UNIT III

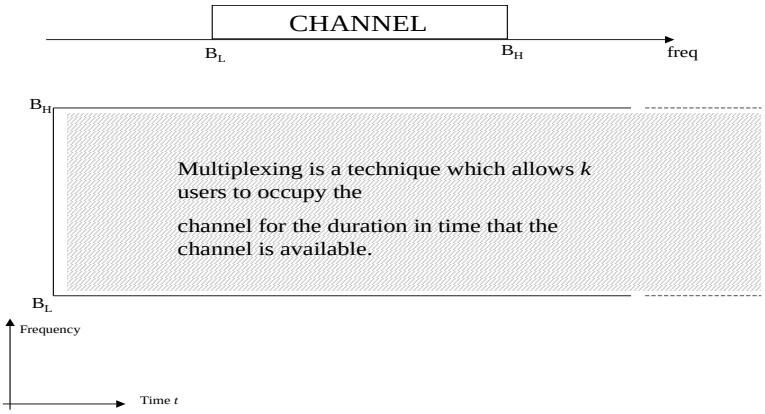
.

Multiplexing – Types of multiplexing – LAN – Project 802 – Ethernet – Token bus – Token ring – FDDI – MAN – IEEE 802.6 – Circuit switching – Packet switching

2.1 MULTIPLEXING

Multiplexing is the name given to techniques, which allow more than one message to be transferred via the same communication channel. The channel in this context could be a transmission line, *e.g.* a twisted pair or co-axial cable, a radio system or a fibre optic system *etc*.

A channel will offer a specified bandwidth, which is available for a time *t*, where *t* may $\rightarrow \infty$. Thus, with reference to the channel there are 2 'degrees of freedom', *i.e.* bandwidth or frequency and time.

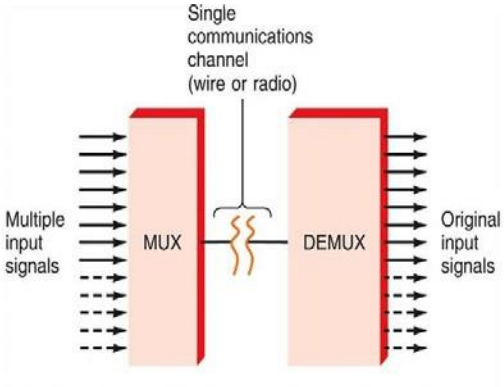


Now consider a signal $v_s(t) = Amp\cos(\omega t + \phi)$. The signal is characterised by amplitude, frequency, phase and time.

Various multiplexing methods are possible in terms of the channel bandwidth and time, and the signal, in particular the frequency, phase or time.

Concept of Multiplexing

- Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams.
- Communication is possible over the air (radio frequency), using a physical media (cable) and light (optical fiber). All mediums are capable of multiplexing.
- When more than one senders tries to send over single medium, a device called



Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium and identifies each and send to different receivers.

- Transmitting two or more signals simultaneously can be accomplished by running multiple cables or setting up one transmitter receiver pair for each channel , but this is an expensive approach.
  - A single cable or radio link can handle multiple signals simultaneously using a technique known as multiplexing.Multiplexing permits hundreds or even thousands of signals to be combined and transmitted over a single medium.
- A device called a multiplexer (often shortened to "mux") combines the input signals into one signal. When the multiplexed signal needs to be separated into its component signal s (for example, when your email is to be delivered to its destination), a device called a d emultiplexer (or "demux") is used.
  - Multiplexing was originally developed in the 1800s for telegraphy. Today, multiplexing is widely used in many telecommunications applications, including telephony, Internet com munications, digital broadcasting and wireless telephony.

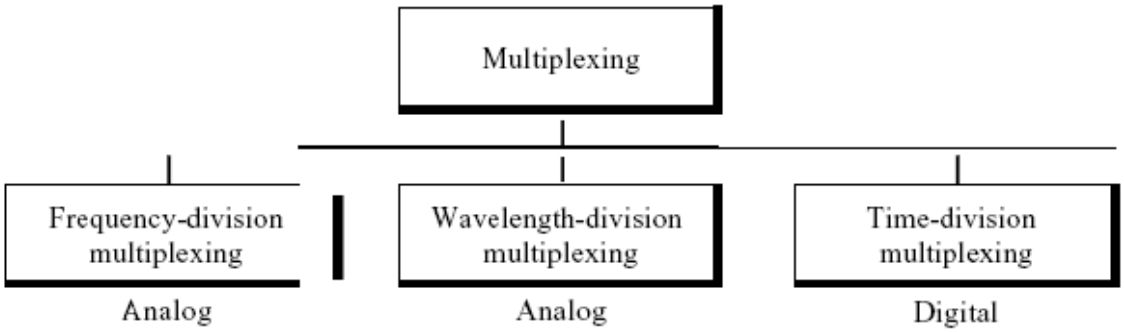


Figure *Categories of multiplexing*

1) <u>Frequency Division Multiplexing FDM</u>

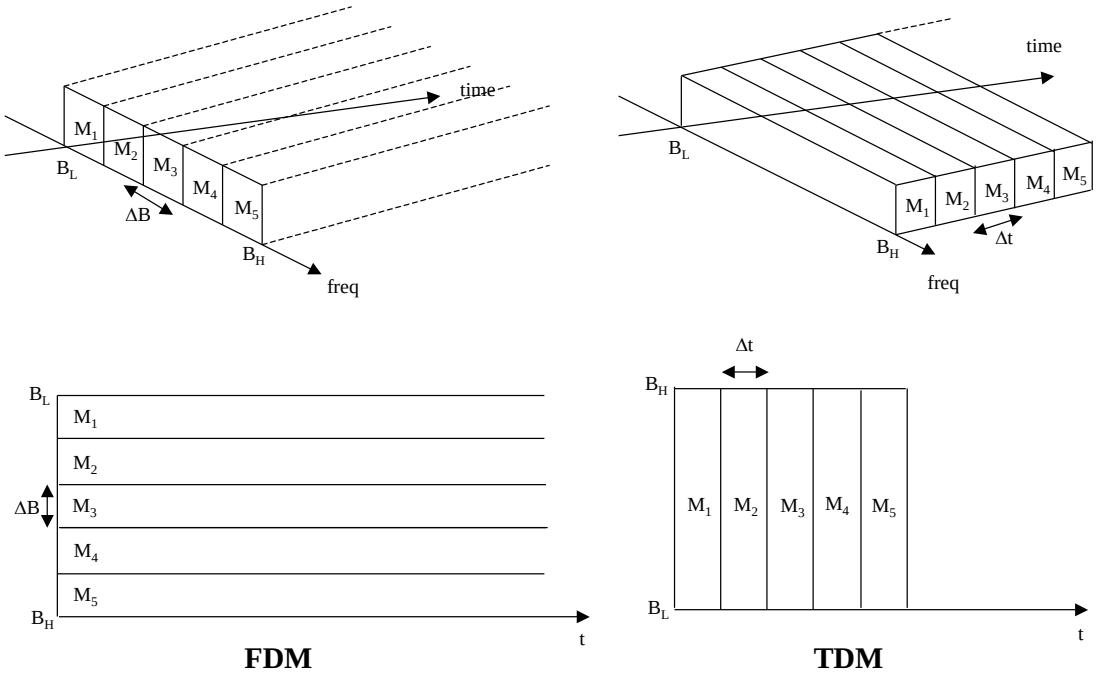
FDM is derived from AM techniques in which the signals occupy the same physical 'line' but in different frequency bands. Each signal occupies its own specific band of frequencies all the time, *i.e.* the messages share the channel **bandwidth**.

2) <u>Time Division Multiplexing TDM</u>

TDM is derived from sampling techniques in which messages occupy all the channel bandwidth but for short time intervals of time, *i.e.* the messages share the channel **time**.

- FDM – messages occupy **narrow** bandwidth – all the time.
- TDM – messages occupy **wide** bandwidth – for short intervals of time.

These two basic methods are illustrated below.



FDM **TDM**

Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

2.1.1 Frequency-Division Multiplexing

Frequency-division multiplexing (FDM) is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined bandwidths of the signals to be transmitted. In FOM, signals generated by each sending device modulate different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported by the link. Carrier frequencies are separated by sufficient bandwidth to accommodate the modulated signal. These bandwidth ranges are the channels through which the various signals travel. Channels can be separated by strips of unused bandwidth-guard bands-to prevent signals from overlapping. In addition, carrier frequencies must not interfere with the original data frequencies.

Figure 1 gives a conceptual view of FDM. In this illustration, the transmission path is divided into three parts, each representing a channel that carries one transmission.

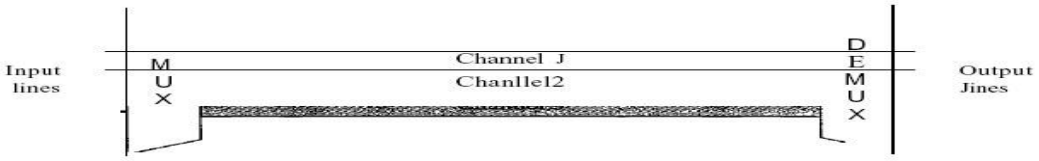


Fig: FDM

We consider FDM to be an analog multiplexing technique; however, this does not mean that FDM cannot be used to combine sources sending digital signals. A digital signal can be converted to an analog signal before FDM is used to multiplex them.

Multiplexing Process

Figure 2 is a conceptual illustration of the multiplexing process. Each source generates a signal of a similar frequency range. Inside the multiplexer, these similar signals modulates different carrier frequencies *(/1,12,* and *h).* The resulting modulated signals are then combined into a single composite signal that is sent out over a media link that has enough bandwidth to accommodate it.

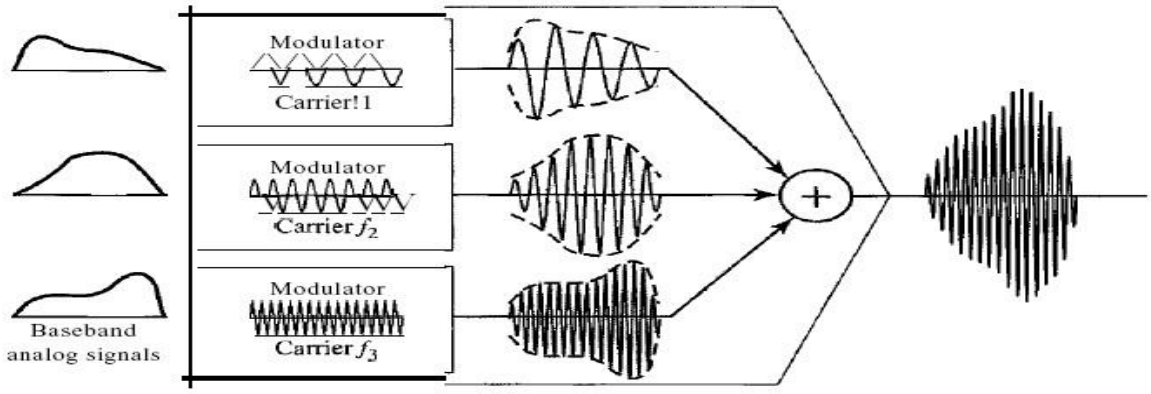


Figure 2 *FDM process*

Demultiplexing Process

The demultiplexer uses a series of filters to decompose the multiplexed signal into its constituent component signals. The individual signals are then passed to a demodulator that separates them from their carriers and passes them to the output lines. Figure 3 is a conceptual illustration of demultiplexing process.

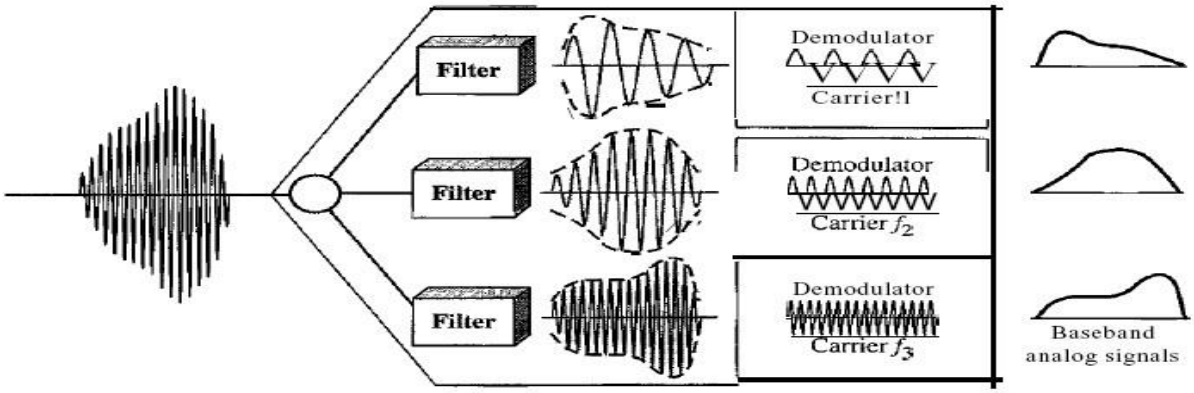
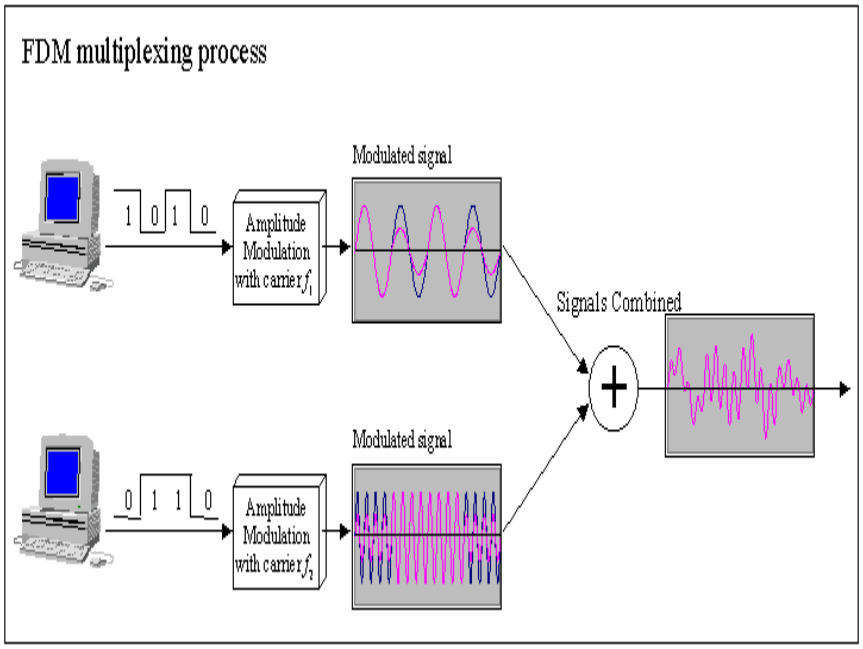


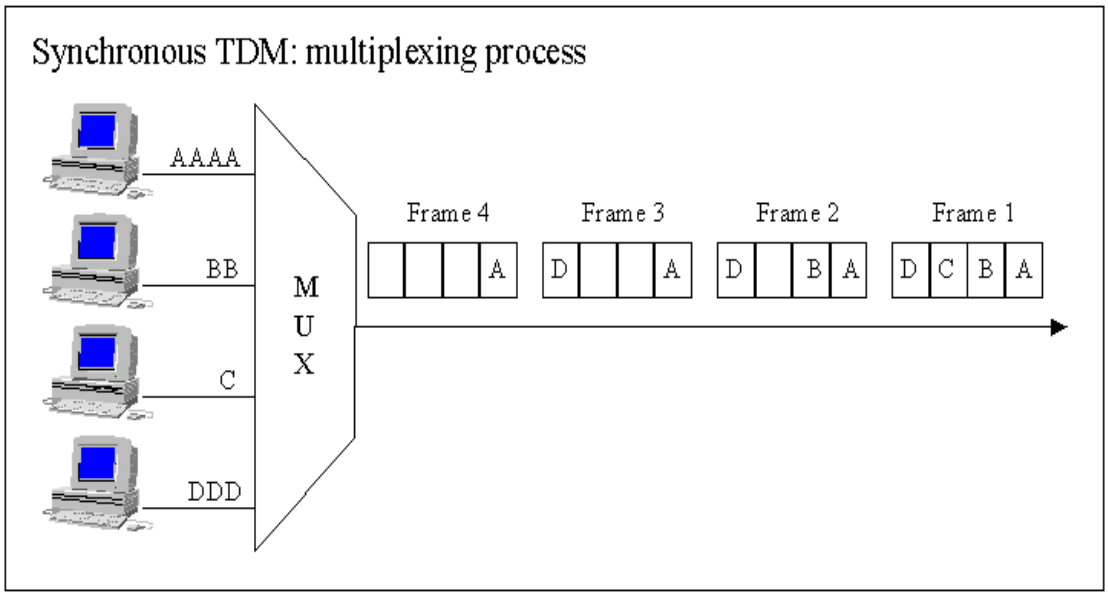
Figure 3 *FDM de-multiplexing example*



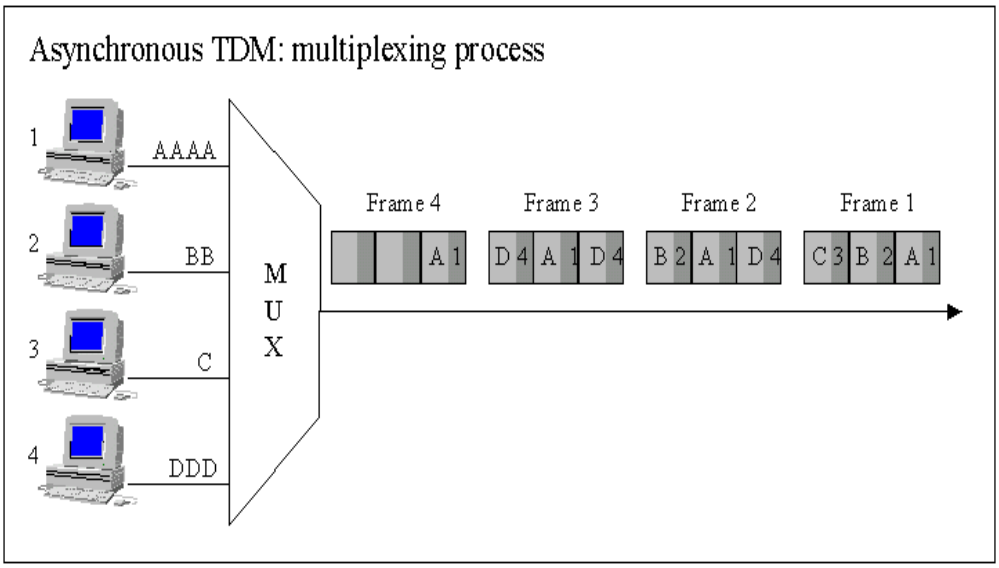
Time Division Multiplexing (TDM): This is possible when data transmission rate of the media is much higher than that of the data rate of the source. Multiple signals can be transmitted if

each signal is allowed to be transmitted for a definite amount of time. These time slots are so small that all transmissions appear to be in parallel.

1. **Synchronous TDM:** Time slots are preassigned and are fixed. Each source is given it's time slot at every turn due to it. This turn may be once per cycle, or several turns per cycle ,if it has a high data transfer rate, or may be once in a no. of cycles if it is slow. This slot is given even if the source is not ready with data. So this slot is transmitted empty.



2. **Asynchronous TDM**: In this method, slots are not fixed. They are allotted dynamically depending on speed of sources, and whether they are ready for transmission.



2.1.2 Wavelength-Division Multiplexing

Wavelength-division multiplexing (WDM) is designed to use the high-data-rate capability of fiber-optic cable. The optical fiber data rate is higher than the data rate of metallic transmission cable. Using a fiber-optic cable for one single line wastes the available bandwidth. Multiplexing allows us to combine several lines into one.

WDM is conceptually the same as FDM, except that the multiplexing and demultiplexing involve optical signals transmitted through fiber-optic channels. The idea is the same: We are combining different signals of different frequencies. The difference is that the frequencies are very high.

Figure 4 gives a conceptual view of a WDM multiplexer and demultiplexer. Very narrow bands of light from different sources are combined to make a wider band of light. At the receiver, the signals are separated by the demultiplexer.

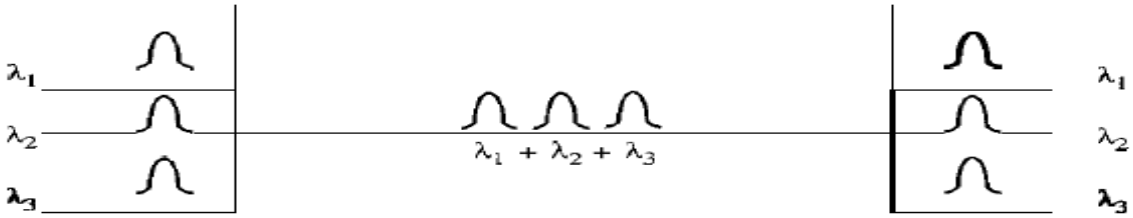


Figure 4 *Wavelength-division multiplexing*

Although WDM technology is very complex, the basic idea is very simple. We want to combine multiple light sources into one single light at the multiplexer and do the reverse at the demultiplexer. The combining and splitting of light sources are easily handled by a prism. Recall from basic physics that a prism bends a beam of light based on the angle of incidence and the frequency. Using this technique, a multiplexer can be made to combine several input beams of light, each containing a narrow band of frequencies, into one output beam of a wider band of frequencies. A demultiplexer can also be made to reverse the process. Figure 5 shows the concept.

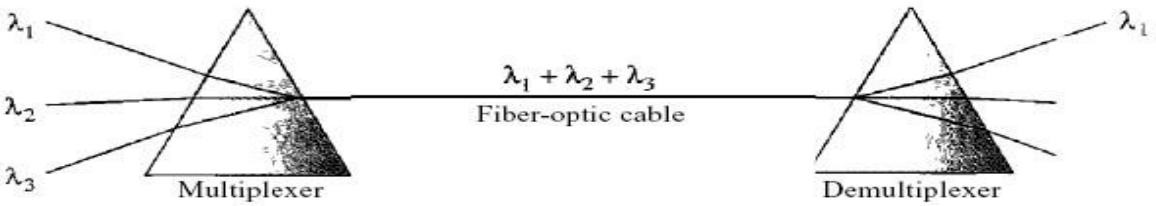


Figure 5 *Prisms in wavelength-division multiplexing and demultiplexing*

2.1.3 Synchronous Time-Division Multiplexing

Time-division multiplexing (TDM) is a digital process that allows several connections to share the high bandwidth of a linle Instead of sharing a portion of the bandwidth as in FDM, time is shared. Each connection occupies a portion of time in the link. Figure 6 gives a conceptual view of TDM. Note that the same link is used as in FDM; here, however, the link is shown sectioned by time rather than by frequency. In the figure, portions of signals 1,2,3, and 4 occupy the link sequentially.

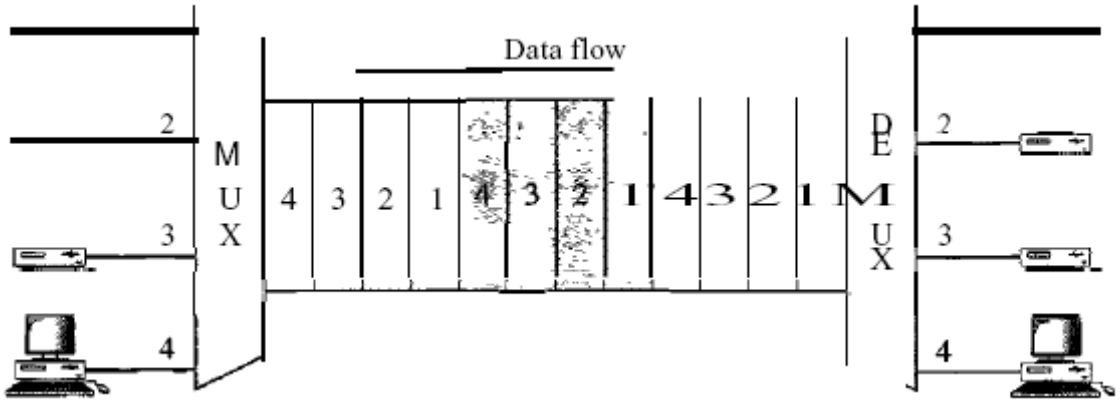


Figure 6 *TDM*

Note that in Figure 6 we are concerned with only multiplexing, not switching. This means that all the data in a message from source 1 always go to one specific destination, be it 1, 2, 3, or 4. The delivery is fixed and unvarying, unlike switching. We also need to remember thatTDM is, in principle, a digital multiplexing technique. Digital data from different sources are combined into one timeshared link. However, this does not mean that the sources cannot produce analog data; analog data can be sampled, changed to digital data, and then multiplexed by using TDM.

We can divide TDM into two different schemes: synchronous and statistical.

In synchronous TDM, each input connection has an allotment in the output even if it is not sending data.

Time Slots and Frames

In synchronous TDM, the data flow of each input connection is divided into units, where each input occupies one input time slot. A unit can be 1 bit, one character, or one block of data. Each input unit becomes one output unit and occupies one output time slot. However, the duration of an output time slot is *n* times shorter than the duration of an input time slot. If an input time slot is *T* s, the output time slot is *Tin* s, where *n* is the number of connections. In other words, a unit

in the output connection has a shorter duration; it travels faster. Figure 7 shows an example of synchronous TDM where *n* is 3.

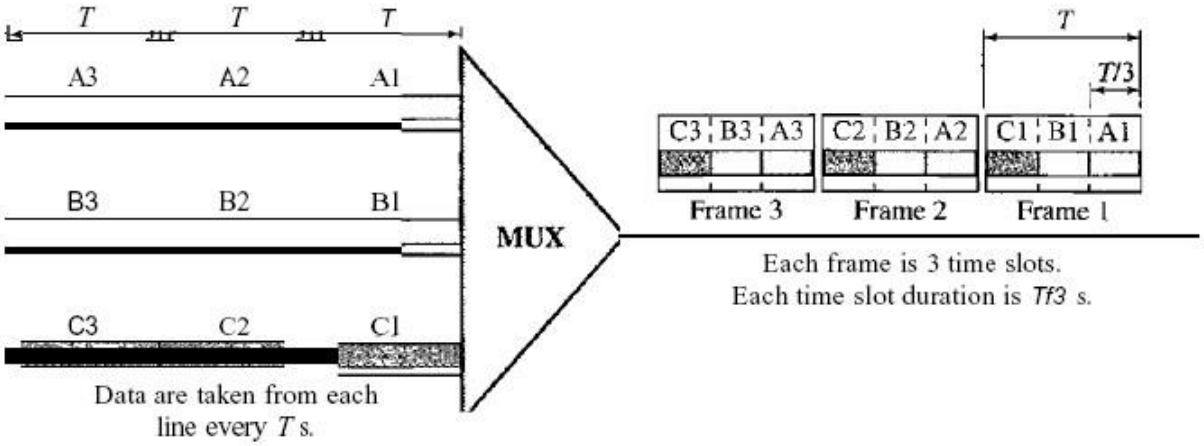


Figure 7 *Synchronous time-division multiplexing*

In synchronous TDM, a round of data units from each input connection is collected into a frame (we will see the reason for this shortly). If we have *n* connections, a frame is divided into *n* time slots and one slot is allocated for each unit, one for each input line. If the duration of the input unit is *T*, the duration of each slot is *Tin* and the duration of each frame is *T* (unless a frame carries some other information, as we will see shortly).

The data rate of the output link must be *n* times the data rate of a connection to guarantee the flow of data. In Figure 7, the data rate of the link is 3 times the data rate of a connection; likewise, the duration of a unit on a connection is 3 times that of the time slot (duration of a unit on the link). In the figure we represent the data prior to multiplexing as 3 times the size of the data after multiplexing. This is just to convey the idea that each unit is 3 times longer in duration before multiplexing than after. Time slots are grouped into frames. A frame consists of one complete cycle of time slots, with one slot dedicated to each sending device. In a system with *n* input lines, each frame has *n* slots, with each slot allocated to carrying data from a specific input line.

Interleaving

TDM can be visualized as two fast-rotating switches, one on the multiplexing side and the other on the demultiplexing side. The switches are synchronized and rotate at the same speed, but in opposite directions. On the multiplexing side, as the switch opens in front of a connection, that

connection has the opportunity to send a unit onto the path. This process is called **interleaving.** On the demultiplexing side, as the switch opens in front of a connection, that connection has the opportunity to receive a unit from the path.

Figure 8 shows the interleaving process for the connection shown in Figure 7.

In this figure, we assume that no switching is involved and that the data from the first connection at the multiplexer site go to the first connection at the demultiplexer

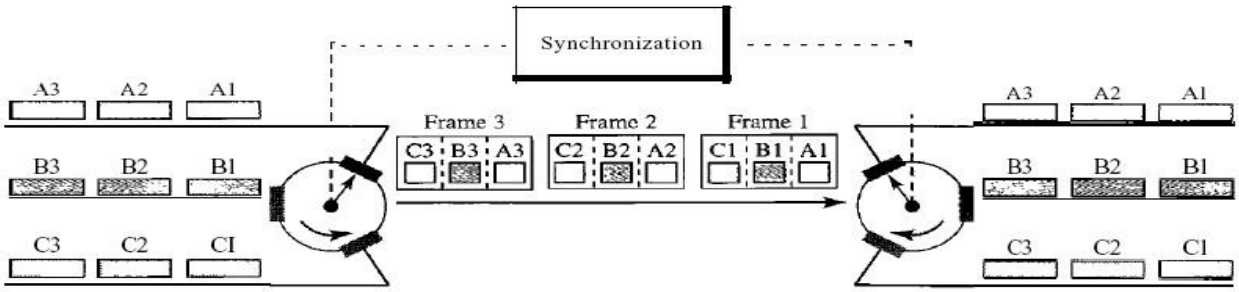


Figure 8 *Interleaving*

- *Empty Slots*
- *Data Rate Management*
    - ***Multilevel Multiplexing***
    - **Multiple-Slot Allocation**
    - **Pulse Stuffing**
- *Frame Synchronizing*
- *Digital Signal Service*

2.1.4 Statistical Time-Division Multiplexing

Addressing

Figure a also shows a major difference between slots in synchronous TDM and statistical TDM. An output slot in synchronous TDM is totally occupied by data; in statistical TDM, a slot needs to carry data as well as the address of the destination.

In synchronous TDM, there is no need for addressing; synchronization and preassigned relationships between the inputs and outputs serve as an address. We know, for example, that input 1 always goes to input 2. If the multiplexer and the demultiplexer are synchronized, this is guaranteed. In statistical multiplexing, there is no fixed relationship between the inputs and outputs because there are no preassigned or reserved slots. We need to include the address of the

receiver inside each slot to show where it is to be delivered. The addressing in its simplest form can be *n* bits to define *N* different output lines with *n* =10g2 *N.* For example, for eight different output lines, we need a 3-bit address.

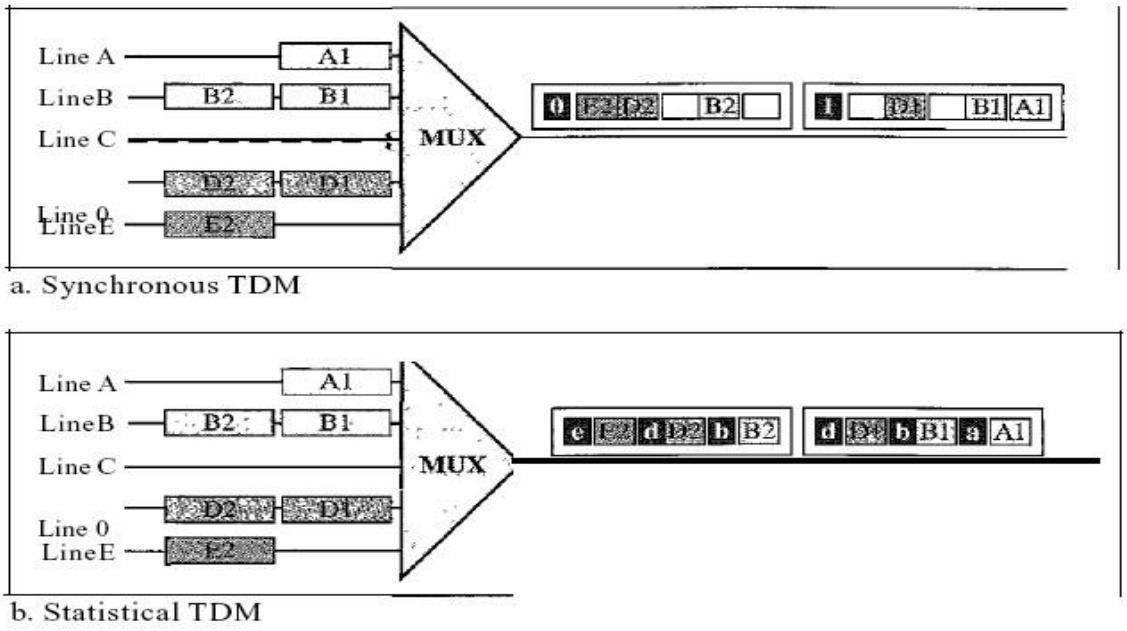


Figure a *TDM slot comparison*

Slot Size

Since a slot carries both data and an address in statistical TDM, the ratio of the data size to address size must be reasonable to make transmission efficient. For example, it would be inefficient to send 1 bit per slot as data when the address is 3 bits. This would mean an overhead of 300 percent. In statistical TDM, a block of data is usually many bytes while the address is just a few bytes.

No Synchronization Bit

There is another difference between synchronous and statistical TDM, but this time it is at the frame level. The frames in statistical TDM need not be synchronized, so we do not need synchronization bits.

Bandwidth

In statistical TDM, the capacity of the link is normally less than the sum of the capacities of each channel. The designers of statistical TDM define the capacity of the link based on the statistics of the load for each channel. If on average only *x* percent of the input slots are filled, the capacity of the link reflects this. Of course, during peak times, some slots need to wait.

Local Area Networks:

Local area networks, generally called LANs, are privately-owned networks within a single building or campus of up to a few kilometres in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information. LANs are distinguished from other kinds of networks by three characteristics:

(1) Their size,

(2) Their transmission technology, and

(3) Their topology.

LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance. Knowing this bound makes it possible to use certain kinds of designs that would not otherwise be possible. It also simplifies network management. LANs may use a transmission technology consisting of a cable to which all the machines are attached, like the telephone company party lines once used in rural areas. Traditional LANs run at speeds of 10 Mbps to 100 Mbps, have low delay (microseconds or nanoseconds), and make very few errors. Newer LANs operate at up to 10 Gbps Various topologies are possible for broadcast LANs. Figure1 shows two of them. In a bus (i.e., a linear cable) network, at any instant at most one machine is the master and is allowed to transmit. All other machines are required to refrain from sending. An arbitration mechanism is needed to resolve conflicts when two or more machines want to transmit simultaneously. The arbitration mechanism may be centralized or distributed. IEEE 802.3, popularly called Ethernet, for example, is a bus-based broadcast network with decentralized control, usually operating at 10 Mbps to 10 Gbps. Computers on an Ethernet can transmit whenever they want to; if two or more packets collide, each computer just waits a random time and tries again later.

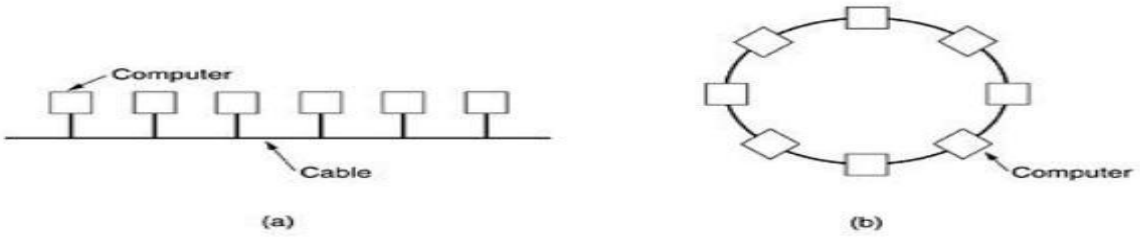
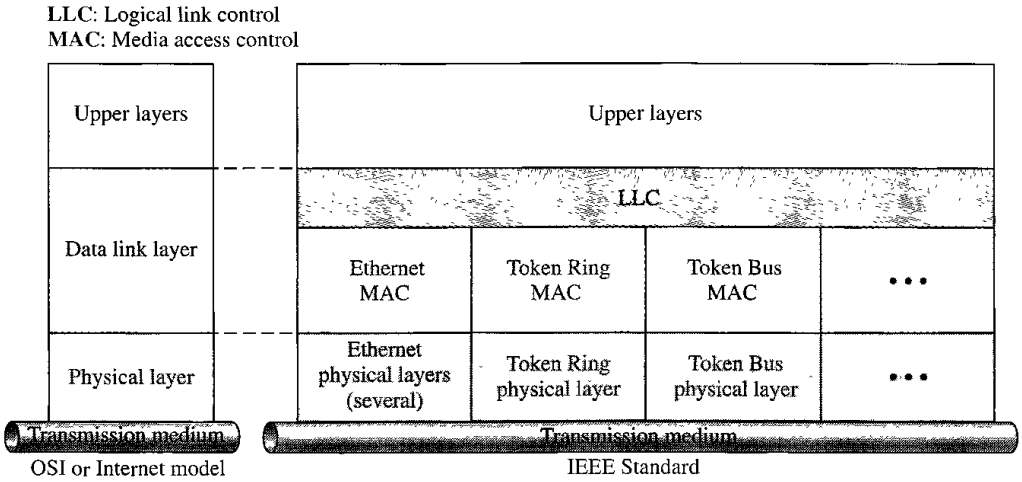


Fig.1: Two broadcast networks . (a) Bus. (b) Ring.

A second type of broadcast system is the ring. In a ring, each bit propagates around on its own, not waiting for the rest of the packet to which it belongs. Typically, each bit circumnavigates the entire ring in the time it takes to transmit a few bits, often before the complete packet has even been transmitted. As with all other broadcast systems, some rule is needed for arbitrating simultaneous accesses to the ring. Various methods, such as having the machines take turns, are in use. IEEE 802.5 (the IBM token ring), is a ring-based LAN operating at 4 and 16 Mbps. FDDI is another example of a ring network.

IEEE STANDARDS

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



Data Link Layer

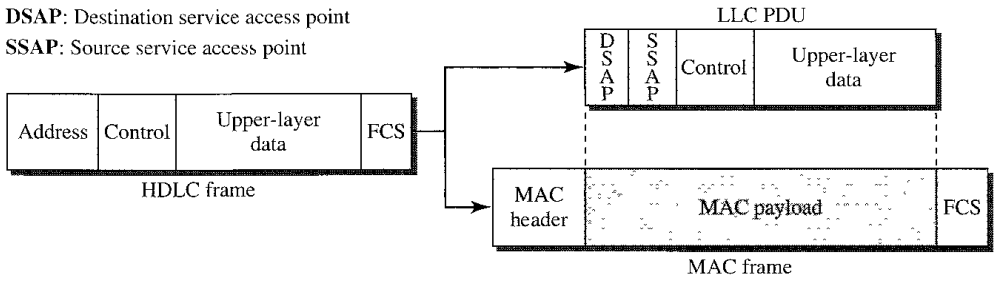
The data link layer in the IEEE standard is divided into two sublayers: LLC and MAC.

Logical Link Control (LLC)

In IEEE Project 802, flow control, error control, and part of the framing duties are collected into one sublayer called the logical link control. Framing is handled in both the LLC sublayer and the MAC sublayer.

The LLC provides one single data link control protocol for all IEEE LANs. In this way, the LLC is different from the media access control sublayer, which provides different protocols for different LANs. A single LLC protocol can provide interconnectivity between different LANs because it makes the MAC sublayer transparent.

Framing LLC defines a protocol data unit (PDU) that is somewhat similar to that of HDLC. The header contains a control field like the one in HDLC; this field is used for flow and error control. The two other header fields define the upper-layer protocol at the source and destination that uses LLC. These fields are called the destination service access point (DSAP) and the source service access point (SSAP). The other fields defined in a typical data link control protocol such as HDLC are moved to the MAC sublayer. In other words, a frame defined in HDLC is divided into a PDU at the LLC sublayer and a frame at the MAC sublayer, as shown in figure.



Need for LLC The purpose of the LLC is to provide flow and error control for the upper-layer protocols that actually demand these services. For example, if a LAN or several LANs are used in an isolated system, LLC may be needed to provide flow and error control for the application layer protocols. However, most upper-layer protocols such as IP, do not use the services of LLC.

Media Access Control (MAC)

IEEE Project 802 has created a sublayer called media access control that defines the specific access method for each LAN. For example, it defines CSMA/CD as the media access method for Ethernet LANs and the token-passing method for Token Ring and Token Bus LANs. Part of the framing function is also handled by the MAC layer.

In contrast to the LLC sublayer, the MAC sublayer contains a number of distinct modules; each defines the access method and the framing format specific to the

corresponding LAN protocol.

Physical Layer

The physical layer is dependent on the implementation and type of physical media used. IEEE defines detailed specifications for each LAN implementation. For example, although there

is only one MAC sublayer for Standard Ethernet, there is a different physical layer specification for each Ethernet implementations.

Key features of LANs are summarized below:

- Limited geographical area – which is usually less than 10 Km and more than 1 m.
- High Speed – 10 Mbps to 1000 Mbps (1 Gbps) and more
- High Reliability – 1 bit error in 10^{11} bits.
- Transmission Media – Guided and unguided media, mainly guided media is used; except in a situation where infrared is used to make a wireless LAN in a room.
- Topology – It refers to the ways in which the nodes are connected. There are various topologies used.
- Medium-Access Control Techniques –Some access control mechanism is needed to decide which station will use the shared medium at a particular point in time.

In this lesson we shall discuss various LAN standards proposed by the IEEE 8.2 committee with the following goals in mind:

- To promote compatibility
- Implementation with minimum efforts
- Accommodate the need for diverse applications

For the fulfillment of the abovementioned goals, the committee came up with a bunch of LAN standards collectively known as IEEE 802 LANs as shown in Fig. 5.3.1. To satisfy diverse requirements, the standard includes CSMA/CD, Token bus, Token Ring medium access control techniques along with different topologies. All these standards differ at the physical layer and MAC sublayer, but are compatible at the data link layer.

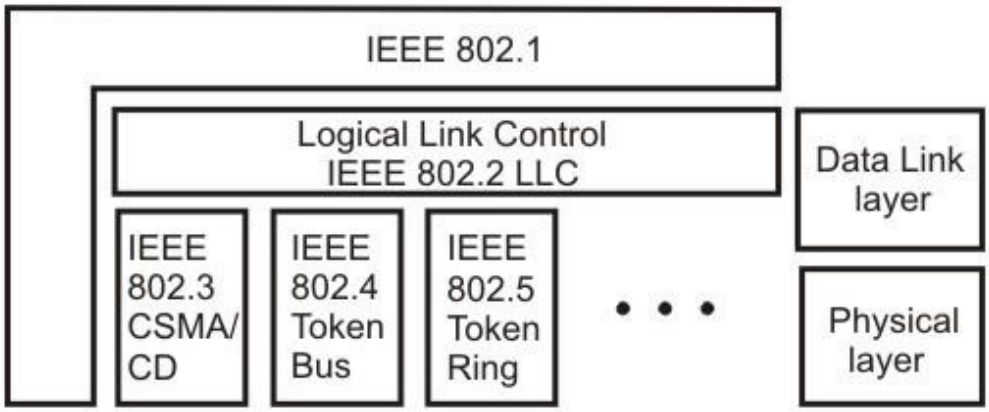


Figure 5.3.1 IEEE 802 Legacy LANs

The **802.1** sublayer gives an introduction to set of standards and gives the details of the interface primitives. It provides relationship between the OSI model and the 802 standards. The **802.2** sublayer describes the **LLC** (logical link layer), which is the upper part of the data link layer. LLC facilitate error control and flow control for reliable communication. It appends a header containing sequence number and acknowledgement number. And offers the following three types of services:

- Unreliable datagram service
- Acknowledged datagram service
- Reliable connection oriental service

The standards 802.3, 802.4 and 802.5 describe three LAN standards based on the CSMA/CD, token bus and token ring, respectively. Each standard covers the physical layer and MAC sublayer protocols. In the following sections we shall focus on these three LAN standards.

IEEE 802.3 and Ethernet

Ethernet - A Brief History

The original Ethernet was developed as an experimental coaxial cable network in the 1970s by Xerox Corporation to operate with a data rate of 3 Mbps using a carrier sense multiple access collision detection (CSMA/CD) protocol for LANs with sporadic traffic requirements. Success with that project attracted early attention and led to the 1980 joint development of the 10-Mbps Ethernet Version 1.0 specification by the three-company consortium: Digital Equipment Corporation, Intel Corporation, and Xerox Corporation.

The original IEEE 802.3 standard was based on, and was very similar to, the Ethernet Version 1.0 specification. The draft standard was approved by the 802.3 working group in 1983 and was subsequently published as an official standard in 1985 (ANSI/IEEE Std. 802.3-1985). Since then, a number of supplements to the standard have been defined to take advantage of improvements in the technologies and to support additional network media and higher data rate capabilities, plus several new optional network access control

features. From then onwards, the term *Ethernet* refers to the family of local-area network (LAN) products covered by the IEEE 802.3 standard that defines what is commonly known as the CSMA/CD protocol. Three data rates are currently defined for operation over optical fiber and twisted-pair cables:

- 10 Mbps—10Base-T Ethernet
- 100 Mbps—Fast Ethernet
- 1000 Mbps—Gigabit Ethernet

Ethernet has survived as the major LAN technology (it is currently used for approximately 85 percent of the world's LAN-connected PCs and workstations) because its protocol has the following characteristics:

- It is easy to understand, implement, manage, and maintain
- It allows low-cost network implementations
- It provides extensive topological flexibility for network installation
- It guarantees successful interconnection and operation of standards-compliant products, regardless of manufacturer

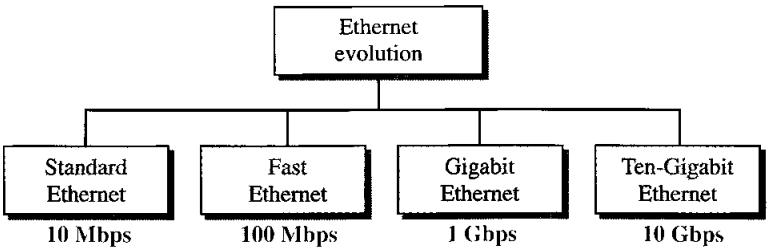
Ethernet Architecture

Ethernet architecture can be divided into two layers:

- **Physical layer:** this layer takes care of following functions.
  - Encoding and decoding
  - Collision detection
  - Carrier sensing
  - Transmission and receipt
- **Data link layer:** Following are the major functions of this layer.
  - Station interface
  - Data Encapsulation /Decapsulation
  - Link management
  - Collision Management

STANDARD ETHERNET

The original Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC). Since then, it has gone through four generations: Standard Ethernet (10 t Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps), and Ten-Gigabit Ethernet (10 Gbps), as shown in the figure:

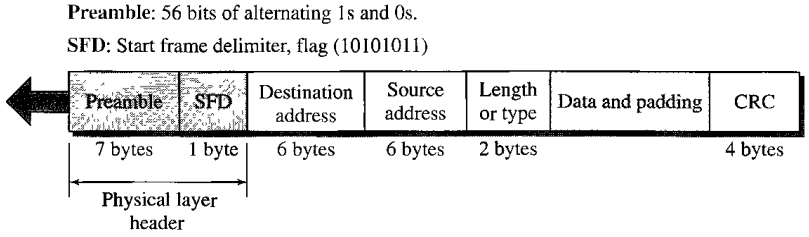


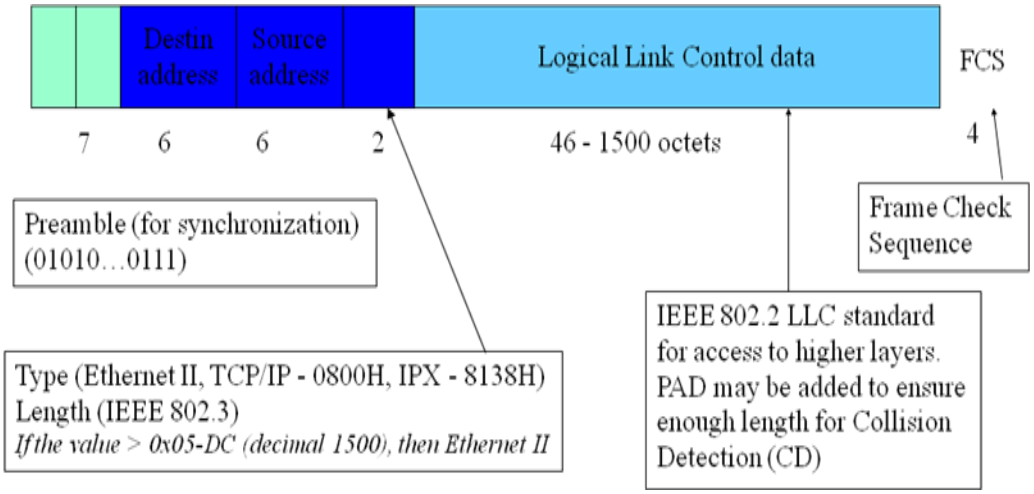
MAC Sublayer

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

Frame Format

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 the figure.

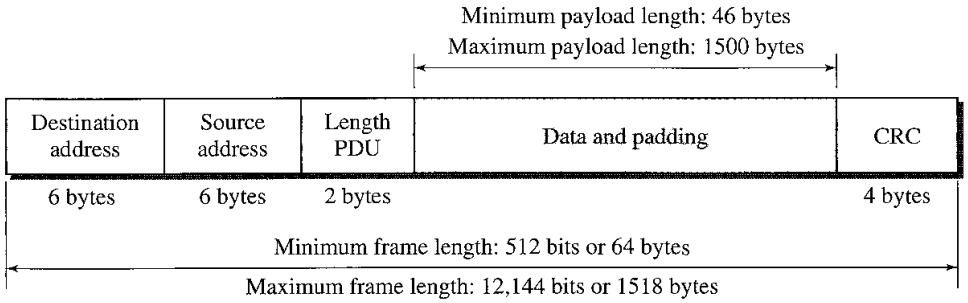




- **Preamble**. The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating 0s and 1s that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The pattern provides only an alert and a timing pulse. The 56-bit pattern allows the stations to miss some bits at the beginning of the frame. The preamble is actually added at the physical layer and is not (formally) part of the frame.
- **Start frame delimiter (SFD).** The second field (1 byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address.
- **Destination address (DA)**. The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet.
- **Source address (SA)**. The SA field is also 6 bytes and contains the physical address of the sender of the packet.
- **Length or type**. 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.
- **Data**. This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.
- **CRC**. The last field contains error detection information, in this case a CRC-32.

Frame Length

Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame, as shown in figure.

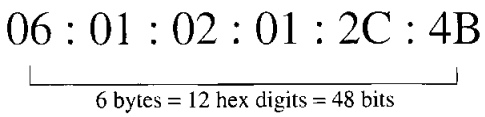


The minimum length restriction is required for the correct operation of CSMA/CD. An Ethernet frame needs to have a minimum length of 512 bits or 64 bytes. Part of this length is the header and the trailer. If we count 18 bytes of header and trailer (6 bytes of source address, 6 bytes of destination address, 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.

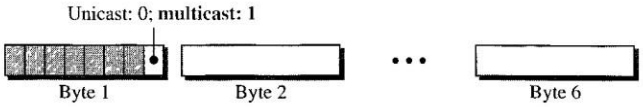
The standard defines the maximum length of a frame (without preamble and SFD field) as 1518 bytes. If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes. The maximum length restriction has two historical reasons. First, memory was very expensive when Ethernet 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.

Addressing

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



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



A unicast destination address defines only one recipient; the relationship between the sender and the receiver is one-to-one. A multicast destination address defines a group of addresses; the relationship between the sender and the receivers is one4o-many. The broadcast address is a special case of the multicast address; the recipients are all the stations on the LAN. A broadcast destination address is forty-eight ls.

Access Method: CSMA/CD

Standard Ethernet uses 1-persistent CSMA/CD

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

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

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

Slot Time and Collision The choice of a 512-bit slot time was not accidental. It was

chosen to allow the proper functioning of CSMA/CD. To understand the situation, let us consider two cases.

In the first case, we assume that the sender sends a minimum-size packet of 512 bits. Before the sender can send the entire packet out, the signal travels through the network and reaches the end of the network. If there is another signal at the end of the network (worst case), a collision occurs. The sender has the opportunity to abort the sending of the frame and to send a jam sequence to inform other stations of the collision. The roundtrip time plus the time required to send the jam sequence should be less than the time needed for the sender to send the minimum frame, 512 bits. The sender needs to be aware of the collision before it is too late, that is, before it has sent the entire frame.

In the second case, the sender sends a frame larger than the minimum size (between 512 and 1518 bits). In this case, if the station has sent out the first 512 bits and has not heard a

collision, it is guaranteed that collision will never occur during the transmission of this frame. The reason is that the signal will reach the end of the network in less than one-half the slot time. If all stations follow the CSMA/CD protocol, they have already sensed the existence of the signal (carrier) on the line and have refrained from sending. If they sent a signal on the line before one- half of the slot time expired, a collision has occurred and the sender has sensed the collision. In other words, collision can only occur during the first half of the slot time, and if it does, it can be sensed by the sender during the slot time. This means that after the sender sends the first 512 bits, it is guaranteed that collision will not occur during the transmission of this frame. The medium belongs to the sender, and no other station will use it. In other words, the sender needs to listen for a collision only during the time the first 512 bits are sent.

Slot Time and Maximum Network Length There is a relationship between the slot time and the maximum length of the network (collision domain). It is dependent on the propagation speed of the signal in the particular medium. In most transmission media, the signal propagates at 2 x 108 m/s (two-thirds of the rate for propagation in air). For traditional Ethernet, we calculate

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

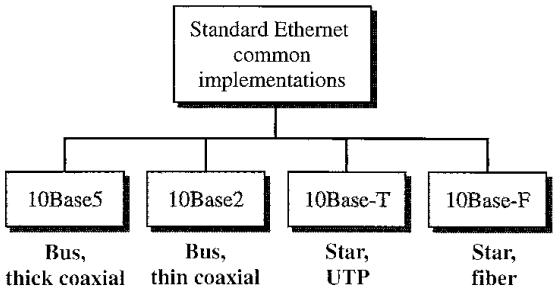
$$\text{MaxLength} = (2 \times 10^{8}) \times (51.2 \times 10^{-6} / 2) = 5120 \text{ m}$$

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

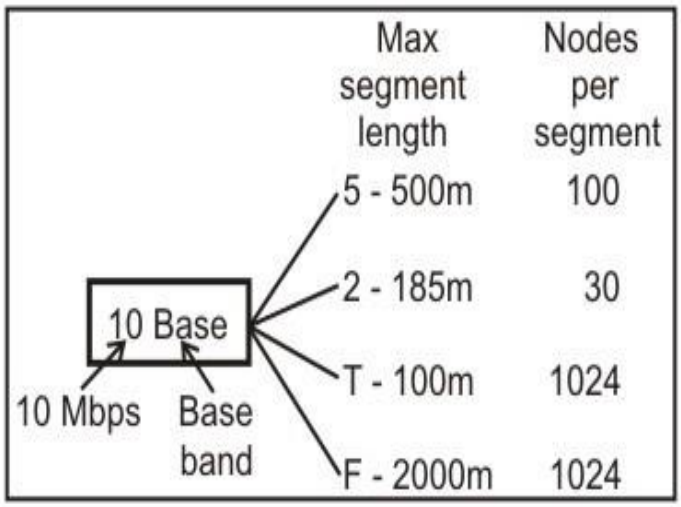
$$\text{MaxLength} = 2500 \text{ m}$$

Physical Layer

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

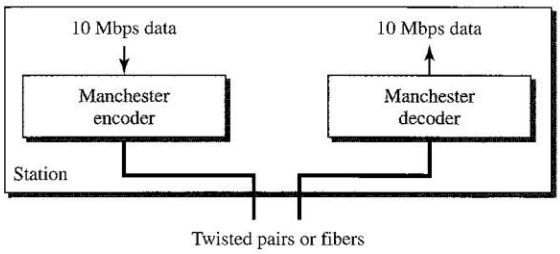


Because Ethernet devices implement only the bottom two layers of the OSI protocol stack, they are typically implemented as network interface cards (NICs) that plug into the host device's motherboard, or presently built-in in the motherboard. Various types cabling supported by the standard are shown in Fig. 5.3.2. The naming convention is a concatenation of three terms indicating the transmission rate, the transmission method, and the media type/signal encoding. Consider for example, 10Base-T. where 10 implies transmission rate of 10 Mbps, Base represents that it uses baseband signaling, and T refers to twisted-pair cables as transmission media. Various standards are discussed below:

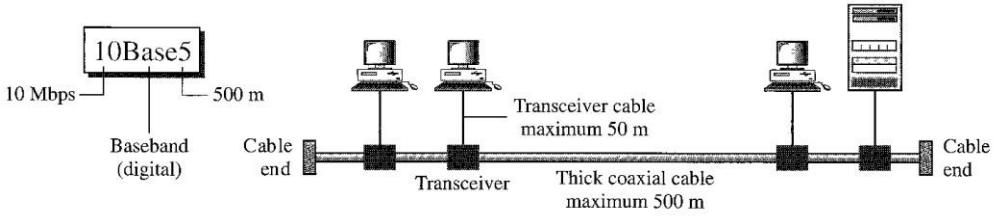


Encoding and Decoding

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. The figure shows the encoding scheme for Standard Ethernet.



10Base5: Thick Ethernet

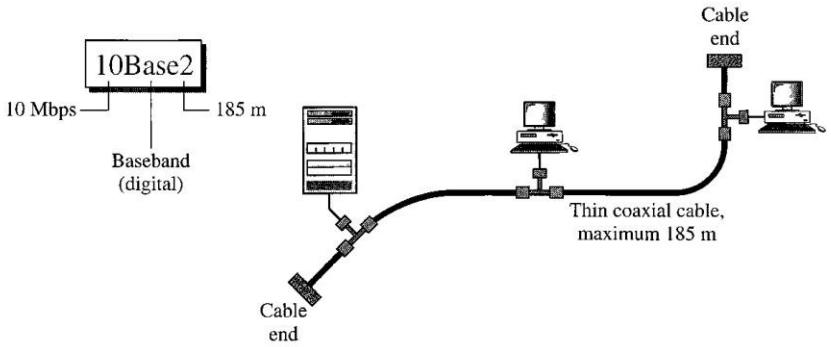


10Base5 was the first Ethernet specification to use a bus topology with an external transceiver (transmitter/receiver) connected via a tap to a thick coaxial cable. The transceiver is responsible for transmitting, receiving, and detecting collisions.

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.

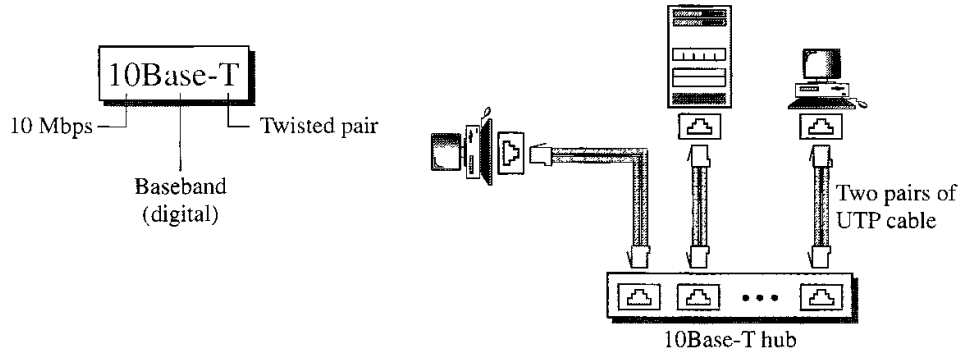
10Base2: Thin Ethernet



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

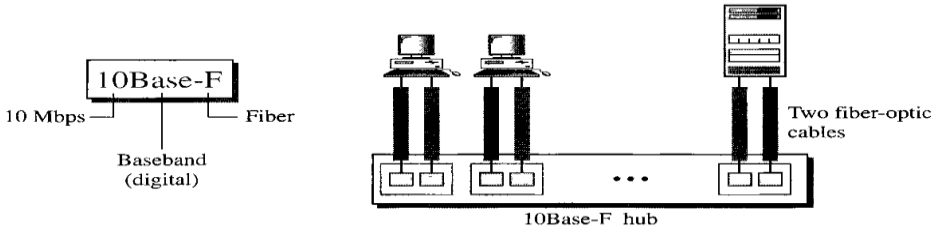
The third implementation is called 10Base-T or twisted-pair Ethernet. 10Base-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable.



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

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



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 sublayer can be turned off.

MAC Control Layer

Standard Ethernet was designed as a connectionless protocol at the MAC sublayer. There is no explicit flow control or error control to inform the sender that the

frame has arrived at the destination without error. When the receiver receives the frame, it does not send any positive or negative acknowledgment.

To provide for flow and error control in full-duplex switched Ethernet, a new sublayer, called the MAC control, is added between the LLC sublayer and the MAC sublayer.

FAST ETHERNET

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:

1. Upgrade the data rate to 100 Mbps.
2. Make it compatible with Standard Ethernet.
3. Keep the same 48-bit address.
4. Keep the same frame format.
5. Keep the same minimum and maximum frame lengths.

MAC Sublayer

A main consideration in the evolution of Ethernet from 10 to 100 Mbps was to keep the MAC sublayer untouched. However, a decision was made to drop the bus topologies and keep only the star topology. For the star topology, there are two choices, as we saw before: half duplex and full duplex. In the half-duplex approach, the stations are connected via a hub; in the full- duplex approach, the connection is made via a switch with buffers at each port.

The access method is the same (CSMA/CD) for the half-duplex approach; for full-duplex Fast Ethernet, there is no need for CSMA/CD. However, the implementations keep CSMA/CD for backward compatibility with Standard Ethernet.

Summary

Table 13.2 *Summary of Fast Ethernet implementations*

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

GIGABIT ETHERNET

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

1. Upgrade the data rate to 1 Gbps.
2. Make it compatible with Standard or Fast Ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. To support autonegotiation as defined in Fast Ethernet.

Summary

Table 13.3 *Summary of Gigabit Ethernet implementations*

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

Ten-Gigabit Ethernet

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

1. Upgrade the data rate to 10 Gbps.
2. Make it compatible with Standard, Fast, and Gigabit Ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. Allow the interconnection of existing LANs into a metropolitan area network (MAN) or a wide area network (WAN).
7. Make Ethernet compatible with technologies such as Frame Relay and ATM.

MAC Sublayer

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

Physical Layer

The physical layer in Ten-Gigabit Ethernet is designed for using fiber-optic cable over long distances. Three implementations are the most common: 10GBase-S, 10GBase-L, and 10GBase- E.

Table 13.4 *Summary of Ten-Gigabit Ethernet implementations*

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

- Explain the operation of IEEE 802 LANs
  - 802.4 – Token bus-based
  - 802.5 – Token ring-based
- Compare performance of the three LANs

Introduction

In the preceding lesson we have mentioned that for the fulfillment of different goals, the IEEE 802 committee came up with a bunch of LAN standards collectively known as

LANs as shown in Fig. 5.4.1. We have already discussed CSMA/CD-based LAN proposed by the IEEE 802.3 subcommittee, commonly known as Ethernet. In this lesson we shall discuss Token bus, Token Ring based LANs proposed by the IEEE 802.4 and IEEE 8.2.5 subcommittees.

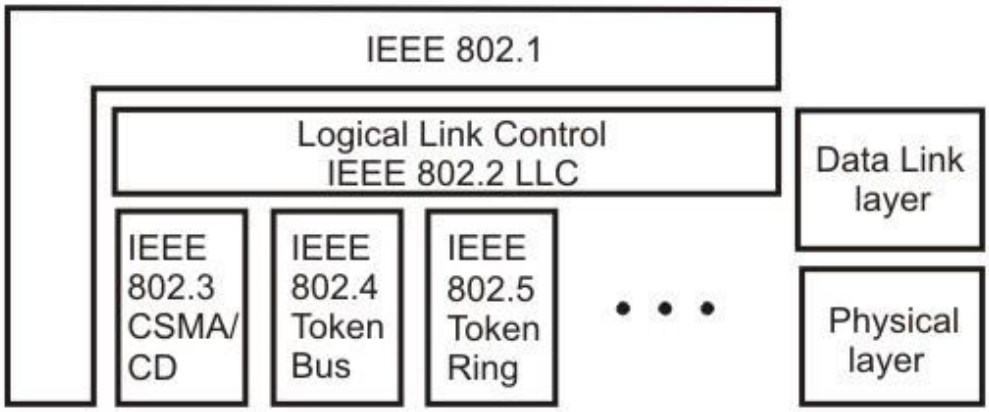


Figure IEEE 802 Legacy LANs

Token Ring (IEEE 802.5)

Token Ring: A Brief History

Originally, IBM developed Token Ring network in the 1970s. It is still IBM's primary local-area network (LAN) technology. The related IEEE 802.5 specification is almost identical to and completely compatible with IBM's Token Ring network. In fact, the IEEE 802.5 specification was modeled after IBM Token Ring, and on the same lines. The term *Token Ring* is generally used to refer to both IBM's Token Ring network and IEEE 802.5 networks.

Before going into the details of the Token Ring protocol, let's first discuss the motivation behind it. As already discussed, the medium access mechanism used by Ethernet (CSMA/CD) may results in collision. Nodes attempt to a number of times before they can actually transmit, and even when they start transmitting there are chances to encounter collisions and entire transmission need to be repeated. And all this become worse one the traffic is heavy i.e. all nodes have some data to transmit. Apart from this there is no way to predict either the occurrence of collision or delays produced by multiple stations attempting to capture the link at the same time. So all these problems with the Ethernet gives way to an alternate LAN technology, Token Ring.

Token Ring and IEEE802.5 are based on token passing MAC protocol with ring topology. They resolve the uncertainty by giving each station a turn on by one. Each node takes turns sending the data; each station may transmit data during its turn. The technique that coordinates this turn mechanism is called Token passing; as a Token is passed in the network and the station that gets the token can only transmit. As one node transmits at a time, there is no chance of collision. We shall discuss the detailed operation in next section.

Stations are connected by point-to-point links using repeaters. Mainly these links are of shielded twisted-pair cables. The repeaters function in two basic modes: Listen mode, Transmit mode. A disadvantage of this topology is that it is vulnerable to link or station failure. But a few measures can be taken to take care of it.

Differences between Token Ring and IEEE 802.5

Both of these networks are basically compatible, although the specifications differ in some ways.

- IEEE 802.5 does not specify a topology, although virtually all IEEE 802.5 implementations are based on the star topology. While IBM's Token Ring network explicitly specifies a star, with all end stations attached to a device called a Multi-Station Access Unit (MSAU).
- IEEE 802.5 does not specify a media type, although IBM Token Ring networks use twisted-pair wire.
- The most common local area network alternative to Ethernet is a network technology developed by IBM, called token ring.
- Where Ethernet relies on the random gaps between transmissions to regulate access to the medium, token ring implements a strict, orderly access method.
- A token-ring network arranges nodes in a logical ring, as shown below. The nodes forward frames in one direction around the ring,

removing a frame when it has circled
the ring once.

- The ring initializes by creating a **token**, which is a special type of frame that gives a station permission to transmit.

- The token circles the ring like any frame until it encounters a station that wishes to transmit data.
- This station then "captures" the token by replacing the token frame with a data-carrying frame, which encircles the network.
- Once that data frame returns to the transmitting station, that station removes the data frame, creates a new token and forwards that token on to the next node in the ring.
- Token-ring nodes do not look for a carrier signal or listen for collisions; the presence of the token frame provides assurance that the station can transmit a data frame without fear of another station interrupting.
- Because a station transmits only a single data frame before passing the token along, each station on the ring will get a turn to communicate in a deterministic and fair manner. Token-ring networks typically transmit data at either 4 or 16 Mbps.

- There are few differences in routing information field size of the two.

Token Ring Operation

Token-passing networks move a small frame, called a *token*, around the network. Possession of the token grants the right to transmit. If a node receiving the token has no information to send, it passes the token to the next end station. Each station can hold the token for a maximum period of time.

If a station possessing the token does have information to transmit, it seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring. While the information frame is circling the ring, no token is on the network (unless the ring supports early token release), which means that other stations wanting to transmit must wait. Therefore, *collisions cannot occur in Token Ring networks*. If *early token release* is supported, a new token can be released immediately after a frame transmission is complete.

The information frame circulates around the ring until it reaches the intended destination station, which copies the information for further processing. The information frame makes a round trip and is finally removed when it reaches the sending station. The sending station can check the returning frame to see whether the frame was seen and subsequently copied by the destination station in error-free form. Then the sending station inserts a new free token on the ring, if it has finished transmission of its packets.

Unlike CSMA/CD networks (such as Ethernet), token-passing networks are *deterministic*, which means that it is possible to calculate the maximum time that will pass before any end station will be capable of transmitting. Token Ring networks are ideal for applications in which delay must be predictable and robust network operation is important.

Priority System

Token Ring networks use a sophisticated priority system that permits certain user-designated, high-priority stations to use the network more frequently. Token Ring frames have two fields that control priority: *the priority field* and the *reservation field.*

Only stations with a priority equal to or higher than the priority value contained in a token can seize that token. After the token is seized and changed to an information frame, only stations with a priority value higher than that of the transmitting station can reserve the token for the next pass around the network. When the next token is generated, it includes the higher priority of the reserving station. Stations that raise a token's priority level must reinstate the previous priority after their transmission is complete.

Ring Maintenance

There are two error conditions that could cause the token ring to break down. One is the *lost token* in which case there is no token the ring, the other is the *busy token* that circulates endlessly. To overcome these problems, the IEEE 802 standard specifies that one of the stations be designated as ‘active monitor’. The monitor detects the lost condition using a timer by *time-out* mechanism and recovers by using a new free token. To detect a circulating busy token, the monitor sets a ‘monitor bit’ to one on any passing busy token. If it detects a busy token with the monitor bit already set, it implies that the sending station has failed to remove its packet and recovers by changing the busy token to a free token. Other stations on the ring have the role of passive monitor. The primary

job of these stations is to detect failure of the active monitor and assume the role of active monitor. A contention-resolution is used to determine which station to take over.

Physical Layer

The Token Ring uses shielded twisted pair of wire to establish point-point links between the adjacent stations. The baseband signaling uses differential Manchester encoding. To overcome the problem of cable break or network failure, which brings the entire network down, one suggested technique, is to use *wiring concentrator* as shown in Fig. 5.4.2.

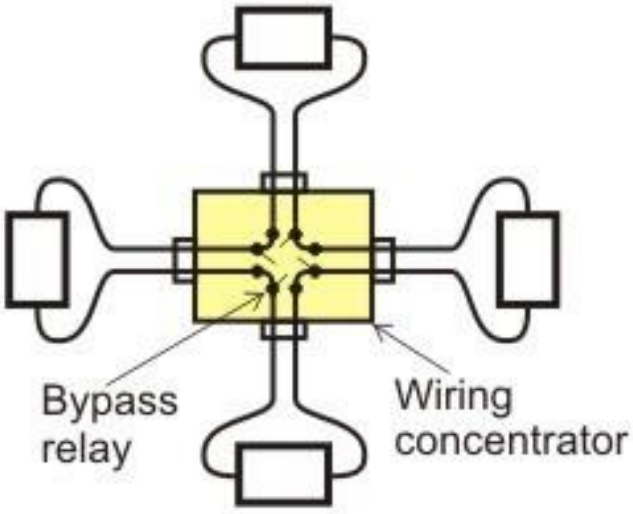
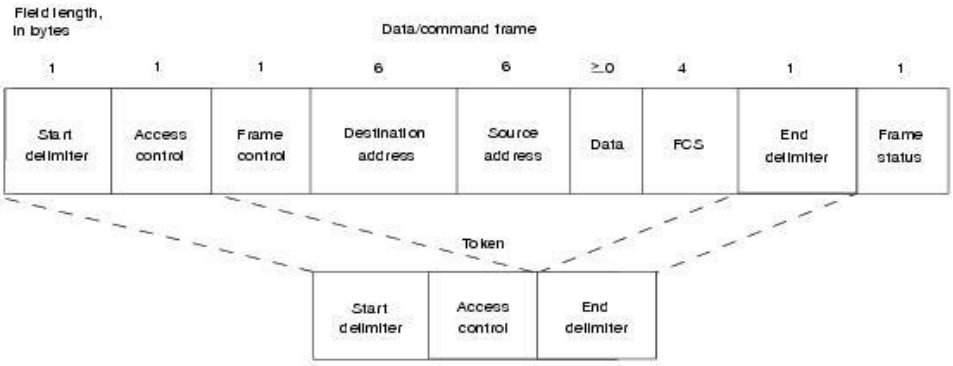


Figure 5.4.2 Star Connected Ring topology

It imposes the reliability in an elegant manner. Although logically the network remains as a ring, physically each station is connected to the *wire center* with two twisted pairs for 2-way communication. Inside the wire center, *bypass relays* are used to isolate a broken wire or a faulty station. This Topology is known as *Star-Connected Ring***.**

Frame Format

Token Ring and IEEE 802.5 support two basic frame types: tokens and data/command frames. Tokens are 3 bytes in length and consist of a start delimiter, an access control byte, and an end delimiter. Data/command frames vary in size, depending on the size of the Information field. Data frames carry information for upper-layer protocols, while command frames contain control information and have no data for upper-layer protocols.



802.5 Token Ring and IEEEsupport two basic frame types: tokens and data/command frames.

- Tokens are 3 bytes in length and consist of a start delimiter, an access control byte, and an end delimiter.
- Data/command frames vary in size, depending on the size of the Information field. Data frames carry information for upper-layer protocols, while command frames contain control information and have no data for upper-layer protocols. Both formats are shown in Figure: IEEE 802.5 and Token Ring Specify Tokens and Data/Command Frames

Token Frame Fields

Start	Access	Ending

Token Frame contains three fields, each of which is 1 byte in length:

- **Start delimiter (1 byte)**: Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.
- **Access-control (1 byte)**: Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).
- **End delimiter (1 byte)**: Signals the end of the token or data/command frame. This field also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.

Data/Command Frame Fields

Start Delimiter	Access Contr	Frame Contr	Destination address	Source addre	Data	Frame check sequence	End Delimiter	Frame Stat

Data/command frames have the same three fields as Token Frames, plus several others. The Data/command frame fields are described below:

- **Frame-control byte (1 byte)**—Indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.
- **Destination and source addresses (2-6 bytes)**—Consists of two 6-byte address fields that identify the destination and source station addresses.
- **Data (up to 4500 bytes)**—Indicates that the length of field is limited by the ring token holding time, which defines the maximum time a station can hold the token.
- **Frame-check sequence (FCS- 4 byte)**—Is filed by the source station with a calculated value dependent on the frame contents. The destination station recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.
- **Frame Status (1 byte)**—This is the terminating field of a command/data frame. The Frame Status field includes the address-recognized indicator and frame-copied indicator.

Token Frame Fields

The three token frame fields illustrated in Figure 9-3 are summarized in the descriptions that follow:

- **Start delimiter** - Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.
- **Access-control byte** - Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).
- **End delimiter** - Signals the end of the token or data/command frame. This field also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.

Data/Command Frame Fields

Data/command frames have the same three fields as Token Frames, plus several others. The Data/command frame fields illustrated in Figure 9-3 are described in the following summaries:

- **Start delimiter** - Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.
- **Access-control byte** - Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to

determine whether a frame is circling the ring endlessly).

- **Frame-control bytes** - Indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.
- **Destination and source addresses** - Consists of two 6-byte address fields that identify the destination and source station addresses.
- **Data** - Indicates that the length of field is limited by the ring token holding time, which defines the maximum time a station can hold the token.
- **Frame-check sequence (FCS)** - Is filed by the source station with a calculated value dependent on the frame contents. The destination station recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.
- **End Delimiter** - Signals the end of the token or data/command frame. The end delimiter also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.
- **Frame Status** - Is a 1-byte field terminating a command/data frame. The Frame Status field includes the address-recognized indicator and frame-copied indicator.

Token Bus (IEEE 802.4)

Token BUS: A Brief History

Although Ethernet was widely used in the offices, but people interested in factory automation did not like it because of the probabilistic MAC layer protocol. They wanted a protocol which can support priorities and has predictable delay. These people liked the conceptual idea of Token Ring network but did not like its physical implementation as a break in the ring cable could bring the whole network down and ring is a poor fit to their linear assembly lines. Thus a new standard, known as Token bus, was developed, having the robustness of the Bus topology, but the known worst-case behavior of a ring. Here

stations are logically connected as a ring but physically on a Bus and follows the collision-free token passing medium access control protocol. So the motivation behind token bus protocol can be summarized as:

- The probabilistic nature of CSMA/ CD leads to uncertainty about the delivery time; which created the need for a different protocol
- The token ring, on the hand, is very vulnerable to failure.
- Token bus provides deterministic delivery time, which is necessary for real time traffic.
- Token bus is also less vulnerable compared to token ring.

Functions of a Token Bus

It is the technique in which the station on bus or tree forms a logical ring, that is the stations are assigned positions in an ordered sequence, with the last number of the sequence followed by the first one as shown in Fig. 5.4.3. Each station knows the identity of the station following it and preceding it.

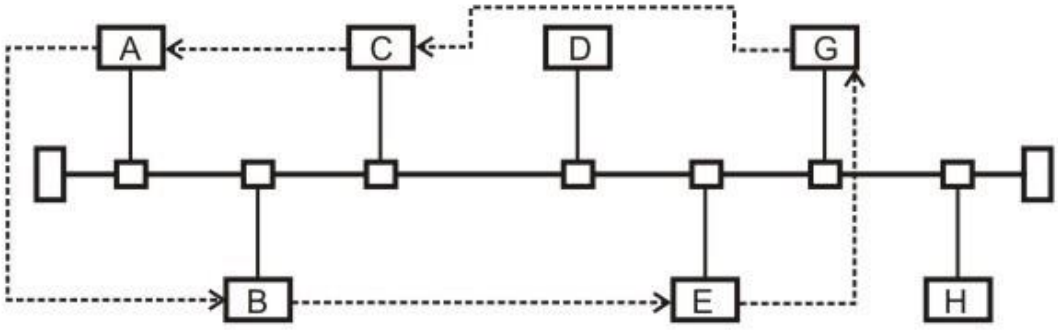


Figure 5.4.3 Token Bus topology

A control packet known as a *Token* regulates the right to access. When a station receives the token, it is granted control to the media for a specified time, during which it may transmit one or more packets and may poll stations and receive responses when the station is done, or if its time has expired then it passes token to next station in logical sequence. Hence, steady phase consists of alternate phases of token passing and data transfer.

The MAC sublayer consists of four major functions: the interface machine (IFM), the access control machine (ACM), the receiver machine (RxM) and the transmit machine (TxM).

IFM interfaces with the LLC sublayer. The LLC sublayer frames are passed on to the ACM by the IFM and if the received frame is also an LLC type, it is passed from RxM component to the LLC sublayer. IFM also provides quality of service.

The **ACM** is the heart of the system. It determines when to place a frame on the bus, and responsible for the maintenance of the logical ring including the *error detection* and *fault recovery*. It also cooperates with other stations ACM's to control the access to the

shared bus, controls the admission of new stations and attempts recovery from faults and failures.

The responsibility of a **TxM** is to transmit frame to physical layer. It accepts the frame from the ACM and builds a MAC protocol data unit (PDU) as per the format.

The **RxM** accepts data from the physical layer and identifies a full frame by detecting the SD and ED (start and end delimiter). It also checks the FCS field to validate an error-free transmission.

Frame Form

The frame format of the Token Bus is shown in Fig. 5.4.4. Most of the fields are same as Token Ring. So, we shall just look at the Frame Control Field in Table 5.4.1

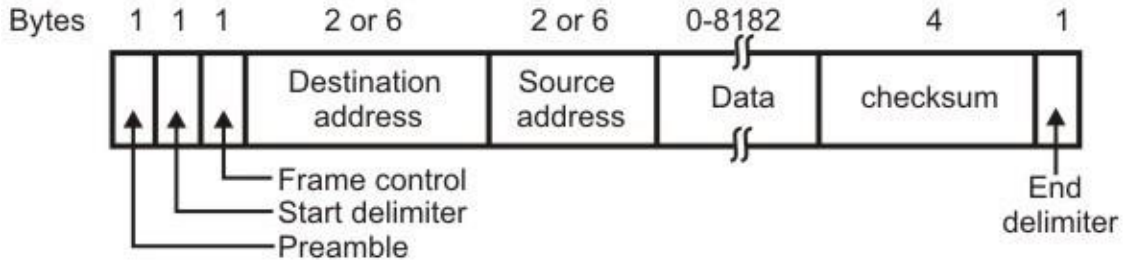


Figure 5.4.4 Token Bus frame format

Table 5.4.1 The Frame Control Field

Frame	Nam	Us
0000 0000	Claim-Token	Ring Initialization
0000 0001	Solicit-successor -1	Addition to the Ring
0000 0010	Solicit-successor -2	Addition to the Ring
0000 0011	Who-follows	Recovery from lost token
0000 0100	Resolve Contention	Multiple station to join the Ring
0000 1000	Token	Pass the Token
0000 1100	Set-Successor	Deletion from the ring

Logical ring maintenance

The MAC performs the following functions as part of its maintenance role of the ring.

Addition to the Ring: Non-participating stations must periodically be granted the opportunity to insert themselves into the ring. Each node in the ring periodically grants an opportunity for new nodes to enter the ring while holding the token. The node issues a solicit–successor–1 packet, inviting nodes with an address between itself and the next

node in logical sequence to request entrance. The transmitting node then waits for a period of time equal to one response window or slot time (twice the end-to-end propagation delay of the medium). If there is no request, the token holder sets its successor node to be the requesting node and transmits the token to it; the requester sets the linkages accordingly and proceeds.

If more than one node requests, to enter the ring, the token holder will detect a garbled transmission. The conflict is resolved by *addressed based contention scheme;* the token holder transmits a resolved contention packet and waits for four response windows. Each requester can transmit in one of these windows, based on the first two bits of its address. If requester hears anything before its windows comes up, it refrains from requesting entrance. If a token holder receives a valid response, then it can proceed, otherwise it tries again and only those nodes that request the first time are allowed to request this time, based on the second pair of bits in their address. This process continues until a valid request is received or no request is received, or a maximum retry count is reached. In latter cases, the token holder passes the token to logical successor in the ring.

Deletion from Ring: A station can voluntarily remove itself from the ring by splicing together its predecessor and successor. The node which wants to be deleted from the ring waits until token comes to it, then it sends a set successor packet to its predecessor, instructing it to splice to its successor.

Fault Management: Errors like duplicate address or broken ring can occur. A suitable management scheme should be implemented for smooth functioning. It is done by the token-holder first, while holding the token, node may hear a packet, indicating that another node has the token. In this case, it immediately drops the token by reverting to listener mode, and the number of token holders drops immediately from one to zero. Upon completion of its turn, it immediately issues a data or token packet. The sequence of steps are as follows:

i. After sending the token, the token issuer will listen for one slot time to make sure that its predecessor is active.
ii. If the issuer does not hear a valid packet, it reissues the token to the same successor one more time.
iii. After two failures, the issuer assumes that its successor has failed and issues a “who-follows” packet, asking for the identity of the node that follows the failed node. The issuer should get back a set successor packet from the second node down the time. If so, the issuer adjusts its linkage and issues a token (back to step i).
iv. If the issuing node gets a response to its “who-follows” packet, it tries again.
v. If the “who-follows” tactic fails, the node issues a solicit-successor-2 packet with full address range (i.e. every node is invited to respond). If this packet works then the ring is established and procedure continues.
vi. If two attempts in step (v) fail, it assumes that a catastrophe has happened; perhaps the node receiver has failed. In any case, the node ceases the activity and listen the bus.

Ring Initialization: Ring is to be initialized by starting the token passing. This is necessary when the network is being setup or when ring is broken down. Some decentralized algorithms should take care of, who starts first, who starts second, etc. it occurs when one or more stations detects a lack of bus activity lasting longer than a specific time. The token may get lost. This can occur on a number of occasions. For example, when network has been just powered up, or a token holding station fails. Once its time out expires, a node will issue a claim token packet. Contending clients are removed in a similar fashion to the response window process.

Relative comparison of the three standards

A comparison of the three standards for different functions is shown in Table 5.4.2 and results of the analysis of the performance of the three standards are summarized below:

- The CSMA/CD protocol shows strong dependence on the parameter 'a', which is the ratio of the propagation time to the transmission time. It offers shortest delay under light load and it is most sensitive under heavy load conditions.
- Token ring is least sensitive to different load conditions and different packet sizes.
- Token bus is highly efficient under light load conditions.

Table 5.4.2 Comparison of the three standards

Function	CSMA/CD	Token bus	Token ring
Access determination	Contention	Token	Token
Packet length	64 bytes (Greater than	None	None
Priority	Not	Supported	Supported
Sensitivity to work	Most	Sensitive	Least
Principle advantage	Simplicity, wide installed	Regulated/fair access	Regulated/fair access
Principle disadvantage	Nondeterministic delay	Complexity	Complexity

Fiber-Distributed Data Interface (FDDI)

Introduction

The IEEE 802.3 and 802.5 LANs, discussed in the previous sections, having data transfer rate in the range of 10 Mb/s to 16 Mb/s have served the purpose very well for many years. But with the availability of powerful computers at a low cost and emergence of new applications, particularly based on multimedia, there is a growing demand for higher network bandwidth. The combined effect of the growth in the number of users and increasing bandwidth requirement per user has led to the development of High Speed

LANs with data transfer rate of 100 Mb/s or more.

The high speed LANs that have emerged can be broadly categorized into three types *based on token passing, successors of Ethernet* and *based on switching technology*. In the first category we have *FDDI* and its variations, and high-speed token ring. In the second category we have the *fast Ethernet* and *Gigabit Ethernet*. In the third category we have *ATM, fiber channel* and the *Ether switches*. In this lesson we shall discuss details of FDDI – the token ring based high speed LAN.

FDDI

Fiber Distributed Data Interface (FDDI), developed by American National Standards Institute (ANSI) is a token passing ring network that operates at 100 Mb/s on optical fiber-medium. Its medium access control approach has close similarity with the IEEE 802.5 standard, but certain features have been added to it for higher reliability and better performance. Key features of FDDI are outlined in this section.

The FDDI standard divides transmission functions into 4 protocols: physical medium dependent (PMD), Physical (PHY), media access control(MAC) and Logical link control(LLC) as shown in Fig. 5.5.1. These protocols correspond to the physical and data link layer of OSI reference model. Apart from these four protocols, one more protocol which span across both data link and physical layer (if considered of OSI), used for the station management.

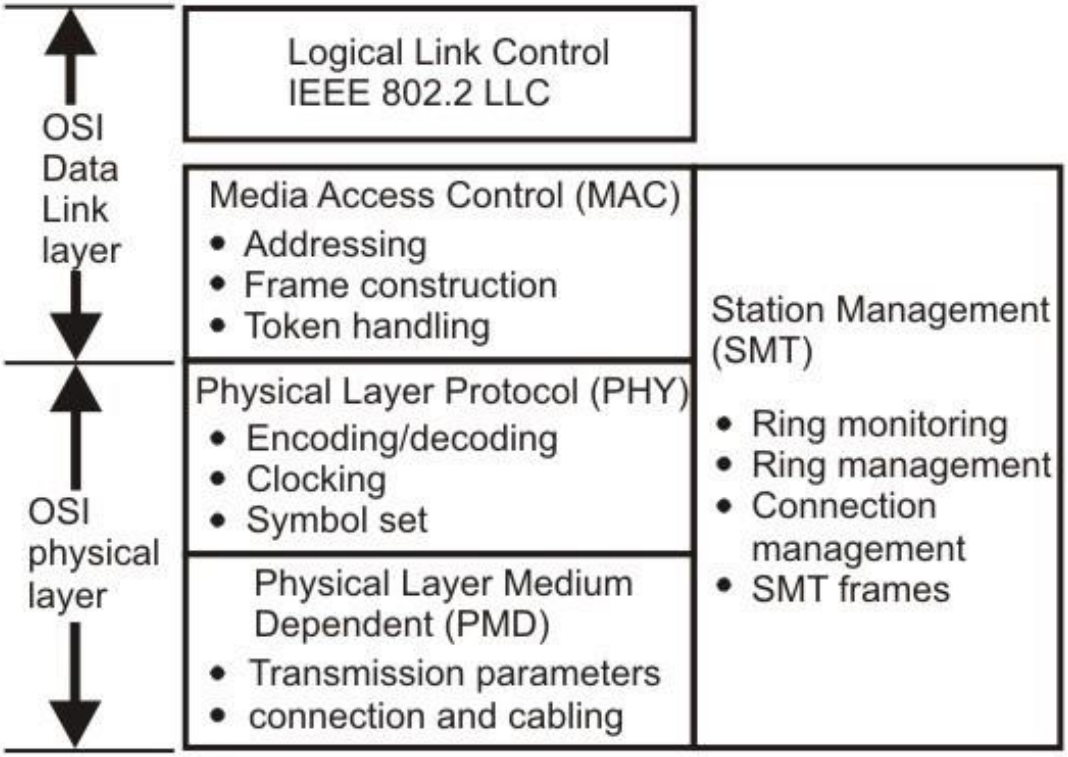
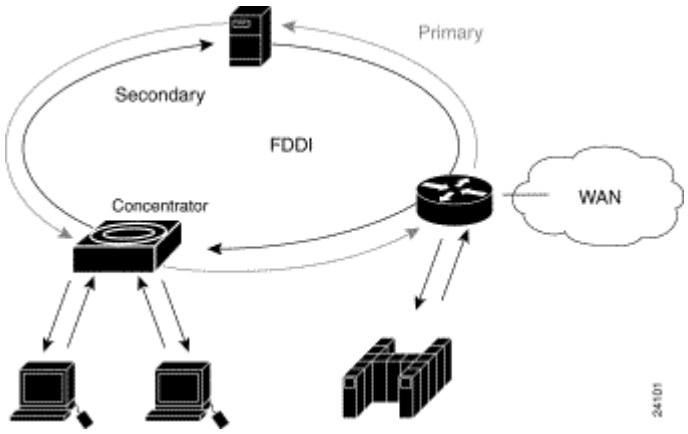


Figure FDDI protocols

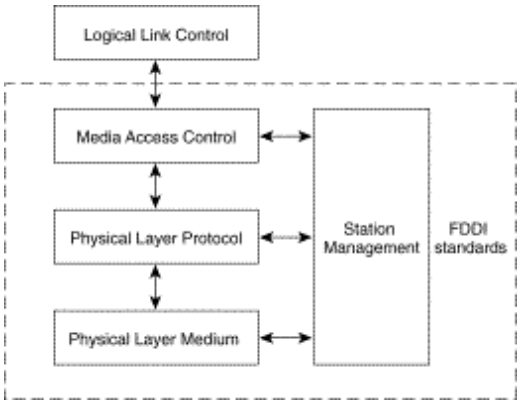
- FDDI networks offered transmission speeds of 100 Mbps, which initially made them quite popular for high-speed networking. With the advent of 100-Mbps Ethernet, which is cheaper and easier to administer, FDDI has waned in popularity.
- FDDI (Fiber-Distributed Data Interface) is a standard for data transmission on fiber optic lines in that can extend in range up to 200 km (124 miles). The FDDI protocol is based on the token ring protocol. In addition to being large geographically, an FDDI local area network can support thousands of users.
- An FDDI network contains two token rings, one for possible backup in case the primary ring fails. The primary ring offers up to 100 Mbps capacity. If the secondary ring is not needed for backup, it can also carry data, extending capacity to 200 Mbps. The single ring can extend the maximum distance; a dual ring can extend 100 km (62 miles).
- FDDI is a product of American National Standards Committee X3-T9 and conforms to the open system interconnect (OSI) model of functional layering. It can be used to interconnect LANs using other protocols. FDDI-II is a version of FDDI that adds the capability to add circuit-switched service to the network so that voice signals can also be



handled. Work is underway to connect FDDI networks to the developing Synchronous Optical Network.

Function of FDDI

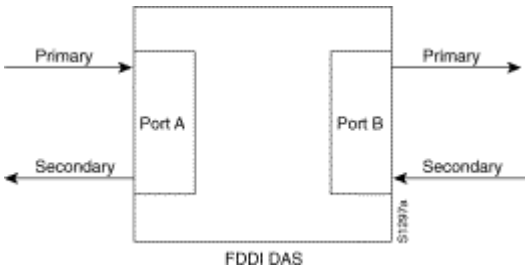
- The Fiber Distributed Data Interface (FDDI) specifies a 100-Mbps token-passing, dual-ring LAN using fiber-optic cable. FDDI is frequently used as high-speed backbone technology because of its support for high bandwidth and greater distances than copper.



- FDDI uses a dual-ring architecture with traffic on each ring flowing in opposite directions (called counter-rotating).
- The dual-rings consist of a primary and a secondary ring.
- During normal operation, the primary ring is used for data transmission, and the secondary ring remains idle.
- The primary purpose of the dual rings, as will be discussed in detail later in this chapter, is to provide superior reliability and robustness. Figure 1 shows the counter-rotating primary and secondary FDDI rings.

FDDI Station-Attachment Types

- One of the unique characteristics of FDDI is that multiple ways actually exist by which to connect FDDI devices. FDDI defines three types of devices: single-attachment station (SAS), dual-attachment station (DAS), and a concentrator.
- An SAS attaches to only one ring (the primary) through a concentrator. One of the primary advantages of connecting devices with SAS attachments is that the devices will not have any effect on the FDDI ring if they are disconnected or powered off. Concentrators will be discussed in more detail in the following discussion.



- Each FDDI DAS has two ports, designated A and B. These ports connect the DAS to the dual FDDI ring. Therefore, each port provides a connection for both the primary and the secondary ring. As you will see in the next section, devices using DAS connections will affect the ring if they are disconnected or powered off. Figure 3 shows FDDI DAS A and B ports with attachments to the primary and secondary rings.
- An FDDI concentrator (also called a *dual-attachment concentrator* [DAC]) is the building block of an FDDI network. It attaches directly to both the primary and secondary rings and ensures that the failure or power-down of any SAS does not bring down the ring.

FDDI Physical layer specification

Trans. Medium	Optical Fiber 62.5/125 um	Twisted pair CAT5-UTP
Data Rate	100 Mbps	100Mbps
Signaling Technique	4B/5B/NRZ-I 125 Mbaud	MTL-3
Max. No. Repeaters	100	100
Max. distance	2Km	100m

FDDI uses 4B/5B code for block coding. The 5-bit code is selected such that it has no more than one leading zero and no more than two trailing zeros and more than three consecutive 0's do not occur. Table 5.5.2 shows the encoded sequence for all the 4-bit

data sequences. The This is normally line coded with NRZ-I.

Topology

The basic topology for FDDI is *dual counter rotating rings:* one transmitting clockwise and the other transmitting counter clockwise as illustrated in the Fig. 5.5.2. One is known as *primary ring* and the other *secondary ring*. Although theoretically both the rings can be used to achieve a data transfer rate of 200 Mb/s, the standard recommends the use of the primary ring for data transmission and secondary ring as a backup.

In case of failure of a node or a fiber link, the ring is restored by wrapping the primary ring to the secondary ring as shown in Fig. 5.5.3. The redundancy in the ring design provides a degree of fault tolerance, not found in other network standards. Further improvement in reliability and availability can be achieved by using *dual ring* of trees and *dual homing* mechanism.

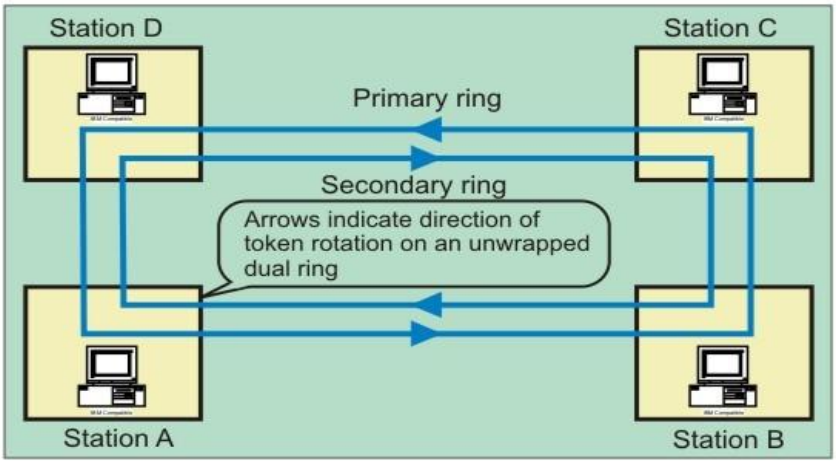


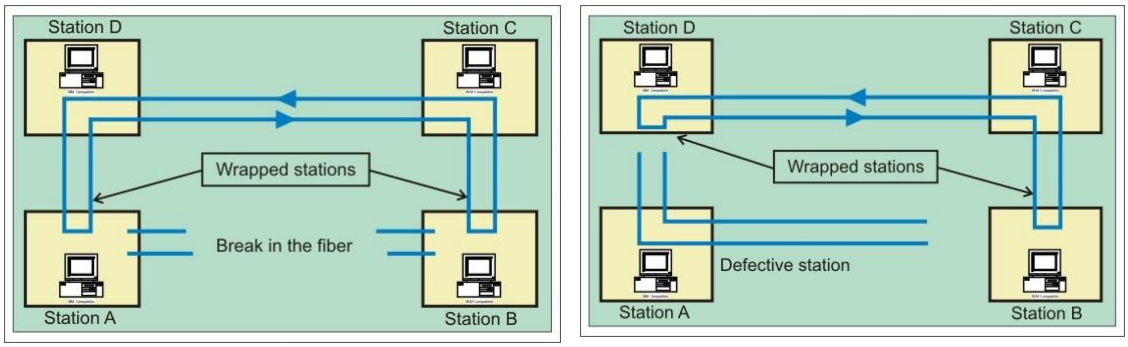
Figure FDDI dual counter-rotating ring topology

Fault Tolerance

FDDI provides a number of fault-tolerant features. In particular, FDDI's dual-ring environment, the implementation of the optical bypass switch, and dual-homing support make FDDI a resilient media technology.

Dual Ring

FDDI's primary fault-tolerant feature is the *dual ring*. If a station on the dual ring fails or is powered down, or if the cable is damaged, the dual ring is automatically wrapped (doubled back onto itself) into a single ring. When the ring is wrapped, the dual-ring topology becomes a single-ring topology. Data continues to be transmitted on the FDDI ring without performance impact during the wrap condition. Figure (a) and Figure (b) illustrate the effect of a ring wrapping in FDDI.



(a) (b)

Figure FDDI ring with a (a) broken link, (b) defective station

When a cable failure occurs, as shown in Fig. 5.5.3(a), devices on either side of the cable fault wrap. Network operation continues for all stations. When a single station fails, as shown in Fig. 5.5.3(b), devices on either side of the failed (or powered-down) station wrap, forming a single ring. Network operation continues for the remaining stations on the ring. It should be noted that FDDI truly provides fault tolerance against a single failure only. When two or more failures occur, the FDDI ring segments into two or more independent rings that are incapable of communicating with each other.

Optical Bypass Switch

An *optical bypass switch* provides continuous dual-ring operation if a device on the dual ring fails. This is used both to prevent ring segmentation and to eliminate failed stations from the ring. The optical bypass switch performs this function using optical mirrors that pass light from the ring directly to the DAS (dual-attachment station) device during normal operation. If a failure of the DAS device occurs, such as a power-off, the optical bypass switch will pass the light through itself by using internal mirrors and thereby will maintain the ring's integrity.

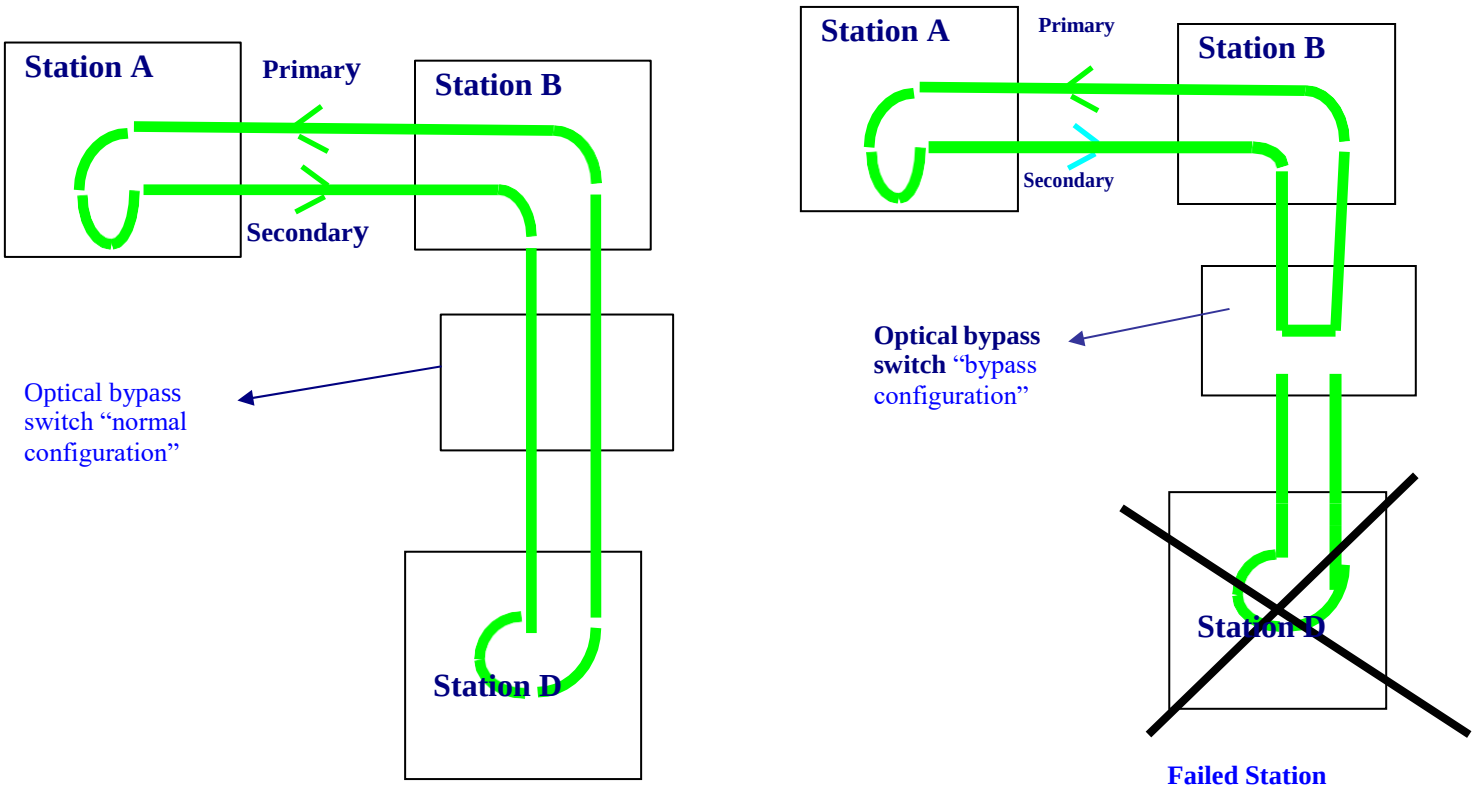


Figure The Optical Bypass switch uses internal mirrors to maintain a network The

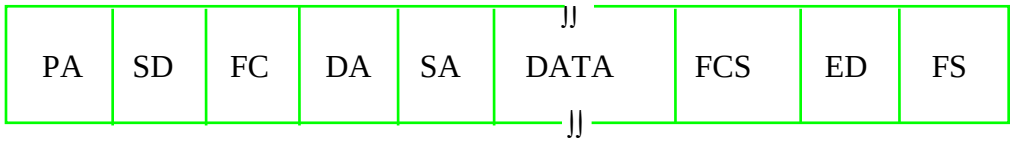
benefit of this capability is that the ring will not enter a wrapped condition in case of a device failure. A somewhat similar technique has been discussed in Token ring section (Star Connected Ring- where relays are used to bypass the faulty node). Figure shows the functionality of an optical bypass switch in an FDDI network. When using the OB, you will notice a tremendous digression of your network as the packets are sent through the OB unit.

Dual Homing: Critical devices, such as routers or mainframe hosts, can use a fault-tolerant technique called *dual homing* to provide additional redundancy and to help guarantee operation. In dual-homing situations, the critical device is attached to two concentrators.

Frame Format

Each Frame is preceded by a preamble (16 idle symbols-1111), for a total of 64 bits, to initialize clock synchronization with the receiver. There are 8 fields in the FDDI frame as shown in Fig. 5.5.5.

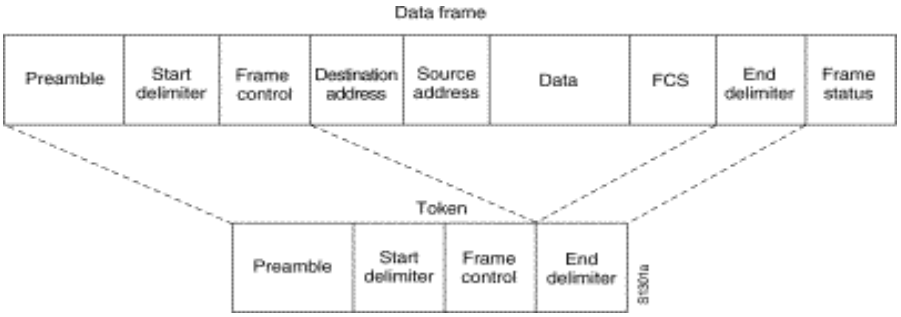
Data/Command Frame



Token

PA :	Preamble
SD :	Starting Delimiter
FC :	Frame Control
DA :	Destination Address
SA :	Source Address
FCS:	Frame Check Sequence
ED :	Ending Delimiter
FS :	Frame Status

Figure Frame format for the FDDI



Let us have a look at the various fields:
SD: The first byte, after the preamble, of the field is the frame's starting flag. As in Token ring these bits are replaced in physical layer by the control codes.

FC: it identifies the frame type i.e. token or a data frame.
Address: the next 2 fields are destination and source addresses. Each address consists of 2-6 bytes.

Data: Each data frame carries up to 4500 bytes.

FCS: FDDI uses the standard IEEE four-byte cyclic redundancy check.
ED: this field consists of half a byte in data frame or a full byte in token frame. This represents end of the Token.

FS: FDDI FS field is similar to that of Token Ring. It is included only in data/Command frame and consists of one and a half bytes.

Media Access Control

The FDDI media access control protocol is responsible for the following services.

(i) Fair and equal access to the ring by using a *timed token protocol*. To transmit on the ring, a station must first acquire the token. A station holds the token until it has transmitted all of its frames or until the transmission time for the appropriate service is over. Synchronous traffic is given a guaranteed bandwidth by ensuring that token rotation time does not exceed a preset value. FDDI implements these using three timers, *Token holding Timer* (THT), which determines how long a station may continue once it has captured a token. *Token Rotation Timer* (TRT) is reset every time a token is seen. When timer expires, it indicates that the token is lost and recovery is started. The *Valid*

Transmission Timer (VTT) is used to time out and recover from some transmit ring errors.

(ii) Construction of frames and tokens are done as per the format shown in Figure 5.5.5. The frame status (FS) byte is set by the destination and checked by the source station, which removes its frame from the ring and generates another token.

(iii) Transmitting, receiving, repeating and stripping frames and tokens from the ring, unlike IEEE 802.5, is possible for several frames on the ring simultaneously. Thus a station will transmit a token immediately after completion of its frame transmission. A station further down the ring is allowed to insert its own frame. This improves the potential throughput of the system. When the frame returns to the sending station, that station removes the frame from the ring by a process called *stripping*.

(iv) It also does *ring initialization, fault isolation* and error detection as we have discussed for IEEE 802.5.

FDDI and the OSI model

The relationship between the OSI model and the FDDI layered architecture is shown in Fig. 5.5.1. The physical layer is divided into two sub layers: PMD and PHY. The lower sub layer is defined by *Physical Layer Medium Dependent* (PMD) standards, which specify requirements such as media and connection types. The upper sub layer is defined in the physical layer protocol (PHY) standard, which is medium-independent. It defines symbols, line status, encoding/decoding techniques, clocking requirements and data framing requirements.

The Data Link Layer is divided into two sub layers, MAC and LLC. The lower sub layer, the FDDI Media Access Control (MAC) standard defines *addressing conventions, frame formats* and the *timed token protocol*. The upper sub layer is defined in the IEEE 802.2 LLC standard, which provides a means for exchanging data between LLC users.

The Station Management (SMT) standard provides services that monitor and control a FDDI station. SMT include facilities for connection management, node configuration, recovery from error condition, and encoding of SMT frames.

The FDDI has been successfully used as a backbone LAN in an enterprise network or in a campus network.

Comparison

Important features of the FDDI with the two popular IEEE 802 LAN standards are given in the Table

Table 5 Comparison of the standards

COMPARISON AMONG STANDARDS			
Parameters	FDDI	IEEE 802.3	IEEE 802.5
• BANDWIDTH	100Mb/s	10Mb/s	4 or 16Mb/s
• NUMBER OF STATIONS	500	1024	250
• MAX. DISTANCE BETWEEN STATIONS	2Km (MMF) 20Km (SMF)	2.8Km	300m (4Mb/s) 100m (RECO.)
• MAX. NETWORK EXTENT	100Km	2.8Km	VARIED WITH CONFIGURATION
• LOGICAL TOPOLOGY	DUAL RING, DUAL RING OF TREES	BUS	SINGLE RING
• PHYSICAL TOPOLOGY	RING, STAR HIERARCHICAL STAR	BUS, STAR	RING BUS HIERARCHICAL STAR
• MEDIA	OPTICAL FIBER	OPTICAL FIBRE, TWISTED-WIRE, COAXIAL CABLE	TWISTED-WIRE OPTICAL FIBER
• ACCESS METHOD	TIMED-TOKEN PASSING	CSMA/CD	TOKEN PASSING
• TOKEN ACQUISITION	CAPTURES THE TOKEN	-	BY SETTING A STATUS BIT
• TOKEN RELEASE	AFTER TRANSMIT	-	AFTER STRIPPING OR AFTER TRANSMIT (16)
• FRAMES ON LAN	MULTIPLE	SINGLE	SINGLE
• FRAMES TRANSMITTED PER ACCESS	MULTIPLE	SINGLE	SINGLE

• MAX. FRAME SIZE	4500 BYTES	1518 BYTES	4500 BYTES (4) 17,800 BYTES (16)

Metropolitan Area Network

A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the cable television network available in many cities. This system grew from earlier community antenna systems used in areas with poor over-the-air television reception. In these early systems, a large antenna was placed on top of a nearby hill and signal was then piped to the subscribers' houses. At first, these were locally-designed, ad hoc systems. Then companies began jumping into the business, getting contracts from city governments to wire up an entire city. The next step was television programming and even entire channels designed for cable only. Often these channels were highly specialized, such as all news, all sports, all cooking, all gardening, and so on. But from their inception until the late 1990s, they were intended for television reception only. To a first approximation, a MAN might look something like the system shown in Fig. In this figure both television signals and Internet are fed into the centralized head end for subsequent distribution to people's homes. Cable television is not the only MAN. Recent developments in high-speed wireless Internet access resulted in another MAN, which has been standardized as IEEE 802.16.

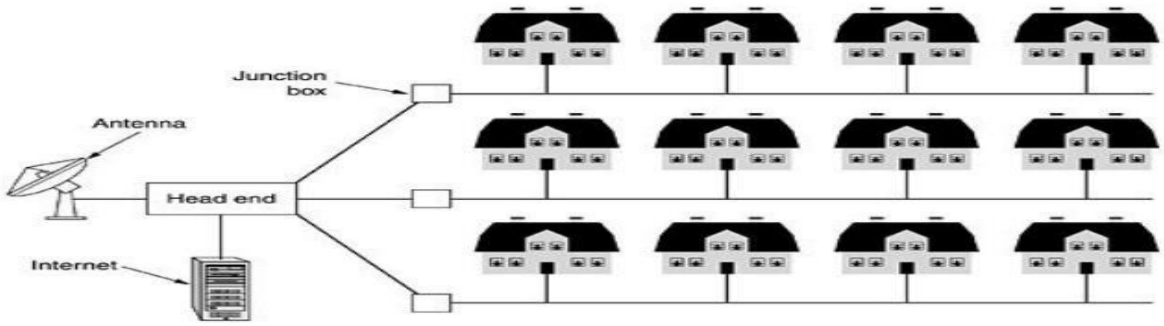
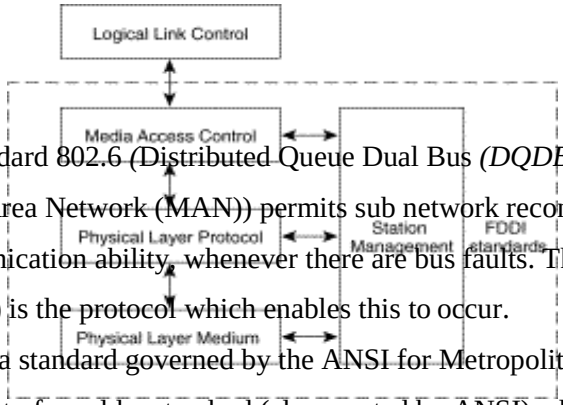


Fig.2: Metropolitan area network based on cable TV.

A MAN is implemented by a standard called DQDB (Distributed Queue Dual Bus) or IEEE 802.16. DQDB has two unidirectional buses (or cables) to which all the computers are attached.

802.6 DQDB



- The IEEE Standard 802.6 (Distributed Queue Dual Bus *(DQDB) Sub network of a* Metropolitan Area Network (MAN)) permits sub network reconfiguration, usually without loss of communication ability, whenever there are bus faults. The Configuration Control Protocol (CCP) is the protocol which enables this to occur.
- **IEEE 802.6** is a standard governed by the ANSI for Metropolitan Area Networks (MAN). It is an improvement of an older standard (also created by ANSI) which used the Fiber distributed data interface (FDDI) network structure.

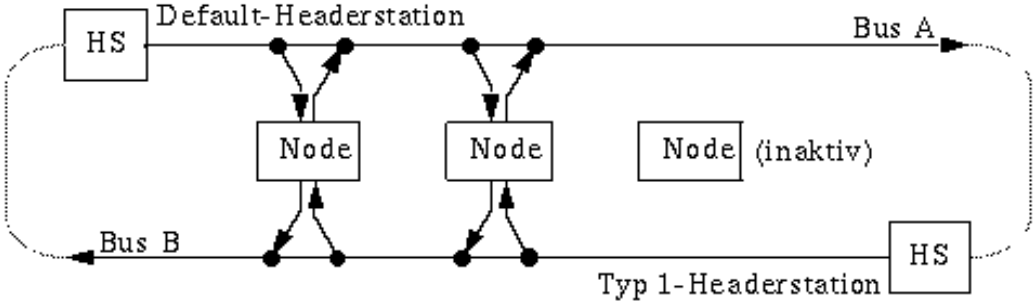
- The FDDI-based standard failed due to its expensive implementation and lack of compatibility with current LAN standards. The IEEE 802.6 standard uses the Distributed Queue Dual Bus (DQDB) network form. This form supports 150 Mbit/s transfer rates.
- It consists of two unconnected unidirectional buses. DQDB is rated for a maximum of 160 km before significant signal degradation over fiber optic cable with an optical wavelength of 1310 nm. This standard has also failed, mostly due to the same reasons that the FDDI standard failed.
- Most MANs now use Synchronous Optical Network (SONET) or Asynchronous Transfer Mode (ATM) network designs, with recent designs using native Ethernet or MPLS.
-

The DQDB Physical Layer

- The Head of Bus (HOB)s act a slot generators so that the bus is never quiet.
- Nodes are located logically adjacent to the bus and are promiscuous readers. They read all slots that come off the bus but may not necessarily alter any of the data.
- Nodes may be passive readers or, in an active system, they may act as repeaters so as to

forestall attenuation.

- If Node 2 wishes to send data in the direction of Node n then it will use Bus A. This implies that it must first reserve a slot by placing a request on Bus B.
- If Node 2 wishes to send data in the direction of Node 1 it must first reserve a slot using Bus A and then send the data on Bus B.



DQDB Operation

- The DQDB configuration is independent of the number of nodes and of the distances involved making DQDB ideal for high-speed transmissions
- DQDB uses 53-byte packets (52 data bytes and one access control byte) for transmissions called slots.
- Slots from different nodes are intermingled in the network traffic.

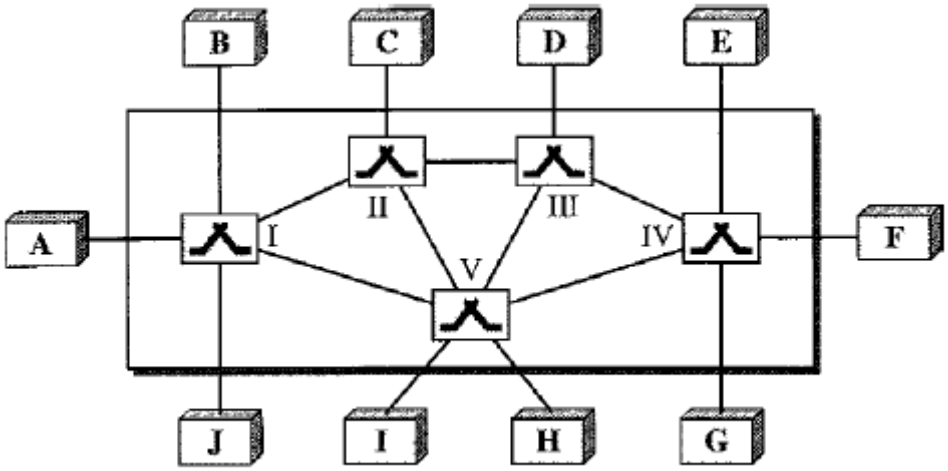
- The head node (the first node connected to the external fiber) is responsible for creating empty slots and sending these down the line to the other nodes to use.
- The down line nodes indicate how many slots are needed using the secondary bus to the head node which then creates empty slots and sends these down the line.
- As the slots move down the line, they are taken by the nodes that have requested them.

Switching

A network is a set of connected devices. Whenever we have multiple devices, we have the problem of how to connect them to make one-to-one communication possible. One solution is to make a point-to-point connection between each pair of devices (a mesh topology) or between a central device and every other device (a star topology). These methods, however, are impractical and wasteful when applied to very large networks. The number and length of the links require too

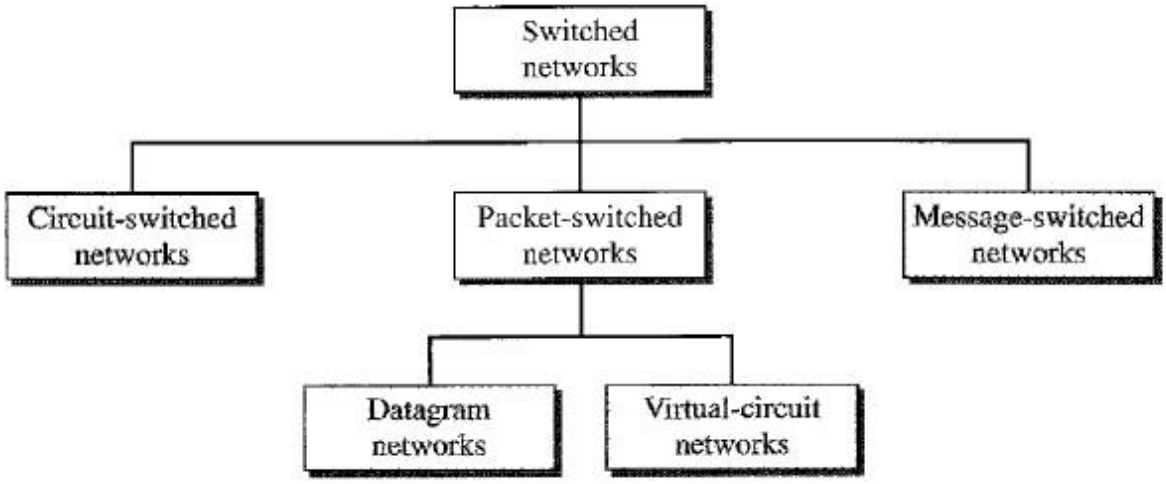
much infrastructure to be cost-efficient, and the majority of those links would be idle most of the time. Other topologies employing multipoint connections, such as a bus, are ruled out because the distances between devices and the total number of devices increase beyond the capacities of the media and equipment.

A better solution is switching. A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch. In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example). Others are used only for routing. Figure shows a switched network.



The end systems (communicating devices) are labeled A, B, C, D, and so on, and the switches are labeled I, II, III, IV, and V. Each switch is connected to multiple links.

Taxonomy of switched networks



CIRCUIT-SWITCHED NETWORKS

A circuit-switched network consists of a set of switches connected by physical links. A connection between two stations is a dedicated path made of one or more links. However, each connection uses only one dedicated channel on each link. Each link is normally divided into *n* channels by using FDM or TDM

Figure shows a trivial circuit-switched network with four switches and four links. Each link is divided into *n (n* is 3 in the figure) channels by using FDM or TDM.

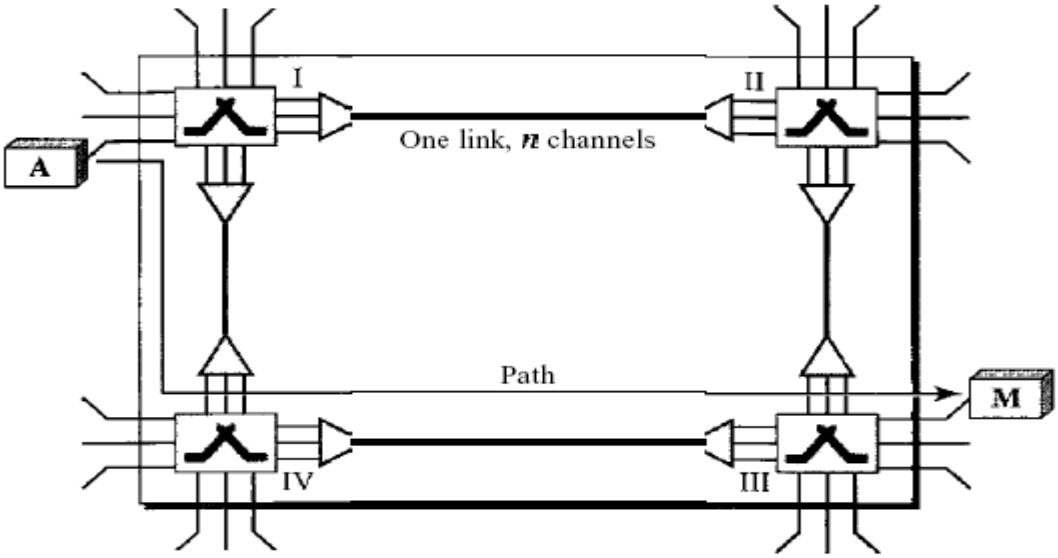


Fig: A trivial circuit-switched network

Three Phases

The actual communication in a circuit-switched network requires three phases: connection setup, data transfer, and connection teardown.

Setup Phase:

Before the two parties (or multiple parties in a conference call) can communicate, a dedicated circuit (combination of channels in links) needs to be established. The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches. For example, in Figure, when system A needs to connect to system M, it sends a setup request that includes the address of system M, to switch I. Switch I finds a channel between itself and switch IV that can be dedicated for this purpose. Switch I then sends the request to switch IV, which finds a dedicated channel between itself and switch III. Switch III informs system M of system A's intention at this time.

In the next step to making a connection, an acknowledgment from system M needs to be sent in the opposite direction to system A. Only after system A receives this acknowledgment is the connection established. Note that end-to-end addressing is required for creating a connection between the two end systems. These can be, for example, the addresses of the computers assigned by the administrator in a TDM network, or telephone numbers in an FDM network.

Data Transfer Phase:

After the establishment of the dedicated circuit (channels), the two parties can transfer data.

Teardown Phase:

When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

Efficiency:

It can be argued that circuit-switched networks are not as efficient as the other two types of networks because resources are allocated during the entire duration of the connection. These resources are unavailable to other connections. In a telephone network, people normally terminate the communication when they have finished their conversation. However, in computer networks, a computer can be connected to another computer even if there is no activity for a long time. In this case, allowing resources to be dedicated means that other connections are deprived.

Delay

Although a circuit-switched network normally has low efficiency, the delay in this type of network is minimal. During data transfer the data are not delayed at each switch; the resources are allocated for the duration of the connection. Figure 8.6 shows the idea of delay in a circuit-switched network when only two switches are involved. As Figure shows, there is no waiting time at each switch. The total delay is due to the time needed to create the connection, transfer data, and disconnect the circuit.

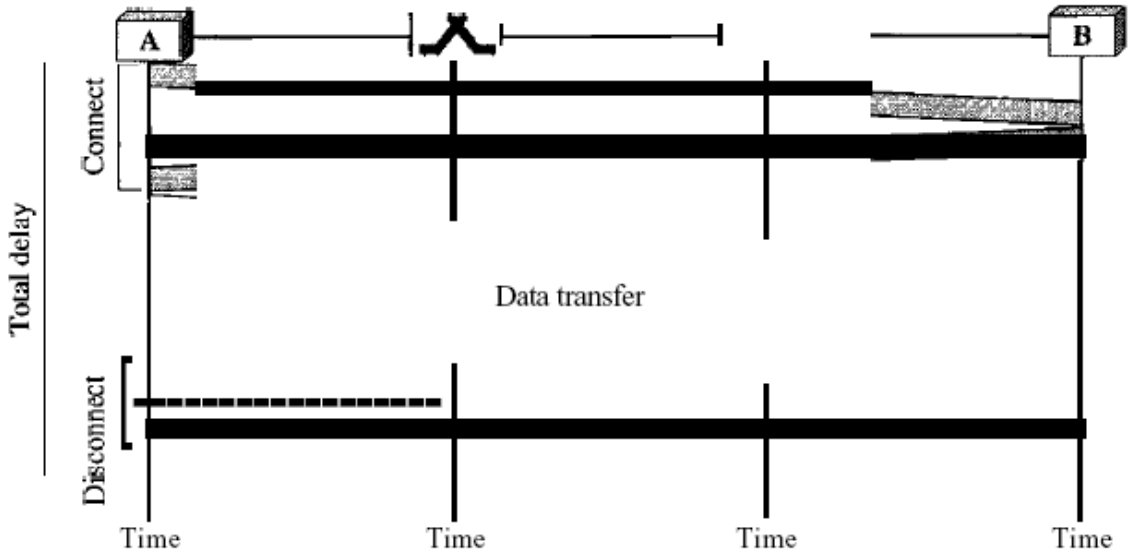


Fig: Delay in a circuit-switched network

The delay caused by the setup is the sum of four parts: the propagation time of the source computer request (slope of the first gray box), the request signal transfer time (height of the first gray box), the propagation time of the acknowledgment from the destination computer (slope of the second gray box), and the signal transfer time of the acknowledgment (height of the second gray box). The delay due to data transfer is the sum of two parts: the propagation time (slope of the colored box) and data transfer time (height of the colored box), which can be very long. The third box shows the time needed to tear down the circuit. We have shown the case in which the receiver requests disconnection, which creates the maximum delay.

DATAGRAM NETWORKS

In a datagram network, each packet is treated independently of all others. Even if a packet is part of a multipacket transmission, the network treats it as though it existed alone. Packets in this approach are referred to as datagrams.

Datagram switching is normally done at the network layer. We briefly discuss datagram networks here as a comparison with circuit-switched and virtual-circuit switched networks Figure shows how the datagram approach is used to deliver four packets from station A to station X. The switches in a datagram network are traditionally referred to as routers. That is why we use a different symbol for the switches in the figure.

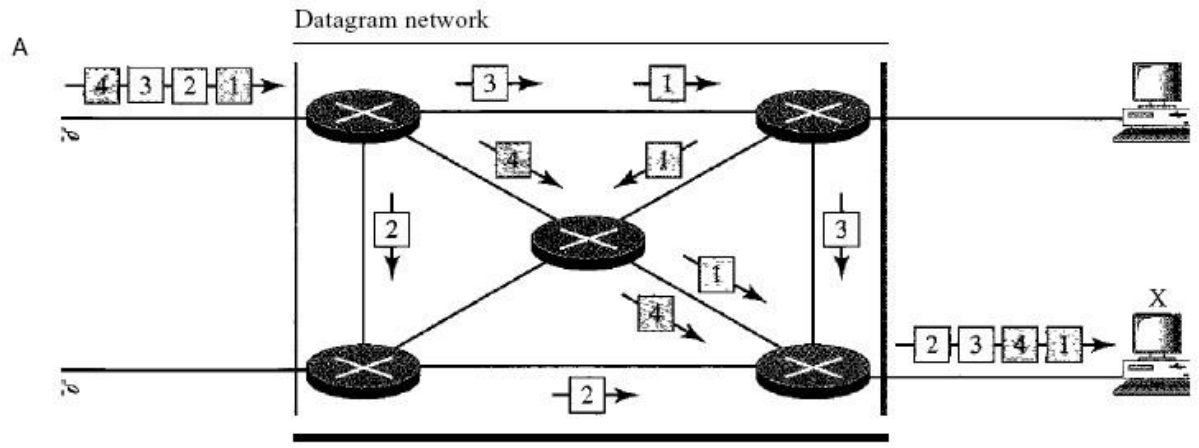


Fig: *A datagram network with four switches (routers)*

In this example, all four packets (or datagrams) belong to the same message, but may travel different paths to reach their destination. This is so because the links may be involved in carrying packets from other sources and do not have the necessary bandwidth available to carry all the packets from A to X. This approach can cause the datagrams of a transmission to arrive at their destination out of order with different delays between the packets. Packets may also be lost or dropped because of a lack of resources. In most protocols, it is the responsibility of an upper-layer protocol to reorder the datagrams or ask for lost datagrams before passing them on to the application.

The datagram networks are sometimes referred to as connectionless networks. The term *connectionless* here means that the switch (packet switch) does not keep information about the connection state. There are no setup or teardown phases. Each packet is treated the same by a switch regardless of its source or destination.

Routing Table

If there are no setup or teardown phases, how are the packets routed to their destinations in a datagram network? In this type of network, each switch (or packet switch) has a routing table which is based on the destination address. The routing tables are dynamic and are updated periodically. The destination addresses and the corresponding forwarding output ports are recorded in the tables. This is different from the table of a circuit switched network in which each entry is created when the setup phase is completed and deleted when the teardown phase is over. Figure shows the routing table for a switch.

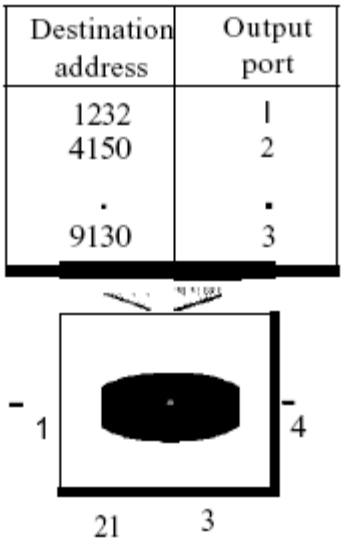


Fig: Routing table in a datagram network

Destination address

Every packet in a datagram network carries a header that contains, among other information, the destination address of the packet. When the switch receives the packet, this destination address is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded. This address, unlike the address in a virtual-circuit-switched network, remains the same during the entire journey of the packet.

Efficiency

The efficiency of a datagram network is better than that of a circuit-switched network; resources are allocated only when there are packets to be transferred. If a source sends a packet and there is a delay of a few minutes before another packet can be sent, the resources can be reallocated during these minutes for other packets from other sources.

Delay

There may be greater delay in a datagram network than in a virtual-circuit network. Although there are no setup and teardown phases, each packet may experience a wait at a switch before it is forwarded. In addition, since not all packets in a message necessarily travel through the same switches, the delay is not uniform for the packets of a message.

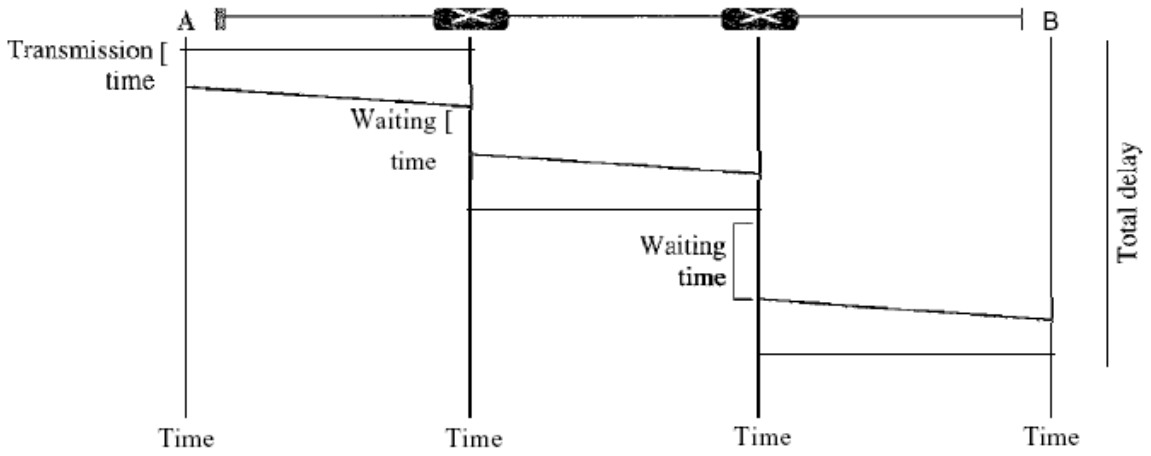


Fig: Delay in a datagram network

The packet travels through two switches. There are three transmission times *(3T),* three propagation delays (slopes 3't of the lines), and two waiting times (WI + *w2)'* We ignore the processing time in each switch. The total delay is

Total delay =*3T* + 3t + WI + W2

VIRTUAL-CIRCUIT NETWORKS:

A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.

1. As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.
2. Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.
3. As in a datagram network, data are packetized and each packet carries an address in the header. However, the address in the header has local jurisdiction (it defines what should be the next switch and the channel on which the packet is being canied), not end-to-end jurisdiction. The reader may ask how the intermediate switches know where to send the packet if there is no

final destination address carried by a packet. The answer will be clear when we discuss virtual-circuit identifiers in the next section.

4. As in a circuit-switched network, all packets follow the same path established during the connection.

5. A virtual-circuit network is normally implemented in the data link layer, while a circuit-switched network is implemented in the physical layer and a datagram network in the network layer. But this may change in the future. Figure is an example of a virtual-circuit network. The network has switches that allow traffic from sources to destinations. A source or destination can be a computer, packet switch, bridge, or any other device that connects other networks.

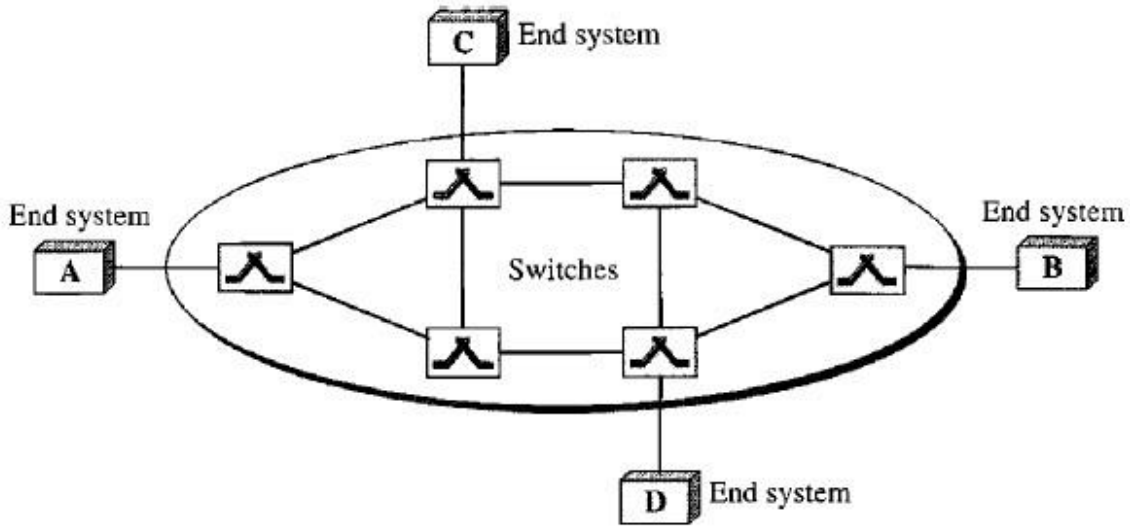


Fig a: *Virtual-circuit network*

Addressing

In a virtual-circuit network, two types of addressing are involved: global and local (virtual-circuit identifier).

Global Addressing: A source or a destination needs to have a global address-an address that can be unique in the scope of the network or internationally if the network is part of an international network. However, we will see that a global address in virtual-circuit networks is used only to create a virtual-circuit identifier, as discussed next.

Virtual-Circuit Identifier: The identifier that is actually used for data transfer is called the virtual-circuit identifier (Vel). A vel, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCl. Figure 8.11 shows how the VCI in a data frame

changes from one switch to another. Note that a VCI does not need to be a large number since each switch can use its own unique set of VCls.

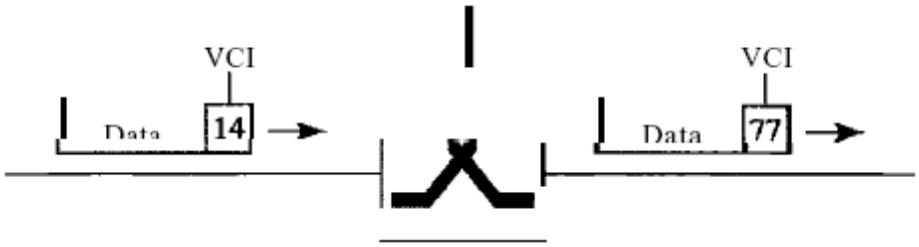


Figure 1 *Virtual-circuit identifier*

Three Phases

As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network: setup, data transfer, and teardown. In the setup phase, the source and destination use their global addresses to help switches make table entries for the connection. In the teardown phase, the source and destination inform the switches to delete the corresponding entry. Data transfer occurs between these two phases. We first discuss the data transfer phase, which is more straightforward; we then talk about the setup and teardown phases.

Data Transfer Phase

To transfer a frame from a source to its destination, all switches need to have a table entry for this virtual circuit. The table, in its simplest form, has four columns. This means that the switch holds four pieces of information for each virtual circuit that is already set up. We show later how the switches make their table entries, but for the moment we assume that each switch has a table with entries for all active virtual circuits. Figure 2 shows such a switch and its corresponding table. And also shows a frame arriving at port 1 with a VCI of 14. When the frame arrives, the switch looks in its table to find port 1 and a VCI of 14. When it is found, the switch knows to change the VCI to 22 and send out the frame from port 3. Figure 3 shows how a frame from source A reaches destination B and how its VCI changes during the trip. Each switch changes the VCI and routes the frame. The data transfer phase is active until the source sends all its frames to the destination. The procedure at the switch is the same for each frame of a message. The process creates a virtual circuit, not a real circuit, between the source and destination.

Setup Phase

In the setup phase, a switch creates an entry for a virtual circuit. For example, suppose source A needs to create a virtual circuit to B. Two steps are required: the setup request and the acknowledgment.

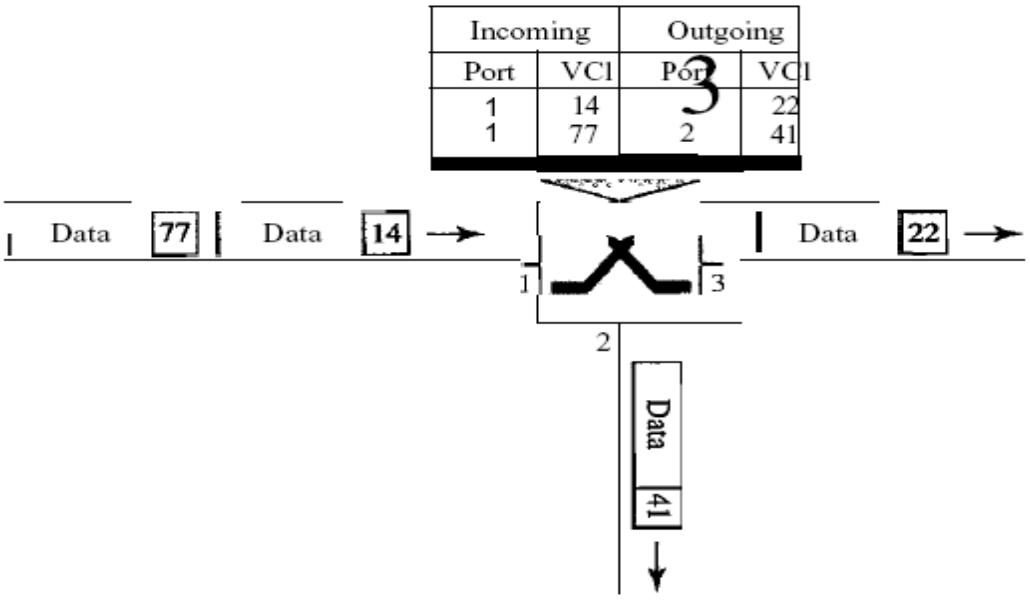


Figure 2 *Switch and tables in a virtual-circuit network*

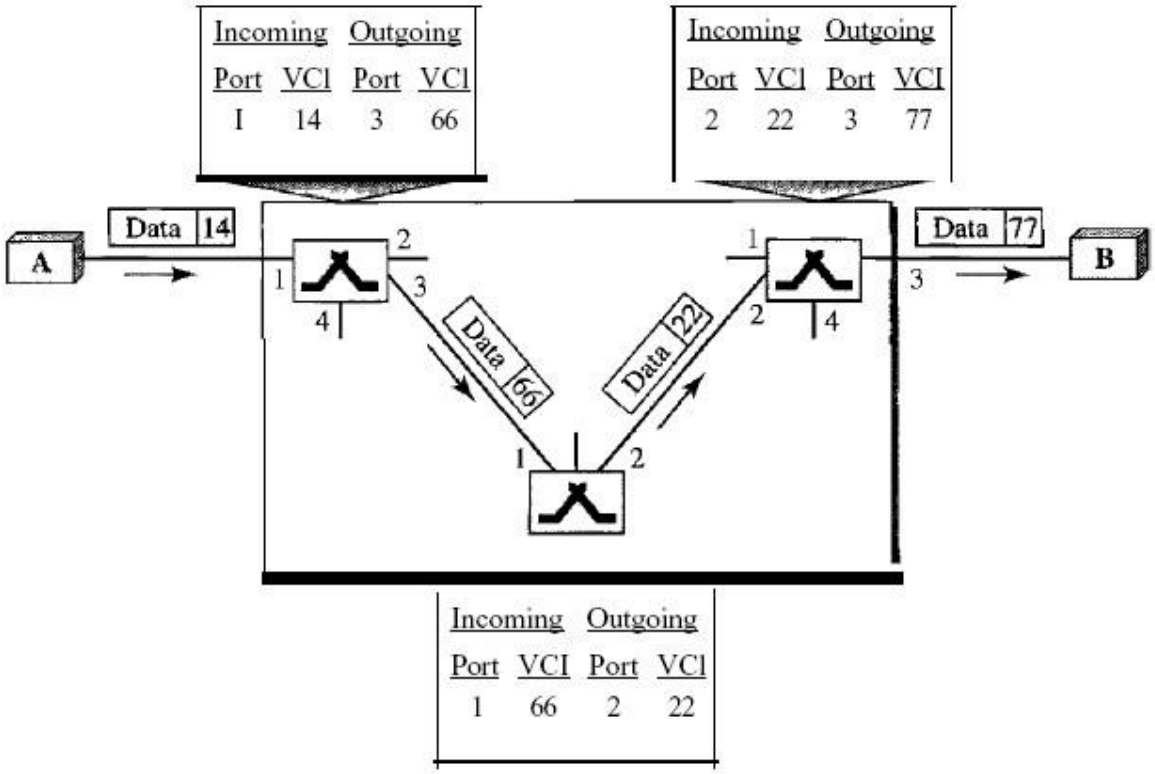


Figure 3 *Source-to-destination data transfer in a virtual-circuit network*

Setup Request

A setup request frame is sent from the source to the destination.

Figure 4 shows the process.

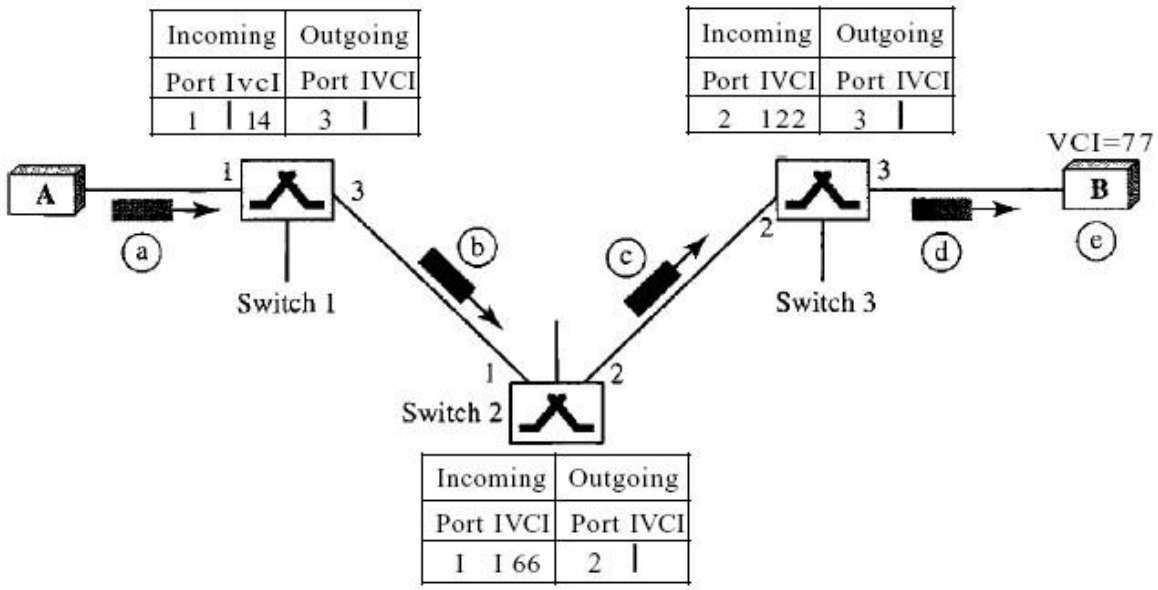


Figure 4 *Setup request in a virtual-circuit network*

a. Source A sends a setup frame to switch 1.

b. Switch 1 receives the setup request frame. It knows that a frame going from A to B goes out through port 3. How the switch has obtained this information is a point covered in future chapters. The switch, in the setup phase, acts as a packet switch; it has a routing table which is different from the switching table. For the moment, assume that it knows the output port. The switch creates an entry in its table for this virtual circuit, but it is only able to fill three of the four columns. The switch assigns the incoming port (1) and chooses an available incoming VCI (14) and the outgoing port (3). It does not yet know the outgoing VCI, which will be found during the acknowledgment step. The switch then forwards the frame through port 3 to switch 2.

c. Switch 2 receives the setup request frame. The same events happen here as at switch 1; three columns of the table are completed: in this case, incoming port (l), incoming VCI (66), and outgoing port (2).

d. Switch 3 receives the setup request frame. Again, three columns are completed: incoming port (2), incoming VCI (22), and outgoing port (3).

e. Destination B receives the setup frame, and if it is ready to receive frames from A, it assigns a VCI to the incoming frames that come from A, in this case 77. This VCI lets the destination know that the frames come from A, and not other sources.

Acknowledgment A special frame, called the acknowledgment frame, completes the entries in the switching tables. Figure 8.15 shows the process.

a. The destination sends an acknowledgment to switch 3. The acknowledgment carries the global source and destination addresses so the switch knows which entry in the table is to be completed. The frame also carries VCI 77, chosen by the destination as the incoming VCI for frames from A. Switch 3 uses this VCI to complete the outgoing VCI column for this entry. Note that 77 is the incoming VCI for destination B, but the outgoing VCI for switch 3.

b. Switch 3 sends an acknowledgment to switch 2 that contains its incoming VCI in the table, chosen in the previous step. Switch 2 uses this as the outgoing VCI in the table.

c. Switch 2 sends an acknowledgment to switch 1 that contains its incoming VCI in the table, chosen in the previous step. Switch 1 uses this as the outgoing VCI in the table.

d. Finally switch 1 sends an acknowledgment to source A that contains its incoming VCI in the table, chosen in the previous step.

e. The source uses this as the outgoing VCI for the data frames to be sent to destination B.

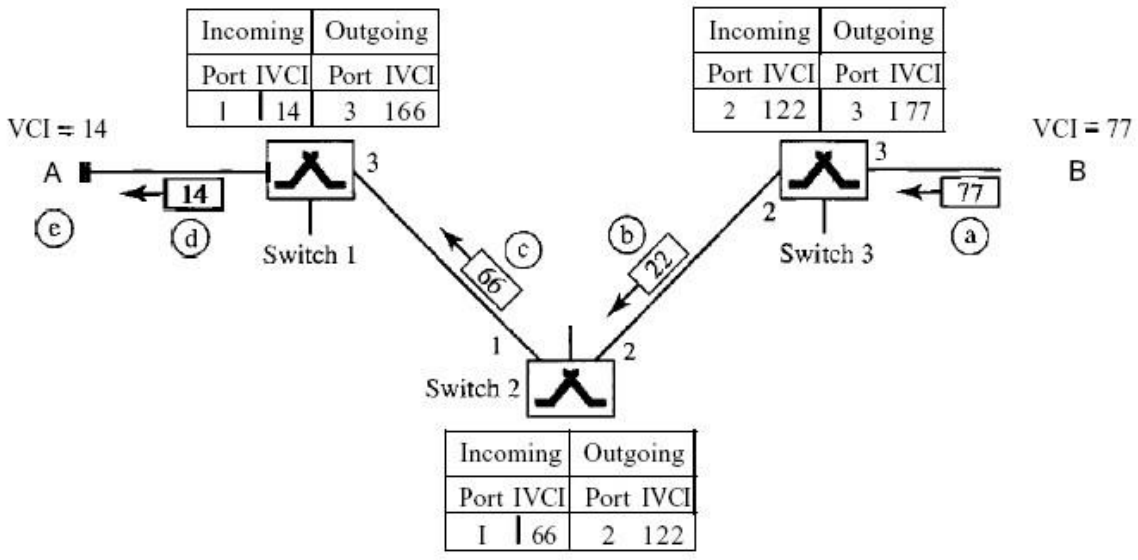


Figure 5 *Setup acknowledgments in a virtual-circuit network*

Teardown Phase

In this phase, source A, after sending all frames to B, sends a special frame called a *teardown request.* Destination B responds with a teardown confirmation frame. All switches delete the corresponding entry from their tables.

Efficiency

As we said before, resource reservation in a virtual-circuit network can be made during the setup or can be on demand during the data transfer phase. In the first case, the delay for each packet is the same; in the second case, each packet may encounter different delays. There is one big advantage in a virtual-circuit network even if resource allocation is on demand. The source can check the availability of the resources, without actually reserving it. Consider a family that wants to dine at a restaurant. Although the restaurant may not accept reservations (allocation of the tables is on demand), the family can call and find out the waiting time. This can save the family time and effort.

Delay in Virtual-Circuit Networks

In a virtual-circuit network, there is a one-time delay for setup and a one-time delay for teardown. If resources are allocated during the setup phase, there is no wait time for individual packets. Below Figure shows the delay for a packet traveling through two switches in a virtual-circuit network.

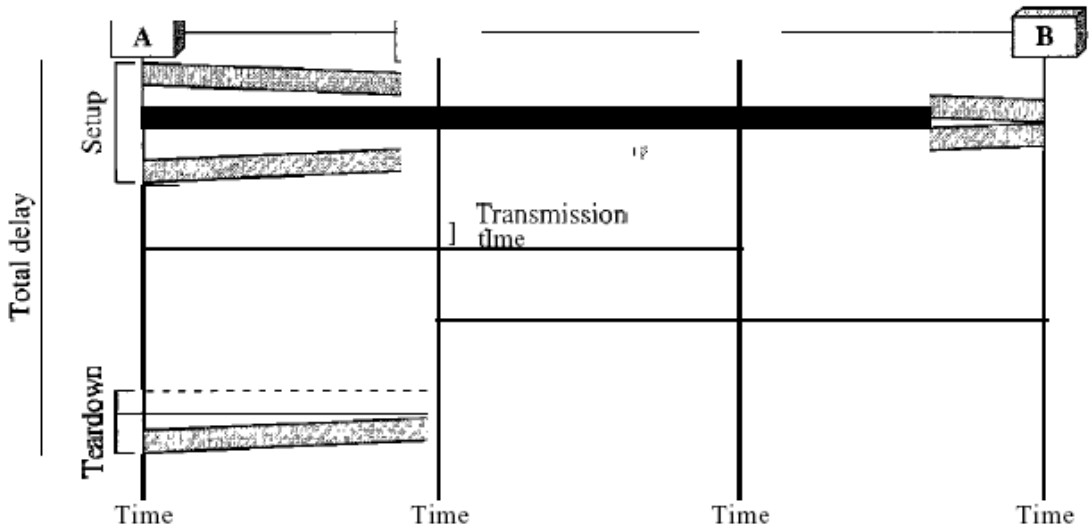


Fig: Delay in a virtual-circuit network

The packet is traveling through two switches (routers). There are three transmission times *(3T),* three propagation times (3't), data transfer depicted by the sloping lines, a setup delay (which includes transmission and propagation in two directions), and a teardown delay (which includes transmission and propagation in one direction). We ignore the processing time in each switch. The total delay time is

Total delay = *3T*+ 3't + setup delay + teardown delay

1. What are the functions of MAC?

MAC sub layer resolves the contention for the shared media. It contains 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.

2. What are the functions of LLC?

The IEEE project 802 models take the structure of an HDLC frame and divides it into 2 sets of functions. One set contains the end user portion of the HDLC frame – the logical address, control information, and data. These functions are handled by the IEEE 802.2 logical link control (LLC) protocol.

3. What is Ethernet?

Ethernet is a multiple-access network, meaning that a set of nodes send and receive frames over a shared link.

4. Define the term carrier sense in CSMA/CD?

All the nodes can distinguish between idle and a busy-link and "collision detect" means that a node listens as it transmits and can therefore detect when a frame it is transmitting has interfered (collided) with a frame transmitted by another node.

5. Define Repeater?

A repeater is a device that forwards digital signals, much like an amplifier forwards analog signals. However, no more than four repeaters may be positioned between any pairs of hosts, meaning that an Ethernet has a total reach of only 2,500m.

6. Define collision detection?

In Ethernet, all these hosts are competing for access to the same link, and as a consequence, they are said to be in the same collision detection.

7. Why Ethernet is said to be a I-*persistent* protocol?

An adaptor with a frame to send transmits with probability '1 'whenever a busy line goes idle.

8. What is exponential back off?

Once an adaptor has detected a collision and stopped its transmission, it waits a certain amount of time and tries again. Each time it tries to transmit but fails, the adaptor doubles the amount of time it waits before trying again. This strategy of doubling the delay

interval between each transmission attempt is a general technique known as exponential back off.

9. What is token holding time (THT)?

It defines that how much data a given node is allowed to transmit each time it possesses the token or equivalently, how long a given node is allowed to hold the token.

10. What are the two classes of traffic in FDDI?

- Synchronous
- Asynchronous

11.What is the use of Switch?

It is used to forward the packets between shared media LANs such as Ethernet. Such switches are sometimes known by the obvious name of LAN switches.

12.What are the functions of LLC?

The IEEE project 802 model takes the structure of an HDLC frame and divides itinto 2 sets of functions. One set contains the end user portion of the HDLC frame - the logical address, control information, and data. These functions are handled by the IEEE802.2 logical link control (LLC) protocol.

1 3 . What are the functions of MAC?

MAC sub layer resolves the contention for the shared media. It contains 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.

14.What are the goals in mind of IEEE 802 committee?

IEEE 802 committee has few goals in mind, namely

- To promote compatibility
- Implementation with minimum efforts
- Accommodate diverse applications

15. List the functions performed by the physical layer of 802.3 standard?

Functions of physical layer are:

i) Data encoding/decoding (To facilitate synchronization and efficient transfer of signal through the medium).
ii) Collision detection (It detects at the transmit side)
iii) Carrier sensing (Channel access senses a carrier on the channel at both the transmit and receive sides)
iv) Transmit/receive the packets (Frame transmitted to all stations connected to the channel)
v) Topology and medium used (Mediums are co-axial cable, twisted pair and fiber optic cable)

16. Why do you require a limit on the minimum size of Ethernet frame?

To detect collision, it is essential that a sender continue sending a frame and at the same time receives another frame sent by another station. Considering maximum

delay with five Ethernet segments in cascade, the size of frame has been found to be 64 bytes such that the above condition is satisfied.

17.What are the different types of cabling supported by Ethernet standard?

Ans. Types of cabling are:

i) 10 BASE 5 - Maximum cable length is 500 meters using 4" diameter coaxial cable.

ii) 10 BASE 2 - Maximum cable length is 185 meters using 0.25" diameter CATV cable.

iii) 10 BASE T - Maximum cable length is 100 meters using twisted-pair cable (CAT-3 UTP).

iv) 10 BASE FL - Maximum cable length is 2 Km using multimode fiber optic cable (125/62.5 micrometer).

18.What is the advantage of token passing protocol over CSMA/CD protocol?

Ans. Advantage of token passing protocol over CSMA/CD protocol:

The CSMA/CD is not a deterministic protocol. A packet may be delivered after many (up to 15) collisions leading to long variable delay. An unfortunate packet may not get delivered at all. This feature makes CSMA/CD protocol unsuitable for real-time applications. On the other hand, token passing protocol is a deterministic approach, which allows a packet to be delivered within a known time frame. It also allows priority to be assigned to packets. These are the two key advantages of token passing protocol over CSMA/CD protocol.

19. What are the drawbacks of token ring topology?

Ans. Token ring protocol cannot work if a link or a station fails. So, it is vulnerable to link and station failure.

20.How the reliability of token ring topology can be improved?

Ans. Reliability of the ring network can be improved by implementing the ring topology using a wiring concentrator. This allows not only to detect fault, but also to isolate the faulty link/station with the help of a bypass relay.

21.What role the active token monitor performs?

Ans. Token ring is maintained with the help of active token monitor. Any one of the stations has the capability to act as active token monitor, but at a particular instant only one acts as active token monitor. It monitors various error situations such as multiple token, orphan packet, etc, and takes appropriate action to come out of the error situation.

22.In what way the MAC protocol of FDDI differs from that of token ring?

Ans: In the frame format of FDDI protocol, preamble is eight bytes instead of one byte in token ring. Also token has one additional byte. FDDI can have multiple frames simultaneously, which cannot be present in token ring. Here, the access method is timed token passing. Multiple frames can be transmitted after capturing a token.First, the entire token is captured and then the data frames are introduced, whereas token ring follows token passing protocol and beginning of token is

converted to the header of a frame.In case of token ring token is released after receiving the acknowledgement (as the data frame returns after circulating the ring). On the other hand, in case of FDDI, token is released immediately after sending data frame, which is known as early token release.

23. How FDDI offers higher reliability than token ring protocol?

Ans: Token ring protocol is applicable in a single ring. Disadvantage of this protocol is that, if one segment of wires fails or a node fails, the protocol cannot work. To increase reliability, ***dual counter ring topology*** used in FDDI protocol, where there are two rings, called primary ring and secondary ring. In case of failure of a node or a fiber link, the ring is restored the by wrapping up the primary ring to the secondary ring. Further improvement in reliability can achieve by using ***dual ring of trees*** and ***dual homing*** mechanism. It will provide multiple paths and if one path fails, another path will be available for passing token or data.

24. What are the functionalities of a Optical Bypass Switch?

Ans: An *optical bypass switch* provides continuous dual-ring operation if a device on the dual ring fails. This is used both to prevent ring segmentation and to eliminate failed stations from the ring. The optical bypass switch performs this function using optical mirrors that pass light from the ring directly to the DAS (dual-attachment station) device during normal operation. If a failure of the DAS device occurs, such as a power-off, the optical bypass switch will pass the light through itself by using internal mirrors and thereby will maintain the ring's integrity. When using the OB, you will notice a tremendous digression of your network as the packets are sent through the OB unit.

25. What are the functionalities provided by SMT standard?

Ans: The Station Management (SMT) standard provides services that monitor and control a FDDI station. SMT include facilities for connection management, node configuration, recovery from error condition, and encoding of SMT frames.

26. Describe various fields in frame format of FDDI?

Ans: Let us have a look at the various fields:
SD: The first byte, after the preamble, of the field is the frame's starting flag. As in Token ring these bits are replaced in physical layer by the control codes.
FC: it identifies the frame type i.e. token or a data frame.
Address: the next 2 fields are destination and source addresses. Each address consists of 2-6 bytes.
Data: Each data frame carries up to 4500 bytes.
FCS: FDDI uses the standard IEEE four-byte cyclic redundancy check.
ED: this field consists of half a byte in data frame or a full byte in token frame. This represents end of the Token.
FS: FDDI FS field is similar to that of Token Ring. It is included only in data/Command frame and consists of one and a half bytes.