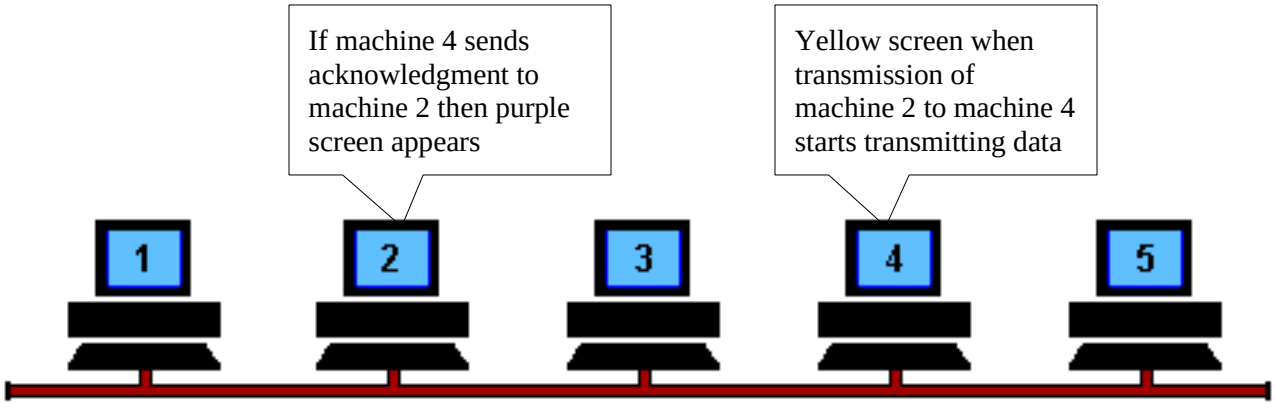
Unit 4: Wired and Wireless LAN:

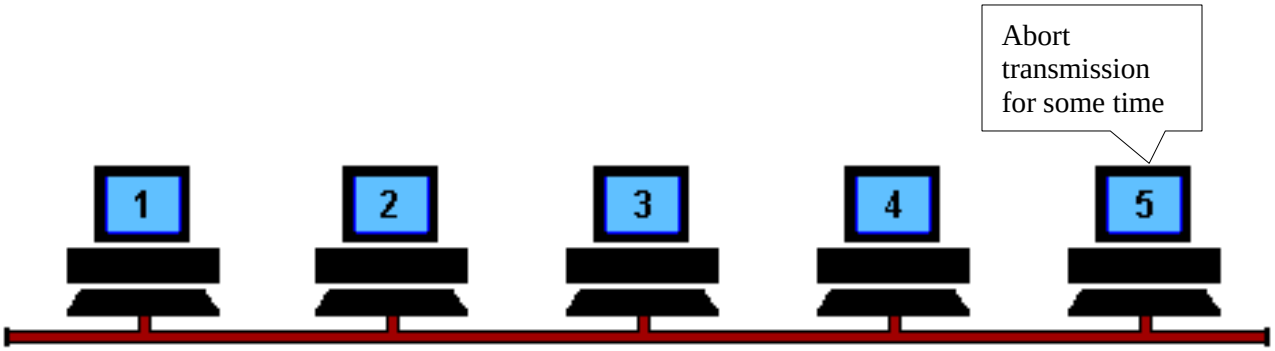
Introduction of IEEE standards:-

- 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, whereas Virtual LAN and priority data in 802.3ac it is extended to 1522 bytes. If the upper layer protocol submit a protocol data unit (PDU) less than 46 bytes.
- The original Ethernet is called as Experimental Ethernet today. It was developed by Robert Metcalfe in 1972 and was based in part on wireless ALOHnet protocol.
- In the last several years, the demand on the network has increased drastically. The old 10 Base5 and 10Base2 Ethernet network were replaced by 10BaseT hubs, allowing for greater manageability of network and the cable plant. AS application increased the demand on the network, newer, high-speed protocols such as FDDI and ATM became available.
- The standards body working on Gigabit Ethernet is the IEEE 802.3z 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.
- CSMA/CD based LAN proposed by IEEE 802.3 subcommittee, commonly known as Ethernet.

1. **IEEE standards 802.3 (Ethernet)**
   - Ethernet is the most widely-installed Local Area Network technology (LAN).
   - Ethernet specified in a standard called IEEE 802.3
   - An Ethernet LAN typically uses coaxial cable or twisted pair wires. It provides speeds up to 10 Mbps.
   - The devices connected to the LAN complete for access using CSMA/CD protocol.



- Machine 2 wants to send a message to machine 4, but first it listen 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. 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 2 acknowledging receipt of the data.
- As we stared before, there is a possibility of two machines try to transmit simultaneously over the cable. The result can be observed in following fig.



- 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.

a. ***CSMA/CD***:-

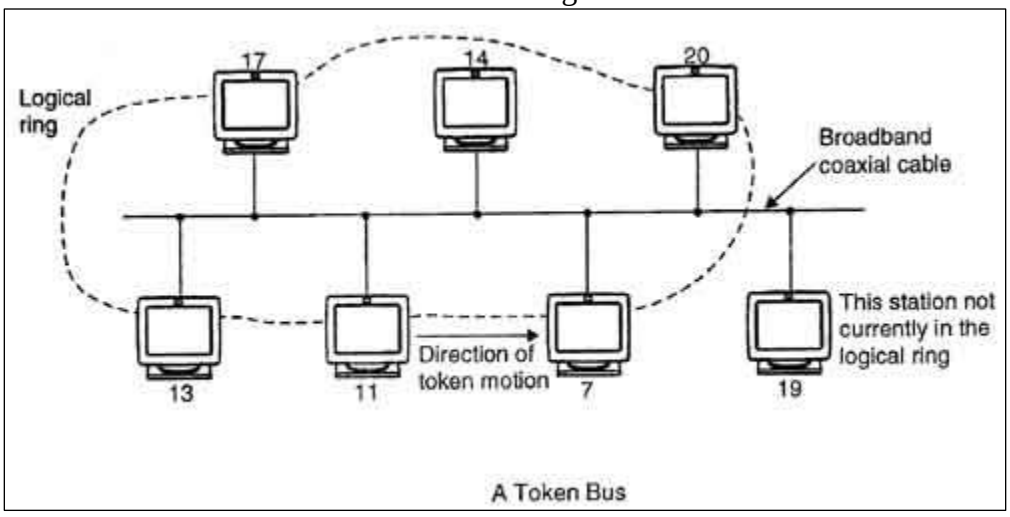
- Carrier Sense Multiple Access with collision Detection is a protocol used to sense whether a medium is busy transmission but is the ability to detect whether a transmission has collided with another.
- CSMA/CD is the protocol used in Ethernet networks to ensure that only one network node is transmitting on the network wire at any one time.
- Carrier Sense means that every Ethernet device listen 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 at a time.
- Collision detection means that when multiple Ethernet devices accidentally transmitted at the same time, they are able to detect this error.
- If the Ethernet system gets clogged up, the CSMA/CD will take the necessary steps to unlock it.
- Working of CSMA/CD:-
  i. A method of CSMA/CD was used to send data over shared single coaxial cable connected to all computers on a network.
  ii. In this method, the computer terminals transmit the data over the 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.

b. ***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 prevents collisions before they happen.
- In CSMA/CA, as soon as a node received packets that are to be sent, it checks to be sure the channel is clear. If the channel is clear, then packet is sent. If the channel is not clear, the nodes wait for a randomly chosen period of time, and then check again to see the channel is clear.
- This period of time is called as backoff factor, and is counted down by a backoff counter.

IEEE 802.4: Token Bus Network

- 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.
- Through 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 nTP seconds to get a turn for a station.



A Token Bus

- When the logical ring is initialized, the highest numbered station may send the first frame.
- The token and frames of data are passed from one station to another following the numeric sequence of the station addresses. Thus, the token follows a logical ring rather than a physical ring.
- The last station in numeric order passes the token back to the first station.
- The token does not follow the physical ordering of workstation attachment to the cable.
- Station 1 might be at one end of the cable and station 2 might be at the other, with station 3 in the middle.

- In such a case, there is no collision as only one station possesses a token at any given time. In token bus, each station receives each frame; the station whose address is specified in the frame processes it and the other stations discard the frame.

MAC Sublayer Function

• When the ring is initialized, stations are inserted into it in order of station address, from highest to lowest.
• Token passing is done from high to low address.
• Whenever a station acquires the token, it can transmit frames for a specific amount of time.
• If a station has no data, it passes the token immediately upon receiving it.
• The token bus defines four priority classes, 0, 2, 4, and 6 for traffic, with 0 the lowest and 6 the highest.
• Each station is internally divided into four substations, one at each priority level *i.e.* 0,2,4 and 6.
• As input comes in to the MAC sublayer from above, the data are checked for priority and routed to one of the four substations.
• Thus each station maintains its own queue of frames to be transmitted.
• When a token comes into the station over the cable, it is passed internally to the priority 6 substation, which can begin transmitting its frames, if it has any.
• When it is done or when its time expires, the token is passed to the priority 4 substation, which can then transmit frames until its timer expires. After this the token is then passed internally to priority 2 substation.
• This process continues until either the priority 0 substation has sent all its frames or its time expires.
• After this the token is passed to the next station in the ring.

Frame format of Token Bus

The various fields present in the frame format are

1. **Preamble**: This. Field is at least 1 byte long. It is used for bit synchronization.

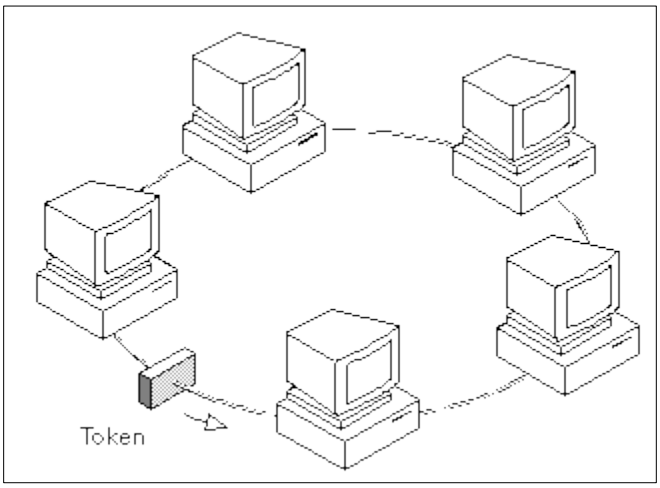
1 byte	1 byte	1 byte	2-6 bytes	2–6 byte	0–8182	4 bytes	1 byte
Preamble	Start delimiter	Frame control	Destination Address	Source Address	Data	Checksum	End Delimiter

Frame format of IEEE 802.4

2. **Start Delimiter**: This one byte field marks the beginning of frame.
3. **Frame Control:** This one byte field specifies the type of frame. It distinguishes data frame from control frames. For data frames it carries frame's priority. For control frames, it specifies the frame type. The control frame types include. Token passing and various ring maintenance frames, including the mechanism for letting new station enter the ring, the mechanism for allowing stations to leave the ring.
4. **Destination address**: It specifies 2 to 6 bytes destination address.
5. **Source address**: It specifies 2 to 6 bytes source address.
6. **Data**: This field may be upto 8182 bytes long when 2 bytes addresses are used & upto 8174 bytes long when 6 bytes address is used.
7. **Checksum**: This 4 byte field detects transmission errors.
8. **End Delimiter**: This one byte field marks the end of frame.

IEEE 802.5: Token Ring Network

- Token Ring is formed by the nodes connected in ring format as shown in the diagram below. 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 atmost be one transmission at a time.
- Since the token rotates in the ring it is guaranteed that every node gets the token with in 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.

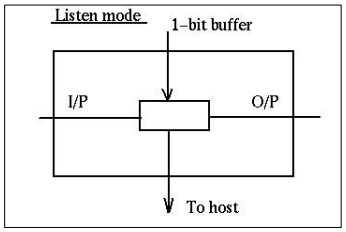


Propagation delay + transmission of n-bits (1-bit delay in each node) > transmission of the token time

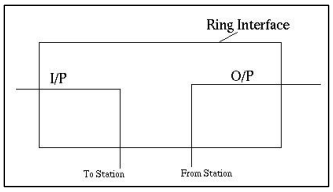
- A station may hold the token for the token-holding time. Which is 10 ms unless the installation sets a different value?
- If there is enough time left after the first frame has been transmitted to send more frames, then these frames may be sent as well.
- After all pending frames have been transmitted 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

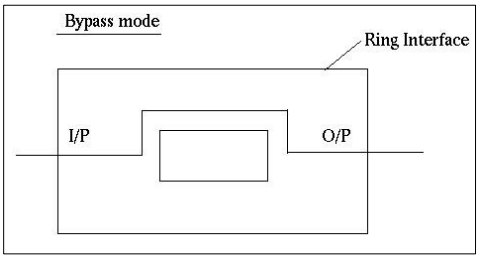
1. **Listen Mode:** In this mode the node listens to the data and transmits the data to the next node. In this mode there is a one-bit delay associated with the transmission.



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

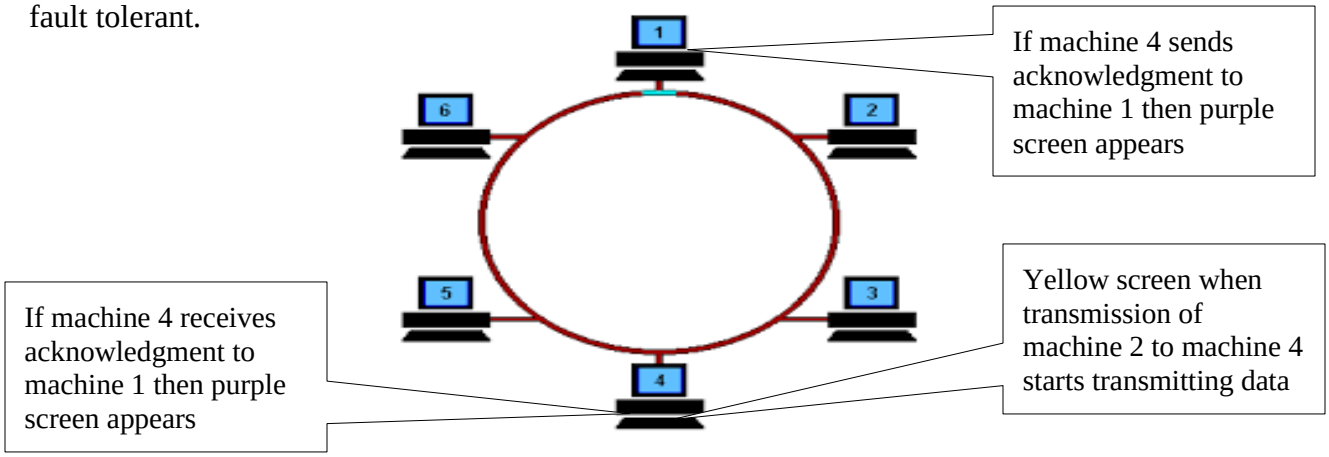


3. **By-pass Mode:** In this mode reached when the node is down. Any data is just bypassed. There is no one-bit delay in this mode.



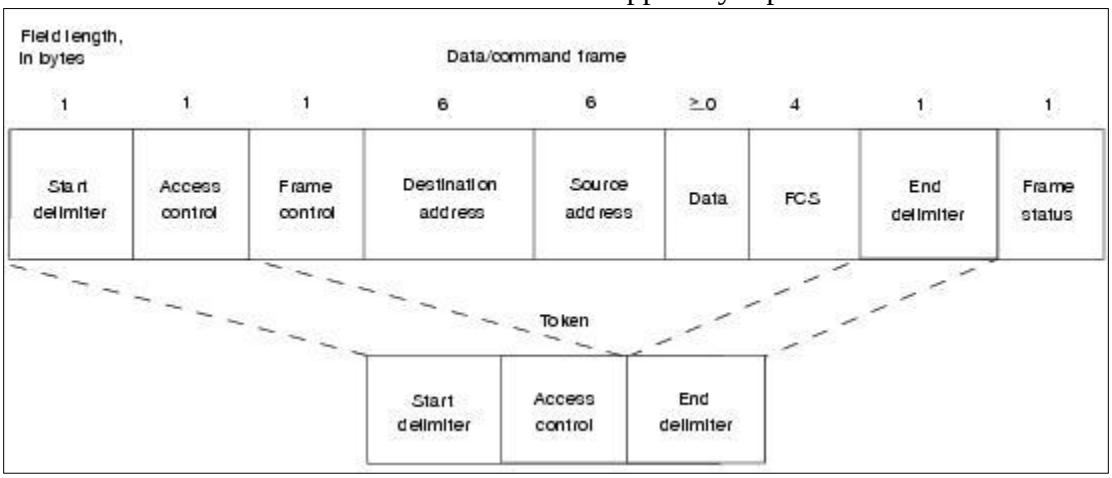
How Token Ring Works:

- At the start, a free Token is circulating on the ring; this is a data frame which to all intents and purposes is an empty vessel for transporting data.
- To use the network, a machine first has to capture the free Token and replace the data with its own message.
- In the example above, machine 1 wants to send some data to machine 4, so it first has to capture the free Token. It then writes its data and the recipient's address onto the Token (represented by the yellow flashing screen).
- The packet of data is then sent to machine 2 who reads the address, realizes it is not its own, so passes it on to machine 3.
- Machine 3 does the same and passes the Token on to machine 4.
- This time it is the correct address and so number 4 reads the message (represented by the yellow flashing screen).
- It cannot, however, release a free Token on to the ring, it must first send the frame back to number 1 with an acknowledgement to say that it has received the data (represented by the purple flashing screen).
- The receipt is then sent to machine 5 who checks the address, realizes that it is not its own and so forwards it on to the next machine in the ring, number 6.Machine 6 does the same and forwards the data to number 1, who sent the original message.
- Machine 1 recognizes the address, reads the acknowledgement from number 4 (represented by the purple flashing screen) and then releases the free Token back on to the ring ready for the next machine to use.
- That's the basics of Token Ring and it shows how data is sent, received and acknowledged, but Token Ring also has a built in management and recovery system which makes it very fault tolerant.



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.



i) Token Frame Fields

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

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

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 Figure 9-3 are described in the following summaries:

- **Start delimiter** - Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.
- **Access-control byte** - Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).
- **Frame-control bytes** - Indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.
- **Destination and source addresses** - Consists of two 6-byte address fields that identify the destination and source station addresses.

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

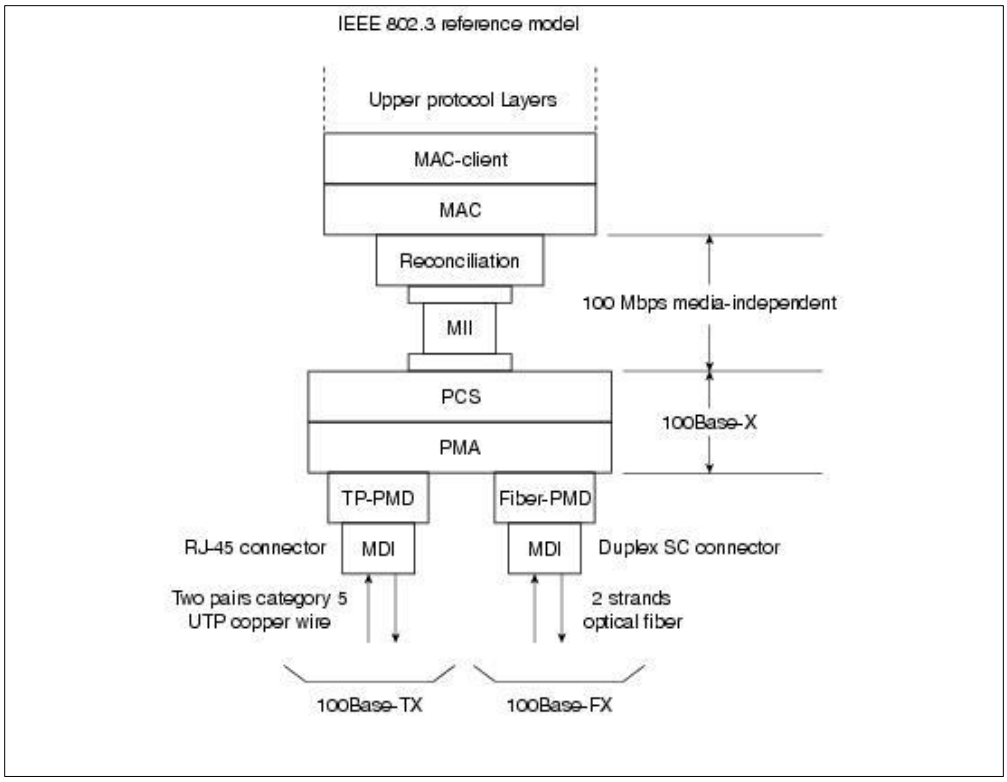
FAST ETHERENT:-

- The Fast Ethernet standards (IEEE802.3u) have 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 suffering and stronger error detection and correction.
- There are three types of Fast Ethernet: 100BASE-TX for use with level 5 UTP cable; 100 BASE-FX for use with fiber-optic cable; and 100 BASE-t4 which utilizes an extra two wires for use with level 3 UTP cable.
- 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 be reconfigured specifically.

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.
- The signal transceivers that were included as part of the PMA function in the generic logical model of the following figure were redefined as the separate physical media-dependent (PMD) sub layers shown in Figure: The 100Base-X Logical Model.

Figure: The 100Base-X Logical Model

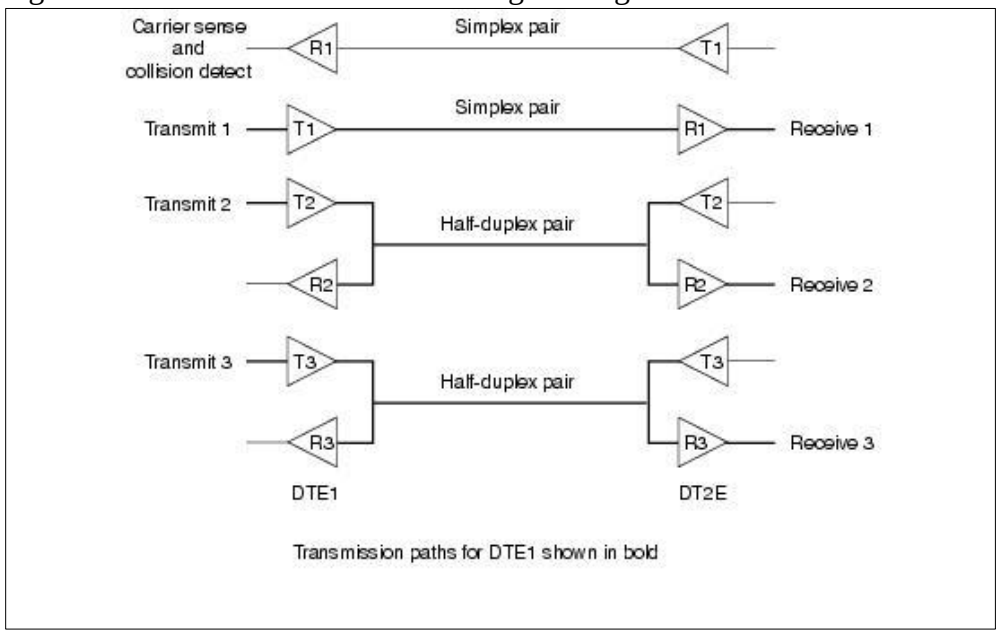


- The 100Base-X encoding procedure is based on the earlier FDDI optical fiber physical media-dependent and FDDI/CDDI copper twisted-pair physical media-dependent signaling standards developed by ISO and ANSI
- The 100Base-TX physical media-dependent sub layer (TP-PMD) was implemented with CDDI semiconductor 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.
- 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.

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 Figure: The 100Base-T4 Wire-Pair Usage during Frame Transmission.
- The simplex pair for the opposite direction provides carrier sense and collision detection. Full-duplex operation cannot be supported on 100Base-T4.

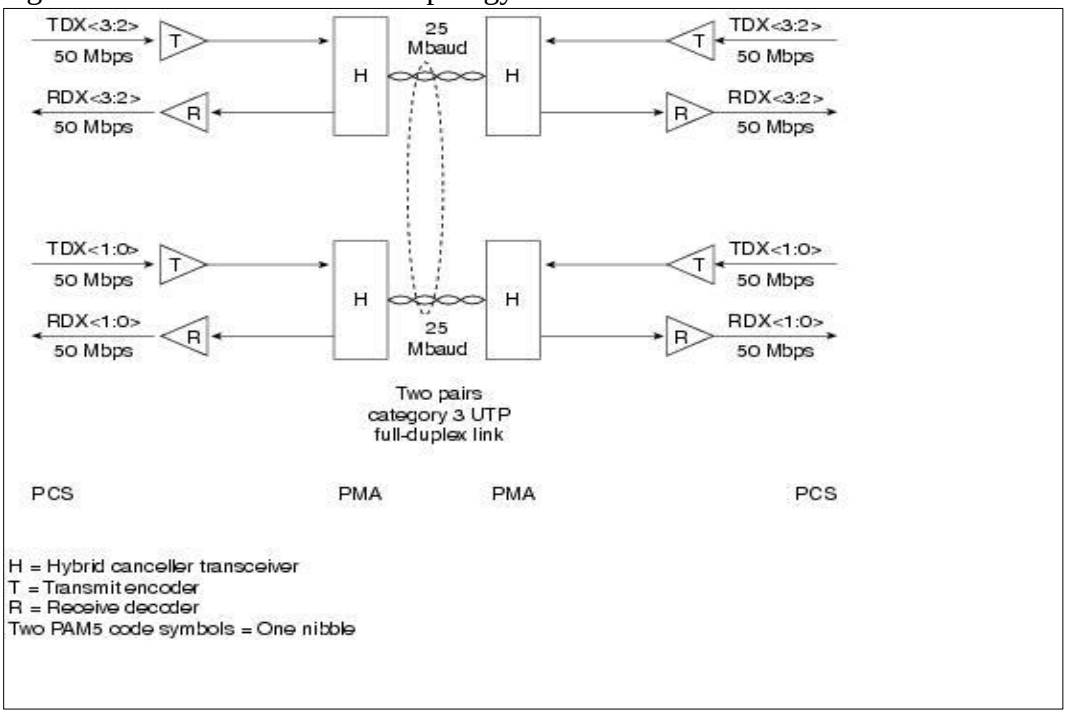
Figure: The 100Base-T4 Wire-Pair Usage during Frame Transmission



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, as shown in Figure: The 100Base-T2 Link Topology. 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.

Figure: The 100Base-T2 Link Topology

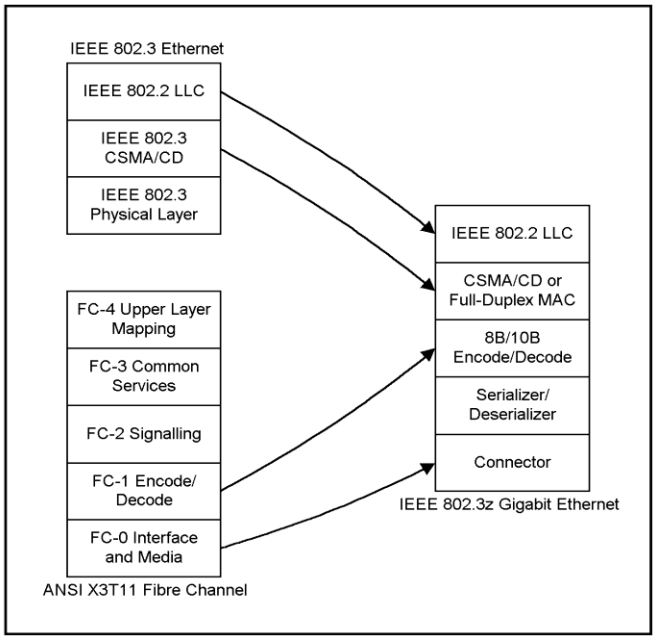


Gigabit Ethernet

- Since its inception at Xerox Corporation in the early 1970s, 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 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.
- The purpose of this technology brief is to provide a technical overview of Gigabit Ethernet. This paper discusses:
  - The architecture of the Gigabit Ethernet protocol, including physical interfaces, 802.3x flow control, and media connectivity options
  - The Gigabit Ethernet standards effort and the timing for Gigabit Ethernet
  - Comparison of Gigabit Ethernet and Asynchronous Transfer Mode (ATM) technologies
  - Gigabit Ethernet topologies
  - Migration strategies to Gigabit Ethernet
- Gigabit Ethernet Protocol Architecture
  - 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.

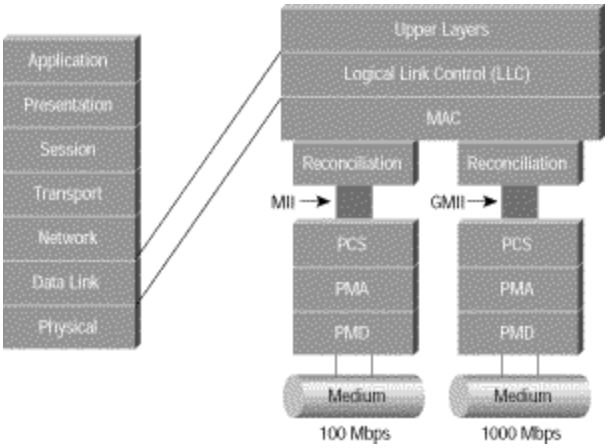
- The challenges involved in accelerating to 1 Gbps have been resolved by merging two technologies together: IEEE 802.3 Ethernet and ANSI X3T11 FiberChannel.
- Figure 1 show how key components from each technology have been leveraged to form Gigabit Ethernet.

Figure : Gigabit Ethernet Protocol Stack



- Leveraging these two technologies means that the standard can take advantage of the existing high-speed physical interface technology of FibreChannel 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 collision detect (CSMA/CD). This scenario helps minimize the technology complexity, resulting in a stable technology that can be quickly developed.
- The actual model of Gigabit Ethernet is shown in Figure 2. Each of the layers will be discussed in detail.

Figure 2: Architectural Model of IEEE 802.3z Gigabit Ethernet



Media Access Control Layer
Logical Link Layer

- 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. Figure describes the IEEE 802.3/Ethernet frame format.

Figure: Ethernet Frame Format

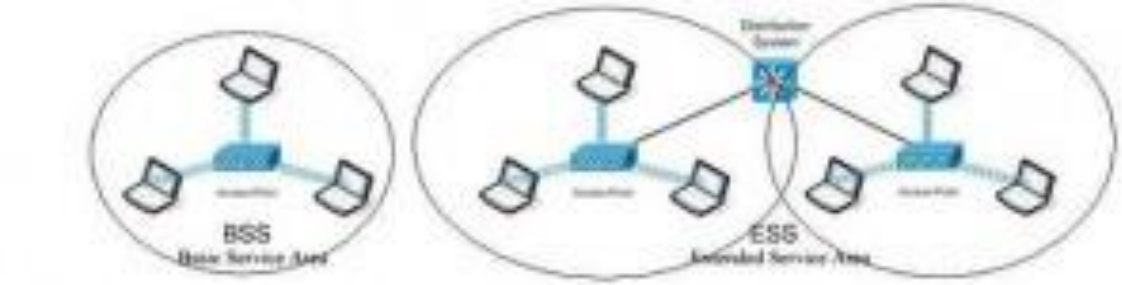


- The original Xerox specification identified a *type* field, which was utilized for protocol identification.
- The IEEE 802.3 specification eliminated the *type* field, replacing it with the *length* field.
- The *length* field is used to identify the length in bytes of the data field. The protocol types in 802.3 frames are left to the data portion of the packet.
- 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.

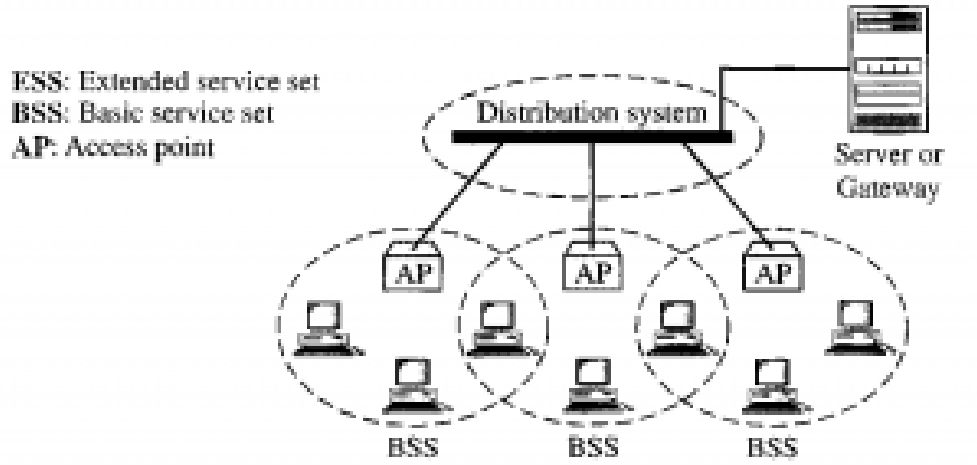
- Therefore, additional information must be added to the LLC in order to provide information regarding those protocols. Protocols that fall into this category include IP and IPX.
- The method used to provide this additional protocol information is called a Sub-network Access Protocol, or SNAP frame. 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.

IEEE 802.11

- IEEE has defined the specifications for wireless LAN, named IEEE 802.11., which covers both physical and data link layers.
- IEEE 802.11 defines two types of services which are
  1) Basic Service Set (BSS)
  2) Extended Service Set (ESS)
- **Basic Service Set (BSS):**
  - IEEE 802.11 has defined the BSS as the basic building block of wireless LAN.
  - A BSS is made of stationary or moving wireless stations and a central base station called as the access point (AP).



  - BSS can exist with and without AP. BSS without access point cannot send data to another BSS.
  - So, it is known as a standalone network or ad **hoc architecture**. In this type of architecture stations can form a network without using AP.
- **Extended Service Set (ESS):**
  - An extended service set consists of two or more BSSs with access points. The BSS in this system are connected to each other via a distribution system which is generally a wired LAN.
  - The distribution system connects the access points to each other. The distribution system can be any type LAN such as **Ethernet**. thus ESS contains two types of station:
    i. Mobile Stations
    ii. Stationary of non-moving stations



- Out of these, the non-moving stations are the access points which are a part of the wired LAN whereas the mobile stations are those contained in the BSS.
- The BSSs are connected to each other to form a network called infrastructure network. In such networks the station close to each other can communicate taking help of access points.
- But if two stations are located in two different BSS wish to communicate with each other, than they have to do through access points. This type of communication is very similar to that in the cellular communication. The BSS acts as a cell and AP as base station.
- **Types of Stations in ESS are as follow:**
  There are three types of stations are defined by IEEE 802.11 depending on their mobility in the wireless LAN as
  - **No transition Mobility:** It is defined as a station which is non-moving (stationary) or moving only inside a BSS.
  - **BSS Transition Mobility:** A station having BSS transition mobility is the one which can move from BSS to another but does not move outside one ESS.
  - **ESS transition Mobility:** A station having ESS transition mobility is the one which can move from one ESS to another. But IEEE 802.11 does not guarantee communication when the station is moving.

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 DM.
   i. Frequency Hopping Spread Spectrum (FHSS):
   - 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 shows frame format of FHSS

- 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.

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
- The longer the chip, the greater the probability that the original data can be recovered and, of course, the more bandwidth required.
- 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 as the spreading code.
- Fig shows the frame format of DSSS.

- The 128 bit preamble is used for signal detection.
- The SFD stands for start of frame delimited.
- 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. OFDM:

- OFDM stands for orthogonal Frequency Division Multiplexing.
- OFDM multicarrier spread spectrum technique.
- In OFDM, high rate serial data stream divided into numerous parallel low-rate data stream that are modulated by a set of subcarrier.

2. May Layer:-

- IEEE 802.11 defines two MAC sublayers i.e. the distributed Coordination Function (DCF) and Point Coordinate Function (PCF).
- MAC layer consists of nine fields as shown in fig:

- Frame control The FC field is 2 bytes long and defines the type of frame and some control information.
- D: In all frames, this field defines the duration of the transmission that is used to set the value of NAV.
- Address: 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.
- Sequence Control:- This fields 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 defines in the FC field.
- FCS: This field is used for error detection.

Bluetooth Communication:-

- 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.

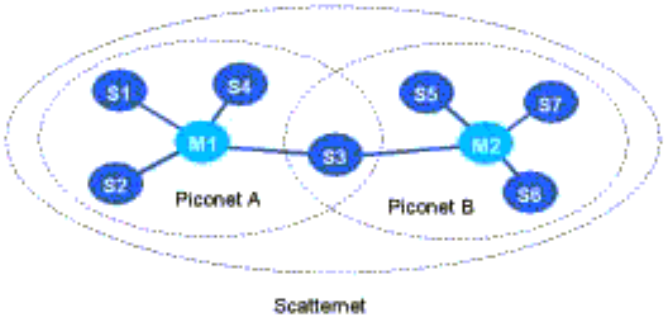
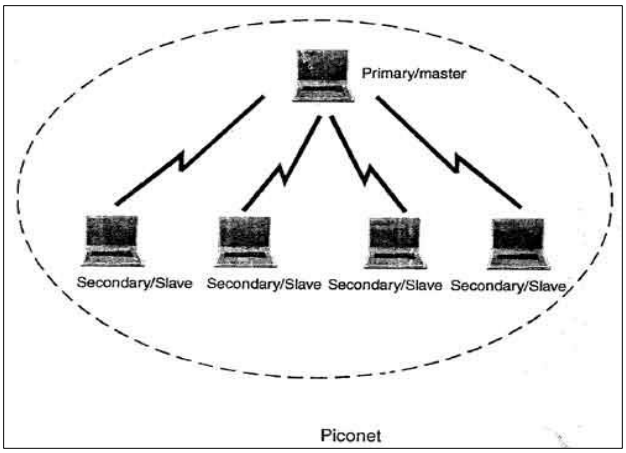


Fig 1: Bluetooth Scatternets and Piconets

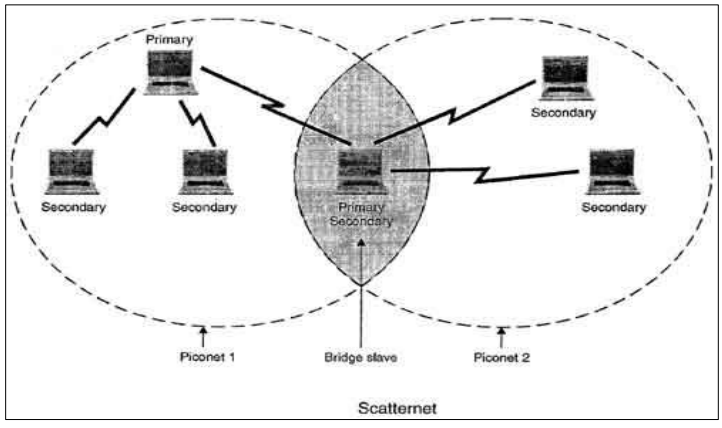
- Multiple piconets with overlapping coverage areas form a scatternet. Each piconet may have only one master, but slaves may participate in different piconets on a time-division multiplex basis. A device may be a master in one piconet and a slave in another or a slave in more than one piconet.
- **Bluetooth Architecture**
  Bluetooth architecture defines two types of networks:
  1. Piconet
  2. Scatternet

1. Piconet



• Piconet is a Bluetooth network that consists of one primary (master) node and seven active secondary (slave) nodes.
• Thus, piconet can have upto eight active nodes (1 master and 7 slaves) or stations within the distance of 10 meters.
• There can be only one primary or master station in each piconet.
• The communication between the primary and the secondary can be one-to-one or one-to-many.
• All communication is between master and a slave. Salve-slave communication is not possible.
• In addition to seven active slave station, a piconet can have upto 255 parked nodes. These parked nodes are secondary or slave stations and cannot take part in communication until it is moved from parked state to active state.

2. Scatternet

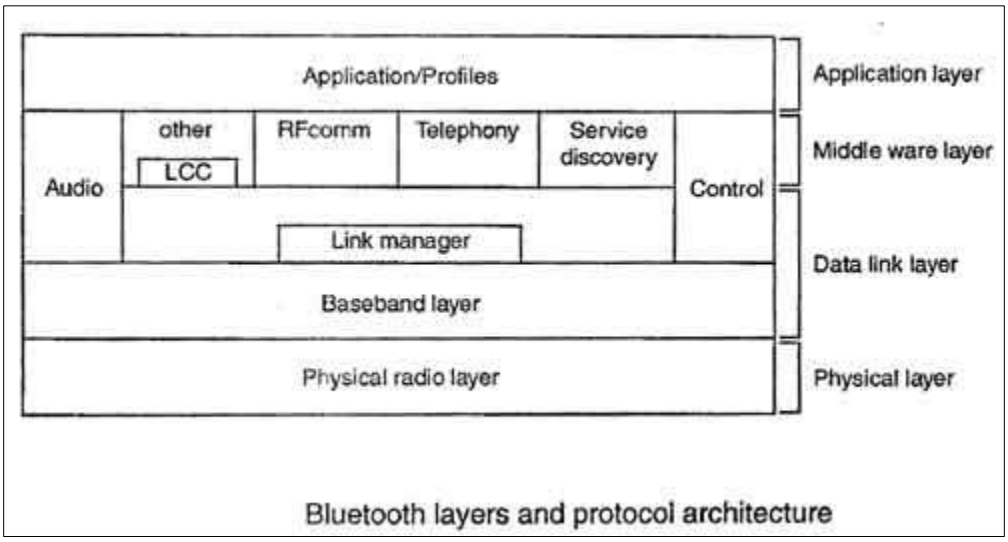


• Scatternet is formed by combining various piconets.
• A slave in one piconet can act as a master or primary in other piconet.
• Such a station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master. This node is also called bridge slave.
• Thus a station can be a member of two

piconets.
• A station cannot be a master in two piconets.

Bluetooth layers and Protocol Stack

• Bluetooth standard has many protocols that are organized into different layers.
• The layer structure of Bluetooth does not follow OS1 model, TCP/IP model or any other known model.
• The different layers and Bluetooth protocol architecture.



Bluetooth layers and protocol architecture

1. **Radio Layer**
   - The Bluetooth radio layer corresponds to the physical layer of OSI model.
   - It deals with ratio transmission and modulation.
   - The radio layer moves data from master to slave or vice versa.
   - It is a low power system that uses 2.4 GHz ISM band in a range of 10 meters.
   - This band is divided into 79 channels of 1MHz each. Bluetooth uses the Frequency Hopping Spread Spectrum (FHSS) method in the physical layer to avoid interference from other devices or networks.
   - Bluetooth hops 1600 times per second, *i.e.* each device changes its modulation frequency 1600 times per second.
   - In order to change bits into a signal, it uses a version of FSK called GFSK *i.e.* FSK with Gaussian bandwidth filtering.
2. **Baseband Layer**
   - Baseband layer is equivalent to the MAC sublayer in LANs.
   - Bluetooth uses a form of TDMA called TDD-TDMA (time division duplex TDMA).
   - Master and slave stations communicate with each other using time slots.
   - The master in each piconet defines the time slot of 625 µsec.
   - In TDD- TDMA, communication is half duplex in which receiver can send and receive data but not at the same time.
   - If the piconet has only no slave; the master uses even numbered slots (0, 2, 4, ...) and the slave uses odd-numbered slots (1, 3, 5, ...). Both master and slave communicate in half duplex mode. In slot 0, master sends & secondary receives; in slot 1, secondary sends and primary receives.

- If piconet has more than one slave, the master uses even numbered slots. The slave sends in the next odd-numbered slot if the packet in the previous slot was addressed to it.
- In Baseband layer, two types of links can be created between a master and slave. These are:
  a. **Asynchronous Connection-less (ACL)**
    - It is used for packet switched data that is available at irregular intervals.
    - ACL delivers traffic on a best effort basis. Frames can be lost & may have to be retransmitted.
    - A slave can have only one ACL link to its master.
    - Thus ACL link is used where correct delivery is preferred over fast delivery.
    - The ACL can achieve a maximum data rate of 721 kbps by using one, three or more slots.
  b. **Synchronous Connection Oriented (SCO)**
    - sco is used for real time data such as sound. It is used where fast delivery is preferred over accurate delivery.
    - In a sco link, a physical link is created between the master and slave by reserving specific slots at regular intervals.
    - Damaged packet; are not retransmitted over sco links.
    - A slave can have three sco links with the master and can send data at 64 Kbps.

3. **Logical Link, Control Adaptation Protocol Layer (L2CAP)**

- The logical unit link control adaptation protocol is equivalent to logical link control sublayer of LAN.
- The ACL link uses L2CAP for data exchange but sco channel does not use it.

The various function of L2CAP is:

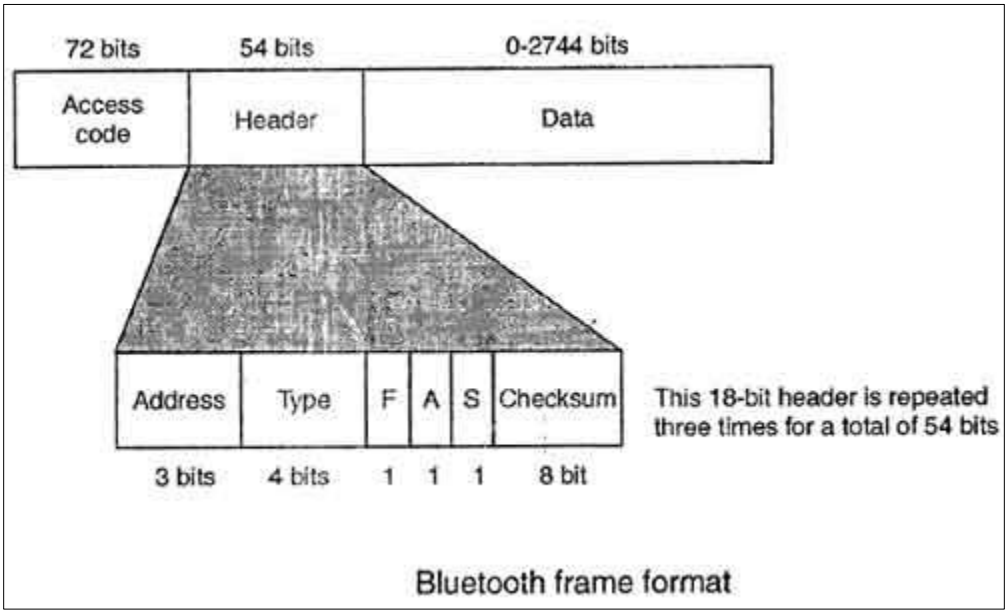
a. Segmentation and reassembly
- L2CAP receives the packets of upto 64 KB from upper layers and divides them into frames for transmission.
- It adds extra information to define the location of frame in the original packet.
- The L2CAP reassembles the frame into packets again at the destination.

b. Multiplexing
- L2CAP performs multiplexing at sender side and demultiplexing at receiver side.
- At the sender site, it accepts data from one of the upper layer protocols frames them and deliver them to the Baseband layer.
- At the receiver site, it accepts a frame from the baseband layer, extracts the data, and delivers them to the appropriate protocol1ayer.

4. **Quality of Service (QOS)**
   - L2CAP handles quality of service requirements, both when links are established and during normal operation.
   - It also enables the devices to negotiate the maximum payload size during connection establishment.

Bluetooth Frame Format

The various fields of blue tooth frame format are:



Bluetooth frame format

1. **Access Code**: It is 72 bit field that contains synchronization bits. It identifies the master.
2. **Header**: This is 54-bit field. It contain 18 bit pattern that is repeated for 3 time.
   The header field contains following subfields:
   (i) **Address**: This 3 bit field can define upto seven slaves (1 to 7). If the address is zero, it is used for broadcast communication from primary to all secondaries.
   (ii)Type: This 4 bit field identifies the type of data coming from upper layers.
   (iii) **F**: This flow bit is used for flow control. When set to 1, it means the device is unable to receive more frames.
   (iv) **A**: This bit is used for acknowledgement.
   (v) **S**: This bit contains a sequence number of the frame to detect retransmission. As stop and wait protocol is used, one bit is sufficient.
   (vi) **Checksum**: This 8 bit field contains checksum to detect errors in header.
3. **Data**: This field can be 0 to 2744 bits long. It contains data or control information coming from upper layers