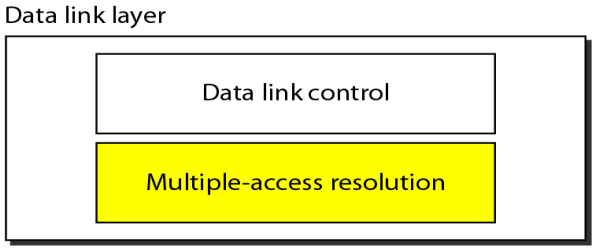
UNIT-III Multiple Access

Syllabus:

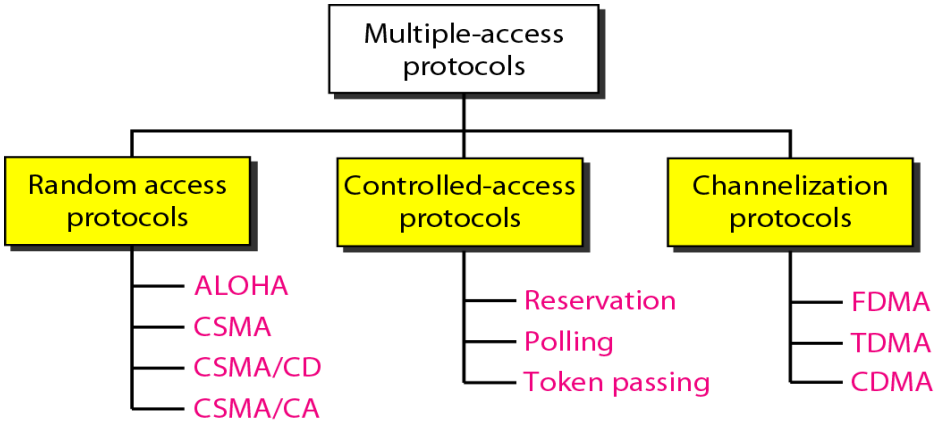
Medium Access Sub layer: Channel allocation problem, Controlled Access, Channelization multiple access protocols, IEEE standard 802.3 & 802.11 for LANS and WLAN, high-speed LANs, Token ring, Token Bus, FDDI based LAN, Network Devices- repeaters, hubs, switches bridges.

Multiple Access Control Protocols

Data link layer is divided into two sub layers such as data link control, multiple access resolution. Data link control main responsibility is error and flow controlling; this layer is also called logical link control (LLC). Multiple access resolution is also called media access control (MAC).



When nodes or stations are connected and use a common link, called a multipoint or broadcast link, we need a multiple-access protocol to coordinate access to the link. All of these protocols belongs to a sub-layer in the data-link layer called media access control (MAC). We categorize them into three groups, as shown in Figure



RANDOM ACCESS PROTOCOLS

In random-access or contention methods, no station is superior to another station andnone is assigned control over another. At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send .

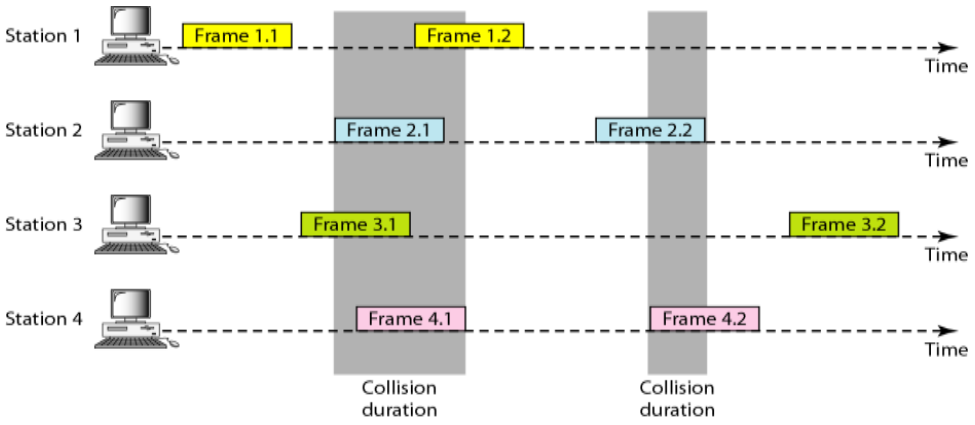
Two features give this method its name. First, there is no scheduled time for a station to transmit. Transmission is random among the stations. That is why these methods are called random access. Second, no rules specify which station should send next.

ALOHA

ALOHA, the earliest random access method, was developed at the University of Hawaiin early 1970. It was designed for a radio (wireless) LAN, but it can be used on any shared medium.

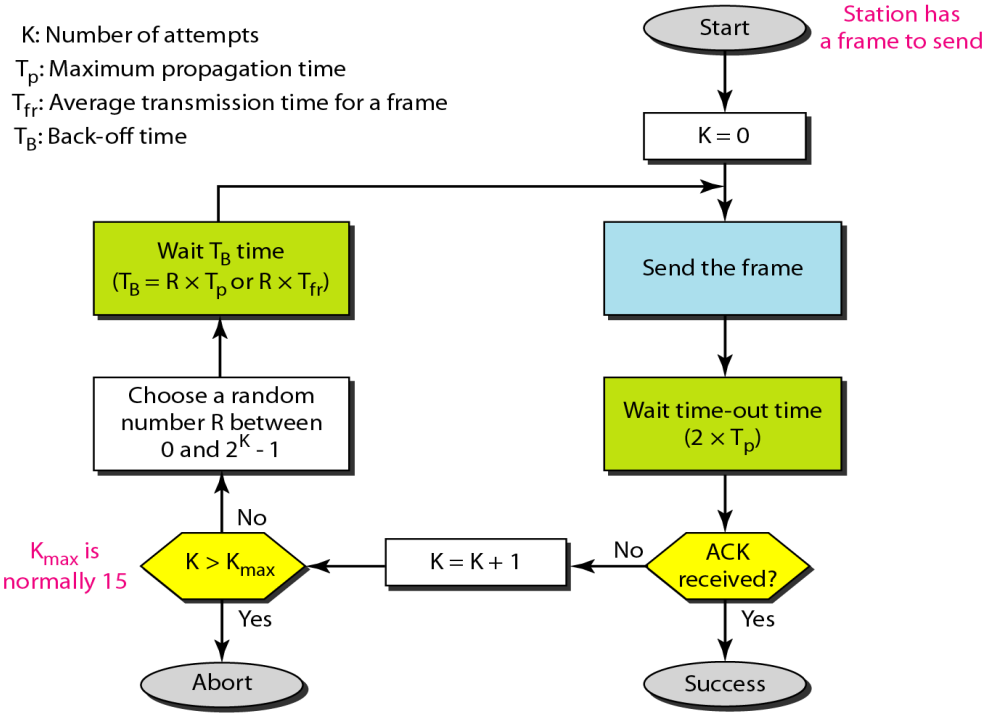
Pure ALOHA

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 (multiple Access). 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.



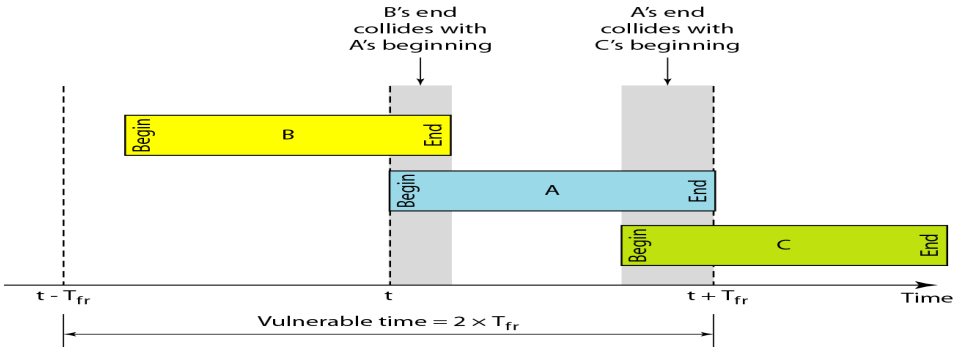
There are four stations that contend with one another for access to the shared channel. The figure shows that each station sends two frames; there are a total of eight frames on the shared medium. Some of these frames collide because multiple frames are in contention for the shared channel. Fig. shows that only two frames survive: one frame from station 1 and one frame from station 3.

The pure ALOHA protocol relies on acknowledgments from the receiver. When a station sends a frame, it expects the receiver to send an acknowledgment. If the acknowledgment does not arrive after a time-out period, the station assumes that the frame 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. The randomness will help avoid more collisions. We call this time the back-off time TB.



Vulnerable time

Let us find the vulnerable time, the length of time in which there is a possibility of collision.We assume that the stations send fixed-length frames with each frame taking T_{fr} seconds to send. Figure shows the vulnerable time for station A.



Station A starts to send a frame at time t. Now imagine station C has started to send its frame after t (between t to t + T_{fr}). This leads to a collision between the frames from station C and station A. On the other hand, suppose that station B starts to send a frame before time t (between t to t -T_{fr}). Here, there is also a collision between frames from station B and station A .Looking at Figure, we see that the vulnerable time during which a collision may occur in pure ALOHA is 2 times the frame transmission time. Therefore, if a station generates only one frame in this vulnerable time (and no other stations generate a frame during this time), the frame will reach its destination successfully.

Pure ALOHA vulnerable time = 2 × T_{fr}

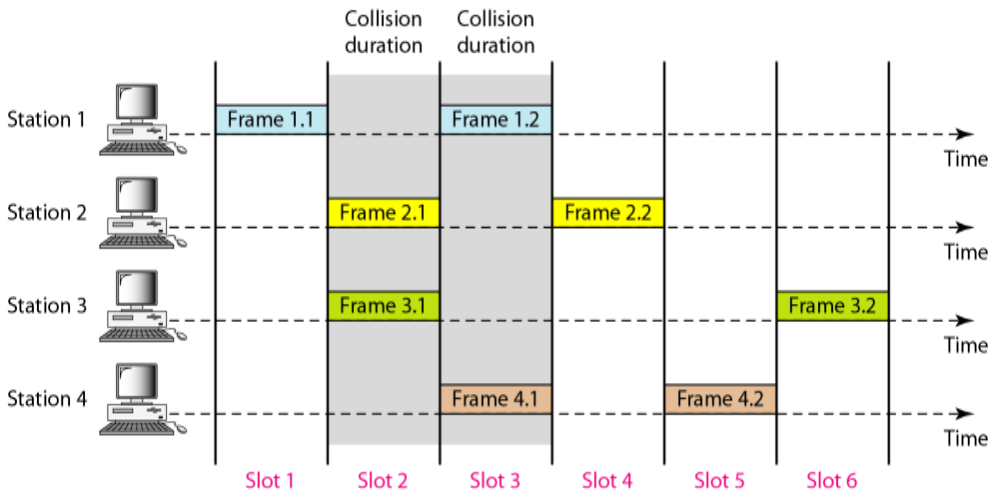
Throughput

Let us call G the average number of frames generated by the system during one frame transmission time. Then it can be proven that the average number of successfully transmitted frames for pure ALOHA is $\mathbf{S = G \times e^{-2G}}$.

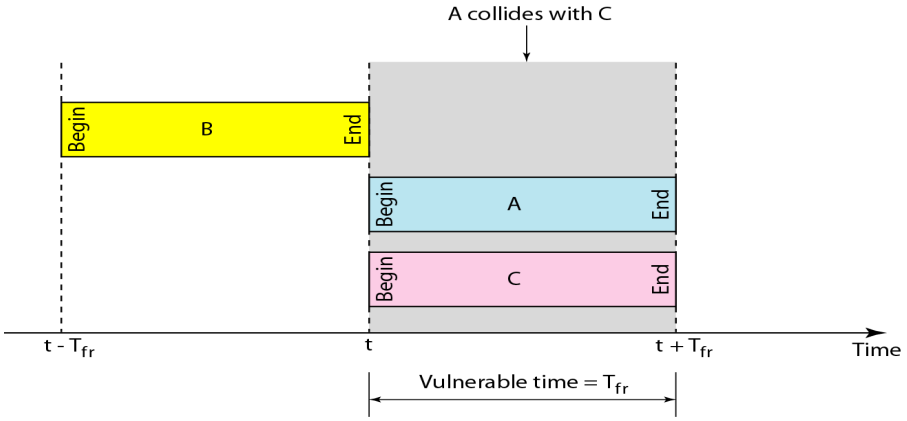
The maximum throughput S_{max} is 0.184,for G =1/2 (one frame during two frame transmission times)

Slotted ALOHA

In slotted ALOHA we divide the time into slots of T_{fr} seconds and force the station to send only at the beginning of the time slot. Figure shows an example of frame collisions in slotted ALOHA.



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. This means that the station which started at the beginning of this slot has already finished sending its frame. Of course, there is still the possibility of collision if two stations try to send at the beginning of the same time slot. However, the vulnerable time is now reduced to one-half, equal to Tfr. Figure shows the situation.



Slotted ALOHA vulnerable time= T_{fr}

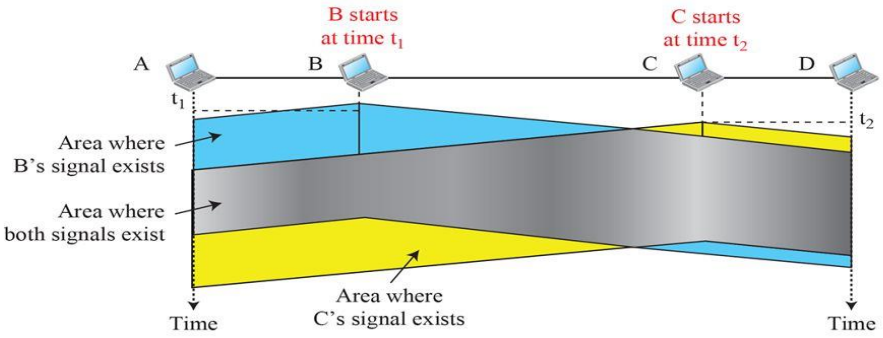
Throughput

It can be proven that the average number of successful transmissions for slotted ALOHA is $S = G \times e^{-G}$. The maximum throughput Smax is 0.368, when G =1.

CSMA

To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The collision can be reduced if a station senses the medium before trying to use it. 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." CSMA can reduce the possibility of collision, but it cannot eliminate it.

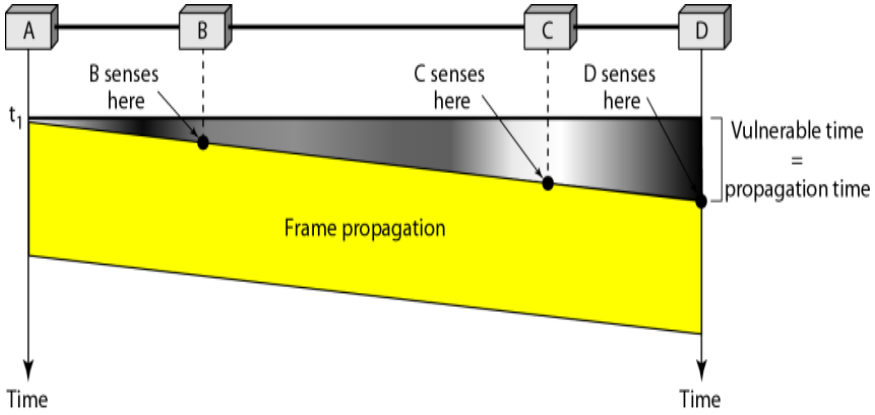
Figure 12.7: Space/time model of a collision in CSMA



At time t1, station B senses the medium and finds it idle, so it sends a frame. At time t2 (t2 > t1), 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

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. When a station sends a frame and any other station tries to send a frame during this time, a collision will result.

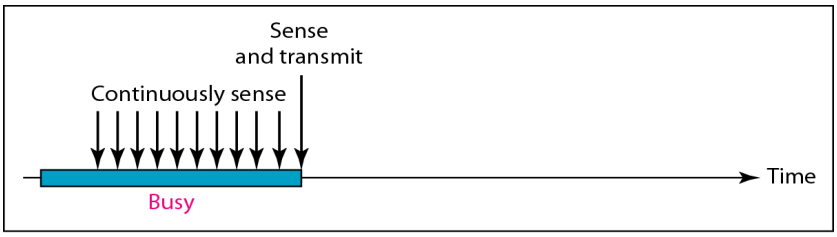


Persistence Methods

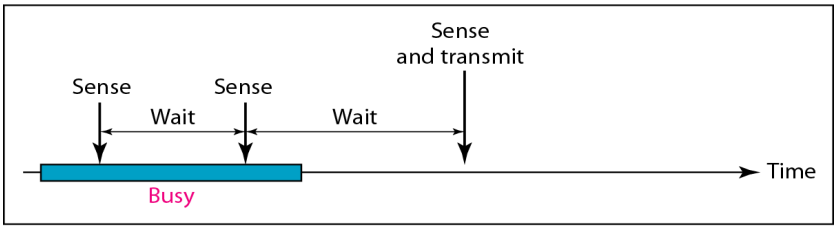
What should a station do if the channel is busy? What should a station do if the channel is idle? Three methods have been devised to answer these questions: the 1-persistent method, the non persistent method, and the p-persistent method. Figure shows the behavior of three persistence methods when a station finds a channel busy.

1-Persistent

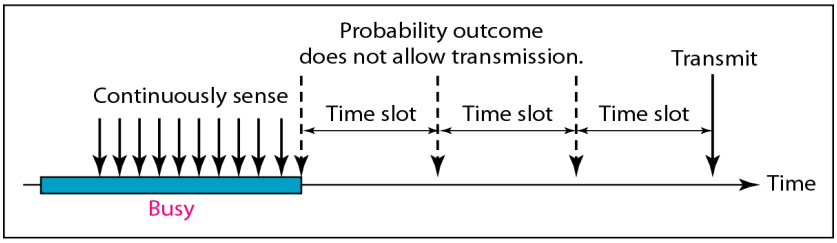
The 1-persistent method is simple and straightforward. In this method, after the station finds the line idle, it sends its frame immediately (with probability 1). This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.



a. 1-persistent



b. Nonpersistent



c. p-persistent

Non persistent

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.

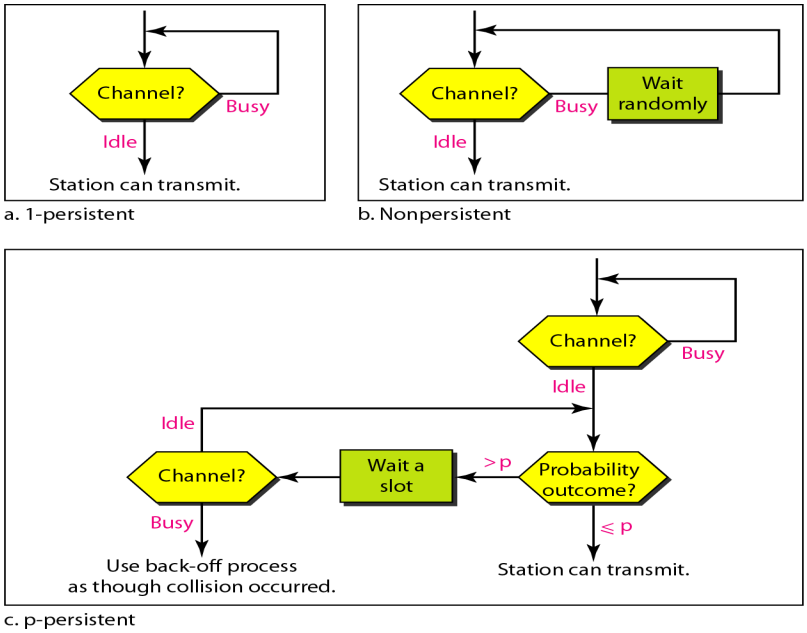
p-Persistent

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. The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency. In this method, after the station finds the line idle it follows these steps:

1. With probability p, the station sends its frame.
2. With probability q =1-p, the station waits for the beginning of the next time slot and checks the line again.

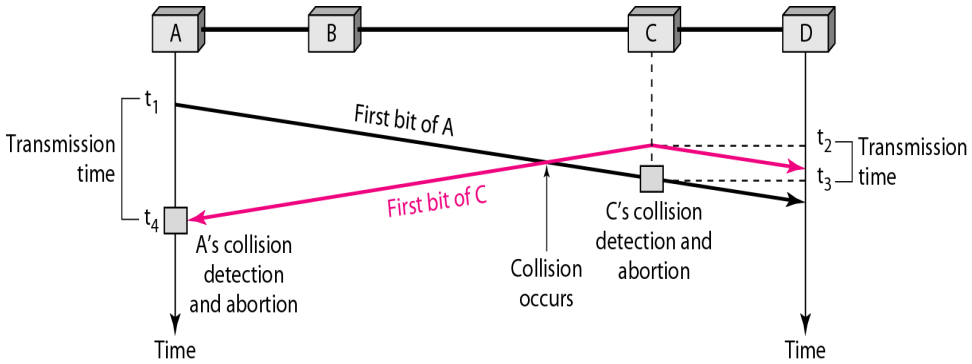
a. If the line is idle, it goes to step 1.

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



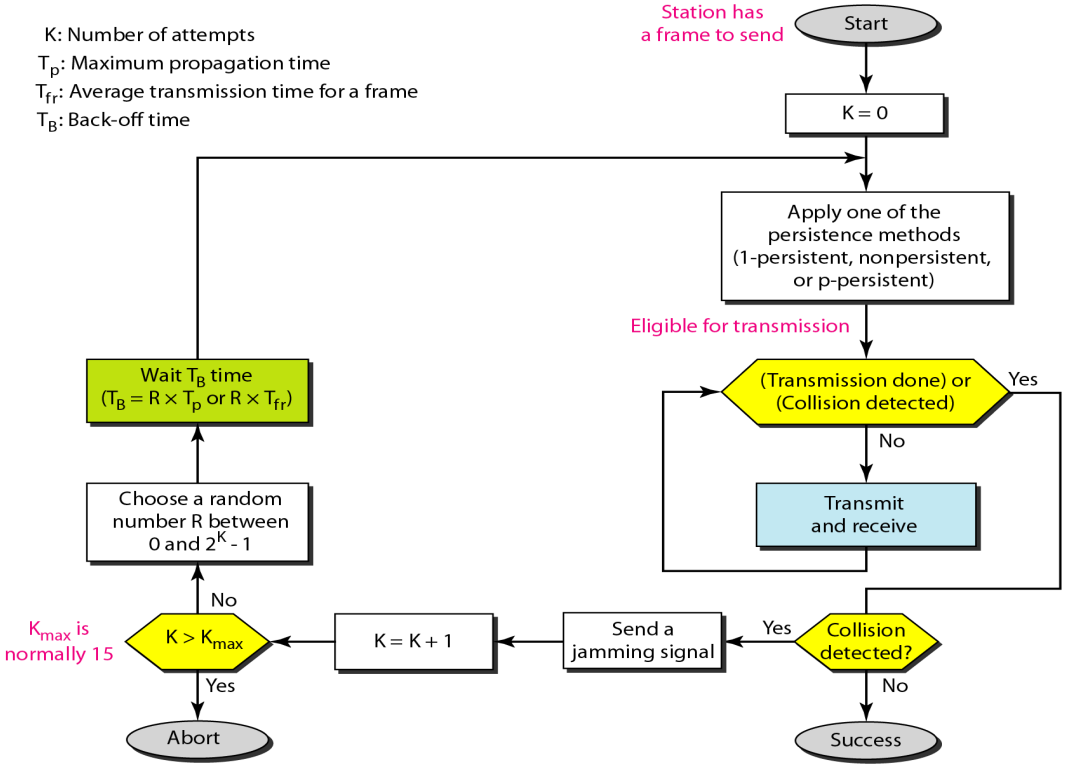
CSMA/CD

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 .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.



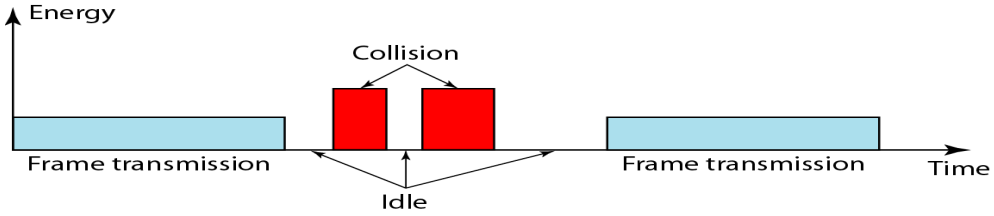
At time t1, station A has executed its persistence procedure and starts sending the bits of its frame. At time t2, station C has not yet sensed the first bit sent by A. Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right. The collision occurs sometime after time t2. Station C detects a collision at time t3 when it receives the first bit of A's frame. Station C immediately aborts transmission. 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 -t1; C transmits for the duration t3 -t2.

To avoid the collision frame transmission time T_{fr} must be at least two times the maximum propagation time *Tp*



Energy Level

We can say that the level of energy in a channel can have three values: zero, normal ,and abnormal. At the zero level, the channel is idle. At the normal level, a station has successfully captured the channel and is sending its frame. At the abnormal level, there is a collision and the level of the energy is twice the normal level.



Throughput

The throughput of CSMA/CD 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. For the 1-persistent method, the maximum throughput is around 50 percent when G =1. For the non-persistent method, the maximum throughput can go up to 90 percent when G is between 3 and 8.

CSMA/CA

Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for wireless networks. Collisions are avoided through the use of CSMA/CA's three strategies: the inter frame space, the contention window, and acknowledgments, as shown in Figure . We discuss RTS and CTS frames later.

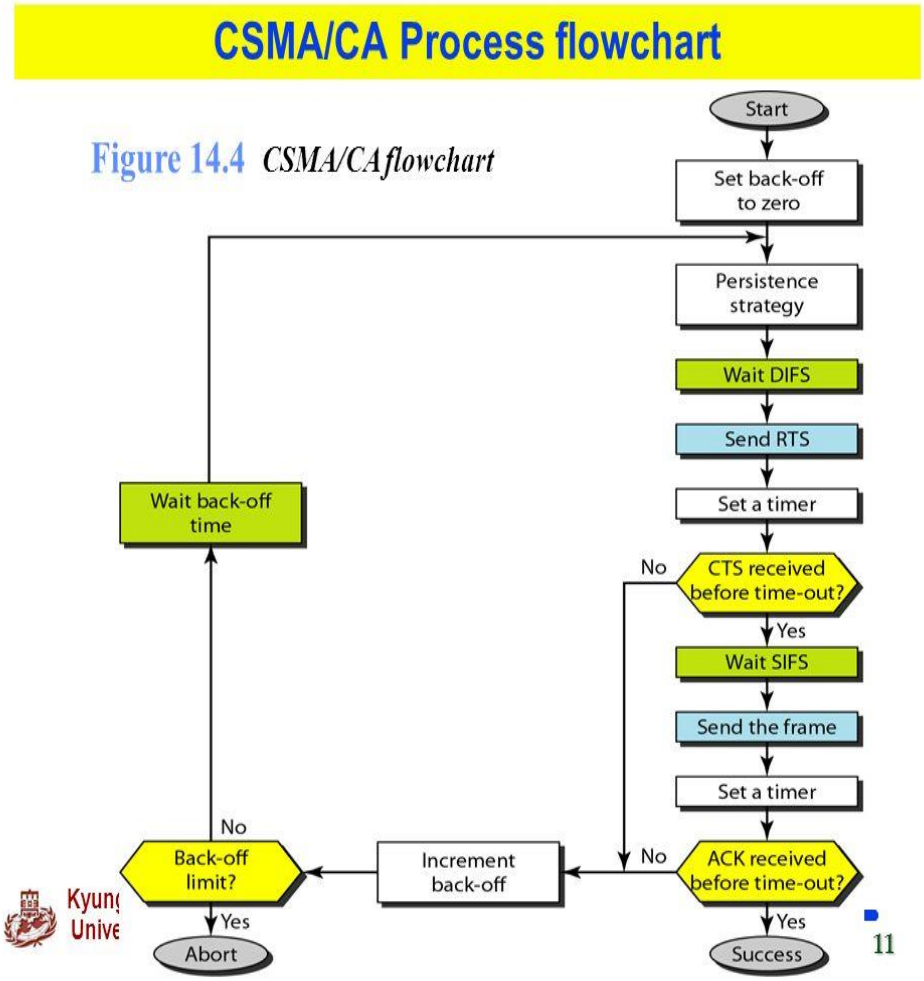
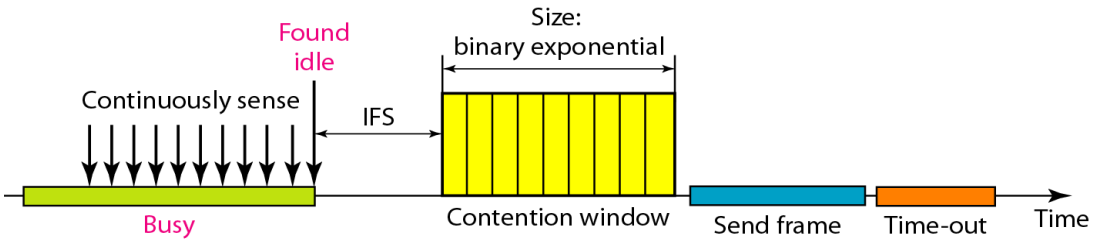


Figure 14.4 *CSMA/CA flowchart*

Inter frame Space (IFS). 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 inter frame space or IFS.

Contention Window. 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.



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. 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.

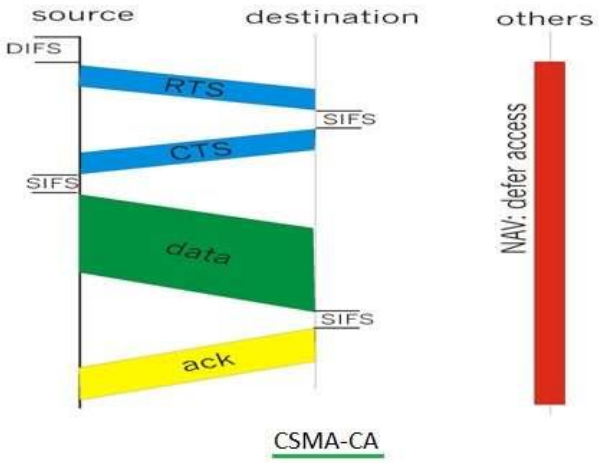
a. The channel uses a persistence strategy with backoff until the channel is idle.

b. After the station is found to be idle, the station waits for a period of time called the DCF 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..

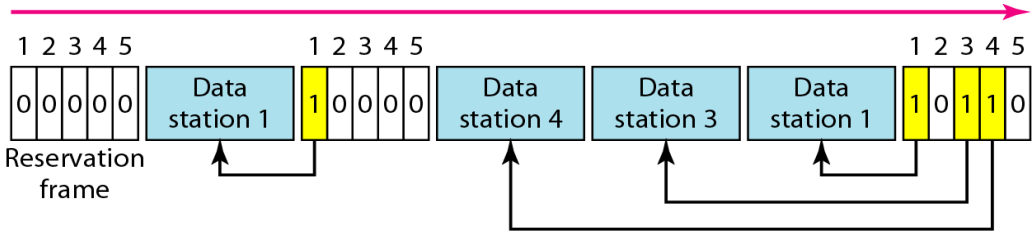


CONTROLLED ACCESS PROTOCOLS

In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations.

Reservation

In the reservation method, a station needs to make a reservation before sending data. Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval. Figure shows a situation with five stations and a five-mini slot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.



Polling

Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations. All data exchanges must be made through the primary

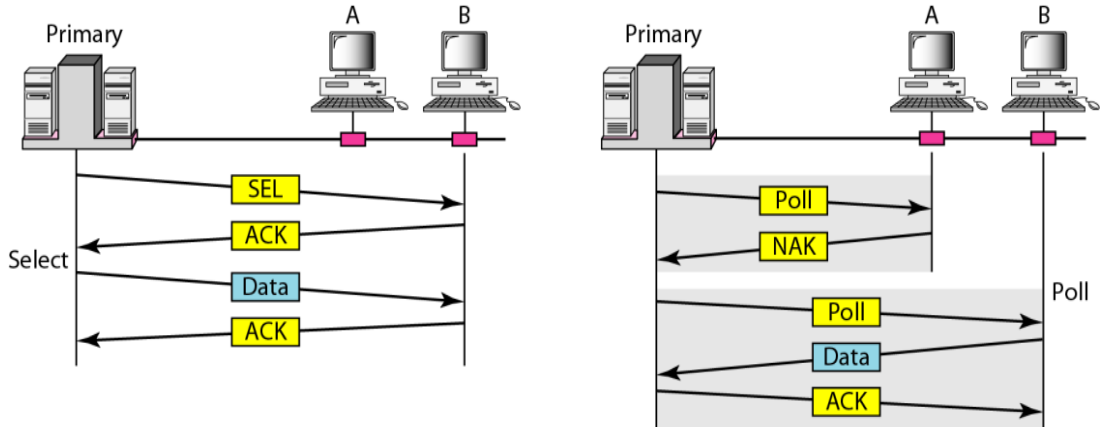
device even when the ultimate destination is a secondary device. The primary device controls the link; the secondary devices follow its instructions. This method uses poll and select functions to prevent collisions.

Select

The select function is used whenever the primary device has something to send . Before sending data, the primary creates and transmits a select (SEL) frame, one field of which includes the address of the intended secondary.

Poll

The poll function is used by the primary device to solicit transmissions from the secondary devices. When the primary is ready to receive data, it must ask (poll) each device in turn if it has anything to send. When the first secondary is approached, it responds either with a NAK frame if it has nothing to send or with data if it does. If the response is negative (a NAK frame), then the primary polls the next secondary in the same manner until it finds one with data to send. When the response is positive (a data frame), the primary reads the frame and returns an acknowledgment (ACK frame), verifying its receipt.



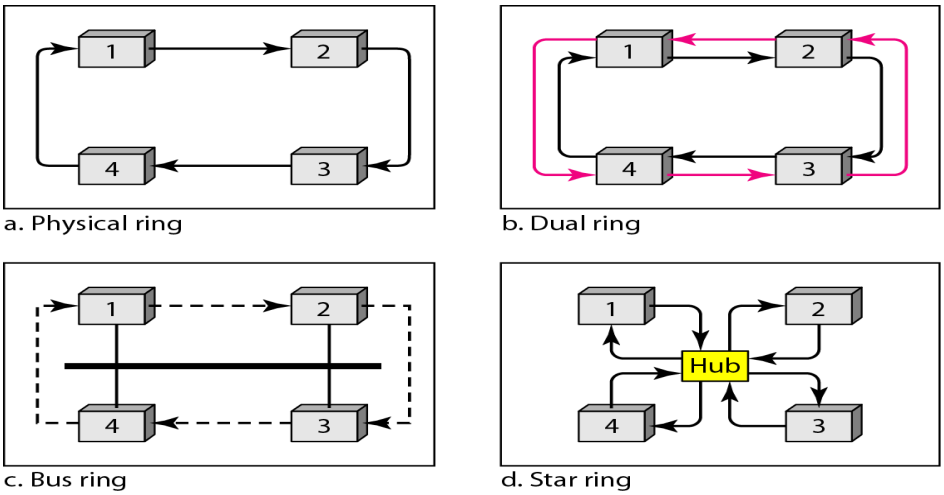
Token Passing

In the token-passing method, the stations in a network are organized in a logical ring. In other words, for each station, there is a predecessor and a successor. The predecessor is the station which is logically before the station in the ring; the successor is the station which is after the station in the ring. The current station is the one that is accessing the channel now. The right to this access has been passed from the predecessor to the current station. The right will be passed to the successor when the current station has no more data to send.

In this method, a special packet called a token circulates through the ring. The possession of the token gives the station the right to access the channel and send its data. When a station has some data to send, it waits until it receives the token from its predecessor. It then holds the token and sends its data. When the station has no more data to send, it releases the token, passing it to the next logical station in the ring. The station cannot send data until it receives the token again in the next round. In this process, when a station receives the token and has no data to send, it just passes the data to the next station.

Logical Ring

In a token-passing network, stations do not have to be physically connected in a ring; the ring can be a logical one. Figure shows four different physical topologies that can create a logical ring.

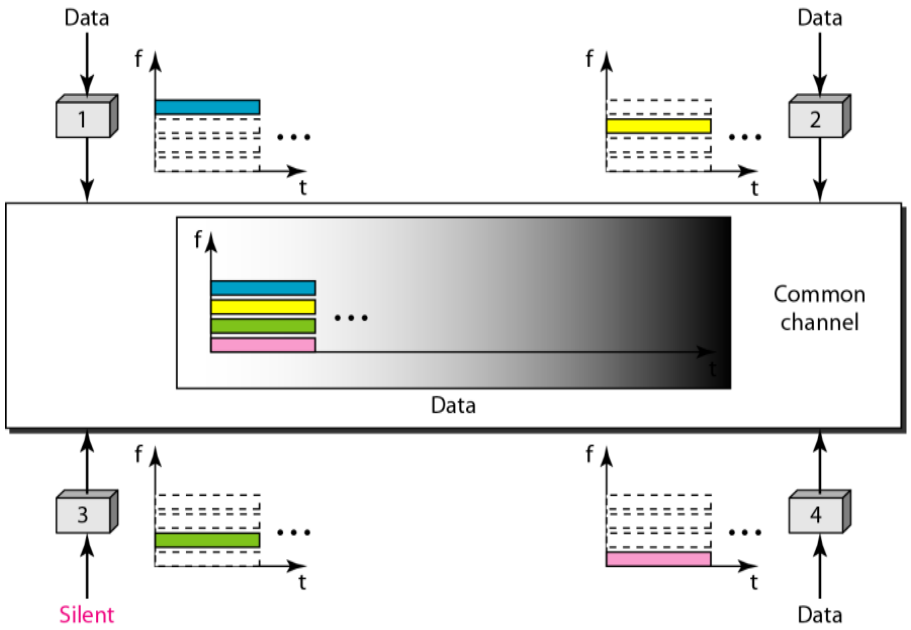


CHANNELIZATION PROTOCOLS

Channelization (or channel partition, as it is sometimes called) is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, among different stations. In this section, we discuss three channelization protocols: FDMA, TDMA, and CDMA.

FDMA

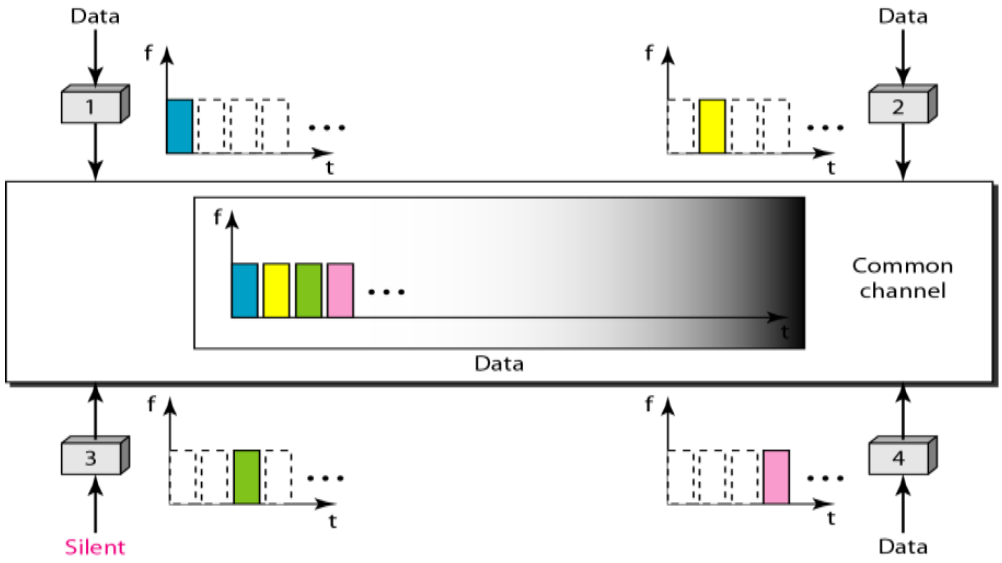
In frequency-division multiple access (FDMA), the available bandwidth is divided into frequency bands. Each station is allocated a band to send its data.. To prevent station interferences, the allocated bands are separated from one another by small guard bands. Figure shows the idea of FDMA.



FDMA specifies a predetermined frequency band for the entire period of communication. This means that stream data (a continuous flow of data that may not be packetized)can easily be used with FDMA.

TDMA

In time-division multiple access (TDMA), the stations share the bandwidth of the channel in time. Each station is allocated a time slot during which it can send data. Each station transmits its data in its assigned time slot. Figure shows the idea behind TDMA.



The main problem with TDMA lies in achieving synchronization between the different stations. Each station needs to know the beginning of its slot and the location of its slot. This may be difficult because of propagation delays introduced in the system if the stations are spread over a large area. To compensate for the delays, we can insert guard times.

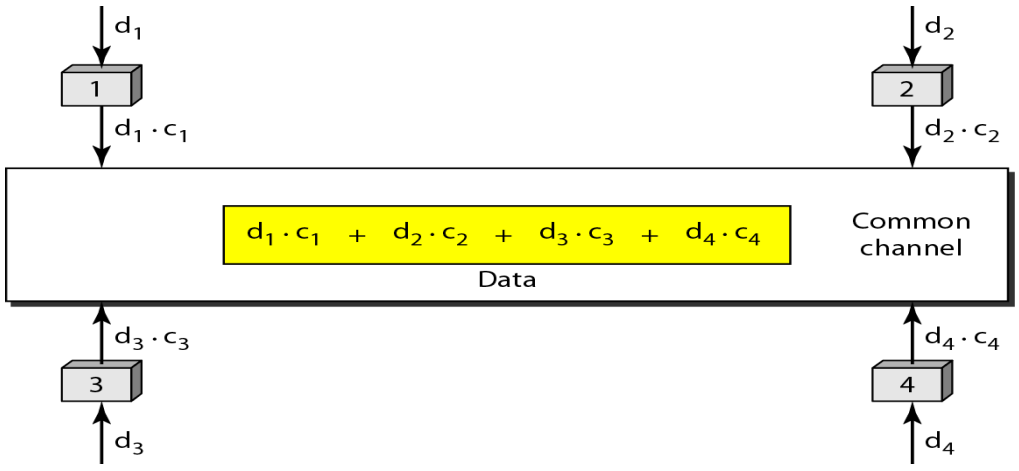
CDMA

Code-division multiple access (CDMA) was conceived several decades ago. Recent advances in electronic technology have finally made its implementation possible. CDMA differs from FDMA in that only one channel occupies the entire bandwidth of the link. It differs from TDMA in that all stations can send data simultaneously; there is no timesharing.

CDMA simply means communication with different codes. Let us assume we have four stations, 1, 2, 3, and 4, connected to the same channel. The data from station 1 are d1, from station 2 are d2, and so on. The code assigned to the first station is c1, to the second is c2, and so on. We assume that the assigned codes have two properties.

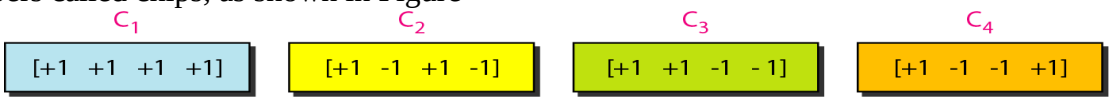
1. If we multiply each code by another, we get 0.
2. If we multiply each code by itself, we get 4 (the number of stations).

With these two properties in mind, let us see how the above four stations can send data using the same common channel, as shown in Figure .Station 1 multiplies its data by its code to get d1 .c1. Station 2 multiplies its data by its code to get d2 .c2, and so on. The data that go on the channel are the sum of all these terms, as shown in the box.



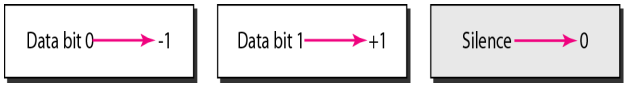
Chips

CDMA is based on coding theory. Each station is assigned a code, which is a sequence of numbers called chips, as shown in Figure



Data Representation

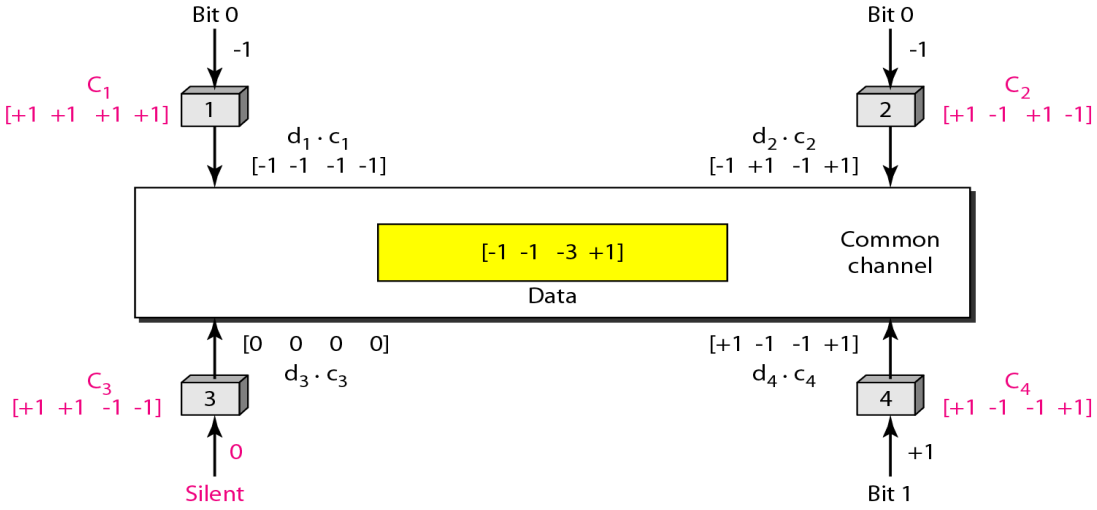
We follow these rules for encoding: If a station needs to send a 0 bit, it encodes it as -1; if it needs to send a 1 bit, it encodes it as +1. When a station is idle, it sends no signal, which is interpreted as a 0. These are shown in Figure



Encoding and Decoding

Now imagine that station 3, which we said is silent, is listening to station 2. Station 3 multiplies the total data on the channel by the station 2 code, which is[+1 -1 +1 -1]to get

$$[-1\text{-}1\ -3\ +1] \bullet [+1\text{-}1\ +1\ -1] = -4/4 = -1$$



Signal Level

The figure shows the corresponding signals for each station (using NRZ-L for simplicity) and the signal that is on the common channel.

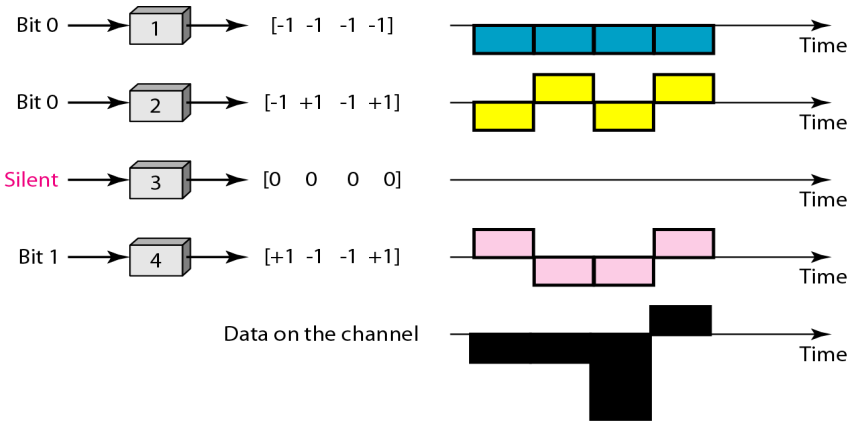
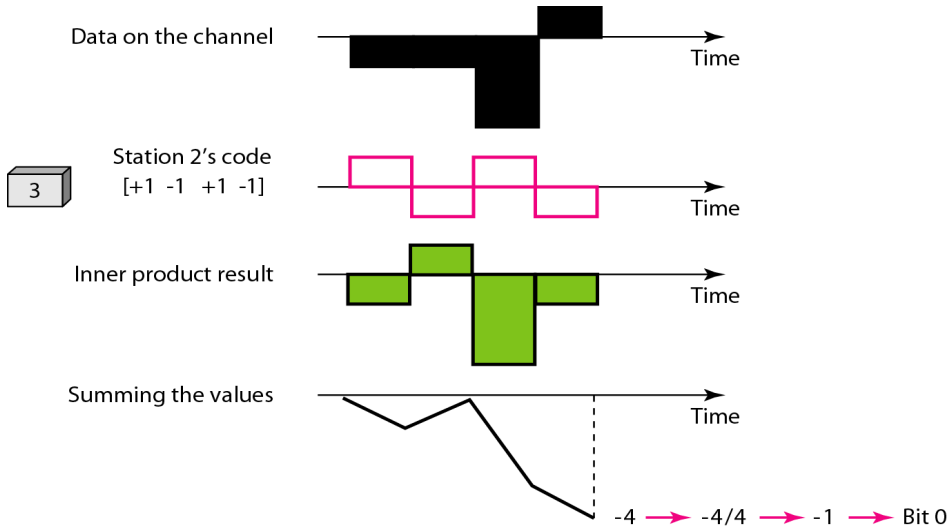


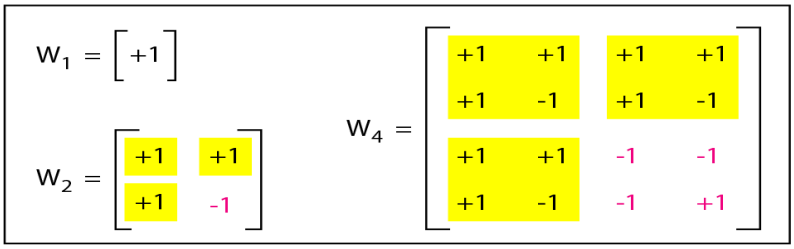
Figure shows how station 3 can detect the data sent by station 2 by using the code for station 2. The total data on the channel are multiplied (inner product operation) by the signal representing station 2 chip code to get a new signal. The station then integrates and adds the area under the signal, to get the value −4, which is divided by 4 and interpreted as bit 0.



Sequence Generation

To generate chip sequences, we use a Walsh table, which is a two-dimensional table with an equal number of rows and columns, as shown in Figure

a. Two basic rules

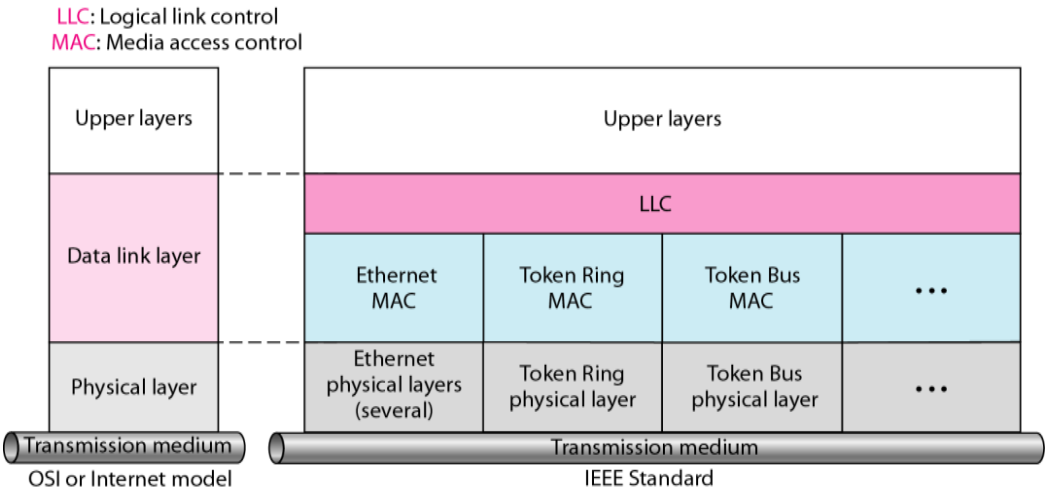


b. Generation of W_1, W_2, and W_4

IEEE Standards for Wired LANs:

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

The relationship of the 802 Standard to the TCP/IP protocol suite is shown in Figure. The IEEE has subdivided the data-link layer into two sub layers: logical link control (LLC) and media access control (MAC). IEEE has also created several physical-layer standards for different LAN protocols.



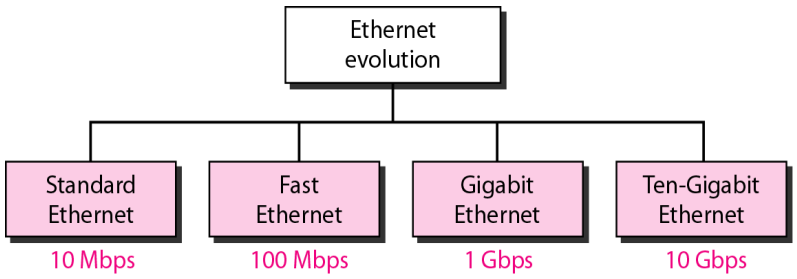
Logical Link Control (LLC)

We said that data link control handles framing, flow control, and error control. In IEEE Project 802, flow control, error control, and part of the framing duties are collected into one sub layer called the logical link control(LLC). **Media Access Control (MAC)**

Earlier we discussed multiple access methods including random access, controlled access, and channelization. IEEE Project 802 has created a sub layer called media access control that defines the specific access method for each LAN.

Ethernet Evolution

The Ethernet LAN was developed in the 1970s by Robert Metcalfe and David Boggs. Since then, it has gone through four generations: Standard Ethernet (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps), and 10 Gigabit Ethernet (10 Gbps), as shown in Figure

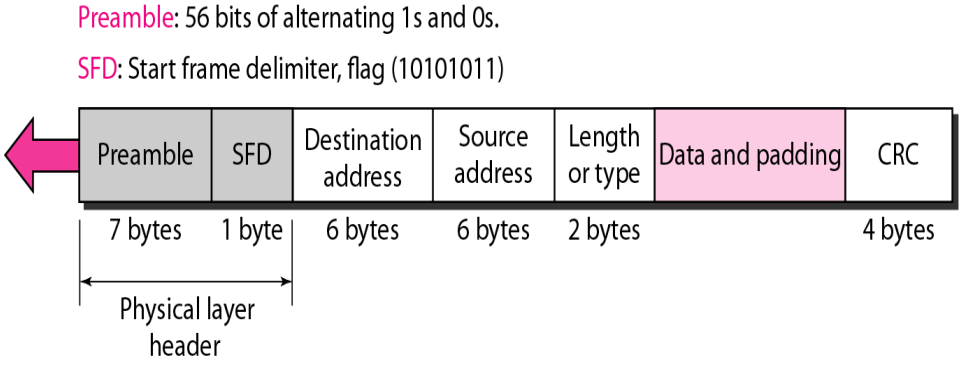


STANDARD ETHERNET

We refer to the original Ethernet technology with the data rate of 10 Mbps as the Standard Ethernet.

Characteristics: .Ethernet provides a connectionless service, which means each frame sent is independent of the previous or next frame.

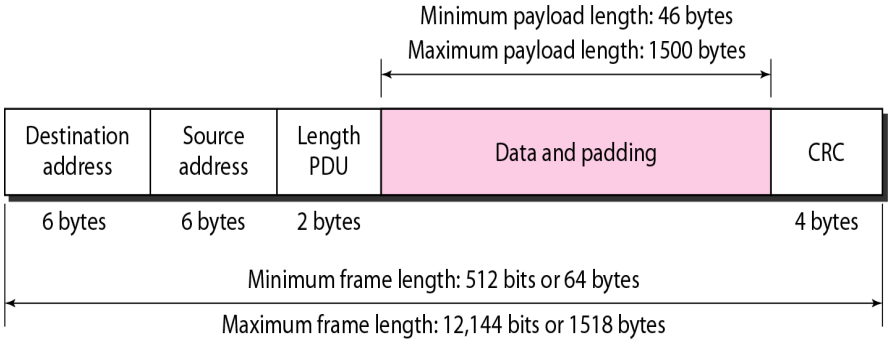
Frame Format



Preamble. This field contains 7 bytes (56 bits) of alternating 0s and 1s that alert the receiving system to the coming frame and enable it to synchronize its clock if it's out of synchronization. The pattern provides only an alert and a timing pulse,
Start frame delimiter (SFD). This 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 are (11)2 and alert the receiver that the next field is the destination address.
Destination address (DA). This field is six bytes (48 bits) and contains the linklayer address of the destination station or stations to receive the packet.
Source address (SA). This field is also six bytes and contains the link-layer address of the sender of the packet
Type. This field defines the upper-layer protocol whose packet is encapsulated in the frame.
Data. This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.
CRC. The last field contains error detection information, in this case a CRC-32. The CRC is calculated over the addresses, types, and data field. If the receiver calculates the CRC and finds that it is not zero (corruption in transmission), it discards the frame

Frame Length

An Ethernet frame needs to have a minimum length of 512 bits or 64 bytes. The minimum length of data from the upper layer is 64 -18 =46 bytes. The standard defines the maximum length of a frame (without preamble and SFD field) as 1518 bytes. The maximum length of the payload is 1500 bytes.



Addressing

Each station on an Ethernet network has its own network interface card (NIC). The NIC fits inside the station and provides the station with a link-layer address. The Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes. For example, the following shows an Ethernet MAC address:

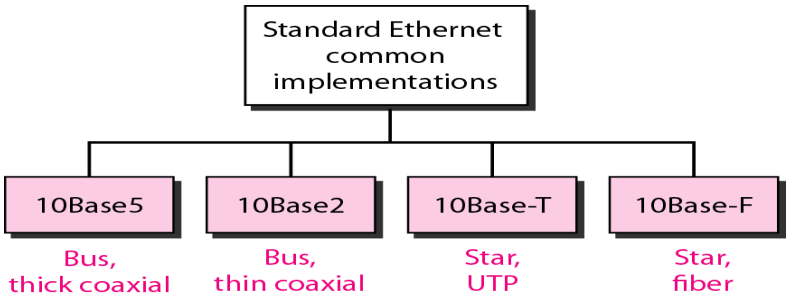
Unicast, Multicast, and Broadcast Addresses

A source address is always a unicast address—the frame comes from only one station. The destination address, however, can be unicast, multicast, or broadcast. Figure shows how to distinguish a unicast address from a multicast address. If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise,it is multicast.

Standard Ethernet

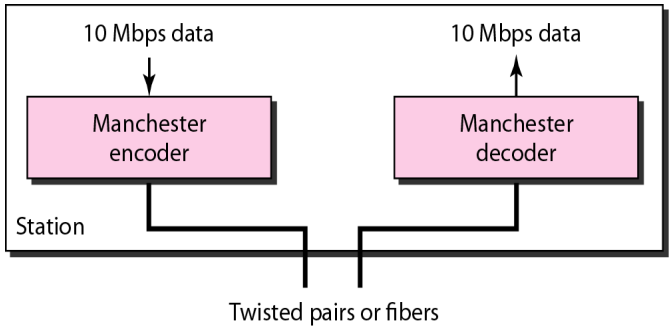
Physical Layer

The Standard Ethernet defines several physical layer implementations; four of the most common



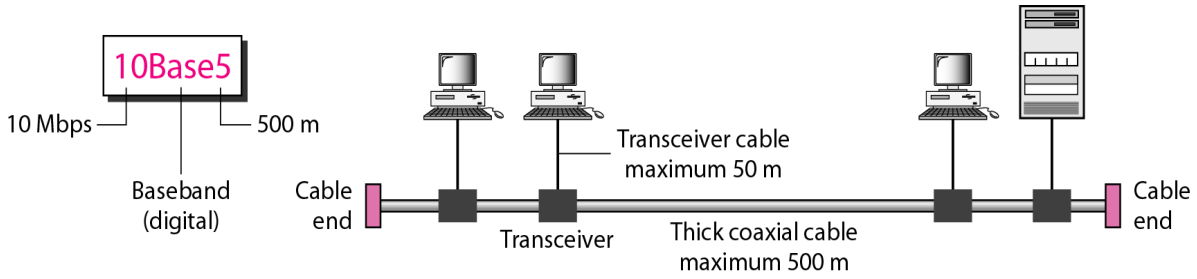
Encoding and Decoding

All standard implementations use digital signaling (baseband) at 10 Mbps. 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.



10Base5: Thick Ethernet

The first implementation is called 10BaseS, thick Ethernet, or Thick net. The nickname derives from the size of the cable, which is roughly the size of a garden hose and too stiff to bend with your hands. 10Base5 was the first Ethernet specification to use a bus topology with an external transceiver (transmitter/receiver) connected via a tap to a thick coaxial cable

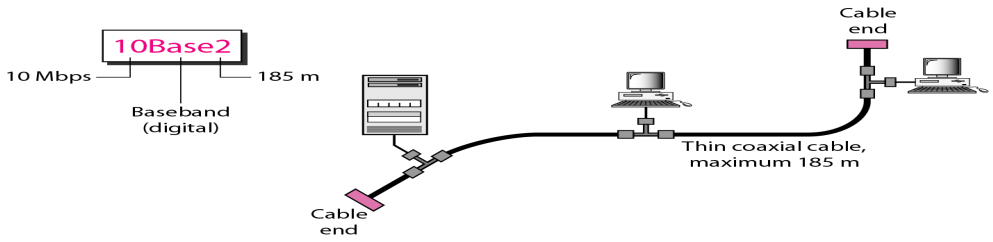


The transceiver is responsible for transmitting, receiving, and detecting collisions. The transceiver is connected to the station via a transceiver cable that provides separate paths for sending and receiving. This means that collision can only happen in the coaxial cable. The maximum length of the coaxial cable must not exceed 500 m, otherwise, there is excessive

degradation of the signal. If a length of more than 500 m is needed, up to five segments, each a maximum of 500-meter, can be connected using repeaters.

10Base2: Thin Ethernet

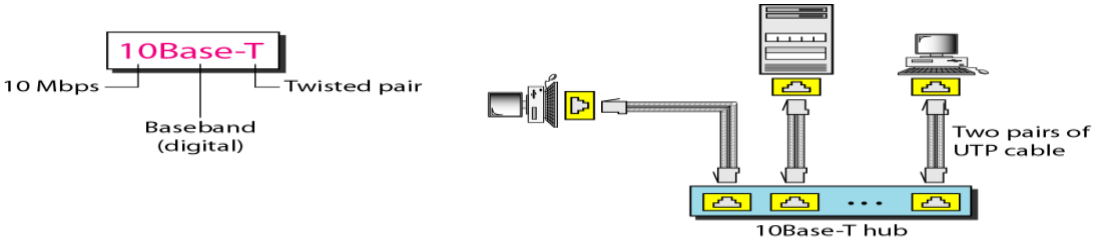
The second implementation is called 10Base2, thin Ethernet, or Cheaper net. 10Base2 also uses a bus topology, but the cable is much thinner and more flexible. The cable can be bent to pass very close to the stations. In this case, the transceiver is normally part of the network interface card (NIC),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



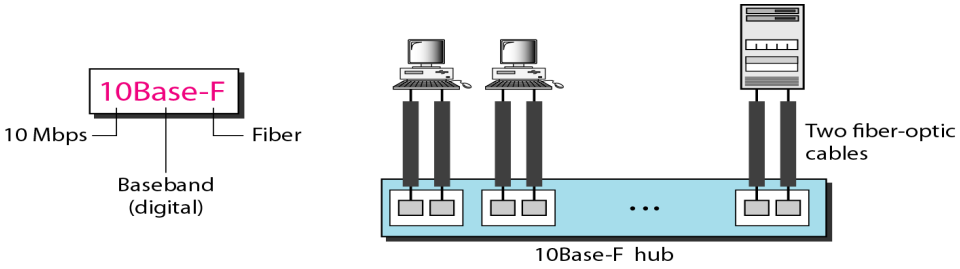
Note that the collision here occurs in the thin coaxial cable. This implementation is more cost effective than 10Base5 because thin coaxial cable is less expensive than thick coaxial and the tee connections are much cheaper than taps. Installation is simpler because the thin coaxial cable is very flexible. However, the length of each segment cannot exceed 185 m (close to 200 m) due to the high level of attenuation in thin coaxial cable.

10Base-T: Twisted-Pair Ethernet

The third implementation is called 10Base-T or twisted-pair Ethernet. 10Base-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable. Note that two pairs of twisted cable create two paths (one for sending and one for receiving) between the station and the hub. Any collision here happens in the hub. The maximum length of the twisted cable here is defined as 100 m, to minimize the effect of attenuation in the twisted cable .



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



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

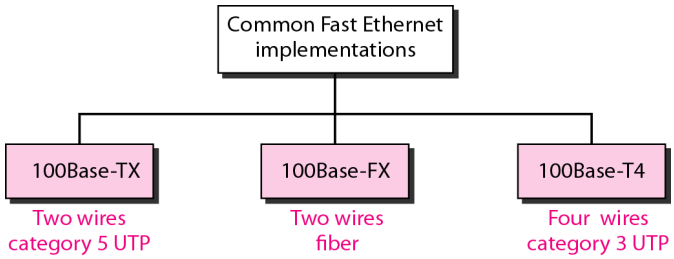
FAST ETHERNET (100 MBPS)

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

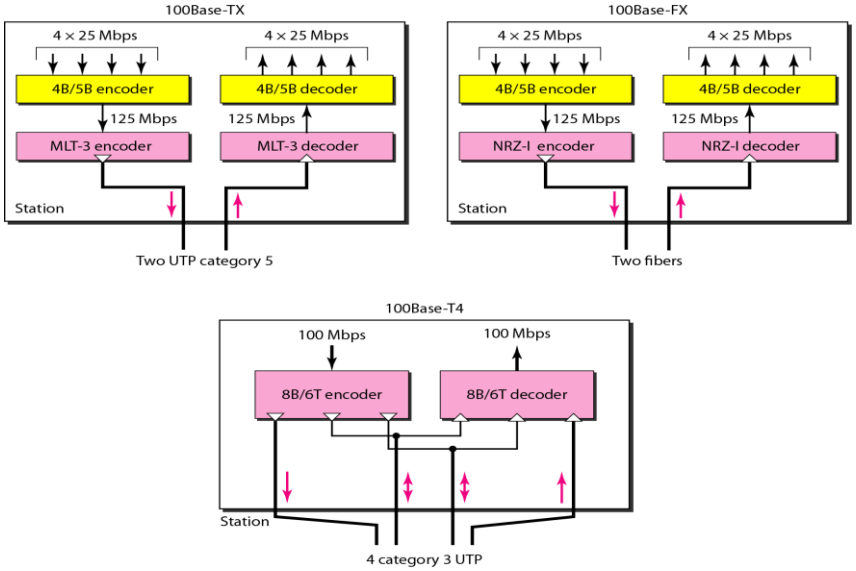
The goals of Fast Ethernet can be summarized as follows:

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

Fast Ethernet Physical layer implementations



Encoding for Fast Ethernet implementation



100Base-TX uses two pairs of twisted-pair cable (either category 5 UTP or STP). For this implementation, the MLT-3 scheme was selected since it has good bandwidth performance. However, since MLT-3 is not a self-synchronous line coding scheme, 4B/5B block coding is used to provide bit synchronization by preventing
the occurrence of a long sequence of 0s and 1s. This creates a data rate of 125 Mbps, which is fed into MLT-3 for encoding.

100Base-FX uses two pairs of fiber-optic cables. Optical fiber can easily handle high bandwidth requirements by using simple encoding schemes. The designers of 100Base-FX selected the NRZ-I encoding scheme for this implementation. However, NRZ-I has a bit synchronization problem for long sequences of 0s (or1s, based on the encoding. To overcome this problem, the designers used 4B/5B block

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. 8B/6T satisfies this requirement. In 8B/6T, eight data elements are encoded as six signal elements.

Summary of Fast Ethernet implementations

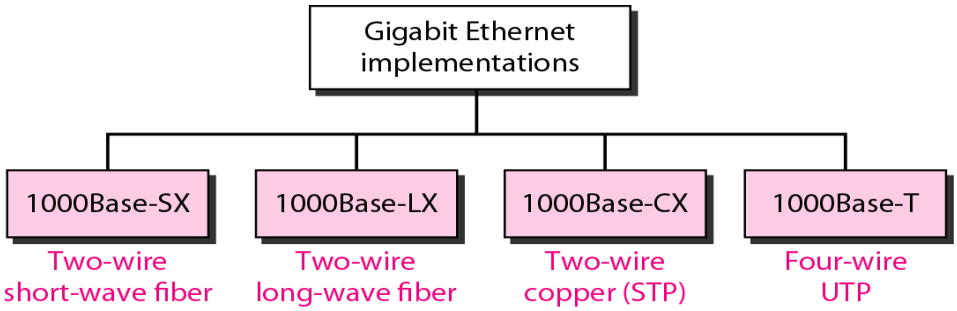
Characteristics	*100Base-TX*	*100Base-FX*	*100Base-T4*
Media	Cat 5 UTP or STP	Fiber	Cat 4 UTP
Number of wires	2	2	4
Maximum length	100 m	100 m	100 m
Block encoding	4B/5B	4B/5B	
Line encoding	MLT-3	NRZ-I	8B/6T

GIGABIT ETHERNET

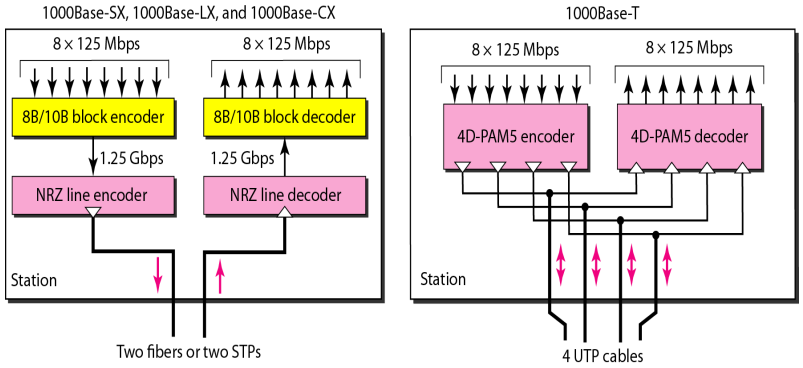
The need for an even higher data rate resulted in the design of the Gigabit Ethernet protocol (1000 Mbps). The IEEE committee calls the standard 802.3z.

The goals of the Gigabit Ethernet design can be summarized as follows:
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. Support auto negotiation as defined in Fast Ethernet.

Gigabit Ethernet implementations



Encoding in Gigabit Ethernet implementations



Gigabit Ethernet cannot use the Manchester encoding scheme because it involves a very high bandwidth (2 GBaud). The two-wire implementations use an NRZ scheme, but NRZ does not self-synchronize properly. To synchronize bits, particularly at this highdata rate, 8B/10B block encoding is used. This block encoding prevents long sequences of 0s or 1s in the stream, but the resulting stream is 1.25 Gbps. Note that in this implementation, one wire is used for sending and one for receiving.

In the four-wire implementation it is not possible to have 2 wires for input and 2 for output, because each wire would need to carry 500 Mbps, which exceeds the capacity for category 5 UTP. As a solution, 4D-PAM5 encoding, is used to reduce the bandwidth. Thus, all four wires are involved in both input and output; each wire carries 250 Mbps, which is in the range for category 5 UTP cable.

Summary of Gigabit Ethernet implementations

Characteristics	*1000Base-SX*	*1000Base-LX*	*1000Base-CX*	*1000Base-T*
Media	Fiber short-wave	Fiber long-wave	STP	Cat 5 UTP
Number of wires	2	2	2	4
Maximum length	550 m	5000 m	25 m	100 m
Block encoding	8B/10B	8B/10B	8B/10B	
Line encoding	NRZ	NRZ	NRZ	4D-PAM5

10 GIGABIT ETHERNET

10 Gigabit Ethernet operates only in full-duplex mode, which means there is no need for contention; CSMA/CD is not used in 10 Gigabit Ethernet. Four implementations are the most common: 10GBase-SR, 10GBase-LR, 10GBase-EW, and 10GBase-X4. Table shows a summary of the 10 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

Basis For Comparison	**Fast Ethernet**	**Gigabit Ethernet**
Basic	Offers 100 Mbps speed.	Provide 1 Gbps speed.
Delay	Generate more delay.	Less comparatively.

Configuration	Simple	Complicated and create more errors.
Coverage	Can cover distance up to 10 km.	Has the limit of 70 km.
Relation	Successor of 10-Base-T Ethernet.	A successor of fast Ethernet.
Round trip delay	100-500 bit times	4000 bit times

IEEE 802.11 Standards (WIRELESS LAN)

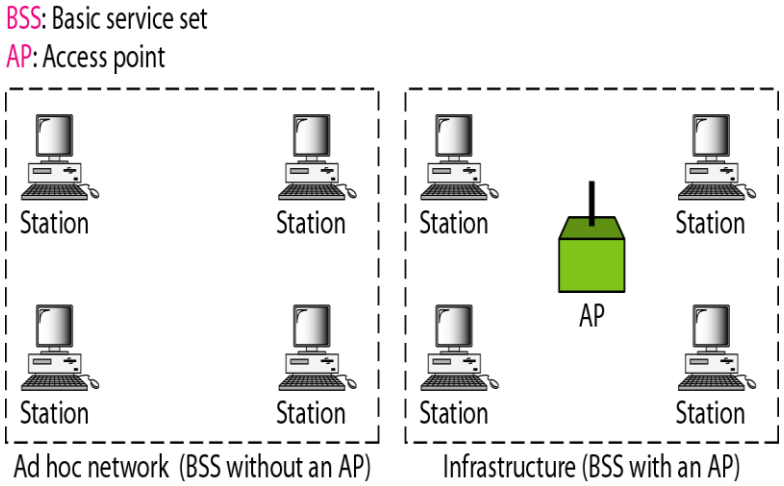
IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data-link layers. It is sometimes called wireless Ethernet. In some countries, including the United States, the public uses the term Wi-Fi as a synonym for wireless LAN.

Architecture

The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

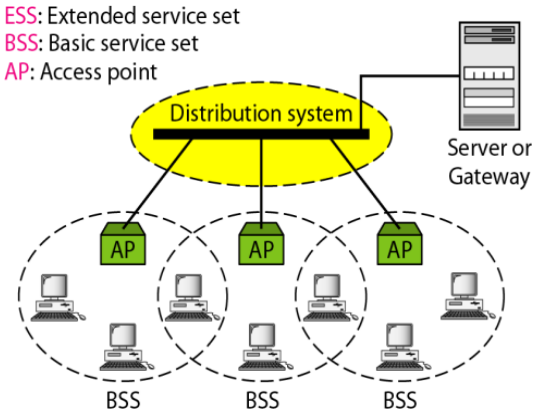
Basic Service Set

IEEE 802.11 defines the basic service set (BSS) as the building blocks 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). Figure shows two sets in this standard. 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 BSS.



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 a wired or a wireless network. 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

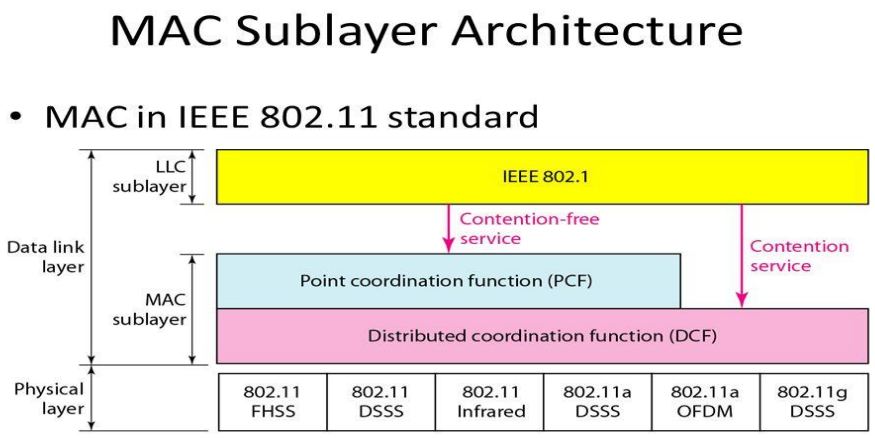


Station Types

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.

MAC Sub-layer

IEEE 802.11 defines two MAC sub-layers: the distributed coordination function (DCF) and point coordination function (PCF). Figure shows the relationship between the two MAC sub-layers, the LLC sub-layer, and the physical layer.



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.

Point Coordination Function (PCF)

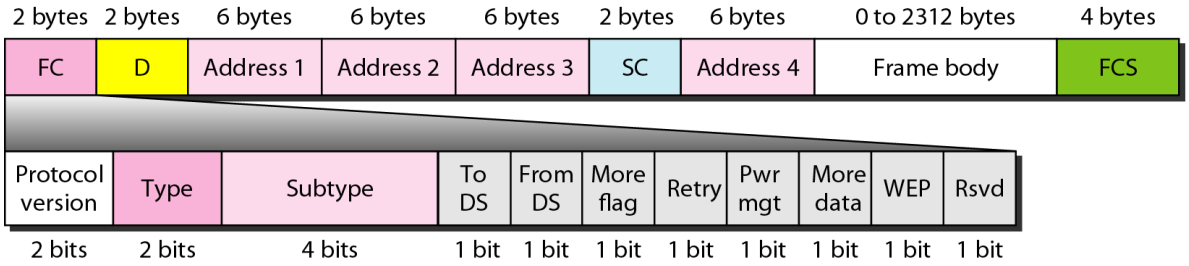
The point coordination function (PCF) is an optional access method that can be implemented in an infrastructure network (not in an ad hoc network). It is implemented on top of the DCF and is used mostly for time-sensitive transmission.

Fragmentation

The wireless environment is very noisy, so frames are often corrupted. 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 in Figure



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

D. This field defines the duration of the transmission that is used to set the value of NAV.

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

Sequence control. This field, often called the SC field, defines a 16-bit value. The first four bits define the fragment number; the last 12 bits define the sequence number, which is the same in all fragments.

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.

Subfields in FC field

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

Frame Types

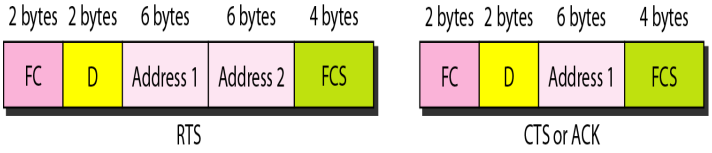
A wireless LAN defined by IEEE 802.11 has three categories of frames: management frames, control frames, and data frames.

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. Figure shows the format



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

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

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.

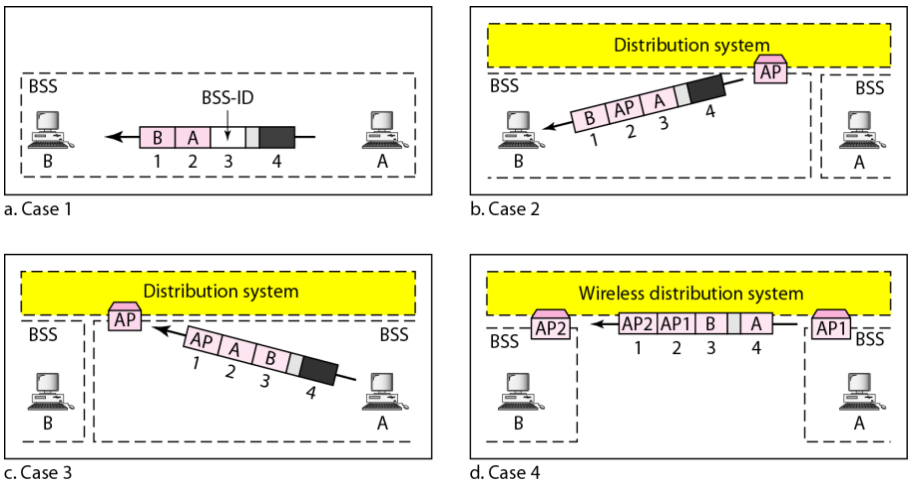
To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

Case 1: 00 In this case, To DS =0 and From =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).

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).

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).

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 wireless distribution system.



a. Case 1 b. Case 2

c. Case 3 d. Case 4

Physical Layer

We discuss six specifications, as shown in Table 15.4. All implementations, except the infrared, operate in the industrial, scientific, and medical (ISM) band, which defines three unlicensed bands in the three ranges 902–928 MHz, 2.400–4.835 GHz, and 5.725–5.850 GHz.

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

High-speed LANs

Recent years have seen rapid changes in the technology, design, and commercial applications for local area networks (LANs). A major feature of this evolution is the introduction of a variety of new schemes for high-speed local networking.

The Emergence of High-speed LANs

• The speed and computing power of personal computers has continued to enjoy explosive growth. Today's more powerful platforms support graphics intensive applications and ever more elaborate graphical user interfaces to the operating system.

• MIS organizations have recognized the LAN as a viable and indeed essential computing platform, resulting in the focus on network computing

• Both of these approaches involve the frequent transfer of potentially large volumes of data in a transaction-oriented environment.

• The effect of these trends has been to increase the volume of data to be handled over LANs and, because applications are more interactive, to reduce the acceptable delay on data transfers.

Requirements for High-Speed LANs

• **Centralized server farms**: In many applications, there is a need for user or client systems to be able to draw huge amounts of data from multiple centralized servers, called server farms. An

example is a color publishing operation in which servers typically contain hundreds of gigabytes of image data that must be downloaded to imaging workstations. As the performance of the servers themselves has increased, increased, the bottleneck has shifted to the network.

• **Power workgroups**: These groups typically consist of a small number of cooperating users who need to draw massive data files across the network. Examples are a software development group that runs tests on a new software version, or a computer- aided design (CAD) company that regularly runs simulations of new designs. In such cases, large amounts of data are distributed to several workstations, processed, and updated at very high speed for multiple iterations.

• **High-speed local backbone**: As processing demand grows, LANs proliferate at a site, and high-speed interconnection is necessary.

The most widely used high-speed LANs today are based on Ethernet and were developed by the IEEE 802.3 standards committee. To keep pace with the changing local networking needs of business, a number of approaches to high speed LAN design have become commercial products. The most important of these are:

• **Fast Ethernet and Gigabit Ethernet**: The extension of 10-Mbps CSMA/CD (Standard Ethernet) to higher speeds is a logical strategy because it t d en s to preserve the investment in existing systems.

• **Fibre Channel**: This standard provides a low-cost, easily scalable approach for achieving very high data rates in local areas.

•**High-speed wireless LANs**: Wireless LAN technology and standards have at last come of age, and high-speed standards and products are being introduced.

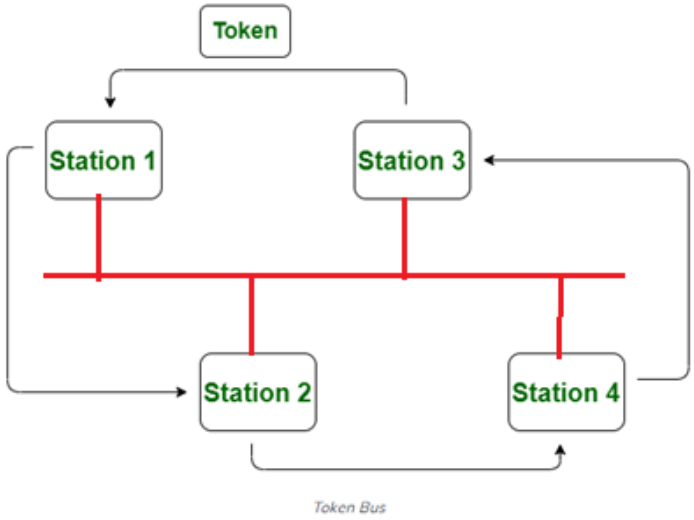
Characteristics of Some High-Speed LANs

	Fast Ethernet	Gigabit Ethernet	Fibre Channel	Wireless LAN
Data Rate	100 Mbps	1 Gbps, 10 Gbps	100 Mbps–3.2 Gbps	1 Mbps–54 Mbps
Transmission Media	UTP, STP, optical Fiber	UTP, shielded cable, optical fiber	Optical fiber, coaxial cable, STP	2.4-GHz, 5-GHz microwave
Access Method	CSMA/CD	Switched	Switched	CSMA/Polling
Supporting Standard	IEEE 802.3	IEEE 802.3	Fibre Channel Association	IEEE 802.11

Token Bus and Token ring Networks

Token Bus

Token Bus **(IEEE 802.4)** is a standard for implementing token ring over virtual ring in LANs. The physical media has a bus or a tree topology and uses coaxial cables. A virtual ring is created with the nodes/stations and the token is passed from one node to the next in a sequence along this virtual ring. Each node knows the address of its preceding station and its succeeding station. A station can only transmit data when it has the token. The working principle of token bus is similar to Token Ring.



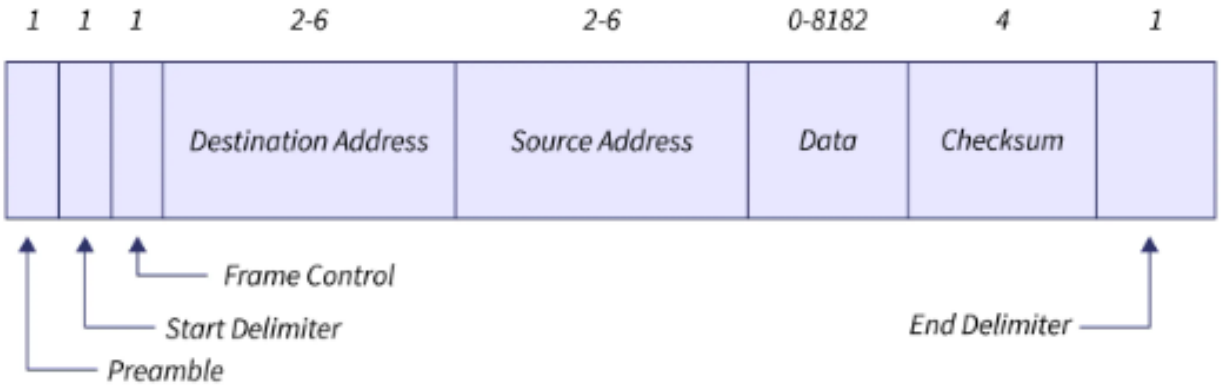
Token Bus

Token Passing Mechanism in Token Bus

A token is a small message that circulates among the stations of a computer network providing permission to the stations for transmission. If a station has data to transmit when it receives a token, it sends the data and then passes the token to the next station; otherwise, it simply passes the token to the next station

Frame Format of Token Bus

The following are the fields in the frame format of the token bus

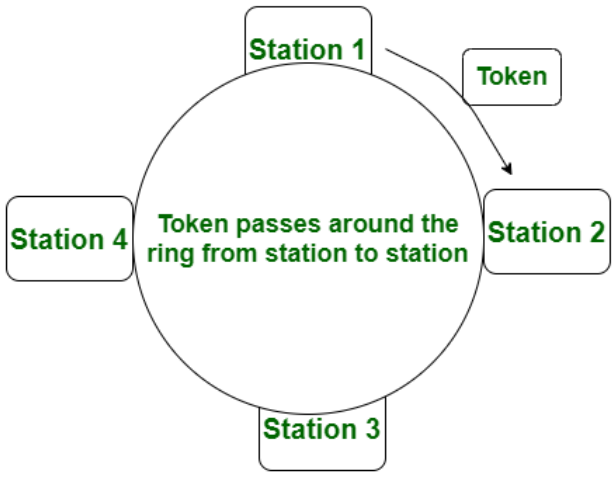


- **Preamble:** It is a 1-byte field and is used for bit synchronization.
- **Start Delimiter:** It is a 1-byte field that marks the beginning of the frame.

- **Frame Control:** It is a 1-byte field that specifies the frame type and distinguishes data frames from control frames.
- **Destination Address:** This is a 2 to 6 bytes field containing the address of the destination station.
- **Source Address:** This is a 2 to 6 bytes field containing the address of the source station.
- **Data:** This variable length field carries the data from the network layer. The field can be up to 8182 bytes when using 2-byte addresses and 8174 bytes when using 6-byte addresses.
- **Checksum:** It is a 4-byte field with checksum bits that detect errors in transmitted data.
- **End Delimiter:** It is a 1-byte field that marks the end of the frame.

Token Ring

Token ring **(IEEE 802.5)** is a communication protocol in a local area network (LAN) where all stations are connected in a ring topology and pass one or more tokens for channel acquisition. A token is a special frame of 3 bytes that circulates along the ring of stations. A station can send data frames only if it holds a token. The tokens are released on successful receipt of the data frame



Token Ring

Token Passing Mechanism in Token Ring

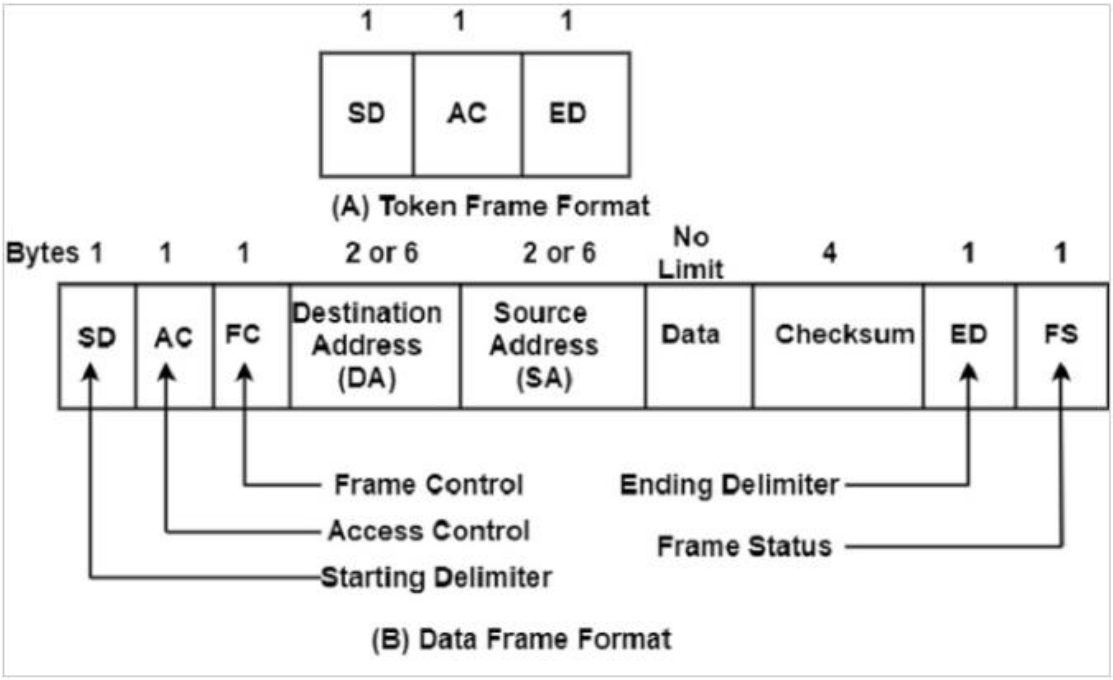
If a station has a frame to transmit when it receives a token, it sends the frame and then passes the token to the next station; otherwise it simply passes the token to the next station. Passing the token means receiving the token from the preceding station and transmitting to the successor station. The data flow is unidirectional in the direction of the token passing. In order that tokens are not circulated infinitely, they are removed from the network once their purpose is completed.

Frame Format of Token Ring

There are three types of frame formats that are supported on a Token Ring network such as token, abort, and frame. The token format is the mechanism by which access to the ring is passed from one computer attached to the network to another device connected to the network.

Here, the token format consists of three bytes, of which the starting and ending delimiters are used to indicate the beginning and end of a token frame. The middle byte of a token frame is an access control byte.

Three bits are used as a priority indicator, three bits are used as a reservation indicator, while one bit is used for the token bit, and another bit position functions as the monitor bit.



The components of the Token Ring Frame Format are as follows −

- **Start Delimiter (SD)** − The first field of the data/command frame, SD, is one byte long and is used to alert the receiving station to the arrival of a frame as well as to allow it to synchronize its retrieval timing.
- **Access Control (AC)** − The AC field is one byte long and includes four subfields. The first three bits are the priority field. The fourth bit is called the token bit.
- **Frame Control (FC)** −The FC field is one byte long and contains two fields. The first is a one-bit field used to indicate the type of information contained in the Protocol Data Unit (PDU).
- **Destination Address (DA)** −The two-to-six-byte DA field contains the physical address of the frame's next destination. If its ultimate destination is another network, the DA is the address of the router to the next LAN on its path.
- **Source Address (SA)** − The SA field is also two to six bytes long and contains the physical address of the sending station. If the ultimate destination of the packet is a station on the same network as the originating station, the SA is that of the originating station.
- **Data** −The sixth field, data, is allotted 4500 bytes and contains the PDU. A token ring frame does not include a PDU length or type field.
- **Checksum** −The checksum field is 4 bytes long. The checksum field is used to cross-check the data at the sending station. This field contains the total number of bytes in the frame. The number is checked at the receiver end after counting the bytes in the received frame.
- **End Delimiter (ED)** −The ED is a second flag field of one byte and indicates the end of the sender's data and control information.
- **Frame Status** −The last byte of the frame is the FS field. It can be set by the receiver to indicate that the frame has been read or by the monitor to indicate that the frame has already been around the ring.

Difference between the Token Bus and the Token Ring:

S. No.	Token Bus Network	Token Ring Network
1.	In the token bus network, the token is passed along a virtual ring.	While in the token ring network the token is passed over a physical ring.
2.	The token bus network is simply designed for large factories.	While the token ring network is designed for the offices.
3.	The token bus network is defined by the **IEEE 802.4 standard.**	While the token ring network is defined by the **IEEE 802.5 standard.**
4.	Token bus network provides better bandwidth.	While the token ring network does not provide better bandwidth as compared to the token bus.
5.	In a token bus network, Bus topology is used.	While in token ring network, Star topology is used.
6.	The maximum time it takes to reach the last station in a token bus network cannot be calculated.	While the maximum time to reach the last station in the token ring network can be calculated.
7	In a token bus network, coaxial cable is used	In token ring network, twisted pair and fiber optic is used.
8	In a token bus network, the cable length is 200m to 500m.	In a token ring network, the cable length is 50m to 1000m.
9.	In token bus network, distributed algorithm provide maintenance.	In a token ring network, a designated monitor station performs station maintenance.

S. No.	Token Bus Network	Token Ring Network
10.	The priority handling mechanism is not associated with the transmission of data through workstations with this network.	The priority handling mechanism is associated with the transmission of data through workstations with this network.
11.	These networks are not much reliable.	These networks are reliable.
12.	It does not keep routing details.	It keeps the information of routing.
13.	The network is less expensive compared to the Token Ring network.	It is expensive.

FDDI based LAN

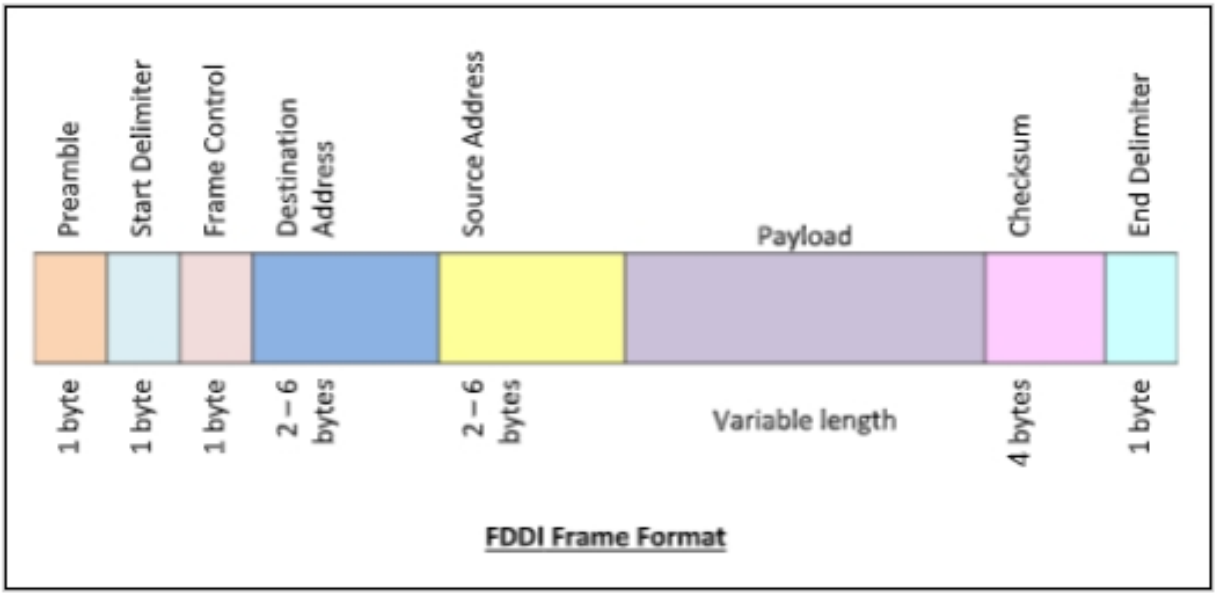
Fiber Distributed Data Interface (FDDI) is a set of ANSI and ISO standards for transmission of data in local area network (LAN) over fiber optic cables. It is applicable in large LANs that can extend up to 200 kilometers in diameter.

Features

- FDDI uses optical fiber as its physical medium.
- It operates in the physical and medium access control (MAC layer) of the Open Systems Interconnection (OSI) network model.
- It provides high data rate of 100 Mbps and can support thousands of users.
- It is used in LANs up to 200 kilometers for long distance voice and multimedia communication.
- It uses ring based token passing mechanism and is derived from IEEE 802.4 token bus standard.
- It contains two token rings, a primary ring for data and token transmission and a secondary ring that provides backup if the primary ring fails. One ring will operate in a clockwise direction and the other in a counterclockwise direction
- FDDI technology can also be used as a backbone for a wide area network (WAN).

Frame Format

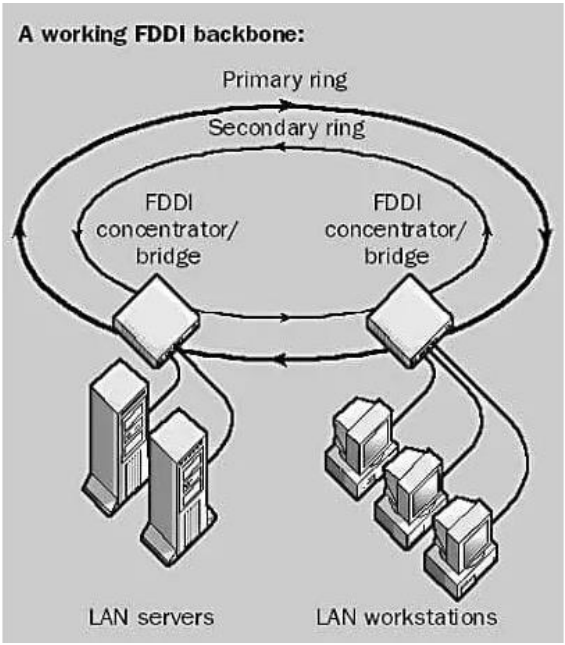
The frame format of FDDI is similar to that of token bus as shown in the following diagram



The fields of an FDDI frame are −

- **Preamble:** 1 byte for synchronization.
- **Start Delimiter:** 1 byte that marks the beginning of the frame.
- **Frame Control:** 1 byte that specifies whether this is a data frame or control frame.
- **Destination Address:** 2-6 bytes that specifies address of destination station.
- **Source Address:** 2-6 bytes that specifies address of source station.
- **Payload:** A variable length field that carries the data from the network layer.
- **Checksum:** 4 bytes frame check sequence for error detection.
- **End Delimiter:** 1 byte that marks the end of the frame.

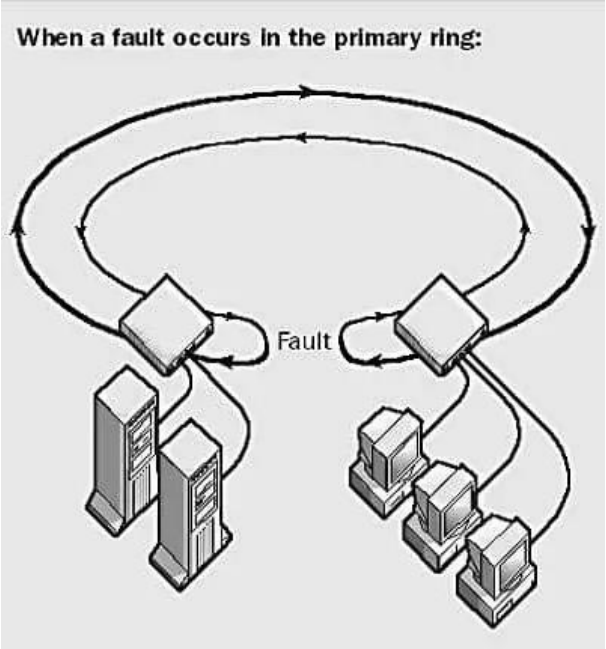
Working



Fiber Distributed Data Interface (FDDI) is usually implemented as a dual token-passing ring within a ring topology (for campus networks) or star topology (within a building). The dual ring consists of a primary and secondary ring. The primary ring carries data. The counter-rotating secondary ring can carry data in the opposite direction, but is more commonly reserved as a

backup in case the primary ring goes down. This provides FDDI with the degree of fault tolerance necessary for network backbones. In the event of a failure on the primary ring, FDDI automatically reconfigures itself to use the secondary ring as shown in the illustration. Faults can be located and repaired using a fault isolation technique called beaconing. However, the secondary ring can also be configured for carrying data, extending the maximum potential bandwidth to 200 Mbps.

Stations connect to one (or both) rings using a media interface connector (MIC). Its two fiber ports can be either male or female, depending on the implementation. There are two different FDDI implementations, depending on whether stations are attached to one or both rings:



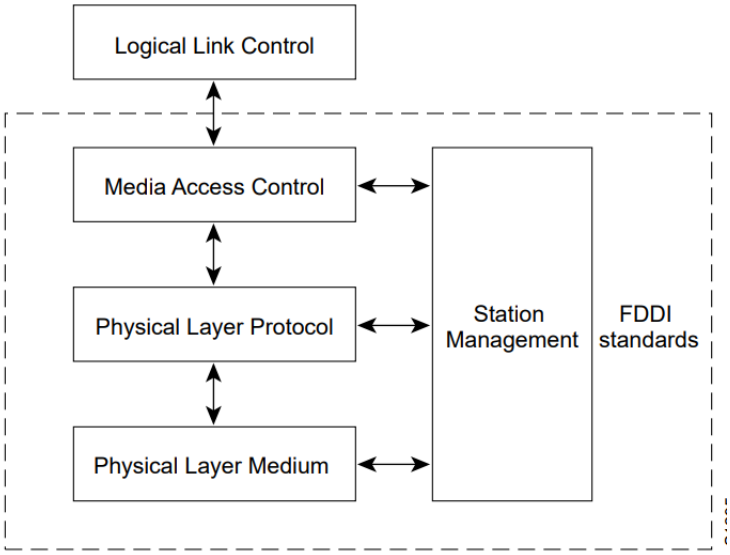
An FDDI concentrator (also called a dual-attachment concentrator [DAC]) is the building block of an FDDI network. It attaches directly to both the primary and secondary rings and ensures that the failure or power-down of any SAS does not bring down the ring. This is particularly useful when PCs, or similar devices that are frequently powered on and off, connect to the ring

FDDI uses a timed token-passing technology similar to that of token ring networks as defined in the IEEE 802.5 standard. FDDI stations generate a token that controls the sequence in which other stations will gain access to the wire. The token passes around the ring, moving from one node to the next. When a station wants to transmit information, it captures the token, transmits as many frames of information as it wants (within the specified access period), and then releases the token. This feature of transmitting multiple data frames per token capture is known as a capacity allocation scheme, in contrast to the priority mechanism used in the IEEE 802.5 token ring standard. Every node on the ring checks the frames. The recipient station then reads the information from the frames, and when the frames return to the originating station, they are stripped from the ring.

There can be up to 500 stations on a dual-ring FDDI network. The maximum circumference for an FDDI ring is 100 kilometers (or 200 kilometers for both rings combined), and there must be a repeater every 2 kilometers or less. Bridges or routers are used to connect the FDDI backbone network to Ethernet or token ring departmental LANs. For these reasons, FDDI is not often used as a wide area network (WAN) solution, but is more often implemented in campus-wide networks as a network backbone.

FDDI is similar to IEEE 802.3 Ethernet and IEEE 802.5 Token Ring in its relationship with the OSI model. Its primary purpose is to provide connectivity between upper OSI layers of common protocols and the media used to connect network devices. Figure below illustrates the four FDDI specifications and their relationship to each other and to the IEEE-defined Logical-Link Control (LLC) sub layer. The LLC sub layer is a component of Layer 2, the MAC layer, of the OSI reference model.

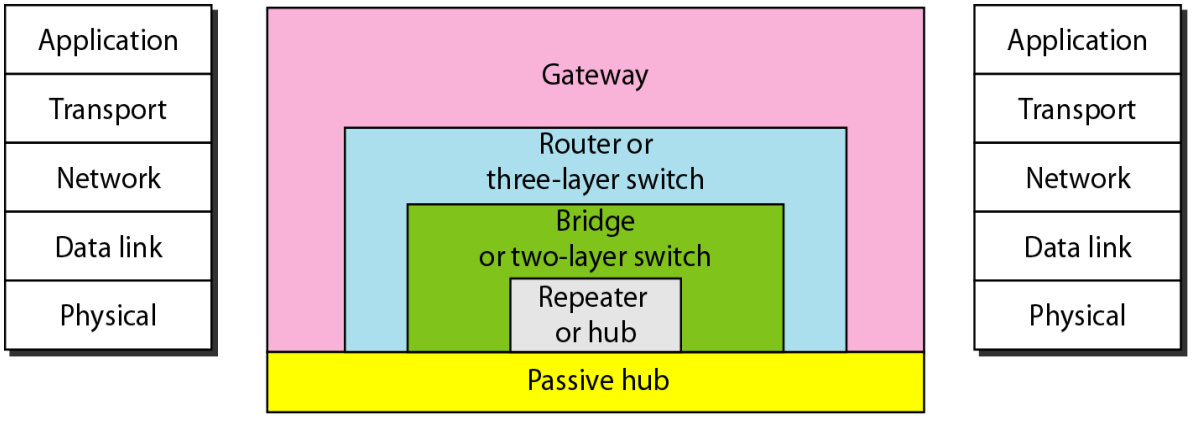
FDDI specifications map to the OSI hierarchical model.



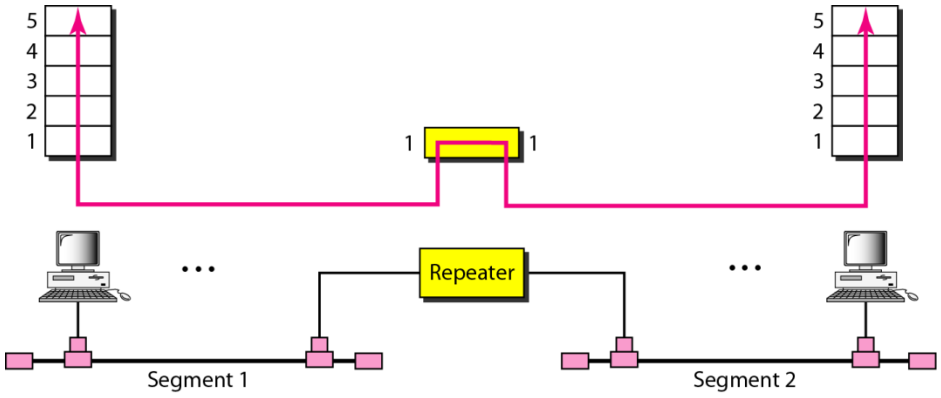
Network Devices -repeaters, hubs, switches and bridges

We divide connecting devices or network devices into five different categories based on the layer in which they operate in a network, as shown in Figure below.
The five categories contain devices which can be defined as

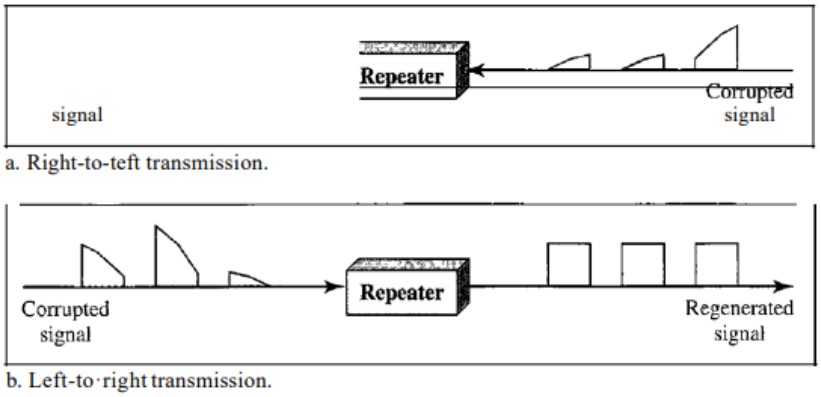
1. Those which operate below the physical layer such as a passive hub.
2. Those which operate at the physical layer (a repeater or an active hub).
3. Those which operate at the physical and data link layers (a bridge or a two-layer switch).
4. Those which operate at the physical, data link, and network layers (a router or a three-layer switch).
5. Those which can operate at all five layers (a gateway)



1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network



Function of a repeater

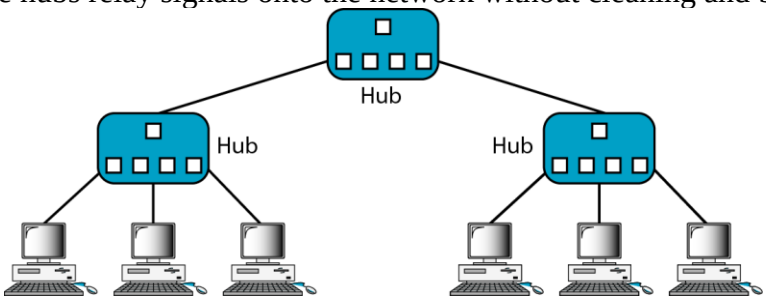


2. Hub – A hub is basically a multi-port **repeater**. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices.

Types of Hubs

- **Active Hub:-** These are the hubs which have their own power supply and can clean , boost and relay the signal along the network. It serves both as a repeater as well as wiring center.

- **Passive Hub:-** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them

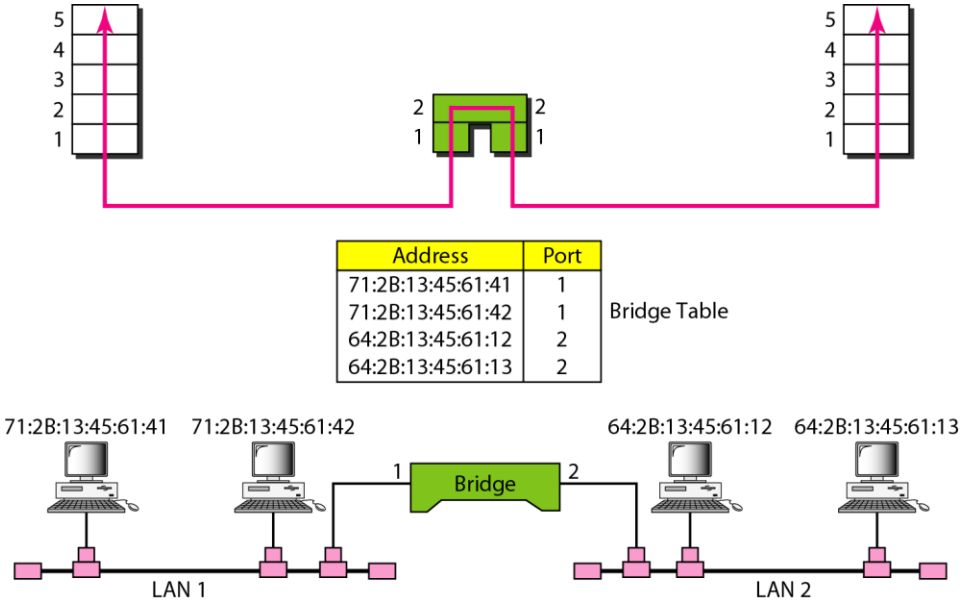


3. Bridge – A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol.

Types of Bridges

- **Transparent Bridges:-** These are the bridge in which the stations are completely unaware of the bridge's existence.

- **Source Routing Bridges:-** In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hop can discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.



4. Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency and performance. Switch is data link layer device. Switch can perform error checking before forwarding data

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets.

6. Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

7. B-router It is also known as bridging router is a device which combines features of both bridge and router. It can work either at data link layer or at network layer. Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.