WIRED LAN's (Ethernet)

1. INTRODUCTION

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

2. IEEE STANDARDS

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

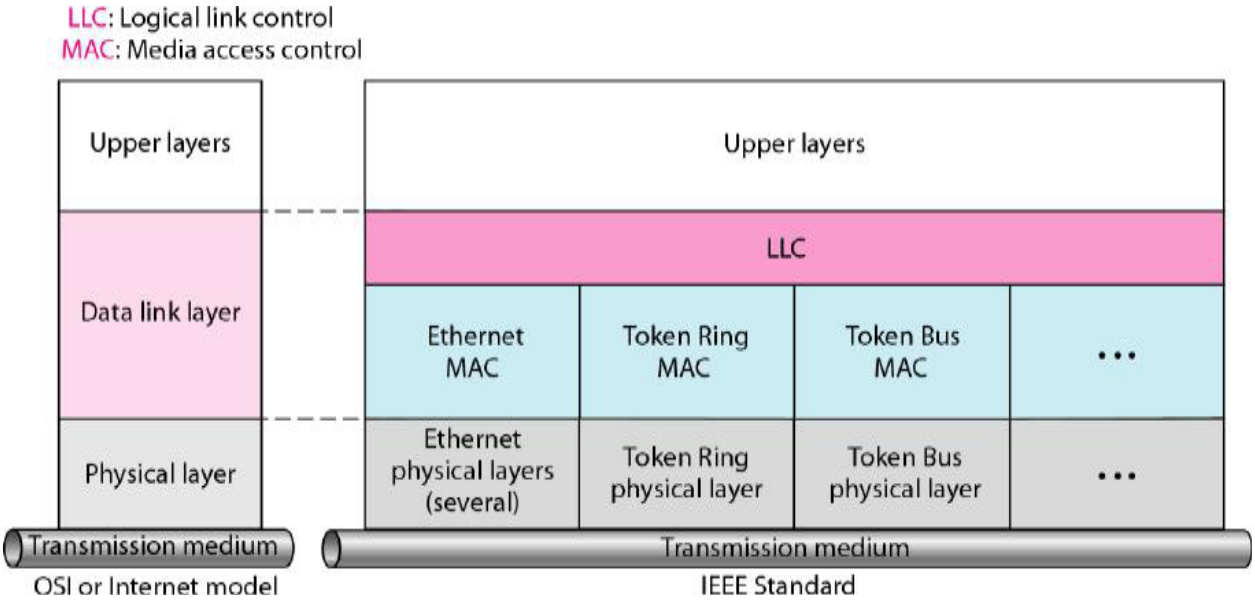


Fig: IEEE standard for LANs

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

a. Standard Ethernet (10 Mbps),

b. Fast Ethernet (100 Mbps),

c. Gigabit Ethernet (1 Gbps), and

d. Ten-Gigabit Ethernet (10 Gbps), as shown in Figure 13.1.

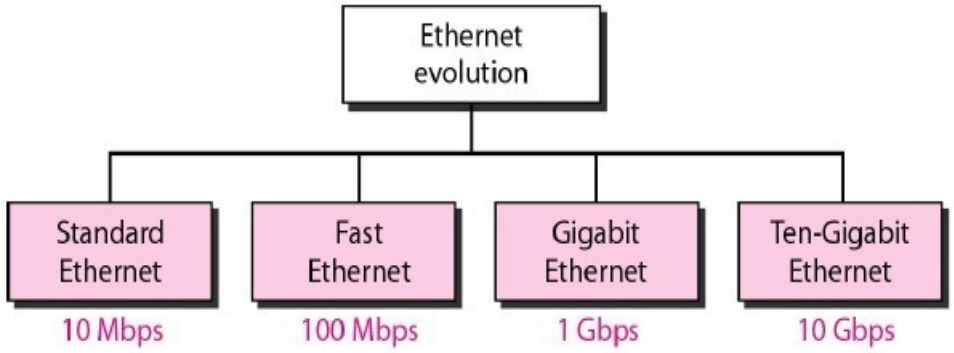


Figure 13.1 Ethernet evolution through four generations

2.1. Standard Ethernet (IEEE 802.3)

Standard Ethernet also known as IEEE 802.3 was the LAN standard proposed by IEEE. Data rate for standard Ethernet is 10 Mbps.

MAC Sublayer

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

- **Frame Format**

The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of protocol data unit (PDU), upper-layer data, and the CRC. Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium. Acknowledgments must be implemented at the higher layers. The format of the MAC frame is shown in Figure 13.2.

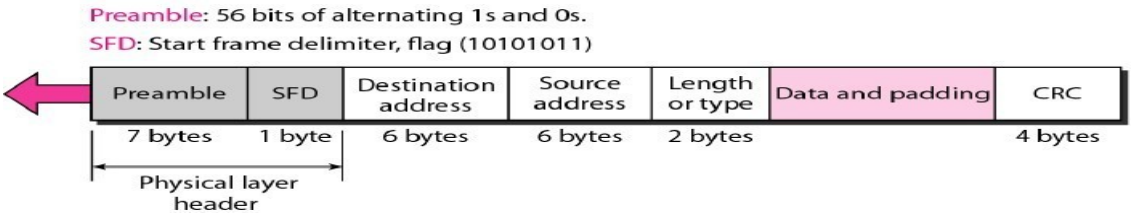


Figure 13.2 802.3 MAC frame

i. **Preamble.** The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating 0s and 1s that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The pattern provides only an alert and a timing pulse. The 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.

ii. **Start frame delimiter (SFD).** The second field (1 byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address.

iii. **Destination address (DA).** The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet.

iv. **Source address (SA).** The SA field is also 6 bytes and contains the physical address of the sender of the packet.

v. **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.

vi. **Data.** This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.

vii. **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 maximumlengths of a frame, as shown in Figure 13.3.

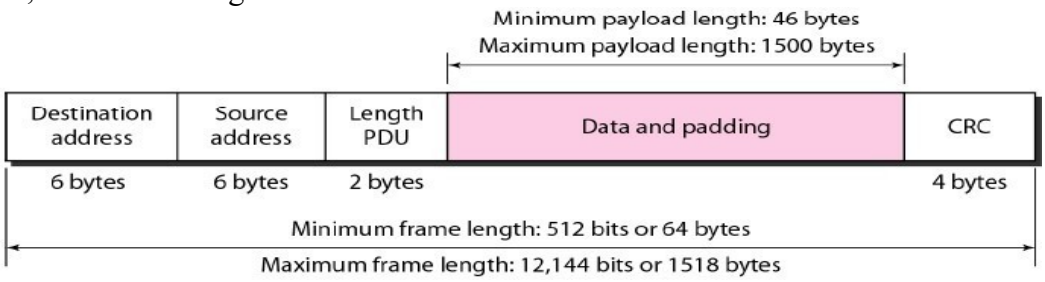


Figure 13.3 Minimum and maximum lengths

The minimum length restriction is required for the correct operation of *CSMA/CD* as we will see shortly. An Ethernet frame needs to have a minimum length of 512 bits or 64 bytes. Part of this length is the header and the trailer. If we count 18 bytes of header and trailer (6bytes of source address, 6 bytes of destination address, 2 bytes of length or type, and 4 bytes of CRC), then the minimum length of data from the upper layer is 64 - 18 = 46 bytes. If the upper-layer packet is less than 46 bytes, padding is added to make up the difference.

The standard defines the maximum length of a frame (without preamble and SFD field) as 1518 bytes. If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes. The maximum length restriction has two historical reasons. First, memory was very expensive when Ethernet was designed: a maximum length restriction helped to reduce the size of the buffer. Second, the maximum length restriction prevents one station from monopolizing the shared medium, blocking other stations that have data to send.

2.2. MAC Addressing

Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC). The NIC fits inside the station and provides the station with a 6-byte physical (MAC) address. As shown in Figure 13.4, the Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.

Figure 13.4 Example of an Ethernet address in hexadecimal notation

Unicast, Multicast, and Broadcast Addresses

Data is transmitted over a network by three simple methods i.e. Unicast, Broadcast, and Multicast Figure 13.5. So let's begin to summarize the difference between these three**:**

- **Unicast**: from one source to one destination i.e. One-to-One
- **Broadcast**: from one source to all possible destinations i.e. One-to-All.
- **Multicast**: from one source to multiple destinations stating an interest in receiving the traffic i.e. One-to-Many.

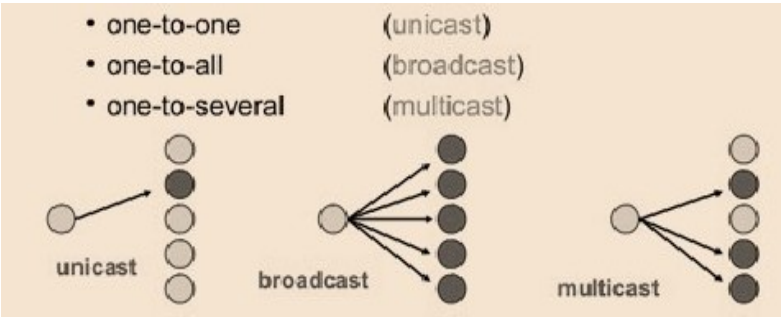


Figure 13.5 Unicasting, Multicasting and Broadcasting

- A source address is always a unicast address as the frame comes from only one station.
- The destination address, however, can be unicast, multicast, or broadcast.
- Figure 13.6 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.

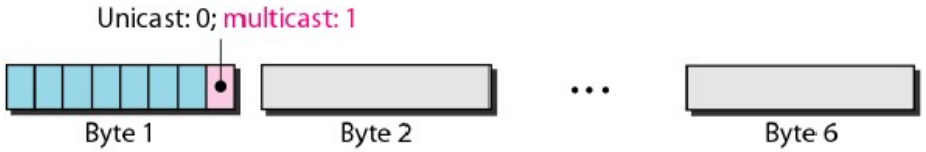


Figure 13.6 Unicast and multicast MAC addresses

- A unicast destination address defines only one recipient; the relationship between the sender and the receiver is one-to-one.
- A multicast destination address defines a group of addresses; the relationship between the sender and the receivers is one-to-many.
- The broadcast address is a special case of the multicast address; the recipients are all the stations on the LAN. A broadcast destination address is forty-eight 1s.

Example 13.1

Define the type of the following destination addresses:

a. 4A:30:10:21:10:1A
b. 47:20:1B:2E:08:EE
c. FF:FF:FF:FF:FF:FF

Solution

To find the type of the address, we need to look at the second hexadecimal digit from the left. If it is even, the address is unicast. If it is odd, the address is multicast. If all digits are F's, the address is broadcast. Therefore, we have the following:

a. This is a unicast address because A in binary is 1010 (even).
b. This is a multicast address because 7 in binary is 0111 (odd).
c. This is a broadcast address because all digits are F's.

The way the addresses are sent out on line is different from the way they are written in hexadecimal notation. The transmission is left-to-right, byte by byte; however, for each byte, the least significant bit is sent first and the most significant bit is sent last. This means that the bit that defines an address as unicast or multicast arrives first at the receiver.

2.3. Categories of Standard Ethernet

The Standard Ethernet defines several physical layer implementations; four of the most common, are shown in Figure 13.7.

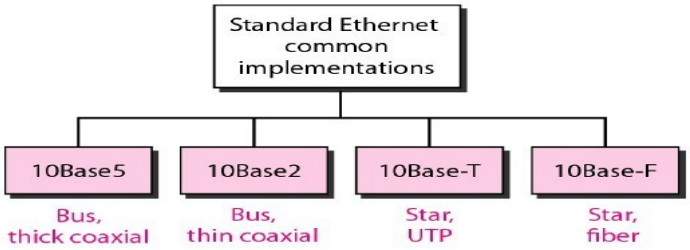


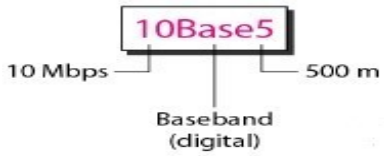
Figure 13.7 Categories of Standard Ethernet

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 **10Base5, thick Ethernet, or Thicknet.** 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. Compared to 10Base5 or 10Base2, we can see that the hub actually replaces the coaxial cable as far as a collision is concerned. The maximum length of the twisted cable here is defined as 100 m, to minimize the effect of attenuation in the twisted cable.

- **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

.Characteristics	*10Base5*	*10Base2*	*10Base-T*	*10Base-F*
Media	Thick Coaxial Cable	Thin Coaxial Cable	2UTP	2Fiber
Maximum length	500m	185m	100m	2000m
Line encoding	Manchester	Manchester	Manchester	Manchester

Table 13.1 shows a summary of Standard Ethernet implementations

2.4. Changes in the Standard

The 10-Mbps Standard Ethernet has gone through several changes before moving to the higher data rates. These changes actually opened the road to the evolution of the Ethernetto become compatible with other high-data-rate LANs. We discuss some of these changes in this section.

2.4.1. Bridged Ethernet

The first step in the Ethernet evolution was the division of a LAN by bridges. A Bridge is a two port switch used to connect two segments of a LAN. Bridges have two effects on an Ethernet LAN:

- They **raise the bandwidth** and
- They separate collision domains.

Raising the Bandwidth

In an unbridged Ethernet network, the total capacity (10 Mbps) is shared among all stations with a frame to send; the stations share the bandwidth of the network. If only one station has frames to send, it benefits from the total capacity (10 Mbps). But if more than one station needs to use the network, the capacity is shared. 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 13.8 shows the situation.

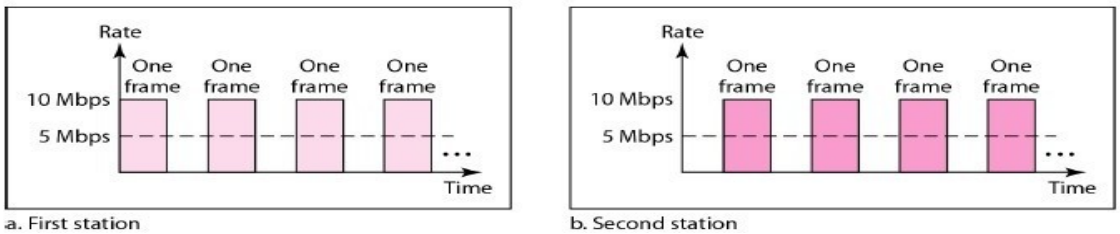


Figure 13.8 Sharing bandwidth

A bridge divides the network into two or more networks. Bandwidth-wise, each network is

independent. For example, in Figure 13.9, a network with 12 stations is divided into two networks, each with 6 stations. Now each network has a capacity of 10 Mbps. The 10-Mbps capacity in each segment is now shared between 6 stations (actually 7 because the bridge acts as a station in each segment), not 12 stations. In a network with a heavy load, each station theoretically is offered 10/6 Mbps instead of 10/12 Mbps, assuming that the traffic is not going through the bridge. It is obvious that if we further divide the network, we can gain more bandwidth for each segment. For example, if we use a four-port bridge, each station is now offered 10/3 Mbps, which is 4 times more than an unbridged network.

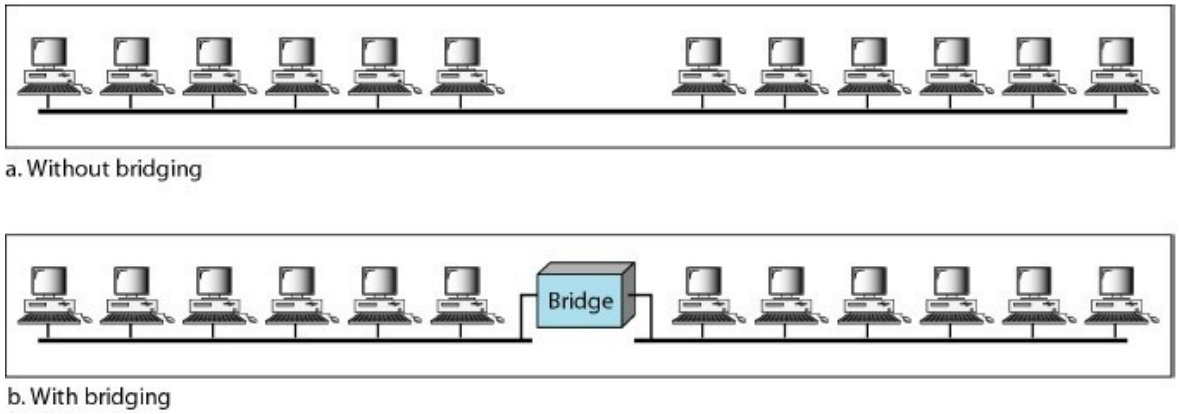


Figure 13.9 A network with and without a bridge

Separating Collision Domains

Another advantage of a bridge is the separation of the collision domain. Figure 13.10 shows the collision domains for an unbridged and a bridged network. You can see that the collision domain becomes much smaller and the probability of collision is reduced tremendously. Without bridging, 12 stations contend for access to the medium; with bridging only 3 stations contend for access to the medium.

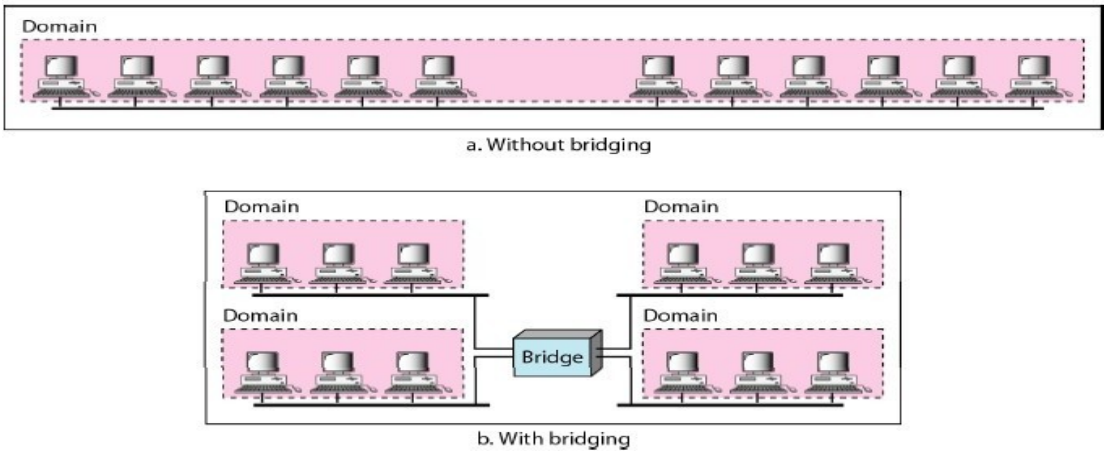


Figure 13.10 Collision domains in an unbridged network and a bridged network

2.4.2. Switched Ethernet

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? 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). 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. 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. Figure 13.11 shows a switched LAN.

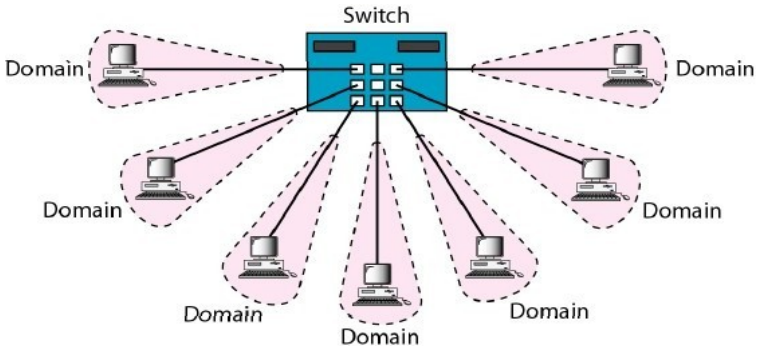


Figure 13.11 Switched Ethernet

2.4.3. Full-Duplex Ethernet

One of the limitations of 10Base5 and 10Base2 is that communication is half-duplex (10Base-T is always full-duplex); a station can either send or receive, but may not do both at the same time. The next step in the evolution was to move from switched Ethernet to full-duplex switched Ethernet. The full-duplex mode increases the capacity of each domain from 10 to 20 Mbps. Figure 13.12 shows a switched Ethernet in full-duplex mode. Note that instead of using one link between the station and the switch, the configuration uses two links: one to transmit and one to receive.

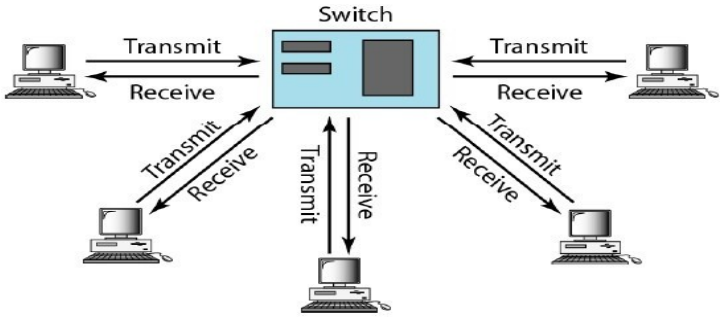


Figure 13.12 Full-duplex switched Ethernet

No Need for CSMA/CD

In full-duplex switched Ethernet, there is no need for the *CSMA/CD* method. In a full duplex switched Ethernet, each station is connected to the switch via two separate links. Each station or switch can send and receive independently without worrying about collision. Each link is a point-to-point dedicated path between the station and the switch. There is no longer a need for carrier sensing; there is no longer a need for collision detection. The job of the MAC layer becomes much easier. The carrier sensing and collision detection functionalities of the MAC sub-layer can be turned off.

2.5. Fast Ethernet (IEEE 802.3u)

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

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

Topology

Fast Ethernet is designed to connect two or more stations together. If there are only two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the center, as shown in Figure 13.13.

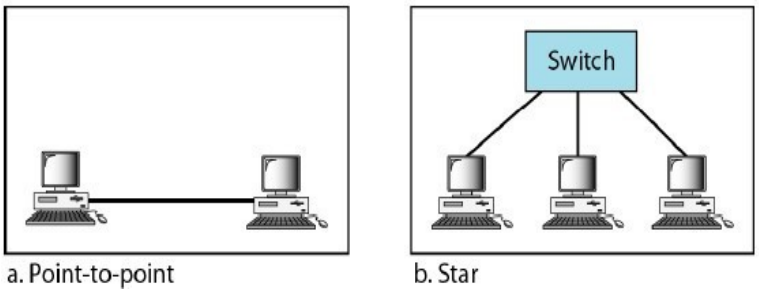


Figure 13.13 Fast Ethernet topology

Implementation

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

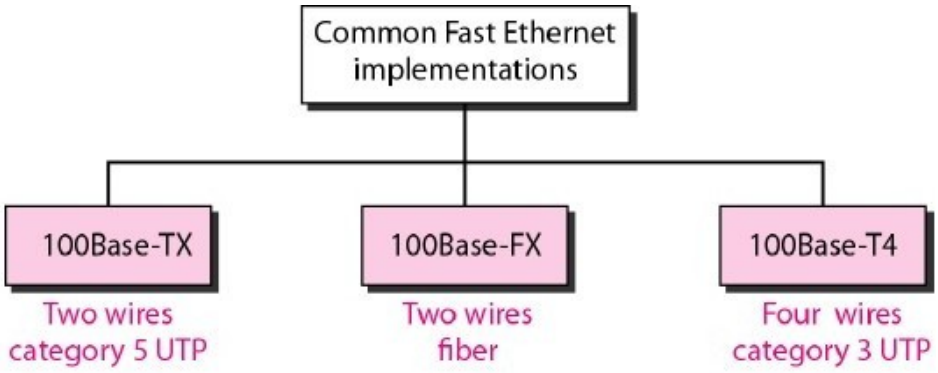


Figure 13.14 Fast Ethernet implementations

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

Table 13.2 Summary of Fast Ethernet implementations

2.6. Gigabit Ethernet (IEEE 802.3z)

The need for an even higher data rate resulted in the design of the Gigabit Ethernet protocol (1000 Mbps). The IEEE committee calls the Standard 802.3z. The goals of the Gigabit Ethernet design can be summarized as follows:

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

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

Topology

Gigabit Ethernet is designed to connect two or more stations. If there are only two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the center. Another possible configuration is to connect several star topologies or let a star topology be part of another as shown in Figure 13.15.

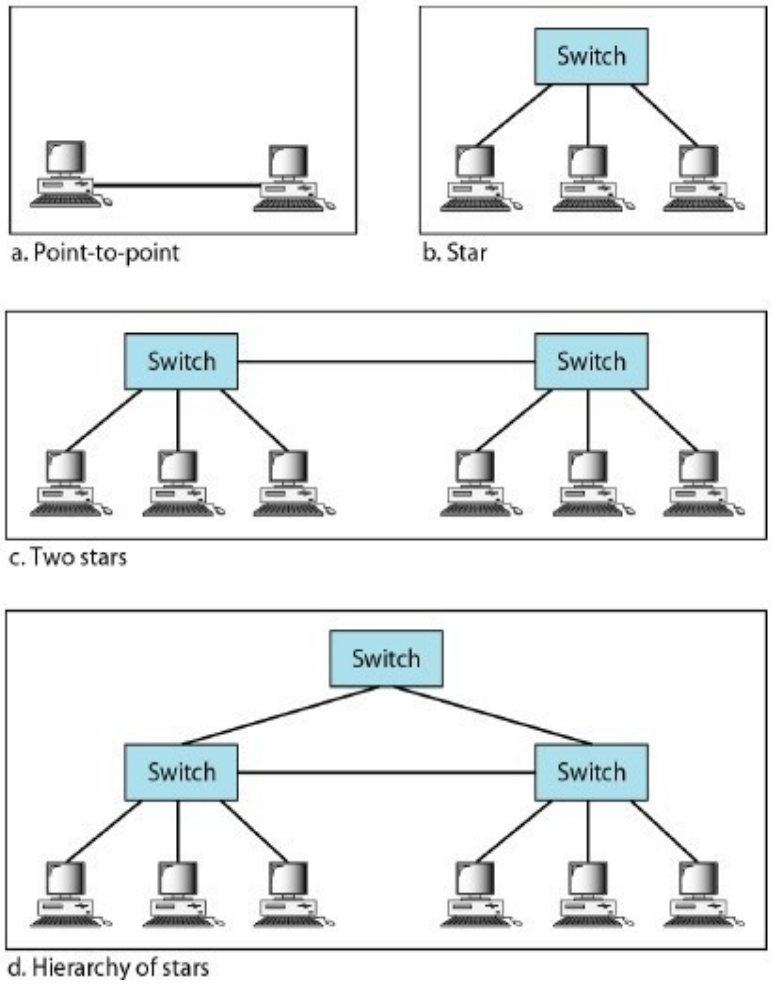


Figure 13.15 Topologies of Gigabit Ethernet

Implementation

Gigabit Ethernet can be categorized as either a two-wire or a four-wire implementation. The two-wire implementations use fiber-optic cable (1000Base-SX, short-wave, or 1000Base-LX, long-wave), or STP (1000Base-CX). The four-wire version uses category 5 twisted-pair cable (1000Base-T). In other words, we have four implementations, as shown in Figure 13.16.

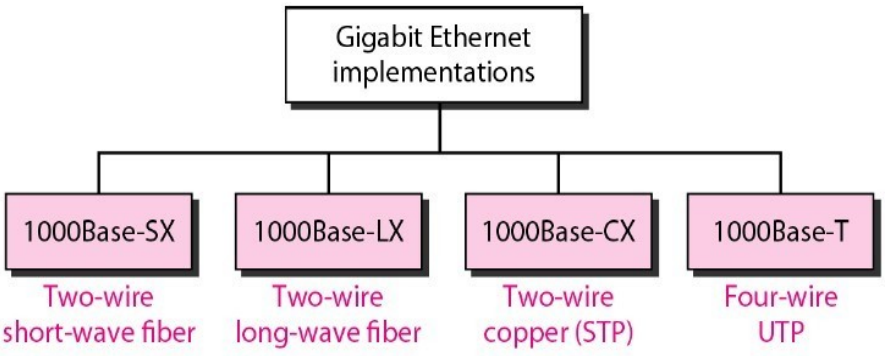


Figure 13.16 Gigabit Ethernet implementations

Summary

Characteristics	1000Base-SX	1000Base-LX	1000Base-CX	1000Base-T
Media	Fiber Short wave	Fiber Long wave	STP	CAT 5 UTP
Number of wires	2	2	2	4
Maximum length	550m	5000m	25m	100m
Line encoding	NRZ	NRZ	NRZ	4D-PAM5

Table 13.3 is a summary of the Gigabit Ethernet implementations.

2.7. Ten-Gigabit Ethernet(IEEE 802.3ae)

The IEEE committee created Ten-Gigabit Ethernet and called it Standard 802.3ae. The goalsof the Ten-Gigabit Ethernet design can be summarized as follows:

a. Upgrade the data rate to 10 Gbps.
b. Make it compatible with Standard, Fast, and Gigabit Ethernet.
c. Use the same 48-bit address.
d. Use the same frame format.
e. *S.* Keep the same minimum and maximum frame lengths.
f. Allow the interconnection of existing LANs into a metropolitan area network (MAN)or a wide area network (WAN).
g. Make Ethernet compatible with technologies such as Frame Relay and ATM.

Ten-Gigabit Ethernet operates only in **full duplex mode** which means there is no need forcontention; *CSMA/CD* is not used in Ten-Gigabit Ethernet.

Implementation

Ten-Gigabit Ethernet is designed for using fiber-optic cable over long distances. Three implementations are the most common: 10GBase-S, 10GBase-L, and 10GBase-E. Table 13.4 shows a summary of the Ten-Gigabit Ethernet implementations:

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

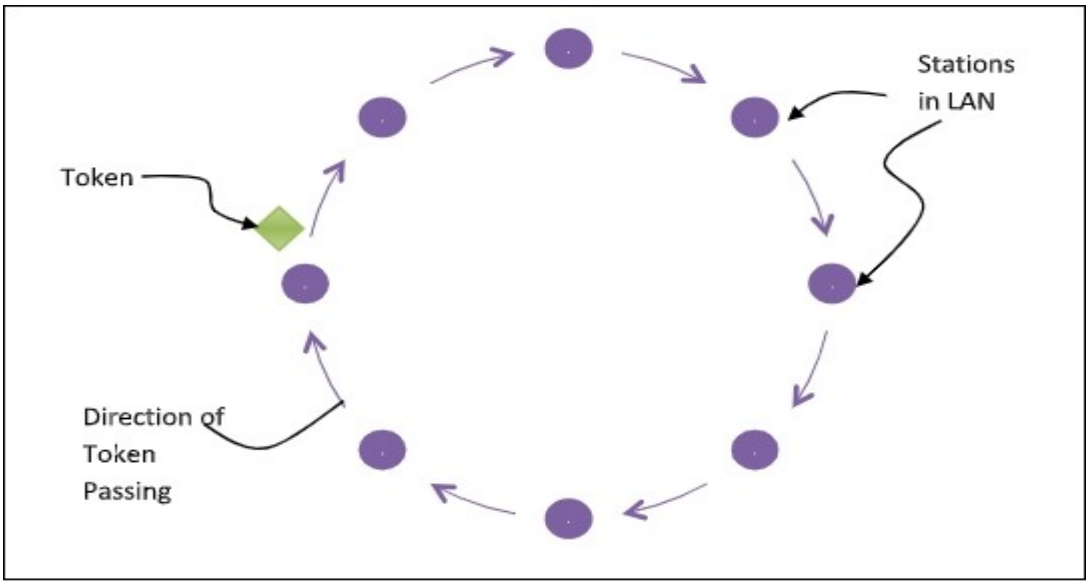
Table 13.4 Summary of Ten-Gigabit Ethernet implementations

Token Ring (IEEE 802.5)

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 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. This is shown in the following diagram –



Wireless LANS (802.11)

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

A. Architecture

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

a) Basic Service Set

IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP). Figure 3.1 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 network.

NOTE: A BSS without an AP is called an ad hoc network; a BSS with an AP is called an infrastructure network.

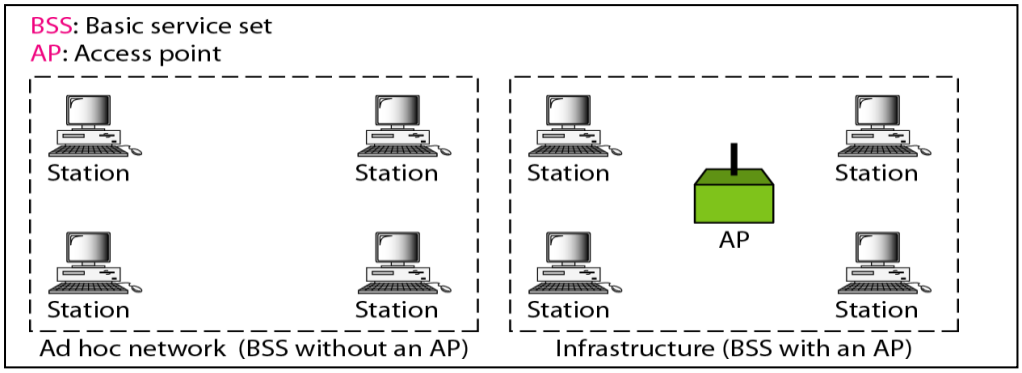


Figure 3.1 Basic service sets (BSSs)

b) Extended Service Set

An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a distribution system, which is usually a wired LAN. The distribution system connects the APs in the BSSs. IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet. Note that the extended service set uses two types of stations: mobile and stationary. The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN. Figure 3.2 shows an ESS.

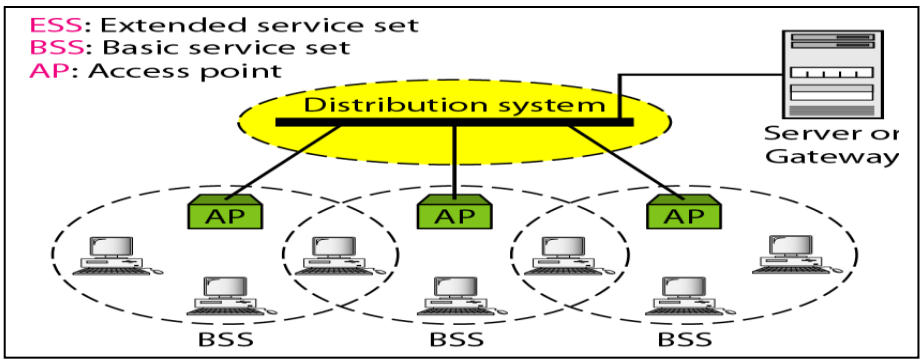


Figure 3.2 Extended service sets (ESSs)

When BSSs are connected, the stations within reach of one another can communicate without the use of an AP. However, communication between two stations in two different BSSs usually occurs via two APs. 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.

B. MAC Sub layer

IEEE 802.11 defines two MAC sublayers: the distributed coordination function (DCF) and point coordination function (PCF). Figure 3.3 shows the relationship between the two MAC sublayers, the LLC sublayer, and the physical layer.

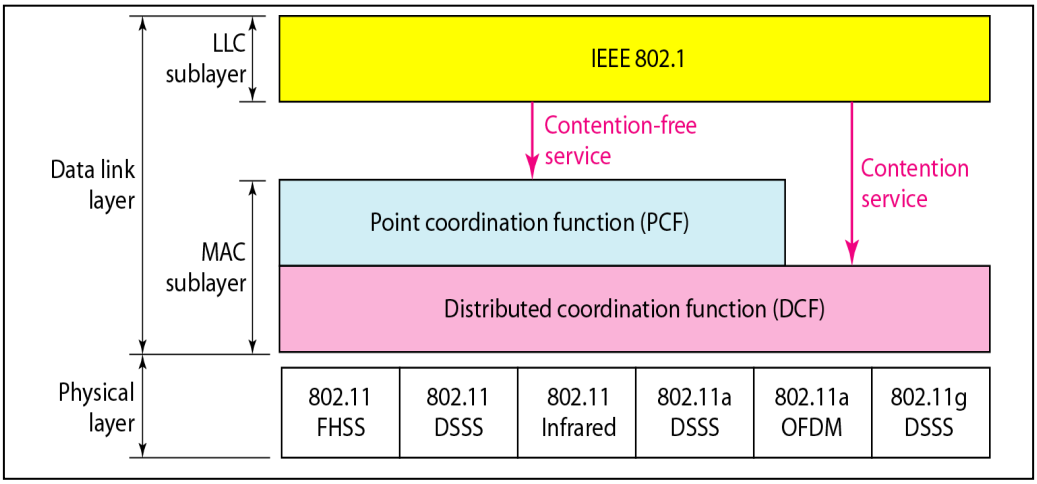


Figure 3.3 MAC layers in IEEE 802.11 standard

1. Distributed Coordination Function

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

- For collision detection a station must be able to send data and receive collision signals at the same time. This can mean costly stations and increased bandwidth requirements.
- Collision may not be detected because of the hidden station problem.
- The distance between stations can be great. Signal fading could prevent a station at one end from hearing a collision at the other end.

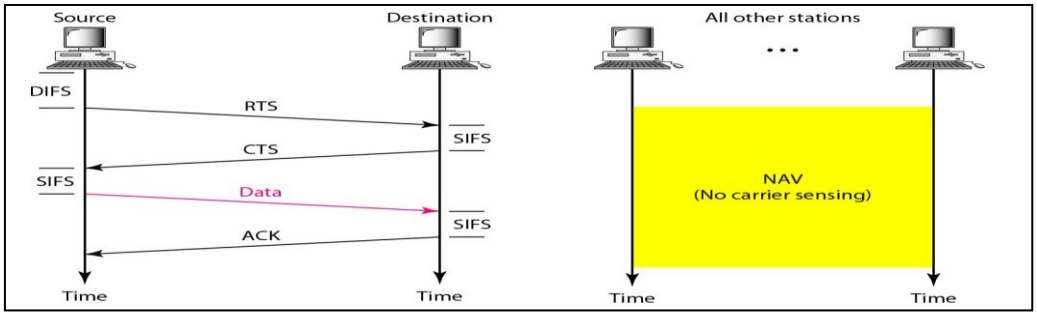


Figure 3.4 CSMA/CA and NAV

- Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.
  - The channel uses a persistence strategy with back-off until the channel is idle.
  - After the station is found to be idle, the station waits for a period of time called the distributed inter-frame space (DIFS); then the station sends a control frame called the request to send (RTS).
- After receiving the RTS and waiting a period of time called the short inter-frame 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.

- The source station sends data after waiting an amount of time equal to SIFS.

- The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received. Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination. On the other hand, the lack of collision in CSMA/CD is a kind of indication to the source that data have arrived.

In other words, how is the collision avoidance aspect of this protocol accomplished? The key is a feature called NAV. When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel. The stations that are affected by this transmission create a timer called a network allocation vector (NAV) that shows how much time must pass before these stations are allowed to check the channel for idleness. Each time a station accesses the system and sends an RTS frame, other stations start their NAV. In other words, each station, before sensing the physical medium to see if it is idle, first checks its NAV to see if it has expired. Figure 3.4 shows the idea of NAV.

Collision During Handshaking What happens if Two or more stations may try to send RTS frames at the same time. These control frames may collide. However, because there is no mechanism for collision detection, the sender assumes there has been a collision if it has not received a CTS frame from the receiver. The back-off strategy is employed, and the sender tries again.

2. Point Coordination Function (PCP)

The point coordination function (PCF) is an optional access method that can be implemented in an infrastructure network (not in an ad hoc network). It is implemented on top of the DCF and is used mostly for time-sensitive transmission. PCF has a centralized, contention-free polling access method. The AP performs polling for stations that are capable of being polled. The stations are polled one after another, sending any data they have to the AP.

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

C. Addressing Mechanism

The IEEE 802.11 addressing mechanism specifies four cases, defined by the value of the two flags in the FC field, To DS and From DS. Each flag can be either 0 or 1, resulting in four different situations. The interpretation of the four addresses (address 1 to address 4) in the MAC frame depends on the value of these flags, as shown in Table 3.1.

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

Table 3.1 Addresses

Note that address 1 is always the address of the next device that the frame will visit. Address 2 is always the address of the previous device that the frame has left. Address 3 is the address of the final destination station if it is not defined by address 1 or the original source station if it is not defined by address 2. Address 4 is the original source when the distribution system is also wireless.

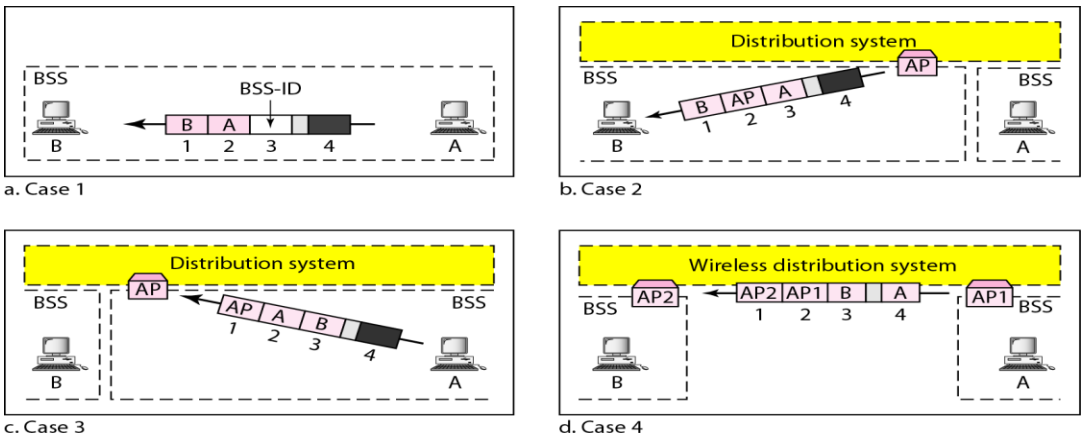


Figure 3.5 Addressing mechanisms

- Case 1: 00 In this case, To DS=0 and From DS =0. This means that the frame is not going to a distribution system (To DS =0) and is not coming from a distribution system (From DS =0). The frame is going from one station in a BSS to another without passing through the distribution system. The addresses are shown in Figure 3.5.
- Case 2: 01 In this case, To DS 0 and From DS =1. This means that the frame is coming from a distribution system (From DS =1). The frame is coming from an AP and going to a station. The addresses are as shown in Figure 3.5. Note that address 3 contains the original sender of the frame (in another BSS).
- Case 3: 10 In this case, To DS=1 and From DS=0. This means that the frame is going to a distribution system (To DS =1). The frame is going from a station to an AP. The ACK is sent to the original station. The addresses are as shown in Figure 3.5. Note that address 3 contains the final destination of the frame in the distribution system.
- 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. Here, we need four addresses to define the original sender, the final destination, and two intermediate APs. Figure 3.5 shows the situation.

D. Physical Layer

We discuss six specifications, as shown in Table 3.2. All implementations, except the infrared, operate in the industrial, scientific, and medical (ISM) band, which defines three unlicensed bands in the three ranges 902–928 MHz, 2.400–4.835 GHz, and 5.725–5.850 GHz.

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

Table 3.2 Physical layer

E. Problems in WLAN

If we try to use CSMA for wireless LAN, then it uses the principle of simply listening to other transmission and only transmits if no one else is transmitting. But there are two problems in using CSMA. They are Hidden and Exposed Station Problems

1. Hidden and Exposed Station Problems

Hidden Station Problem Figure 3.6 shows an example of the hidden station problem. Station B has a transmission range shown by the left oval (sphere in space); every station in this range can hear any signal transmitted by station B. Station C has a transmission range shown by the right oval (sphere in space); every station located in this range can hear any signal transmitted by C. Station C is outside the transmission range of B; likewise, station B is outside the transmission range of C. Station A, however, is in the area covered by both Band C; it can hear any signal transmitted by B or C.

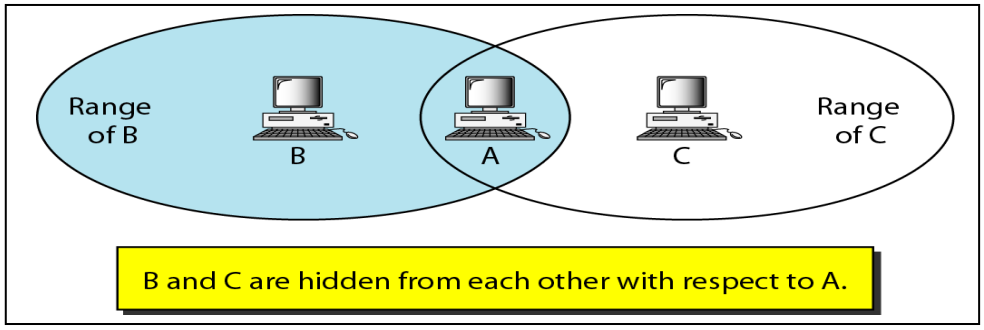


Figure 3.6 Hidden station problem

Assume that station B is sending data to station A. In the middle of this transmission, station C also has data to send to station A. However, station C is out of B's range and transmissions from B cannot reach C. Therefore C thinks the medium is free. Station C sends its data to A, which results in a collision at A because this station is receiving data from both B and C. In this case, we say that stations Band C are hidden from each other with respect to A. Hidden stations can reduce the capacity of the network because of the possibility of collision.

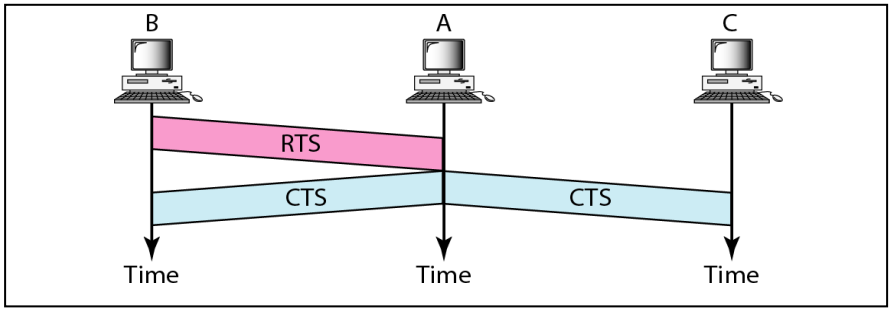


Figure 3.7 Use of handshaking to prevent hidden station problem

The solution to the hidden station problem is the use of the handshake frames (RTS and CTS). Figure 3.7 shows that the RTS(request to send) message from B reaches A, but not C. However, because both B and C are within the range of A, the CTS(clear to send) message, which contains the duration of data transmission from B to A reaches C. Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

2. Exposed Station Problem

Exposed Station Problem Now consider a situation that is the inverse of the previous one: the exposed station problem. In Figure 3.8, station A is transmitting to station B. Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B. However, station C is exposed to transmission from A; it hears what A is sending and thus refrains from sending. In other words, C is too conservative and wastes the capacity of the channel.

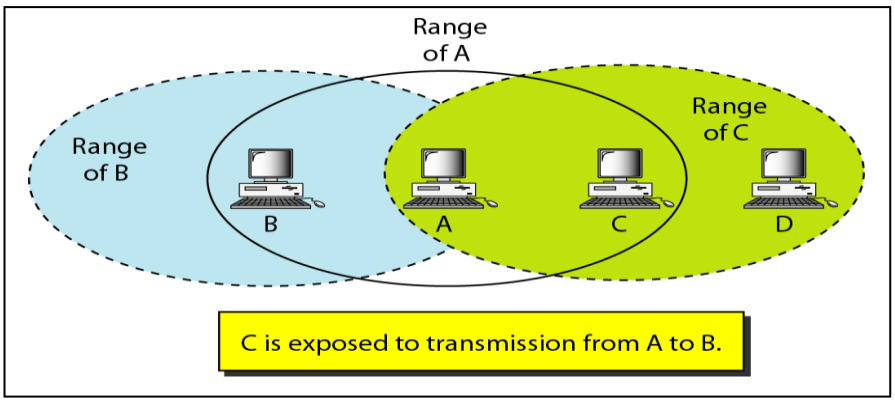


Figure 3.8 Exposed station problem

The handshaking messages RTS and CTS cannot help in this case, despite what you might think. Station C hears the RTS from A, but does not hear the CTS from B. Station C, after hearing the RTS from A, can wait for a time so that the CTS from B reaches A; it then sends an RTS to D to show that it needs to communicate with D. Both stations B and A may hear this RTS, but station A is in the sending state, not the receiving state. Station B, however, responds with a CTS. The problem is here. If station A has started sending its data, station C cannot hear the CTS from station D because of the collision; it cannot send its data to D. It remains exposed until A finishes sending its data as Figure 3.9 shows.

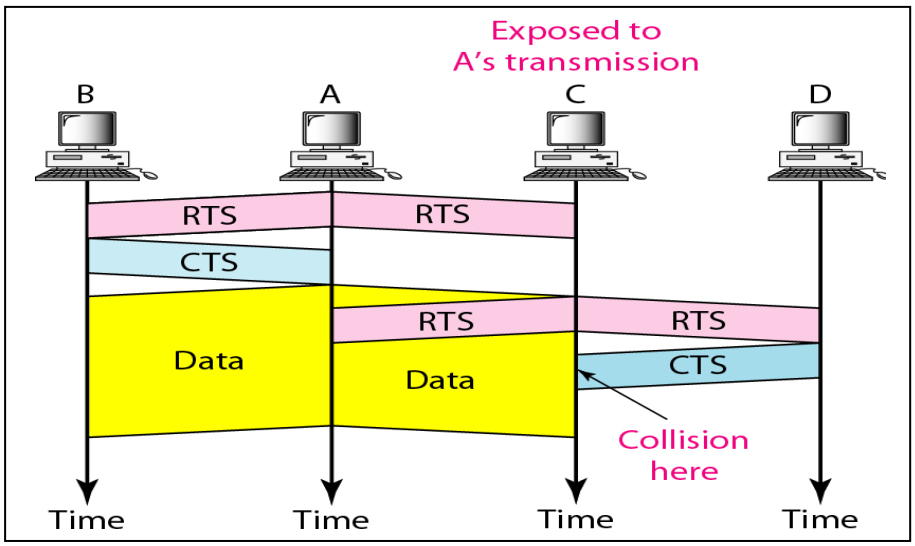
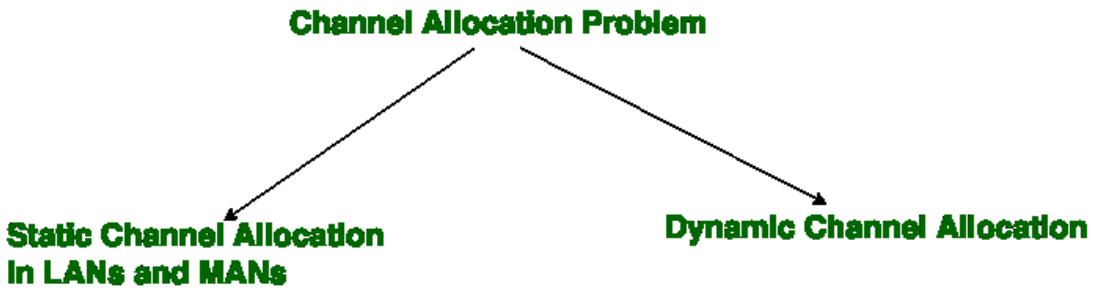


Figure 3.9 Use of handshaking in exposed station problem

Channel allocation

Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks. There are user's quantity may vary every time the process takes place. If there are N numbers of users and channel is divided into N equal-sized sub channels, Each user is assigned one portion. If the number of users are small and don't vary at times, then Frequency Division Multiplexing can be used as it is a simple and efficient channel bandwidth allocating technique.

Channel allocation problem can be solved by two schemes: Static Channel Allocation in LANs and MANs, and Dynamic Channel Allocation.



These are explained as following below.

1. **Static Channel Allocation in LANs and MANs:**
   It is the classical or traditional approach of allocating a single channel among multiple competing users using Frequency Division Multiplexing (FDM). if there are N users, the frequency channel is divided into N equal sized portions (bandwidth), each user being assigned one portion. since each user has a private frequency band, there is no interference between users.

The process of static channel allocation scheme is explained below −

- If there are N users, the bandwidth is divided into N equal sized partitions, where each user is assigned with one portion. This is because, each user has a private frequency band.
- When there is only a small and constant number of users, each user has a heavy load of traffic, this division is a simple and efficient allocation mechanism.
- Let us take a wireless example of FM radio stations, each station gets a portion of FM band and uses it most of the time to broadcast its signal.
- When the number of senders is large and varying or traffic is suddenly changing, FDM faces some problems.
- If the spectrum is cut up into N regions and fewer than N users are currently interested in communicating, a large piece of valuable spectrum will be wasted. And if more than N users want to communicate, some of them will be denied permission for lack of bandwidth, even if some of the users who have been assigned a frequency band hardly ever transmit or receive anything.
- A static allocation is a poor fit to most computer systems, in which data traffic is extremely burst, often with peak traffic to mean traffic ration of 1000:1, consequently most of the channels will be idle most of the time.

- The poor performance of static FDM can easily be seen with simple queueing theory calculation.
    - ✓ Let us start with mean time delay T,
    - ✓ Send a frame onto a channel of capacity C bps.
    - ✓ Let us assume frames arrive randomly at an average arrival time λ frames/sec
    - ✓ Average length of the frame is 1/μ bits.
    - ✓ With the help of these parameters the service rate of channel is μC frame/sec
    - ✓ Standard queueing theory result is −
    - ✓ T= 1/(μC- λ)
    - ✓ Now divide the single channel into N independent subchannels, each with capacity C/N bps.
    - ✓ The mean input rate on each subchannel is λ/N.
    - ✓ Finally we get

      TN=1/(μ(C/N) – (λ/N))

      = N/(μC- λ)

      = NT

2. Dynamic Channel Allocation:

There are some key assumptions in Dynamic channel allocation, which are as follows −

- **Independent Traffic** − This model consists of N independent stations with a program or user that generates frames for transmission. Once a frame has been generated the station is blocked and it does not do anything until the frame has been successfully transmitted.
- **Single channel** − A single channel is available for all communication All stations can transmit on it and all can receive from it.
- **Observable collision** − All stations can detect that a collision has occurred. A collided frame must be transmitted later.
- **Continuous or slotted time** − Time may be assumed continuous; frame transmission can begin at any instant. In other way, time may be slotted or divided into discrete intervals. Frame transmission must then begin at the start of a slot.
- **Carrier sense or No carrier sense** − With the carrier sense assumption, stations can tell if the channel is in use before trying to use it. Station will transmit only when the channel is free.

Example:

Let us consider cellular telephone in a city, users move and they can turn a cell phone on and off at any time. Therefore, the set of cell phones are operating in the range of a given cell tower that varies constantly.

In such a situation a dynamic channel allocation scheme is needed where a mapping can be established when a new station appears, and the mapping can be removed when the station disappears.

Multiple access protocols

Data Link Layer

The data link layer is used in a computer network to transmit the data between two devices or nodes. It divides the layer into parts such as **data link control** and the **multiple access resolution/protocol**. The upper layer has the responsibility to flow control and the error control in the data link layer, and hence it is termed as **logical of data link control**. Whereas the lower sub-layer is used to handle and reduce the collision or multiple access on a channel. Hence it is termed as **media access control** or the multiple access resolutions.

Data Link Control

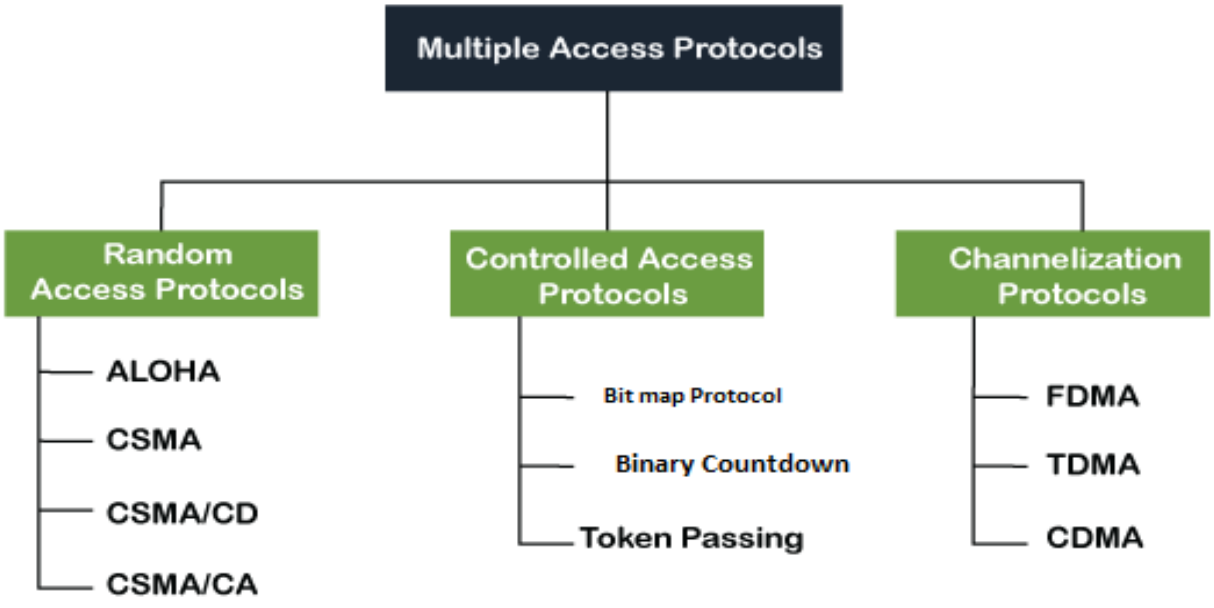
A data link control is a reliable channel for transmitting data over a dedicated link using various techniques such as framing, error control and flow control of data packets in the computer network.

What is a multiple access protocol?

When a sender and receiver have a dedicated link to transmit data packets, the data link control is enough to handle the channel. Suppose there is no dedicated path to communicate or transfer the data between two devices. In that case, multiple stations access the channel and simultaneously transmits the data over the channel. It may create collision and cross talk. Hence, the multiple access protocol is required to reduce the collision and avoid crosstalk between the channels.

For example, suppose that there is a classroom full of students. When a teacher asks a question, all the students (small channels) in the class start answering the question at the same time (transferring the data simultaneously). All the students respond at the same time due to which data is overlap or data lost. Therefore it is the responsibility of a teacher (multiple access protocol) to manage the students and make them one answer.

Following are the types of multiple access protocol that is subdivided into the different process as:



A. Random Access Protocol

In this protocol, all the station has the equal priority to send the data over a channel. In random access protocol, one or more stations cannot depend on another station nor any station control another station. Depending on the channel's state (idle or busy), each station transmits the data frame. However, if more than one station sends the data over a channel, there may be a collision or data conflict. Due to the collision, the data frame packets may be lost or changed. And hence, it does not receive by the receiver end.

Following are the different methods of random-access protocols for broadcasting frames on the channel.

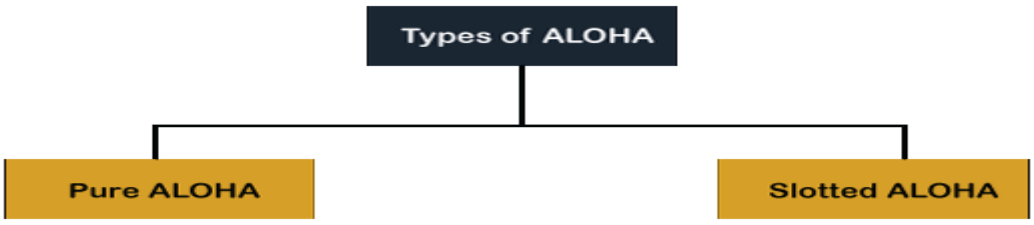
- Aloha
- CSMA
- CSMA/CD
- CSMA/CA

ALOHA Random Access Protocol

It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.

Aloha Rules:

1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires retransmission of data after some random amount of time.

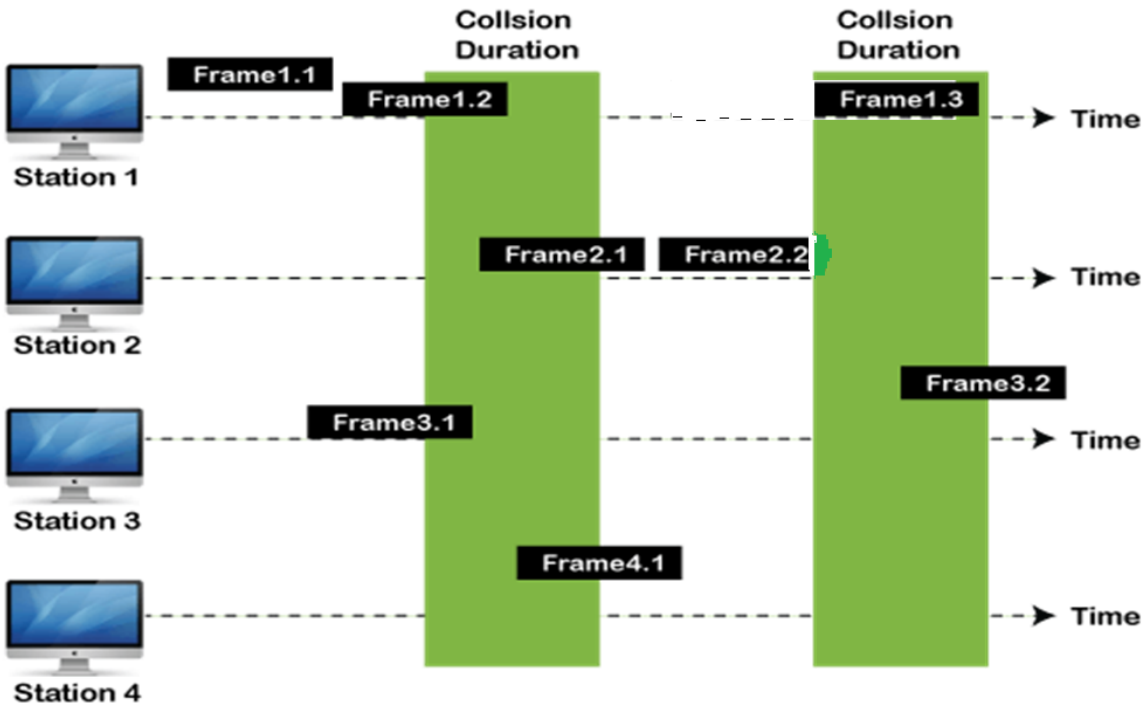


Pure Aloha

Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not

acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

1. The total vulnerable time of pure Aloha is 2 * Tfr.
2. Maximum throughput occurs when G = 1/ 2 that is 18.4%.
3. Successful transmission of data frame is S = G * e ^ - 2 G.



Frames in Pure ALOHA

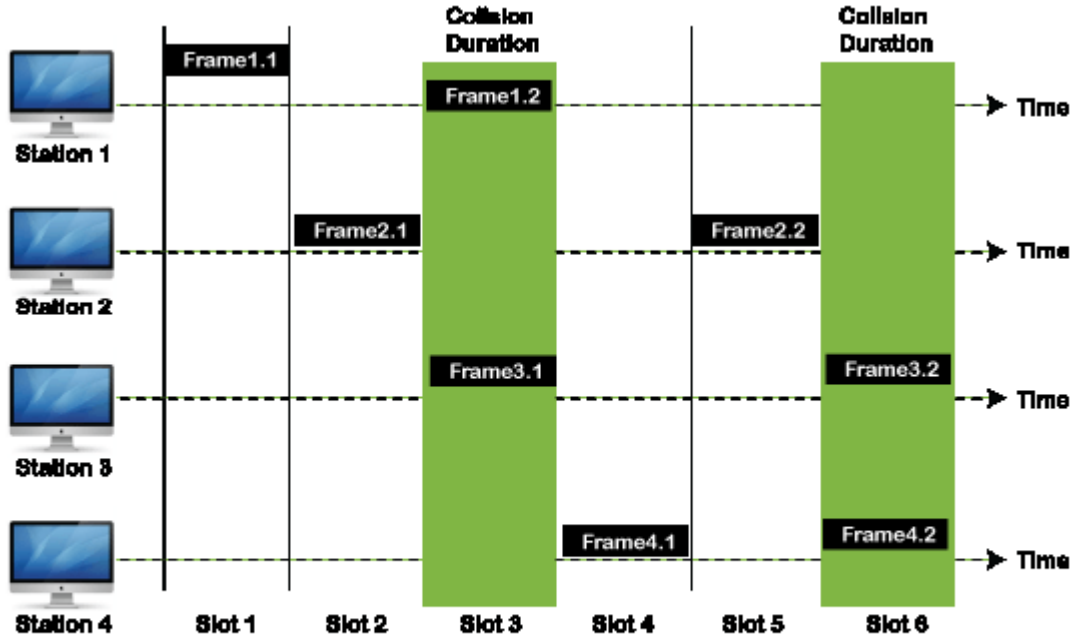
As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same time, other frames are lost or destroyed. Whenever two frames fall on a shared channel simultaneously, collisions can occur, and both will suffer damage. If the new frame's first bit enters the channel before finishing the last bit of the second frame. Both frames are completely finished, and both stations must retransmit the data frame.

Slotted Aloha

The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.

1. Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.

2. The probability of successfully transmitting the data frame in the slotted Aloha is S = G * e ^ - 2 G.
3. The total vulnerable time required in slotted Aloha is Tfr.



Frames in Slotted ALOHA

CSMA (Carrier Sense Multiple Access)

It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

CSMA Access Modes

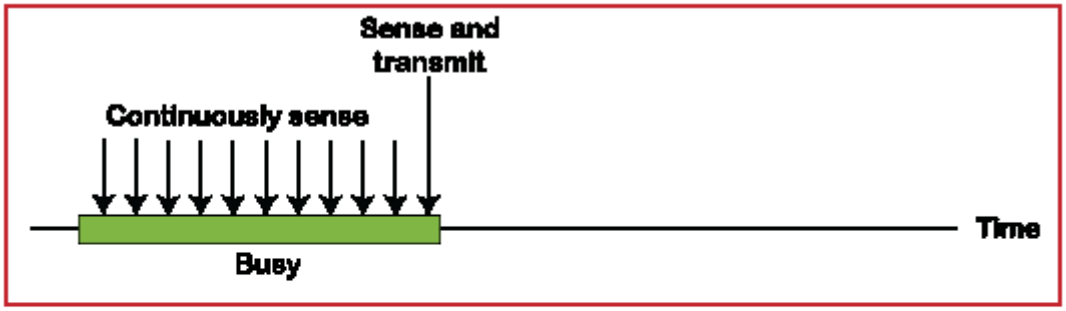
1-Persistent: In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data. Else it must wait and keep track of the status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle.

Non-Persistent: It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.

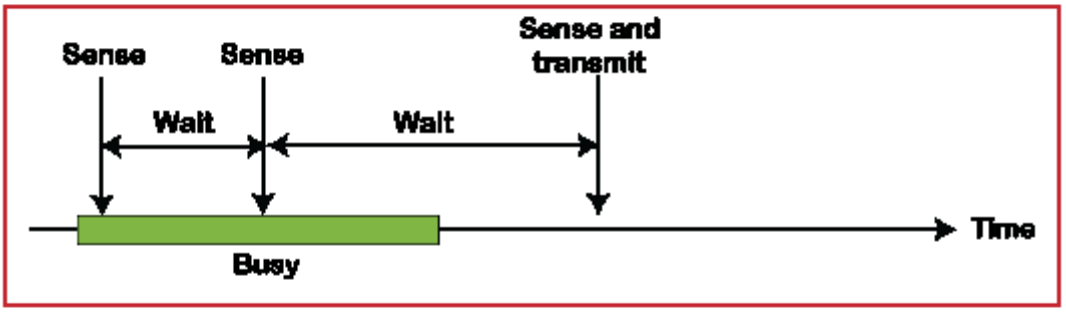
P-Persistent: It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a **P** probability. If the data is not transmitted, it waits for a (**q = 1-p probability**) random time and resumes the frame with the next time slot.

O- Persistent: It is an O-persistent method that defines the superiority of the station before the

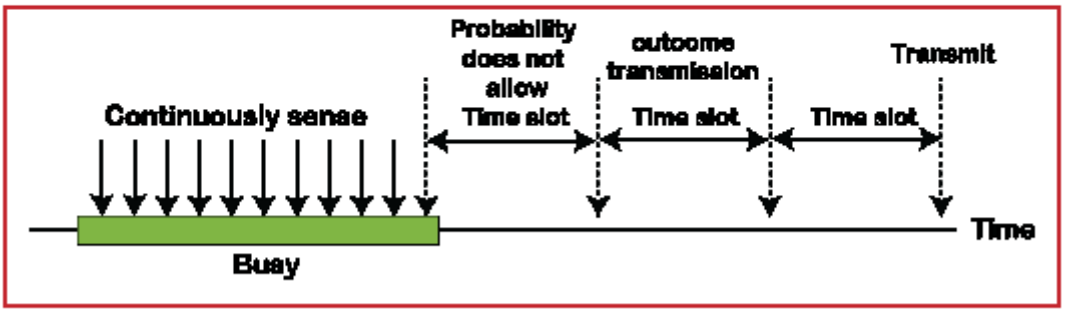
transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.



a. 1-persistent



b. Nonpersistent



c. p-persistent

CSMA/ CD

It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer. Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful. If the frame is successfully received, the station sends another frame. If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission. After that, it waits for a random time before sending a frame to a channel.

CSMA/CD, as well as many other LAN protocols, uses the conceptual model of Fig. 4-5. At the point marked t 0, a station has finished transmitting its frame. Any other station having a frame to send may now attempt to do so. If two or more stations decide to transmit simultaneously, there will be a collision. If a station detects a collision, it aborts its transmission, waits a random period of time, and then tries again (assuming that no other station has started transmitting in the meantime). Therefore, our model for CSMA/CD will consist of alternating contention and transmission periods, with idle periods occurring when all stations are quiet (e.g., for lack of work).

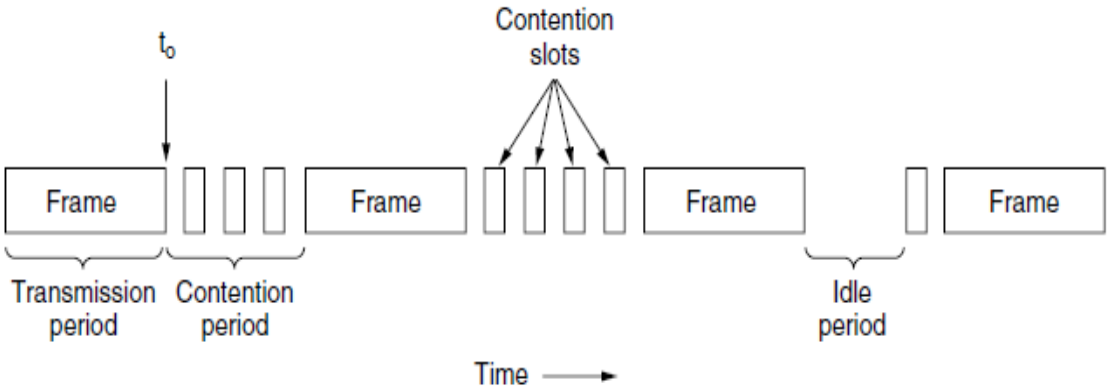


Figure 4-5. CSMA/CD can be in contention, transmission, or idle state.

CSMA/ CA

It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer. When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. If the station receives only a single (own) acknowledgments, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal.

Following are the methods used in the CSMA/ CA to avoid the collision:

Interframe space: In this method, the station waits for the channel to become idle, and if it gets the channel is idle, it does not immediately send the data. Instead of this, it waits for some time, and this time period is called the **Interframe** space or IFS. However, the IFS time is often used to define the priority of the station.

Contention window: In the Contention window, the total time is divided into different slots. When the station/ sender is ready to transmit the data frame, it chooses a random slot number of slots as **wait time**. If the channel is still busy, it does not restart the entire process, except that it restarts the timer only to send data packets when the channel is inactive.

Acknowledgment: In the acknowledgment method, the sender station sends the data frame to the shared channel if the acknowledgment is not received ahead of time.

Collision free Protocols

- Pay constant overhead to achieve performance guarantee
- Good when network load is high

Almost all collisions can be avoided in **CSMA/CD** but they can still occur during the contention period. The collision during the contention period adversely affects the system performance, this

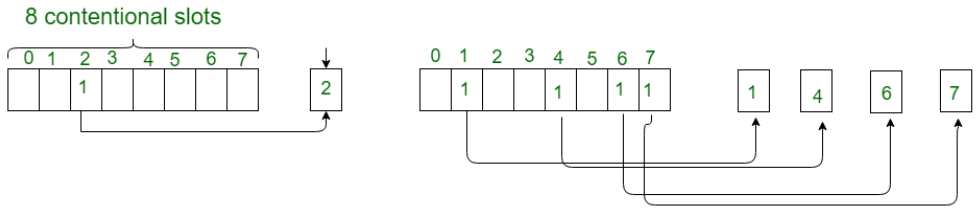
happens when the cable is long and length of packet are short. This problem becomes serious as fiber optics network came into use. Here we shall discuss some protocols that resolve the collision during the contention period.

- Bit-map Protocol
- Binary Countdown
- Token Passing

1. Bit-map Protocol:

Bit map protocol is collision free Protocol. In bitmap protocol method, each contention period consists of exactly N slots. If any station has to send frame, then it transmits a 1 bit in the corresponding slot. For example, if station 2 has a frame to send, it transmits a 1 bit to the 2nd slot.

In general, Station 1 Announce the fact that it has a frame questions by inserting a 1 bit into slot 1. In this way, each station has complete knowledge of which station wishes to transmit. There will never be any collisions because everyone agrees on who goes next. Protocols like this in which the desire to transmit is broadcasting for the actual transmission are called Reservation Protocols.

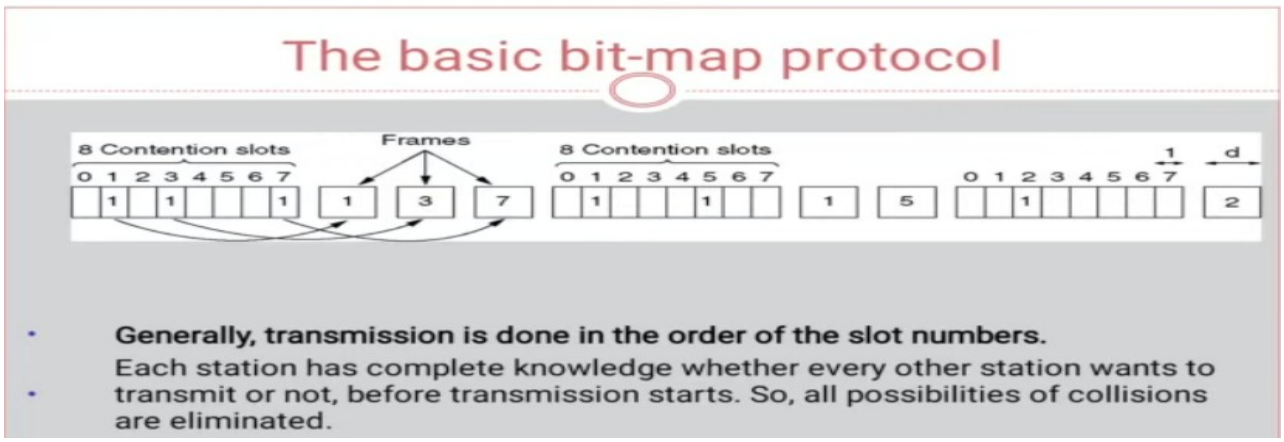


A Bit-map Protocol.

Bit Map Protocol fig (1.1)

For analyzing the performance of this protocol, We will measure time in units of the contention bits slot, with a data frame consisting of d time units. Under low load conditions, the bitmap will simply be repeated over and over, for lack of data frames. All the stations have something to send all the time at high load, the N bit contention period is prorated over N frames, yielding an overhead of only 1 bit per frame.

Generally, high numbered stations have to wait for half a scan before starting to transmit low numbered stations have to wait for half a scan(N/2 bit slots) before starting to transmit, low numbered stations have to wait on an average 1.5 N slots.

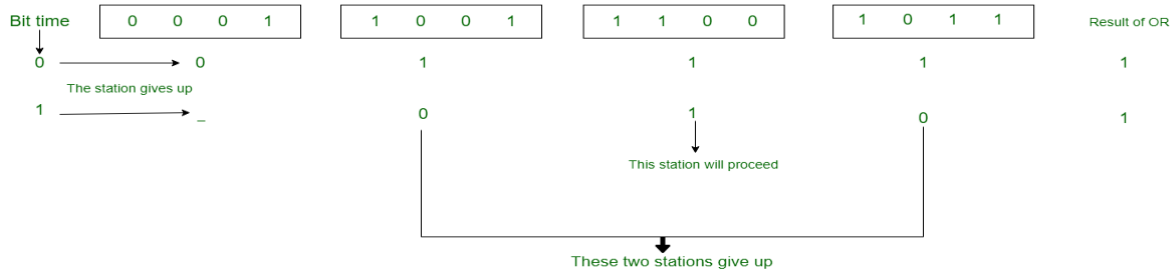


2. Binary Countdown:

Binary countdown protocol is used to overcome the overhead 1 bit per binary station. In binary countdown, binary station addresses are used. A station wanting to use the channel broadcast its address as binary bit string starting with the high order bit. All addresses are assumed of the same length. Here, we will see the example to illustrate the working of the binary countdown.

In this method, different station addresses are read together who decide the priority of transmitting. If these stations 0001, 1001, 1100, 1011 all are trying to seize the channel for transmission. All the station at first broadcast their most significant address bit that is 0, 1, 1, 1 respectively. The most significant bits are read together. Station 0001 see the 1 MSB in another station address and knows that a higher numbered station is competing for the channel, so it gives up for the current round.

Other three stations 1001, 1100, 1011 continue. The next station at which next bit is 1 is at station 1100, so station 1011 and 1001 give up because there 2nd bit is 0. Then station 1100 starts transmitting a frame, after which another bidding cycle starts.



Binary Countdown fig (1.2)

Algorithm:

A problem with the basic bit-map protocol is that overhead is 1 contention bit slot per station. We can do better than that by using binary station addresses.

1. Each station has a binary address. All addresses are the same length.
2. To transmit, a station broadcasts its address as a binary bit string, starting with high- order bit.
3. As soon as a station sees that a high-order bit position that is 0 in its address has been overwritten with a 1, it gives up.
4. After the winning station has transmitted its frame, there is no information available telling how many other stations to send, so the algorithm begins all over with the next frame.

Example:

Suppose that five stations contend for channel access which have the addresses: 1011, 0010, 0111, 1110and 1101.
The iterative steps are –
Step 1: All stations broadcast their most significant bit, i.e. 1, 0, 0, 1, 1.
Step 2: Stations 0010 and 0111 sees 1 bit in other stations, and so they give up competing for the channel.
Step 3: The stations 1011, 1110 and 1101 continue. They broadcast their next bit, i.e. 0, 1,1. Stations 1011 sees 1 bit in other stations, and so it gives up competing for the channel.

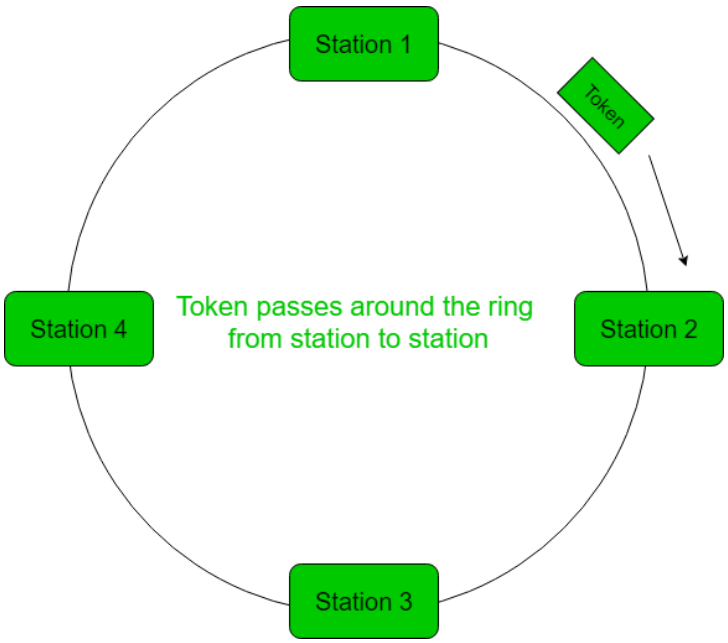
Step 4: The stations 1110 and 1101 continue. They broadcast their next bit, i.e. 1, 0. Since station 1110 has 1 while the other 0, station 1110 gets the access to the channel.

The procedure is illustrated as follows:

Station Address	Bit Time 0 1 2 3	Station status
1011	1 0 - -	Gives up after bit time 1
0010	0 - - -	Gives up after bit time 0
0101	0 - - -	Gives up after bit time 0
1110	1 1 1 -	Gets channel access after bit time 2
1101	1 1 0 -	Gives up after bit time 2

3. Token Passing

- In token passing scheme, the stations are connected logically to each other in form of ring and access to stations is governed by tokens.
- A token is a special bit pattern or a small message, which circulate from one station to the next in some predefined order.
- In Token ring, token is passed from one station to another adjacent station in the ring whereas incase of Token bus, each station uses the bus to send the token to the next station in some predefined order.
- In both cases, token represents permission to send. If a station has a frame queued for transmission when it receives the token, it can send that frame before it passes the token to the next station. If it has no queued frame, it passes the token simply.
- After sending a frame, each station must wait for all N stations (including itself) to send the token to their neighbours and the other N – 1 stations to send a frame, if they have one.
- There exists problems like duplication of token or token is lost or insertion of new station, removal of a station, which need be tackled for correct and reliable operation of this scheme.



Performance of token ring can be concluded by 2 parameters:-

1. **Delay**, is a measure of time between when a packet is ready and when it is delivered. So, the average time (delay) required to send a token to the next station = a/N.
2. **Throughput**, which is a measure of successful traffic.
   Throughput, $S = 1/(1 + a/N)$ for $a<1$

   and

   $S = 1/\{a(1 + 1/N)\}$ for $a>1$.

   where N = number of stations

   $a = T_p/T_t$

(T_p = propagation delay and T_t = transmission delay)

Advantages of Token passing:

- It may now be applied with routers cabling and includes built-in debugging features like protective relay and auto reconfiguration.
- It provides good throughput when conditions of high load.

Disadvantages of Token passing:

- Its cost is expensive.
- Topology components are more expensive than those of other, more widely used standard.
- The hardware element of the token rings are designed to be tricky. This implies that you should choose on manufacture and use them exclusively.

Transparent Bridges

A transparent bridge is a bridge in which the stations are completely unaware of the bridge's existence. If a bridge is added or deleted from the system, reconfiguration of the stations is unnecessary. According to the IEEE 802.1 d specification, a system equipped with transparent bridges must meet three criteria:

1. Frames must be forwarded from one station to another.
2. The forwarding table is automatically made by learning frame movements in the network.
3. Loops in the system must be prevented.

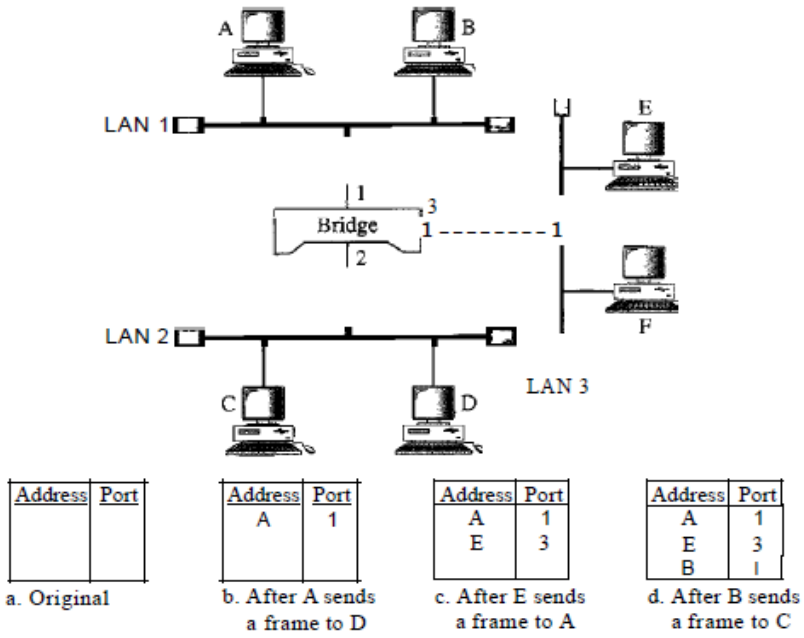
Forwarding: A transparent bridge must correctly forward the frames.

Learning: The earliest bridges had forwarding tables that were static. The systems administrator would manually enter each table entry during bridge setup. Although the process was simple, it was not practical. If a station was added or deleted, the table had to be modified manually. The same was true if a station's MAC address changed, which is not a rare event. For example, putting in a new network card means a new MAC address.

A better solution to the static table is a dynamic table that maps addresses to ports automatically. To make a table dynamic, we need a bridge that gradually learns from the frame movements. To do this, the bridge inspects both the destination and the source addresses. The destination address is used for the forwarding decision (table lookup); the source address is used for adding entries to the table and for updating purposes.

Let us elaborate on this process by using Figure 15.6.

Figure 15.6 *A learning bridge and the process of learning*



1. When station A sends a frame to station D, the bridge does not have an entry for either D or A. The frame goes out from all three ports; the frame floods the network. However, by looking at the source address, the bridge learns that station A must be located on the LAN connected to port 1. This means that frames destined for A, in the future, must be sent out through port 1. The bridge adds this entry to its table. The table has its first entry now.

2. When station E sends a frame to station A, the bridge has an entry for A, so it forwards the frame only to port 1. There is no flooding. In addition, it uses the source address of the frame, E, to add a second entry to the table.

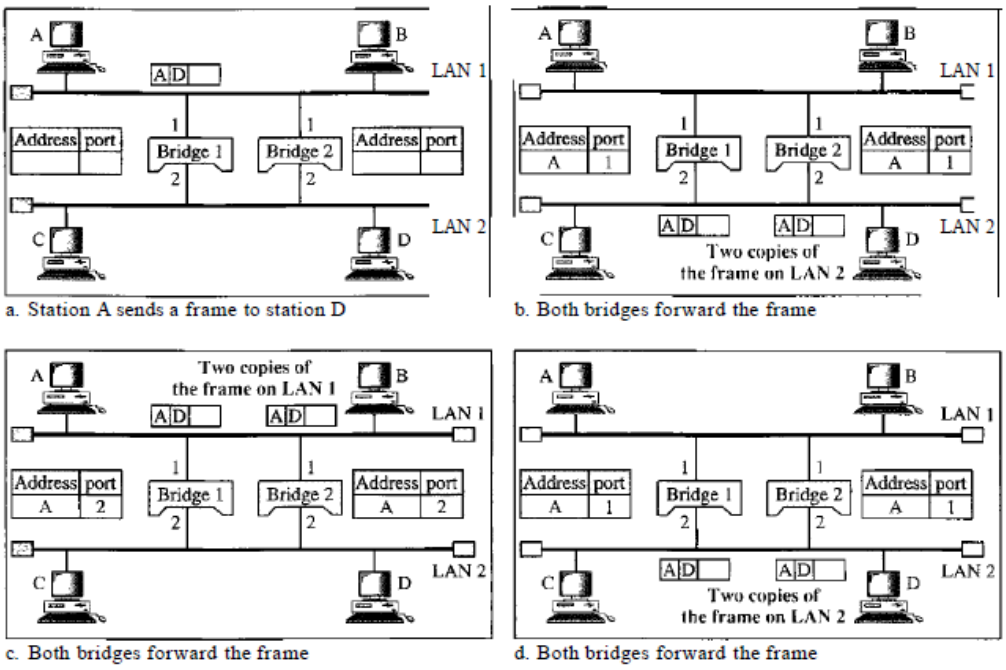
3. When station B sends a frame to C, the bridge has no entry for C, so once again it floods the network and adds one more entry to the table.

4. The process of learning continues as the bridge forwards frames.

Loop Problem:

Transparent bridges work fine as long as there are no redundant bridges in the system. Systems administrators, however, like to have redundant bridges (more than one bridge between a pair of LANs) to make the system more reliable. If a bridge fails, another bridge takes over until the failed one is repaired or replaced. Redundancy can create loops in the system, which is very undesirable. Figure 15.7 shows a very simple example of a loop created in a system with two LANs connected by two bridges.

Figure 15.7 *Loop problem in a learning bridge*



a. Station A sends a frame to station D

b. Both bridges forward the frame

c. Both bridges forward the frame

d. Both bridges forward the frame

1. Station A sends a frame to station D. The tables of both bridges are empty. Both forward the frame and update their tables based on the source address A.

2. Now there are two copies of the frame on LAN 2. The copy sent out by bridge 1 is received by bridge 2, which does not have any information about the destination address D; it floods the bridge. The copy sent out by bridge 2 is received by bridge 1 and is sent out for lack of information about D. Note that each frame is handled separately because bridges, as two nodes on a network sharing the medium, use an access method such as CSMA/CD. The tables of both bridges are updated, but still there is no information for destination D.

3. Now there are two copies of the frame on LAN 1. Step 2 is repeated, and both copies flood the network.

4. The process continues on and on. Note that bridges are also repeaters and regenerate frames. So in each iteration, there are newly generated fresh copies of the frames.

To solve the looping problem, the IEEE specification requires that bridges use the spanning tree algorithm to create a loopless topology.

Spanning Tree:

In graph theory, a **spanning tree** is a graph in which there is no loop. In a bridged LAN, this means creating a topology in which each LAN can be reached from any other LAN through one path only (no loop). We cannot change the physical topology of the system because of physical connections between cables and bridges, but we can create a logical topology that overlays the physical one. Figure 15.8 shows a system with four LANs and five bridges. We have shown the physical system and its representation in graph theory. Although some textbooks represent the LANs as nodes and

the bridges as the connecting arcs, we have shown both LANs and bridges as nodes. The connecting arcs show the connection of a LAN to a bridge and vice versa. To find the spanning tree, we need to assign a cost (metric) to each arc. The interpretation of the cost is left up to the systems administrator. It may be the path with minimum hops (nodes), the path with minimum delay, or the path with maximum bandwidth. If two ports have the same shortest value, the systems administrator just chooses one. We have chosen the minimum hops. However, as we will see in Chapter 22, the hop count is normally 1 from a bridge to the LAN and 0 in the reverse direction.

The process to find the spanning tree involves three steps:

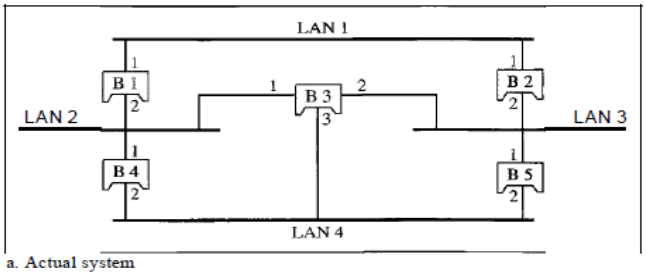
1. Every bridge has a built-in ID (normally the serial number, which is unique). Each bridge broadcasts this ID so that all bridges know which one has the smallest ID. The bridge with the smallest ID is selected as the *root* bridge (root of the tree). We assume that bridge B1 has the smallest ID. It is, therefore, selected as the root bridge.

2. The algorithm tries to find the shortest path (a path with the shortest cost) from the root bridge to every other bridge or LAN. The shortest path can be found by examining the total cost from the root bridge to the destination. Figure 15.9 shows the shortest paths.

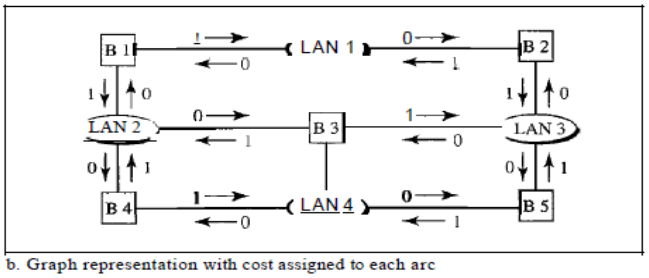
3. The combination of the shortest paths creates the shortest tree, which is also shown in Figure 15.9.

4. Based on the spanning tree, we mark the ports that are part of the spanning tree, the forwarding ports, which forward a frame that the bridge receives. We also mark those ports that are not part of the spanning tree, the blocking ports, which block the frames received by the bridge. Figure 15.10 shows the physical systems of LANs with forwarding points (solid lines) and blocking ports (broken lines).

Figure 15.8 *A system of connected LANs and its graph representation*



a. Actual system

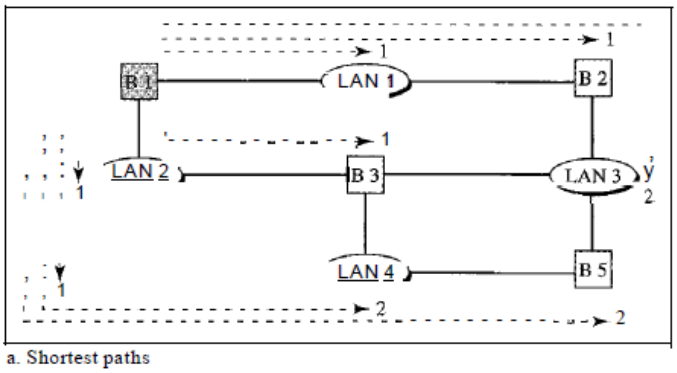


b. Graph representation with cost assigned to each arc

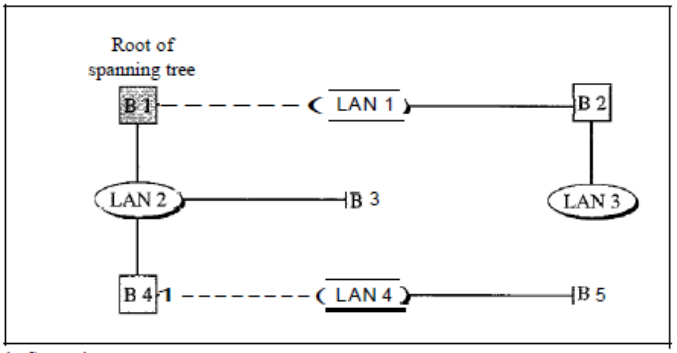
Note that there is only one single path from any LAN to any other LAN in the spanning tree system. This means there is only one single path from one LAN to any other LAN. No loops are created. You can prove to yourself that there is only one path from LAN 1 to LAN 2, LAN 3, or LAN 4. Similarly, there is only one path from LAN 2 to LAN 1, LAN 3, and LAN 4. The same is true for LAN 3 and LAN 4.

Dynamic Algorithm We have described the spanning tree algorithm as though it required manual entries. This is not true. Each bridge is equipped with a software package that carries out this process dynamically. The bridges send special messages to one another, called bridge protocol data units (BPDUs), to update the spanning tree. The spanning tree is updated when there is a change in the system such as a failure of a bridge or an addition or deletion of bridges.

Figure 15.9 *Finding the shortest paths and the spanning tree in a system of bridges*

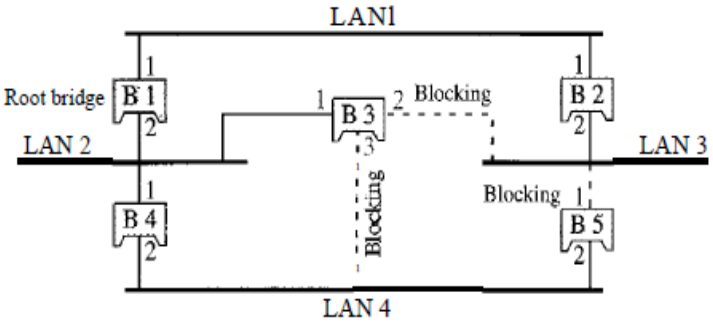


a. Shortest paths



b. Spanning tree

Figure 15.10 *Forwarding and blocking ports after using spanning tree algorithm*



Ports 2 and 3 of bridge B3 are blocking ports (no frame is sent out of these ports).
Port 1 of bridge B5 is also a blocking port (no frame is sent out of this port).

Source Routing Bridges

Another way to prevent loops in a system with redundant bridges is to use source **routing** bridges. A transparent bridge's duties include filtering frames, forwarding, and blocking. In a system that has source routing bridges, these duties are performed by the source station and, to some extent, the destination station.

In source routing, a sending station defines the bridges that the frame must visit. The addresses of these bridges are included in the frame. In other words, the frame contains not only the source and destination addresses, but also the addresses of all bridges to be visited.

The source gets these bridge addresses through the exchange of special frames with the destination prior to sending the data frame.

Source routing bridges were designed by IEEE to be used with Token Ring LANs. These LANs are not very common today.

Bridges Connecting Different LANs:

Theoretically a bridge should be able to connect LANs using different protocols at the data link layer, such as an Ethernet LAN to a wireless LAN. However, there are many issues to be considered:

O Frame format. Each LAN type has its own frame format (compare an Ethernet frame with a wireless LAN frame).

D Maximum data size. If an incoming frame's size is too large for the destination LAN, the data must be fragmented into several frames. The data then need to be reassembled at the destination. However, no protocol at the data link layer allows the fragmentation and reassembly of frames. We will see in Chapter 19 that this is allowed in the network layer. The bridge must therefore discard any frames too large for its system.

O Data rate. Each LAN type has its own data rate. (Compare the 10-Mbps data rate of an Ethernet with the I-Mbps data rate of a wireless LAN.) The bridge must buffer the frame to compensate for this difference.

D Bit order. Each LAN type has its own strategy in the sending of bits. Some send the most significant bit in a byte first; others send the least significant bit first.

O Security. Some LANs, such as wireless LANs, implement security measures in the data link layer. Other LANs, such as Ethernet, do not. Security often involves encryption (see Chapter 30). When a bridge receives a frame from a wireless LAN, it needs to decrypt the message before forwarding it to an Ethernet LAN.

D **Multimedia support.** Some LANs support multimedia and the quality of services needed for this type of communication; others do not.