BLUETOOTH

- Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, and so on. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously.
- Bluetooth technology has several applications. Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology.
- Today, Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard.

Architecture:

Bluetooth defines two types of networks: piconet and scatternet.

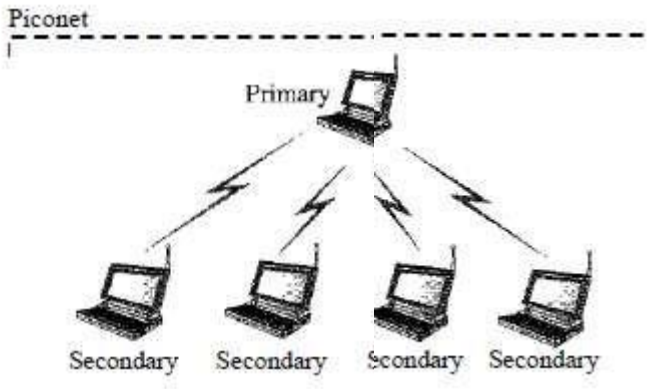
Piconets

- A Bluetooth network is called a piconet, or a small net. A piconet can have up to eightstations, one of which is called the primary the rest are called secondaries.
- Note that a piconet can have only one primary station. The communication between theprimary and the secondary can be one-to-one or one-to-many.

Fig: Piconet.

- 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.

Scatternet:



- 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.

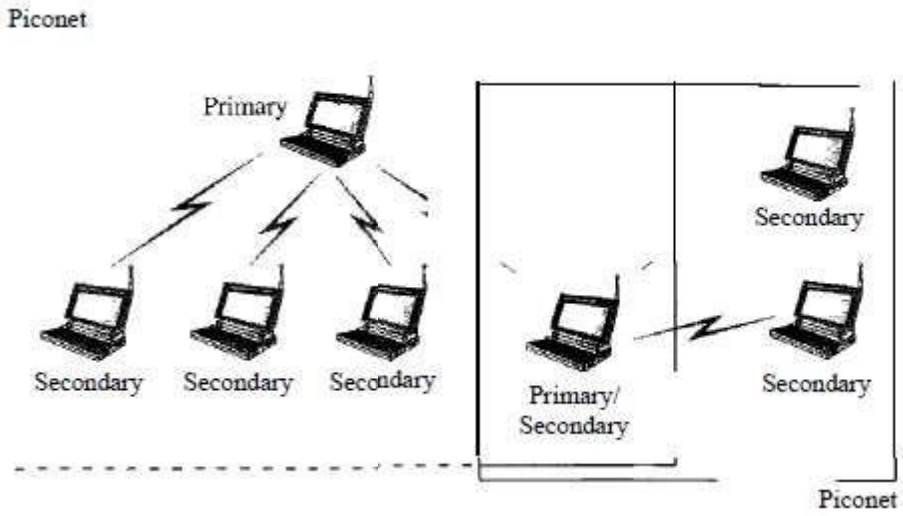


Fig: Scatternet.

Bluetooth Devices:

- A Bluetooth device has a built-in short-range radio transmitter. The current data rate is1 Mbps with a 2.4-GHz bandwidth.

Bluetooth Layers

- Bluetooth uses several layers.

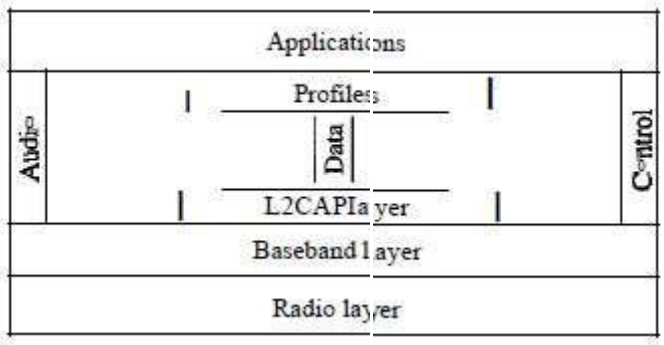


Fig: Bluetooth layers.

Radio Layer

- The radio layer is roughly equivalent to the physical layer of the Internet model. Bluetooth devices are low-power and have a range of 10 m.

Band

- Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.

FHSS

- Bluetooth uses the frequency-hopping spread spectrum (FHSS) method in the physical layer to avoid interference from other devices or other networks.
- Bluetooth hops 1600 times per second.

Modulation:

- Bluetooth uses a sophisticated version of FSK, called GFSK. GFSK has a carrier frequency. Bit 1 is represented by a frequency deviation above the carrier; bit ()is represented by a frequency deviation below the carrier. The frequencies, in megahertz

Baseband Layer:

- The baseband layer is roughly equivalent to the MAC sub layer in LANs. The access method is TDMA. The primary and secondary communicate with each other using time slots.
- Note that the communication is only between the primary and a secondary; secondaries cannot communicate directly with one another.

TDMA:

- Bluetooth uses a form of TDMA. TDD-TDMA (time division duplex TDMA). TDD-TDMA is a kind of half-duplex communication in which the secondary and receiver send and receive data, but not at the same time.
- This issimilar to walkie-talkies using different carrier frequencies.

Single-Secondary Communication:

- If the piconet has only one secondary, the TDMA operation is very simple. The primary uses even numbered slots (0, 2, 4, ...); the secondary uses odd-numbered slots (1, 3, 5, ...).
- TDD-TDMA allows the primary and the secondary to communicate in half-duplex mode. In slot 0, the primary sends, and the secondary receives; in slot 1, the secondary sends, and the primary receives. The cycle is repeated.

Multiple-Secondary Communication:

- The process is a little more involved if there ismore than one secondary in the piconet. The primary uses the even-numbered slots,but a secondary sends in the next odd-numbered slot if the packet in the previous slot wasaddressed to it.

- All secondaries listen on even-numbered slots, but only one secondary sends in any odd-numbered slot.

Physical Links

- Two types of links can be created between a primary and a secondary: SCQ links and ACL links.
- SCO A synchronous connection-oriented (SCO)
- ACL An asynchronous connectionless link (ACL)

Frame Format:

- Access code. This 72-bit field normally contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from another.

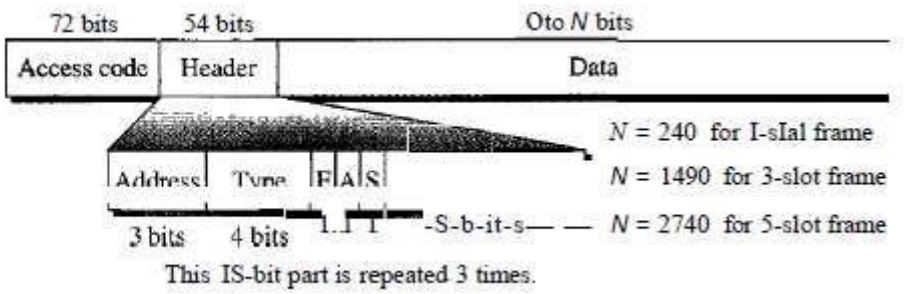


Fig: Frame formattypes.

- Header. This 54-bit field is a repeated I8-bit pattern. Each pattern has the following subfields:

1. **Address.** The 3-bit address subfield can define up to seven secondaries (Ito 7). If the address is zero, it is used for broadcast communication from the primary to all secondaries.
2. **Type.** The 4-bit type subfield defines the type of data coming from the upper layers. We discuss these types later.
3. **F**. This I-bit subfield is for flow control. When set (1), it indicates that the device is unable to receive more frames (buffer is full).
4. **A**. This I-bit subfield is for acknowledgment. Bluetooth uses Stop-and-Wait ARQ; 1 bit is sufficient for acknowledgment.
5. **S**. This I-bit subfield holds a sequence number. Bluetooth uses Stop-and-Wait ARQ; 1 bit is sufficient for sequence numbering.
6. **HEC**. The 8-bit header error correction subfield is a checksum to detect errors in each 18-bit header section.

Payload. This subfield can be 0 to 2740 bits long. It contains data or control information corning from the upper layers.

L2CAP

- The Logical Link Control and Adaptation Protocol, or L2CAP (L2 here means LL),is roughly equivalent to the LLC sublayer in LANs. It is used for data exchange on an ACL link; SCQ channels do not use L2CAP.The L2CAP has specific duties: multiplexing, segmentation and reassembly, quality of service (QoS), and group management.

Fig: L2CAP data packet format.

Multiplexing

- The L2CAP can do multiplexing. At the sender site, it accepts data from one of the upper-layer protocols, frames them, and delivers 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 protocol layer.

Segmentation and Reassembly:

- The L2CAP divides these large packets into segments and adds extra information to define the location of the segments in the original packet. TheL2CAP segments the packet at the source and reassembles them at the destination.

QoS

- Bluetooth allows the stations to define a quality-of-service level.

Group Management

- Another functionality of L2CAP is to allow devices to create a type of logical addressing between themselves. This is similar to multicasting.

Other Upper Layers

- Bluetooth defines several protocols for the upper layers that use the services of L2CAP;these protocols are specific for each purpose.

DATA LINK CONTROL (DLC)

DLC SERVICES

Data link control functions include framing and flow and error control.

1. Framing

- Data transmission in the physical layer means moving bits in the form of a signal from the source to the destination.
- The physical layer provides bit synchronization to ensure that the sender and receiver use the same bit duration and timing.
- The data-link layer, on the other hand, needs to pack bits into frames, so that each frame is distinguishable from another.
- Framming in the data-link layer separates a message from one source to a destination by adding a sender address and a destination address. The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

Frame size

- Frames can be fixed or variable size. In fixed size framing, there is no need for defining the boundaries of the frames; The size itself can be used as a delimiter. In variable size framing, prevalent in local – area networks. In variable size framing, we need a way to define the end of one frame and the beginning of the next.

Character-Oriented Framming

- In character-oriented (or byte-oriented) framing, data to be carried are 8-bit characters from a coding system such as ASCII. The header, which normally carries the source and destination addresses and other control information, and the trailer, which carries error detection redundant bits.

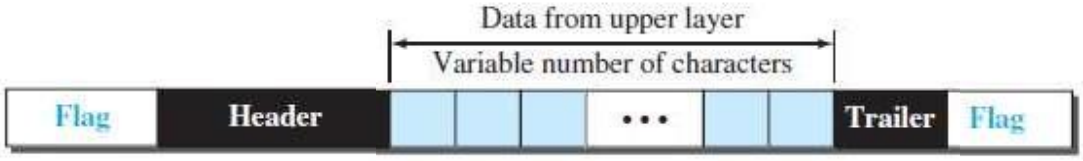


Fig1 : A frame in a character-oriented protocol.

- In byte stuffing (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag.
- The data section is stuffed with an extra byte.
- The byte is usually called the escape character (ESC) and has a predefined bit pattern.
- Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not as a delimiting flag.
- Fig 2 shows the situation.

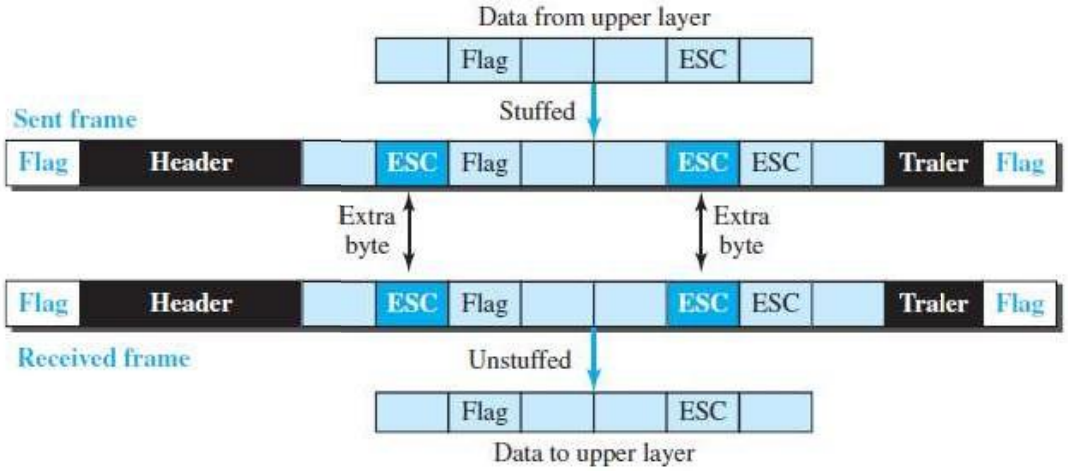


Fig 2: Byte stuffing and unstuffing

- Byte stuffing is the process of adding one extra byte whenever there is a flag or escape character in the text.

Bit Oriented Framming

- In bit-oriented framing, in addition to headers we still need a delimiter to separate one frame from the other.
- Most protocols use a especial 8 bit pattern flag, 01111110, as the delimeter to define the begining and end of the frame, as shown in fig3

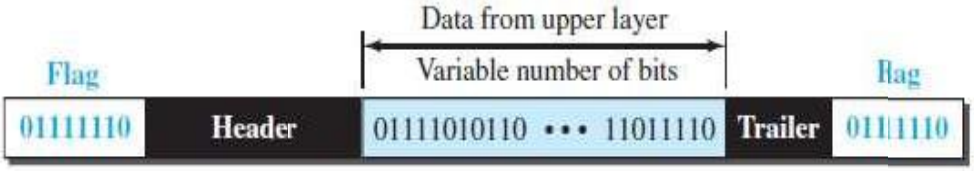


Fig 3: A frame in a bit-oriented protocol

- This flag can create the same type of problem, to prevent the pattern from looking like a flag.

- The stragery is called bit stuffing.
- Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow 0 in the data, so that the receiver does not mistake the pattern 01111110 for a flag.

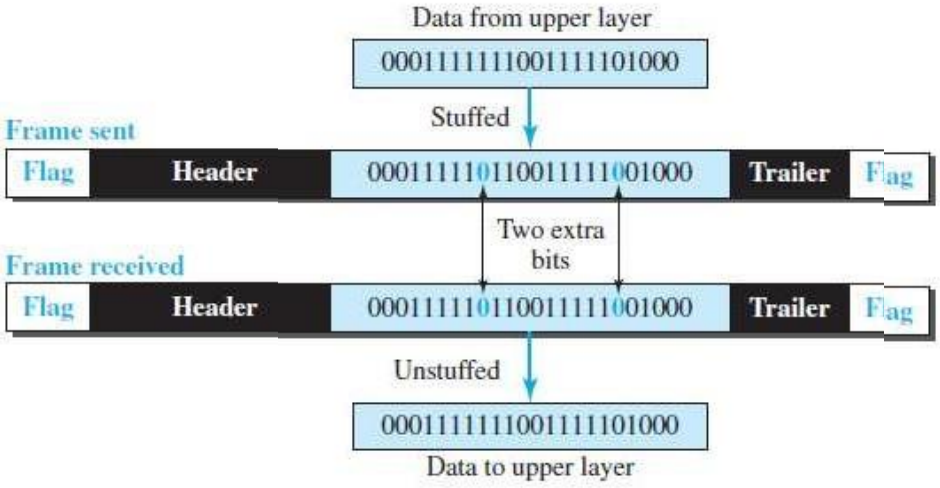


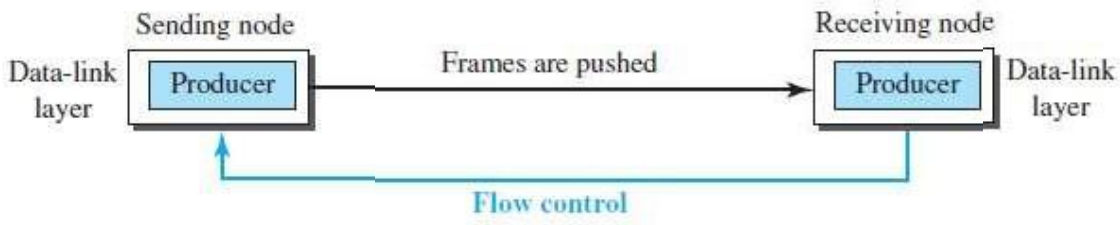
Fig 4: Bit stuffing and unstuffing

2. **Flow and Error Control**
   - One of the responsibilities of the data-link control sublayer is flow and error control at the data- link layer.

   Flow Control
   - Whenever an entity produces items and another entity consumes them, there should be a balance between production and consumption rates.
   - If the items are produced faster than they can be consumed, the consumer can be overwhelmed and may need to discard some items.
   - We need to prevent losing the data items at the consumer site for that flow control is needed

Fig 5: Flow control at the data-link layer

- The figure shows that the data-link layer at the sending node tries to push frames toward the data-link layer at the receiving node.



- If the receiving node cannot process and deliver the packet to its network at the same rate that the frame arrive, it becomes overwhelmed with frames.
- Flow control in this case can be feedback from the receiving node to the sending node to stop or slow down pushing frames.

Buffers:

- Although flow control can be implemented in several ways, one of the solutions is normally to use two buffers; one at the sending data-link layer and the other at the receiving data-link layer.
- A buffer is a set of memory locations that can hold packets at the sender and receiver.
- The flow control communication can occur by sending signals from the consumer to the producer.
- When the buffer of the receiving data–link layer is full, it informs the sending data–link layer to stop pushing frames.

Error Control:

- We need to implement error control at the data-link layer to prevent the receiving node from delivering corrupted packets to its network layer. Error control at the data-link layer is normally very simple and implemented using one of the following two methods.
  - In the first method, if the frame is corrupted, it is silently discarded; if it is not corrupted, the packet is delivered to the network layer. This method is used mostly in wired LANs such as Ethernet.
  - In the second method, if the frame is corrupted, it is silently discarded; if it is not corrupted, an acknowledgment is sent (for the purpose of both flow and error control) to the sender.

Combination of flow and Error Control

- Flow and error control can be combined, In a simple situation, the acknowledgment that is sent for flow control can also be used for error control to tell the sender the packet has arrived uncorrupted.

Connectionless and connection-oriented

A DLC protocol can be either connectionless or connection oriented.

Connectionless Protocol:

- In a connectionless protocol, frames are sent from one node to the next without any relationship between the frames; each frame is independent.

- Note that the term connectionless here does not mean that there is no physical connection between the nodes; it means that there is no connection between frames.
- The frames are not numbered and there is no sense of ordering.
- Most of the data-link protocols for LANs are connectionless protocols.

Connection-Oriented Protocols:

- In a connection-oriented protocol, a logical connection should first be established between the two nodes.(setup phase)
- After all frames that are somehow related to each other are transmitted, the logical connection is terminated.(transfer phase)
- In this type of communication, the frames are numbered and sent in order.
- If they are not received in order, the receiver needs to wait until all frames belonging to the same set are received and then deliver them in order to the network layer.

DATA-LINK LAYER PROTOCOLS

Four protocols have been defined for the data-link layer to deal with flow and error control: Simple, Stop-and-Wait, Go-Back-N, and Selective- Repeat.

Simple Protocol:

- Our first protocol is a simple protocol with neither flow nor error control. We assume that the receiver can immediately handle any frame it receives.
- In other words, the receiver can never be overwhelmed with incoming frames.

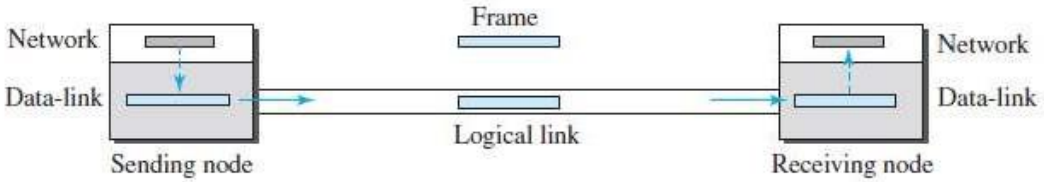


Fig 6: Simple Protocol.

- The data- link layer at the sender gets a packet from its network layer, makes a frame out of it, and sends the frame.
- The data-link layer at the receiver receives a frame from the link, extracts the packet from the frame, and delivers the packet to its network layer.
- The data-link layers of the sender and receiver provide transmission services for their network layers.

FSMs

- The sender site should not send a frame until its network layer has a message to send.
- The receiver site cannot deliver a message to its network layer until a frame arrives.
- Each FSM has only one state, the ready state. The sending machine remains in the ready state until a request comes from the process in the network layer.
- When this event occurs, the sending machine encapsulates the MESSAZGE in a frame and sends it to the receiving machine.
- The receiving machine remains in the ready state until a frame arrives from the sending machine
- When this event occurs, the receiving machine decapsulates the message out of the frame and delivers it to the process at the network layer.

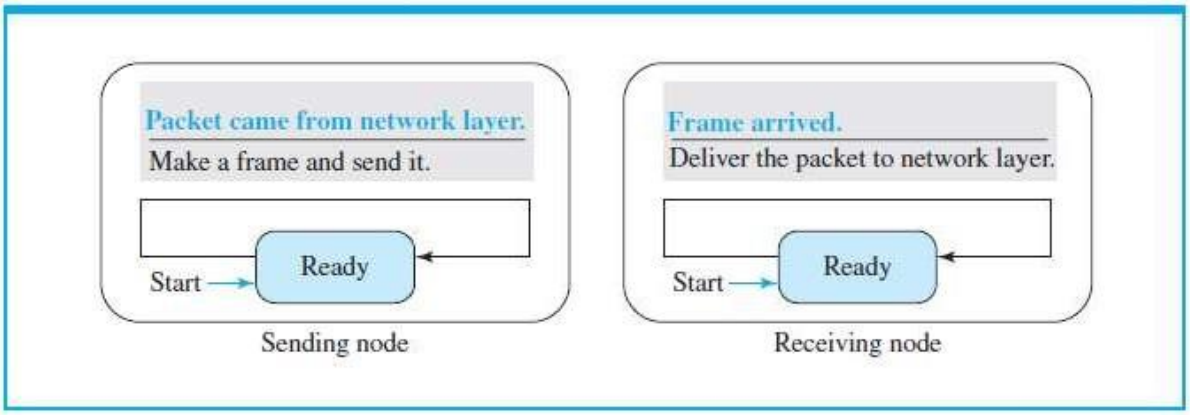


Fig: FSMs for the simple protocol

Stop and Wait Protocol

- Our Second protocol is called the Stop-and-Wait protocol, which uses both flow and error control
- In this protocol, the sender sends one frame at a time and waits for an acknowledgement before sending the next one.
- To detect corrupted frames, we need to add a CRC to each data frame.
- When a frame arrives at the receiver site, it is checked. If its CRC is incorrect, the frame is corrupted and silently discarded.
- The silence of the receiver is a signal for the sender that a frame was either corrupted or lost.
- Every time the sender sends a frame, it starts a timer. If an acknowledgment arrives before the timer expires, the timer is stopped and the sender sends the next frame (if it has one to send).

- If the timer expires, the sender resends the previous frame, assuming that the frame was either lost or corrupted.
- This means that the sender needs to keep a copy of the frame until its acknowledgment arrives.
- When the corresponding acknowledgment arrives, the sender discards the copy and sends the next frame if it is ready.

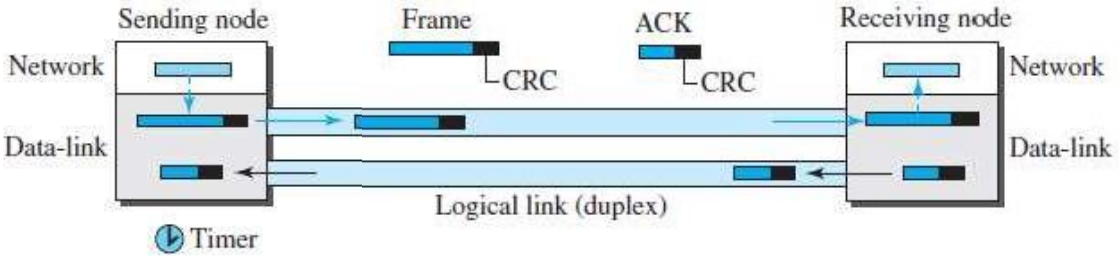


Fig: Stop-and-Wait protocol.

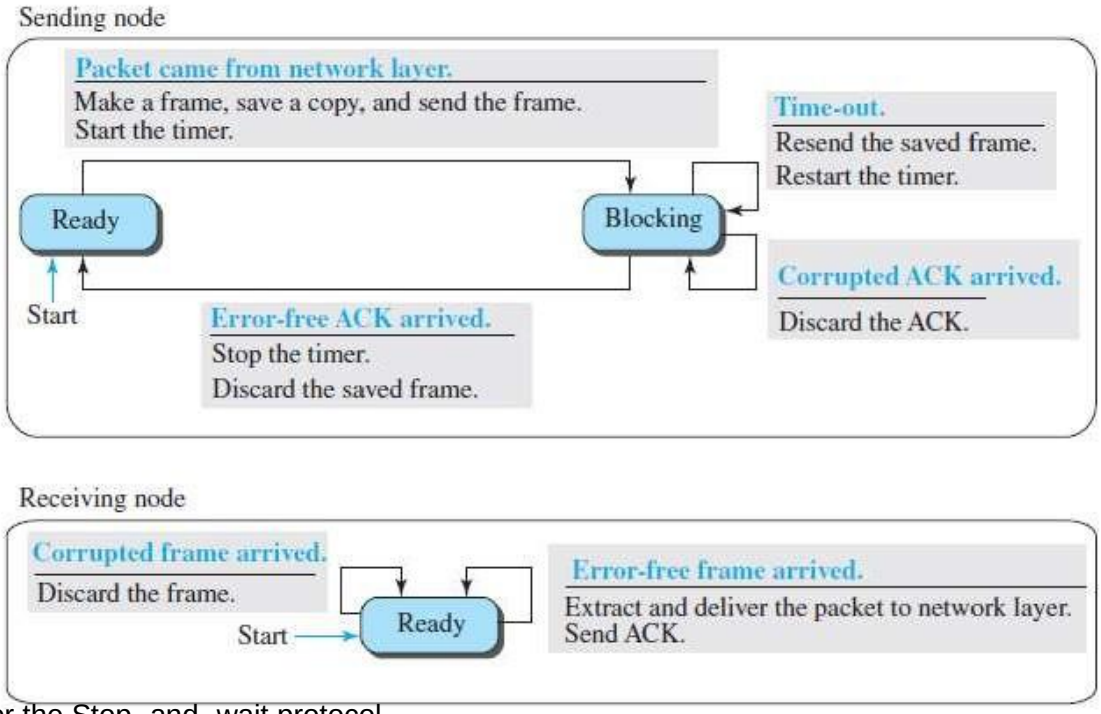


Fig: FSM for the Stop- and- wait protocol.

We describe the sender and receiver states below.

Sender States

- The sender is initially in the ready state, but it can move between the ready and blocking state.

Ready State.

- When the sender is in this state, it is only waiting for a packet from the network layer.
- If a packet comes from the network layer, the sender creates a frame, saves a copy of the frame, starts the only timer and sends the frame.
- Thesender then moves to the blocking state.

Blocking State.

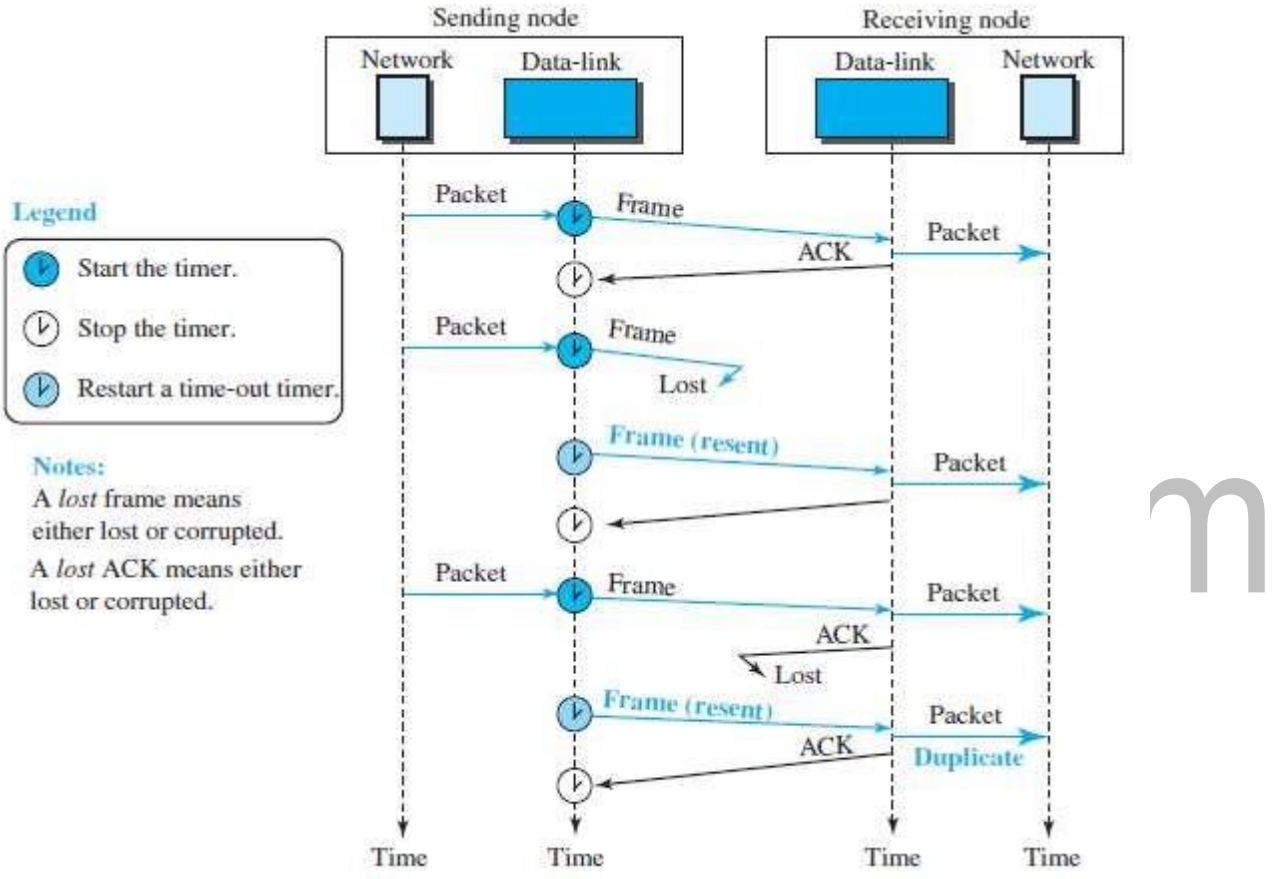
- When the sender is in this state, three events can occur:

a. If a time-out occurs, the sender resends the saved copy of the frame and restarts the timer.
b. If a corrupted ACK arrives, it is discarded.
c. If an error-free ACK arrives, the sender stops the timer and discards the saved opy of the frame. It then moves to the ready state.

Receiver

The receiver is always in the ready state. Two events may occur:

a. If an error-free frame arrives, the message in the frame is delivered to the network layer and an ACK is sent.
b. If a corrupted frame arrives, the frame is discarded.



Piggybacking

- The two protocols we discussed in this section are designed for unidirectional communication, in which data is flowing only in one direction although the acknowledgment may travel in the other direction.
- Protocols have been designed in the past to allow data to flow in both directions.
- However, to make the communication more efficient, the data in one direction is piggybacked with the acknowledgment in the other direction.

HDLC

- **High-level Data Link Control (HDLC)** is a bit-oriented protocol for communication over point-to- point and multipoint links.

Configurations and Transfer Modes:

HDLC provides two common transfer modes that can be used in different configurations: normal response mode (NRM) and asynchronous balanced mode (ABM).

In normal response mode (NRM), the station configuration is unbalanced. We have one primary station and multiple secondary stations.

- A primary station can send commands; a secondary station can only respond. The NRM is used for both point-to-point and multipoint links.

Framing :

- HDLC defines three types of frames: information frames (I-frames), supervisory frames (S-frames), and unnumbered frames (U-frames).
- I frames are used to data-link user data and control information relating to user data (piggybacking).
- S-frames are used only to transport control information. U-frames are reserved for system management.

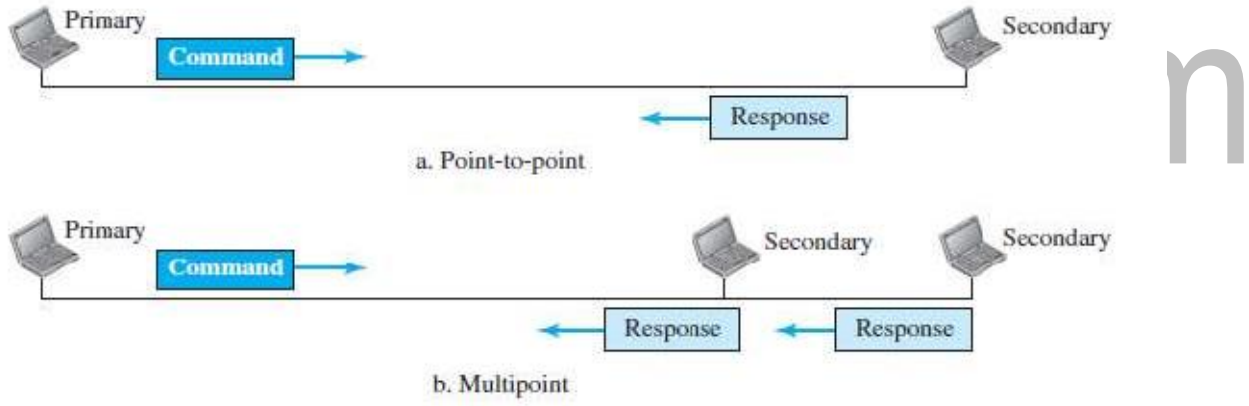


Fig: Asynchronous balanced mode

Fig: Normal Response mode

- Each frame in HDLC may contain up to six fields, a beginning flag field, an address field, a control field, an information field, a frame check sequence (FCS) field, and an ending flag field.

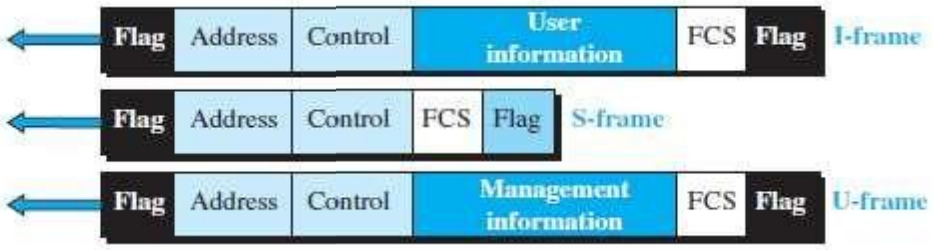


Fig: HDLC frames

- **Flag field:** This field contains synchronization pattern 01111110, which identifies both the beginning and the end of a frame.
- **Address field:** This field contains the address of the secondary station.
- **Control field.** The control field is one or two bytes used for flow and error control.
- **Information field.** The information field contains the user's data from the network layer or management information. Its length can vary from one network to another
- **FCS field.** The frame check sequence (FCS) is the HDLC error detection field. It can contain either a 2- or 4-byte CRC.

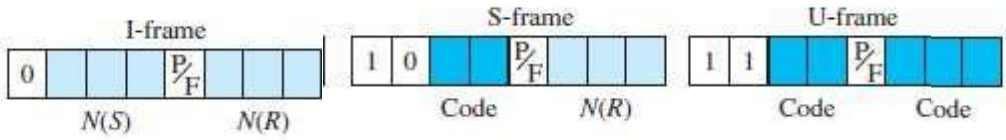


Fig: Control field format for the different frame types.

Control Field for I-Frames

- I-frames are designed to carry user data from the network ayer.
- In addition, they can include flow- and error-control information (piggybacking).
- The subfields in the control field are used to define these functions.
- The first bit defines the type. If the first bit of the control field is 0, this means the frame is an I- frame.
- The next 3 bits, called N(S), define the sequence number of the frame. Note that with 3 bits, we can define a sequence number between 0 and 7.

- The last 3 bits, called N(R), correspond to the acknowledgment number when piggybacking is used.

Control Fieldfor S-Frames

- Supervisory frames are used for flow and error control whenever piggybacking is either impossible or inappropriate.
- S-frames do not have information fields. If the first 2 bits of the control field are 10, this means the frame is an S-frame.
- The last 3 bits, called N(R), correspond to the acknowledgment number (ACK) or negative acknowledgment number (NAK), depending on the type of S-frame. The 2 bits called ***code*** are

  used to define the type of S-frame itself.
- We have four types of S- frames,

Receive ready (RR):

- If the value of the code subfield is 00.

Receive not ready (RNR) :

- If the value of the code subfield is 10.

Reject (REJ):

- If the value of the code subfield is 01.
- The value of N(R) is the negative acknowledgment number.

Selective reject (SREJ):

- If the value of the code subfield is 11, it is an SREJ Sframe.

Control Field forU-Frames:

- Unnumbered frames are used to exchange session management and control information between connected devices.
- Unlike S-frames, U-frames contain an information field, but one used for system management information, not user data.
- As with S-frames, however, much of the information carried by U-frames is contained in codes included in the control field.

POINT-TO-POINT PROTOCOL (PPP)

- One of the most common protocols for point-to-point access is the **Point-to-Point Protocol (PPP).**

Services:

Services Provided by PPP

- PPP defines the format of the frame to be exchanged between devices. It also defines how two devices can negotiate the establishment of the link and the exchange of data.
- The new version of PPP, called ***Multilink*** PPP, provides connections over multiple links.

Services Not Provided by PPP

- PPP does not provide flow control.

Framing:

Flag:A PPP frame starts and ends with a 1-byte flag with the bit pattern 01111110. **Address:**The address field in this protocol is a constant value and set to 11111111 (broadcast address).

Control: This field is set to the constant value 00000011.

Protocol: The protocol field defines what is being carried in the data field: either user data or other information. This field is by default 2 bytes long, but the two parties can agree to use only 1 byte.

Payload field: This field carries either the user data or other information.

FCS: The frame check sequence (FCS) is simply a 2-byte or 4-byte standard CRC.

Byte Stuffing:

- Since PPP is a byte-oriented protocol, the flag in PPP is a byte that needs to be escaped whenever it appears in the data section of the frame.
- The escape byte is 01111101,which means that every time the flag like pattern appears in the data, this extra byte is stuffed to tell the receiver that the next byte is not a flag.

Transition Phases:

- A PPP connection goes through phases which can be shown in a transition phase diagram. The transition diagram, which is an FSM, starts with the ***dead*** state.
- In this state, there is no active carrier and the line is quiet. When one of the two nodes starts the communication, the connection goes into the ***establish*** state.

- In this state, options are negotiated between the two parties. If the two parties agree that they need authentication then the system needs to do authentication otherwise, the parties can simply start communication.
- The link-control protocol packets, discussed shortly, are used for this purpose. Several packets may be exchanged here.
- Data transfer takes place in the ***open*** state. When a connection reaches this state, the exchange of data packets can be started.
- The connection remains in this state until one of the endpoints wants to terminate the connection. In this case, the system goes to the ***terminate*** state. The system remains in this state until the carrier is dropped, which moves the system to the ***dead*** state again.

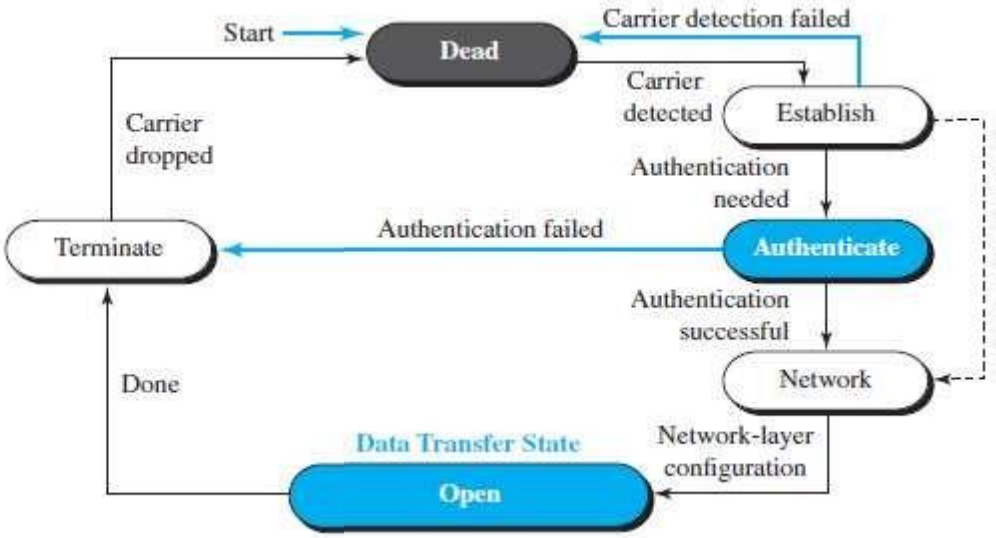


Fig: Transition phases

Multiplexing:

- PPP is a link-layer protocol, it uses another set of protocols to establish the link, authenticate the parties involved, and carry the network-layer data.
- Three sets of protocols are defined to make PPP powerful: The Link Control Protocol (LCP), two Authentication Protocols (APs), and several Network Control Protocols (NCPs).

Link Control Protocol:

- The **Link Control Protocol (LCP)** is responsible for establishing, maintaining, configuring, and terminating links. It also provides negotiation mechanisms to set options between the two endpoints.

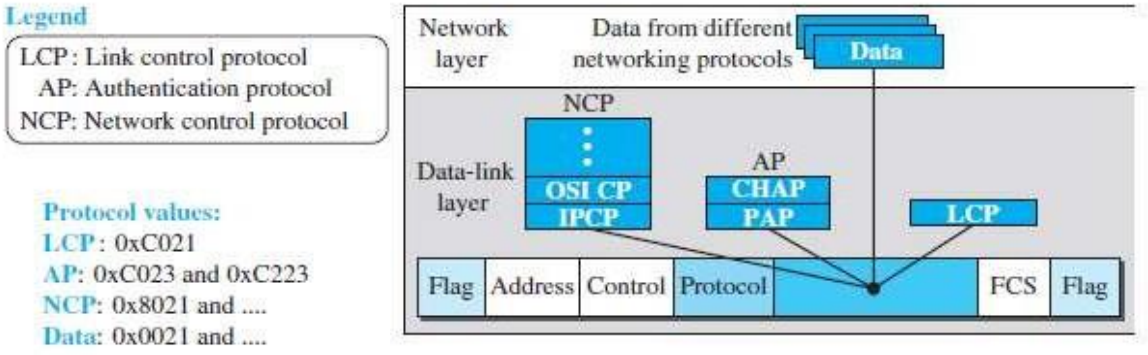


Fig: Multiplexing in PPP

- All LCP packets are carried in the payload field of the PPP frame with the protocol field set to C021 in hexadecimal.

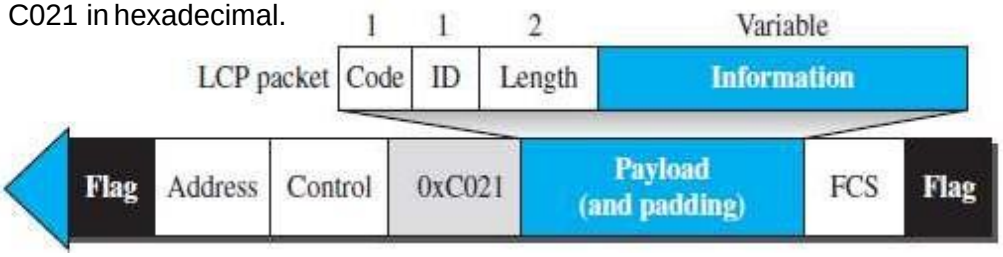


Fig: LCP packet encapsulated in a frame.

LCP packets:

- There are three categories of packets. The first category, comprising the first four packet types, is used for link configuration during the establish phase.
- The second category, comprising packet types 5 and 6, is used for link termination during the termination phase. The last five packets are used for link monitoring and debugging.
- The ID field holds a value that matches a request with a reply.
- The length field defines the length of the entire LCP packet. The information field contains information, such as options, needed for some LCP packets.

Table: LCP packets

Code	Packet Type	Description
0x01	Configure-request	Contains the list of proposed options and their values
0x02	Configure-ack	Accept all options proposed
0x03	Configure-nak	Announces that some options are not acceptable
0x04	Configurw-reject	Announces that some options are not recognized

0x05	Terminate-request	Request to shut down the line
0x06	Terminate-ack	Accept the shutdown request
0x07	Code-reject	Announces an unknown code
0x08	Protocol-reject	Announces an unknown protocol
0x09	Echo-request	A type of hello message to check if the other end is alive
0x0A	Echo-reply	The response to the echo-request message
0x0B	Discard-request	A request to discard the packet

Authentication Protocols:

- Authentication plays a very important role in PPP because PPP is designed for use overdial-up links where verification of user identity is necessary.
- Authentication means validating the identity of a user who needs to access a set of resources. PPP has created two protocols for authentication: Password Authentication Protocol and Challenge Handshake Authentication Protocol.

PAP:

- The **Password Authentication Protocol (PAP)** is a simple authentication procedure with a two- step process:

a. The user who wants to access a system sends an authentication identification(usually the user name) and a password.

b. The system checks the validity of the identification and password and either accepts or denies connection.

CHAP:

- The **Challenge Handshake Authentication Protocol (CHAP)** is a three-way handshaking authentication protocol that provides greater security than PAP. In this method, the password is kept secret; it is never sent online.

a. The system sends the user a challenge packet containing a challenge value, usually a few bytes.

b. The user applies a predefined function that takes the challenge value and the user's own password and creates a result. The user sends the result in the response packet to the system.

c. The system does the same. It applies the same function to the password of the user (known to the system) and the challenge value to create a result. If the result created is the same as the result sent in the response packet, access is granted; otherwise, it is denied. CHAP is more secure than PAP.

Network Control Protocols:
IPCP:

- One NCP protocol is the **Internet Protocol Control Protocol (IPCP).** This protocol configures the link used to carry IP packets in the Internet.

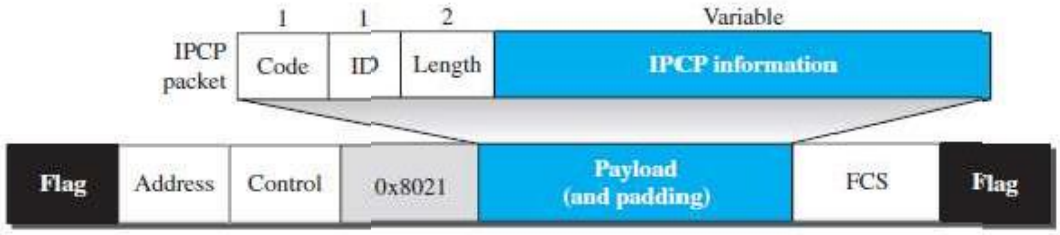


Fig: IPCP packet encapsulated in PPP frame

Table Code value for IPCP packets:

Code	IPCP Packet
0x01	Configure-request
0x02	Configure-ack
0x03	Configure-nak
0x04	Confugure-reject
0x05	Configure-request
0x06	Terminate-ack
0x07	Code-reject

Wired LANs: Ethernet

ETHERNET PROTOCOL:

IEEE Project 802

- The IEEE has subdivided the data-link layer into two sublayers: **logical link control (LLC)** and **media access control (MAC).** IEEE has also created several physical-layer standards for different LAN protocols.

Logical Link Control (LLC)

- In IEEE Project 802, flow control, error control, and part of the framing duties are collected into one sub layer called the logical link control(LLC). Framing is handled in both the LLC sub layer and the MAC sub layer.
- The LLC provides a single link-layer control protocol for all IEEE LANs. This means LLC protocol can provide interconnectivity between different LANs because it makes the MAC sub layer transparent.

Media Access Control (MAC)

- IEEE Project 802 has created a sub layer called **media access control** that defines the specific access method for each LAN.
- For example, itdefines CSMA/CD as the media access method for Ethernet LANs and defines thetoken-passing method for Token Ring and Token Bus LANs.

Ethernet Evolution:

- The Ethernet LAN was developed in the 1970s by Robert Metcalfe and David Boggs.Since then, it has gone through four generations: **Standard Ethernet** (10 Mbps), **FastEthernet** (100 Mbps), **Gigabit Ethernet** (1 Gbps), and **10 Gigabit Ethernet**(10 Gbps),

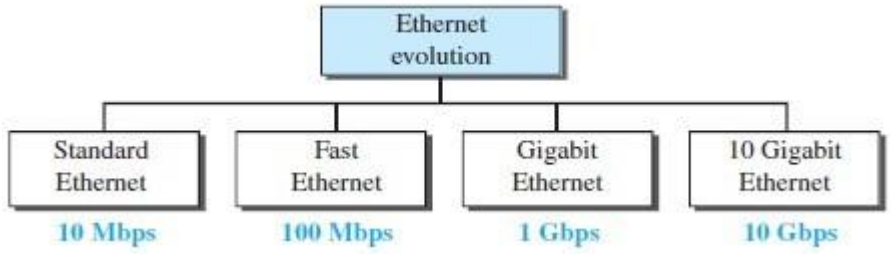


Fig: Ethernet evolution through four generations.

STANDARD ETHERNET:

- The original Ethernet technology with the data rate of 10 Mbps as the *Standard Ethernet.*

Characteristics:

Some characteristics of the Standard Ethernet are

1) Connectionless and Unreliable Service

- Ethernet provides a connectionless service, which means each frame sent is independent of the previous or next frame.
- Ethernet has no connection establishment or connection termination phases. The sender sends a frame whenever it has it; the receiver may or may not be ready for it.
- The sender may overwhelm the receiver with frames, which may result in dropping frames. If a frame drops, the sender will not know about it.
- Ethernet is also unreliable like IP and UDP.

Frame Format

The Ethernet frame contains seven fields

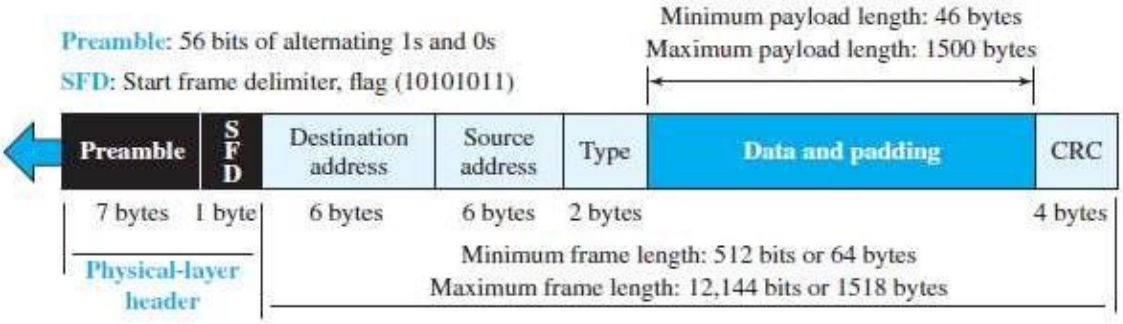


Fig: Ethernet Frame

- **Preamble.** This field contains 7 bytes (56 bits) of alternating 0s and 1s that alert the receiving system to the coming frame.
- **Start frame delimiter (SFD).** This field (1 byte: 10101011) signals the beginning of the frame.
- **Destination address (DA).** This field is six bytes (48 bits) and contains the link layer address of the destination station or stations to receive the packet.
- **Source address (SA).** This field is also six bytes and contains the link-layer address of the sender of the packet.
- **Type.** This field defines the upper-layer protocol whose packet is encapsulated in the frame. This protocol can be IP, ARP, OSPF.
- **Data.** This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.
- **CRC.** The last field contains error detection information.

Frame Length

- An Et hernet frame needs to have a minimum length of 512 bits or64 bytes. Part of this length is
  the header and the trailer. If we count 18 bytes of header and trailer (6 bytes of source address, 6 bytes of destination address, 2 bytes of length or type, and 4 bytes of CRC), then the minimum length of data from the upper layer is64 − 18 = 46 bytes.
- The standard defines the maximum length of a frame (without preamble and SFD field) as 1518 bytes.

Minimum frame length: 64 bytes — Minimum data length: 46 bytes

Maximum frame length: 1518 bytes — Maximum data length: 1500bytes

Addressing

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

  For example: 4A:30:10:21:10:1A

Transmission of Address Bits

- The way the addresses are sent out online is different from the way they are written in hexadecimal notation. The transmission is left to right, byte by byte.

Example: Show how the address 47:20:1B:2E:08:EE is sent out online.

Solution:

The address is sent left to right, byte by byte; for each byte, it is sent right to left, bit by bit, as shown below:

Hexadecimal	47	20	1B	2E	08	EE
Binary	01000111	00100000	00011011	00101110	00001000	11101110
Transmitted ←	11100010	00000100	11011000	01110100	00010000	01110111

Unicast, Multicast, and Broadcast Addresses:

- A source address is always a unicast address - the frame comes from only one station.
- The destination address, can be unicast, multicast, or broadcast. If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise,it is multicast.
- In a **unicast transmission**, all stations will receive the frame, the intended recipient keeps and handles the frame; the rest discard it.

- In a **multicast transmission**, all stations will receive the frame, the stations that are members of the group keep and handle it; the rest discard it.
- In a **broadcast transmission**, all stations (except the sender) will receive the frame and all stations (except the sender) keep and handle it.

Access Method:

- Since the network that uses the standard Ethernet protocol is a broadcast network, we need to use an access method to control access to the sharing medium. The standard Ethernet chose CSMA/CD with 1-persistent method.

Efficiency of Standard Ethernet

The practical efficiency of standard Ethernet has been measured to be

Efficiency 5 **1** / **(1** 1 **6.4** 3 **a)**

in which the parameter "**a**" is the number of frames that can fit on the medium. It can be calculated as **a** = (propagation delay)/(transmission delay).

Implementation:

The Standard Ethernet defined several implementations,

Table: Summary of standard Ethernet implementation

Implementation	Medium	Medium Length	Encoding
10Base5	Thick coax	500m	Manchester
10Base2	Thin coax	185m	Manchester
10Base-T	2 UTP	100m	Manchester
10Base-F	2 Fiber	2000m	Manchester

10Base5: Thick Ethernet

- The first implementation is called **10Base5, thick Ethernet,**or **Thicknet.**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.

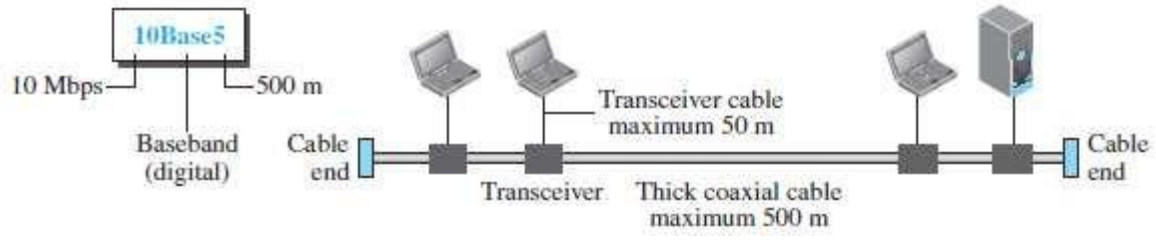


Fig: 10Base5 implementation

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.

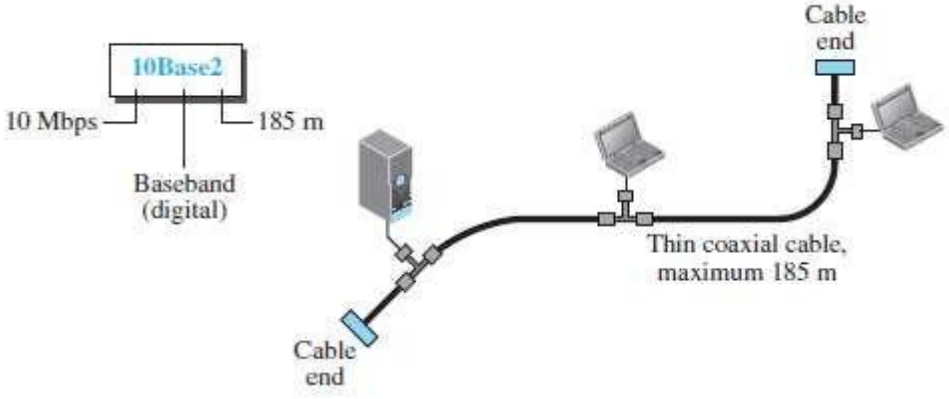


Fig: 10Base2 implementation

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.

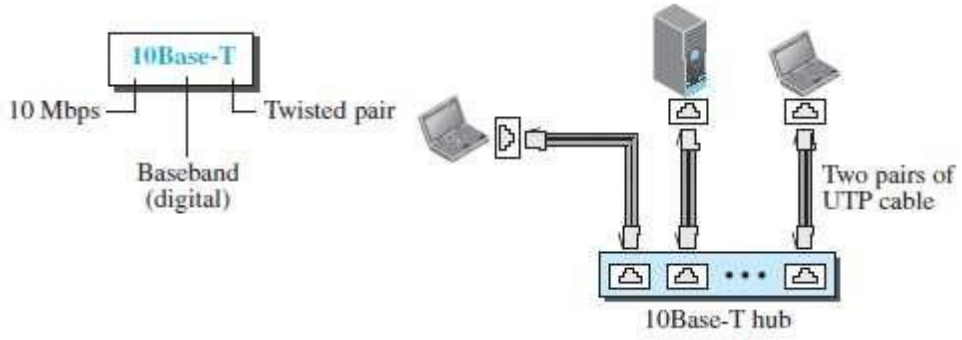


Fig: 10Base- T implementation

10Base-F: Fiber Ethernet

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

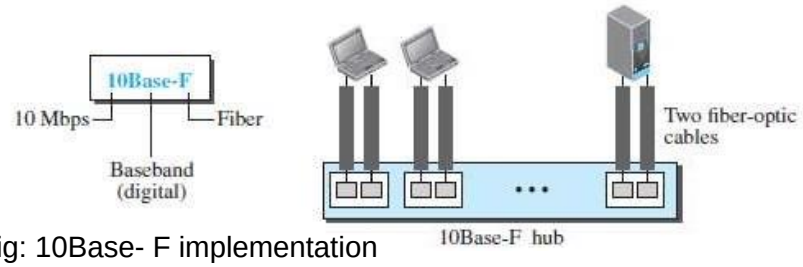


Fig: 10Base- F implementation