UNIT – 2

DATA LINK LAYER & MEDIA ACCESS

Introduction About Data Link Layer Addressing & Media Access – DLC Services – Data-Link Layer Protocols – Media Access Control – Wired Lans: Ethernet – Wireless Lans – Introduction (IEEE 802.11) – Bluetooth – Connecting Devices.

2.1 INTRODUCTION ABOUT DATA LINK LAYER ADDRESSING & MEDIA ACCESS

Data Link Layer is second layer of OSI Layered Model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate. Data link layer works between two hosts which are directly connected in some sense. This direct connection could be point to point or broadcast. Systems on broadcast network are said to be on same link.

The work of data link layer tends to get more complex when it is dealing with multiple hosts on single collision domain. Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals assembles them in a recognizable frame format, and hands over to upper layer.

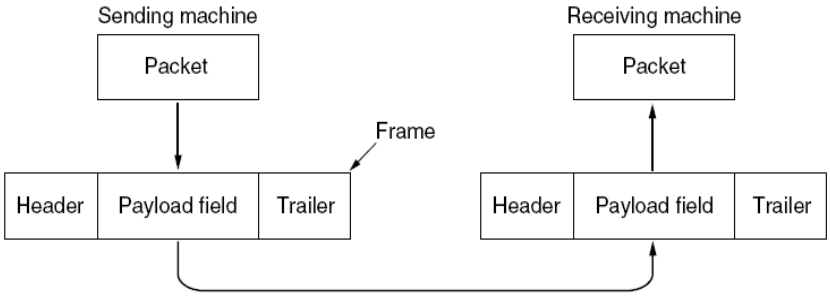
The data link layer uses the services of the physical layer to send and receive bits over communication channels. It has a number of functions, including:

(1) Providing a well-defined service interface to the network layer.

(2) Dealing with transmission errors.

(3) Regulating the flow of data so that slow receivers are not swamped

by fast senders. To accomplish these goals, the data link layer takes the packets it gets from the network layer and encapsulates them into frames for transmission. Each frame contains a frame header, a payload field for holding the packet, and a frame trailer, as illustrated in following figure. Frame management forms the heart of what the data link layer does. In the following sections we will examine all the above mentioned issues in detail.



Data link layer has two sub-layers:

- **Logical Link Control:** It deals with protocols, flow-control, and error control
- **Media Access Control:** It deals with actual control of media

Functionality of Data-link Layer

Data link layer does many tasks on behalf of upper layer. These are:

- **Framing**

  Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver' end, data link layer picks up signals from hardware and assembles them into frames.

- **Addressing**

  Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.

- **Synchronization**

  When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.

- **Error Control**

  Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.

- **Flow Control**

  Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machines to exchange data on same speed.

- **Multi-Access**

  When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple Systems.

Media Access Control (MAC)

In Layer 2 of a network, the Media Access Control (MAC) sub layer provides addressing and channel access control mechanisms that enable several terminals or network nodes to communicate in a network. The MAC sub layer acts as an interface between the logical link control (LLC) Ethernet sub layer and Layer 1 (the physical layer). The MAC sub layer emulates a full-duplex logical communication channel in a multipoint network.

This channel may provide unicast, multicast or broadcast communication service. The MAC sub layer uses MAC protocols to prevent collisions. In Layer 2, multiple devices on the same physical link can uniquely identify one another at the data link layer, by using the MAC addresses that are assigned to all ports on a switch. A MAC algorithm accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC address.

A MAC address is a 12-digit hexadecimal number (48 bits in long). MAC addresses are usually written in one of these formats:

- MM:MM:MM:SS:SS:SS
- MM-MM-MM-SS-SS-SS

The first half of a MAC address contains the ID number of the adapter manufacturer. These IDs are regulated by an Internet standards body. The second half of a MAC address represents the serial number assigned to the adapter by the manufacturer. Contrast MAC addressing, which works at Layer 2, with IP addressing, which runs at Layer 3 (networking and routing). One way to remember the difference is that the MAC addresses apply to a physical or virtual node, whereas IP addresses apply to the software implementation of that node. MAC addresses are typically fixed on a per-node basis, whereas IP addresses change when the node moves from one part of the network to another.

2.2 DLC SERVICES

The two main functions of the data link layer are data link control and media access control. The first, data link control, deals with the design and procedures for communication between two adjacent nodes: node-to-node communication. The second function of the data link layer is media access control, or how to share the link Data link control functions include framing, flow and error control, and software implemented protocols that provide smooth and reliable transmission of frames between nodes. To implement data link control, we need protocols. Each protocol is a set of rules that need to be implemented in software and run by the two nodes involved in data exchange at the data link layer. We discuss five protocols: two for noiseless (ideal) channels and three for noisy (real) channels. Those in the first category are not actually implemented, but provide a foundation for understanding the protocols in the second category. Data Link Control is the service provided by the Data Link Layer to provide reliable data transfer over the physical medium. For example, In the half-duplex transmission mode, one device can only transmit the data at a time.

If both the devices at the end of the links transmit the data simultaneously, they will collide and leads to the loss of the information. The Data link layer provides the coordination among the devices so that no collision occurs.

The services that the data link layer provides are:

- Encapsulation of network layer data packets into frames
- Frame synchronization
- In the logical link control (LLC) sublayer:
  - Error control (automatic repeat request, ARQ), in addition to ARQ provided by some transport-layer protocols, to forward error correction (FEC) techniques provided on the physical layer, and to error-detection and packet canceling provided at all layers, including the network layer. Data-link-layer error control (i.e. retransmission of erroneous packets) is provided in wireless networks and V.42 telephone network modems, but not in LAN protocols such as Ethernet, since bit errors are so uncommon in short wires. In that case, only error detection and canceling of erroneous packets are provided.
  - Flow control, in addition to the one provided on the transport layer. Data-link-layer flow control is not used in LAN protocols such as Ethernet, but in modems and wireless networks.
- In the medium access control (MAC) su blayer:
  - Multiple access protocols for channel-access control, for example CSMA/CD protocols for collision detection and re-transmission in Ethernet bus networks and hub networks, or the CSMA/CA protocol for collision avoidance in wireless networks.
  - Physical addressing (MAC addressing)
  - LAN switching (packet switching), including MAC filtering, Spanning Tree Protocol (STP) and Shortest Path Bridging (SPB)
  - Data packet queuing or scheduling
  - Store-and-forward switching or cut-through switching
  - Quality of Service (QoS) control
  - Virtual LANs (VLAN)

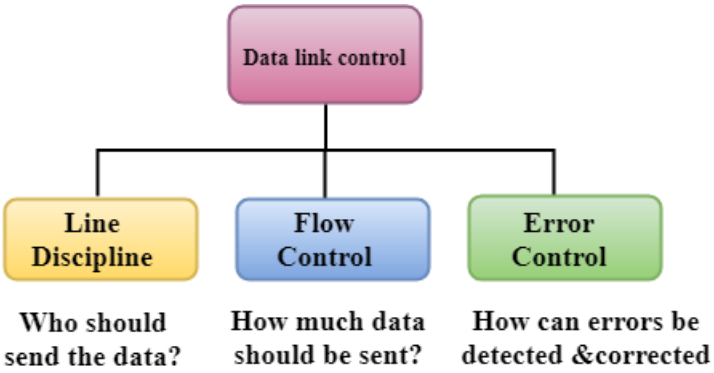
The Data link layer provides three functions:

- Line discipline
- Flow Control
- Error Control

Data Link Control is the service provided by the Data Link Layer to provide reliable data transfer over the physical medium. For example, In the half-duplex transmission mode, one device can only transmit the data at a time. If both the devices at the end of the links transmit the data simultaneously, they will collide and leads to the loss of the information. The Data link layer provides the coordination among the devices so that no collision occurs.

The Data link layer provides three functions:

- Line discipline
- Flow Control
- Error Control



Line Discipline

- Line Discipline is a functionality of the Data link layer that provides the coordination among the link systems. It determines which device can send, and when it can send the data.

Line Discipline can be achieved in two ways:

- ENQ/ACK
- Poll/select

END/ACK

END/ACK stands for Enquiry/Acknowledgement is used when there is no wrong receiver available on the link and having a dedicated path between the two devices so that the device capable of receiving the transmission is the intended one.

END/ACK coordinates which device will start the transmission and whether the recipient is ready or not.

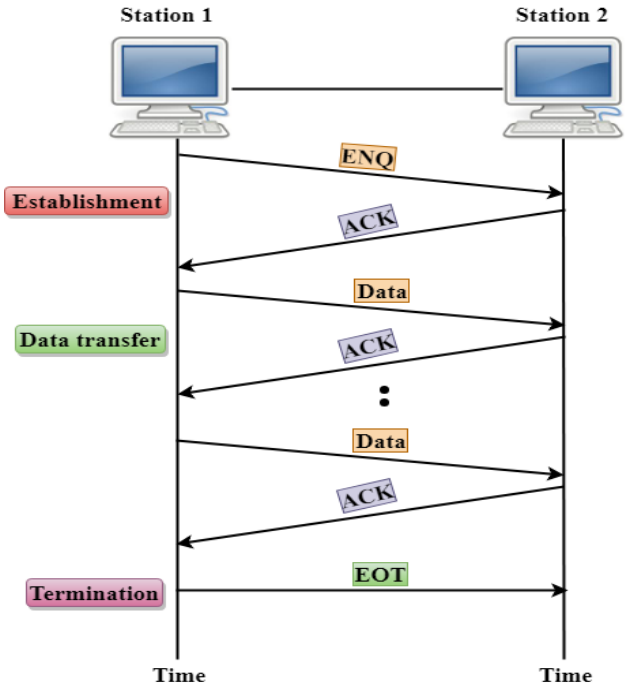
Working of END/ACK

The transmitter transmits the frame called an Enquiry (ENQ) asking whether the receiver is available to receive the data or not.

The receiver responses either with the positive acknowledgement (ACK) or with the negative acknowledgement(NACK) where positive acknowledgement means that the receiver is ready to receive the transmission and negative acknowledgement means that the receiver is unable to accept the transmission.

Following are the responses of the receiver:

- If the response to the ENQ is positive, the sender will transmit its data, and once all of its data has been transmitted, the device finishes its transmission with an EOT (END-of-Transmission) frame.
- If the response to the ENQ is negative, then the sender disconnects and restarts the transmission at another time.
- If the response is neither negative nor positive, the sender assumes that the ENQ frame was lost during the transmission and makes three attempts to establish a link before giving up.



Poll/Select

The Poll/Select method of line discipline works with those topologies where one device is designated as a primary station, and other devices are secondary stations.

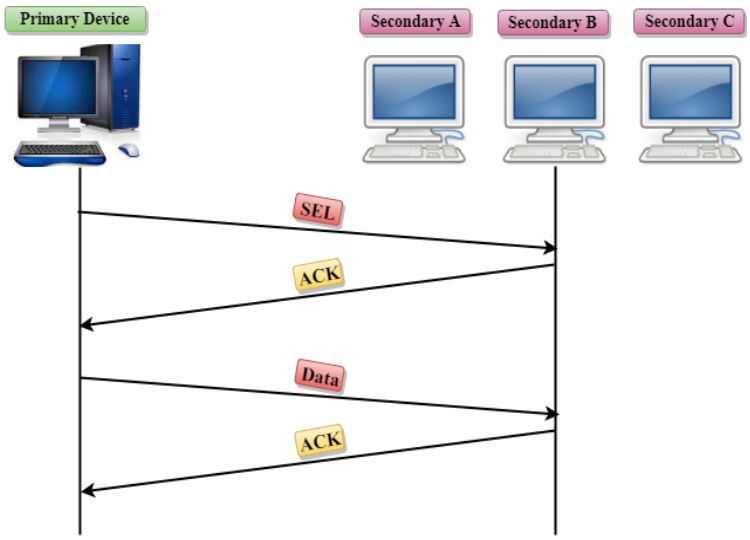
Working of Poll/Select

- In this, the primary device and multiple secondary devices consist of a single transmission line, and all the exchanges are made through the primary device even though the destination is a secondary device.
- The primary device has control over the communication link, and the secondary device follows the instructions of the primary device.
- The primary device determines which device is allowed to use the communication channel. Therefore, we can say that it is an initiator of the session.
- If the primary device wants to receive the data from the secondary device, it asks the secondary device that they anything to send, this process is known as polling.

- If the primary device wants to send some data to the secondary device, then it tells the target secondary to get ready to receive the data, this process is known as selecting.

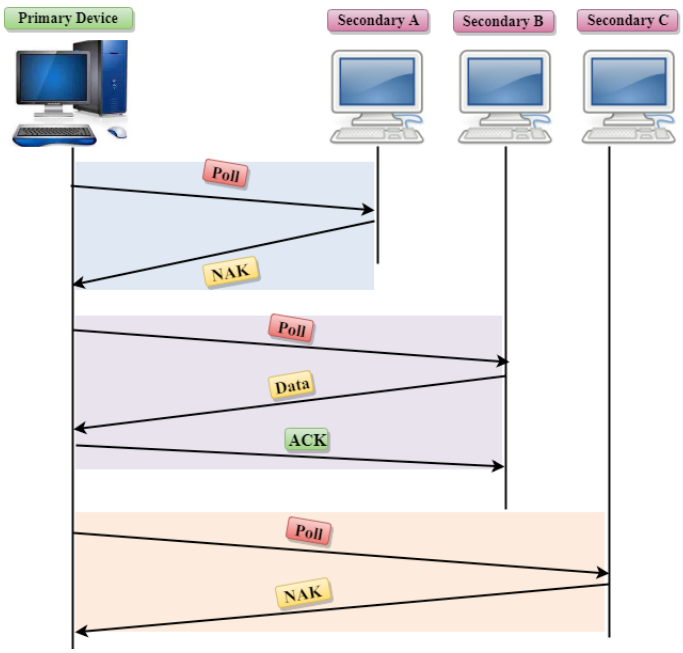
Select

- The select mode is used when the primary device has something to send.
- When the primary device wants to send some data, then it alerts the secondary device for the upcoming transmission by transmitting a Select (SEL) frame, one field of the frame includes the address of the intended secondary device.
- When the secondary device receives the SEL frame, it sends an acknowledgement that indicates the secondary ready status.
- If the secondary device is ready to accept the data, then the primary device sends two or more data frames to the intended secondary device. Once the data has been transmitted, the secondary sends an acknowledgement specifies that the data has been received.



Poll

- The Poll mode is used when the primary device wants to receive some data from the secondary device.
- When a primary device wants to receive the data, then it asks each device whether it has anything to send.
- Firstly, the primary asks (poll) the first secondary device, if it responds with the NACK (Negative Acknowledgement) means that it has nothing to send. Now, it approaches the second secondary device, it responds with the ACK means that it has the data to send. The secondary device can send more than one frame one after another or sometimes it may be required to send ACK before sending each one, depending on the type of the protocol being used.



Flow Control

- It is a set of procedures that tells the sender how much data it can transmit before the data overwhelms the receiver.
- The receiving device has limited speed and limited memory to store the data. Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.
- It requires a buffer, a block of memory for storing the information until they are processed.

Two methods have been developed to control the flow of data:

- Stop-and-wait
- Sliding window

Stop-and-wait

- In the Stop-and-wait method, the sender waits for an acknowledgement after every frame it sends.
- When acknowledgement is received, then only next frame is sent. The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame.

Advantage of Stop-and-wait

The Stop-and-wait method is simple as each frame is checked and acknowledged before the next frame is sent.

Disadvantage of Stop-and-wait

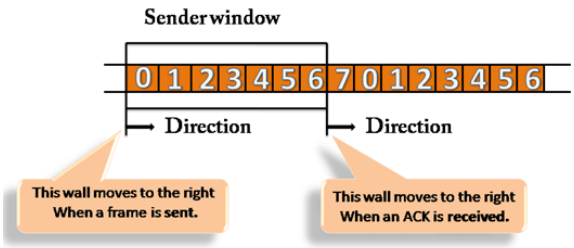
Stop-and-wait technique is inefficient to use as each frame must travel across all the way to the receiver, and an acknowledgement travels all the way before the next frame is sent. Each frame sent and received uses the entire time needed to traverse the link.

Sliding Window

- The Sliding Window is a method of flow control in which a sender can transmit the several frames before getting an acknowledgement.
- In Sliding Window Control, multiple frames can be sent one after the another due to which capacity of the communication channel can be utilized efficiently.
- A single ACK acknowledge multiple frames.
- Sliding Window refers to imaginary boxes at both the sender and receiver end.
- The window can hold the frames at either end, and it provides the upper limit on the number of frames that can be transmitted before the acknowledgement.
- Frames can be acknowledged even when the window is not completely filled.
- The window has a specific size in which they are numbered as modulo-n means that they are numbered from 0 to n-1. For example, if n = 8, the frames are numbered from 0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1.....
- The size of the window is represented as n-1. Therefore, maximum n-1 frames can be sent before acknowledgement.
- When the receiver sends the ACK, it includes the number of the next frame that it wants to receive. For example, to acknowledge the string of frames ending with frame number 4, the receiver will send the ACK containing the number 5. When the sender sees the ACK with the number 5, it got to know that the frames from 0 through 4 have been received.

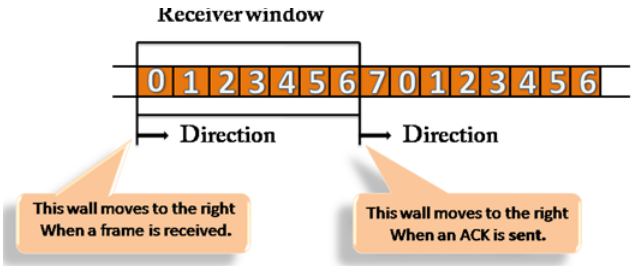
Sender Window

- At the beginning of a transmission, the sender window contains n-1 frames, and when they are sent out, the left boundary moves inward shrinking the size of the window. For example, if the size of the window is w if three frames are sent out, then the number of frames left out in the sender window is w-3.
- Once the ACK has arrived, then the sender window expands to the number which will be equal to the number of frames acknowledged by ACK.
- For example, the size of the window is 7, and if frames 0 through 4 have been sent out and no acknowledgement has arrived, then the sender window contains only two frames, i.e., 5 and 6. Now, if ACK has arrived with a number 4 which means that 0 through 3 frames have arrived undamaged and the sender window is expanded to include the next four frames. Therefore, the sender window contains six frames (5,6,7,0,1,2).



Receiver Window

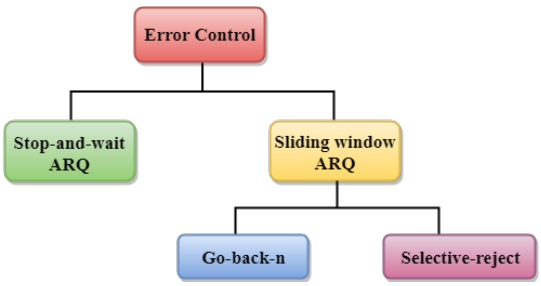
- At the beginning of transmission, the receiver window does not contain n frames, but it contains n-1 spaces for frames.
- When the new frame arrives, the size of the window shrinks.
- The receiver window does not represent the number of frames received, but it represents the number of frames that can be received before an ACK is sent. For example, the size of the window is w, if three frames are received then the number of spaces available in the window is (w-3).
- Once the acknowledgement is sent, the receiver window expands by the number equal to the number of frames acknowledged.
- Suppose the size of the window is 7 means that the receiver window contains seven spaces for seven frames. If the one frame is received, then the receiver window shrinks and moving the boundary from 0 to 1. In this way, window shrinks one by one, so window now contains the six spaces. If frames from 0 through 4 have sent, then the window contains two spaces before an acknowledgement is sent.



Error Control

Error Control is a technique of error detection and retransmission.

Categories of Error Control:



Stop-and-wait ARQ

Stop-and-wait ARQ is a technique used to retransmit the data in case of damaged or lost frames.

This technique works on the principle that the sender will not transmit the next frame until it receives the acknowledgement of the last transmitted frame.

Four features are required for the retransmission:

- The sending device keeps a copy of the last transmitted frame until the acknowledgement is received. Keeping the copy allows the sender to retransmit the data if the frame is not received correctly.
- Both the data frames and the ACK frames are numbered alternately 0 and 1 so that they can be identified individually. Suppose data 1 frame acknowledges the data 0 frame means that the data 0 frame has been arrived correctly and expects to receive data 1 frame.
- If an error occurs in the last transmitted frame, then the receiver sends the NAK frame which is not numbered. On receiving the NAK frame, sender retransmits the data.
- It works with the timer. If the acknowledgement is not received within the allotted time, then the sender assumes that the frame is lost during the transmission, so it will retransmit the frame.

Two possibilities of the retransmission:

- **Damaged Frame:** When the receiver receives a damaged frame, i.e., the frame contains an error, then it returns the NAK frame. For example, when the data 0 frame is sent, and then the receiver sends the ACK 1 frame means that the data 0 has arrived correctly, and transmits the data 1 frame. The sender transmits the next frame: data 1. It reaches undamaged, and the receiver returns ACK 0. The sender transmits the next frame: data 0. The receiver reports an error and returns the NAK frame. The sender retransmits the data 0 frame.
- **Lost Frame:** Sender is equipped with the timer and starts when the frame is transmitted. Sometimes the frame has not arrived at the receiving end so that it can be acknowledged neither positively nor negatively. The sender waits for acknowledgement until the timer goes off. If the timer goes off, it retransmits the last transmitted frame.

Sliding Window ARQ

Sliding Window ARQ is a technique used for continuous transmission error control.

Three Features used for retransmission:

- In this case, the sender keeps the copies of all the transmitted frames until they have been acknowledged. Suppose the frames from 0 through 4 have been transmitted, and the last acknowledgement was for frame 2, the sender has to keep the copies of frames 3 and 4 until they receive correctly.
- The receiver can send either NAK or ACK depending on the conditions. The NAK frame tells the sender that the data have been received damaged. Since the sliding window is

a continuous transmission mechanism, both ACK and NAK must be numbered for the identification of a frame. The ACK frame consists of a number that represents the next frame which the receiver expects to receive. The NAK frame consists of a number that represents the damaged frame.

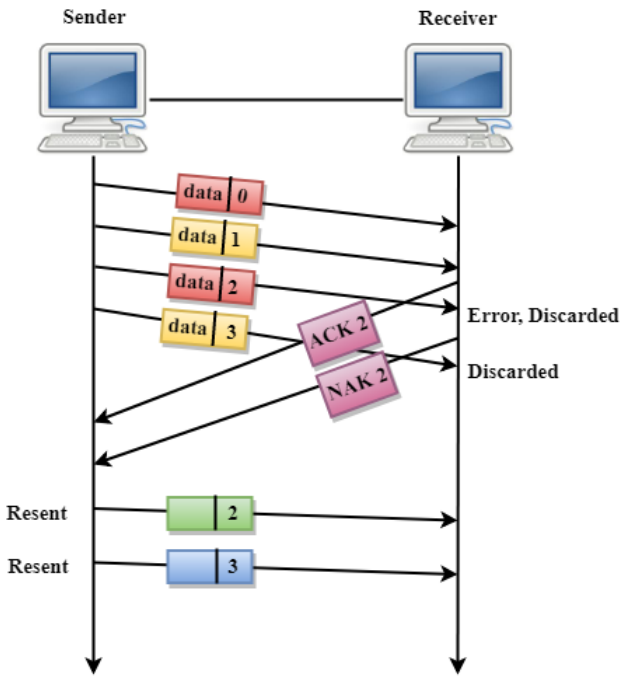
- The sliding window ARQ is equipped with the timer to handle the lost acknowledgements. Suppose then n-1 frames have been sent before receiving any acknowledgement. The sender waits for the acknowledgement, so it starts the timer and waits before sending any more. If the allotted time runs out, the sender retransmits one or all the frames depending upon the protocol used.

Two protocols used in sliding window ARQ:

- **Go-Back-n ARQ:** In Go-Back-N ARQ protocol, if one frame is lost or damaged, then it retransmits all the frames after which it does not receive the positive ACK.

Three possibilities can occur for retransmission:

- **Damaged Frame:** When the frame is damaged, then the receiver sends a NAK frame.



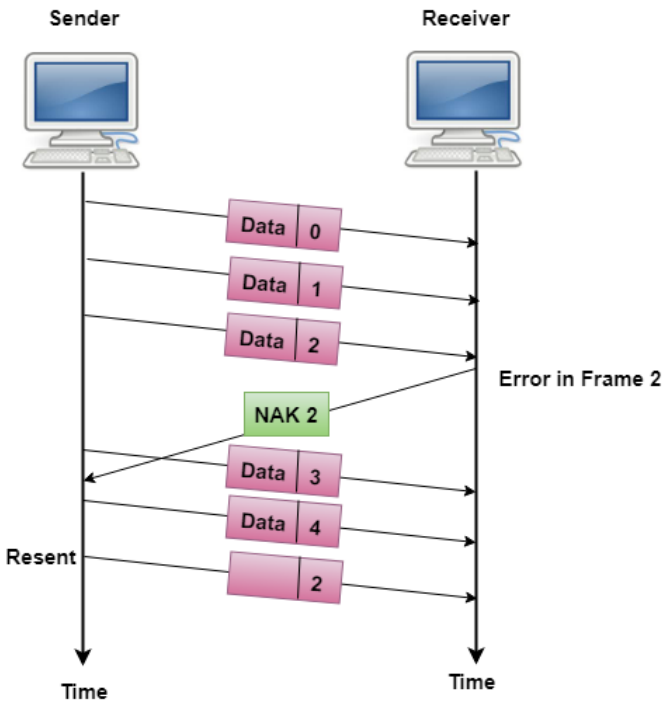
In the above figure, three frames have been transmitted before an error discovered in the third frame. In this case, ACK 2 has been returned telling that the frames 0,1 have been received successfully without any error. The receiver discovers the error in data 2 frame, so it returns the NAK 2 frame. The frame 3 is also discarded as it is transmitted after the damaged frame. Therefore, the sender retransmits the frames 2,3.

- **Lost Data Frame:** In Sliding window protocols, data frames are sent sequentially. If any of the frames is lost, then the next frame arrive at the receiver is out of sequence. The receiver checks the sequence number of each of the frame, discovers the frame that has been skipped, and returns the NAK for the missing frame. The sending device retransmits the frame indicated by NAK as well as the frames transmitted after the lost frame.

- **Lost Acknowledgement:** The sender can send as many frames as the windows allow before waiting for any acknowledgement. Once the limit of the window is reached, the sender has no more frames to send; it must wait for the acknowledgement. If the acknowledgement is lost, then the sender could wait forever. To avoid such situation, the sender is equipped with the timer that starts counting whenever the window capacity is reached. If the acknowledgement has not been received within the time limit, then the sender retransmits the frame since the last ACK.

Selective-Reject ARQ

- Selective-Reject ARQ technique is more efficient than Go-Back-n ARQ.
- In this technique, only those frames are retransmitted for which negative acknowledgement (NAK) has been received.
- The receiver storage buffer keeps all the damaged frames on hold until the frame in error is correctly received.
- The receiver must have an appropriate logic for reinserting the frames in a correct order.
- The sender must consist of a searching mechanism that selects only the requested frame for retransmission.



2.3 DATA-LINK LAYER PROTOCOLS

The data link layer provides service to the Network Layer above it:

- The network layer is interested in getting messages to the corresponding network layer module on an adjacent machine.

- The remote Network Layer peer should receive the identical message generated by the sender (e.g., if the data link layer adds control information, the header information must be removed before the message is passed to the Network Layer).
- The Network Layer wants to be sure that all messages it sends, will be delivered correctly (e.g., none lost, no corruption). Note that arbitrary errors may result in the loss of both data and control frames.
- The Network Layer wants messages to be delivered to the remote peer in the exact same order as they are sent

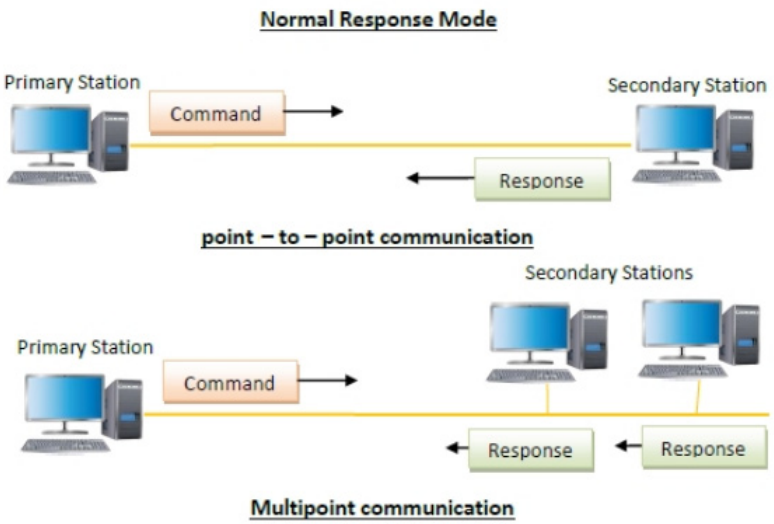
High-Level Data Link Control (HDLC)

High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes. Since it is a data link protocol, data is organized into frames. A frame is transmitted via the network to the destination that verifies its successful arrival. It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications.

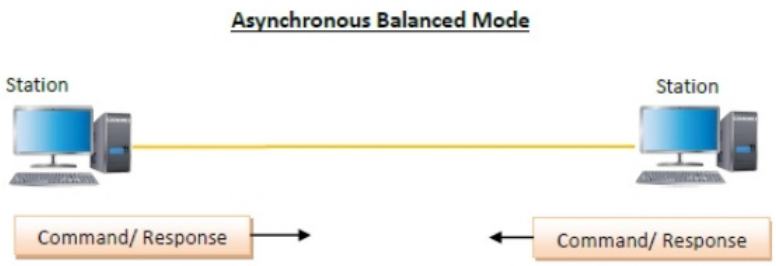
Transfer Modes

HDLC supports two types of transfer modes, normal response mode and asynchronous balanced mode.

Normal Response Mode (NRM) − Here, two types of stations are there, a primary station that send commands and secondary station that can respond to received commands. It is used for both point - to - point and multipoint communications.



Asynchronous Balanced Mode (ABM) − Here, the configuration is balanced, i.e. each station can both send commands and respond to commands. It is used for only point - to - point communications.



HDLC Frame

HDLC is a bit - oriented protocol where each frame contains up to six fields. The structure varies according to the type of frame. The fields of a HDLC frame are −

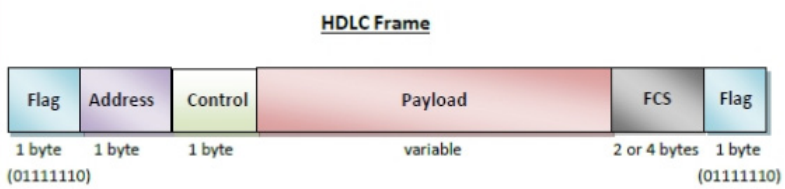
Flag − It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.

Address − It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent by the secondary station, it contains the address of the primary station. The address field may be from 1 byte to several bytes.

Control − It is 1 or 2 bytes containing flow and error control information.

Payload − This carries the data from the network layer. Its length may vary from one network to another.

FCS − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)



Types of HDLC Frames

There are three types of HDLC frames. The type of frame is determined by the control field of the frame −

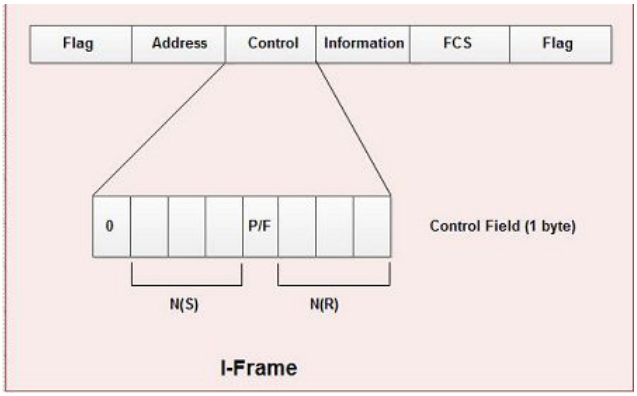
I-frame − I-frames or Information frames carry user data from the network layer. They also include flow and error control information that is piggybacked on user data. The first bit of control field of I-frame is 0.

S-frame − S-frames or Supervisory frames do not contain information field. They are used for flow and error control when piggybacking is not required. The first two bits of control field of S-frame is 10.

U-frame − U-frames or Un-numbered frames are used for myriad miscellaneous functions, like link management. It may contain an information field, if required. The first two bits of control field of U-frame is 11

Information frames

- I-frames carry user›s data and control information about user›s data.
- I-frame carries user data in the information field.
- The I-frame format is shown in diagram.



- The first bit of control field is always zero, *i.e.* the presence of zero at this place indicates that it is I-frame.
- Bit number 2, 3 & 4 in control field is called N(S) that specifies the sequence number of the frame. Thus it specifies the number of the frame that is currently being sent. Since it is a 3.bit field, only eight sequence numbers are possible 0, 1,2,3,4,5,6, 7 (000 to 111).
- Bit number 5 in control field is P/F i.e. Poll/Final and is used for these two purposes. It has, meaning only when it is set i.e. when P/F=1. It can represent the following two cases.

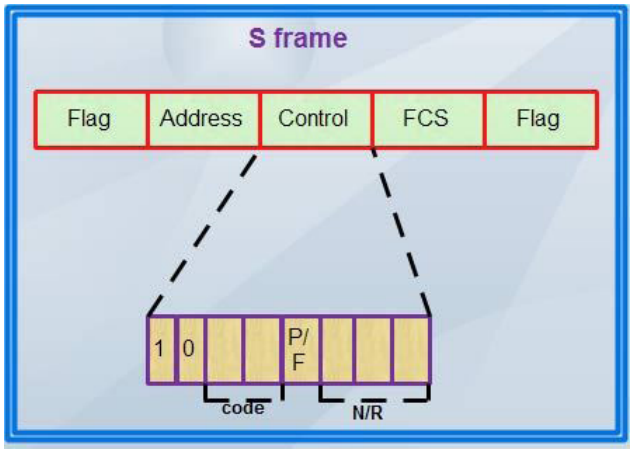
  (i) It means poll when frame is sent by a primary station to secondary (when address field contains the address of receiver).

  (ii) It means final when frame is sent by secondary to a primary (when the address field contains the address of the sender).
- Bit number 6, 7, and 8 in control field specifies N(R) i.e. the sequence number of the frame expected in return in two-way communication.

  If last frame received was error-free then N(R) number will be that of the next frame is sequence. If the last frame was not received correctly, the N(R) number will be the number of the damaged frame, asking for its retransmission.

Supervisory frame

- S-frame carries control information, primarily data link layer flow and error controls.
- It does not contain information field.
- The format of S-frame is shown in diagram.



- The first two bits in the control field of S-frame are always 10.
- Then there is a bit code field that specifies four types of S-frame with combination 00,01, 10, 11 as shown in table :-

Table: Types of S-frame

Code	Command
00	RR Receive Ready
01	REJ Reject
10	RNR Receive Not Ready
11	SREJ Selective Reject

(1) RR, Receive Ready-used to acknowledge frames when no I-frames are availab1e to piggyback the acknowledgement.

(2) REJ Reject-used by the receiver to send a NAK when error has occurred.

(3) RNR Receive Not Ready-used for flow control.

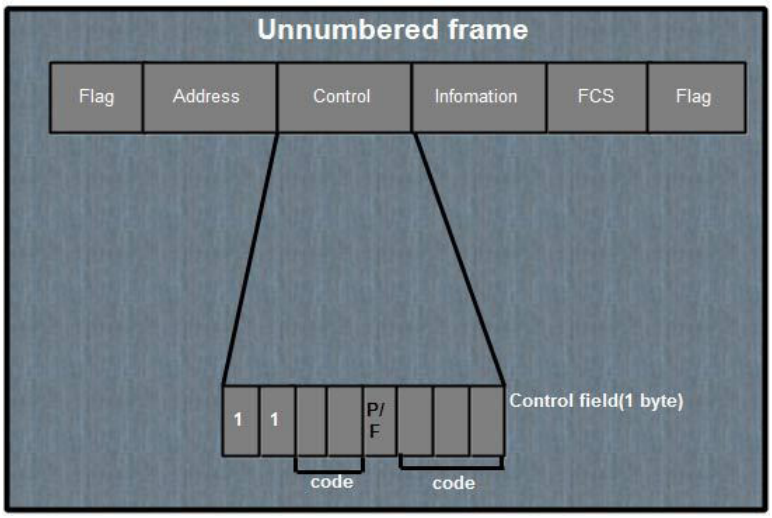
(4) SREJ Selective Reject-indicates to the transmitter that it should retransmit the frame indicated in the N(R) subfield.

- There is no N(S) field in control field of S-frame as S-frames do not transmit data.
- *P/F* bit is the fifth bit and serves the same purpose as discussed earlier.
- Last three bits in control field indicates N(R) *i.e.* they correspond to the ACK or NAK value.

Unnumbered frame

- U-frames are reserved for system management and information carried by them is used for managing the link
- U-frames are used to exchange session management and control information between the two connected devices.

- Information field in U-frame does not carry user information rather, it carries system management information.
- The frame format of U-frame is shown in diagram.
- U-frame is identified by the presence of 11 in the first and second bit position in control field.
- These frames do not contain N(S) or N(R) in control field.



- U-frame contains two code fields, one two hit and other three bit.
- These five bits can create upto 32 different U-frames.
- *P/F* bit in control field has same purpose in V-frame.

Protocol Structure - HDLC: High Level Data Link Control

Flag - The value of the flag is always (0x7E).

Address field - Defines the address of the secondary station which is sending the frame or the destination of the frame sent by the primary station. It contains Service Access Point (6bits), a Command/Response bit to indicate whether the frame relates to information frames (I-frames) being sent from the node or received by the node, and an address extension bit which is usually set to true to indicate that the address is of length one byte. When set to false it indicates an additional byte follows.

Extended address - HDLC provides another type of extension to the basic format. The address field may be extended to more than one byte by agreement between the involved parties.

Control field - Serves to identify the type of the frame. In addition, it includes sequence numbers, control features and error tracking according to the frame type.

FCS - The Frame Check Sequence (FCS) enables a high level of physical error control by allowing the integrity of the transmitted frame data to be checked.

Related Protocols: LAPB, ISDN, X.25, Frame Relay, SDLC

Point - To - Point Protocol (PPP)

Point - to - Point Protocol (PPP) is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers. It is a byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds. Since it is a data link layer protocol, data is transmitted in frames. It is also known as RFC 1661.

This protocol offers several facilities that were not present in SLIP. Some of these facilities are:

(1) PPP defines the format of the frame to be exchanged between the devices.

(2) It defines link control protocol (LCP) for:-

(a) Establishing the link between two devices.

(b) Maintaining this established link.

(c) Configuring this link.

(d) Terminating this link after the transfer.

(3) It defines how network layer data are encapsulated in data link frame.

(4) PPP provides error detection.

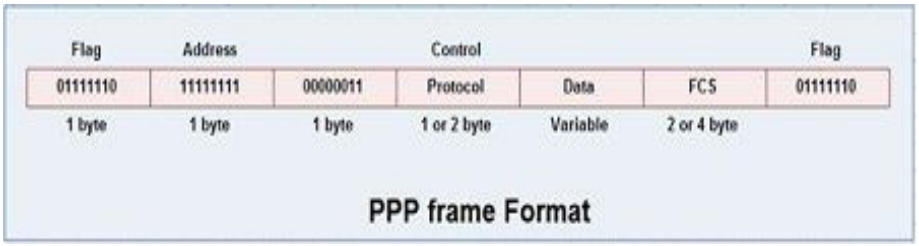
(5) Unlike SLIP that supports only IP, PPP supports multiple protocols.

(6) PPP allows the IP address to be assigned at the connection time i.e. dynamically. Thus a temporary IP address can be assigned to each host.

(7) PPP provides multiple network layer services supporting a variety of network layer protocol. For this PPP uses a protocol called NCP (Network Control Protocol).

(8) It also defines how two devices can authenticate each other.

PPP Frame Format



PPP frame Format

The frame format of PPP resembles HDLC frame. Its various fields are:

(1) Flag field: Flag field marks the beginning and end of the PPP frame. Flag byte is 01111110. (1 byte).

(2) Address field: This field is of 1 byte and is always 11111111. This address is the broadcast address i.e. all the stations accept this frame.

(3) **Control field**: This field is also of 1 byte. This field uses the format of the U-frame (unnumbered) in HDLC. The value is always 00000011 to show that the frame does not contain any sequence numbers and there is no flow control or error control.

(4) **Protocol field:** This field specifies the kind of packet in the data field i.e. what is being carried in data field.

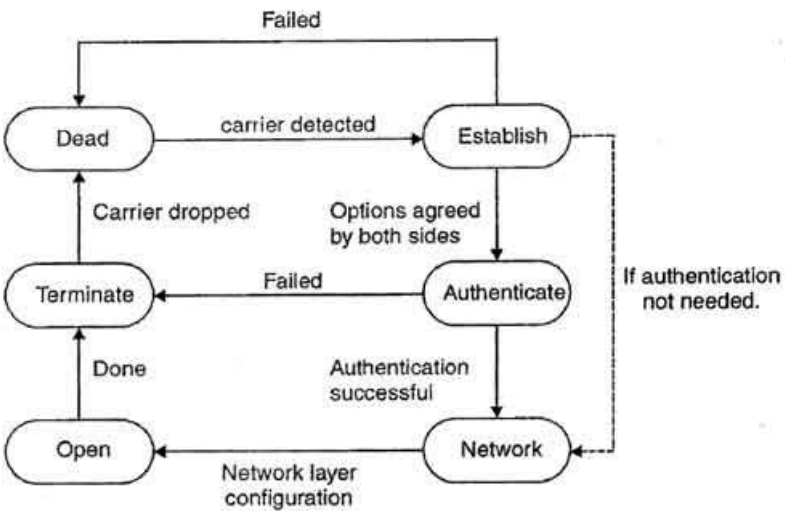
(5) **Data field:** Its length is variable. If the length is not negotiated using LCP during line set up, a default length of 1500 bytes is used. It carries user data or other information.

(6) **FCS field:** The frame checks sequence. It is either of 2 bytes or 4 bytes. It contains the checksum.

Transition Phases in PPP

The PPP connection goes through different states as shown in fig.

(1) **Dead**: In dead phase the link is not used. There is no active carrier and the line is quiet.



Transition phases

(2) **Establish**: Connection goes into this phase when one of the nodes start communication. In this phase, two parties negotiate the options. If negotiation is successful, the system goes into authentication phase or directly to networking phase. LCP packets are used for this purpose.

(3) **Authenticate**: This phase is optional. The two nodes may decide during the establishment phase, not to skip this phase. However if they decide to proceed with authentication, they send several authentication packets. If the result is successful, the connection goes to the networking phase; otherwise, it goes to the termination phase.

(4) **Network**: In network phase, negotiation for the network layer protocols takes place. PPP specifies that two nodes establish a network layer agreement before data at the network layer can be exchanged. This is because PPP supports several protocols at network layer. If a node is running multiple protocols simultaneously at the network layer, the receiving node needs to know which protocol will receive the data.

(5) **Open**: In this phase, data transfer takes place. The connection remains in this phase until one of the endpoints wants to end the connection.

(6) **Terminate**: In this phase connection is terminated.

Point-to-point protocol Stack

PPP uses several other protocols to establish link, authenticate users and to carry the network layer data.

The various protocols used are:

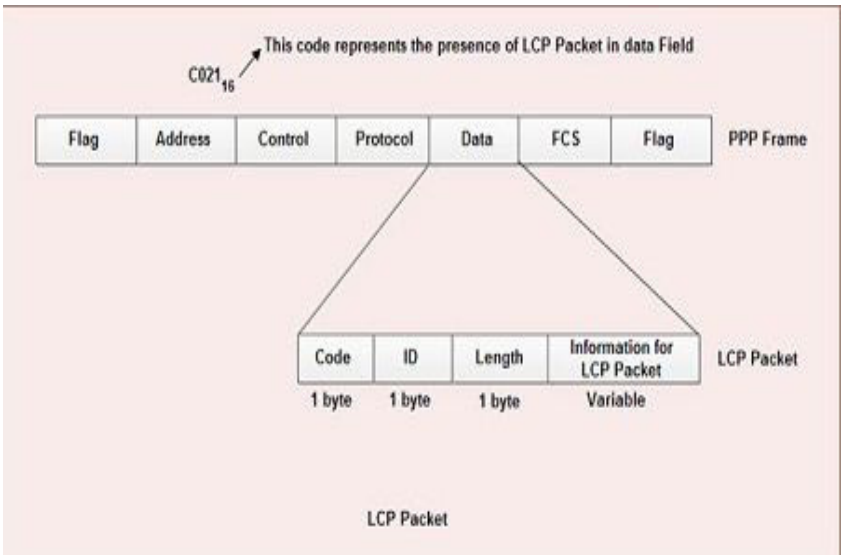
(1) Link Control Protocol

(2) Authentication Protocol

(3) Network Control Protocol

(1) Link Control Protocol

- It is responsible for establishing, maintaining, configuring and terminating the link.
- It provides negotiation mechanism to set options between two endpoints.



- All LCP packets are carried in the data field of the PPP frame.
- The presence of a value $C021_{16}$ in the protocol field of PPP frame indicates that LCP packet is present in the data field.
- The various fields present in LCP packet are:

  (1) **Code**: 1 byte-specifies the type of LCP packet.

  (2) I**D**: 1 byte-holds a value used to match a request with the reply.

  (3) **Length**: 2 byte-specifies the length of entire LCP packet.

  (4) **Information**: Contains extra information required for some LCP packet.

- There are eleven different type of LCP packets. These are categorized in three groups:
  (1) **Configuration packet**: These are used to negotiate options between the two ends. For example: configure-request, configure-ack, configure-nak, configure-reject are some configuration packets.
  (2) **Link termination packets**: These are used to disconnect the link between two end points. For example: terminate-request, terminate-ack, are some link termination packets.
  (3) **Link monitoring and debugging packets**: These are used to monitor and debug the links. For example: code-reject, protocol-reject, echo-request, echo-reply and discard-request are some link monitoring and debugging packets.

(2) Authentication Protocol

Authentication protocols help to validate the identity of a user who needs to access the resources.

There are two authentication protocols:

(1) Password Authentication Protocols (PAP)

(2) Challenge Handshake Authentication Protocol (CHAP)

(1) AP (Password Authentication Protocol)

This protocol provides two step authentication procedures:

Step 1: User name and password is provided by the user who wants to access a system.

Step 2: The system checks the validity of user name and password and either accepts or denies the connection.

- PAP packets are also carried in the data field of PPP frames.
- The presence of PAP packet is identified by the value $C023_{16}$ in the protocol field of PPP frame.
- There are three PAP packets.
  1) **Authenticate-request**: used to send user name & password.
  2) **Authenticate-ack**: used by system to allow the access.
  3) **Authenticate-nak**: used by system to deny the access.

(2) CHAP (Challenge Handshake Authentication Protocol)

- It provides more security than PAP.
- In this method, password is kept secret, it is never sent on-line.
- It is a three-way handshaking authentication protocol:
  (1) System sends. a challenge packet to the user. This packet contains a value, usually a few bytes.

(2) Using a predefined function, a user combines this challenge value with the user password and sends the resultant packet back to the system.

(3) System then applies the same function to the password of the user and challenge value and creates a result. If result is same as the result sent in the response packet, access is granted, otherwise, it is denied.

- **There are 4 types of CHAP packets:**

  (1) Challenge-used by system to send challenge value.

  (2) Response-used by the user to return the result of the calculation.

  (3) Success-used by system to allow access to the system.

  (4) Failure-used by the system to deny access to the system.

(3) Network Control Protocol (NCP)

- After establishing the link and authenticating the user, PPP connects to the network layer. This connection is established by NCP.
- Therefore NCP is a set of control protocols that allow the encapsulation of the data coming from network layer.
- After the network layer configuration is done by one of the NCP protocols, the users can exchange data from the network layer.
- PPP can carry a network layer data packet from protocols defined by the Internet, DECNET, Apple Talk, Novell, OSI, Xerox and so on.
- None of the NCP packets carry networks layer data. They just configure the link at the network layer for the incoming data.

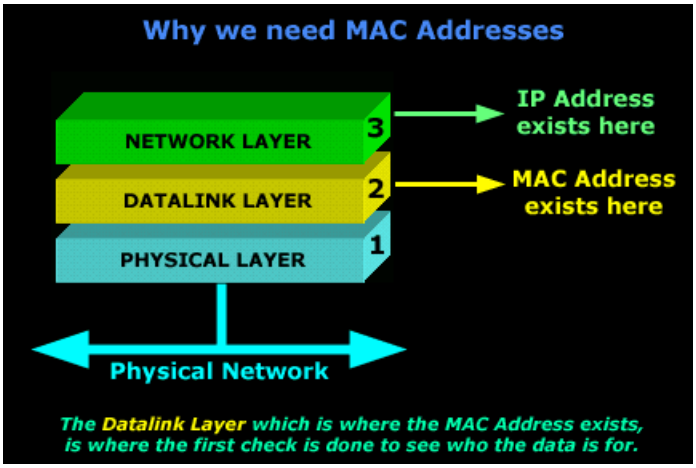
2.4 MEDIA ACCESS CONTROL

Media Access Control (MAC) addresses are talked about in various sections on the site, such as the OSI-Layer 2, Multicast, Broadcast and Unicast. We are going to analyze them in depth here so we can get a firm understanding of them since they are part of the fundamentals of networking.

MAC addresses are physical addresses, unlike IP addresses which are logical addresses. Logical addresses require you to load special drivers and protocols in order to be able to configure your network card/computer with an IP Address, whereas a MAC address doesn't require any drivers whatsoever. The reason for this is that the MAC address is actually "burnt-in" into your network card's memory chipset.

The Reason for MAC

Each computer on a network needs to be identified in some way. If you're thinking of IP addresses, then you're correct to some extent, because an IP address does identify one unique machine on a network, but that is not enough. The diagram below provides a visual representation how important MAC Addresses are on our network and at which layer of the OSI Model they exist:

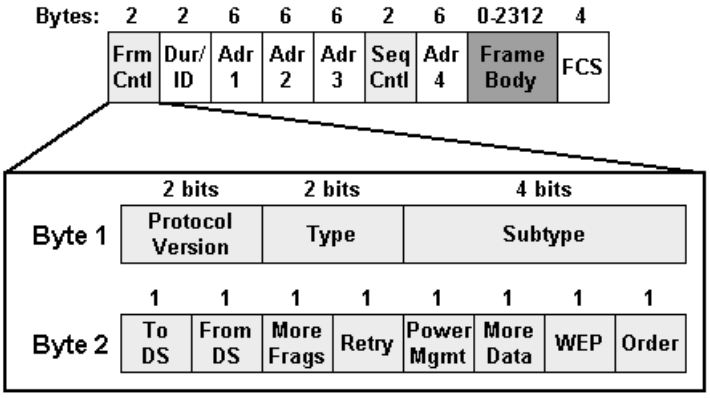


You see, the IP address of a machine exists on the **3rd Layer** of the OSI model and, when a packet reaches the computer, it will travel from Layer 1 upwards, so we need to be able to identify the computer before Layer 3.This is where the **MAC address - Layer 2** comes into the picture. All machines on a network will listen for packets that have their MAC address in the destination field of the packet (they also listen for broadcasts and other stuff, but that's analyzed in other sections).

The Physical Layer understands the electrical signals on the network and creates the frame which gets passed to the Data link layer. If the packet is destined for the computer then the MAC address in the destination field of the packet will match, so it will accept it and pass it onto the Layer above (3) which, in turn, will check the network address of the packet (IP Address), to make sure it matches with the network address to which the computer has been configured.

MAC Frame Format

Since there are various types of Network Interfaces (Ethernet, Token Ring, FDDI etc.) the MAC frame format differs by protocol according to it's design. However most will have at a minimum the following fields:



MAC Control Field

The MAC control field contains all information used for flow control, connection establishment and teardown as well as error control. Not all protocols provide for establishment/

teardown, flow control and error recovery. The content of this field is dependent upon the specified standards for that particular data link layer protocol (Ethernet, Token Ring, FDDI etc.)

Destination / Source MAC Fields

The source MAC address field contains the MAC address of the source machine--the transmitting device (since some computers with MAC addresses aren't called computers--cell phones have MAC addresses), and the destination device is the receiver. The destination MAC is closer to the 'front' (left side in the diagram) of the frame for easier scanning, mostly because it is the destination device that is important as that is the device we are trying to reach.

When the receiver responds to the frame, it will use the source address to generate the destination portion of the frame it sends out. In other words, the source MAC in the frame received becomes the destination MAC in the frame transmitted as a response.

LLC PDU Field

When talking about network communication protocols such as Ethernet or FDDI or Token Ring, they are described as being Physical and Data Link layer protocols--they perform functions that are said to be Physical and Data Link Layer functions as listed in the OSI Model of networking. For Ethernet and Token Ring the Data Link layer is described as being broken into two sub-layers, the MAC sublayer (for the MAC address and Media Access Control functions) and the Logical Link Control sublayer **LLC.**

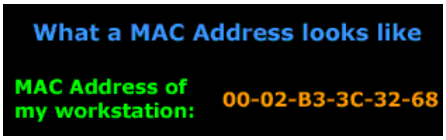
The Logical Link Control Packet Data Unit field (LLC PDU) contains data from the from the LLC sub-layer of the data link layer protocol (eg. Ethernet, FDDI, Token Ring etc.). The LLC information is used to keep track of which piece of data is sent to which IP address and application. For example, the LLC information helps a web browser keep track of which data being received is part of an image in a web page, and which data is the text in the body of the web page itself.

CRC Checksum Field

This field contains what is called a 'checksum' that is the product of a Cyclic Redundancy Check (CRC check). A CRC check is a mathematical forumula that uses the data as input and produces a numeric result that is almost as unique as the input data. Using the CRC checksum value it is possible to verify the the integrity of the frame. Before transmitting the frame, the source computer calculates the checksum and places the checksum value in this field. The receiving computer looks at the same data in the frame and also calculates the checksum. If the CRC it calculates is different from the CRC checksum in the CRC checksum field, the CRC check has failed. Frames that fail this checksum test are discarded because there is a near certainty that the frame is damaged.

Examining a MAC Address

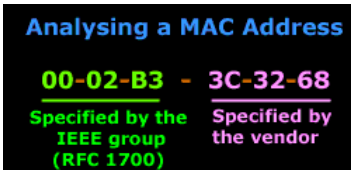
Let's now have a look at a MAC address and see what it looks like! We will use our workstation's MAC address as an example:



MAC Addresses are always presented in HEX format, just as our example above. It is very rare that a MAC address is represented in Binary format because it is simply too long and difficult to understand, as we will see further on.

When a vendor, e.g Intel, produces network cards for computers, they don't just assign them any MAC address they like, this would create a big confusion in identifying who is the vendor of each network card and could possibly result in clashing with another MAC address from another vendor e.g D-link, who happened to choose the same MAC address for their network card!

To avoid these kind of problems, the IEEE group split the MAC address in half, and used the first half to identify the vendor, and the second half is for the vendor to allocate as serial numbers:

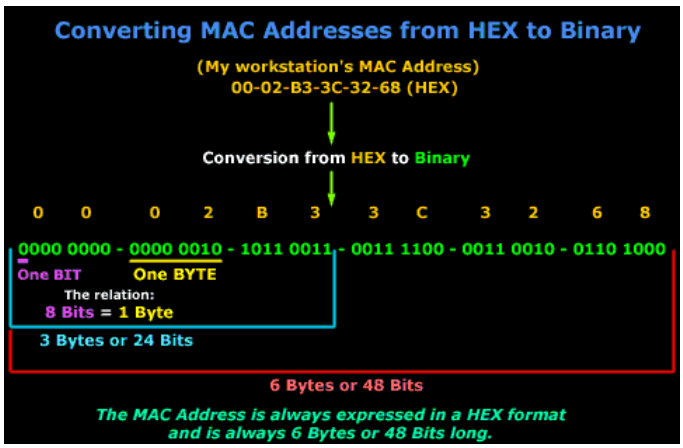


The **Vendor code** is specified by RFC - 1700. You might find a particular vendor having more than just one code; this is because of the wide range of products they might have. They just apply for more, as they need !

Keep in mind that even tho the MAC address is «burnt-in» to the network card›s memory, some vendors will allow you to download special programs to change the **second half of the MAC address** on the card. This is because the vendors actually reuse the same MAC addresses for their network cards because they create so many that they run out of numbers ! But at the same time, the chances of you buying two network cards which have the same MAC address are so small that it's almost impossible !

Let'S Start Talking Bits And Bytes!

Now that we know what a MAC address looks like, we need to start analyzing it. A MAC address of any network card is always the same length, that is, 6 Bytes long or 48 Bits long. If you're scratching your head wondering where these figures came from, then just have a look at the picture below which makes it a bit easier to understand:



2.5 WIRED LANS: ETHERNET

- LAN (Local Area Network) refers to a group of computers interconnected into a network so that they are able to communicate, exchange information and share resources (e.g. printers, application programs, database etc).
- In LAN same computer resources can be used by multiple users in the network.
- Each computer in a LAN can effectively send and receive any information addressed to it.
- This information is in the form of data 'packets'.
- Ethernet is most widely used LAN Technology, which is defined under IEEE standards 802.3.
- The reason behind its wide usability is Ethernet is
- Easy to understand, implement, maintain and allows low cost network implementation.
- Also, Ethernet offers flexibility in terms of topologies which are allowed.
- Ethernet operates in two layers of OSI model, Physical Layer and Data Link Layer.
- In order to handle collision, the Access control mechanism used in Ethernet is CSMA/CD.

Types of Ethernet

(i) Fast Ethernet

- Fast Ethernet refers to an Ethernet network that can transfer data at a rate of 100 Mbit/s.

(ii) Gigabit Ethernet

- Gigabit Ethernet delivers a data rate of 1,000 Mbit/s (1 Gbit/s).

(iii) 10 Gigabit Ethernet

- 10 Gigabit Ethernet is the recent generation and delivers a data rate of 10 Gbit/s (10,000 Mbit/s).

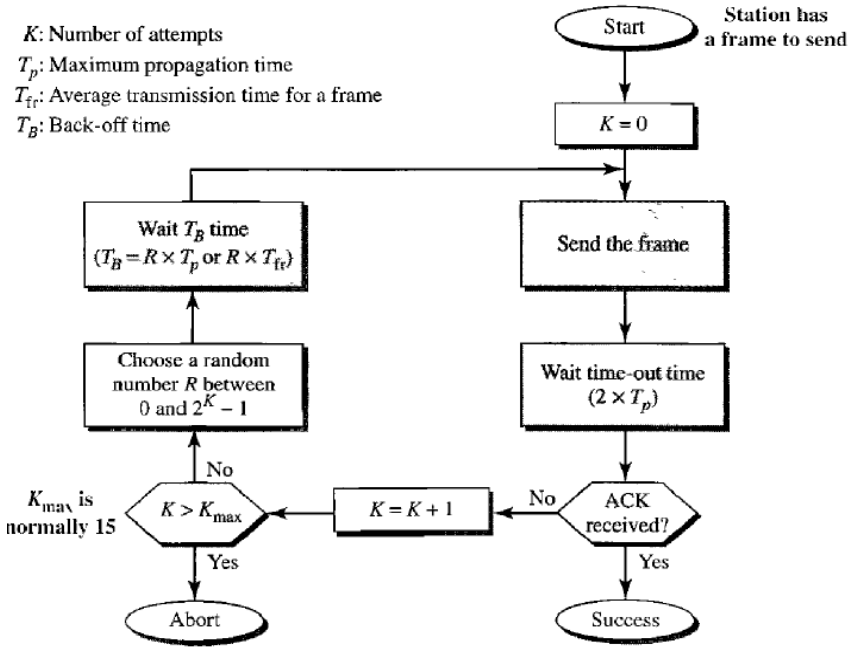
It is generally used for backbones in high-end applications requiring high data rates

Traditional Ethernet (Concept of CSMA/CD)

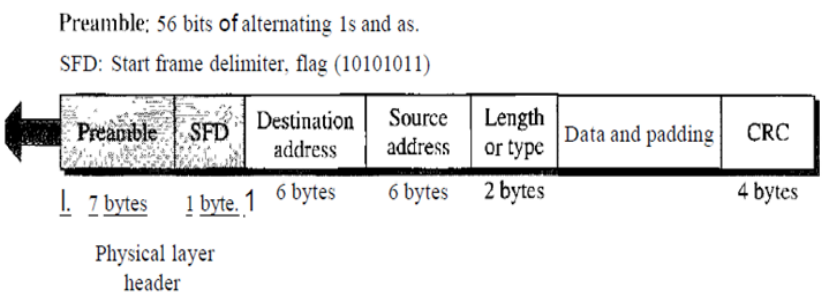
- Traditional Ethernet supports **data transfers at the rate of 10 megabits** per second (Mbps).
- Ethernet cables are manufactured in several standard specifications.
- The most popular Ethernet cable is **CAT5 cable** .
- Data is transmitted in the form of packets.
- **Sense channel prior** to actual packet transmission.
    - Transmit packet only if channel is sensed idle; else, suspend the transmission until channel becomes idle.

- After packet transmission is started, the node monitors its own transmission to see if the packet has to be collision or not.

- Carrier-sense multiple access with collision detection (CSMA/CD).
  - **CS = carrier sense**
  - **MA = multiple access**
  - **CD = collision detection**
- Used **most particularly in early** Ethernet technology for local area networking.
- It **detects collisions by sensing transmissions** from other stations while transmitting a frame.



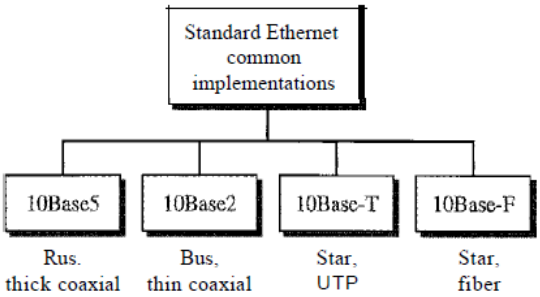
Frame Format



- **Preamble**: It is seven bytes (56 bits) that provides bit synchronization. It consists of alternating Os and 1s. The purpose is to provide alert and timing pulse.
- 2. **Start Frame Delimiter (SFD)**: It is one byte field with unique pattern: 10 10 1011. It marks the beginning of frame.

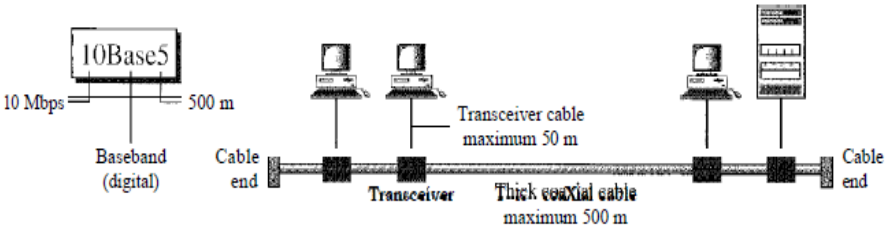
- 3. **Destination Address (DA)**: It is six byte field that contains physical address of packet's destination.
- 4. **Source Address (SA)**: It is also a six byte field and contains the physical address of source or last device to forward the packet (most recent router to receiver).
- 5. **Length**: This two byte field specifies the length or number of bytes in data field.
- 6. **Data**: It can be of 46 to 1500 bytes, depending upon the type of frame and the length of the information field.
- 7. **Frame Check Sequence (FCS)**: This for byte field contains CRC for error detection.

802.3 is a standard specification for Ethernet, a method of physical communication in a local area network (LAN), which is maintained by the Institute of Electrical and Electronics Engineers (IEEE). In general, 802.3 specify the physical media and the working characteristics of Ethernet. The original Ethernet supports a data rate of 10 megabits per second (Mbps).



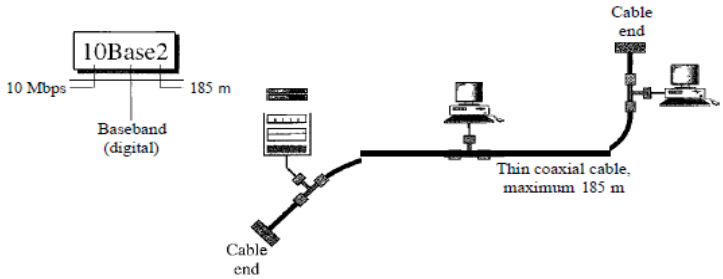
10Base5: Thick Ethernet

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



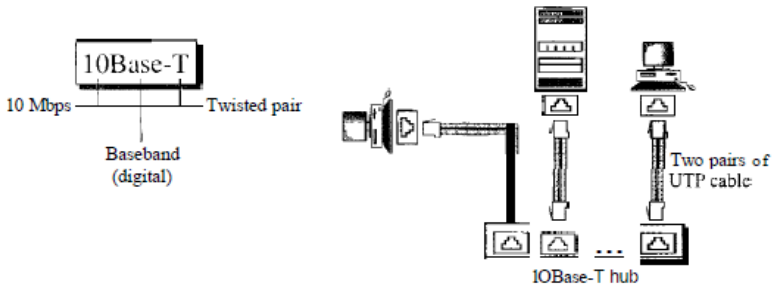
10Base2: Thin Ethernet

The second implementation is called lOBase2, **thin** Ethernet, or Cheaper net.



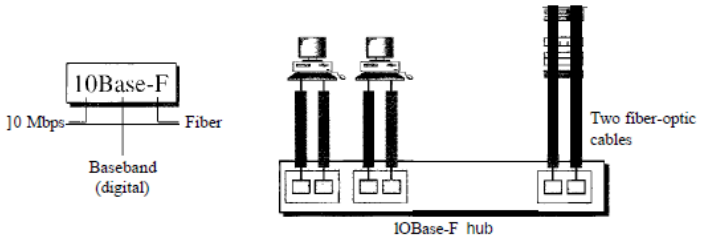
10Base-T: Twisted-Pair Ethernet

The third implementation is called 10Base-T or twisted-pair Ethernet.



10Base-F: Fiber Ethernet

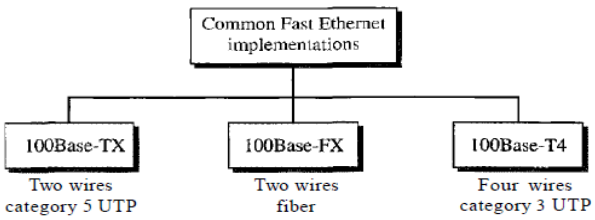
Although there are several types of optical fiber 10-Mbps Ethernet, the most common is called 10Base-F. 10Base-F uses a star topology to connect stations to a hub. The stations are connected to the hub using two fiber-optic cables, as shown in Figure 3..



Fast Ethernet

- Operates at 100 Mbps; faster speeds needed for CAD, image processing, real-time audio and video.
- No change in frame format, addressing, or access method.
- Data rate and collision domain are changed.
- Physical implementation is star topology.
  - 100Base-X (100Base-TX and 100Base-FX).
  - 100Base-T4.

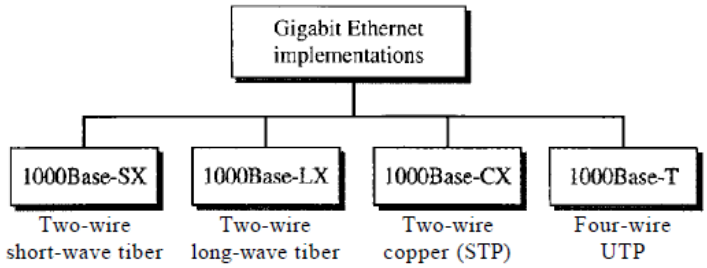
Fast Ethernet implementations



Gigabit Ethernet

- Data rate of 1000 Mbps or 1 Gbps.
- Usually implemented as full-duplex with no CSMA/CD.
- 1000Base-X uses shortwave optical fiber (1000Base-SX), long-wave optical fiber (1000Base-LX), or twisted-pair cables (1000Base-T).

Gigabit Ethernet implementations



2.6 WIRELESS LANS

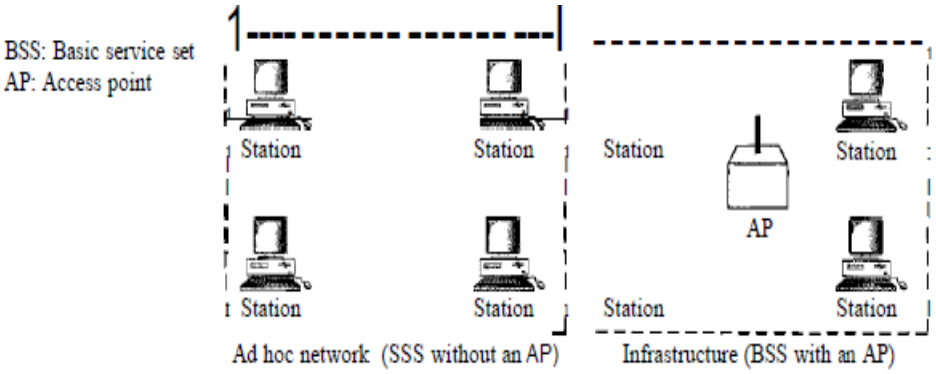
IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

Architecture

The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

Basic Service Set

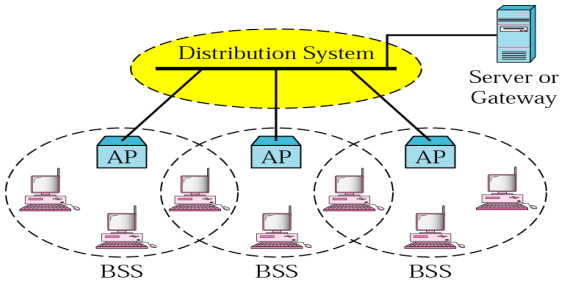
IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP). Following figure shows two sets in this standard. The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture. In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS. ABSS with an AP is sometimes referred to as an infrastructure network.



Extended service set (ESS) – two or more BSSs with APs connected through a distribution system (wired LAN) in an infrastructure network.

Station Types.

- No-transition mobility – either stationary or moving only inside a BSS.
- BSS-transition mobility – c
- an move from one BSS to another, but confined inside one ESS.
- ESS-transition mobility – can move from one ESS to another.



Physical Layer -Five specifications

(1) 802.11 FHSS.

(2) 802.11 DSSS.

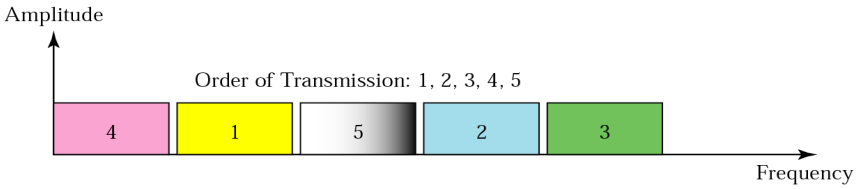
(3) 802.11a OFDM.

(4) 802.11b HR-DSSS.

(5) 802.11g OFDM.

FHSS

- Frequency-hopping spread spectrum in a 2.4 GHz band.
- Carrier sends on one frequency for short duration then hops to another frequency for same duration, hops again to another for same amount of time and so on.
- Spreading adds security since only sender and receiver agree on sequence of allocated bands Contention is handled by MAC sub layer since all stations use the same sub bands

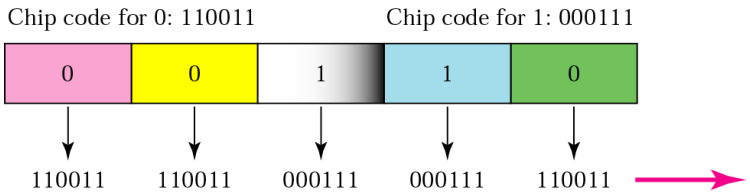


- Pseudorandom number generator selects the hopping sequence.
- Data rate is of 1 or 2 Mbps.

DSSS

- Direct sequence spread spectrum in a 2.4 GHz band.

- Each bit is replaced by a sequence of bits called a chip code, implemented at the physical layer.
- Sender splits each byte of data into several parts and sends them concurrently on different frequencies.
- Data rate is 1 or 2 Mbps.



OFDM

- Orthogonal frequency-division multiplexing using a 5-GHz band.
- Same as FDM except all sub bands are used by only one source at a given time.
- Security increased by assigning sub bands randomly.
- Data rates of 18 Mbps and 54 Mbps.
- Often used in power-line networking.

HR DSSS

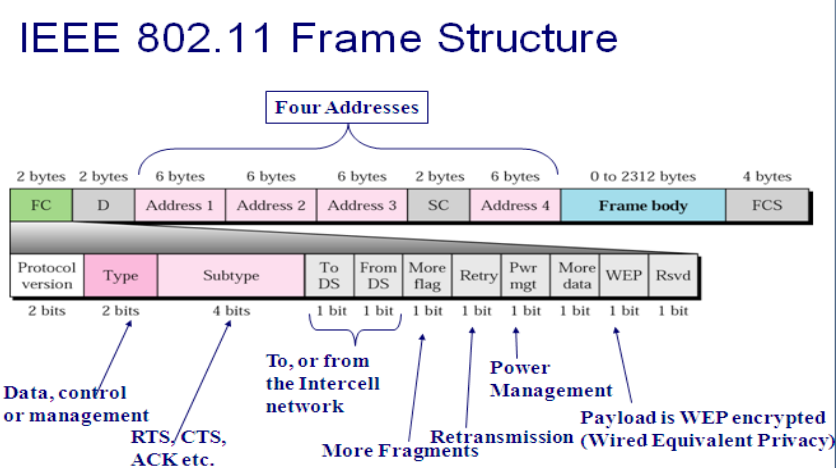
- High-rate DSSS using a 2.4 GHz band.
- Similar to DSSS except for encoding method.
- Uses complementary code keying (CCK), encoding 4 or 8 bits to one CCK symbol.
- Defines four data rates: 1, 2, 5.5, and 11 Mbps.

Fragmentation

- Wireless environment is very noisy.
- Corrupt frames must be retransmitted.
- Large frames must be divided into smaller ones to increase efficiency.

Frame Types

- Management frames – used for initial communication between stations and access points.
- Control frames – used for accessing the channel and acknowledging frames.
- Data frames – used for carrying data and control information.
    - IEEE 802.11 Frame Structure.



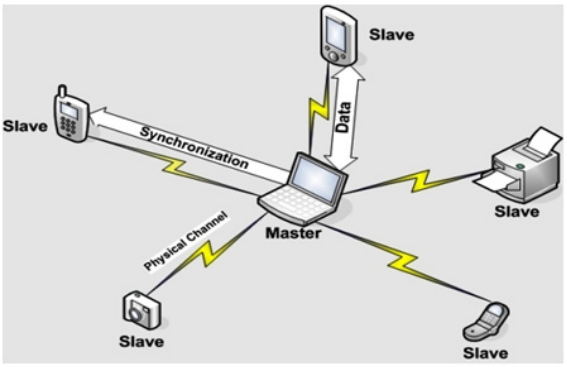
2.7 BLUETOOTH

A Bluetooth technology is a high speed low powered wireless technology link that is designed to connect phones or other portable equipment together. It is a specification (IEEE 802.15.1) for the use of low power radio communications to link phones, computers and other network devices over short distance without wires. Wireless signals transmitted with Bluetooth cover short distances, typically up to 30 feet (10 meters).

It is achieved by embedded low cost transceivers into the devices. It supports on the frequency band of 2.45GHz and can support upto 721KBps along with three voice channels. This frequency band has been set aside by international agreement for the use of industrial, scientific and medical devices (ISM).rd-compatible with 1.0 device. Bluetooth can connect up to "**eight devices"** simultaneously and each device offers a unique 48 bit address from the IEEE 802 standard with the connections being made point to point or multipoint.

How Bluetooth Works:

Bluetooth Network consists of a Personal Area Network or a piconet which contains a minimum of 2 to maximum of 8 Bluetooth peer devices- Usually a single master and up to 7 slaves. A master is the device which initiates communication with other devices. The master device governs the communications link and traffic between itself and the slave devices associated with it. A slave device is the device that responds to the master device. Slave devices are required to synchronize their transmit/receive timing with that of the masters. In addition, transmissions by slave devices are governed by the master device (i.e., the master device dictates when a slave device may transmit). Specifically, a slave may only begin its transmissions in a time slot immediately following the time slot in which it was addressed by the master, or in a time slot explicitly reserved for use by the slave device.



The frequency hopping sequence is defined by the Bluetooth device address (BD_ADDR) of the master device. The master device first sends a radio signal asking for response from the particular slave devices within the range of addresses. The slaves respond and synchronize their hop frequency as well as clock with that of the master device.

Scatternets are created when a device becomes an active member of more than one piconet. Essentially, the adjoining device shares its time slots among the different piconets.

Bluetooth Specifications:

- **Core Specifications** : It defines the Bluetooth protocol stack and the requirements for testing and qualification of Bluetooth-based products.
- **The profiles specification**: It defines usage models that provide detailed information about how to use the Bluetooth protocol for various types of applications.

The core specification consists of 5 layers:

- **Radio**: Radio specifies the requirements for radio transmission – including frequency, modulation, and power characteristics – for a Bluetooth transceiver.
- **Baseband Layer**: It defines physical and logical channels and link types (voice or data); specifies various packet formats, transmit and receive timing, channel control, and the mechanism for frequency hopping (hop selection) and device addressing.It specifies point to point or point to multipoint links. The length of a packet can range from 68 bits (shortened access code) to a maximum of 3071 bits.
- **LMP- Link Manager Protocol (LMP):** defines the procedures for link set up and ongoing link management.
- **Logical Link Control and Adaptation Protocol (L2CAP):** is responsible for adapting upper-layer protocols to the baseband layer.
- **Service Discovery Protocol (SDP):** – allows a Bluetooth device to query other Bluetooth devices for device information, services provided, and the characteristics of those services.

The key features of Bluetooth technology:

- Less complication

- Less power consumption
- Available at cheaper rates
- Robustness

Classification

Various ***types of Bluetooth technology*** are available in the markets which help the consumers to communicate wirelessly. The different types of Bluetooth devices are PC cards, radios, dongles, and headsets. Laptops and other Internet enabled equipments use Bluetooth technology such as wireless mouse and keyboard to communicate wirelessly. Music players like iPods, music phones, or other MP3 players make use of stereo headphones.

Applications

The first and foremost application of Bluetooth technology would be to eradicate the tangling of cables that would mess up the room.

(1) Bluetooth's biggest contribution is to provide a phone with a headset that works wirelessly. This is possible by providing the caller with an earpiece and a small microphone attached to the caller's shirt. The mobile phone can be located in a bag or anywhere in the body. The caller can dial a number even without touching a button on the mobile phone. This technology has the advantage of eliminating the radiation hitting the cerebral region.

(2) PDA, PC or laptop which has enabled Bluetooth can communicate with each other and update with its latest information. This technology has helped in synchronizing the data easily.

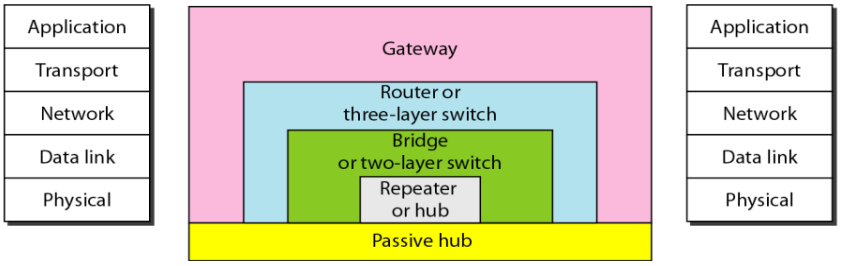
(3) It is difficult to send emails while travelling in a flight. On landing of the flight, the Bluetooth enabled laptop can send the email only when it gets in touch with the user's phone.

(4) Wireless mouse and keyboards are introduced.

(5) One will be alerted on his/her mobile phone when your laptop receives the mail.

(6) You can try to locate a printer via laptop. You will get the printout of that document once that printer is located.

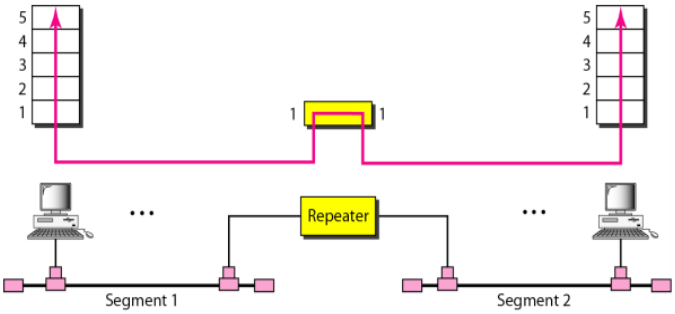
2.8 CONNECTING DEVICES



Working of Repeater

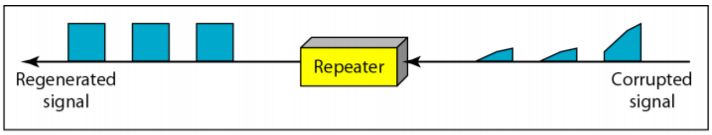
- Repeaters are used in transmission systems and used to regenerate the signals, when they travel over a longer distance, so that the strength of the signal remains the same.

- A repeater can operates at first layer of the OSI layer that is physical layer and it is a 2 port device.
- Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted.
- It used to extend the length in which the signal can be transmitted over the same network and can cover longer distances.

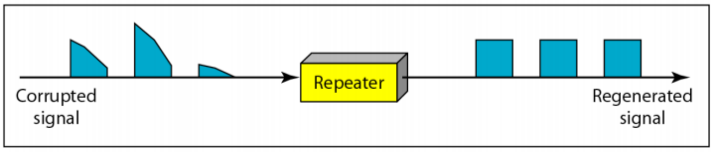


Functions of Repeaters

- The main function of the repeater is to simply regenerate the signal which it receives and retransmits a refreshed signals back into the network towards the others.
- Receive a signal before it becomes too weak or corrupted.
- Can extend only the physical length of network.
- A repeater forwards every frame; it has no filtering capability.
- Repeater is responsible for careful routing of packets such that it would not end up in the wrong network
- Repeater is most basic of these devices is the repeater.



a. Right-to-left transmission.



b. Left-to-right transmission.

Advantages of Repeaters

- **Simple to connect and Cost effective.**
- Ability to strengthen signal.
- Repeaters easily extend the length of network.
- They require no processing over head, so very little if any performance degradation occurs.

- Repeater is to carry signal from one Ethernet cable to the other cable without loss of signal strength.
- If a repeater identifies any collision, it sends the signal to the all connected ports.

Disadvantages of Repeaters

- Repeaters cannot connect different network architectures.
- Repeaters do not reduce network traffic.
- The number of repeaters must be limited.
- Repeaters do not segment the network.
- A repeater does not amplify the signal.
- Too many repeaters on a network create noise on the wire and increase the possibility of packet collisions.
- Devices that are separated only by a repeater are part of the same collision domain.

HUB

- A hub is basically a multiport repeater.
- A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.
- Hubs cannot filter data, so data packets are sent to all connected devices.
- Some hubs have ports for other type of cable such as coaxial cable.
- Hubs range in size from four ports up to and for specific to the network types.

Types of HUB

- These are some hubs which are

  (i) Passive Hub.

  (ii) Active Hub.

  (iii) Switch/ Intelligent Hub.

Passive Hub:

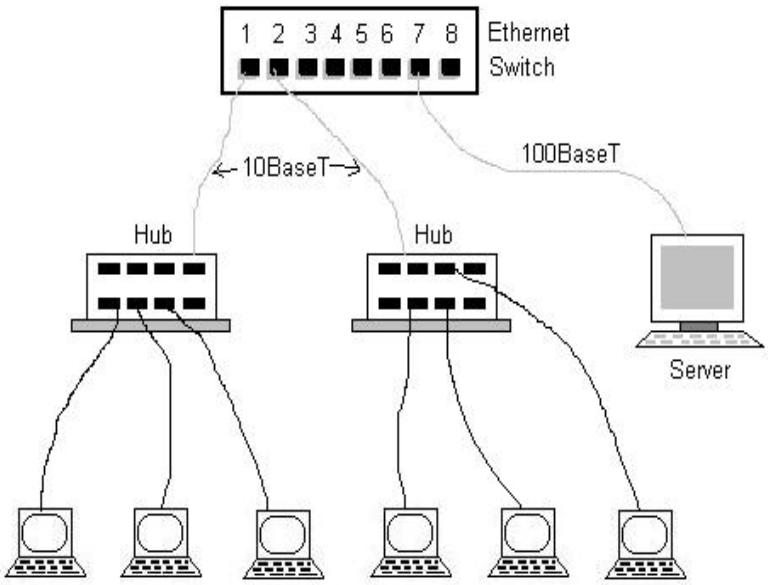
- It provides no signal regeneration.
- They are simply cables connected together so that the signal is passed to other nodes without regeneration.
- These are not used often today because of loss of cable length that is allowed.

Active Hub:

- It acts as repeaters and regenerates the data signals to all ports.
- They have no real intelligence to tell whether the signal needs to go to all ports that is blindly repeated.

Switch Hub:

- Switch hub are multi ports bridges.
- They filter traffic between the ports on the switch by using the address of computers transmitting to them.
- It can be used when data performance is needed or when collision need to be reduce.



Advantages of HUB

- It is cheaper and can connect different media types.
- It can extend total distance of the network.
- It does not affect performance of the network seriously.
- It is Available in 4 to 24 port sizes
- Hubs need almost no configuration.
- Active hub can extend maximum network media distance.
- No processing is done at the hub to slow down performance.
- It is a central point of connection among media segments.
- Cables from network devices plug in to the ports on the hub.

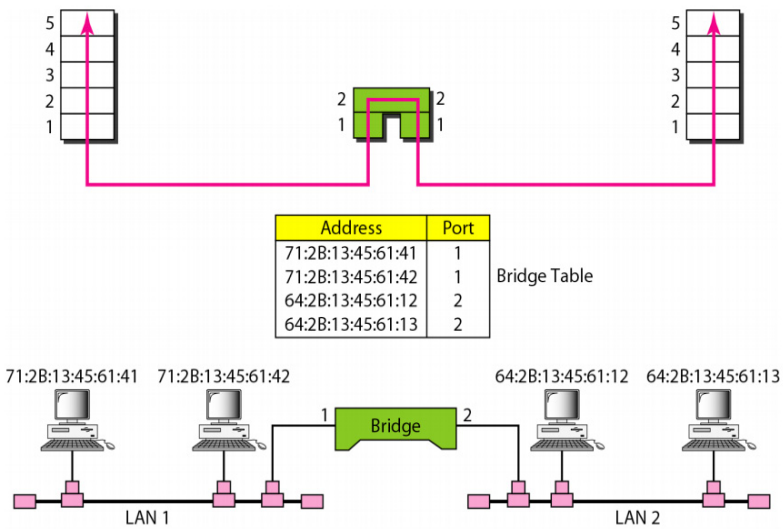
Disadvantages of HUB

- It does not operate in full duplex mode.
- It does not have mechanism to reduce the network traffic.
- It cannot filter information i.e. it passes packets to all the connected segments.
- Since hubs can act as multiport repeaters the network using them must follow the same rules as repeaters.

- It does not have mechanisms such as collision detection and retransmission of packets.
- It cannot connect different network architectures such as token ring and Ethernet etc.

BRIDGES

- Operates in both the physical and the data link layer.
- As a physical layer device, it regenerates the signal it receives.
- As a data link layer device, the bridge can check the PHYSICAL / MAC addresses (source and destination) contained in the frame.
- A bridge has a table used in filtering decisions and maps address to ports.
- It can check the destination address of a frame and decide if the frame should be forwarded or dropped.
- If the frame is to be forwarded, then decision must specify the port.
- Today Learning bridges have been introduced that build a list of the MAC addresses on the interface by observing the traffic on the network. This is a leap in the development field of manually recording of MAC addresses.



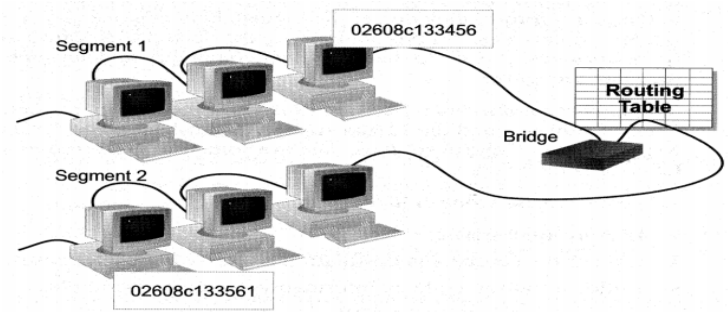
Types of Bridges:

There are mainly three types in which bridges can be characterized:

- **Transparent Bridge:** As the name signifies, it appears to be transparent for the other devices on the network. The other devices are ignorant of its existence. It only blocks or forwards the data as per the MAC address.
- **Source Route Bridge:** It derives its name from the fact that the path which packet takes through the network is implanted within the packet. It is mainly used in Token ring networks.
- **Translational Bridge:** The process of conversion takes place via Translational Bridge. It converts the data format of one networking to another. For instance Token ring to Ethernet and vice versa.

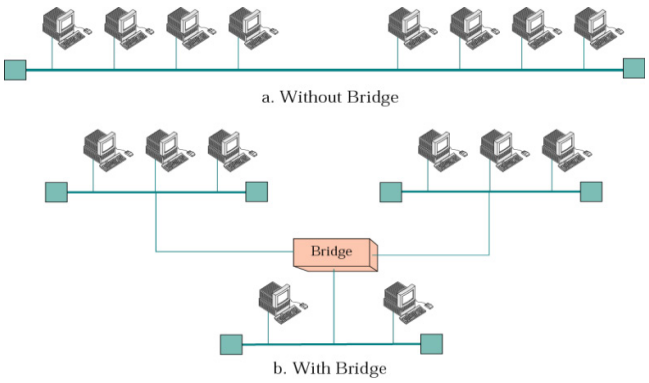
How Bridges Work

- Bridges work at the Media Access Control Sub-layer of the OSI model
  - Routing table is built to record the **segment no. of address**.
  - If destination address is in the **same segment as the source address, stops transmit.**
  - Otherwise, **forward to the other segment**.



Characteristics of Bridges

- **Routing Tables** – Is used to determine the network of destination station of a received packet.
- **Filtering** – Is used by bridge to allow only those packets send to the remote network. Packets are filtered with respect to their destination and multicast addresses.
- **Forwarding –** the process of passing a packet from one network to another.
- **Learning Algorithm** – the process by which the bridge learns how to reach stations on the internetwork.



Advantages of using a bridge

- Extend physical network.
- Reduce network traffic with minor segmentation.
- Creates separate collision domains.
- Reduce collisions.
- Connect different architecture.

Disadvantages of using bridges

- Slower that repeaters due to filtering.
- Do not filter broadcasts.
- More expensive than repeaters.

SWITCHES

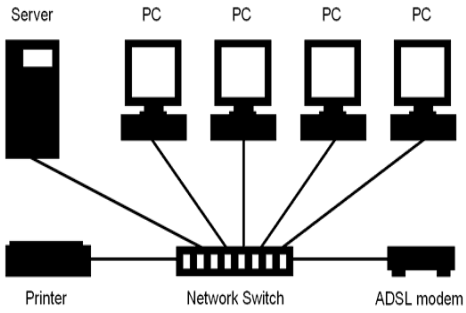
- Switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI model.
- Some switches can also process data at the network layer (layer 3) by additionally incorporating routing functionality.
- Such switches are commonly known as layer-3 switches or multilayer switches.
- Two layer switches operate at PHY and data link layer.
- Three layer switches operates at network layer.

Role of switches in a network

- Switches are most commonly used as the network connection.
- In the hierarchical internetworking model and similar network architectures, switches are also used deeper in the network to provide connections between the switches.
- Switches are the linkage points of an Ethernet network.
- A switch does so by having an in-built learning of the MAC address of the devices connected to it.
- Switches operate in full-duplex mode where devices can send and receive data from the switch at the simultaneously.

Typical switch management features

- Turn particular port range on or off.
- Link bandwidth and duplex settings.
- Priority settings for ports.
- IP management by IP clustering.
- Use of Spanning Tree Protocol (STP) and Shortest Path Bridging (SPB) technologies.
- Simple Network Management Protocol (SNMP) monitoring of device and link health.
- It can deal VLAN settings, link and Port mirroring.



Benefits or advantages of Switches

Following are the benefits or advantages of Switches:

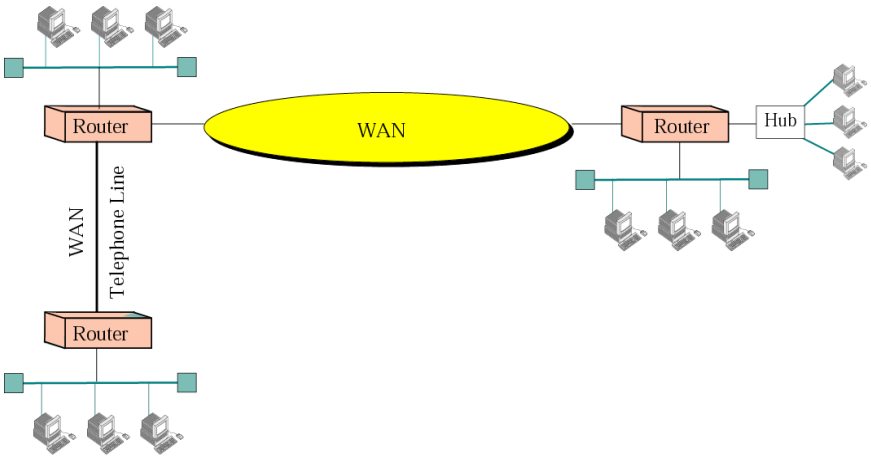
- They increase the available bandwidth of the network.
- They help in reducing workload on individual host PCs.
- They increase the performance of the network.
- Networks which use switches will have less frame collisions.
- This is due to the fact that switches create collision less area for each connection.
- Switches can be directly connected to servers and workstations.

Drawbacks or disadvantages of Switches

- They are more expensive compare to network bridges.
- Network connectivity issues are difficult to be traced through the network switch.
- Broadcast traffic may be troublesome.
- If switches are in promiscuous mode, they are weak to security attacks e.g. spoofing IP address or capturing of Ethernet frames.
- Proper design and configuration is needed in order to handle multicast packets.
- While limiting broadcasts, they are not as good as routers.

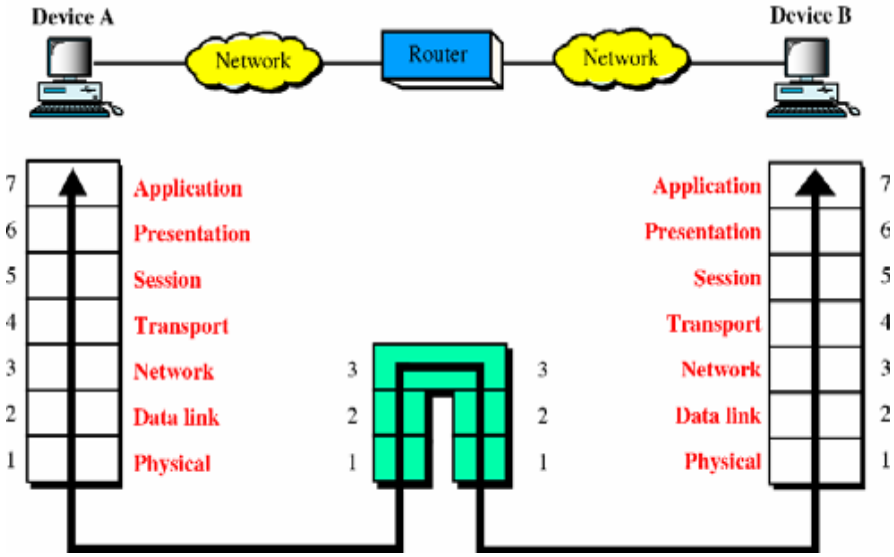
ROUTERS

Routers are network layer devices and are particularly identified as Layer- 3 devices of the OSI Model. They process logical addressing information in the Network header of a packet such as IP Addresses. Router is used to create larger complex networks by complex traffic routing. It has the ability to connect dissimilar LANs on the same protocol. It also has the ability to limit the flow of broadcasts. A router primarily comprises of a hardware device or a system of the computer which has more than one network interface and routing software.



Functionality:

When a router receives the data, it determines the destination address by reading the header of the packet. Once the address is determined, it searches in its **routing table** to get know how to reach the destination and then forwards the packet to the higher hop on the route. The hop could be the final destination or another router.



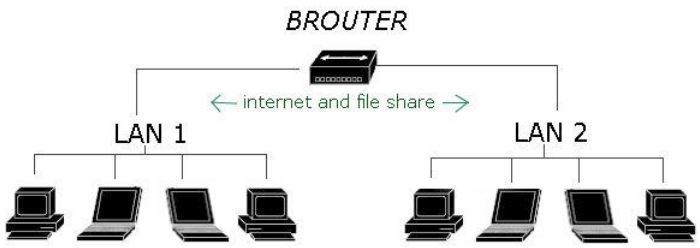
Routing tables play a very pivotal role in letting the router makes a decision. Thus a routing table is ought to be updated and complete. The two ways through which a router can receive information are:

- **Static Routing**: In static routing, the routing information is fed into the routing tables manually. It does not only become a time-taking task but gets prone to errors as well.
- The manual updating is also required in case of statically configured routers when change in the topology of the network or in the layout takes place. Thus static routing is feasible for tinniest environments with minimum of one or two routers.
- **Dynamic Routing**: For larger environment dynamic routing proves to be the practical solution. The process involves use of peculiar routing protocols to hold communication.

The purpose of these protocols is to enable the other routers to transfer information about to other routers, so that the other routers can build their own routing tables.

BROUTERS

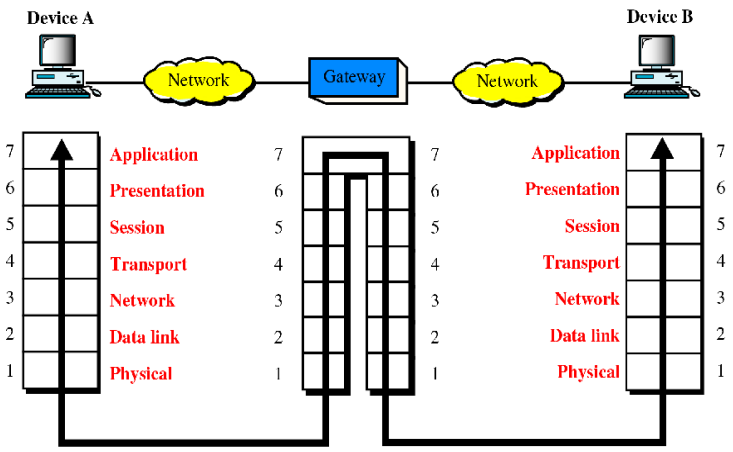
Brouters are the combination of both the bridge and routers. They take up the functionality of the both networking devices serving as a bridge when forwarding data between networks, and serving as a router when routing data to individual systems. Brouter functions as a filter that allows some data into the local network and redirects unknown data to the other network. Brouters are rare and their functionality is embedded into the routers functioned to act as bridge as well.



GATEWAYS

Gateway is a device which is used to connect multiple networks and passes packets from one packet to the other network. Acting as the 'gateway' between different networking systems or computer programs, a gateway is a device which forms a link between them. It allows the computer programs, either on the same computer or on different computers to share information across the network through protocols. A router is also a gateway, since it interprets data from one network protocol to another.

Others such as bridge convert the data into different forms between two networking systems. Then a software application converts the data from one format into another. Gateway is a viable tool to translate the data format, although the data itself remains unchanged. Gateway might be installed in some other device to add its functionality into another.



Network card

Network cards also known as Network Interface Cards (NICs) are hardware devices that connect a computer with the network. They are installed on the mother board. They are responsible for developing a physical connection between the network and the computer. Computer data is translated into electrical signals send to the network via Network Interface Cards.

They can also manage some important data-conversion function. These days network cards are software configured unlike in olden days when drivers were needed to configure them. Even if the NIC doesn't come up with the software then the latest drivers or the associated software can be downloaded from the internet as well.

Network protocols

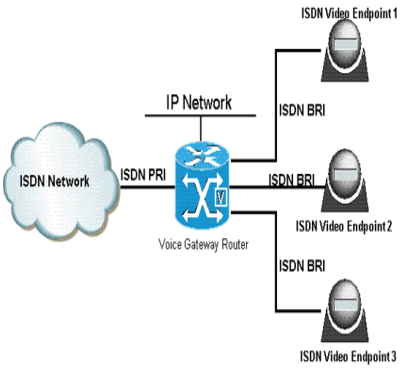
Network protocols define a language of instructions and conventions for communication between the network devices. It is essential that a networked computer must have one or more protocol drivers. Usually, for two computers to interconnect on a network, they must use identical protocols. At times, a computer is designed to use multiple protocols. Network protocols like HTTP, TCP/IP offer a basis on which much of the Internet stands.

System requirement:

- The **bus compatibility** should be verified on installing an NIC into the system. The commonly used bus system is Peripheral Component Interconnect (PCI).
- Memory I/O addresses and IRQ are needed.
- Need of drivers if not already installed.

ISDN (Integrated Services Digital Network)

ISDN are used to send over graphic or audio data files. It is a WAN technology that can be used in place of a dial up link. The accessibility of ISDN depends upon the provision of the service by the service provider, the quality of the line set up to your area. It surely provides higher speed than a modem and has the capability to pick up the line and drop it considerably at a faster rate.



ISDN can create numerous communication routes on a single line. Nowadays, even faster and cheaper technologies that ISDN have found their way in the realm of technology.

MODEMS

Modem is a device which converts the computer-generated digital signals of a computer into analog signals to enable their travelling via phone lines. The 'modulator-demodulator' or

modem can be used as a dial up for LAN or to connect to an ISP. Modems can be both external, as in the device which connects to the USB or the serial port of a computer, or proprietary devices for handheld gadgets and other devices, as well as internal; in the form of add-in expansion cards for computers and PCMCIA cards for laptops.

Configuration of a modem differs for both the external and internal modem. For internal modems, IRQ – Interrupt request is used to configure the modem along with I/O, which is a memory address. Typically before the installation of built-in modem, integrated serial interfaces are disabled, simultaneously assigning them the COM2 resources.

For external connection of a modem, the modem assigns and uses the resources itself. This is especially useful for the USB port and laptop users as the non-complex and simpler nature of the process renders it far much more beneficial for daily usage.

Upon installation, the second step to ensure the proper working of a modem is the installation of drivers.

The modem working speed and processing is dependent on two factors:

- Speed of UART – Universal Asynchronous Receiver or Transmitter chip (installed in the computer to which the modem connection is made).
- Speed of the modem itself.