CHAPTER 12

Local Area Networks

A **local area network (LAN)** is a data communication system that allows a number of independent devices to communicate directly with each other in a limited geographic area.

LANs are dominated by four architectures: Ethernet, Token Bus, Token Ring, and fiber distributed data interface (FDDI). Ethernet, Token Bus, and Token Ring are standards of the IEEE and are part of its Project 802; FDDI is an ANSI standard.

The data link control portion of the LAN protocols in use today are all based on HDLC. However, each protocol has adapted HDLC to fit the specific requirements of its own technology. (For example, ring technology has different needs than star technology, as we will see later in this chapter.) Differences in the protocols are necessary to handle the differing needs of the designs.

12.1 PROJECT 802

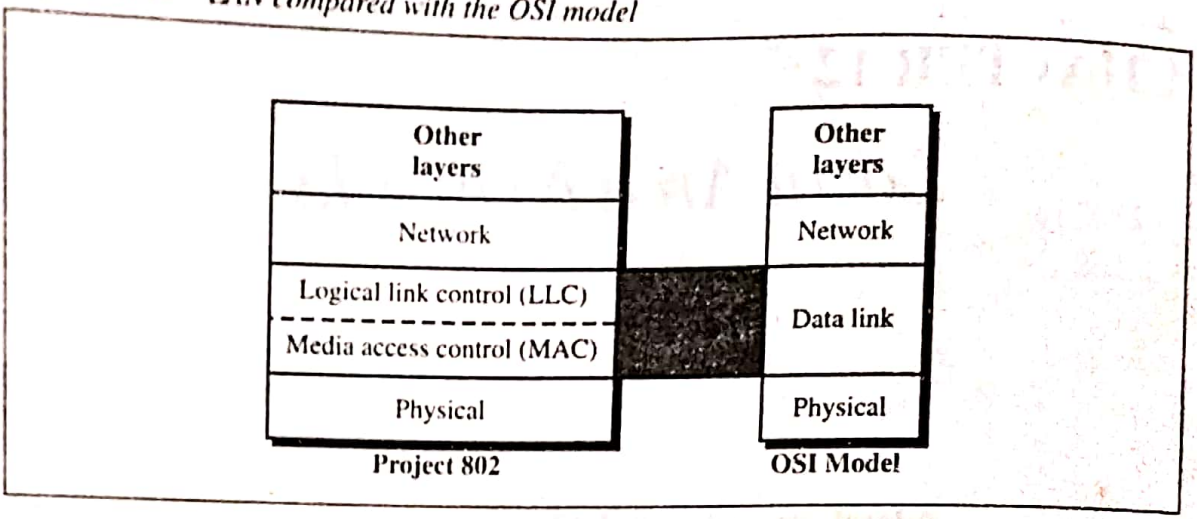
In 1985, the Computer Society of the IEEE started a project, called **Project 802,** to set standards to enable intercommunication between equipment from a variety of manufacturers. Project 802 does not seek to replace any part of the OSI model. Instead, it is a way of specifying functions of the physical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

> In 1985, the Computer Society of the IEEE developed Project 802. It covers the first two layers of the OSI model and part of the third level.

The relationship of **IEEE Project 802** to the OSI model is shown in Figure 12.1. The IEEE has subdivided the data link layer into two sublayers: **logical link control (LLC)** and **medium access control (MAC).**

The LLC is non-architecture-specific; that is, it is the same for all IEEE-defined LANs. The MAC sublayer, on the other hand, contains a number of distinct modules; each carries proprietary information specific to the LAN product being used.

Figure 12.1 *LAN compared with the OSI model*

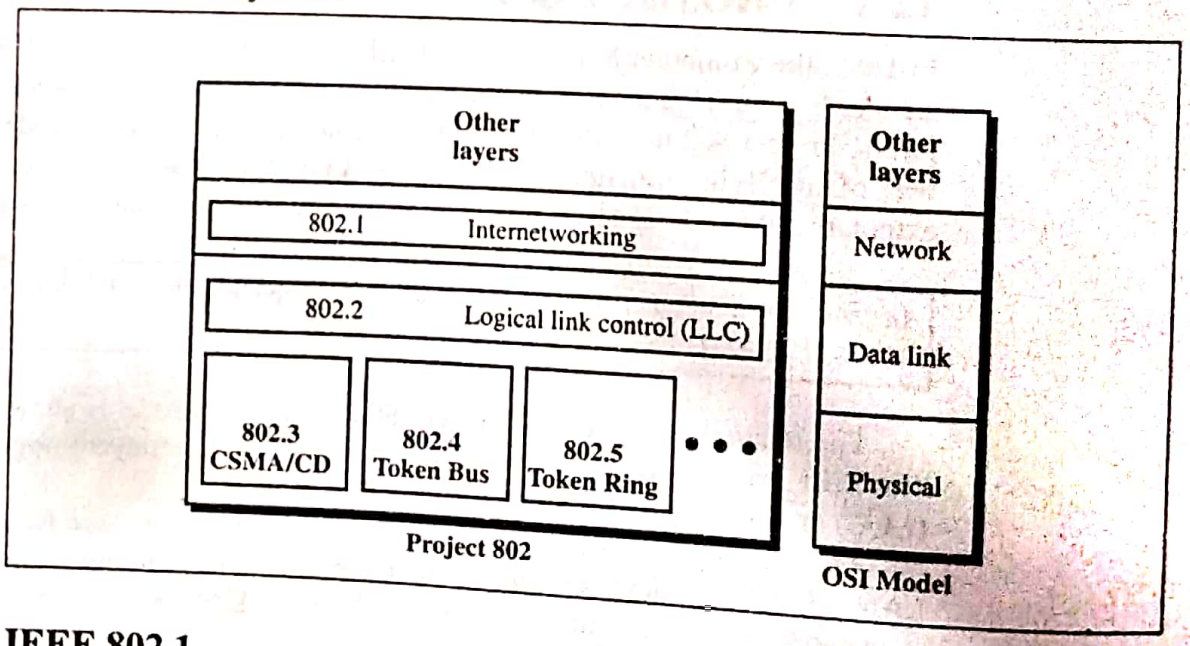


Project 802 has split the data link layer into two different sublayers: logical link control (LLC) and media access control (MAC).

In addition to the two sublayers, Project 802 contains a section governing **internetworking.** This section assures the compatibility of different LANs and MANs across protocols and allows data to be exchanged across otherwise incompatible networks.

The strength of Project 802 is modularity. By subdividing the functions necessary for LAN management, the designers were able to standardize those that can be generalized and to isolate those that must remain specific. Each subdivision is identified by a number: 802.1 (internetworking); 802.2 (LLC); and the MAC modules 802.3 (CSMA/CD), 802.4 (Token Bus), 802.5 (Token Ring), and others (see Figure 12.2).

Figure 12.2 *Project 802*



IEEE 802.1

IEEE 802.1 is the section of Project 802 devoted to internetworking issues in LANs and MANs. Although not yet complete, it seeks to resolve the incompatibilities

between network architectures without requiring modifications in existing addressing, access, and error recovery mechanisms, among others. Some of these issues will be discussed in Chapter 21.

IEEE 802.1 is an internetworking standard for LANs.

LLC

In general, the IEEE Project 802 model takes the structure of an HDLC frame and divides it into two sets of functions. One set contains the end-user portions of the frame: the logical addresses, control information, and data. These functions are handled by the **IEEE 802.2** logical link control (LLC) protocol. LLC is considered the upper layer of the IEEE 802 data link layer and is common to all LAN protocols.

IEEE 802.2 logical link control (LLC) is the upper sublayer of the data link layer.

MAC

The second set of functions, the medium access control (MAC) sublayer, resolves the **contention** for the shared media. It contains the synchronization, flag, flow, and error control specifications necessary to move information from one place to another, as well as the physical address of the next station to receive and route a packet. MAC protocols are specific to the LAN using them (Ethernet, Token Ring, and Token Bus, etc.).

Media access control (MAC) is the lower sublayer of the data link layer.

Protocol Data Unit (PDU)

The data unit in the LLC level is called the **protocol data unit (PDU).** The PDU contains four fields familiar from HDLC: a destination service access point (DSAP), a source service access point (SSAP), a control field, and an information field (see Figure 12.3).

DSAP and SSAP

The DSAP and SSAP are addresses used by the LLC to identify the protocol stacks on the receiving and sending machines that are generating and using the data. The first bit of the DSAP indicates whether the frame is intended for an individual or a group. The first bit of the SSAP indicates whether the communication is a command or response PDU (see Figure 12.3).

Control

The control field of the PDU is identical to the control field in HDLC. As in HDLC, PDU frames can be I-frames, S-frames, or U-frames and carry all of the codes and information that the corresponding HDLC frames carry (see Figure 12.4).

Figure 12.3 *PDU format*

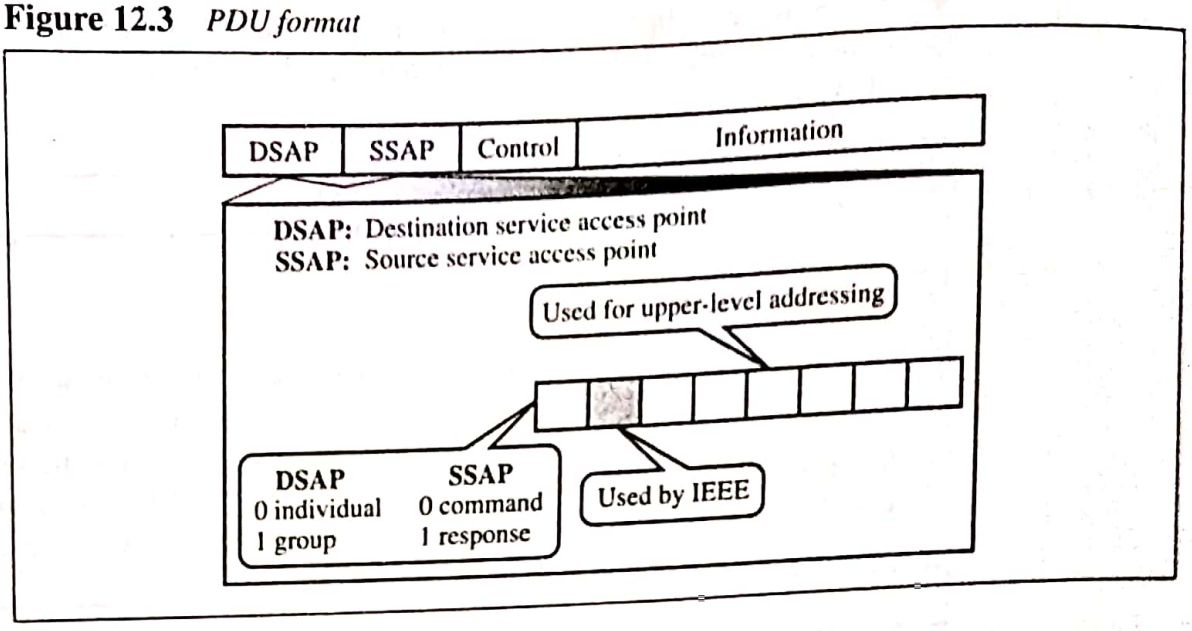
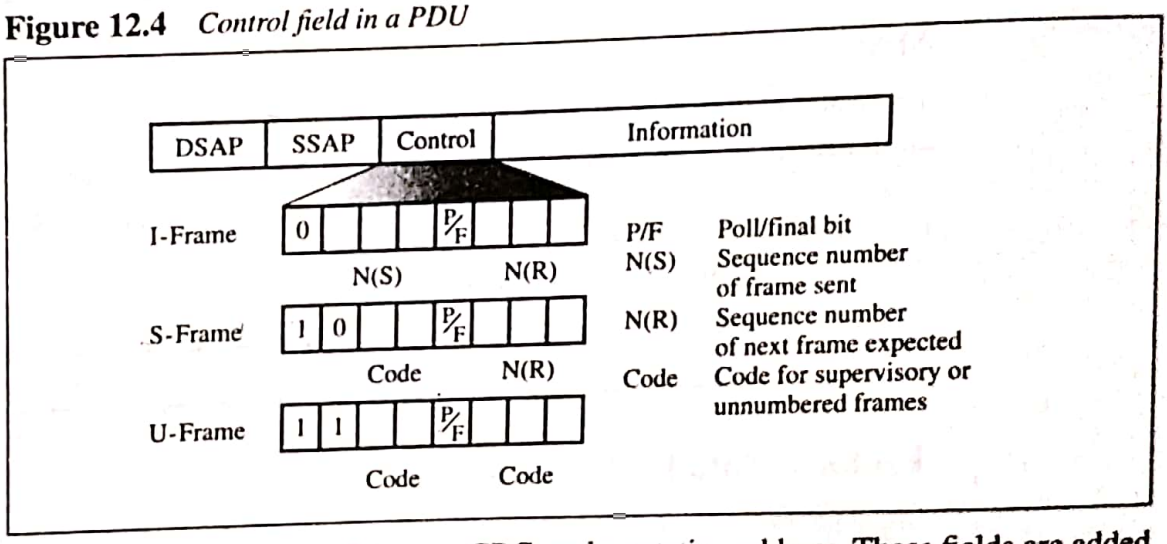


Figure 12.4 *Control field in a PDU*



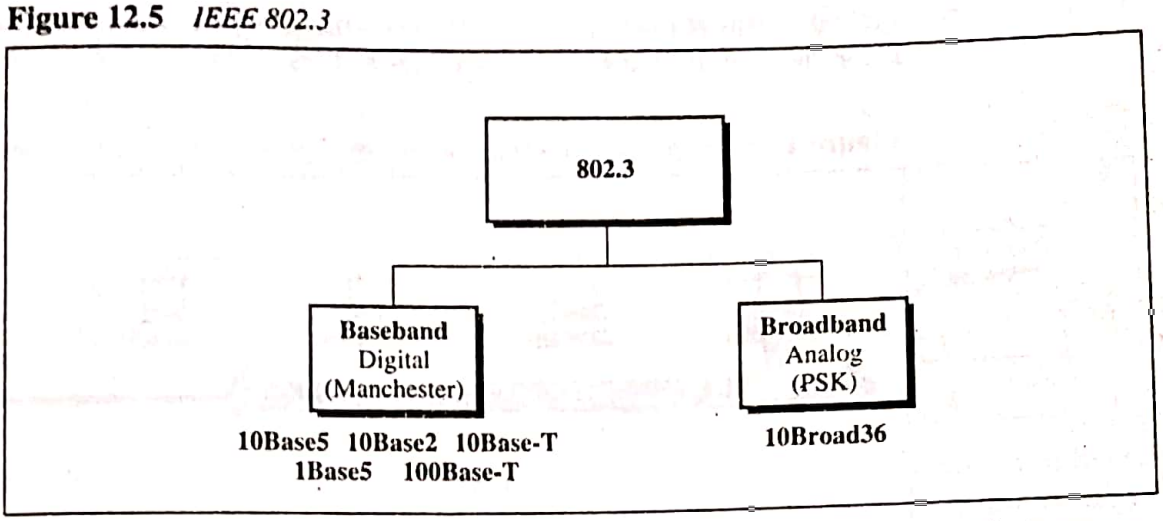
The PDU has no flag fields, no CRC, and no station address. These fields are added in the lower sublayer (the MAC layer).

12.2 ETHERNET

IEEE 802.3 supports a LAN standard originally developed by **Xerox** and later extended by a joint venture between Digital Equipment Corporation, Intel Corporation, and Xerox. This was called **Ethernet.**

IEEE 802.3 defines two categories: **baseband** and **broadband,** as shown in Figure 12.5. The word *base* specifies a digital signal (in this case, Manchester encoding). The word *broad* specifies an analog signal (in this case, PSK encoding). IEEE divides the baseband category into five different standards: **10Base5, 10Base2, 10Base-T, 1Base5,** and **100Base-T.** The first number (10, 1, or 100) indicates the data rate in Mbps. The last number or letter (5, 2, 1, or T) indicates the maximum cable length or the type of cable. IEEE defines only one specification for the broadband

Figure 12.5 *IEEE 802.3*



category: 10Broad36. Again, the first number (10) indicates the data rate. The last number defines the maximum cable length. However, the maximum cable length restriction can be changed using networking devices such as repeaters or bridges (see Chapter 21).

Access Method: CSMA/CD

Whenever multiple users have unregulated access to a single line, there is a danger of signals overlapping and destroying each other. Such overlaps, which turn the signals into unusable noise, are called **collisions.** As traffic increases on a multiple-access link, so do collisions. A LAN therefore needs a mechanism to coordinate traffic, minimize the number of collisions that occur, and maximize the number of frames that are delivered successfully. The access mechanism used in an Ethernet is called **carrier sense multiple access with collision detection (CSMA/CD,** standardized in IEEE 802.3).

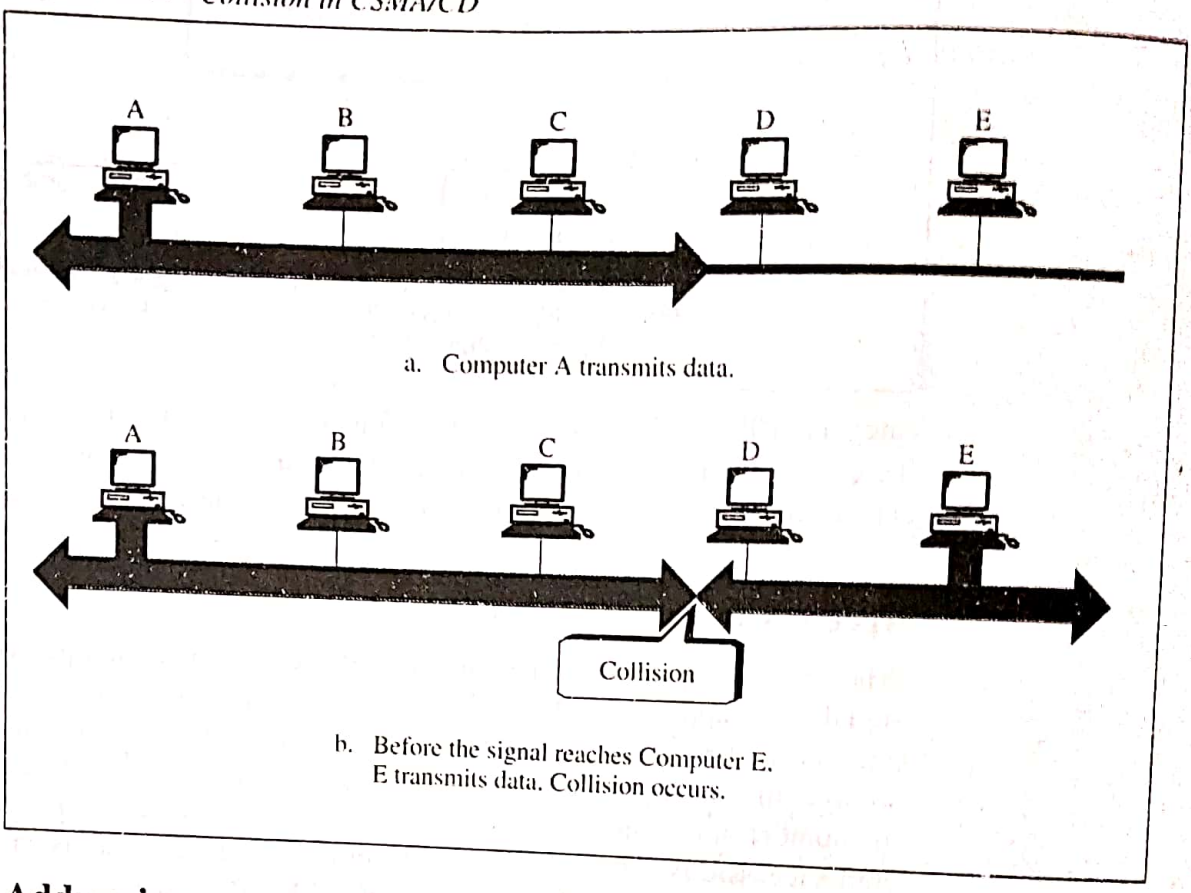
CSMA/CD is the result of an evolution from **multiple access (MA)** to **carrier sense multiple access (CSMA),** and, finally, to carrier sense multiple access with collision detection (CSMA/CD). The original design was a multiple access method in which every workstation had equal access to a link. In MA, there was no provision for traffic coordination. Access to the line was open to any node at any time, with the assumption that the odds of two devices competing for access at the same time were small enough to be unimportant. Any station wishing to transmit did so, then relied on acknowledgments to verify that the transmitted frame had not been destroyed by other traffic on the line.

In a CSMA system, any workstation wishing to transmit must first listen for existing traffic on the line. A device listens by checking for a voltage. If no voltage is detected, the line is considered idle and the transmission is initiated. CSMA cuts down on the number of collisions but does not eliminate them. Collisions can still occur. If another station has transmitted too recently for its signal to have reached the listening station, the listener assumes the line is idle and introduces its own signal onto the line.

The final step is the addition of collision detection (CD). In CSMA/CD the station wishing to transmit first listens to make certain the link is free, then transmits its data, then listens again. During the data transmission, the station checks the line for the extremely high voltages that indicate a collision. If a collision is detected, the station

quits the current transmission and waits a predetermined amount of time for the line to clear, then sends its data again (see Figure 12.6).

Figure 12.6 *Collision in CSMA/CD*



Addressing

Each station on an Ethernet network (such as a PC, workstation, or printer) has its own **network interface card (NIC).** The NIC usually fits inside the station and provides the station with a six-byte physical address. The number on the NIC is unique.

Electrical Specification

Signaling

The baseband systems use Manchester digital encoding (see Chapter 5). There is one broadband system, 10Broad36. It uses digital/analog conversion (differential PSK).

Data Rate

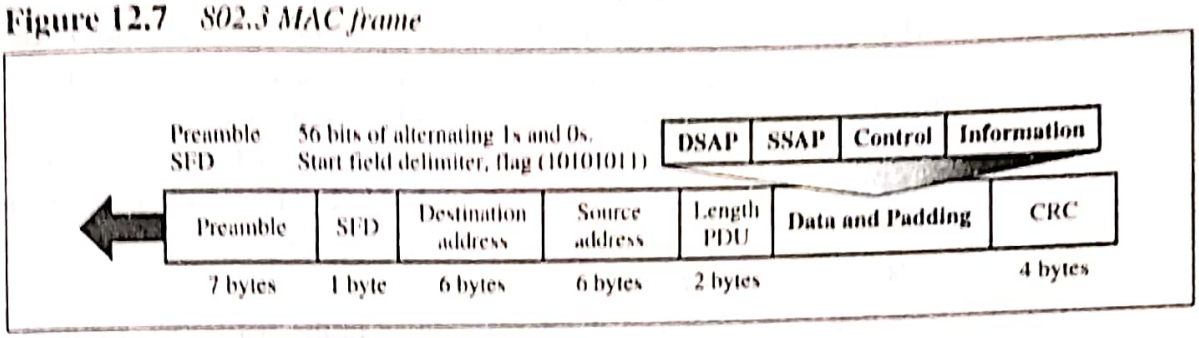
Ethernet LANs can support data rates between 1 and 100 Mbps.

Frame Format

IEEE 802.3 specifies one type of frame containing seven fields: preamble, SFD, DA, SA, length/type of PDU, 802.2 frame, and the CRC. Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreli-

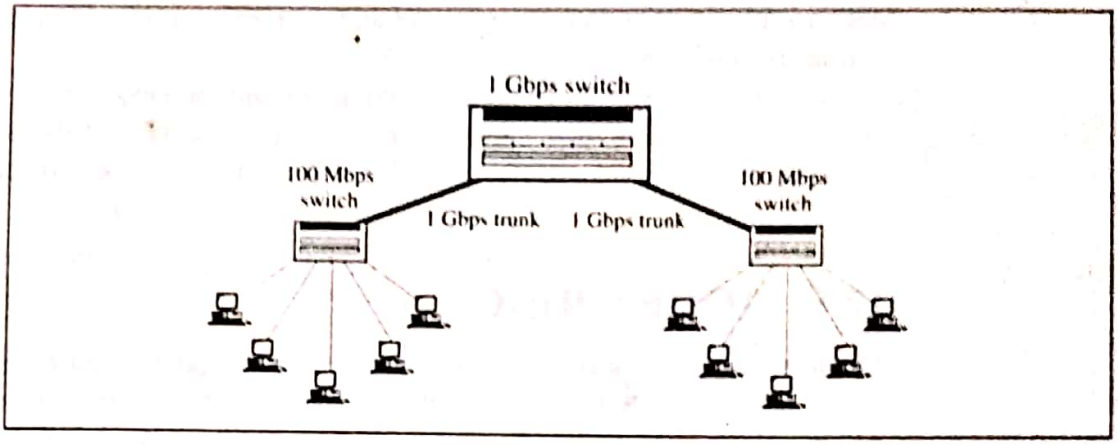
able medium. Acknowledgments must be implemented at the higher layers. The format of the MAC frame in CSMA/CD is shown in Figure 12.7.

Figure 12.7 *802.3 MAC frame*



- **Preamble.** The first field of the 802.3 frame, the **preamble,** contains seven bytes (56 bits) of alternating 0s and 1s that alert the receiving system to the coming frame and enable it to synchronize its input timing. The pattern 1010101 provides only an alert and a timing pulse; it can be too easily aliased to be useful in indicating the beginning of the data stream. HDLC combined the alert, timing, and start synchronization into a single field: the flag. IEEE 802.3 divides these three functions between the preamble and the second field, the **start frame delimiter (SFD).**
- **Start frame delimiter (SFD).** The second field (one byte: 10101011) of the 802.3 frame signals the beginning of the frame. The SFD tells the receiver that everything that follows is data, starting with the addresses.
- **Destination address (DA).** The **destination address (DA)** field is allotted six bytes and contains the physical address of the packet's next destination. A system's physical address is a bit pattern encoded on its network interface card (NIC). Each NIC has a unique address that distinguishes it from any other NIC. If the packet must cross from one LAN to another to reach its destination, the DA field contains the physical address of the router connecting the current LAN to the next one. When the packet reaches the target network, the DA field contains the physical address of the destination device.
- **Source address (SA).** The **source address (SA)** field is also allotted six bytes and contains the physical address of the last device to forward the packet. That device can be the sending station or the most recent router to receive and forward the packet.
- **Length/type of PDU.** These next two bytes indicate the number of bytes in the coming PDU. If the length of the PDU is fixed, this field can be used to indicate type, or as a base for other protocols. For example, Novell and the Internet use it to identify the network layer protocol that is using the PDU.
- **802.2 frame (PDU).** This field of the 802.3 frame contains the entire 802.2 frame as a modular, removable unit. The PDU can be anywhere from 46 to 1500 bytes long, depending on the type of frame and the length of the information field. The PDU is generated by the upper (LLC) sublayer, then linked to the 802.3 frame.
- **CRC.** The last field in the 802.3 frame contains the error detection information, in this case a CRC-32.

Figure 12.20 *Use of Gigabit Ethernet*



Four implementations have been designed for Gigabit Ethernet: 1000Base-LX, 1000Base-SX, 1000Base-CX, and 1000Base-T. The encoding is 8B/10B, which means a group of 8 binary bits are encoded into a group of 10 binary bits. Table 12.1 shows the features of the four implementations.

Table 12.1 *Comparison between the Gigabit Ethernet implementations*

Feature	1000Base-SX	1000Base-LX	1000Base-CX	1000Base-T
Medium	Optical fiber (multimode)	Optical fiber (multi- or single-mode)	STP	UTP
Signal	Short-wave laser	Long-wave laser	Electrical	Electrical
Max. distance	550 m	550 m (multimode) 5000 m (single mode)	25 m	25 m

12.4 TOKEN BUS

Local area networks have a direct application in factory automation and process control, where the nodes are computers controlling the manufacturing process. In this type of application, real-time processing with minimum delay is needed. Processing must occur at the same speed as the objects moving along the assembly line. Ethernet (IEEE 802.3) is not a suitable protocol for this purpose because the number of collisions is not predictable and the delay in sending data from the control center to the computers along the assembly line is not a fixed value. **Token Ring (IEEE 802.5;** see next section) is also not a suitable protocol because an assembly line resembles a bus topology and not a ring. **Token Bus (IEEE 802.4)** combines features of Ethernet and Token Ring. It combines the physical configuration of Ethernet (a bus topology) and the collision-free (predictable delay) feature of Token Ring. Token Bus is a physical bus that operates as a logical ring using **tokens.**

Stations are logically organized into a ring. A token is passed among stations. If a station wants to send data, it must wait and capture the token. However, like Ethernet, stations communicate via a common bus.

Token Bus is limited to factory automation and process control and has no commercial application in data communication. Also, the details of the operation are very involved. For these two reasons, we will not discuss this protocol further.

12.5 TOKEN RING

As mentioned previously, the network access mechanism used by Ethernet (CSMA/CD) is not infallible and may result in collisions. Stations may attempt to send data multiple times before a transmission makes it onto the link. This redundancy may create delays of indeterminable length if the traffic is heavy. There is no way to predict either the occurrence of collisions or the delays produced by multiple stations attempting to capture the link at the same time.

Token Ring resolves this uncertainty by requiring that stations take turns sending data. Each station may transmit only during its turn and may send only one frame during each turn. The mechanism that coordinates this rotation is called **token passing.** A token is a simple placeholder frame that is passed from station to station around the ring. A station may send data only when it has possession of the token.

> Token Ring allows each station to send one frame per turn.

Access Method: Token Passing

Token passing is illustrated in Figure 12.21. Whenever the network is unoccupied, it circulates a simple three-byte token. This token is passed from NIC to NIC in sequence until it encounters a station with data to send. That station waits for the token to enter its network board. If the token is free, the station may then send a data frame. It keeps the token and sets a bit inside its NIC as a reminder that it has done so, then sends its one data frame.

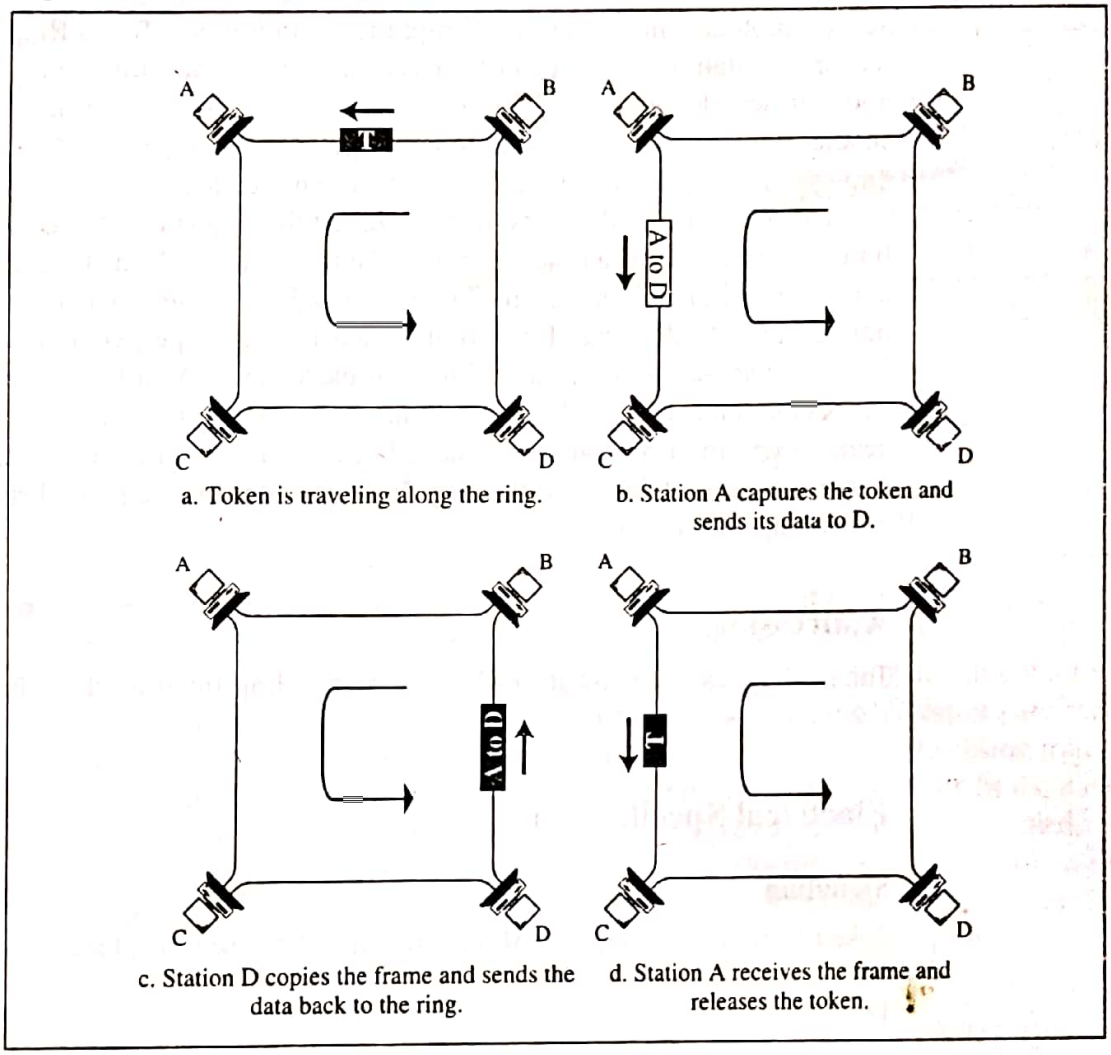
This data frame proceeds around the ring, being regenerated by each station. Each intermediate station examines the destination address, finds that the frame is addressed to another station, and relays it to its neighbor. The intended recipient recognizes its own address, copies the message, checks for errors, and changes four bits in the last byte of the frame to indicate address recognized and frame copied. The full packet then continues around the ring until it returns to the station that sent it.

The sender receives the frame and recognizes itself in the source address field. It then examines the address-recognized bits. If they are set, it knows the frame was received. The sender then discards the used data frame and releases the token back to the ring.

Priority and Reservation

Generally, once a token has been released, the next station on the ring with data to send has the right to take charge of the ring. However, in the IEEE 802.5 model, another

Figure 12.21 *Token passing*



option is possible. The busy token can be reserved by a station waiting to transmit, regardless of that station's location on the ring. Each station has a priority code. As a frame passes by, a station waiting to transmit may reserve the next open token by entering its priority code in the **access control (AC) field** of the token or data frame (discussed later in this section). A station with a higher priority may remove a lower priority reservation and replace it with its own. Among stations of equal priority, the process is first-come, first-served. Through this mechanism, the station holding the reservation gets the opportunity to transmit as soon as the token is free, whether or not it comes next physically on the ring.

Time Limits

To keep traffic moving, Token Ring imposes a time limit on any station wanting to use the ring. A starting delimiter (the first field of either a token or data frame) must reach each station within a specified interval (usually 10 milliseconds). In other words, each station expects to receive frames within regular time intervals (it receives a frame and expects to receive the next frame within a specified period).

Monitor Stations

Several problems may occur to disrupt the operation of a Token Ring network. In one scenario, a station may neglect to retransmit a token or a token may be destroyed by noise, in which case there is no token on the ring and no station may send data. In another scenario, a sending station may neglect to remove its used data frame from the ring or may not release the token once its turn has ended.

To handle these situations, one station on the ring is designated as a **monitor station.** The monitor sets a timer each time the token passes. If the token does not reappear in the allotted time, it is presumed to be lost and the monitor generates a new token and introduces it to the ring. The monitor guards against perpetually recirculating data frames by setting a bit in the AC field of each frame. As a frame passes, the monitor checks the status field. If the status bit has been set, it knows that the packet has already been around the ring and should have been discarded. The monitor then destroys the frame and puts a token onto the ring. If the monitor fails, a second station, designated as back-up, takes over.

Addressing

Token Ring uses a six-byte address, which is imprinted on the NIC card similar to Ethernet addresses.

Electrical Specification

Signaling

Token Ring uses differential Manchester encoding (see Chapter 5).

Data Rate

Token Ring supports data rates of up to 16 Mbps. (The original specification was 4 Mbps.)

Frame Formats

The Token Ring protocol specifies three types of frames: data/command, token, and **abort.** The token and abort frames are both truncated data/command frames (see Figure 12.22).

Data/Command Frame

In Token Ring, the data/command frame is the only one of the three types of frames that can carry a PDU and is the only one addressed to a specific destination rather than being available to the ring at large. This frame can carry either the user data or the management commands. The nine fields of the frame are start delimiter (SD), access control (AC), frame control (FC), destination address (DA), source address (SA), 802.2 PDU frame, CRC, end delimiter (ED), and frame status (FS).

Page No.
Date

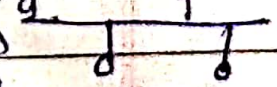
Project 802 (1985) Computer Society of the IEEE

To Set Standard to enable intercommunication b/w equipment from varity of manufact-urers. It covers the first two layers in OSI model & part of the third level

802.1	internetworking	Network layer
802.2	logical Link Control LLC	DLL
802.3	CSMA/CD	— Physical/DLL
802.4	Token Bus	— "
802.5	Token Ring	= "

MAC (Physical Address of the next Station to receive & route the packet)
└ using protocol (Ethernet, Token Ring, Token Bus)

Pure ALOHA :→ Random Access protocol
↳ (any time transmit the data) not sense the carrier
So Collision is possible

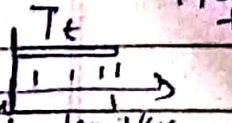


→ Acknowledgement: yes
↳ No Ack mean Collision
~~wait random~~ retransmission

→ LAN based!

→ Only transmission time consider, No propagation time

→ Vulnerable time = T_t no one can transmit the data otherwise Collision occurs



$V_t = 2 \times T_t$ $\quad T_t = \frac{m}{BW} = \frac{1000 \text{ bit}}{100 \text{ kbps}} = \frac{10 \text{ mil}}{\text{sec}}$

→ Efficiency η =

$$n = Gxe^{-2G}$$

Page No.
Date

No. of station who want to transmit the data

$$\frac{dn}{dG} = Gxe^{-2G}(-2) + e^{-2G}(1) = 0$$

$$e^{-2G}(-2G+1) = 0 \Rightarrow -2G+1 = 0$$

$$G = 1/2$$

Pure ALOHA

→ Any time transmission can be started

→ $VT = 2 \times T_t$

$n = Gxe^{-2G}$ put $G = 1/2$

→ 18.4% efficiency

Slotted ALOHA

Time slot

$T_t = \frac{m}{Bw}$

$VT = T_t$

$n = Gxe^{-G}$

$\frac{dn}{dG} = 0 \Rightarrow Gxe^{-G}(-1) + e^{-G}(1) = 0$

$\Rightarrow e^{-G}(-G+1) = 0$

$\Rightarrow -G+1 = 0$

$-G = -1$

$G = 1$

$n = 1xe^{-1} = \frac{1}{e} = \frac{1}{2.71} = .360 = 36.8\%$

MAC

DLL

→ Random

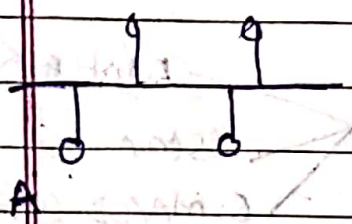
→ Control A

→ Channeli

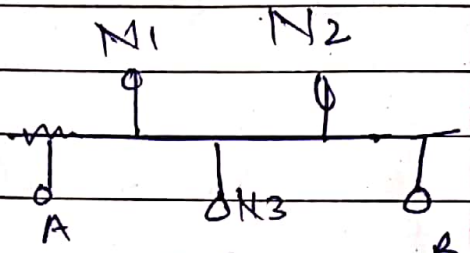
Bandwidth Wastage throughput low

Page No.
Date

CSMA ← 1-Persistant
0-Persistant
p-persistant



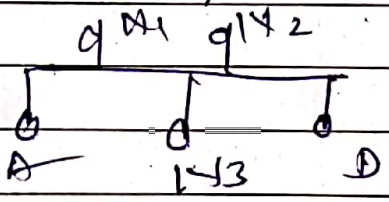
1- persistant :→



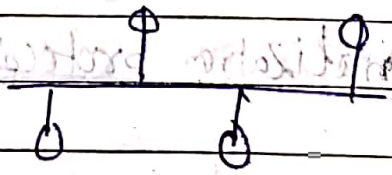
↳ Continuously checking sensing the channel signal. Ethernet

High Chances of collision occurs.

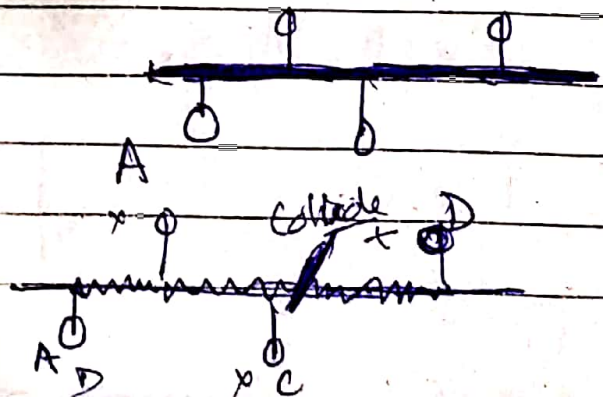
Zero
0- persistant (wait for random amount of time)



p- persistant (Hybrid Approach) (p) value probability wifi



CSMA/CD No ACK System Here.



How A Know his data was Collide