4...

Wired and Wireless LANs

Objectives...

- To learn about IEEE Standards
- To study Standard Ethernet, Fast Ethernet, Gigabit Ethernet, Ten-Gigabit Ethernet
- To know Backbone Networks and its types
- To get knowledge of Virtual LANs Membership and IEEE standards advantages
- To learn about Wireless LAN
- To get knowledge of IEEE 802.11 Architecture and Bluetooth Architecture (Piconet Scatternet)

4.1 IEEE STANDARDS

- IEEE 802.3 is a collection of IEEE standards defining the physical layer, and the media access control (MAC) sublayer of the data link layer, of wired Ethernet. This is generally a LAN technology with some WAN applications. Physical connections are made between nodes and/or infrastructure devices (hubs, switches, routers) by various types of copper or fiber cable.
- 802.3 is a technology that can support the IEEE 802.1 network architecture.
- The maximum packet size is 1518 bytes, although to allow the Q-tag for Virtual LAN and priority data in 802.3ac it is extended to 1522 bytes. If the upper layer protocol submits a protocol data unit (PDU) less than 46 bytes, 802.3 will pad the data field to achieve the minimum 46 bytes. The minimum frame size will then always be of 64 bytes.
- Although it is not technically correct, the terms packet and frame are often used interchangeably. The ISO/IEC 8802-3 and ANSI/IEEE 802.3 standards refer to MAC sub-layer frames consisting of the destination address, the source address,

length/type, data payload, and frame check sequence (FCS) fields. The preamble and start frame delimiter (SFD) are (usually) together considered a header to the MAC frame. This header and the MAC frame constitute a packet.pad

- The original Ethernet is called Experimental Ethernet today. It was developed by Robert Metcalfe in 1972 (patented in 1978) and was based in part on the wireless ALOHA net protocol. It is not in use anywhere, but is thought to be the only Ethernet by some purists. The first Ethernet that was generally used outside Xerox was the DIX Ethernet. However, as DIX Ethernet was derived from Experimental Ethernet, and as many standards have been developed that are based on DIX Ethernet, the technical community has accepted the term Ethernet for all of them. Therefore, the term Ethernet can be used to name networks using any of the following standardized media and functions.
- In the last several years, the demand on the network has increased drastically. The old 10Base5 and 10Base2 Ethernet networks were replaced by 10BaseT hubs, allowing for greater manageability of the network and the cable plant. As applications increased the demand on the network, newer, high-speed protocols such as FDDI and ATM became available. However, in the last two years, Fast Ethernet has become the backbone of choice because its simplicity and its reliance on Ethernet. The primary goal of Gigabit Ethernet is to build on that topology and knowledge base to build a higher-speed protocol without forcing customers to throw away existing networking equipment.
- The standards body working on Gigabit Ethernet is the IEEE 803.2z Task Force, which has established an aggressive timetable for development of the Gigabit Ethernet standard. The possibility of a Gigabit Ethernet Standard was raised in mid-1995 after the final ratification of the Fast Ethernet Standard. By November 1995 there was enough interest to form a high-speed study group. This group met at the end of 1995 and several times during early 1996 to study the feasibility of Gigabit Ethernet. The meetings grew in attendance, reaching 150 to 200 individuals. Numerous technical contributions were offered and evaluated.
- In July 1996, the 802.3z Task Force was established with the charter to develop a standard for Gigabit Ethernet. Basic concept agreement on technical contributions for the standard was achieved at the November 1996 IEEE meeting. The first draft of the standard was produced and reviewed in January 1997; the final standard was approved in June 1998.
- CSMA/CD (Carrier Sense Multiple Access/Collision Detection) based LAN proposed by the IEEE 802.3 subcommittee, commonly known as Ethernet.
- In this section we shall discuss Ethernet (CSMA/CD), Token bus, Token ring based LANs proposed by the IEEE 802. 3, IEEE 802.4 and IEEE 802.5, subcommittees.

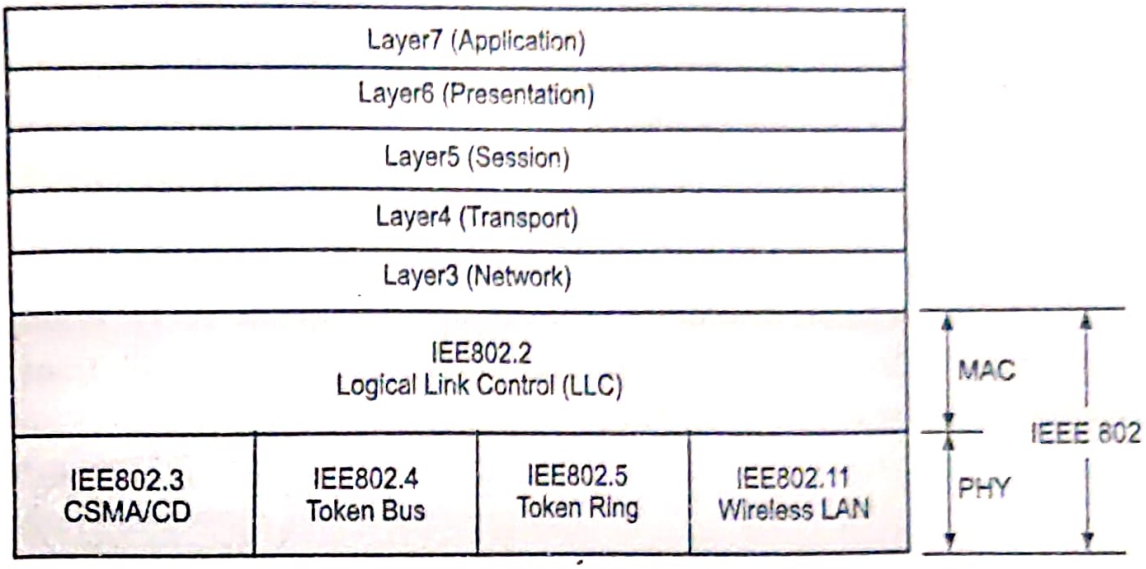


Fig. 4.1: IEEE Standards in OSI Layer

4.1.1 IEEE Standard 802.3 (Ethernet)

- The Institute for Electrical and Electronic Engineers developed an Ethernet standard known as IEEE Standard 802.3. Ethernet is the most widely-installed Local Area Network technology.
- This standard defines rules for configuring an Ethernet network and also specifies how the elements in an Ethernet network interact with one another. By following to the IEEE standard, network equipment and network protocols can communicate efficiently.
- An Ethernet LAN typically uses coaxial cable or twisted pair wires. It provides speeds up to 10 Megabits per second (10 Mbps).
- The devices connected to the LAN compete for access using CSMA/CD protocol.

Example:

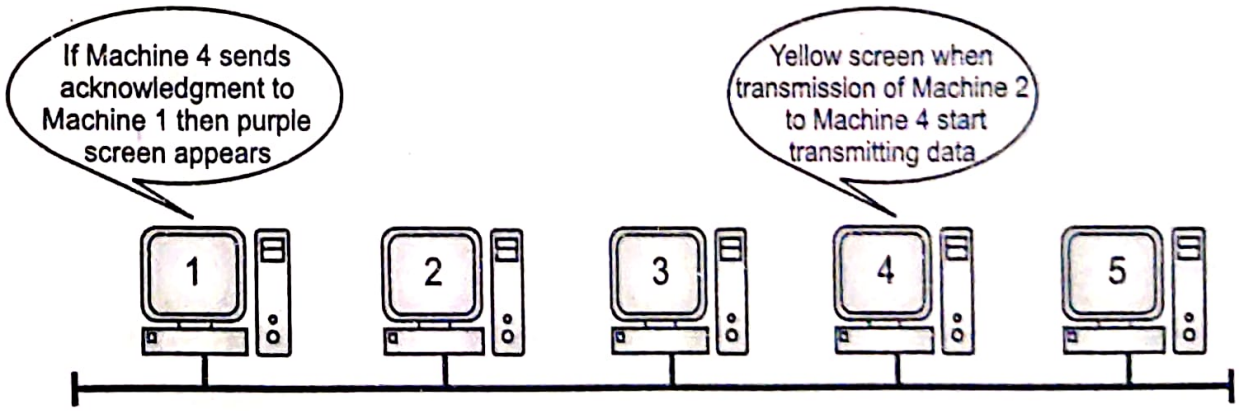


Fig. 4.2: Ethernet Transmission

- In above fig., Machine 2 wants to send a message to Machine 4, but first it listens to the cable to make sure that no one else is using the network.

- If it is all clear it starts to transmit its data on to the network (represented by the yellow screens). Each packet of data contains the destination address, the senders address and the data to be transmitted.
- The signal moves down the cable and is received by every machine on the network but because it is only addressed to number 4, the other machines ignore it.
- Machine 4 then sends a message back to number 1 acknowledging receipt of the data (represented by the purple screens).
- As we stated before, there is a possibility of two machines try to transmit simultaneously over the cable. The result can be observed in the Fig. 4.3.

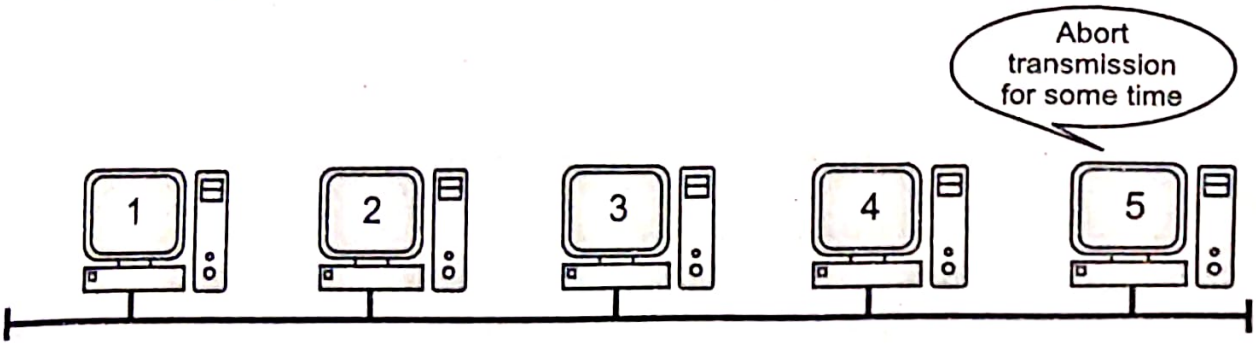


Fig. 4.3: Abort Transmission

- What happens is that Machine 2 and 5 decide to transmit at the same time. The packets collide and each machine has the ability to detect the collision and immediately abort transmission. Then they wait for random period of time and transmit again.

Protocols:

1. CSMA/CD:

- Carrier Sense Multiple Access with Collision Detection is a protocol used to sense whether a medium is busy before transmission but is the ability to detect whether a transmission has collided with another.
- CSMA/CD is the protocol used in Ethernet networks to ensure that only one network node is transmitting on the network wire at any one time.
- Carrier Sense means that every Ethernet device listens to the Ethernet wire before it attempts to transmit. If the Ethernet device senses that another device is transmitting, it will wait to transmit.
- Multiple Access means that more than one Ethernet device can be sensing (listening and waiting to transmit) at a time.
- Collision Detection means that when multiple Ethernet devices accidentally transmit at the same time, they are able to detect this error.
- The collision detection in CSMA/CD that was mentioned earlier functions when the interfaces start relaying out signals simultaneously. This can happen because the

transmission of data is not instantaneous. In other words, if the Ethernet system gets clogged up, the CSMA/CD will take the necessary steps to unblock it.

- The collision detector of the CSMA/CD functions by releasing its own signal. In some Ethernet systems it is the 24 mA.

Working of CSMA/CD:

- A method called CSMA/CD was used to send data over shared single coaxial cable connected to all computers on a network.
- In this method, the computer terminals (also called as stations) transmit the data over cable whenever the cable is idle, if more than one station transmits at same time and if they collide, the transmission will be stopped by such stations. They will wait for some random time and restart transmission.
- The concept of sharing single cable or wire between multiple stations was used for first time in Hawaiian Islands. It was called ALOHA systems; built to allow radio communication between machines located at different places in Hawaiian Islands. Later Xerox PARC built a 2.94 mbps CSMA/CD system to connect multiple personal computers on a single cable. It was named as Ethernet.
- Ethernet or IEEE 802.3 standards only define MAC (Data link) and Physical layer of standard OSI model.

2. CSMA/CA:

- CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) is a protocol for carrier transmission in 802.11 networks.
- Unlike CSMA/CD which deals with transmissions after a collision has occurred, CSMA/CA acts to prevent collisions before they happen.
- In CSMA/CA, as soon as a node receives a packet that is to be sent, it checks to be sure the channel is clear (no other node is transmitting at the time). If the channel is clear, then the packet is sent. If the channel is not clear, the node waits for a randomly chosen period of time, and then checks again to see if the channel is clear.
- This period of time is called the back-off factor, and is counted down by a back-off counter. If the channel is clear when the back-off counter reaches zero, the node transmits the packet. If the channel is not clear when the back-off counter reaches zero, the back-off factor is set again, and the process is repeated.

4.1.2 IEEE Standard 802.4 (Token Bus)

- IEEE 802.4 standard evolved from the needs of companies like General Motors implementing terminals for factory automation.
- 802.3 was not suitable for them as a station in ethernet has to wait for a long time to send a frame in worst case. 802.3 frames do not have priorities which makes important frames waiting for unimportant frames.

- A token bus system is a medium access control technique for bus/tree stations form a logical ring around which a token is passed.
- A station receiving the token may transmit data and then must pass the token on to next station in the ring.
- Though it is similar to token ring it does not implement the ring physically as it has drawback of getting entire network down in case one terminal is down.
- If there are n stations the token bus network and TP seconds are required to send a frame. It will take not more than n TP seconds to get a turn for a station.

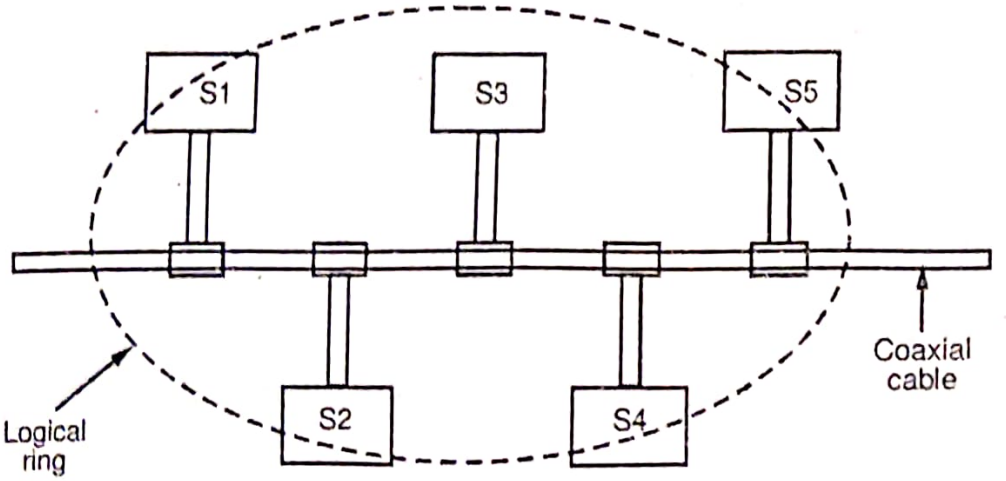


Fig. 4.4: Token Bus

- The stations can be configured so that they can be a part of the logical ring or may opt out of the ring.
- Initially highest number station gets the token. Then it passes the token to its neighbour (right or left).
- Token thus moves around the ring with token holder permitted send the frame.
- If station has no data it must pass the token to next station.
- The 85 ohm broadband cable is used at physical layer.

Frame Format of Token Bus Protocol:

- The token bus frame format is shown in Fig. 4.5

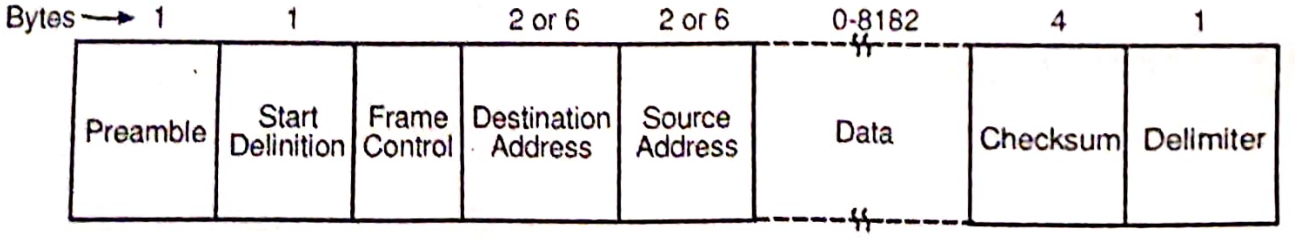


Fig. 4.5: Token Bus (802.4) Frame Format

- Fields of 802.4 (token bus) frame format are listed below:
  1. **Preamble:** It is used to synchronize the receiver's clock as in case of Ethernet (802.3).
  2. **Starting and ending delimiter:** These fields are for frame synchronization mark the frame boundaries.
  3. **Frame control:** This field is used to indicate whether the frame is data frame or control frame. For data frames, it carries frame's priority. Token bus defines four classes of priorities 0, 2, 4, and 6 for traffic with 0 lowest and 6 highest. Each station puts the data as per their priority in the substations. Each substation with different priority maintains its own queue of frames to be transmitted. When token comes to a station, it is first given to the substation with priority 6, so that it can transmit the frames first, and then it is given to substation with priority 4 and so on. In this field, there can be indicator of whether destination is allowed to acknowledge the frame or not.

     In case of control, the frames have token passing and ring maintenance frames. They also manage the job of letting new stations enter the ring or existing ones to leave the ring.
  4. **Source address and destination address:** It is similar to 802.3. These fields are 2 byte or 6 byte long. But they should either all byte or 6 byte on source cable for all stations.
  5. **Data field:** It can be extended upto 8182 bytes when 2 byte address is used and 8174 bytes when 3 bytes address is used.
  6. **Checksum:** It is used to detect transmission errors. CRC polynomial as in 802.3 is used.

4.1.3 IEEE Standard 802.5 (Token Ring)

- The token ring protocol is the second most widely-used protocol on Local Area Networks (LANs) after Ethernet.
- The IEEE 802.5 token ring technology provides for data transfer rates of either 4 or 16 Mbps. It is a collection of individual point-to-point links, connecting each terminal, that happen to form a circle.
- Token Ring is formed by the nodes connected in ring format as shown in the Fig. 4.6.

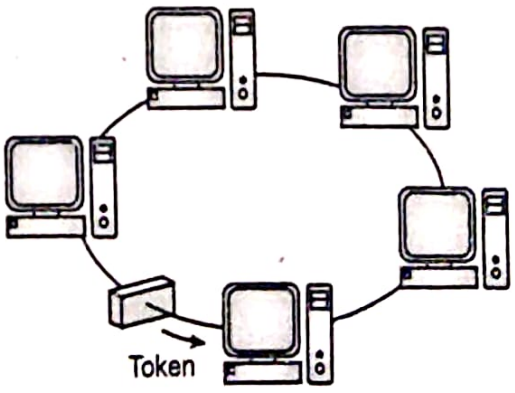


Fig. 4.6: Token Ring (802.5)

- The principle used in the token ring network is that a token is circulating in the ring and whichever node grabs that token will have right to transmit the data.
- Whenever, a station wants to transmit a frame it inverts a single bit of the 3-byte token which instantaneously changes it into a normal data packet. Because there is only one token, there can at most be one transmission at a time.
- Since, the token rotates in the ring it is guaranteed that every node gets the token within some specified time. So there is an upper bound on the time of waiting to grab the token so that starvation is avoided.
- There is also an upper limit of 250 on the number of nodes in the network. To distinguish the normal data packets from token (control packet) a special sequence is assigned to the token packet. When any node gets the token it first sends the data it wants to send, then recirculates the token.
- If a node transmits the token and nobody wants to send the data the token comes back to the sender. If the first bit of the token reaches the sender before the transmission of the last bit, then error situation arises. So to avoid this we should have: propagation delay + transmission of n-bits (1-bit delay in each node) > transmission of the token time.
- A station may hold the token for the token-holding time which is 10 ms unless the installation sets a different value. If there is enough time left after the first frame has been transmitted to send more frames, then these frames may be sent as well.
- After all pending frames have been transmitted or the transmission frame would exceed the token-holding time, the station regenerates the 3-byte token frame and puts it back on the ring.

Modes of Operation:

1. **Listen Mode:** In this mode the node listens to the data and transmits the data to the next node. In this mode there is a one-bit delay associated with the transmission.

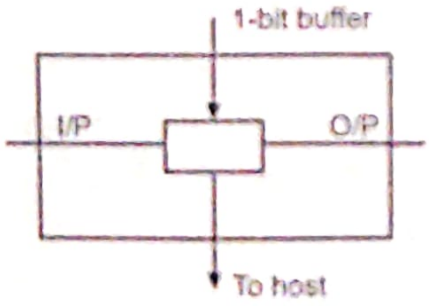


Fig. 4.7: Listen Mode

2. **Transmit Mode:** In this mode the node just discards the any data and puts the data onto the network.

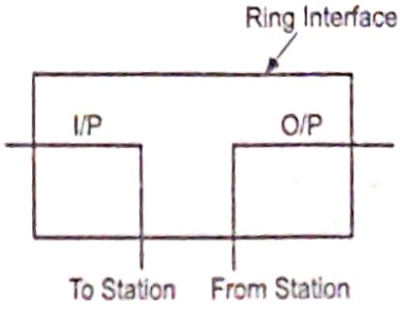


Fig. 4.8: Transmit Mode

3. **By-pass Mode:** When the node is down, By-pass mode is reached. Any data is just bypassed. There is no one-bit delay in this mode.

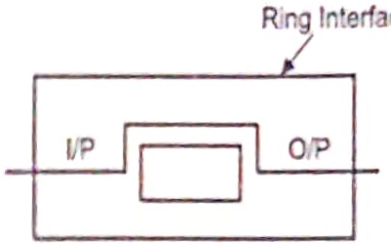


Fig. 4.9: By-pass Mode

Transactions of Token Ring:

- A special 'three-byte' frame pattern called a "token" circulates around the ring (See Fig. 4.10). A station wishing to transmit on the ring must seize the token.
- The station then alters one bit of the token which then becomes the first part of the normal data frame the station wishes to transmit.
- Only having one token on the ring means that only one station can transmit at a time. This solves the problem of contention and access to the common media.
- In the example, Machine 1 wants to send some data to Machine 4. It captures the token, writes its data and the recipient's address onto the Token (indicated by the yellow screen).
- The packet of data travels first to Machines 2 and 3 that read the address, realize it is not its own, and pass the token to Machine 4. This time it is the correct address and so number 4 stores the packet (represented by the yellow screen).
- Then Machine 4 sends an acknowledgement back to Machine 1 to say that it has received the packet (represented by the purple screen).
- Machines 5 and 6 forward the acknowledgement to Machine 1, who sent the original message.
- As soon as Machine 1 receives the acknowledgement (ACK) from machine 4 (indicated by the purple flashing screen) regenerates the free token back on to the ring ready for the next machine to use.

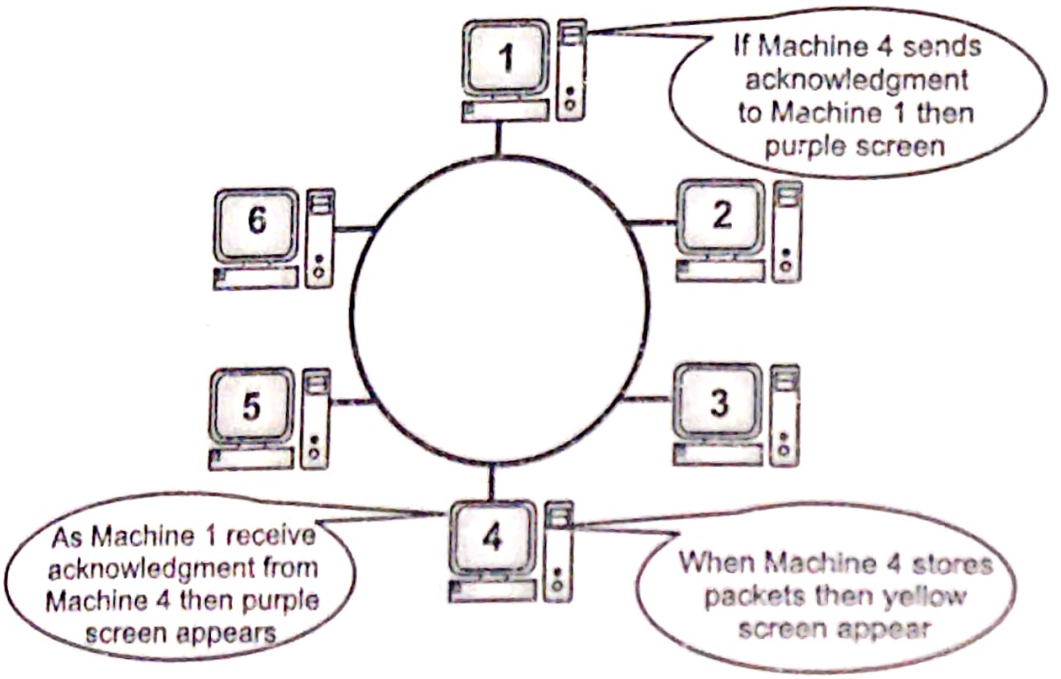


Fig. 4.10: Token Ring Transactions

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.

Fault-Management Mechanisms:

- Token Ring networks employ several mechanisms for detecting and compensating for network faults. For example, one station in the Token Ring network is selected to be the active monitor. This station, which potentially can be any station on the network, acts as a centralized source of timing information for other ring stations and performs a variety of ring-maintenance functions. One of these functions is the removal of continuously circulating frames from the ring. When a sending device fails, its frame may continue to circle the ring. This can prevent other stations from transmitting their own frames and essentially can lock up the network. The active monitor can detect such frames, remove them from the ring, and generate a new token.

- The IBM Token Ring network's star topology also contributes to overall network reliability. Because all information in a Token Ring network is seen by active MSAUs, these devices can be programmed to check for problems and selectively remove stations from the ring, if necessary.
- A Token Ring algorithm called beaconing detects and tries to repair certain network faults. Whenever a station detects a serious problem with the network (such as a cable break), it sends a beacon frame, which defines a failure domain. This domain includes the station reporting the failure, its Nearest Active Upstream Neighbor (NAUN), and everything in between. Beaconing initiates a process called autorecon figuration, in which nodes within the failure domain automatically perform diagnostics in an attempt to reconfigure the network around the failed areas. Physically, the MSAU can accomplish this through electrical reconfiguration.

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.
- Both formats are shown in Fig. 4.11.

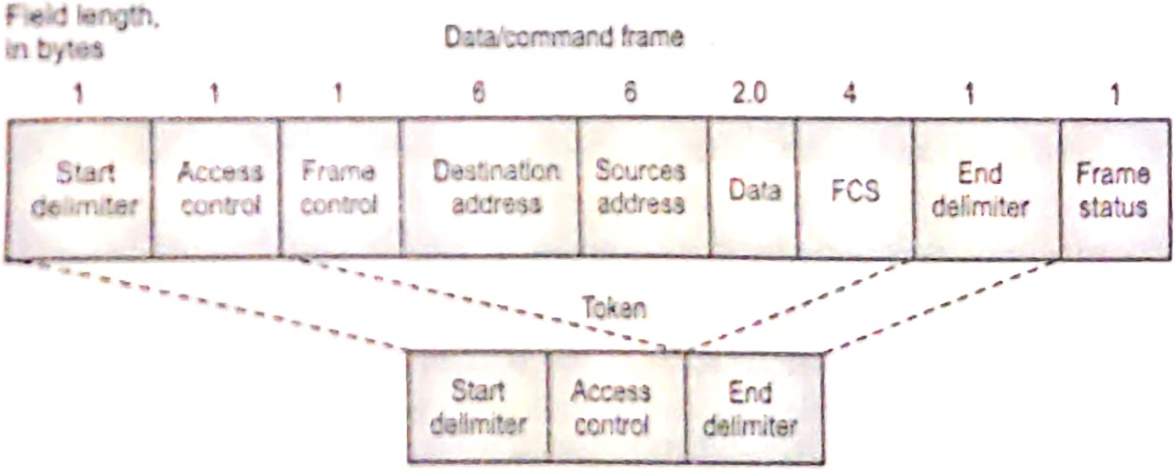


Fig. 4.11: IEEE 802.5 and token ring specify tokens and data/command frames

(i) Token Frame Fields:

- The three token frame fields illustrated in Fig. 4.11 are summarized in the descriptions that follow:

1. **Start delimiter:** This field 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.

2. **Access-control byte:** This field 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).
3. **End delimiter:** This field 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.

(ii) 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 Fig. 4.11 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:** This field indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.
  - **Destination and source addresses:** This field consists of two 6-byte address fields that identify the destination and source station addresses.
  - **Data:** This field 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):** This field is filled 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:** This field is a 1-byte field terminating a command/data frame. The Frame Status field includes the address-recognized indicator and frame-copied indicator.

4.2 STANDARD ETHERNET (S-19, W-22, S-23)

- The Standard Ethernet defines several physical layer implementations; four of the most Common.

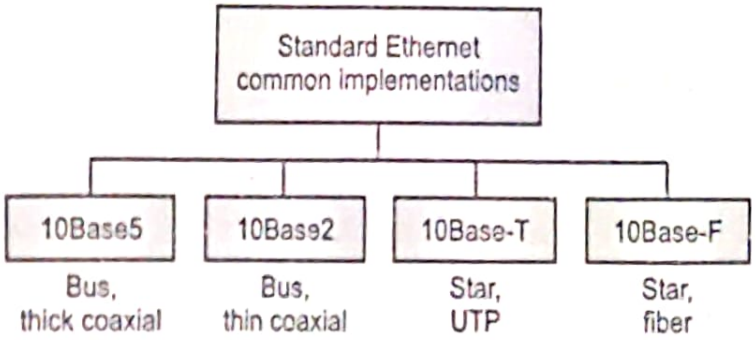


Fig. 4.12: Categories of Standard Ethernet

Encoding and Decoding:

- All standard implementations use digital signalling (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. Manchester encoding is self-synchronous, providing a transition at each bit interval. Fig. 4.13 shows the encoding scheme for Standard Ethernet.

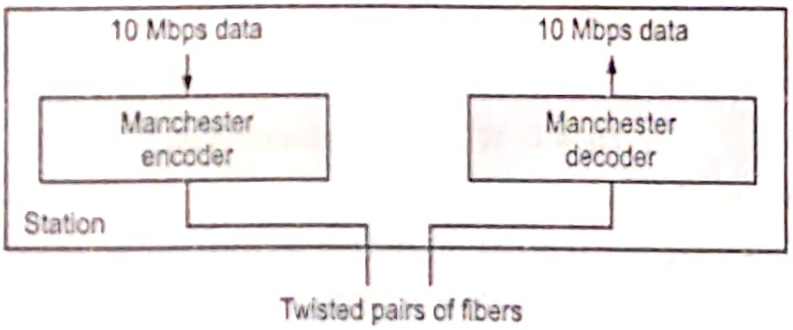


Fig. 4.13: Encoding in a Standard Ethernet implementation

a. 10Base5: Thick Ethernet

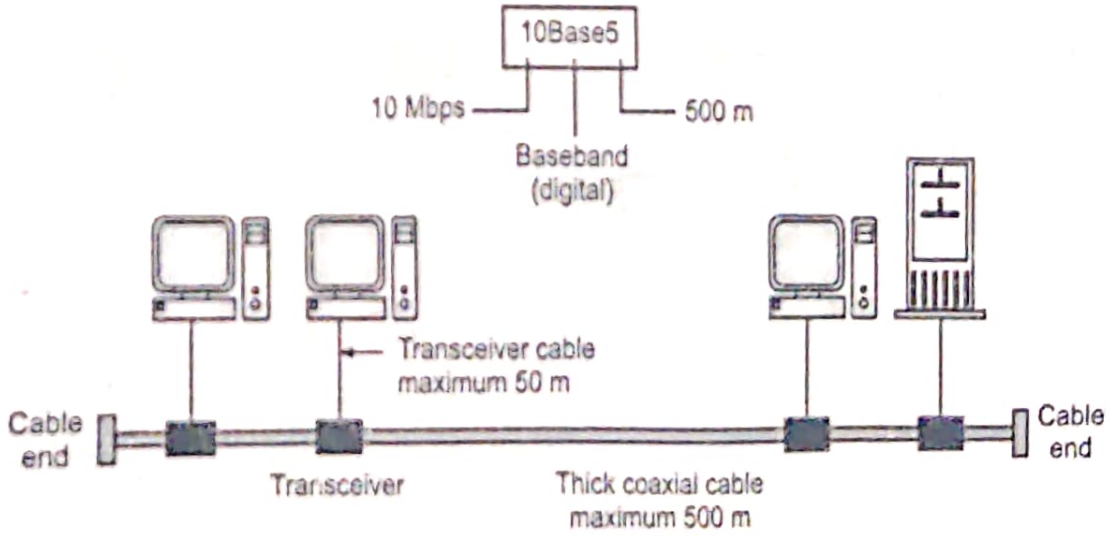


Fig. 4.14: 10Base5 implementation

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

b. 10Base2: Thin Ethernet

- The second implementation is called 10Base2, thin Ethernet, or Cheapernet. 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.

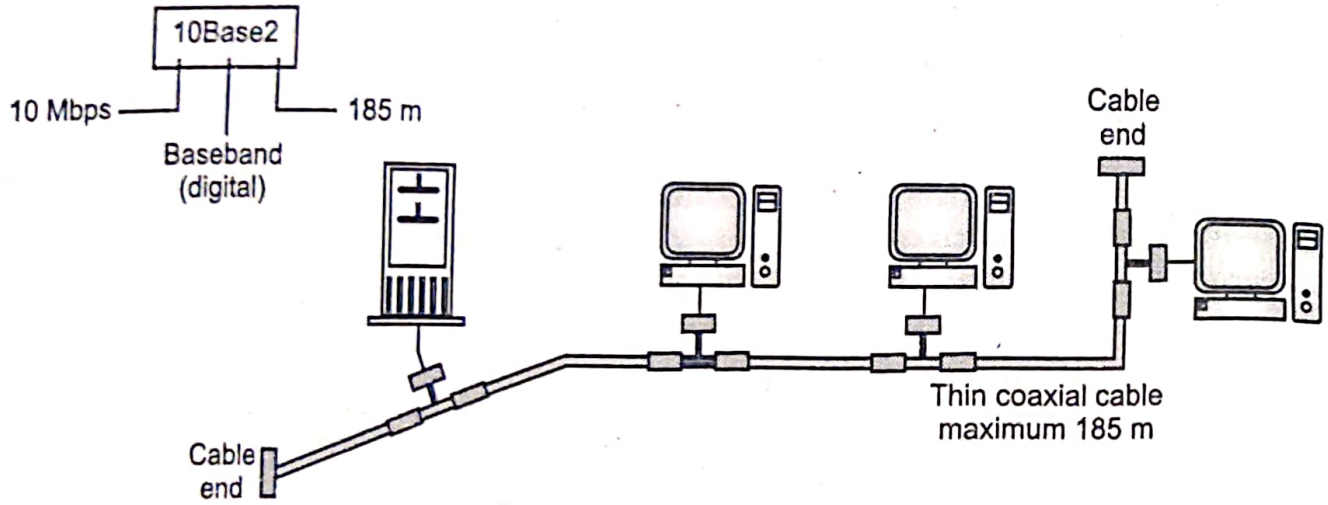


Fig. 4.15: 10Base2-T implementation

c. 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.

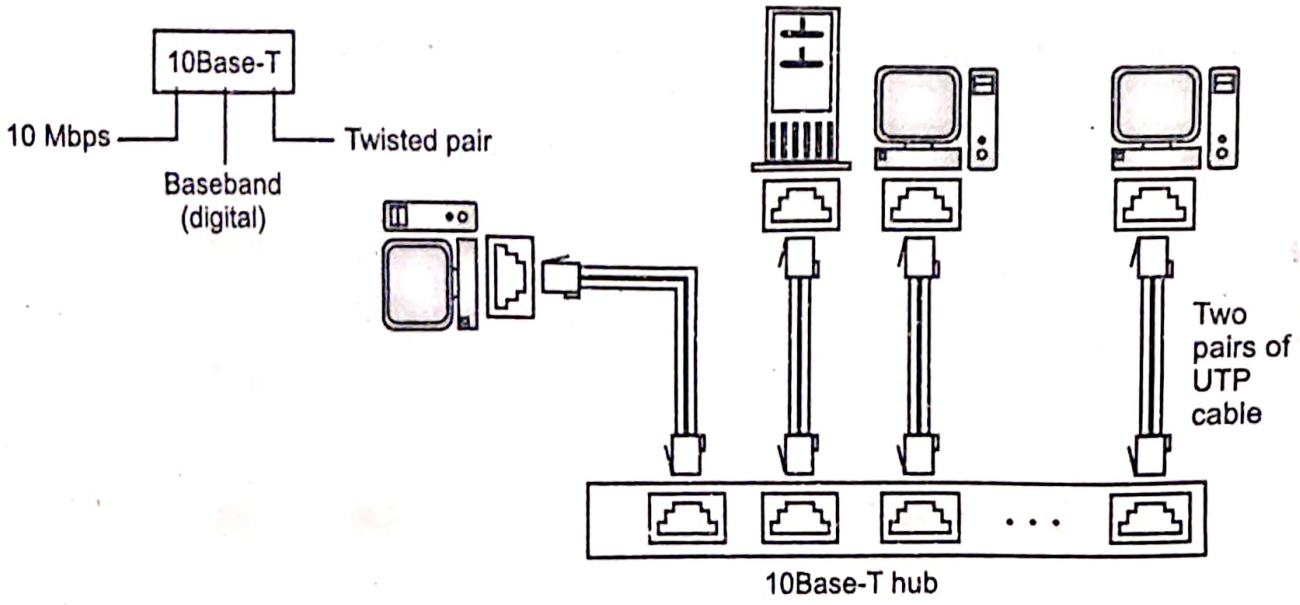


Fig. 4.16: 10Base-T implementation

- Note that two pairs of twisted cable create two paths 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.

d. 10Base-F: Fiber Ethernet

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

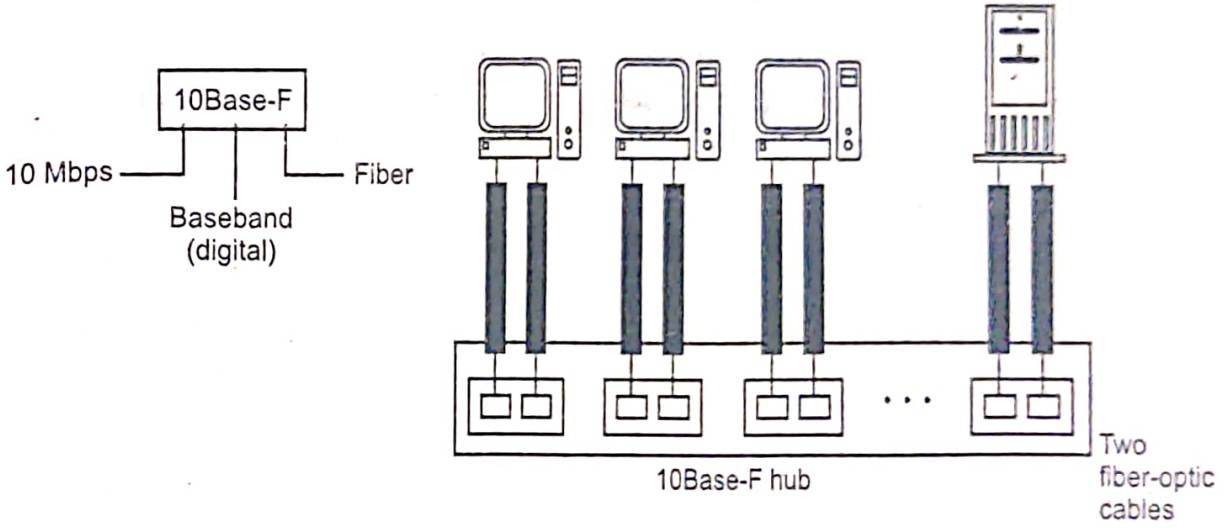


Fig. 4.17: 10Base-F: Fiber Ethernet

4.3 FAST ETHERNET (S-18, W-22)

Goals:

- The Fast Ethernet standard (IEEE 802.3u) has been established for Ethernet networks that need higher transmission speeds. This standard raises the Ethernet speed limit from 10 Mbps to 100 Mbps with only minimal changes to the existing cable structure. Fast Ethernet provides faster throughput for video, multimedia, graphics, Internet surfing and stronger error detection and correction.

Topology

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

Implementations:

- There are three types of Fast Ethernet: 100BASE-TX for use with level 5 UTP cable; 100BASE-FX for use with fiber-optic cable; and 100BASE-T4 which utilizes an extra two wires for use with level 3 UTP cable. The 100BASE-TX standard has become the most popular due to its close compatibility with the 10BASE-T Ethernet standard.

- Network managers who want to incorporate Fast Ethernet into an existing configuration are required to make many decisions. The number of users in each site on the network that need the higher throughput must be determined; which segments of the backbone need to be reconfigured specifically for 100BASE-T; plus what hardware is necessary in order to connect the 100BASE-T segments with existing 10BASE-T segments. Gigabit Ethernet is a future technology that promises a migration path beyond Fast Ethernet so the next generation of networks.
- Increasing the Ethernet transmission rate by a factor of ten over 10Base-T was not a simple task and the effort resulted in the development of three separate physical layer standards for 100 Mbps over UTP cable: 100Base-TX and 100Base-T4 in 1995 and 100Base-T2 in 1997. Each was defined with different encoding requirements and a different set of media-dependent sublayers, even though there is some overlap in the link cabling. Table compares the physical layer characteristics of 10Base-T to the various 100Base versions.

Table 4.1: Summary of 100Base-T Physical Layer Characteristics

Ethernet Version	Transmit Symbol Rate*	Encoding	Cabling	Full-Duplex Operation
10Base-T	10 MBd	Manchester	Two pairs of UTP Category -3 or better	Supported
100Base-TX	125 MBd	4B/5B	Two pairs of UTP Category -5 or Type 1 STP	Supported
100Base-T4	33 MBd	8B/6T	Four pairs of UTP Category -3 or better	Not supported
100Base-T2	25 MBd	PAM5x5	Two pairs of UTP Category -3 or better	Supported

[* One baud = One transmitted symbol per second, where the transmitted symbol may contain the equivalent value of 1 or more binary bits.]

- Although not all three 100-Mbps versions were successful in the marketplace, all three have been discussed in the literature and all three did impact future designs. As such, all three are important to consider here.

1. **100Base-X:**

- 100Base-X was designed to support transmission over either two pairs of Category 5 UTP copper wire or two strands of optical fiber. Although the encoding, decoding and clock recovery procedures are the same for both media, the signal transmission is different—electrical pulses in copper and light pulses in optical fiber.

- The 100Base-X encoding procedure is based on the earlier FDDI optical fiber physical media-dependent and FDDI/CDDI copper twisted-pair physical media-dependent signaling standards developed by ISO and ANSI. The 100Base-TX physical media-dependent sublayer (TP-PMD) was implemented with CDDI semiconductor transceivers and RJ-45 connectors; the fiber PMD was implemented with FDDI optical transceivers and the Low Cost Fiber Interface Connector (commonly called the duplex SC connector).
- The 4B/5B encoding procedure is the same as the encoding procedure used by FDDI, with only minor adaptations to accommodate Ethernet frame control. Each 4-bit data nibble (representing half of a data byte) is mapped into a 5-bit binary code-group that is transmitted bit-serial over the link.

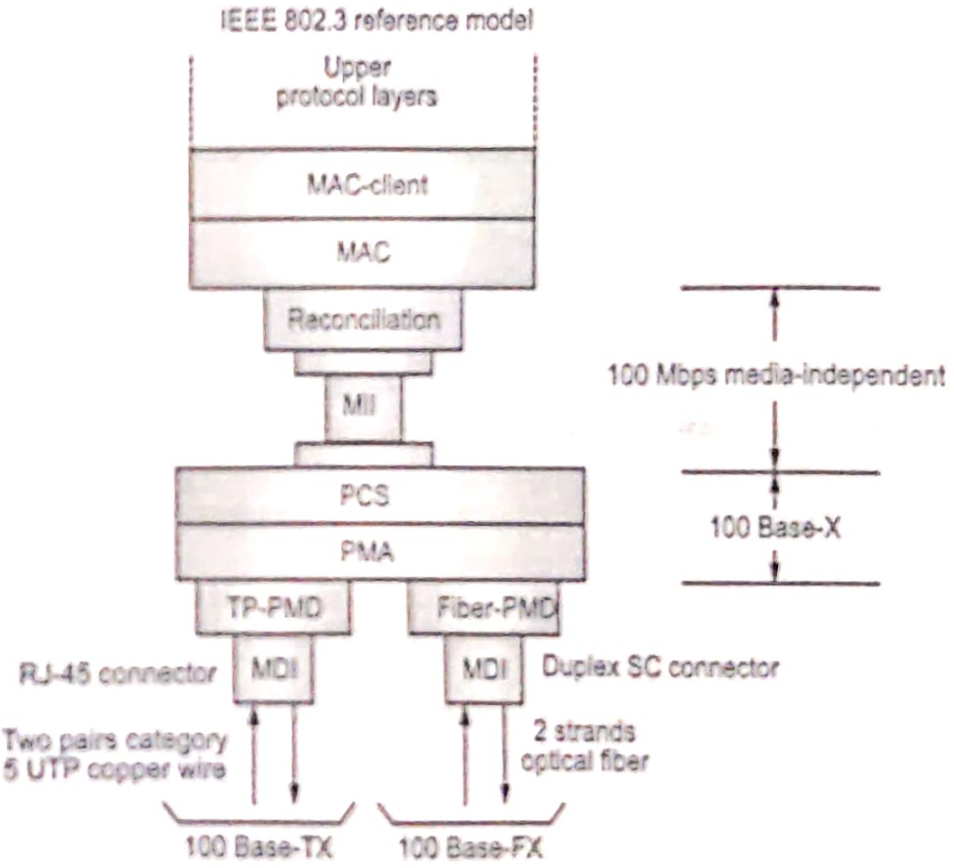


Fig. 4.18: The 100Base-X Logical Model

- The expanded code space provided by the 32 5-bit code-groups allow separate assignment for the following:
- The 16 possible values in a 4-bit data nibble (16 code-groups).
- Four control code-groups that are transmitted as code-group pairs to indicate the Start-of-Stream Delimiter (SSD) and the End-of-Stream Delimiter (ESD). Each MAC frame is "encapsulated" to mark both the beginning and end of the frame. The first

byte of preamble is replaced with SSD code-group pair that precisely identifies the frame's code-group boundaries. The ESD code-group pair is appended after the frame's FCS field.

- A special IDLE code-group that is continuously sent during interframe gaps to maintain continuous synchronization between the NICs at each end of the link. The receipt of IDLE is interpreted to mean that the link is quiet.
- Eleven invalid code-groups that are not intentionally transmitted by a NIC (although one is used by a repeater to propagate receive errors). Receipt of any invalid code-group will cause the incoming frame to be treated as an invalid frame.

MAC Sublayer:

- Fig. 4.19 show how a MAC frame is encapsulated before being transmitted as a 100Base-X code-group stream.
- 100Base-TX transmits and receives on the same link pairs and uses the same pin assignments on the MDI as 10Base-T. 100Base-TX and 100Base-FX both support half-duplex and full-duplex transmission.

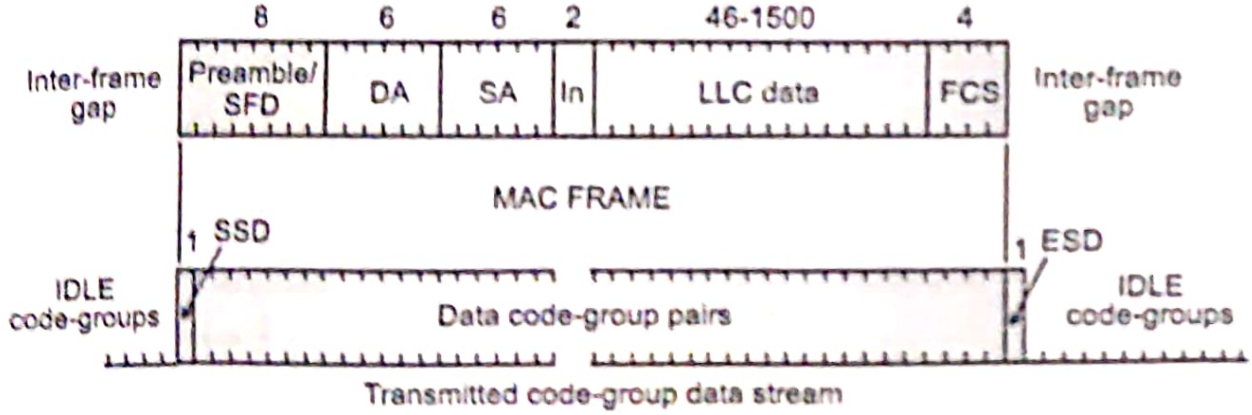


Fig. 4.19: The 100Base-X Code-Group Stream with Frame Encapsulation

2. 100Base-T4:

- 100Base-T4 was developed to allow 10BaseT networks to be upgraded to 100-Mbps operation without requiring existing four-pair Category 3 UTP cables to be replaced with the newer Category 5 cables. Two of the four pairs are configured for half-duplex operation and can support transmission in either direction, but only in one direction at a time. The other two pairs are configured as simplex pairs dedicated to transmission in one direction only. Frame transmission uses both half-duplex pairs, plus the simplex pair that is appropriate for the transmission direction, as shown in Fig. 4.20. The simplex pair for the opposite direction provides carrier sense and collision detection. Full-duplex operation cannot be supported on 100Base-T4.

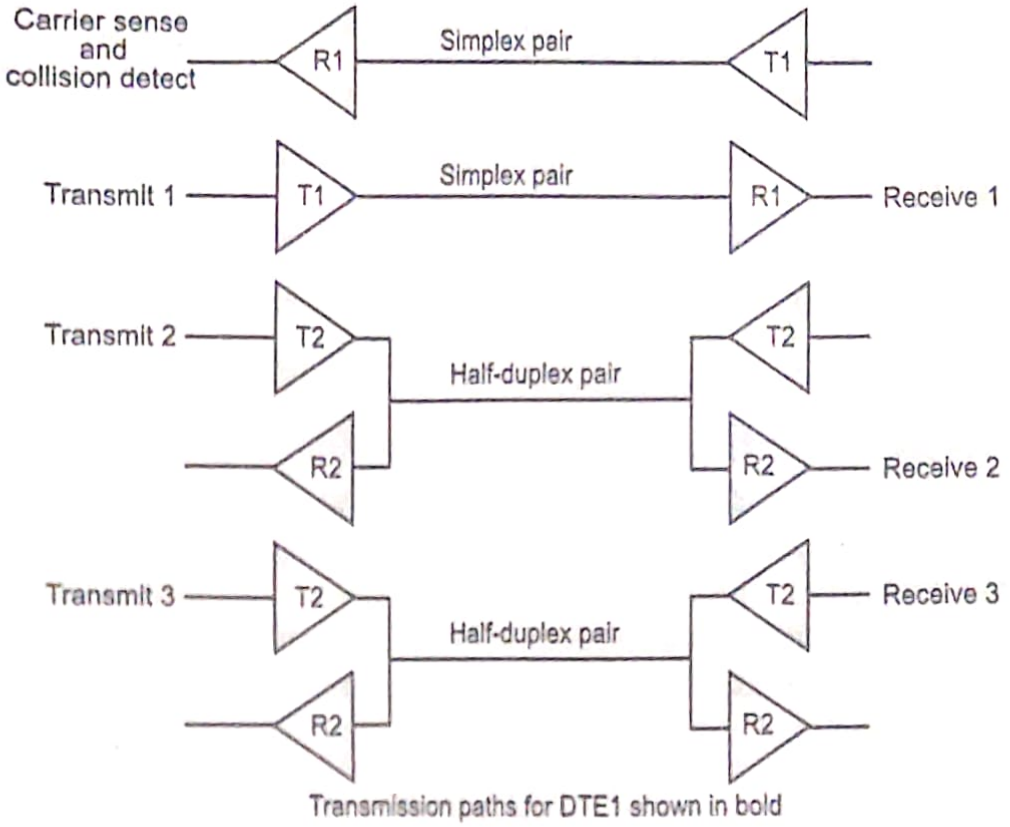


Fig. 4.20: The 100Base-T4 Wire-Pair Usage during Frame Transmission

- 100Base-T4 uses an 8B6T encoding scheme in which each 8-bit binary byte is mapped into a pattern of six ternary (three-levels: +1, 0, –1) symbols known as 6T code-groups. Separate 6T code-groups are used for IDLE and for the control code-groups that are necessary for frame transmission. IDLE received on the dedicated receive pair indicates that the link is quiet.

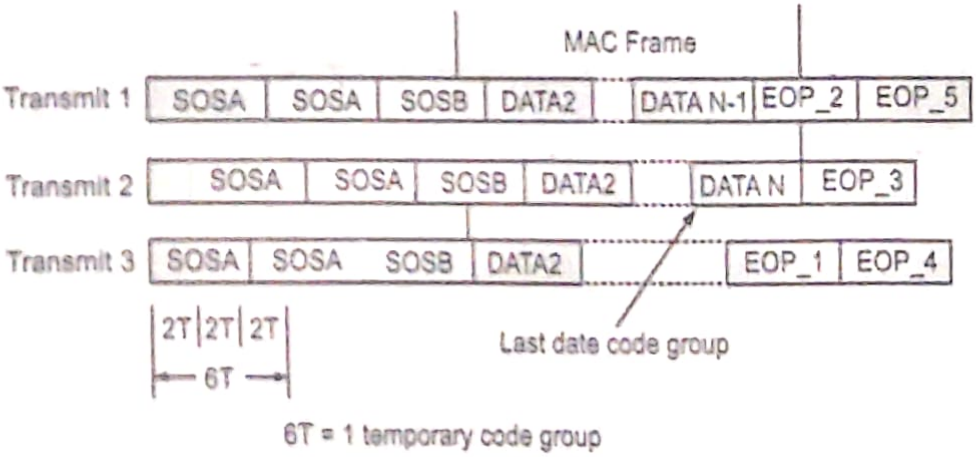


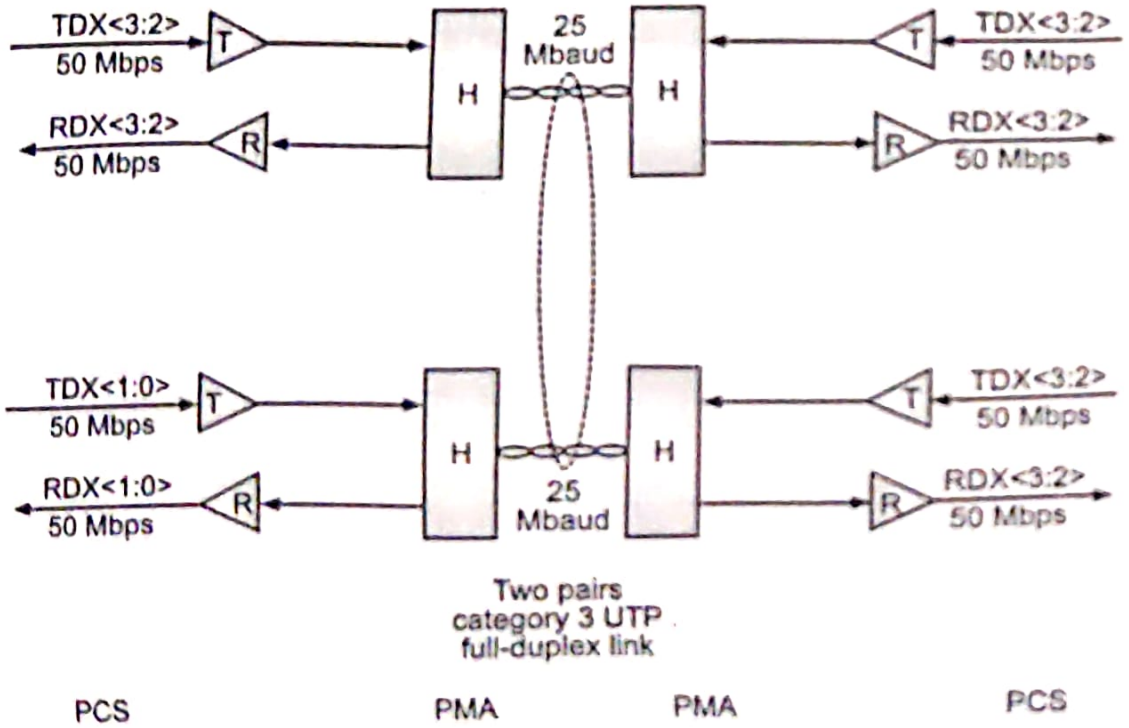
Fig. 4.21: The 100Base-T4 Frame Transmission Sequence

- During frame transmission, 6T data code-groups are transmitted in a delayed round-robin sequence over the three transmit wire-pairs, as shown in Fig. 4.22.
- Each frame is encapsulated with start-of-stream and end-of-packet 6T code-groups that mark both the beginning and end of the frame and the beginning and end of the

6T code-group stream on each wire pair. Receipt of a non-IDLE code-group over the dedicated receive-pair any time before the collision window expires indicates that a collision has occurred.

3. 100Base-T2:

- The 100Base-T2 specification was developed as a better alternative for upgrading networks with installed Category 3 cabling than was being provided by 100Base-T4. Two important new goals were defined:
  - To provide communication over two pairs of Category 3 or better cable.
  - To support both half-duplex and full-duplex operation.
- 100Base-T2 uses a different signal transmission procedure than any previous twisted-pair Ethernet implementations. Instead of using two simplex links to form one full-duplex link, the 100Base-T2 dual-duplex baseband transmission method sends encoded symbols simultaneously in both directions on both wire pairs. The term "TDX<3:2>" indicates the 2 most significant bits in the nibble before encoding and transmission. "RDX<3:2>" indicates the same 2 bits after receipt and decoding.



H = Hybrid canceller transceiver
T = Transmit encoder
R = Receive decoder
Two PAM5 code symbols = one nibble

Fig. 4.22: The 100Base-T2 Link Topology

- Dual-duplex baseband transmission requires the NIC's at each end of the link to be operated in a master/slave loop-timing mode. Which NIC will be master and which will be slave is determined by auto negotiation during link initiation. When the link is

operational, synchronization is based on the master NIC's internal transmit clock. The slave NIC uses the recovered clock for both transmit and receive operations, as shown in Fig. 4.22. Each transmitted frame is encapsulated, and link synchronization is maintained with a continuous stream of IDLE symbols during interframe gaps.

- The 100Base-T2 encoding process first scrambles the data frame nibbles to randomize the bit sequence. It then maps the two upper bits and the two lower bits of each nibble into two five-level (+2, +1, 0, –1, –2) pulse amplitude-modulated (PAM5) symbols that are simultaneously transmitted over the two wire pairs (PAM5x5). Different scrambling procedures for master and slave transmissions ensure that the data streams travelling in opposite directions on the same wire pair are uncoordinated.
- Signal reception is essentially the reverse of signal transmission. Because the signal on each wire pair at the MDI is the sum of the transmitted signal and the received signal, each receiver subtracts the transmitted symbols from the signal received at the MDI to recover the symbols in the incoming data stream. The incoming symbol pair is then decoded, unscrambled and reconstituted as a data nibble for transfer to the MAC.

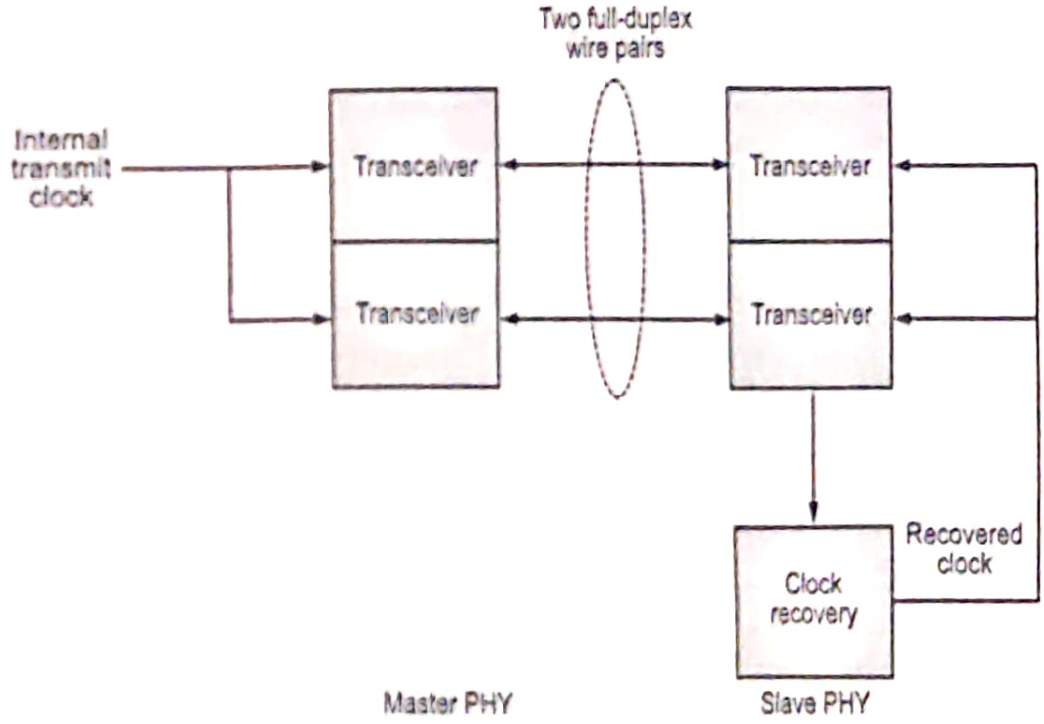


Fig. 4.23: The 100Base-T2 Link Topology

4.4 GIGABIT ETHERNET

- Since, its inception at Xerox Corporation in the early 1970's, Ethernet has been the dominant networking protocol. Of all current networking protocols, Ethernet has, by far, the highest number of installed ports and provides the greatest cost performance relative to Token Ring, Fiber Distributed Data Interface (FDDI) and Asynchronous Transfer Mode (ATM) for desktop connectivity. Fast Ethernet, which increased

Ethernet speed from 10 to 100 megabits per second (Mbps), provided a simple, cost-effective option for backbone and server connectivity.

- Gigabit Ethernet builds on top of the Ethernet protocol, but increases speed tenfold over Fast Ethernet to 1000 Mbps or 1 gigabit per second (Gbps). This protocol, which was standardized in June 1998, promises to be a dominant player in high-speed local area network backbones and server connectivity. Since, Gigabit Ethernet significantly leverages on Ethernet, customers will be able to leverage their existing knowledge base to manage and maintain gigabit networks.
- 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 as Fast Ethernet.

4.4.1 Gigabit Ethernet Protocol Architecture

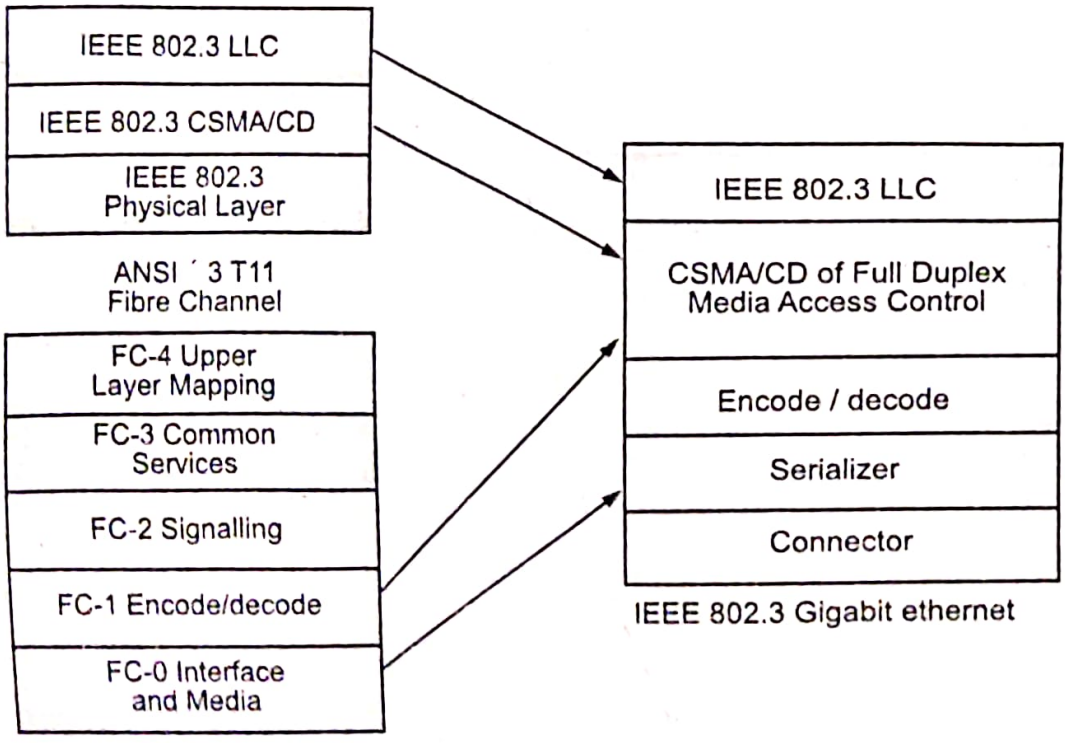


Fig. 4.24: Gigabit Ethernet Protocol Stack

- In order to accelerate speeds from 100 Mbps Fast Ethernet up to 1 Gbps, several changes need to be made to the physical interface. It has been decided that Gigabit Ethernet will look identical to Ethernet from the data link layer upward. The challenges involved in accelerating to 1 Gbps have been resolved by merging two technologies together; IEEE 802.3 Ethernet and ANSI X3T11 Fiber Channel. Fig. 4.25

shows how key components from each technology have been leveraged to form Gigabit Ethernet.

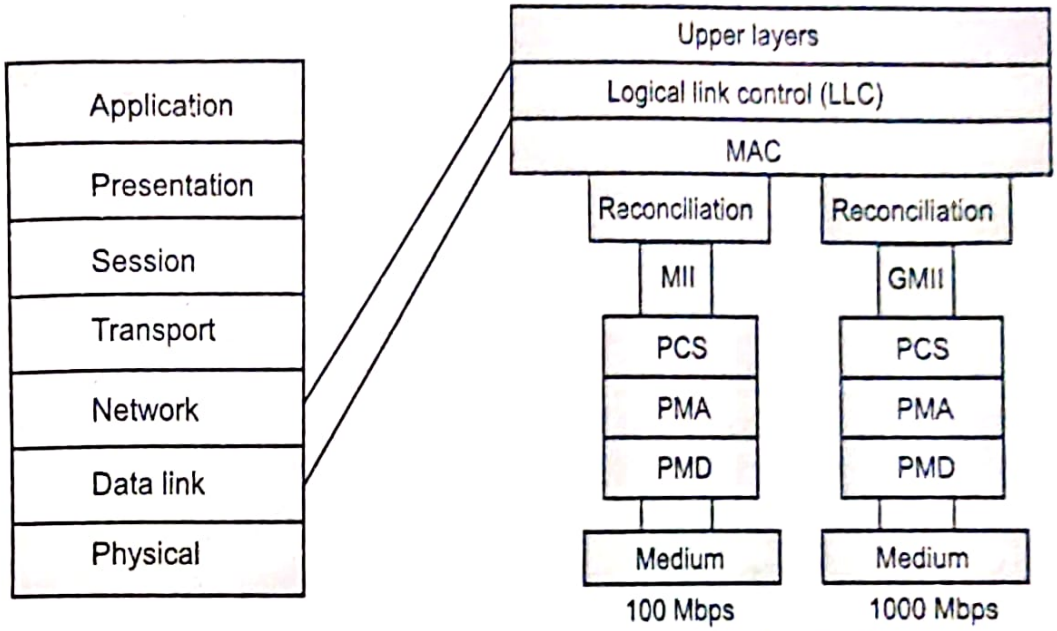


Fig. 4.25: Architectural Model of IEEE 802.3z Gigabit Ethernet

- Leveraging these two technologies means that the standard can take advantage of the existing high-speed physical interface technology of Fiber Channel while maintaining the IEEE 802.3 Ethernet frame format, backward compatibility for installed media and use of full- or half-duplex Carrier Sense Multiple Access with Collision Detect (CSMA/CD). This scenario helps minimize the technology complexity, resulting in a stable technology that can be quickly developed.

4.4.2 Topology

- Gigabit Ethernet is designed to connect two or more stations. If there are only two stations, they can be connected point to point. Three or more stations need to be connected in a star topology with a hub or a switch at the center. Another possible configuration is to connect several star topologies or let a star topology be part of another as shown in Fig. 4.26.

4.4.3 Implementation

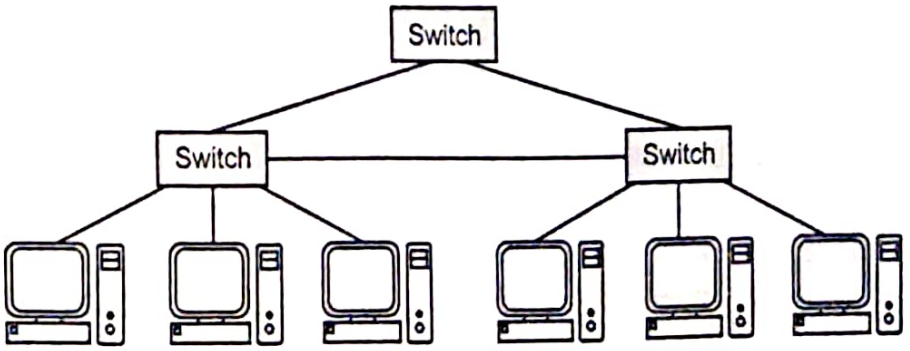


Fig.4.26: Hierarchy of stars

- Gigabit Ethernet can be classified as either a two-wire or a four-wire implementation. The two-wire implementation use fiber-optic cable (1000Base-SX, short-wave, or 1000Base-LX, long-wave), or STP (1000Base-CX). The four-wire version uses category 5 twisted-pair cable (1000Base-T).
- Fig. 4.27 shows the physical implementation.

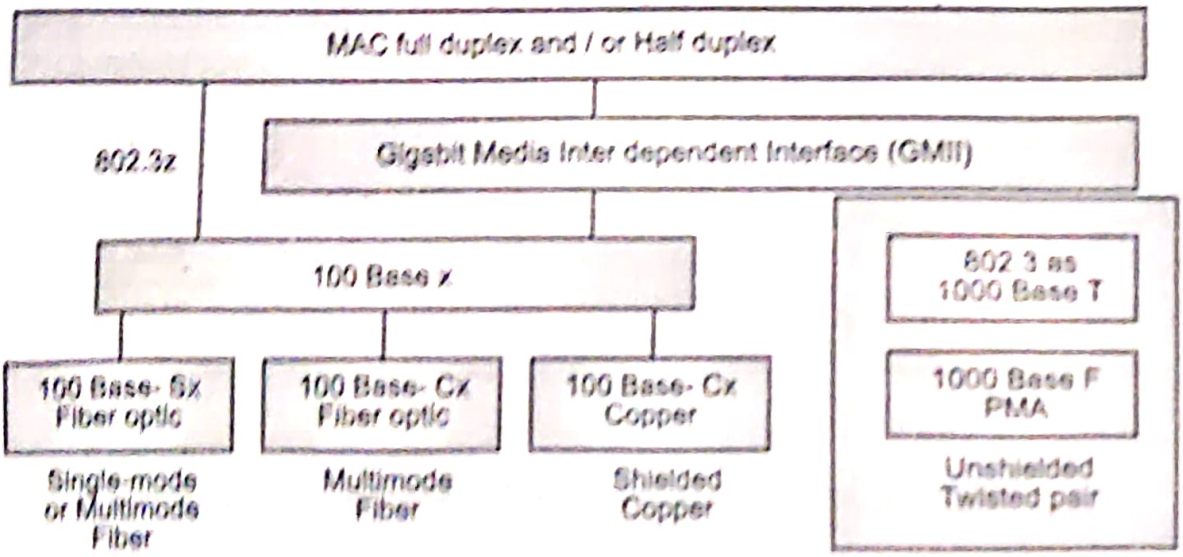


Fig. 4.27: 802.3z and 802.3ab Physical Layouts

1. Gigabit Ethernet Interface Carrier:

- The Gigabit interface converter (GBIC) allows network managers to configure each gigabit port on a port-by-port basis for short-wave (SX), long-wave (LX), long-haul (LH) and copper physical interfaces (CX).
- LH GBICs extended the single-mode fiber distance from the standard 5 km to 10 km. Cisco views LH as a value add, although it's not part of the 802.3z standard, allowing switch vendors to build a single physical switch or switch module that the customer can configure for the required laser/fiber topology.
- As stated earlier, Gigabit Ethernet initially supports three key media: short-wave laser, long-wave laser, and short copper. In addition, fiber- optic cable comes in three types: Multimode (62.5 μm), multimode (50 μm), and Single mode. A diagram for the GBIC is shown in Fig. 4.28.
- The Fiber Channel Physical Medium Dependent (PMD) specification currently allows for 1.062-gigabaud signaling in full duplex. Gigabit Ethernet will increase this signaling rate to 1.25 Gbps. The 8B/10B encoding (to be discussed later) allows a data transmission rate of 1000 Mbps. The current connector type for Fiber Channel and therefore for Gigabit Ethernet, is the SC connector for both single-mode and multimode fiber.
- The Gigabit Ethernet specification calls for media support for multimode fiber-optic cable, single-mode fiber-optic cable and a special balanced shielded 150-ohm copper cable.

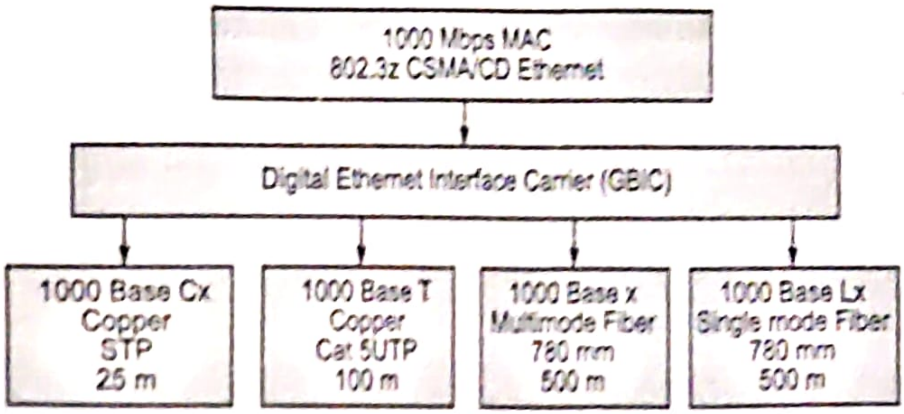


Fig. 4.28: Function of the GBIC Interface

- In contrast, Gigabit Ethernet switches without GBICs either cannot support other lasers or need to be ordered customized to the laser types required.

2. Long-Wave and Short-Wave Lasers over Fiber-Optic Media:

- Two laser standards will be supported over fiber: 1000BaseSX (short-wave laser) and 1000BaseLX (long-wave laser). Short- and long-wave lasers will be supported over multimode fiber.
- Two types of multimode fiber are available: 62.5 and 50 micron-diameter fibers. Long-wave lasers will be used for single-mode fiber, because this fiber is optimized for long-wave laser transmission. There is no support for short-wave laser over single-mode fiber.
- The key differences between the use of long and short-wave laser technologies are cost and distance.
- Lasers over fiber-optic cable take advantage of variations in attenuation in a cable. At different wavelengths, "dips" in attenuation are found over the cable. Short and long-wave lasers take advantage of those dips and illuminate the cable at different wavelengths.
- Short-wave lasers are readily available because variations of these lasers are used in compact-disc technology. Long-wave lasers take advantage of attenuation dips at longer wavelengths in the cable. The net result is that although short-wave lasers will cost less, they transverse a shorter distance. In contrast, long-wave lasers are more expensive but these transverse longer distances.
- Single-mode fiber has been traditionally used in the networking cable plants to achieve long distance. In Ethernet, for example, single-mode cable ranges reach up to 10 km. Single-mode fiber, using a 9-micron core and 1300-nanometer laser, demonstrate the highest-distance technology. The small core and lower-energy laser elongate the wavelength of the laser and allow it to transverse greater distances. This setup enables single-mode fiber to reach the greatest distances of all media with the least reduction in noise.

- Gigabit Ethernet will be supported over two types of multimode fiber: 62.5 and 50 micron-diameter fibers.
- The 62.5-micron fiber is typically seen in vertical campus and building cable plants and has been used for Ethernet, Fast Ethernet and FDDI backbone traffic. This type of fiber, however, has a lower modal bandwidth (the ability of the cable to transmit light), especially with short-wave lasers. In other words, short-wave lasers over 62.5-micron fiber will be able to transverse shorter distances than long-wave lasers.
- Relative to 62.5-micron fiber, the 50-micron fiber has significantly better model bandwidth characteristics and will be able to transverse longer distances with short-wave lasers.

3. 150-Ohm Balanced Shielded Copper Cable (1000BaseCX):

- For shorter cable runs (of 25 meters or less), Gigabit Ethernet will allow transmission over a special balanced 150-ohm cable. This is a new type of shielded cable; it is not unshielded twisted-pair (UTP) or IBM Type I or II.
- In order to minimize safety and interference concerns caused by voltage differences, both transmitters and receivers will share a common ground. The return loss for each connector is limited to 20 dB to minimize transmission distortions. The connector type for 1000BaseCX will be a DB-9 connector. A new connector is being developed by AMP called the HSSDC.

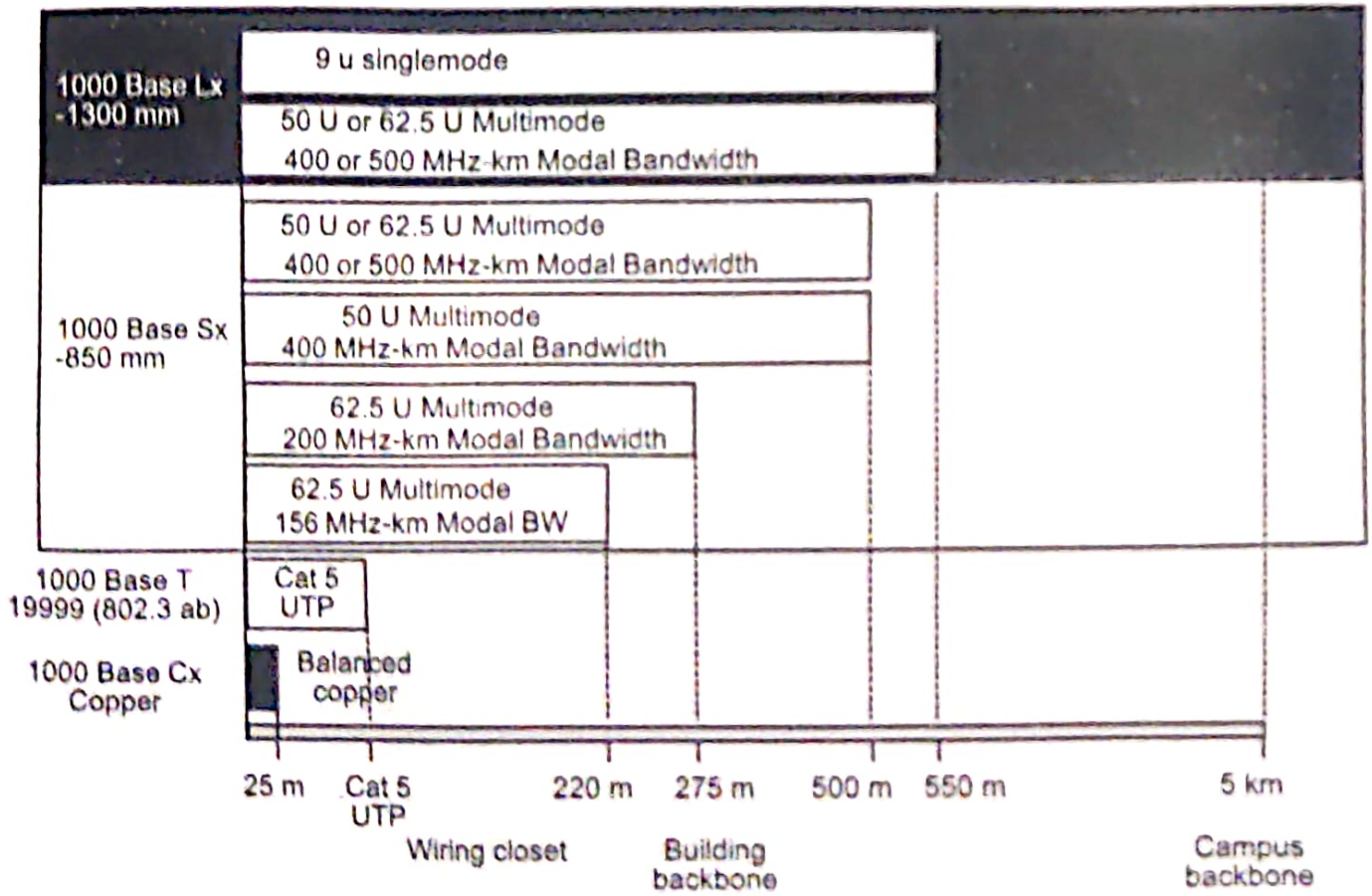


Fig. 4.29: 802.3z and 802.3ab Distance Chart

- The application for this type of cabling will be short-haul data-center interconnections and inter- or intra-rack connections. Because of the distance limitation of 25 meters, this cable will not work for interconnecting data centers to riser closets.
- The distances for the media supported under the IEEE 802.3z standard are shown in Fig. 4.29.

Serializer/Deserializer :

- The Physical Media Attachment (PMA) sublayer for Gigabit Ethernet is identical to the PMA for Fiber Channel. The Serializer/deserializer is responsible for supporting multiple encoding schemes and allowing presentation of those encoding schemes to the upper layers. Data entering the physical sublayer (PHY) will enter through the PMD and will need to support the encoding scheme appropriate to that media. The encoding scheme for Fiber Channel is 8B/10B, designed specifically for fiber-optic cable transmission. Gigabit Ethernet uses a similar encoding scheme.
- The difference between Fiber Channel and Gigabit Ethernet, however, is that Fiber Channel utilizes 1.062-gigabaud signaling whereas Gigabit Ethernet utilizes 1.25-gigabaud signaling. A different encoding scheme will be required for transmission over UTP. This encoding will be performed by the UTP or 1000BaseT PHY.

8B/10B Encoding :

- The Fiber Channel FC-1 layer describes the synchronization and the 8B/10B encoding scheme. FC-1 defines the transmission protocol, including serial encoding and decoding to and from the physical layer, special characters, and error control.
- Gigabit Ethernet utilizes the same encoding/decoding as specified in the FC-1 layer of Fiber Channel. The scheme utilized is the 8B/10B encoding. This scheme is similar to the 4B/5B encoding used in FDDI; however, 4B/5B encoding was rejected for Fiber Channel because of its lack of DC balance. The lack of DC balance can potentially result in data-dependent heating of lasers because a transmitter sends more 1's than 0's, resulting in higher error rates.
- Encoding data transmitted at high speeds provides some advantages:
  - Encoding limits the effective transmission characteristics, such as ratio of 1's to 0's, on the error rate.
  - Bit-level clock recovery of the receiver can be greatly improved by using data encoding.
  - Encoding increases the possibility that the receiving station can detect and correct transmission or reception errors
  - Encoding can help distinguish data bits from control bits
- All these features have been incorporated into the Fiber channel FC-1 specification.
- In Gigabit Ethernet, the FC-1 layer takes decoded data from the FC-2 layer 8 bits at a time from the reconciliation sublayer (RS), which "bridges" the Fiber Channel physical

interface to the IEEE 802.3 Ethernet upper layers. Encoding takes place via an 8- to 10-bit character mapping. Decoded data comprises 8 bits with a control variable. This information is, in turn, encoded into a 10-bit transmission character.

- Encoding is accomplished by providing each transmission character with a name, denoted as Zxx.y. Z is the control variable that can have two values: D for Data and K for Special Character. The xx designation is the decimal value of the binary number composed of a subset of the decoded bits. The y designation is the decimal value of the binary number of remaining decoded bits. This scenario implies that there are 256 possibilities for Data (D designation) and 256 possibilities for Special Characters (K designation). However, only 12 Kxx.y values are valid transmission characters in Fiber Channel. When data is received, the transmission character is decoded into one of the 256 8-bit combinations.

4.4.4 MAC Sublayer (S-18, W-18)

- Gigabit Ethernet has two approaches for medium access: half duplex and full-duplex.

1. Full Duplex Mode:

- In the full duplex mode, there is a centre switch connected to the all computer or other switches. In this mode, each switch as buffers for each input port in which data are stored until they transmitted. There is no collision in this mode, as we discussed before. This means that CSMA/CD is not used. Lack of collision implies that the maximum length of the cable is determined by the signal attenuation in the cable, not by the collision detection process.

2. Half-Duplex Mode:

- Gigabit Ethernet can also be used in half-duplex mode, although it is rare. In this case, a switch can be replaced by a hub, which acts as the common cable in which a collision might occur. The half-duplex approach uses CSMA/CD. However, as we saw before, the maximum length of the network in this approach is totally dependent on the minimum frame size. Three methods have been defined: Traditional, carrier extension, and frame bursting.

4.4.5 Ethernet Frame Format (S-18, 19)

- Gigabit Ethernet has been designed to adhere to the standard Ethernet frame format. This setup maintains compatibility with the installed base of Ethernet and Fast Ethernet products, requiring no frame translation. Fig. 4.30 describes the IEEE 802.3/Ethernet frame format.
- The original Xerox specification identified a *type* field, which was utilized for protocol identification. The IEEE 802.3 specification eliminated the *type* field, replacing it with the *length* field. The *length* field is used to identify the length in bytes of the data field. The protocol type in 802.3 frames are left to the data portion of the packet.

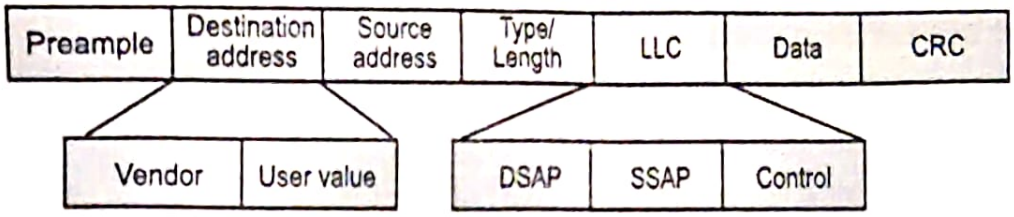


Fig. 4.30: Ethernet Frame Format

- The Logical Link Control (LLC) is responsible for providing services to the network layer regardless of media type, such as FDDI, Ethernet, Token Ring, and so on. The LLC layer makes use of LLC Protocol Data Units (PDUs) in order to communicate between the Media Access Control (MAC) layer and the upper layers of the protocol stack.
- The LLC layer uses three variables to determine access into the upper layers via the LLC-PDU. Those addresses are the destination service access point (DSAP), source service access point (SSAP), and control variable.
- The DSAP address specifies a unique identifier within the station providing protocol information for the upper layer; the SSAP provides the same information for the source address.
- The LLC defines service access for protocols that conform to the Open System Interconnection (OSI) model for network protocols. Unfortunately, many protocols do not obey the rules for those layers. Therefore, additional information must be added to the LLC in order to provide information regarding those protocols. Protocols that fall into this category include IP and IPX.
- The method used to provide this additional protocol information is called a Subnetwork Access Protocol, or SNAP frame. A SNAP encapsulation is indicated by the SSAP and DSAP addresses being set to "0 x AA". When that address is seen, we know that a SNAP header follows. The SNAP header is 5 bytes long: the first 3 bytes consist of the organization code, which is assigned by the IEEE; the second 2 bytes use the *type* value set from the original Ethernet specifications.

4.5 TEN-GIGATBIT ETHERNET – GOALS, MAC SUBLAYER, PHYSICAL LAYER

10 Gigabit Ethernet

- Gigabit Ethernet (10GE, 10GbE, or 10 GigE) is a group of computer networking technologies for transmitting Ethernet frames at a rate of 10 gigabits per second. It was first defined by the IEEE 802.3ae-2002 standard.
- Gigabit Ethernet is the fastest and most recent of the Ethernet standards. This Ethernet is defined only for full-duplex operation which does not use CSMA/CD.

Standards:

- IEEE 802.3ae and IEEE 802.aq: define 10Gb/s for fiber media. IEEE 802.3ae defines a version of Ethernet with a nominal rate of 10Gbit/s that makes it 10 times faster than Gigabit Ethernet.

- IEEE 802.3ak and IEEE 802.an: 10Gb/s over copper cables.

Goals:

1. Upgrade the data rate of 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 connection; 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-I, and 10GBase-E. Table 4.2 shows a summary of the Ten-Gigabit Ethernet implementations.

Table 4.2: 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-nm single mode
Maximum length	300 m	10 km	40km

4.6 BACKBONE NETWORK

- Backbone is most important part of a system which provides the central support to the rest system, for example backbone of a human body that balance and hold all the body parts. Similarly in Computer Networks a **Backbone Network** is as a Network containing a high capacity connectivity infrastructure that backbone to the different part of the network.
- Actually a backbone network allows multiple LANs to get connected in a backbone network, not a single station is directly connected to the backbone but the stations are part of LAN, and backbone connects those LANs.

Backbone LANs:

- Because of increasing use of distributed applications and PCs, a new flexible strategy for LANs has been introduced. If a premises wide data communication system is to be

supported then we need a networking system which can span over the required distance and which capable of interconnecting all the equipment in a single building or in a group of buildings.

- It is possible to develop a single LAN for this purpose but practically this scheme faces the following drawbacks:

1. **Poor Reliability:**

- With a single LAN, the reliability will be poor since a service interruption even for a short duration can cause major problem to the user.

2. **Capacity:**

- There is a possibility that a single LAN may be saturated due to increase in number of devices beyond a certain number.

3. **Cost:**

- A single LAN can not give its optimum performance for the diverse requirements of communication and interconnection.
- So the alternative for using a single LAN is to use low cost low capacity LANs in each building or department and then interconnection all these LANs with high capacity LAN. Such network is called as Backbone LAN. The backbone network allows several LANs to be connected. In the backbone network, no station is directly connected with backbone, instead each station is a part of LAN, and the LANs are connected to the backbone.
- The backbone itself is a LAN, it uses a LAN protocol such as ethernet, hence each connection in the backbone is itself another LAN.

Type of Backbone Architectures:

- The two very common used architectures are: Bus backbone, Star backbone. These are explained as following below.

1. **Bus Backbone:**

- In Bus backbone the topology used for the backbone is bus topology.

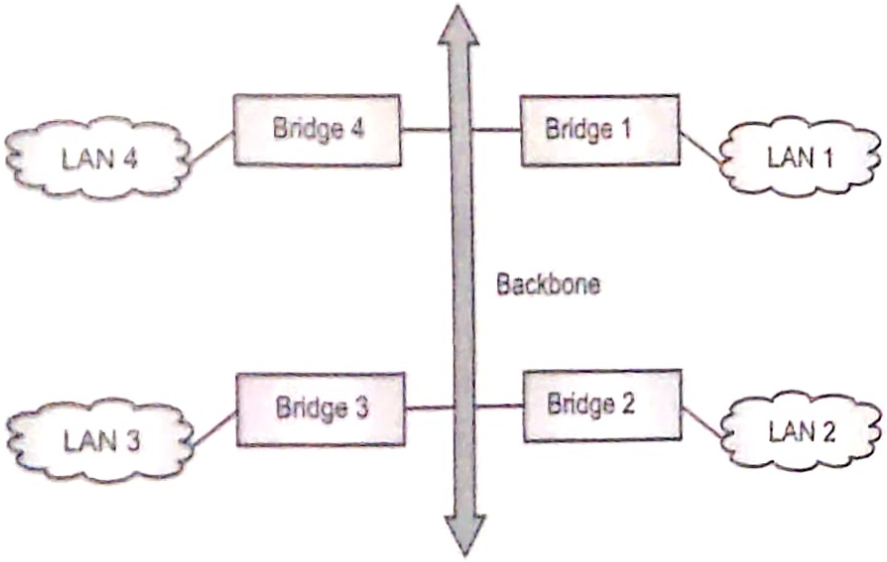


Fig. 4.31: Structure of a Bus backbone

- In above the Bus backbone structure is used as a distribution backbone for connecting different buildings in an organization. Each building may have either a single LAN or another backbone which comes in star backbone. The structure is a bridge based (bridge is the connecting device) backbone with four LANs.

Working:

- In above structure if a station in LAN 2 wants to send a frame to some other station in Same LAN then Bridge 2 will not allow the frame to pass to any other LAN, hence this frame will not reach the backbone. If a station from LAN 1 wants to send a frame to a station in LAN 4 then Bridge 1 passes this frame to the backbone. This frame is then received by Bridge 4 and delivered to the destination.

2. Star Backbone:

- The topology of this backbone is star topology.

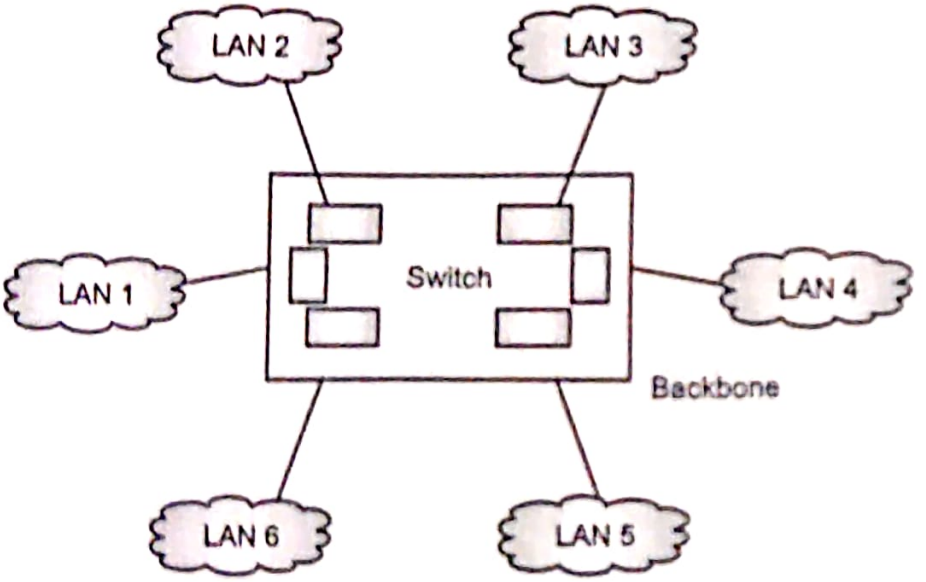


Fig. 4.32: Star Backbone

- Above figure shows the Star backbone in this configuration, the backbone is simply a switch which is used to connect various LANs. The switch does the job of backbone and connects the LANs as well. These types of backbone are basically used as distribution backbone inside a building.
- There is one more category of backbone network is Interconnecting of Remote LANs:

3. Interconnection of Remote control:

- In this type of backbone network the connection are done through the bridge called remote bridges which acts as connecting devices in connect LANs as point to point network link.
- Example of point to point networks is leased telephone lines or ADLS lines. Such a point to point network can be considered as being equivalent to a LAN without stations.

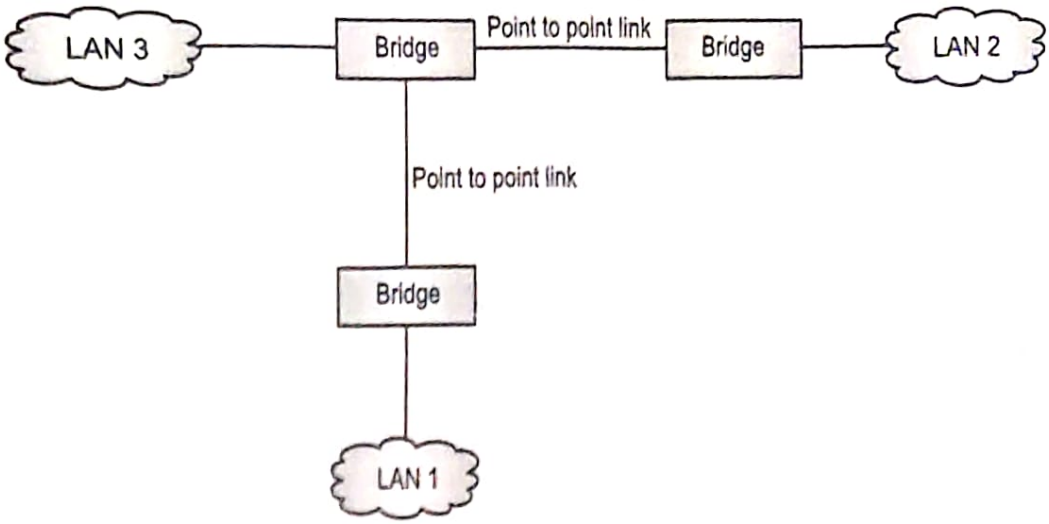
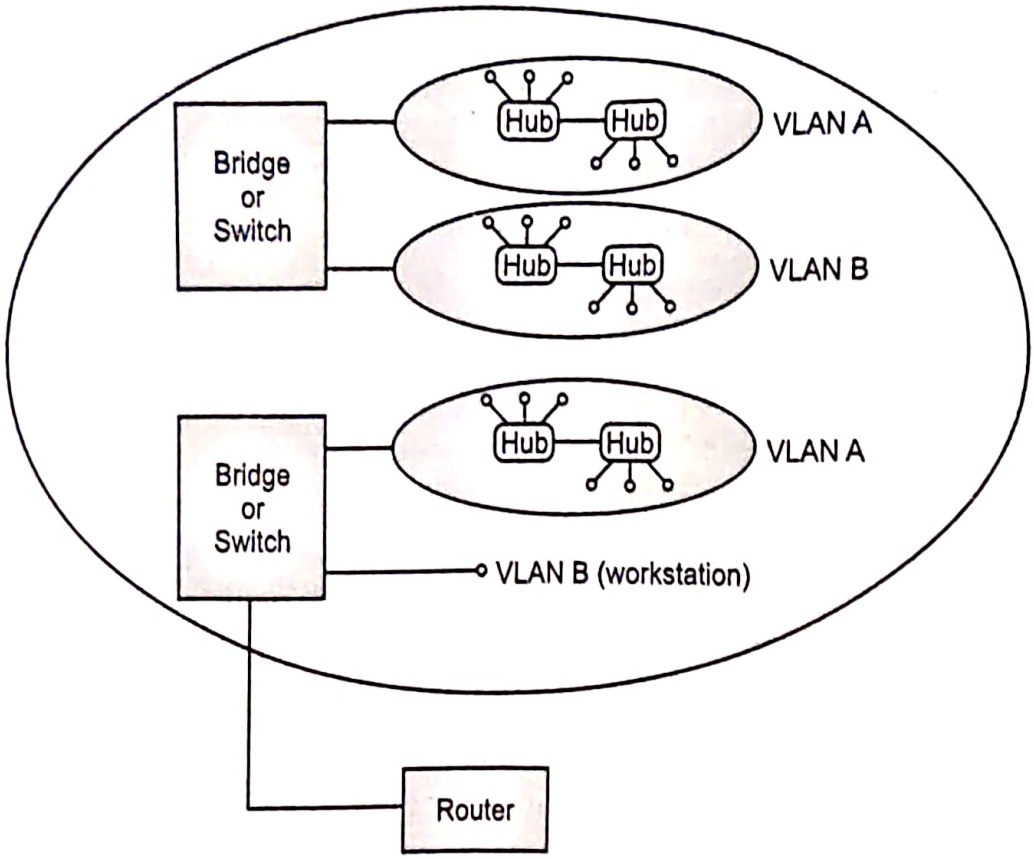


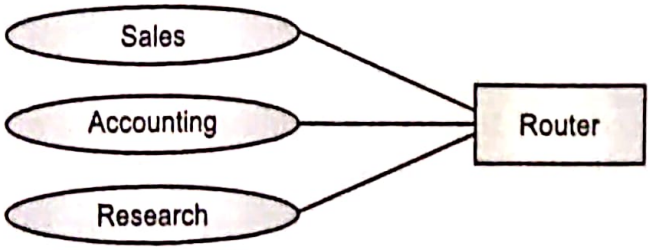
Fig. 4.33: Connecting remote LANs to each other

4.7 VIRTUAL LAN

- In a traditional LAN, workstations are connected to each other by means of a hub or a repeater. These devices propagate any incoming data throughout the network. However, if two people attempt to send information at the same time, a collision will occur and all the transmitted data will be lost. Once the collision has occurred, it will continue to be propagated throughout the network by hubs and repeaters.
- The workstations, hubs, and repeaters together form a LAN segment. A LAN segment is also known as a collision domain since collisions remain within the segment. The area within which broadcasts and multicasts are confined is called a broadcast domain or LAN. Thus a LAN can consist of one or more LAN segments. Defining broadcast and collision domains in a LAN depends on how the workstations, hubs, switches, and routers are physically connected together. This means that everyone on a LAN must be located in the same area.
- VLAN's allow a network manager to logically segment a LAN into different broadcast domains (see Figure 4.34). Since this is a logical segmentation and not a physical one, workstations do not have to be physically located together. Users on different floors of the same building, or even in different buildings can now belong to the same LAN.
- VLAN's also allow broadcast domains to be defined without using routers. Bridging software is used instead to define which workstations are to be included in the broadcast domain. Routers would only have to be used to communicate between two VLAN's.
- Virtual Local Area Networks or Virtual LANs (VLANs) are a logical group of computers that appear to be on the same LAN irrespective of the configuration of the underlying physical network.



Physical View



Logical View

Fig. 4.34: Physical and logical view of a VLAN

- Network administrators partition the networks to match the functional requirements of the VLANs so that each VLAN comprise of a subset of ports on a single or multiple switches or bridges. This allows computers and devices in a VLAN to communicate in the simulated environment as if it is a separate LAN.

Features of VLANs:

- A VLAN forms sub-network grouping together devices on separate physical LANs.
- VLAN's help the network manager to segment LANs logically into different broadcast domains.
- VLANs function at layer 2, i.e. Data Link Layer of the OSI model.
- There may be one or more network bridges or switches to form multiple, independent VLANs.

- Using VLANs, network administrators can easily partition a single switched network into multiple networks depending upon the functional and security requirements of their systems.
- VLANs eliminate the requirement to run new cables or reconfiguring physical connections in the present network infrastructure.
- VLANs help large organizations to re-partition devices aiming improved traffic management.
- VLANs also provide better security management allowing partitioning of devices according to their security criteria and also by ensuring a higher degree of control connected devices.
- VLANs are more flexible than physical LANs since they are formed by logical connections. This aids is quicker and cheaper reconfiguration of devices when the logical partitioning needs to be changed.

Types of VLANs:

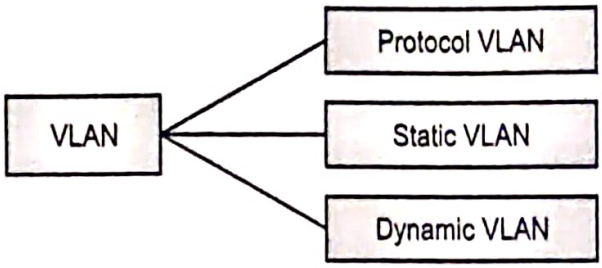


Fig. 4.35: Types of VLANs

- **Protocol VLAN** – Here, the traffic is handled based on the protocol used. A switch or bridge segregates, forwards or discards frames the come to it based upon the traffics protocol.
- **Port-based VLAN** – This is also called static VLAN. Here, the network administrator assigns the ports on the switch / bridge to form a virtual network.
- **Dynamic VLAN** – Here, the network administrator simply defines network membership according to device characteristics.

Difference between LAN and VLAN:

Sr. No.	LAN	VLAN
1.	LAN stands for Local Area Network.	VLAN stands for Virtual Local Area Network.
2.	The cost of Local Area Network is high.	The cost of Virtual Local Area Network is less.
3.	The latency of Local Area Network is high.	The latency of Virtual Local Area Network is low.

Contd...

4.	The devices which are used in LAN are: Hubs, Routers and switch.	The devices which are used in VLAN are: Bridges and switch.
5.	In local area network, the Packet is advertised to each device.	In virtual local area network, packet is send to specific broadcast domain.
6.	Local area network is less efficient than virtual local area network.	Virtual local area network is greater efficient than local area network.

4.8 WIRELESS LAN

- A wireless LAN or WLAN is the linking of two or more computers or devices using spread-spectrum or OFDM modulation technology based to enable communication between devices in a limited area.
- This gives users the mobility to move around within a broad coverage area and still be connected to the network.
- For the home user, wireless has become popular due to ease of installation, and location freedom with the gaining popularity of laptops.
- Public businesses such as malls have begun to offer wireless access to their customers; some are even provided as a free service.
- Large wireless network projects are being put up in many major cities.

Need of wireless LAN:

- An increasing number of LAN users are becoming mobile. These mobile users require that they should be connected to the network regardless of where they are because they want simultaneous access to the network. This makes the use of cables, or wired LANs, impractical if not impossible.
- Wireless LANs are very easy to install. There is no requirement for wiring every workstation and every room. This ease of installation makes wireless LANs inherently flexible.
- If a workstation must be moved, it can be done easily and without additional wiring, cable drops or reconfiguration of the network.
- Another advantage is its portability. If a company moves to a new location, the wireless system is much easier to move than ripping up all of the cables that a wired system would have snaked throughout the building.
- Most of these advantages also translate into budgetary savings.

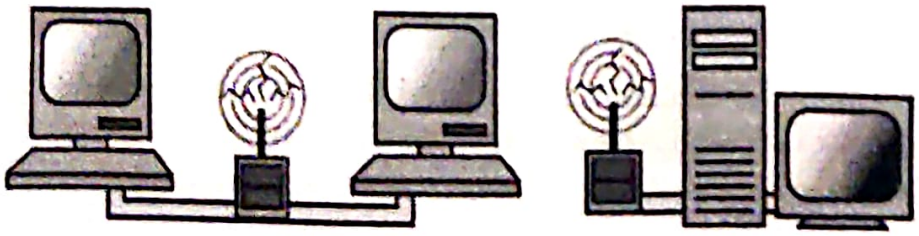


Fig. 4.36: Wireless LAN

- Not all networks are connected with cabling; some networks are wireless. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations and the file server or hubs.
- Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected.
- For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.
- Wireless networks are great for allowing laptop computers or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables.

Objectives of Wireless LAN:

- Objectives of wireless LAN includes:

1. **Convenience:** The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking environment (home or office). With the increasing saturation of laptop-style computers, this is particularly relevant.
2. **Mobility:** With the emergence of public wireless networks, users can access the internet even outside their normal work environment. Most chain coffee shops, for example, offer their customers a wireless connection to the internet at little or no cost.
3. **Productivity:** Users connected to a wireless network can maintain a nearly constant affiliation with their desired network as they move from place to place. For a business, this implies that an employee can potentially be more productive as his or her work can be accomplished from any convenient location. For example, a hospital or warehouse may implement Voice over WLAN applications that enable mobility and cost savings.
4. **Deployment:** Initial setup of an infrastructure-based wireless network requires little more than a single access point. Wired networks, on the other hand, have the additional cost and complexity of actual physical cables being run to numerous locations (which can even be impossible for hard-to-reach locations within a building).
5. **Expandability:** Wireless networks can serve a suddenly-increased number of clients with the existing equipment. In a wired network, additional clients would require additional wiring.
6. **Cost:** Wireless networking hardware is at worst a modest increase from wired counterparts. This potentially increased cost is almost always more than outweighed by the savings in cost and labor associated to running physical cables.

Design goals of Wireless LAN:

- Design goals of Wireless LAN are listed below:
  1. **Global operation:** LAN equipment may be carried from one country to another and this operation should be legal, (frequency regulations national and international).
  2. **Low power:** Take into account that devices communicating via WLAN are typically running on battery power. Specially,power saving modes and power management functions.
  3. **Protection of investment:** A lot of money has been invested for Wired LANs, WLANs should be able to interoperate with existing network, (same data type and services).
  4. **Safety and Security:** Safe to operate. Encryption mechanism, do not allow roaming profiles for tracking people, (privacy).
  5. **Transparency for applications:** Existing applications should continue to work.
  6. **Simplified spontaneous co-operation:** No complicated setup routines but operate spontaneously after power.
  7. **Easy to use:** WLANs are made for simple users, they should not require complex management but rather work on a plug-and-play basis.

4.8.1 How Wireless LAN Works?

- Wireless LAN (WLAN) uses electromagnetic airwaves (radio and infrared) to communicate information from one point to another without relying on any physical connection.
- Radio waves are often referred to as radio carriers because they simply perform the function of delivering energy to a remote receiver.
- The data being transmitted is superimposed on the radio carrier so that it can be accurately extracted at the receiving end.
- This is generally referred to as modulation of the carrier by the information being transmitted.
- Once data is superimposed (modulated) onto the radio carrier, the radio signal occupies more than a single frequency, since the frequency or bit rate of the modulating information adds to the carrier.

4.8.2 Advantages of Wireless LAN

- Wireless LAN offer the following productivity, service, convenience and cost advantages over traditional wired networks:

1. **Mobility improves productivity and Service:** Wireless LAN systems can provide LAN users with access to real-time information anywhere in their organization. This mobility supports productivity and service opportunities not possible with wired networks.
2. **Installation Speed and Simplicity:** Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.
3. **Installation Flexibility:** Wireless technology allows the network to go where wire cannot go.
4. **Reduced Cost-of-Ownership:** While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves, adds and changes.
5. **Scalability:** Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from independent networks suitable for a small number of users to full infrastructure networks of thousands of users that allow roaming over a broad area.
6. **Planning:** Wireless ad hoc networks allow for communication without planning. Wired networks need wiring plans.
7. **Robustness:** Wireless networks can survive disasters, if the wireless devices survive people can still communicate.

4.8.3 Disadvantages of Wireless LAN

- Wireless LAN technology, while replete with the conveniences and advantages described above, has its share of downfalls.
- For a given networking situation, wireless LANs may not be desirable for a number of reasons.
- Most of these have to do with the inherent limitations of the technology.

1. **Reliability:** Like any radio frequency transmission, wireless networking signals are subject to a wide variety of interference, as well as complex propagation effects that are beyond the control of the network administrator. One of the most insidious problems that can affect the stability and reliability of a wireless LAN is the microwave oven. In the case of typical networks, modulation is achieved by complicated forms of Phase-Shift Keying (PSK) or Quadrature Amplitude Modulation (QAM), making interference and propagation effects all the more disturbing. As a result, important network resources such as servers are rarely connected wirelessly.

2. **Range:** The typical range of a common 802.11g network with standard equipment is on the order of tens of meters. While sufficient for a typical home, it will be insufficient in a larger structure. To obtain additional range, repeaters or additional access points will have to be purchased. Costs for these items can add up quickly. Other technologies are in the development phase, however, which feature increased range, hoping to render this disadvantage irrelevant.
3. **Speed:** The speed on most wireless networks (typically 1-108 Mbit/s) is reasonably slow compared to the slowest common wired. There are also performance issues caused by TCP and its built-in congestion avoidance. For most users, however, this observation is irrelevant since the speed bottleneck is not in the wireless routing but rather in the outside network connectivity itself.
4. **Security:** Wireless LAN transceivers are designed to serve computers throughout a structure with uninterrupted service using radio frequencies. Because of space and cost, the antennas typically present on wireless networking cards in the end computers are generally relatively poor. In order to properly receive signals using such limited antennas throughout even a modest area, the wireless LAN transceiver utilizes a fairly considerable amount of power. What this means is that not only can the wireless packets be intercepted by a nearby adversary's poorly-equipped computer, but more importantly, a user willing to spend a small amount of money on a good quality antenna can pick up packets at a remarkable distance; perhaps hundreds of times the radius as the typical user. In fact, there are even computer users dedicated to locating and sometimes even cracking into wireless networks, known as wardrivers.

   On a wired network, any adversary would first have to overcome the physical limitation of tapping into the actual wires, but this is not an issue with wireless packets. To combat this consideration, wireless networks users usually choose to utilize various encryption technologies available such as Wi-Fi Protected Access (WPA). Some of the older encryption methods, such as WEP are known to have weaknesses that a dedicated adversary can compromise.
5. **QoS:** WLAN offer typically lower QoS. Lower bandwidth due to limitaitons in radio transmission and higher error rates due to interference.
6. **Proprietary Solutions:** Slow standardization procedures lead to many proprietary solutions only working in a homogeneous environment.

4.8.4 IEEE Standard 802.11 (WLAN) (S-22, W-22)

- IEEE has defined the specifications for wireless LAN, named IEEE 802.11, which covers both physical and data link layers.

- Fig. 4.37 shows various components of WLAN which described below:

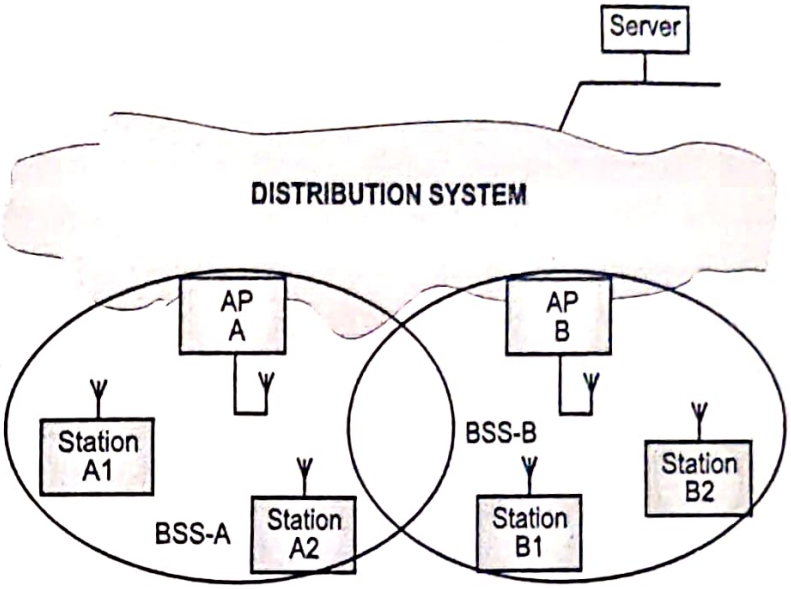
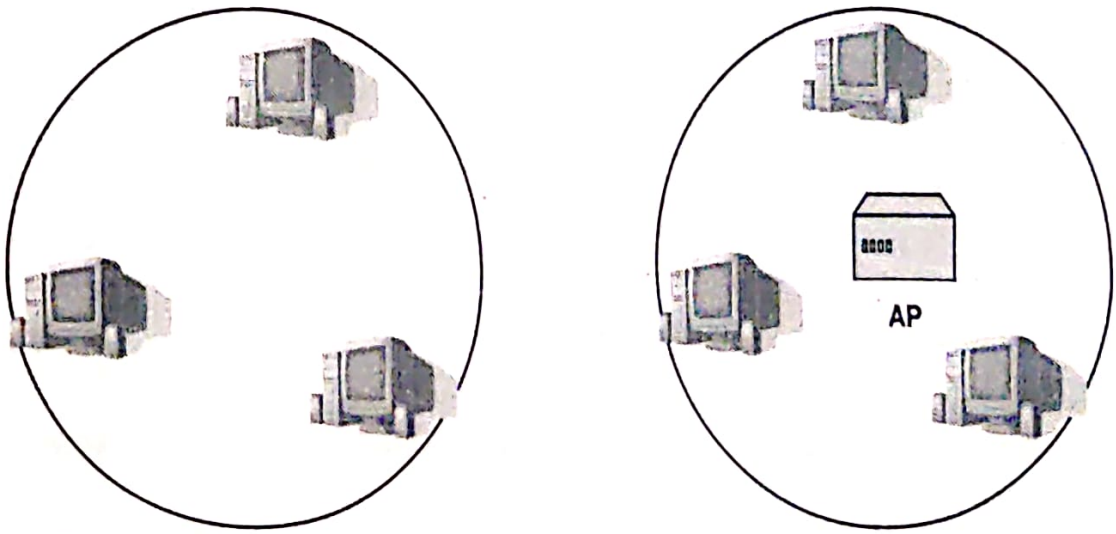


Fig. 4.37: Components of WLAN

Architecture of 802.11 (WLAN):

- Each computer, mobile which is portable or fixed, is referred to as a station in 802.11 wireless networks.
- When two or more stations come together to communicate with each other, they form a **Basic Service Set (BSS)**.
- The minimum BSS consists of two stations. 802.11 LANs use the BSS as the standard building block.
- The BSS can be either without AP (Access Point) or with AP which is as shown in Fig. 4.38.



(a) BSS without AP (b) BSS with AP

Fig. 4.38: Types of BSS

- The BSS without AP can not send data to another BSS. So it is called as standalone or ad-hoc network.
- Two or more BSSs are interconnected using a Distribution System or DS.
- This concept of DS increases network coverage, which can be either wired or wireless.
- Entry to the DS is accomplished with the use of access points.
- An access point is a station, thus addressable. So data moves between the BSS and the DS with the help of these access points.
- Creating large and complex networks using BSSs and DSs leads us to the next level of hierarchy, the Extended Service Set or ESS.
- An Extended Service set contains two or more BSS with APs. The BSSs in the system are connected to each other via a distribution system which is generally a wired LAN as shown in Fig. 4.39.

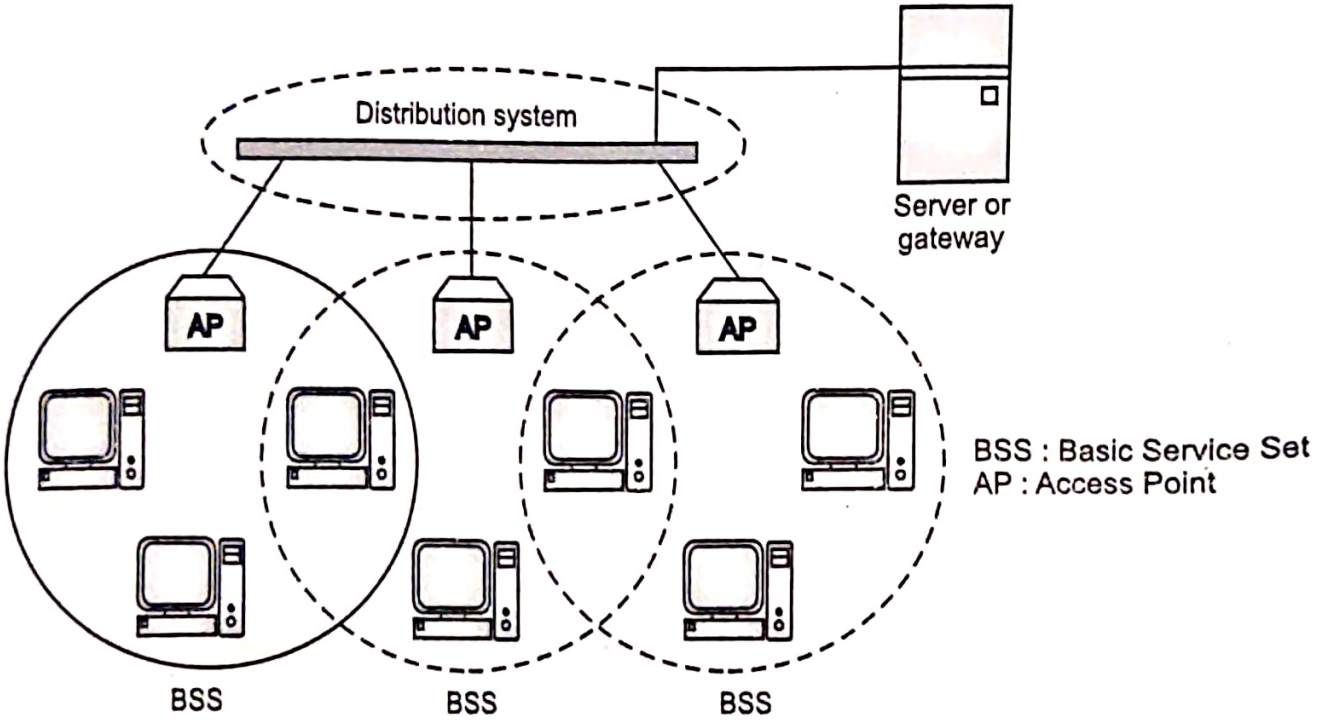


Fig. 4.39: Extended Service Set (ESS)

- The beauty of the ESS is the entire network looks like an independent basic service set.
- This means that stations within the ESS can communicate or even more between BSSs transparently.
- The implementation of the DS is not specified by 802.11. So a distribution system may be created from existing or new technologies.
- As the implementation for the DS is not specified, 802.11 specify the services, which the DS must support. Services are divided into two sections, Station Services (SS) and Distribution System Services (DSS).

Layers of 802.11 (WLAN):

1. Physical Layer:

- 802.11 provides Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and OFDM (Orthogonal Frequency Division Multiplexing), physical definitions which supports 1 and 2 Mbps data transfer rates and of DM.

(i) Frequency Hopping Spread Spectrum (FHSS):

- Frequency Hopping Spread Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver.
- Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise.
- FHSS is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both transmitter and receiver.
- Fig. 4.40 shows frame format of FHSS.

<table>
<tr><td>80 bit preamble</td><td>SFD 16 bits</td><td>LENGTH 12 bits</td><td>PSF 4 bits</td><td>CRC 16 bits</td><td>CRC 16 bits</td></tr>
<tr><td colspan="2">PLCP Preamble</td><td colspan="3">PLCP Header</td><td>Payload MPDU</td></tr>
<tr><td colspan="6">PPDU</td></tr>
</table>

Fig. 4.40: FHSS Frame Format

- The 80 bit Preamble has a 0101 sync format and is used for signal detection.
- The SFD stands for Start of Frame Delimiter.
- The LENGTH field indicates the Payload length in bytes.
- The PSF stands for Payload Signaling Field and indicates the rate used and some bits for future use.
- The hopping rules say that there are 79 hopping channels and that the minimum hop should be 6 channels. The transmitter should settle on the new channel within 224 microseconds.

(ii) Direct Sequence Spread Spectrum (DSSS):

- DSSS generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code).
- The longer the chip, the greater the probability that the original data can be recovered and, of course, the more bandwidth required.
- Each bit is transmitted as 11 chips using a Barker Sequence.
- Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for

retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

- With direct sequence spread spectrum the transmission signal is spread over an allowed band.
- A random binary string is used to modulate the transmitted signal. This random string is called the spreading code.
- The data bits are mapped to a pattern of chips and mapped back into a bit at the destination.
- The number of chips that represent a bit is the spreading ratio. The higher the spreading ratio, the more the signal is resistant to interference. The lower the spreading ratio, the more bandwidth is available to the user.
- The FCC dictates that the spreading ratio must be more than 10. IEEE 802.11 standard requires a spreading ratio of 11.
- Fig. 4.41 shows frame format of DSSS.

<table>
<tr><td>128 bit
preamble</td><td>SFD 16 bits</td><td>SIGNAL
8 bits</td><td>SERVICE
8 bits</td><td>LENGTH
16 bits</td><td>CRC
16 bits</td><td></td></tr>
<tr><td colspan="2">PLCP Preamble</td><td colspan="4">PLCP Header</td><td>Payload
MPDU</td></tr>
<tr><td colspan="7">PPDU</td></tr>
</table>

Fig. 4.41: DSSS Frame Format

- The **128 bit preamble** is used for signal detection.
- The **SFD** stands for Start of Frame Delimiter
- The **SIGNAL** field indicates the speed used.
- The **SERVICE** field is reserved for future use and now contains 00.
- The **LENGTH** field indicates the Payload length in bytes.

(iii) Orthogonal Frequency Division Multiplexing (OFDM):

- OFDM is multicarrier spread spectrum technique.
- In OFDM, high rate serial data stream divided into numerous parallel low-rate data streams that are modulated by a set of subcarriers.
- In OFDM, subcarriers are orthogonal with overlapping spectra. It uses 5GHz ISM band for its operation.
- The basic working of OFDM is same as that of FDM but the main difference is that all the frequency sub bands are used by one source at a given time.

2. MAC Layer:

- IEEE 802.11 defines two MAC sublayers i.e. the Distributed Coordination Function (DCF) and Point Coordination Function (PCF). DCF is the fundamental, required

contention-based access service for all networks. PCF is an optical contention-free service, used for non-QoS STAs.

- The Point Coordination Function (PCF) is an optional access method which is implemented in an infrastructure network and not in ad-hoc network. It is implemented on top of the DCF and is used for time sensitive transmission.
- Fig. 4.42 shows the relationship between the two MAC sublayers, the LLC sublayer and the physical layer.

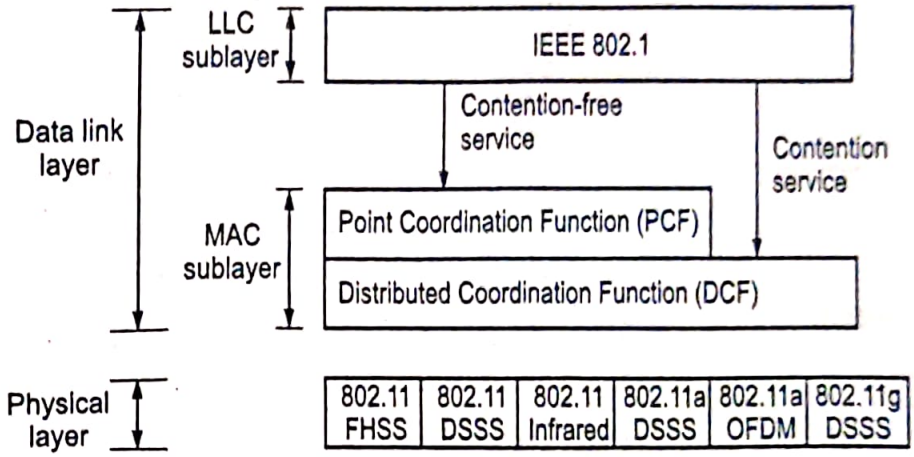


Fig. 4.42: MAC Layer

- MAC provides a reliable delivery mechanism for user data over noisy, unreliable wireless medium.
- Before transmitting frames, a station must first gain access to the medium, which is a radio channel that stations share.
- CSMA/CA is the protocol used to access method defined by IEEE at the MAC sub layer is called the distributed coordination function.
- The MAC layer consists of nine fields as shown in Fig. 4.43.

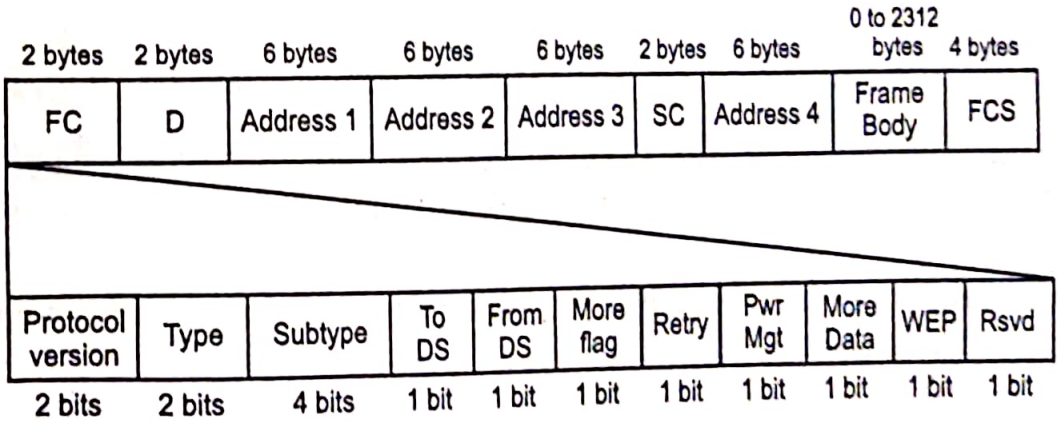


Fig. 4.43: Frame Format

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

Table 4.3: Subfields in FC fields

Field	Explanation
Version	Current version is 0.
Type	Type of information: Management (00), Control (01), or Data (10).
Subtype	Subtype (RTS, CTS, ACK).
TO DS	Shown in Table 4.4.
From DS	Shown in Table 4.4.
More flag	When set to 1, means more fragments.
Retry	When set to 1 means retransmitted frame.
Power management	When set to 1 means station is in power management made.
More data	When set to 1, means station has more data to send.
WEP	Wired equivalence privacy.
Rsvd	Reserved.

- **D:** In all frames, this field defines the duration of the transmission that is used to set the value of NAV.
- **Addresses:** There are four address fields, each 6 bytes long. The meaning of each address field depends on the value of the TO DS and From DS subfields.

Table 4.4: Addresses

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

- **Sequence Control:** This field defines the sequence number of the frame to be used in flow control.
- **Frame Body:** This field between 0 to 2312 bytes contains information based on the type and the subtype defined in the FC field.
- **FCS:** This field is used for error detection.

4.8.5 IEEE Standard 802.11x (S-19)

- 802.11x refers to a group of evolving wireless local area network (WLAN) standards that are under development as elements of the IEEE 802.11 family of specifications, but that have not yet been formally approved or deployed.

- As of August 2004, these incomplete standards included the following:
  1. **802.11e:** Adds Quality of Service (QoS) features to exiting 802.11 family specifications.
  2. **802.11f:** Adds Access Point Interoperability to existing 802.11 family specifications.
  3. **802.11h:** Resolves interference issues with existing 802.11 family specifications.
  4. **802.11j:** Japanese regulatory extensions to 802.11 family specifications.
  5. **80211k:** Radio resource measurement for 802.11 specifications so that a wireless network can be used more efficiently.
  6. **802.11m:** Enhanced maintenance features, improvements, and amendments to existing 802.11 family specifications.
  7. **802.11n:** Next generation of 802.11 family specifications, with throughput in excess of 100 Mbps.
- Above standards are being developed with the goal that they support all the 802.11 family specifications in current use.
- 802.11x is also sometimes used as a generic term for any existing or proposed standard of the 802.11 family.

4.9 BLUETOOTH

(W-18, S-18, S-19, S-22, S-23)

- Bluetooth is an open specification for short-range wireless transmission of voice and data. It provides a simple, low-cost seamless wireless connectivity between Personal Digital Assistants (PDAs), cellular phones, laptops and other portable handheld devices.
- Bluetooth can be used for bridging data networks, connecting peripherals to devices and forming ad hoc connections between groups of information appliances.
- Bluetooth is the initiative of a consortium called the Bluetooth Special Interest Group (SIG), whose original members include industry leaders Ericsson, IBM, Intel, Nokia, and Toshiba.

4.9.1 How Bluetooth Works ?

- Bluetooth supports transmission of voice and data over 2.4 GHz radio frequencies, using a frequency-hopping scheme with a maximum of 1600 hops per second, resulting in a new frequency being used to transmit each packet.
- This scheme allows for smooth operation in spite of fading due to reflecting obstacles or excessive distance, and in spite of noise due to Electro Magnetic Interference (EMI), such as that generated by microwave ovens.
- In addition, Bluetooth uses short packets and fast acknowledgements to increase reliability and employs forward error correction to reduce the effects of random noise.

- The range of transmission for Bluetooth is typically between 0.1 and 10 meters but can be as much as 100 meters using higher transmission power. The system's automatic power adaptation adjusts transmission power to the minimum needed for reliable transmission in any given situation, which reduces the chance of eavesdropping.
- Bluetooth also includes encryption and authentication mechanisms. The entire Bluetooth technology is implemented in a single 9-millimeter-by-9-millimeter chip.
- Bluetooth data transmission normally takes place over an asynchronous channel that provides 721 Kbps in the forward direction and 57.6 Kbps in the return direction, but synchronous data transmission at 432.6 Kbps in both directions is also supported.
- Time-Division Duplexing (TDD) is employed to alternate transmission between the two directions and thus provide full-duplex communication.
- Each TDD slot normally carries one packet, but packets can be spread across up to five slots. Signaling is baseband and uses a binary FM scheme.
- Channels can be routed by using a combination of circuit switching and packet switching.
- Bluetooth voice transmission can use up to three concurrent synchronous 64 Kbps voice-only channels or one channel that simultaneously supports both asynchronous data and synchronous voice transmission.
- The voice channels use the continuous variable-slope delta modulation coding scheme.
- Bluetooth supports concurrent connections among up to eight devices, forming what is called a Piconet. Each device is temporarily assigned a unique 3-bit MAC address for the duration of the connection.
- A master/slave relationship exists between one device and all other devices for the duration of the connection for the purpose of establishing clocking and the hopping sequence. In all other respects, the devices operate as peers during a connection.
- Unconnected devices are in standby mode and listen for connection attempts every 1.28 seconds on each of 32 preassigned hopping frequencies.
- Link setup and authentication is performed using the Link Manager Protocol (LMP), which uses the link controller services built into the chip.
- Connections between devices can be either point-to-point or point-to-multipoint, and piconets can be joined, with each piconet having a different hopping sequence.
- Bluetooth is both a hardware-based radio system and a software stack that specifies the linkages between layers.
- This supports flexibility in implementation across different devices and platforms. It also provides robust guidelines for maximum interoperability and compatibility.

4.9.2 Bluetooth Architectures (W-22)

- Bluetooth communication occurs between a master radio and a slave radio. Bluetooth radios are symmetric in that the same device may operate as a master and also the slave. Each radio has a 48-bit unique device address (BD_ADDR) that is fixed.
- Two or more radio devices together form ad-hoc networks called piconets. All units within a piconet share the same channel.
- Each piconet has one master device and one or more slaves. There may be up to seven active slaves at a time within a piconet. Thus, each active device within a piconet is identifiable by a 3-bit active device address. Inactive slaves in unconnected modes may continue to reside within the piconet.
- A master is the only one that may initiate a Bluetooth communication link. However, once a link is established, the slave may request a master/slave switch to become the master.
- Slaves are not allowed to talk to each other directly. All communication occurs within the slave and the master. Slaves within a piconet must also synchronize their internal clocks and frequency hops with that of the master.
- Each piconet uses a different frequency hopping sequence. Radio devices used Time Division Multiplexing (TDM).
- A master device in a piconet transmits on even numbered slots and the slaves may transmit on odd numbered slots.

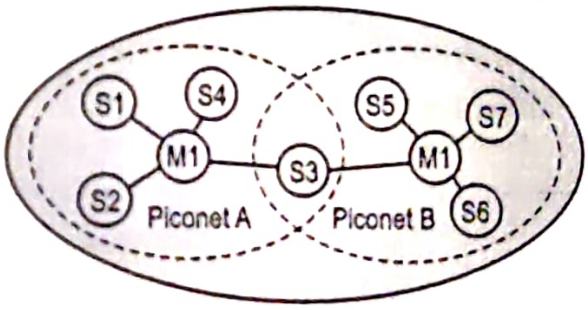


Fig. 4.44: Bluetooth Scatternets and Piconets

- Multiple piconets with overlapping coverage areas form a scatternet. Each piconet may have only one master, but slaves may participate in different piconets on a time-division multiplex basis.
- A device may be a master in one piconet and a slave in another or a slave in more than one piconet.

4.9.2.1 Piconet Architecture

- A Bluetooth network is called a *piconet* or a small net.
- A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries.

- All the secondary stations synchronize their clocks and hopping sequence with the primary. Note that a piconet can have only one primary station.
- The communication between the primary and the secondary can be one-to-one or one-to-many. Fig. 4.45 shows a piconet architecture of bluetooth.

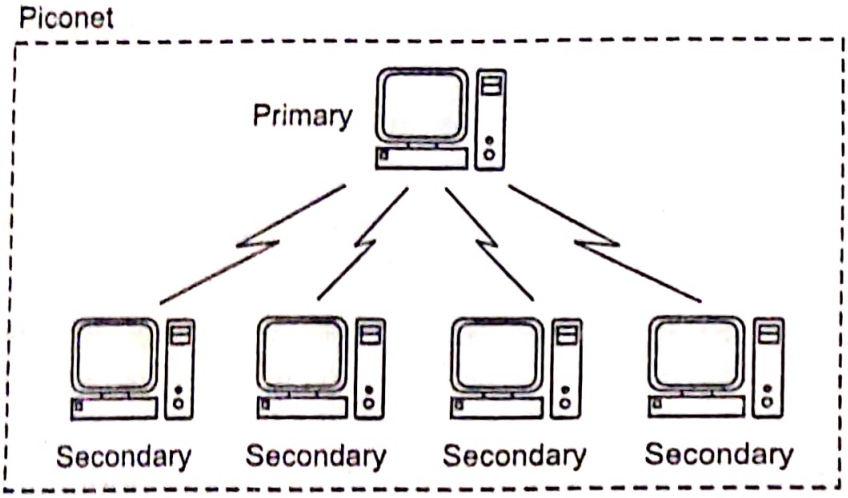


Fig. 4.45: A Piconet Architecture

- Although a piconet can have a maximum of seven secondaries, an additional eight secondaries can be in the *parked state*.
- A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state.
- Because only eight stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

4.9.2.2 Scatternet Architecture

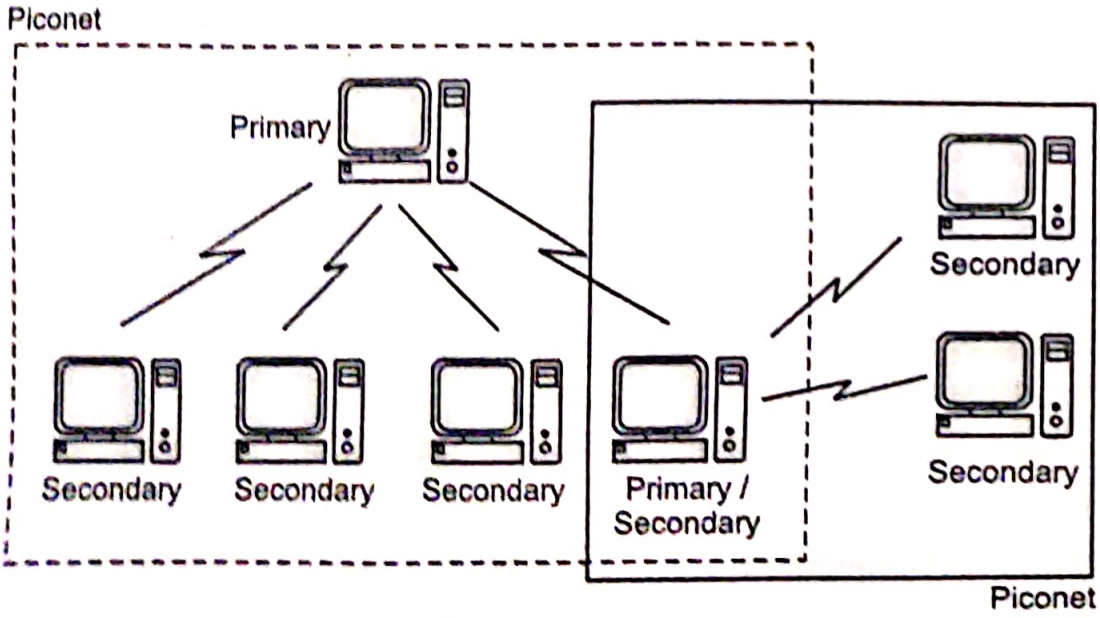


Fig. 4.46: Scatternet Architecture

Piconets can be combined to form what is called a scatternet.

- A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet.
- A station can be a member of two piconets. Fig. 4.46 illustrates a scatternet architecture of bluetooth.

4.9.3 Bluetooth Protocol Stack

- The heart of the Bluetooth specification is the Bluetooth protocol stack. By providing well-defined layers of functionality, the Bluetooth specification ensures interoperability of Bluetooth devices and encourages adoption of Bluetooth technology.
- As you can see in Fig. 4.47 these layers range from the low-level radio link to the profiles.

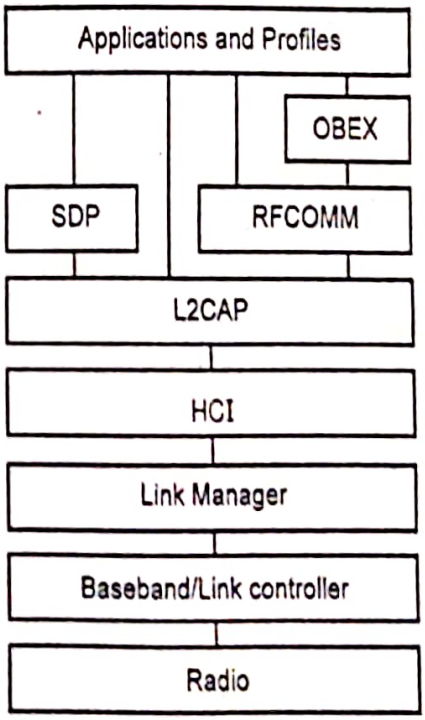


Fig. 4.47: Bluetooth Protocol Stack

4.9.3.1 Lower Layers (Radio, Baseband, Link Control Layers)

- At the base of the Bluetooth protocol stack is the **radio layer.**
- The radio module in a Bluetooth device is responsible for the modulation and demodulation of data into RF signals for transmission in the air.
- The radio layer describes the physical characteristics of the Bluetooth receiver-transmitter components.
- These include modulation characteristics, radio frequency tolerance, and sensitivity level.
- Above the radio layer is the **baseband and link controller layer.**

- The Bluetooth specification does not establish a clear distinction between the responsibilities of the baseband and those of the **link controller**.
- The best way to think about it is that the baseband portion of the layer is responsible for properly formatting data for transmission to and from the radio layer. In addition, it handles the synchronization of links.
- The link controller portion of this layer is responsible for carrying out the link manager's commands and establishing and maintaining the link stipulated by the **link manager**.
- The link manager itself translates the **Host Controller Interface** (HCI) commands it receives into baseband-level operations.
- It is responsible for establishing and configuring links and managing power-change requests, among other tasks.
- The Bluetooth specification defines two types of links between Bluetooth devices:
  1. **Synchronous, Connection-Oriented (SCO),** for isochronous and voice communication using, for example, headsets.
  2. **Asynchronous, Connectionless (ACL),** for data communication, such as the exchange of vCards.
- Each link type is associated with a specific packet type.
- A **SCO** link provides reserved channel bandwidth for communication between a master and a slave, and supports regular, periodic exchange of data with no retransmission of SCO packets.
- An ACL link exists between a master and a slave the moment a connection is established.
- The data packets Bluetooth uses for **ACL** links all have 142 bits of encoding information in addition to a payload that can be as large as 2712 bits.
- The extra amount of data encoding heightens transmission security. It also helps to maintain a robust communication link in an environment filled with other devices and common noise.
- The HCI **(Host Controller Interface)** layer acts as a boundary between the lower layers of the Bluetooth protocol stack and the upper layers.
- The Bluetooth specification defines a standard **HCI** to support Bluetooth systems that are implemented across two separate processors.
- For example, a Bluetooth system on a computer might use a Bluetooth module's processor to implement the lower layers of the stack (radio, baseband, link controller, and link manager). It might then use its own processor to implement the upper layers (**L2CAP, RFCOMM, OBEX**, and Selected profiles).
- In this scheme, the lower portion is known as the Bluetooth module and the upper portion as the Bluetooth host.

- Of course, it is not required to partition the Bluetooth stack in this way. Bluetooth headsets, for example, combine the module and host portions of the stack on one processor because they need to be small and self-contained.
- In such devices, the HCI may not be implemented at all unless device testing is required.
- Because the Bluetooth HCI is well defined, you can write drivers that handle different Bluetooth modules from different manufacturers. Apple provides an HCI controller object that supports a USB implementation of the HCI layer.

4.9.3.2 Upper Layers

L2CAP Layer:

- Above the HCI layer are the upper layers of the protocol stack. The first of these is the **L2CAP (Logical link control and Adaptation protocol)** layer.
- The L2CAP is primarily responsible for:
  1. Establishing connections across existing ACL links or requesting an ACL link if one does not already exist.
  2. Multiplexing between different higher layer protocols, such as RFCOMM and SDP, to allow many different applications to use a single ACL link.
  3. Repackaging the data packets it receives from the higher layers into the form expected by the lower layers.
- The **L2CAP** employs the concept of channels to keep track of where data packets come from and where they should go.
- You can think of a channel as a logical representation of the data flow between the L2CAP layers in remote devices.
- Because it plays such a central role in the communication between the upper and lower layers of the Bluetooth protocol stack, the L2CAP layer is a required part of every Bluetooth system.
- Above the L2CAP layer, the remaining layers of the Bluetooth protocol stack are not quite so linearly ordered.
- However, it makes sense to discuss the service discovery protocol next, because it exists independently of other higher-level protocol layers. In addition, it is common to every Bluetooth device.

Service Discovery Protocol (SDP):

- **The SDP (Service Discovery Protocol)** defines actions for both servers and clients of Bluetooth services. The specification defines a service as any feature that is usable by another (remote) Bluetooth device. A single Bluetooth device can be both a server and a client of services.
- **An SDP** client communicates with an SDP server using a reserved channel on an L2CAP link to find out what services are available. When the client finds the desired

service, it requests a separate connection to use the service. The reserved channel is dedicated to SDP communication so that a device always knows how to connect to the SDP service on any other device. An SDP server maintains its own SDP database, which is a set of service records that describe the services the server offers. Along with information describing how a client can connect to the service, the service record contains the service's UUID, or Universally Unique Identifier.

Radio Frequency Communication (RFCOMM):

- Above the L2CAP layer is the **RFCOMM layer**. This is the most important layer in the Bluetooth architecture. The RFCOMM protocol emulates the serial cable line settings and status of an RS-232 serial port. RFCOMM connects to the lower layers of the Bluetooth protocol stack through the L2CAP layer.
- It connects the serial ports of all the devices according to the requirement. It also supports the OBEX protocol.

OBEX (Object Exchange):

- OBEX (Object Exchange) is a transfer protocol that defines data objects and a communication protocol two devices can use to easily exchange those objects. Bluetooth adopted OBEX from the IrDA IrOBEX specification because the lower layers of the IrOBEX protocol are very similar to the lower layers of the Bluetooth protocol stack.
- In addition, the IrOBEX protocol is already widely accepted and therefore a good choice for the Bluetooth SIG, which strives to promote adoption by using existing technologies.
- A Bluetooth device wanting to set up an OBEX communication session with another device is considered to be the client device.
  1. The client first sends SDP requests to make sure the other device can act as a server of OBEX services.
  2. If the server device can provide OBEX services, it responds with its OBEX service record. This record contains the RFCOMM channel number the client should use to establish an RFCOMM channel.
  3. Further communication between the two devices is conveyed in packets, which contain requests, responses, and data. The format of the packet is defined by the OBEX session protocol.

4.9.4 Bluetooth Frame Structure

- There are several frame formats of the Bluetooth the most and important common of which is shown in Fig. 4.39.
- Bluetooth frame begins with an access code that usually identifies the master so that slaves within radio range of two masters can tell which traffic is for them.
- Next comes a 54-bit header containing typical MAC sublayer fields. Then comes the data field, of up to 2744 bits.

Header field:

- Let us take a quick look at the header of Bluetooth frame.
  - **The Address field:** Identifies which of the eight active devices the frame is intended for.
  - **Type field:** Identifies the frame type, the type of error correction used in the data field, and how many slots long the frame is.
  - **Flow bit:** Flow bit is asserted by a slave when its buffer is full and cannot receive any more data.
  - **Acknowledgement bit:** It is used to piggyback an ACK onto a frame.
  - **Sequence bit:** It is used to number the frames to detect retransmission; the protocol is stop-and-wait, so 1 bit is enough.
  - **Checksum:** Then comes the 8-bit header Checksum.
- The entire 18-bit header is repeated three times to form the 54-bit header shown in Fig. 4.48.
- On the receiving side, a simple circuit examines all three copies of each bit. If all three are the same, the bit is accepted. If not, the majority opinion wins. Thus, 54 bits of transmission capacity are used to send 10 bits of header.

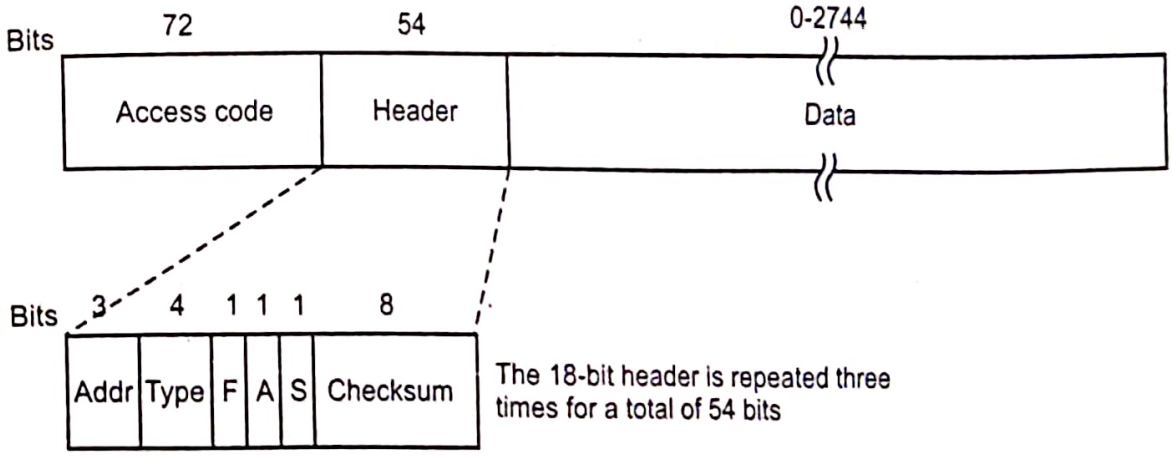


Fig. 4.48: A Typical Bluetooth Data Frame

4.10 BLUETOOTH APPLICATIONS

Important application of Bluetooth are given below:

- It allows a transfer of images (or) word documents (or) applications (or) audio and video files between devices without the help of cables.
- It can be used for remote sales technology allowing wireless access to vending machines and other commercial enterprises.
- It provides inter accessibility of PDAs, palmtops and desktops for file and data exchanges.
- It can be used to setup a personal area network (PAN) or a wireless personal area network (WPAN).

- It is used in the short-range transmission of data from sensors devices to sensor nodes like mobile phones.
- It is used by modern healthcare devices to send signals to monitors.

Summary

- A WLAN, or wireless LAN, is a network that allows devices to connect and communicate wirelessly. Unlike a traditional wired LAN, in which devices communicate over Ethernet cables, devices on a WLAN communicate via Wi-Fi.
- IEEE 802 is a collection of networking standards that cover the physical and data-link layer specifications for technologies such as Ethernet and wireless.
- IEEE 802 specifications also split the data link layer into two different layers: an LLC layer and a MAC layer.
- IEEE Standards are: 802 - LAN/MAN, 802.1 - Media access control (MAC), 802.2 - Logical Link Control (LLC), 802.3 - Carrier Sense Multiple Access with Collision Detection (CSMA/CD),802.11 - Wireless Networking "WiFi".
- A standard Ethernet network can transmit data at a rate up to 10 Megabits per second (10 Mbps). Other LAN types include Token Ring, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM) and LocalTalk.
- In computer networks, Fast Ethernet is a variation of Ethernet standards that carry data traffic at 100 Mbps (Mega bits per second) in local area networks (LAN).
- Gigabit Ethernet, a transmission technology based on the Ethernet frame format and protocol used in local area networks (LANs), provides a data rate of 1 billion bits per second (one gigabit).
- 10 gigabit Ethernet is a telecommunication technology that offers data speeds up to 10 billion bits per second.
- A backbone or core network is a part of a computer network which interconnects pieces of various networks, providing a path for the exchange of information between different LANs or subnetworks.
- Backbone network contains a Distributed (Bus backbone) and collapsed backbone (Star backbone).
- A VLAN (virtual LAN) is a subnetwork which can group together collections of devices on separate physical local area networks (LANs).
- Wireless LANs (WLANs) are wireless computer networks that use high-frequency radio waves instead of cables for connecting the devices within a limited area forming LAN (Local Area Network). Users connected by wireless LANs can move around within this limited area such as home, school, campus, office building, railway platform, etc.

- Bluetooth wireless technology is a worldwide specification for a small-form factor, low-cost radio solution that provides links between mobile computers, mobile phones, other portable handheld devices, and connectivity to the Internet.

Check Your Understanding

1. Ethernet frame consists of _____.
   (a) MAC address (b) IP address
   (c) Default mask (d) Network address
2. MAC address is of _____.
   (a) 24 bits (b) 36 bits
   (c) 42 bits (d) 48 bits
3. In a backbone, the _____ backbone is a just switch.
   (a) bus (b) ring
   (c) star (d) mesh
4. An interconnected collection of Piconet is called _____.
   (a) Scatternet (b) Micronet
   (c) Mininet (d) Multinet
5. Bluetooth is the wireless technology for _____.
   (a) Local area network
   (b) Personal area network
   (c) Metropolitan area network
   (d) Wide area network

ANSWERS

1. (a)	2. (d)	3. (c)	4. (a)	5. (b)

Practice Questions

Q.I Answer the following questions in short.

1. What is IEEE standards?
2. Describe Fast Ethernet.
3. What is network interface card?
4. What is Wireless LAN?
5. What is Bluetooth in WLAN?

Q.II Answer the following questions.

1. Write a short note on IEEE standards 802.11.
2. How Bluetooth works?
3. With suitable diagram describe Bluetooth architecture.
4. Write short notes on:

i) Scartternet architecture.

ii) Piconet architecture.

5. What is VLAN? What are types of VLAN?
6. What is Backbone network?
7. What is Ethernet? What are its types? Explain any one.
8. What are the different categories of Fast Ethernet?
9. Explain BSS and ESS in detail.

Q.III Define the following terms:

1. Ethernet
2. Star backbone
3. Bus backbone
4. VLAN
5. CSMA/CD

Previous Exams Questions

Summer 2018

1. Describe the frame format and physical layer of Ethernet. SM

Ans. Please refer to section 4.4.5 and 4.5.

2. Explain Bluetooth in detail. SM

Ans. Please refer to section 4.9.

3. Write short note on: MAC sublayer with its frame format. SM

Ans. Please refer to section 4.4.4.

Winter 2018

1. Explain Bluetooth in detail. SM

Ans. Please refer to section 4.9.

2. Write short note on: MAC sublayer with its frame format. SM

Ans. Please refer to section 4.4.4.

Summer 2019

1. Explain IEEE 802.11 in detail. SM

Ans. Please refer to section 4.8.5.

2. Describe the frame format and physical layer of Ethernet. SM

Ans. Please refer to sections 4.4.5 and 4.5.

3. Write short note on: Bluetooth. SM

Ans. Please refer to section 4.9.