.

3. File Transfer Profile (FTP): Allows devices to transfer files over Bluetooth.

4. Headset Profile (HSP): Enables Bluetooth headsets to communicate with devices.

5. Hands-Free Profile (HFP): Enables hands-free phone use, including voice commands and audio streaming.

6. Advanced Audio Distribution Profile (A2DP): Streams high-quality audio from devices to Bluetooth speakers or headsets.

7. Audio/Video Remote Control Profile (AVRCP): Enables remote control of audio and video playback on devices.

8. Personal Area Networking Profile (PAN): Enables devices to form a personal area network, allowing them to share internet connections and files.

9. Device ID Profile (DID): Enables devices to identify themselves and their capabilities to other devices.

10. Health Device Profile (HDP): Enables devices to share health-related data, such as heart rate and blood pressure.

Wi-Fi Architecture , Wi-Fi connecting LAN, Introduction to Li-Fi.

Wi-Fi Architecture

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 :

1. 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).
2. Figure shows two sets in this standard. The BSS without anAP is a stand-alone network and cannot send data to other BSSs.
3. 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.
4. A BSS without an AP is called an ad hoc network; a BSS with an AP is called an infrastructure network.

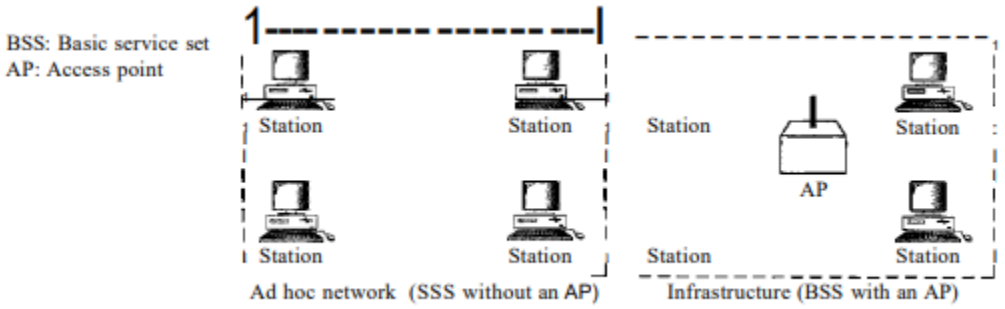


Figure: Basic service sets (BSSs)

Extended Service Set:

1. 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.
2. 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.
3. Note that the extended service set uses two types of stations: mobile and stationary. The mobile stations are normal stations inside a BSS.
4. The stationary stations are AP stations that are part of a wired LAN. Figure Shows an ESS.

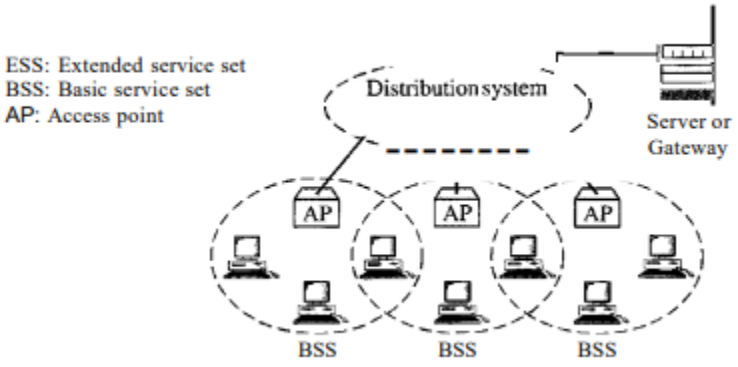


Figure:Extended service sets (ESSs)

5. 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.
6. The idea is similar to communication in a cellular network if we consider each BSS to be a cell and each AP to be a base station. Note that a mobile station can belong to more than one BSS at the same time.

Station Types:

1. IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN: no-transition, BSS·transition, and ESS-transition mobility.
2. IEEE 802.11 423 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.
3. 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.

Wi-Fi connecting LAN

WiFi connects to a Local Area Network (LAN) through the following steps:

1. WiFi Client Discovery: The WiFi client (e.g., laptop, smartphone) searches for available WiFi networks.

2. Association: The client selects a network and sends an association request to the Access Point (AP).

3. Authentication: The AP requests authentication credentials (e.g., password, username) from the client.

4. Authorization: The AP verifies the credentials and grants access to the network.

5. DHCP: The client receives an IP address and other network settings from a DHCP server.

6. LAN Connection: The client is now connected to the LAN, allowing communication with other devices on the network.

7. Internet Access: The client can access the internet through the LAN's internet connection.

The WiFi connection to LAN enables devices to:

- Access shared resources (e.g., files, printers)

- Communicate with other devices on the network

- Connect to the internet

- Use network services (e.g., DNS, DHCP)

The WiFi network is typically connected to a wired LAN through an Access Point (AP) or a Wireless Router, which acts as a bridge between the wireless and wired networks.

Introduction to Li-Fi

1. LiFi is a new wireless communication technology that uses visible light to transmit data. It is said to be able to provide 100 times faster internet connectivity than existing WiFi offerings.
2. LiFi works by using visible light, like the light that is emitted by any regular lamp or bulb, to transmit data.
3. The advantage of LiFi is that it uses the visible light spectrum, which is almost 10,000 times larger than the spectrum occupied by radio waves.
4. LiFi is a wireless communication technology that uses visible light to transmit data [1]. Here are some key points about LiFi.
5. LiFi is a high-speed wireless communication technology that uses visible light (presently using LEDs) to transmit information.

How LiFi works:

- LiFi uses LED light bulbs to transmit data.

- The LED light is switched on and off at a very high speed, beyond the human eye's ability to notice.

- This switching on and off of the light is used to transmit data.

Advantages of LiFi:

- LiFi can provide 100 times faster internet connectivity than existing WiFi offerings.

- LiFi uses the visible light spectrum, which is almost 10,000 times larger than the spectrum occupied by radio waves.

- LiFi is more suitable in electromagnetic-sensitive areas like hospitals, airplane cabins, and nuclear power plants.

Disadvantages of LiFi:

- LiFi would be useless in conditions where there is no light.

- LiFi has high installation charges.

- LiFi is less reliable due to its dependence on visible light.

Comparison with WiFi:

- LiFi uses visible light to transmit data, while WiFi uses radio waves.

- LiFi has a shorter range than WiFi and is unable to penetrate walls.

- LiFi is more secure than WiFi because the data is confined to the immediate environment and cannot be intercepted by unauthorized entities outside the designated space.