Syllabus

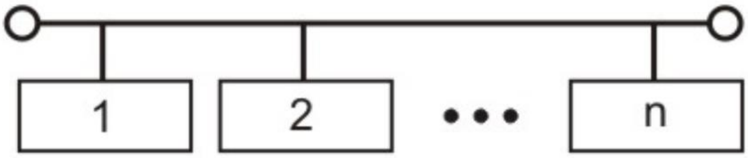
LANS and MANS: Project 802, Ethernet, Token Bus, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet, DQDB, SMDS, PPP

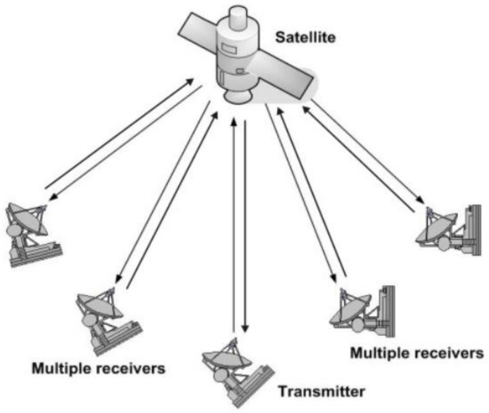
Computer networks can be broadly categorized into two types based on transmission technologies:

- Broadcast Networks.
- Point-to-Point Networks.

Broadcast Networks

Broadcast network have a single communication channel that is shared by all the machines on the network as shown in Figs. (A) and (B). All the machines on the network receive short messages, called packets in certain contexts, sent by any machine. An address field within the packet specifies the intended recipient. Upon receiving a packet, machine checks the address field. If packet is intended for itself, it processes the packet; if packet is not intended for itself it is simply ignored.



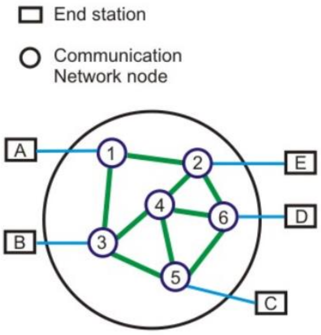


This system generally also allows possibility of addressing the packet to all destinations (all nodes on the network). When such a packet is transmitted and received by all the machines on the network. This mode of operation is known as ***Broadcast Mode***. Some Broadcast systems also supports transmission to a sub-set of machines, something known as ***Multicasting***.

Point-to-Point Networks

A network based on point-to-point communication is shown in Fig. (C). The end devices that wish to communicate are called *stations*. The switching devices are called *nodes*. Some Nodes connect to other nodes and some to attached stations. It uses FDM or

TDM for node-to-node communication. There may exist multiple paths between a source-destination pair for better network reliability. The switching nodes are not concerned with the contents of data. Their purpose is to provide a switching facility that will move data from node to node until they reach the destination.



As a general rule (although there are many exceptions), smaller, geographically localized networks tend to use broadcasting, whereas larger networks normally use are point-to-point communication.

Classification based on Scale

Alternative criteria for classifying networks are their scale. They are divided into Local Area (LAN), Metropolitan Area Network (MAN) and Wide Area Networks (WAN).

Local Area Network (LAN)

LAN is usually privately owned and links the devices in a single office, building or campus of up to few kilometers in size. These are used to share resources (may be hardware or software resources) and to exchange information. LANs are distinguished from other kinds of networks by three categories: their size, transmission technology and topology.
LANs are restricted in size, which means that their worst-case transmission time is bounded and known in advance. Hence this is more reliable as compared to MAN and WAN. Knowing this bound makes it possible to use certain kinds of design that would not otherwise be possible. It also simplifies network management.

LAN typically used transmission technology consisting of single cable to which all machines are connected. Traditional LANs run at speeds of 10 to 100 Mbps (but now much higher speeds can be achieved). The most common LAN topologies are bus, ring and star.

Metropolitan Area Networks (MAN)

MAN is designed to extend over the entire city. It may be a single network as a cable TV network or it may be means of connecting a number of LANs into a larger network so that resources may be shared. For example, a company can use a MAN to connect the LANs in all its offices in a city. MAN is wholly owned and operated by a private company or may be a service provided by a public company.

The main reason for distinguishing MANs as a special category is that a standard has been adopted for them. It is **DQDB** (Distributed Queue Dual Bus) or IEEE 802.6.

Wide Area Network (WAN)

WAN provides long-distance transmission of data, voice, image and information over large geographical areas that may comprise a country, continent or even the whole world. In contrast to LANs, WANs may utilize public, leased or private communication devices, usually in combinations, and can therefore span an unlimited number of miles.

A WAN that is wholly owned and used by a single company is often referred to **as *enterprise network.***

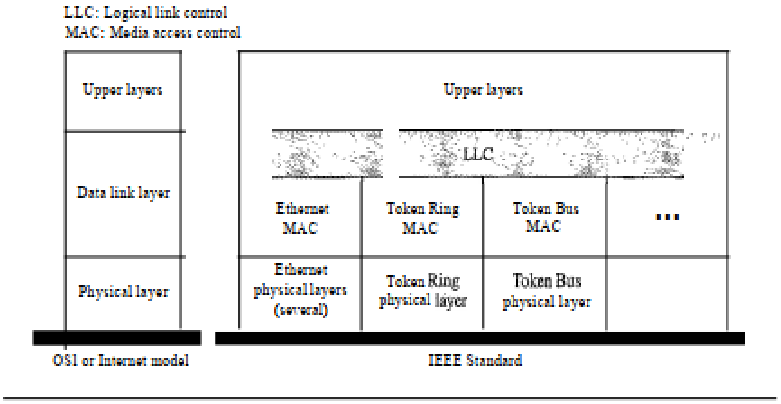
Project 802

In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers.

Project 802 does not seek to replace any part of the OSI or the Internet model. Instead, it is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.

The standard was adopted by the American National Standards Institute (ANSI). In 1987, the International Organization for Standardization (ISO) also approved it as an international standard under the designation ISO 8802.

The relationship of the 802 Standard to the traditional OSI model is shown in Figure below. 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.



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 (lot Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (l Gbps), and Ten-Gigabit Ethernet (l0 Gbps).

On a regular Ethernet segment, all stations share the available bandwidth of 10 Mb/s. With the increase in traffic, the number of packet collisions goes up, lowering the overall throughput. In such a scenario, there are two basic approaches to increase the bandwidth. One is to replace the Ethernet with a higher speed version of Ethernet. Use of Fast Ethernet operating at 100 Mb/s and Gigabit Ethernet operating at 1000 Mb/s belong to this category. This approach requires replacement of the old network interface cards (NICs) in each station by new ones.

The other approach is to use Ethernet switches (let us call it switched Ethernet approach) that use a high-speed internal bus to switch packets between multiple (8 to 32) cable segments and offer dedicated 10 Mb/s bandwidth on each segment/ports. In this approach, there is no need to replace the NICs; replacement of the hub by a switch serves the purpose.

Switched Ethernet

Switched Ethernet gives dedicated 10 Mb/s bandwidth on each of its ports. On each of the ports one can connect either a thick/thin segment or a computer. In Ethernet (IEEE 802.3) the topology, though physically is star but logically is BUS, i.e. the collision domain of all the nodes in a LAN is common. In this situation only one station can send the frame. If more than one station sends the frame, there is a collision.

In Switched Ethernet, the collision domain is separated. The hub is replaced by a switch, which functions as a fast bridge. It can recognize the destination address of the received frame and can forward the frame to the port to which the destination station is connected. The other ports are not involved in the transmission process. The switch can receive another frame from another station at the same time and can route this frame to its own final destination. In this case, both the physical and logical topologies are star.

There are two possible forwarding techniques that can be used in the implementation of Ethernet switches: *store-and-forward* and *cut-through*. In the first case, the entire frame is captured at the incoming port, stored in the switch's memory, and after an address lookup to determine the LAN destination port, forwarded to the appropriate port. The lookup table is automatically built up. On the other hand, a cut-through switch begins to transmit the frame to the destination port as soon as it decodes the destination address from the frame header.

Store-and-forward approach provides a greater level of error detection because damaged frames are not forwarded to the destination port. But it introduces longer delay of about 1.2 msec for forwarding a frame and suffers from the chance of loosing data due to reliance on buffer memory. The **cut-through switches**, on the other hand, has reduced latency but has higher switch cost.

The throughput can be further increased on switched Ethernet by using fullduplex technique, which uses separate wire pairs for transmitting and receiving. Thus a station can transmit and receive simultaneously, effectively doubling the throughput to 20 Mb/s on each port.

Fast Ethernet

The 802.u or the fast Ethernet, as it is commonly known, was approved by the IEEE 802 Committee in June 1995. It may not be considered as a new standard but an addendum to the existing 802.3 standard. The fast Ethernet uses the same frame format, same CSMA/CD protocol and same interface as the 802.3, but uses a data transfer rate of 100 Mb/s instead of 10 Mb/s. However, fast Ethernet is based entirely on 10-Base-T, because of its advantages (Although technically 10-BASE-5 or 10-BASE-2 can be used with shorter segment length).

Fortunately, the Ethernet is designed in such a way that the speed can be increased if collision domain is decreased. The only two changes made in the MAC layer are the data rate and the collision domain. The data rate is increased by a factor of 10 and collision domain is decreased by a factor of 10. To increase the data rate without changing the minimum size of the frame (576 bits or 76 bytes in IEEE 802.3), it is necessary to decrease the round-trip delay time. With the speed of 100Mbps the roundtrip time reduce to 5.76 microseconds (576 bits/100 Mbps; which was 57.6 microsecond for 10Mbps Normal Ethernet). This means that the collision domain is decreased 10 fold from 2500 meters (in IEEE802.3) to 250 meters (fast Ethernet).

IEEE has designed two categories of Fast Ethernet: 100Base-X and 100Base-T4.100Base-X uses two-wire interface between a hub and a station while 100Base-T4 uses four-wire interface. 100-Base-X itself is divided into two: 100Base-TX and 100base-FX.

100 BASE-T4:

This option is designed to avoid overwriting. It is used for half-duplex communication using four wire-pairs of the existing category 3 UTP cables, which are already available for telephone services in homes/offices. Two of four pairs are bi-directional; other two are unidirectional. This means that there are 3 pairs to be used for carrying data, in each direction (2 bi-directional and 1 uni-directional). Because 100Mbps data cannot be handled by voice-grade UTP, this specification splits the 100 Mbps flow into three 33.66 Mbps flows.

100 BASE TX:

This option uses two pairs of category 5 UTP or two shielded twisted-pair (STP) cable to connect a station to hub as shown in Fig. 5.6.4. One pair is used to carry frames from the hub to the station and other to carry frames from station to hub. It uses 4B/5B encoding to handle 100 Mbps using NRZ-I signaling. The distance between station and hub should be less than 100 meters.

100 BASE FX:

This option uses two Fiber optic cables, one carry frames from station to hub and other from hub to station. The encoding is using 4B/5B and it uses NRZI signaling. The distance between station and hub should be less than 2000 meters.

Gigabit Ethernet

In March 1996, the IEEE 802.3 committee approved the 802.3z Gigabit Ethernet Standardization project. At that time as many as 54 companies expressed their intent to participate in the standardization project. The Gigabit Ethernet Alliance was formed in May 1996 by 11 companies. The Alliance represents a multi-vendor effort to provide open and inter-operable Gigabit Ethernet products. The objectives of the alliance are:

- Supporting extension of existing Ethernet and Fast Ethernet technology in response to demand for higher network bandwidth.

- Developing technical proposals for the inclusion in the standard.
- Establishment of inter-operability test procedures and processes.

Gigabit Ethernet is not simply a straight Ethernet running at 1 Gb/s. In fact, the ways it differs from its predecessors may be more important than its similarities. Some of the important differences are highlighted below.

- The cabling requirement of gigabit Ethernet is very different. The technology is based on fiber optic cable. Multi-mode fiber is able to transmit at gigabit rate to at least 580 meters and with single-mode runs exceeding 3 km. Fiber optic cabling is costly. In order to reduce the cost of cabling, the 802.3z working group also proposed the use of twisted pair or cable or coaxial cable for distances up to 30 meters.
- Gigabit Ethernet also relies on a modified MAC layer. At gigabit speed, two stations 200 meters apart will not detect a collision, when both simultaneously send 64-byte frames. This inability to detect collision leads to network instability. A mechanism known as *carrier extension* has been proposed for frames shorter than 512 bytes. The number of repeater hops is also restricted to only one in place of two for 100 Base-T.
- Flow Control is a major concern in gigabit Ethernet because of buffer overflow and junked frames in heavily loaded condition. The solution proposed by IEEE subcommittee is the 802.3x. The X-on/X-off protocol works over any full-duplex Ethernet, fast Ethernet or gigabit Ethernet link. When a switch buffer is close to capacity, the receiving device signals the sending station and tells it to stop transmitting until the buffer becomes empty.
- Finally, one important feature, which Ethernet technology lacks, is the Quality of Service (QoS). The gigabit Ethernet is a connectionless technology that transmits variable length frames. As such, it simply cannot guarantee that the real-time packets get the preferential treatment they require.

Token Ring – IEEE 802.5

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.

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.

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.
- 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.

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.

Token Bus (IEEE 802.4)

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. 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.

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 include:

The FDDI standard divides transmission functions into 4 protocols: physical medium dependent (PMD), Physical (PHY), media access control (MAC) and Logical link control (LLC).

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.

The basic topology for FDDI is *dual counter rotating rings:* one transmitting clockwise and the other transmitting counter clockwise. 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. 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.

Point-to-Point Protocol

Although HDLC is a general protocol that can be used for both point-to-point and multipoint configurations, one of the most common protocols for point-to-point access is the Point-to-Point Protocol (PPP). Today, millions of Internet users who need to connect their home computers to the server of an Internet service provider use PPP. The majority of these users have a traditional modem; they are connected to the Internet through a telephone line, which provides the services of the physical layer. But to control and manage the transfer of data, there is a need for a point-to-point protocol at the data link layer. PPP is by far the most common. PPP provides several services:

I. PPP defines the format of the frame to be exchanged between devices.
II. PPP defines how two devices can negotiate the establishment of the link and the exchange of data.
III. PPP defines how network layer data are encapsulated in the data link frame.
IV. PPP defines how two devices can authenticate each other.
V. PPP provides multiple network layer services supporting a variety of network layer protocols.
VI. PPP provides connections over multiple links.
VII. PPP provides network address configuration. This is particularly useful when a home user needs a temporary network address to connect to the Internet.