

UNIT II : DATA-LINK LAYER & MEDIA ACCESS

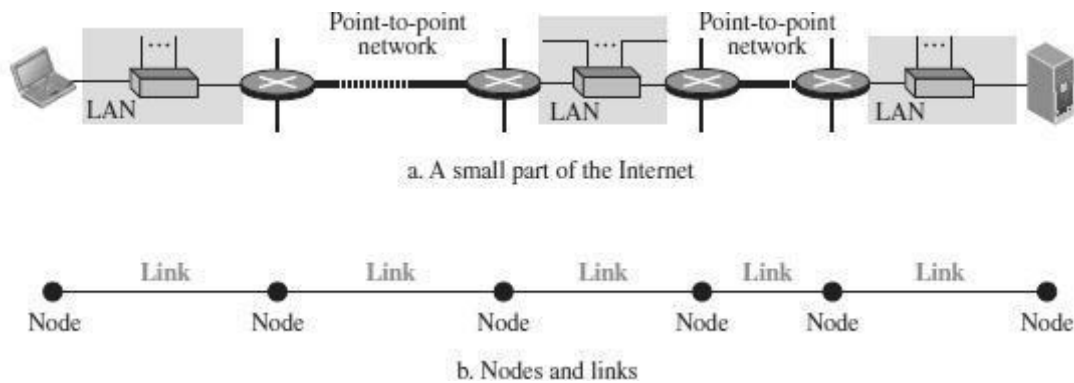
Introduction – Link-Layer Addressing – DLC Services – Data-Link Layer Protocols – HDLC – PPP – Media Access Control – Wired LANs: Ethernet – Wireless LANs – Introduction – IEEE 802.11, Bluetooth – Connecting Devices

1. INTRODUCTION

- In the OSI model, the data link layer is the 2nd layer from the bottom.
- It is responsible for **transmitting frames from one node to next node**.
- The main responsibility of the Data Link Layer is to transfer the datagram across an individual link.
- An important characteristic of a Data Link Layer is that datagram can be handled by different link layer protocols on different links in a path.
- The other responsibilities of this layer are
 - **Framing** - Divides the stream of bits received into data units called frames.
 - **Physical addressing** – If frames are to be distributed to different systems on the same network, data link layer adds a header to the frame to define the sender and receiver.
 - **Flow control**- If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender ,the Data link layer imposes a flow control mechanism.
 - **Error control**- Used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.
 - **Medium Access control** - Used to determine which device has control over the link at any given time.

Nodes and Links

- Communication at the data-link layer is node-to-node.
- The communication channel that connects the adjacent nodes is known as links, and in order to move the datagram from source to the destination, the datagram must be moved across an individual link.
- A data unit from one point in the Internet needs to pass through many networks (LAN and WAN) to reach another point.
- These LANs and WANs are connected by routers.
- The two end hosts and the routers are **nodes** and the networks in-between are **links**.



- The first node is the source host; the last node is the destination host.
- The other four nodes are four routers.
- The first, the third, and the fifth links represent the three LANs; the second and the fourth links represent the two WANs.

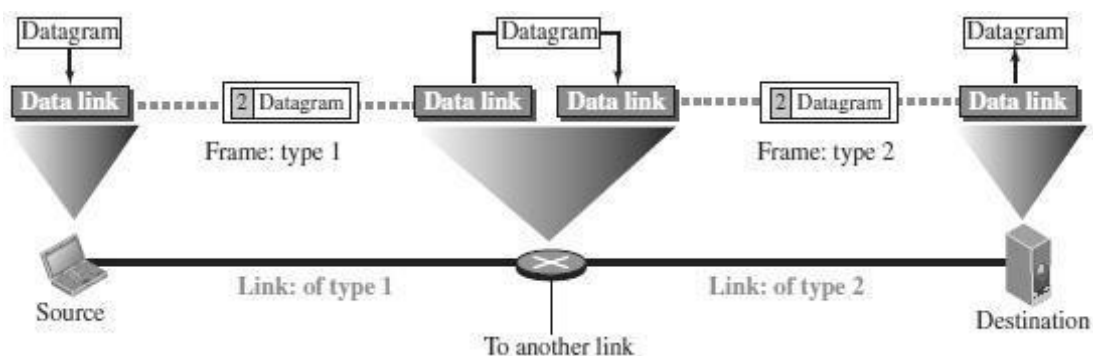
Two Categories of Links

Point- to-Point link and Broadcast link.

- In a point-to-point link, the link is dedicated to the two devices
- In a broadcast link, the link is shared between several pairs of devices.

Data Link Layer Services

- The data-link layer is located between the physical and the network layers.
- The datalink layer provides services to the network layer; it receives services from the physical layer.
- When a packet is travelling, the data-link layer of a node (host or router) is responsible for delivering a datagram to the next node in the path.
- For this purpose, the data-link layer of the sending node needs to encapsulate the datagram and the data-link layer of the receiving node needs to decapsulate the datagram.

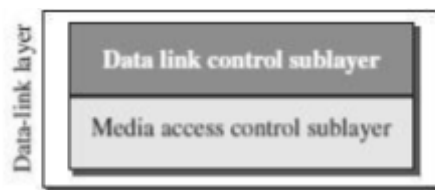


- The datagram received by the data-link layer of the source host is encapsulated in a frame.
- The frame is logically transported from the source host to the router.

- The frame is decapsulated at the data-link layer of the router and encapsulated at another frame.
- The new frame is logically transported from the router to the destination host.

Sublayers in Data Link layer

- We can divide the data-link layer into two sublayers: **data link control (DLC)** and **media access control (MAC)**.
- The data link control sublayer deals with all issues common to both point-to-point and broadcast links
- The media access control sublayer deals only with issues specific to broadcast links.

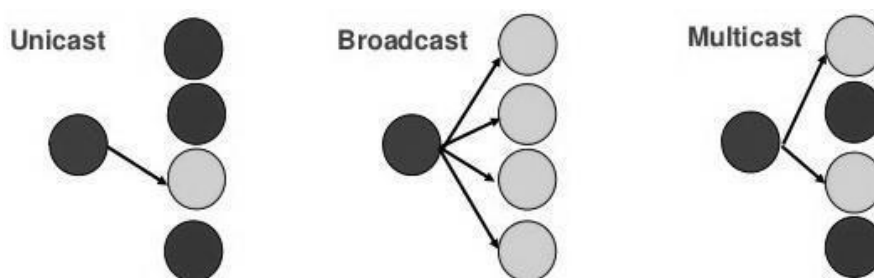


2. LINK-LAYER ADDRESSING

- A link-layer address is sometimes called a link address, sometimes a physical address, and sometimes a MAC address.
- Since a link is controlled at the data-link layer, the addresses need to belong to the data-link layer.
- When a datagram passes from the network layer to the data-link layer, the datagram will be encapsulated in a frame and two data-link addresses are added to the frame header.
- These two addresses are changed every time the frame moves from one link to another.

THREE TYPES OF ADDRESSES

The link-layer protocols define three types of addresses: unicast, multicast, and broadcast.



Unicast Address :

Each host or each interface of a router is assigned a unicast address. Unicasting means one-to-one communication. A frame with a unicast address destination is destined only for one entity in the link.

Multicast Address :

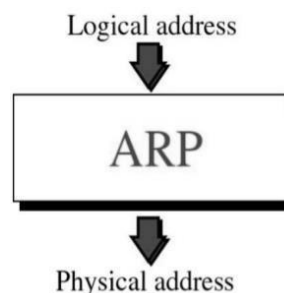
Link-layer protocols define multicast addresses. Multicasting means one-to-many Communication but not all.

Broadcast Address :

Link-layer protocols define a broadcast address. Broadcasting means one-to-all communication. A frame with a destination broadcast address is sent to all entities in the link.

ADDRESS RESOLUTION PROTOCOL (ARP)

- o ARP stands for Address Resolution Protocol.
- o ARP is the most important protocol of the Data Link Layer.
- o ARP is a network layer protocol used to **convert a IP address (Network/Logical address) into a MAC Address (Hardware /Physical address).**

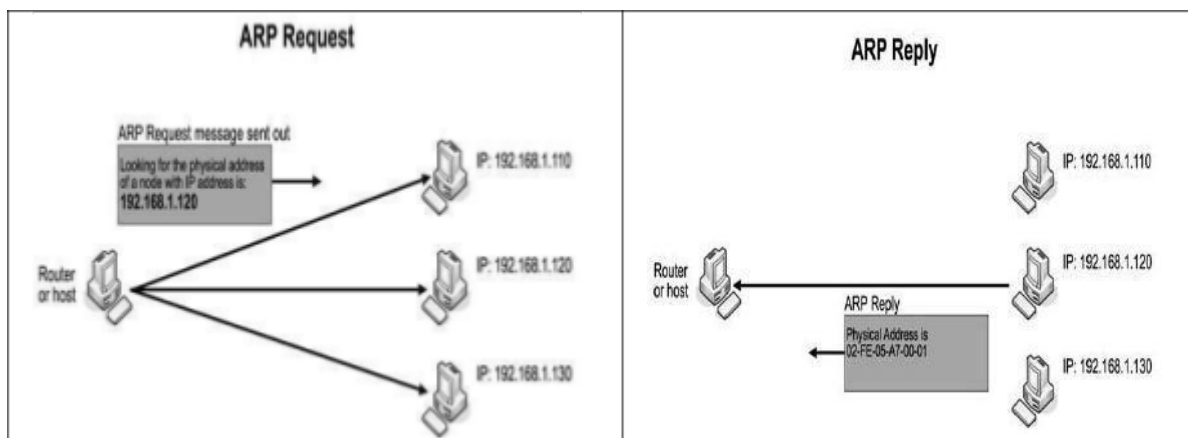


- o The computer programs/applications use logical address (IP address) to send/receive messages, however the actual communication happens over the physical address (MAC address).
- o To send a datagram over a network, we need both the logical and physical address.
- o IP addresses are made up of 32 bits whereas MAC addresses are made up of 48 bits.
- o ARP enables each host to build a table of IP address and corresponding physical address.
- o ARP relies on broadcast support from physical networks.
- o The Address Resolution Protocol is a request and response protocol.
- o The types of ARP messages are:
 1. ARP request
 2. ARP reply

ARP Operation

- o ARP maintains a cache table in which MAC addresses are mapped to IP addresses.
- o If a host wants to send an IP datagram to a host, it first checks for a mapping in the cache table.
- o If no mapping is found, it needs to invoke the Address Resolution Protocol over the network.
- o It does this by broadcasting an ARP query onto the network.
- o This query contains the target IP address.
- o Each host receives the query and checks to see if it matches its IP address.
- o If it does match, the host sends a response message that contains its link-layer address (MAC Address) back to the originator of the query.
- o The originator adds the information contained in this response to its ARP table.
- o For example,

To determine system B's physical (MAC) address, system A broadcasts an ARP request containing B's IP address to all machines on its network.



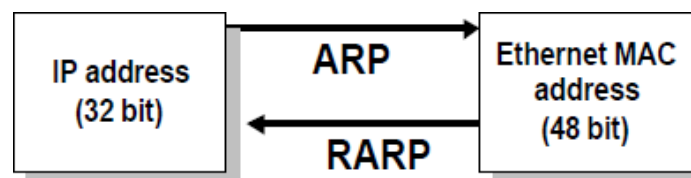
- o All nodes except the destination discard the packet but update their ARP table.
- o Destination host (System B) constructs an ARP Response packet
- o ARP Response is unicast and sent back to the source host (System A).
- o Source stores target Logical & Physical address pair in its ARP table from ARP Response.
- o If target node does not exist on same network, ARP request is sent to default router.

ARP Packet

Hardware Type		Protocol Type
Hardware length	Protocol length	Operation Request:1, Reply:2
Source hardware address		
Source protocol address		
Destination hardware address (Empty in request)		
Destination protocol address		

RARP – Reverse ARP

- Reverse Address Resolution protocol (RARP) allows a host to convert its MAC address to the corresponding IP address.



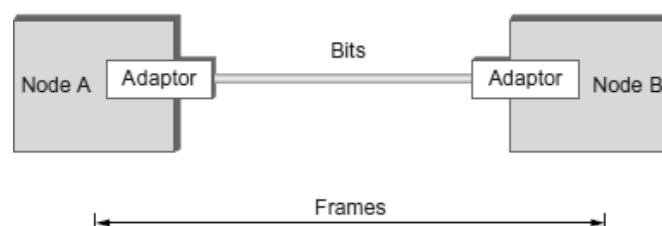
3. DLC SERVICES

- The data link control (DLC) deals with procedures for communication between two adjacent nodes—node-to-node communication—no matter whether the link is dedicated or broadcast.
- Data link control service include

(1) Framing (2) Flow Control (3) Error Control

1. FRAMING

- The data-link layer packs the bits of a message into frames, so that each frame is distinguishable from another.



- Although the whole message could be packed in one frame, that is not normally done.
- One reason is that a frame can be very large, making flow and error control very inefficient.

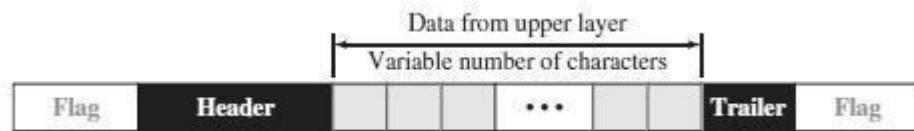
- When a message is carried in one very large frame, even a single-bit error would require the retransmission of the whole frame.
- When a message is divided into smaller frames, a single-bit error affects only that small frame.
- Framing in the data-link layer separates a message from one source to 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 of fixed or variable size.
- Frames of fixed size are called cells. 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, we need a way to define the end of one frame and the beginning of the next. Two approaches were used for this purpose: a character-oriented approach and a bit-oriented approach.

Character-Oriented Framing

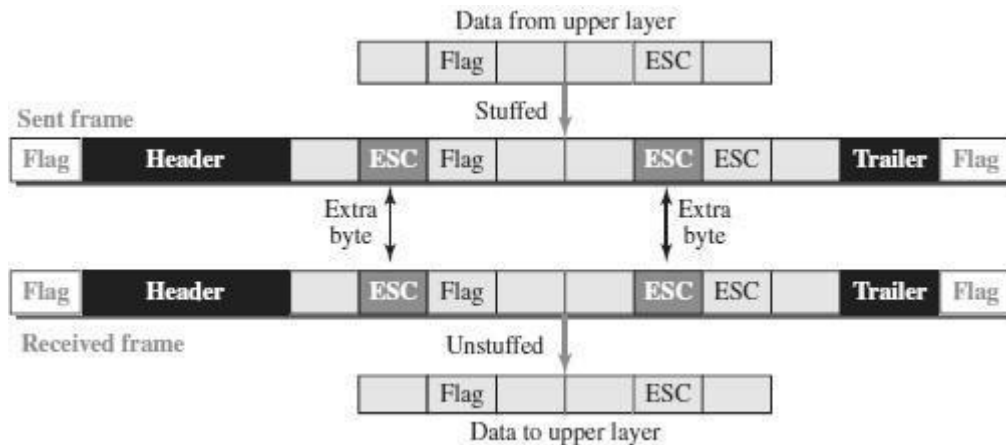
- In character-oriented (or byte-oriented) framing, data to be carried are 8-bit characters.
- To separate one frame from the next, an 8-bit (1-byte) flag is added at the beginning and the end of a frame.
- The flag, composed of protocol-dependent special characters, signals the start or end of a frame.



- Any character used for the flag could also be part of the information.
- If this happens, when it encounters this pattern in the middle of the data, the receiver thinks it has reached the end of the frame.
- To fix this problem, a **byte-stuffing** strategy was added to character-oriented framing.

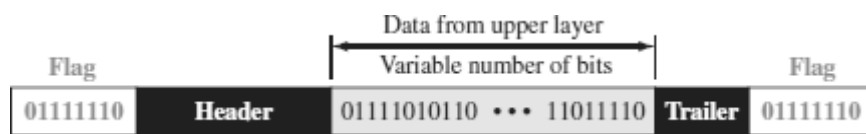
Byte Stuffing (or) Character Stuffing

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



Bit-Oriented Framing

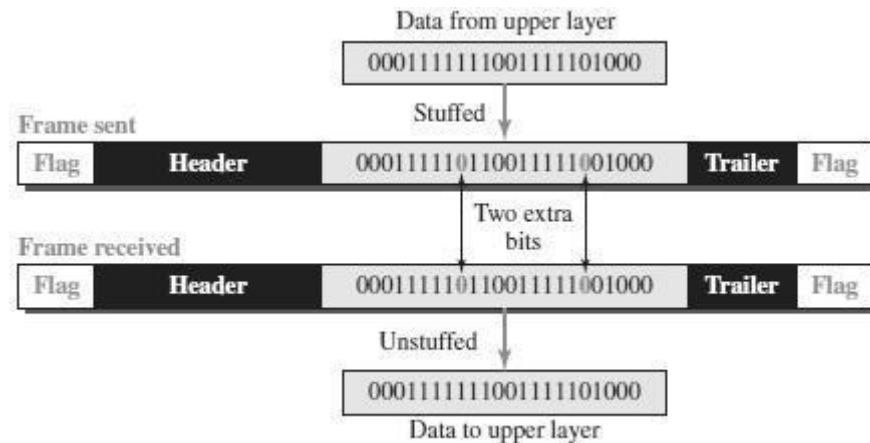
- In bit-oriented framing, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on.
- In addition to headers and trailers, we still need a delimiter to separate one frame from the other.
- Most protocols use a special 8-bit pattern flag, 01111110, as the delimiter to define the beginning and the end of the frame



- If the flag pattern appears in the data, the receiver must be informed that this is not the end of the frame.
- This is done by stuffing 1 single bit (instead of 1 byte) to prevent the pattern from looking like a flag. The strategy is called **bit stuffing**.

Bit Stuffing

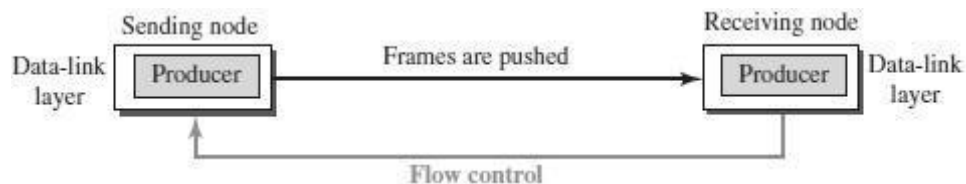
- **Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow a 0 in the data, so that the receiver does not mistake the pattern 01111110 for a flag.**
- In bit stuffing, if a 0 and five consecutive 1 bits are encountered, an extra 0 is added.
- This extra stuffed bit is eventually removed from the data by the receiver.
- The extra bit is added after one 0 followed by five 1's regardless of the value of the next bit.
- This guarantees that the flag field sequence does not inadvertently appear in the frame.



2.

FLOW CONTROL

- o **Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.**
- o The receiving device has limited speed and limited memory to store the data.
- o Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.
- o It requires a buffer, a block of memory for storing the information until they are processed.

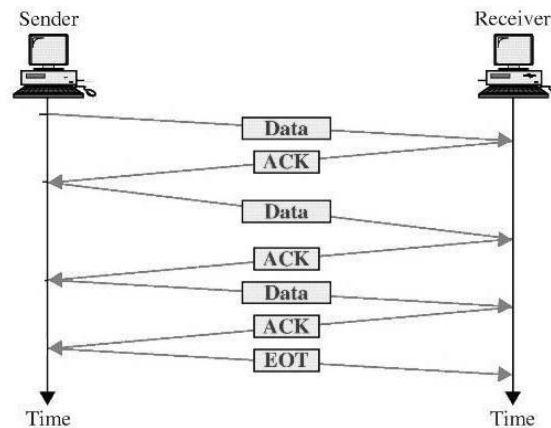


Two methods have been developed to control the flow of data:

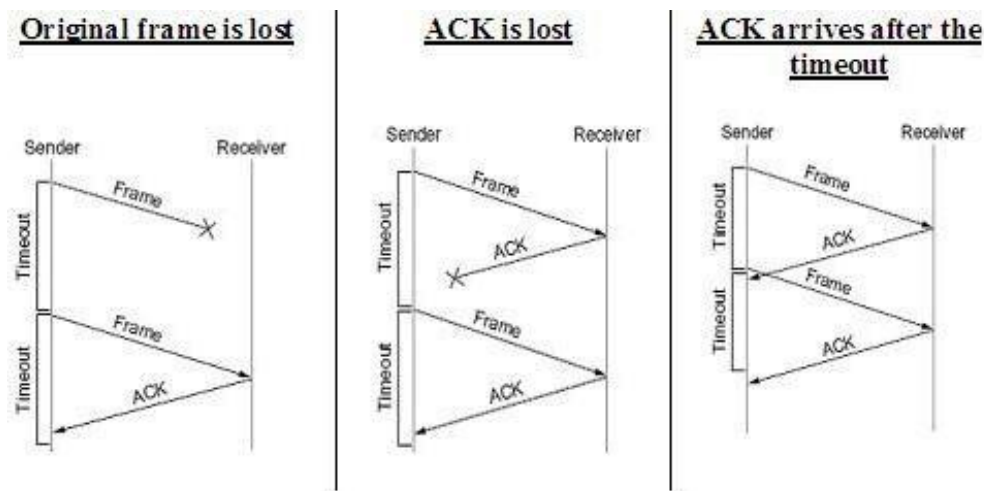
- o Stop-and-Wait
- o Sliding Window
- o

STOP-AND-WAIT

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



- o 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.
- o The acknowledgement may not arrive because of the following three scenarios :
 1. Original frame is lost
 2. ACK is lost
 3. ACK arrives after the timeout



Advantage of Stop-and-wait

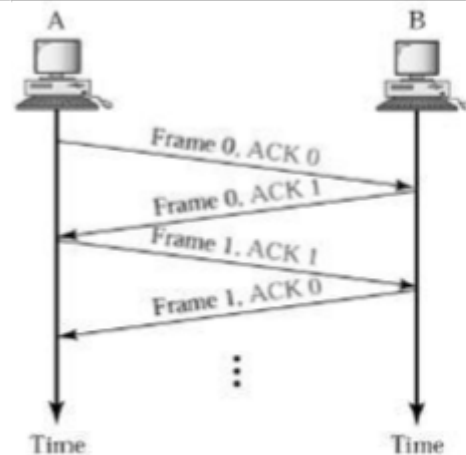
- o The Stop-and-wait method is simple as each frame is checked and acknowledged before the next frame is sent

Disadvantages of Stop-And-Wait

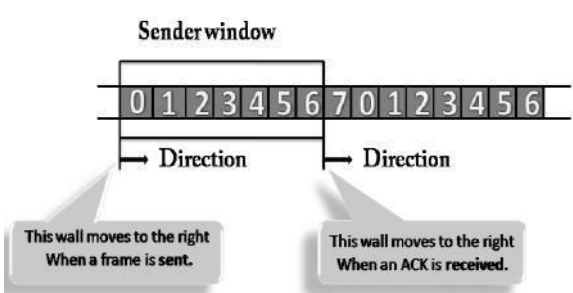
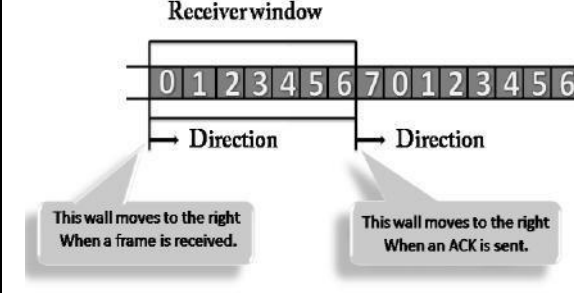
- o In stop-and-wait, at any point in time, there is only one frame that is sent and waiting to be acknowledged.
- o This is not a good use of transmission medium.
- o To improve efficiency, multiple frames should be in transition while waiting for ACK.

PIGGYBACKING

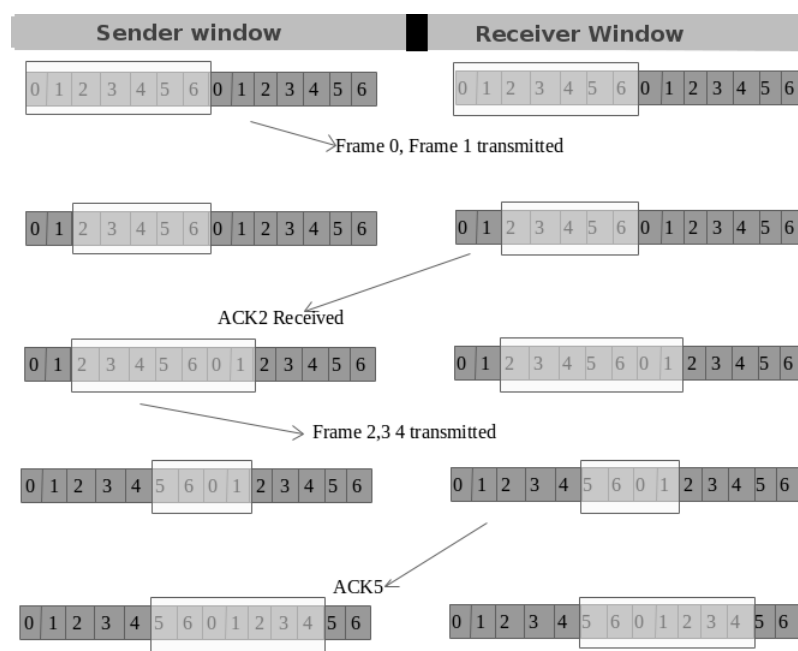
- A method to combine a data frame with ACK.
- Piggybacking saves bandwidth
- Station A and B both have data to send.
- Instead of sending separately, station A sends a data frame that includes an ACK.
- Station B does the same thing.

**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	Receiver Window
	
<ul style="list-style-type: none"> o At the beginning of a transmission, the sender window contains n-1 frames. o When a frame is sent, the size of the window shrinks. o For example, if the size of the window is 'w' and if three frames are sent out, then the number of frames left out in the sender window is w-3. o 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. 	<ul style="list-style-type: none"> o At the beginning of transmission, the receiver window does not contain n frames, but it contains n-1 spaces for frames. o When the new frame arrives, the size of the window shrinks. o For example, the size of the window is w and if three frames are received then the number of spaces available in the window is (w-3). o Once the acknowledgement is sent, the receiver window expands by the number equal to the number of frames acknowledged.

Example of Sliding Window



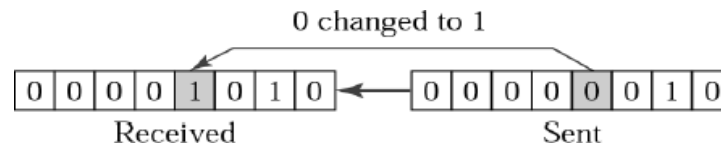
3. ERROR CONTROL

Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected. Error Control is a technique of error detection and retransmission.

TYPES OF ERRORS

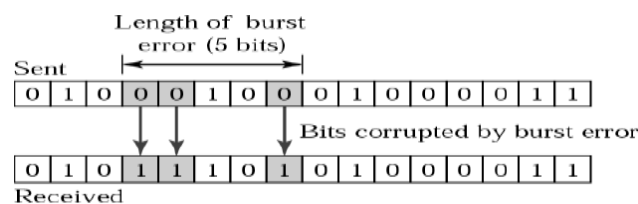
SINGLE-BIT ERROR

The term Single-bit error means that only one bit of a given data unit (such as byte, character, data unit or packet) is changed from 1 to 0 or from 0 to 1.



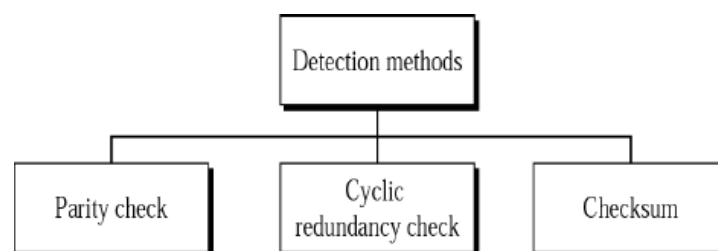
BURST ERROR

The term Burst Error means that two or more bits in the data unit have changed from 1 to 0 or from 0 to 1.



ERROR DETECTION TECHNIQUES / METHODS

The basic idea behind any error detection scheme is to add additional information to a frame that can be used to determine if errors have been introduced.



PARITY CHECK

- One bit, called parity bit is added to every data unit so that the total number of 1's in the data unit becomes even (or) odd.
- The source then transmits this data via a link, and bits are checked and verified at the destination.
- Data is considered accurate if the number of bits (even or odd) matches the number transmitted from the source.
- This techniques is the most common and least complex method.

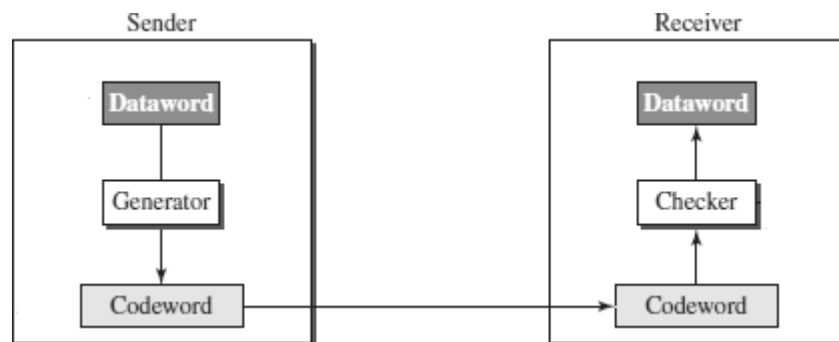
1. **Even parity** – Maintain even number of 1s E.g., 1011 → 1011 1
2. **Odd parity** – Maintain odd number of 1s E.g., 1011 → 1011 0

CYCLIC REDUNDANCY CHECK

- Cyclic codes refers to encoding messages by adding a fixed-length check value.
- CRCs are popular because they are simple to implement, easy to analyze mathematically and particularly good at detecting common errors caused in transmission channels.

Steps Involved :

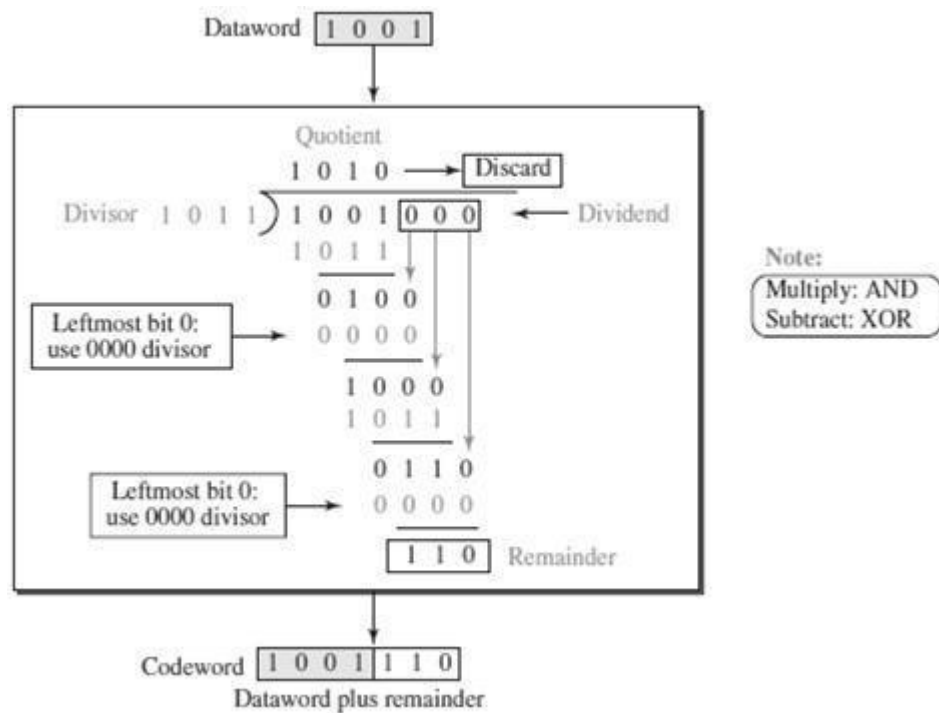
- Consider the original message (dataword) as $M(x)$ consisting of 'k' bits and the divisor as $C(x)$ consists of 'n+1' bits.
- The original message $M(x)$ is appended by 'n' bits of zero's. Let us call this zero-extended message as $T(x)$.
- Divide $T(x)$ by $C(x)$ and find the remainder.
- The division operation is performed using XOR operation.
- The resultant remainder is appended to the original message $M(x)$ as CRC and sent by the sender(codeword).



Example 1:

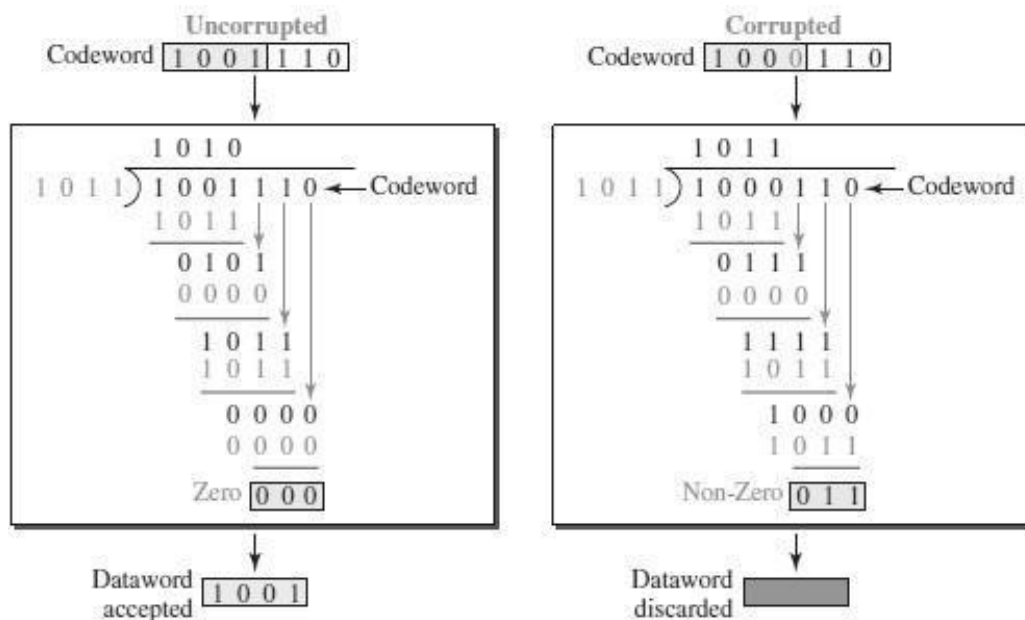
- Consider the Dataword / Message $M(x) = 1001$
- Divisor $C(x) = 1011$ ($n+1=4$)
- Appending 'n' zeros to the original Message $M(x)$.
- The resultant messages is called $T(x) = 1001$ **000**. (here $n=3$)
- Divide $T(x)$ by the divisor $C(x)$ using XOR operation.

Sender Side :



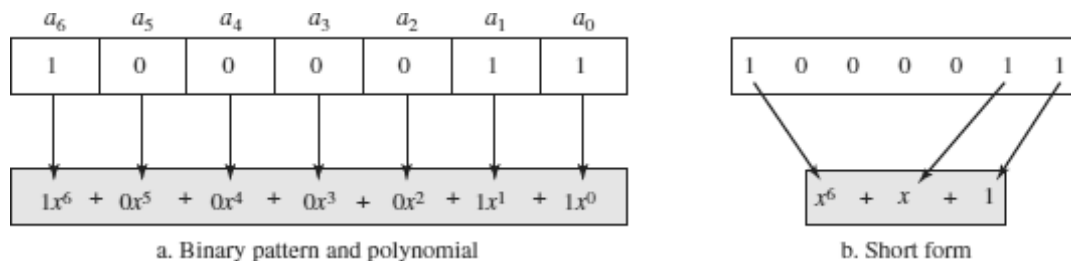
Receiver Side:

(For Both Case – Without Error and With Error)



Polynomials

- A pattern of 0s and 1s can be represented as a **polynomial** with coefficients of 0 and 1.
- The power of each term shows the position of the bit; the coefficient shows the value of the bit.

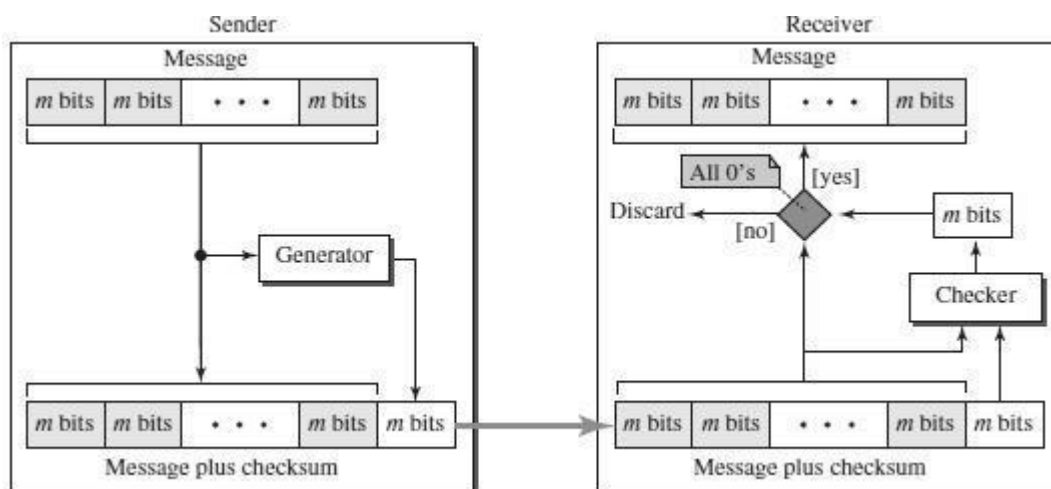


INTERNET CHECKSUM

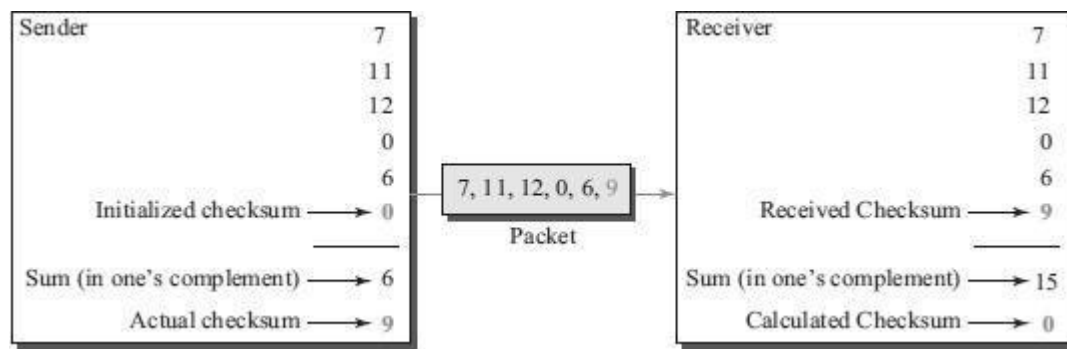
- Checksum is a calculated value that is used to determine the integrity of data.

Procedure to calculate the traditional checksum

Sender	Receiver
<ol style="list-style-type: none"> 1. The message is divided into 16-bit words. 2. The value of the checksum word is initially set to zero. 3. All words including the checksum are added using one's complement addition. 4. The sum is complemented and becomes the checksum. 5. The checksum is sent with the data. 	<ol style="list-style-type: none"> 1. The message and the checksum are received. 2. The message is divided into 16-bit words. 3. All words are added using one's complement addition. 4. The sum is complemented and becomes the new checksum. 5. If the value of the checksum is 0, the message is accepted; otherwise, it is rejected.



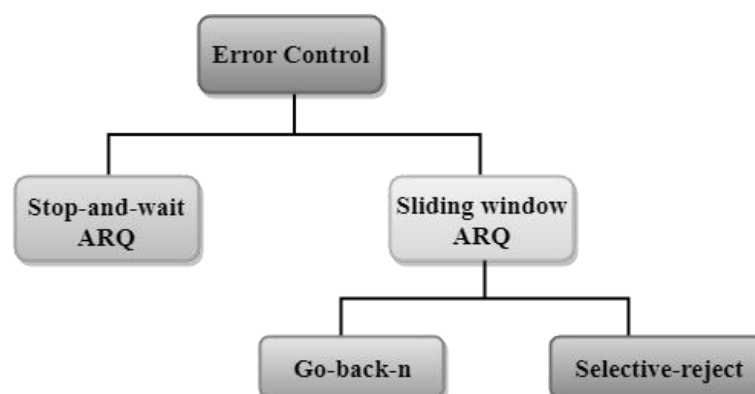
Example : Let the message to be transmitted be 7,11,12,0,6.



ERROR CONTROL

- Error control includes both error detection and error correction.
- Whenever an error is detected, specified frames are retransmitted
- It allows the receiver to inform the sender if a frame is lost or damaged during transmission and coordinates the retransmission of those frames by the sender.
- Includes the following actions:
 - **Error detection**
 - Positive Acknowledgement (**ACK**): if the frame arrived with no errors
 - Negative Acknowledgement (**NAK**): if the frame arrived with errors
 - Retransmissions after **Timeout**: Frame is retransmitted after certain amount of time if no acknowledgement was received
- Error control in the data link layer is based on automatic repeat request (ARQ).

Categories of Error Control

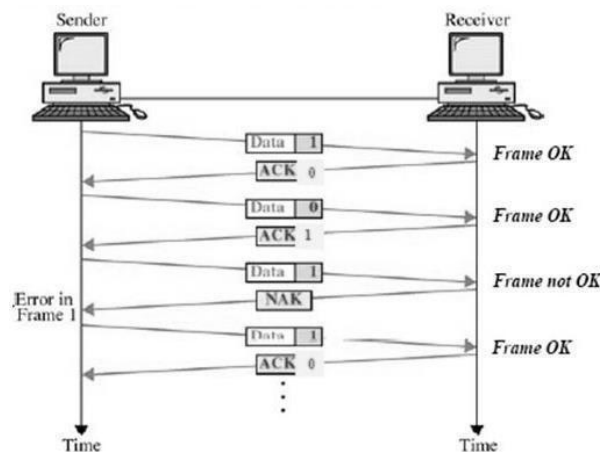


STOP-AND-WAIT ARQ

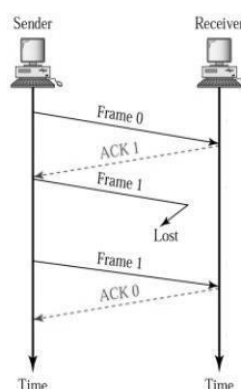
- Stop-and-wait ARQ is a technique used to retransmit the data in case of damaged or lost frames.
- This technique works on the principle that the sender will not transmit the next frame until it receives the acknowledgement of the last transmitted frame.

Two possibilities of the retransmission in Stop and Wait ARQ:

- o **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 frame DATA 1 is sent, and then the receiver sends the ACK 0 frame means that the data 1 has arrived correctly. The sender transmits the next frame: DATA 0. It reaches undamaged, and the receiver returns ACK 1. The sender transmits the third frame: DATA 1. The receiver reports an error and returns the NAK frame. The sender retransmits the DATA 1 frame.



- o **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 cannot be acknowledged either positively or negatively. The sender waits for acknowledgement until the timer goes off. If the timer goes off, it retransmits the last transmitted frame.



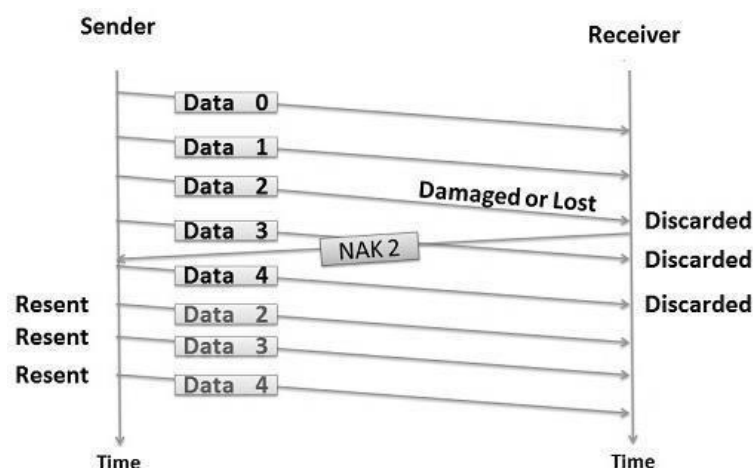
SLIDING WINDOW ARQ

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

Two protocols used in sliding window ARQ:

1. GO-BACK-N ARQ

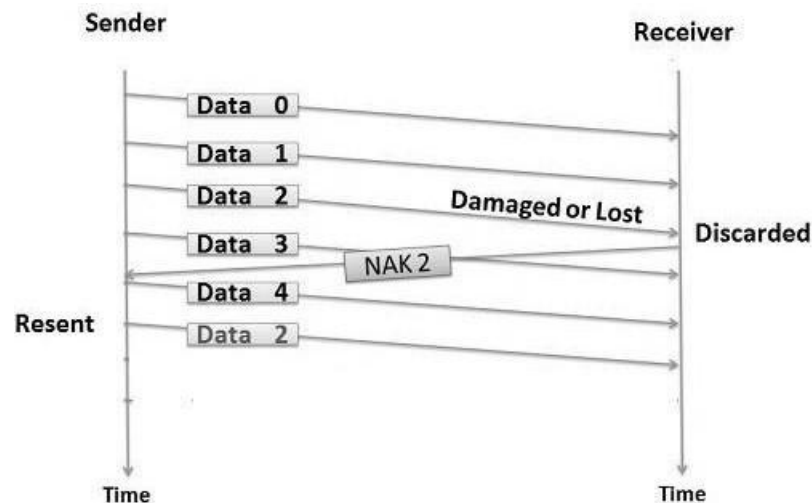
- o In Go-Back-N ARQ protocol, if one frame is lost or damaged, then it retransmits all the frames after which it does not receive the positive ACK.



- o In the above figure, three frames (Data 0,1,2) have been transmitted before an error discovered in the third frame.
- o The receiver discovers the error in Data 2 frame, so it returns the NAK 2 frame.
- o All the frames including the damaged frame (Data 2,3,4) are discarded as it is transmitted after the damaged frame.
- o Therefore, the sender retransmits the frames (Data2,3,4).

2. SELECTIVE-REJECT(REPEAT) ARQ

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



- o In the above figure, three frames (Data 0,1,2) have been transmitted before an error discovered in the third frame.
- o The receiver discovers the error in Data 2 frame, so it returns the NAK 2 frame.
- o The damaged frame only (Data 2) is discarded.
- o The other subsequent frames (Data 3,4) are accepted.
- o Therefore, the sender retransmits only the damaged frame (Data2).

4. DATA-LINK LAYER PROTOCOLS

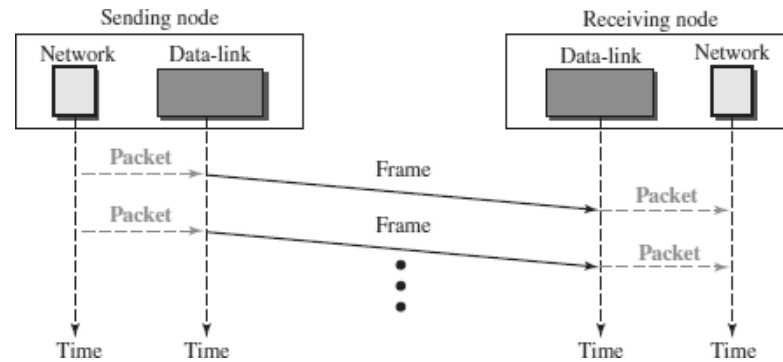
Four protocols have been defined for the data-link layer controls.

They are

1. Simple Protocol
2. Stop-and-Wait Protocol
3. Go-Back-N Protocol
4. Selective-Repeat Protocol

1.SIMPLE PROTOCOL

- o The first protocol is a simple protocol with neither flow nor error control.
- o We assume that the receiver can immediately handle any frame it receives.
- o In other words, the receiver can never be overwhelmed with incoming frames.
- o The data-link layers of the sender and receiver provide transmission services for their network layers.



- o The data-link layer at the sender gets a packet from its network layer, makes a frame out of it, and sends the frame.
- o 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.

NOTE :**· STOP-AND-WAIT PROTOCOL**

REFER STOP AND WAIT FROM FLOW CONTROL

· GO-BACK-N PROTOCOL

REFER GO-BACK-N ARQ FROM ERROR CONTROL

· SELECTIVE-REPEAT PROTOCOL

REFER SELECTIVE-REPEAT ARQ FROM ERROR CONTROL

5. HDLC (HIGH-LEVEL DATA LINK CONTROL)

- o High-level Data Link Control (HDLC) is a bit-oriented protocol
- o HDLC is used for communication over point-to-point and multipoint links.
- o HDLC implements the Stop-and-Wait protocol.

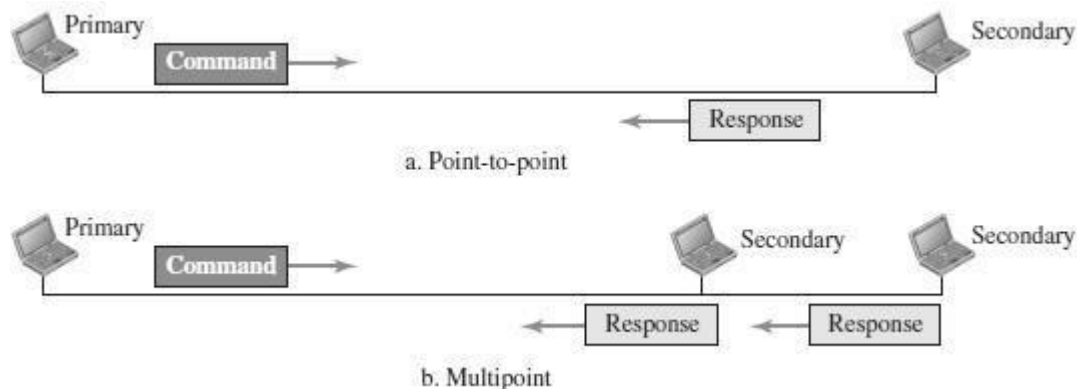
HDLC CONFIGURATIONS AND TRANSFER MODES

HDLC provides two common transfer modes that can be used in different configurations:

1. Normal response mode (NRM)
2. Asynchronous balanced mode (ABM).

Normal response mode (NRM)

- o In normal response mode (NRM), the station configuration is unbalanced.
- o We have one primary station and multiple secondary stations.
- o A *primary station* can send commands; a *secondary station* can only respond.
- o The NRM is used for both point-to-point and multipoint links.

**Asynchronous balanced mode (ABM)**

- o In ABM, the configuration is balanced.
- o The link is point-to-point, and each station can function as a primary and a secondary (acting as peers).
- o This is the common mode today.

**HDLC FRAMES**

HDLC defines three types of frames:

1. Information frames (I-frames) - used to carry user data
2. Supervisory frames (S-frames) - used to carry control information
3. Unnumbered frames (U-frames) – reserved for system management

Each type of frame serves as an envelope for the transmission of a different type of message.

Each frame in HDLC may contain up to six fields:

1. Beginning flag field
2. Address field
3. Control field
4. Information field (User Information/ Management Information)
5. Frame check sequence (FCS) field
6. Ending flag field

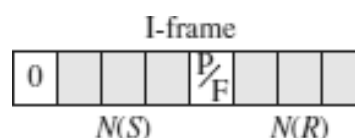
In multiple-frame transmissions, the ending flag of one frame can serve as the beginning flag of the next frame.

I – FrameS – FrameU – Frame

- o **Flag field** - This field contains synchronization pattern 01111110, which identifies both the beginning and the end of a frame.
- o **Address field** - This field contains the address of the secondary station. If a primary station created the frame, it contains a 'to' address. If a secondary station creates the frame, it contains a 'from' address. The address field can be one byte or several bytes long, depending on the needs of the network.
- o **Control field**. The control field is one or two bytes used for flow and error control.
- o **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.
- o **FCS field**. The frame check sequence (FCS) is the HDLC error detection field. It can contain either a 16- bit or 32-bit CRC.

CONTROL FIELD FORMAT FOR THE DIFFERENT FRAME TYPESControl Field for I-Frames

- o I-frames are designed to carry user data from the network layer. In addition, they can include flow-control and error-control information

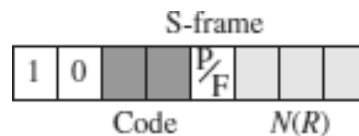


- o The first bit defines the type. If the first bit of the control field is 0, this means the frame is an I-frame.
- o The next 3 bits, called $N(S)$, define the sequence number of the frame.
- o The last 3 bits, called $N(R)$, correspond to the acknowledgment number when piggybacking is used.
- o The single bit between $N(S)$ and $N(R)$ is called the P/F bit. If this bit is 1 it means poll (the frame is sent by a primary station to a secondary).

- o If this bit is 0 it means final(the frame is sent by a secondary to a Primary).

Control Field for S-Frames

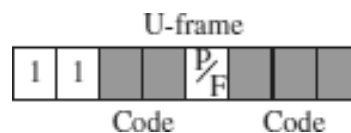
- o Supervisory frames are used for flow and error control whenever piggybacking is either impossible or inappropriate.
- o S-frames do not have information fields



- o If the first 2 bits of the control field are 10, this means the frame is an S-frame.
- o 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.
- o The 2 bits called code are used to define the type of S-frame itself.
- o With 2 bits, we can have four types of S-frames –
Receive ready (RR), Receive not ready (RNR), Reject (REJ) and Selective reject (SREJ).

Control Field for U-Frames

- o Unnumbered frames are used to exchange session management and control information between connected devices.
- o U-frames contain an information field, but used only for system management information and not user data.



- o If the first 2 bits of the control field are 11, this means the frame is an U-frame.
 - o U-frame codes are divided into two sections: a 2-bit prefix before the P/F bit and a 3-bit suffix after the P/F bit.
 - o Together, these two segments (5 bits) can be used to create up to 32 different types of U-frames.
-

6. POINT-TO-POINT PROTOCOL (PPP)

- o Point-to-Point Protocol (PPP) was devised by IETF (Internet Engineering Task Force) in 1990 as a Serial Line Internet Protocol (SLIP).
- o PPP is a data link layer communications protocol used to establish a direct connection between two nodes.
- o It connects two routers directly without any host or any other networking device in between.
- o It is used to connect the Home PC to the server of ISP via a modem.
- o It is a byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds.
- o Since it is a data link layer protocol, data is transmitted in frames. It is also known as RFC 1661.

Services Provided by PPP

The main services provided by Point - to - Point Protocol are –

1. Defining the frame format of the data to be transmitted.
2. Defining the procedure of establishing link between two points and exchange of data.
3. Stating the method of encapsulation of network layer data in the frame.
4. Stating authentication rules of the communicating devices.
5. Providing address for network communication.
6. Providing connections over multiple links.
7. Supporting a variety of network layer protocols by providing a range of services.

PPP Frame

PPP is a byte - oriented protocol where each field of the frame is composed of one or more bytes.



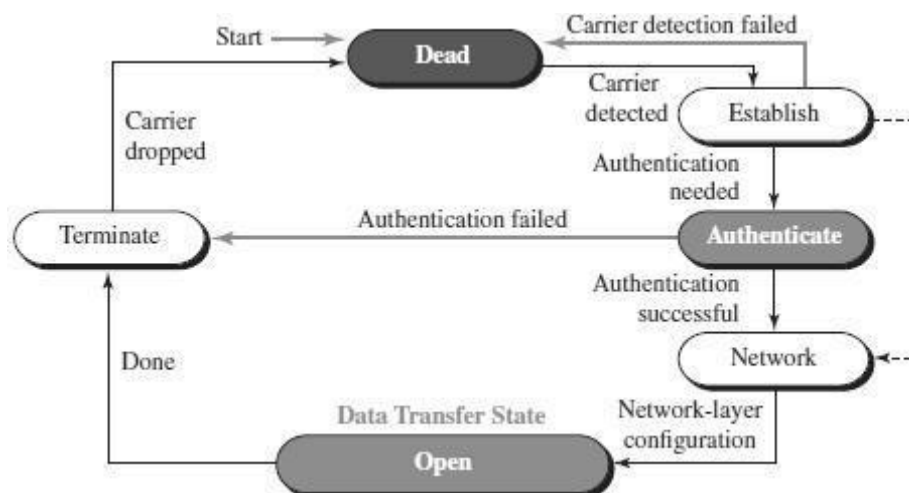
1. **Flag** – 1 byte that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
2. **Address** – 1 byte which is set to 11111111 in case of broadcast.
3. **Control** – 1 byte set to a constant value of 11000000.
4. **Protocol** – 1 or 2 bytes that define the type of data contained in the payload field.
5. **Payload** – This carries the data from the network layer. The maximum length of the payload field is 1500 bytes.
6. **FCS** – It is a 2 byte(16-bit) or 4 bytes(32-bit) frame check sequence for error detection. The standard code used is CRC.

Byte Stuffing in PPP Frame

Byte stuffing is used in PPP payload field whenever the flag sequence appears in the message, so that the receiver does not consider it as the end of the frame. The escape byte, 01111101, is stuffed before every byte that contains the same byte as the flag byte or the escape byte. The receiver on receiving the message removes the escape byte before passing it onto the network layer.

Transition Phases in PPP

The PPP connection goes through different states as shown in a *transition phase* diagram.



- ❖ **Dead:** In dead phase the link is not used. There is no active carrier and the line is quiet.
- ❖ **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.
- ❖ **Authenticate:** This phase is optional. The two nodes may decide whether they need this phase during the establishment phase. 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.
- ❖ **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.
- ❖ **Open:** In this phase, data transfer takes place. The connection remains in this phase until one of the endpoints wants to end the connection.
- ❖ **Terminate:** In this phase connection is terminated.

Components/Protocols of PPP

Three sets of components/protocols are defined to make PPP powerful:

- ❖ Link Control Protocol (LCP)
- ❖ Authentication Protocols (AP)
- ❖ Network Control Protocols (NCP)

Link Control Protocol (LCP) – It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also provides negotiation mechanisms to set options between the two endpoints. Both endpoints of the link must reach an agreement about the options before the link can be established.

Authentication Protocols (AP) – 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.
- 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.

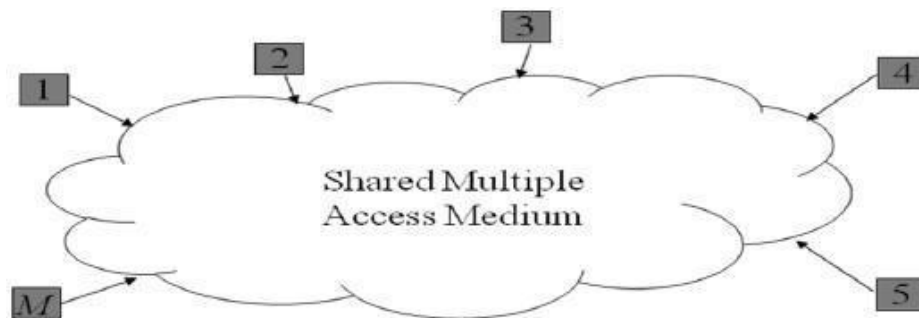
CHAP is more secure than PAP, especially if the system continuously changes the challenge value. Even if the intruder learns the challenge value and the result, the password is still secret.

Network Control Protocols (NCP) – PPP is a multiple-network-layer protocol. It can carry a network-layer data packet from protocols defined by the Internet. PPP

has defined a specific Network Control Protocol for each network protocol. These protocols are used for negotiating the parameters and facilities for the network layer. For every higher-layer protocol supported by PPP, one NCP is there.

7. MEDIA ACCESS CONTROL (MAC)

- When two or more nodes transmit data at the same time, their frames will collide and the link bandwidth is wasted during collision.
- To coordinate the access of multiple sending/receiving nodes to the shared link, we need a protocol to coordinate the transmission.
- These protocols are called Medium or Multiple Access Control (MAC) Protocols. MAC belongs to the data link layer of OSI model
- MAC defines rules for orderly access to the shared medium. It tries to ensure that no two nodes are interfering with each other's transmissions, and deals with the situation when they do.



Issues involved in MAC

The key issues involved are –

- **Where** the control is exercised - refers to whether the control is exercised in a centralized or distributed manner
- **How** the control is exercised - refers to in what manner the control is exercised

Goals of MAC

1. Fairness in sharing
2. Efficient sharing of bandwidth
3. Need to avoid packet collisions at the receiver due to interference

MAC Management

- Medium allocation (collision avoidance)
- Contention resolution (collision handling)

MAC Types

- **Round-Robin** : – Each station is given opportunity to transmit in turns. Either a central controller polls a station to permit to go, or stations can coordinate among themselves.
- **Reservation** : - Station wishing to transmit makes reservations for time slots in advance. (Centralized or distributed).
- **Contention (Random Access)** : - No control on who tries; If collision occurs, retransmission takes place.

MECHANISMS USED

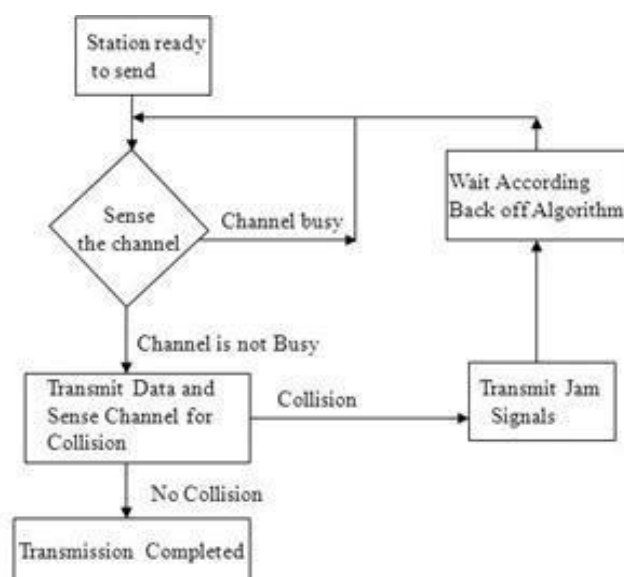
- Wired Networks :
 - CSMA / CD – Carrier Sense Multiple Access / Collision Detection
- Wireless Networks :
 - CSMA / CA – Carrier Sense Multiple Access / Collision Avoidance

CARRIER SENSE MULTIPLE ACCESS / COLLISION DETECTION (CSMA / CD)

Carrier Sense in CSMA/CD means that all the nodes sense the medium to check whether it is idle or busy.

- If the carrier sensed is idle, then the node transmits the entire frame.
- If the carrier sensed is busy, the transmission is postponed.

Collision Detect means that a node listens as it transmits and can therefore detect when a frame it is transmitting has collided with a frame transmitted by another node.

Flowchart of CSMA/CD Operation

Transmitter Algorithm in CSMA/CD

Transmitter Algorithm defines the procedures for a node that senses a busy medium.

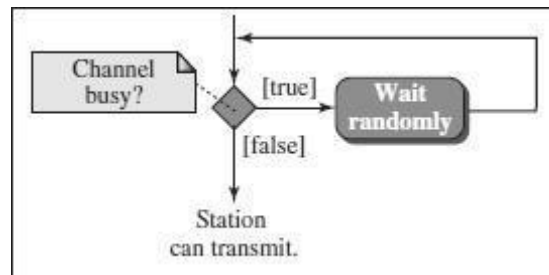
Three types of Transmitter Algorithm exist.

They are

1. Non-Persistent Strategy
2. Persistent Strategy : 1-Persistent & P-Persistent

Non-Persistent Strategy

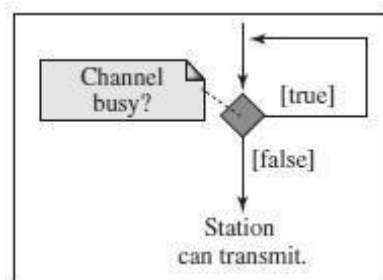
- In the non-persistent method, a station that has a frame to send senses the line.
- If the line is idle, it sends immediately.
- If the line is not idle, it waits a random amount of time and then senses the line again.



- The non-persistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.
- However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

Persistent Strategy**1-Persistent :**

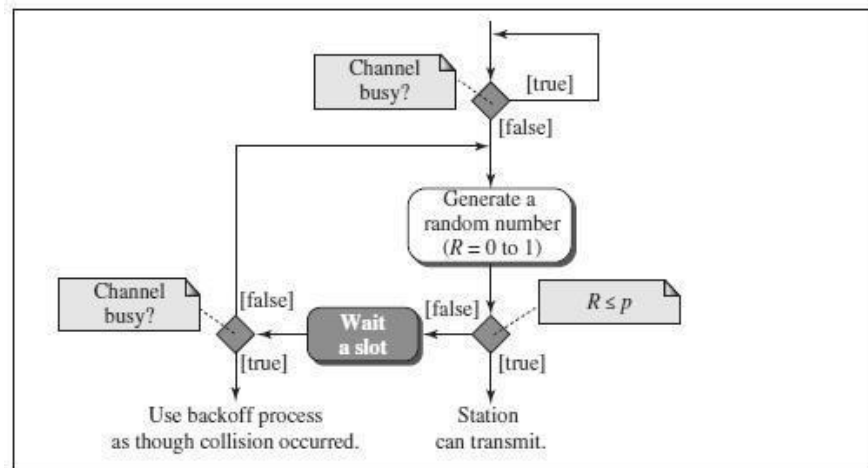
- The 1-persistent method is simple and straightforward.
- In this method, after the station finds the line idle, it sends its frame immediately (with probability 1).



- This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

P-Persistent :

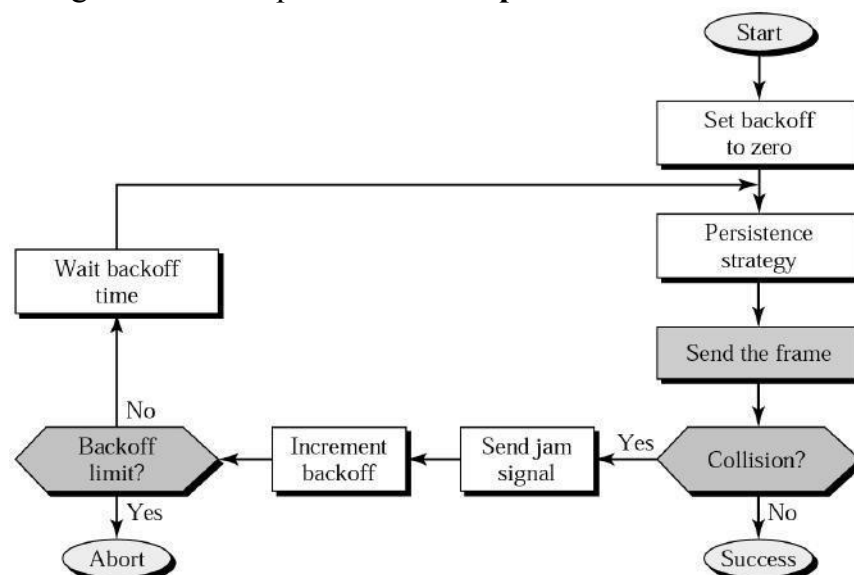
- In this method, after the station finds the line idle it follows these steps:
- With probability p , the station sends its frame.
- With probability $q = 1 - p$, the station waits for the beginning of the next time slot and checks the line again.



- The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time.
- The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency.

EXPONENTIAL BACK-OFF

- Once an adaptor has detected a collision and stopped its transmission, it waits a certain amount of time and tries again.
- Each time it tries to transmit but fails, the adaptor doubles the amount of time it waits before trying again.
- This strategy of doubling the delay interval between each retransmission attempt is a general technique known as **exponential back-off**.



CARRIER SENSE MULTIPLE ACCESS / COLLISION AVOIDANCE (CSMA/CA)

- Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for wireless networks.
- Wireless protocol would follow exactly the same algorithm as the Ethernet—Wait until the link becomes idle before transmitting and back off should a collision occur.
- Collisions are avoided through the use of CSMA/CA's three strategies: the interframe space, the contention window, and acknowledgments

Interframe Space (IFS) - First, collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period of time called the *interframe space* or *IFS*.

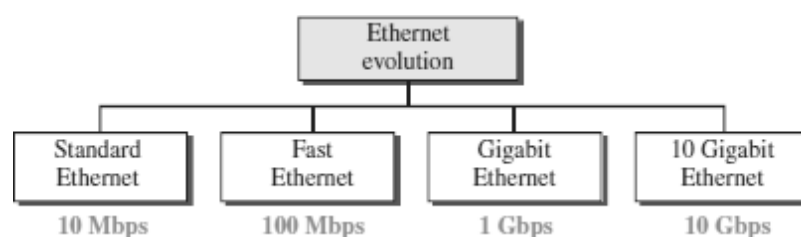
Contention Window - The **contention window** is an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time. The number of slots in the window changes according to the binary exponential backoff strategy. This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.

Acknowledgment - In addition, the data may be corrupted during the transmission. The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.

8. WIRED LAN : ETHERNET (IEEE 802.3)

- Ethernet was developed in the mid-1970's at the Xerox Palo Alto Research Center (PARC),
- IEEE controls the Ethernet standards.
- The Ethernet is the most successful local area networking technology, that uses bus topology.
- The Ethernet is **multiple-access networks** that is set of nodes send and receive frames over a shared link.
- Ethernet uses the **CSMA / CD** (Carrier Sense Multiple Access with Collision Detection) mechanism.

EVOLUTION OF ETHERNET

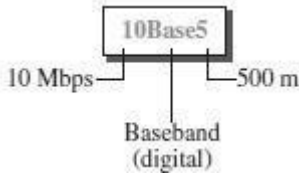
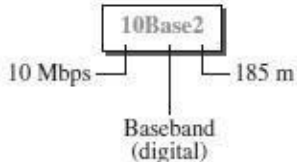
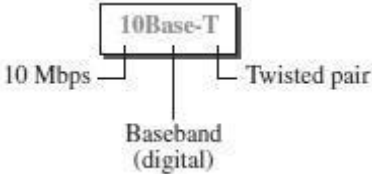
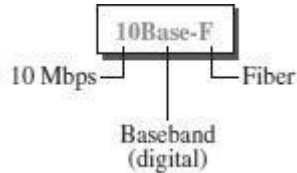


Standard Ethernet (10 Mbps)

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

Standard Ethernet types are

1. 10Base5: Thick Ethernet,
2. 10Base2: Thin Ethernet ,
3. 10Base-T: Twisted-Pair Ethernet
4. 10Base-F: Fiber Ethernet.

<p><u>10Base5: Thick Ethernet</u></p>  <ul style="list-style-type: none"> • 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. 	<p><u>10Base2: Thin Ethernet</u></p>  <ul style="list-style-type: none"> • 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. • In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.
<p><u>10Base-T: Twisted-Pair Ethernet</u></p>  <ul style="list-style-type: none"> • 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. 	<p><u>10Base-F: Fiber Ethernet</u></p>  <ul style="list-style-type: none"> • 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.

Fast Ethernet (100 Mbps)

Fast Ethernet or 100BASE-T provides transmission speeds up to 100 megabits per second and is typically used for LAN backbone systems.

The 100BASE-T standard consists of three different component specifications –

1. 100 BASE-TX
2. 100BASE-T4
3. 100BASE-FX

<u>100 BASE-TX</u>	<u>100BASE-T4</u>	<u>100BASE-FX</u>
100Base-TX uses two pairs of twisted-pair cable either UTP or STP. A 100Base-TX network can provide a data rate of 100 Mbps.	A new standard, called 100Base-T4 , was designed to use four pairs of UTP for transmitting 100 Mbps.	100Base-FX uses two pairs of fiber-optic cables. Optical fiber can easily handle high bandwidth requirements.

Gigabit Ethernet (1 Gbps)

- The Gigabit Ethernet upgrades the data rate to 1 Gbps(1000 Mbps).
- Gigabit Ethernet can be categorized as either a two-wire or a four-wire implementation.
- The two-wire implementations use fiber-optic cable (**1000Base-SX**, short-wave, or **1000Base-LX**, long-wave), or STP (**1000Base-CX**).
- The four-wire version uses category 5 twisted-pair cable (**1000Base-T**).

10 Gigabit Ethernet(10 Gbps)

10 Gigabit Ethernet is an upcoming Ethernet technology that transmits at 10 Gbps.

10 Gigabit Ethernet enables a familiar network technology to be used in LAN, MAN and WAN architectures.

10 Gigabit Ethernet uses multimode optical fiber up to 300 meters and single mode fiber up to 40 kilometers.

Four implementations are the most common: **10GBase-SR**, **10GBase-LR**, **10GBase-EW**, and **10GBase-X4**.

ACCESS METHOD/ PROTOCOL OF ETHERNET

The access method of Ethernet is CSMA/CD.

Note : Refer CSMA/CD from MAC

COLLISION DETECTION IN ETHERNET

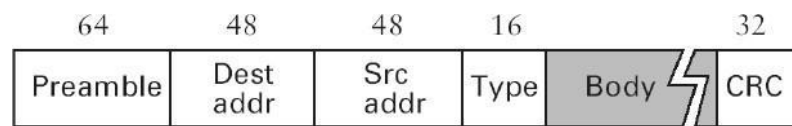
As the Ethernet supports collision detection, senders are able to determine a collision.

At the moment an adaptor detects that its frame is colliding with another, it first makes sure to transmit a **32-bit jamming sequence** along with the **64-bit preamble** (totally 96 bits) and then stops the transmission.

These **96 bits** are sometimes called **Runt Frame**.

FRAME FORMAT OF ETHERNET

The Ethernet frame is defined by the format given in the Fig.



The 64-bit **preamble** allows the receiver to synchronize with the signal; it is a sequence of alternating 0's and 1's.

Both the **source and destination** hosts are identified with a 48-bit **address**.

The packet **type** field serves as the demultiplexing key.

Each frame contains up to 1500 bytes of **data(Body)**.

CRC is used for Error detection

Ethernet Addresses

Every Ethernet host has a unique Ethernet address (48 bits – 6 bytes).

Ethernet address is represented by sequence of six numbers separated by colons.

Each number corresponds to 1 byte of the 6 byte address and is given by pair of hexadecimal digits.

Eg: 8:0:2b:e4:b1:2 is the representation of

00001000 00000000 00101011 11100100 10110001 00000010

Each frame transmitted on an Ethernet is received by every adaptor connected to the Ethernet.

In addition to **unicast** addresses an Ethernet address consisting of **all 1s** is treated as **broadcast** address.

Similarly the address that has the **first bit set to 1** but it is not the broadcast address is called **multicast** address.

ADVANTAGES OF ETHERNET

Ethernets are successful because

It is extremely *easy to administer and maintain*. There are no switches that can fail, no routing or configuration tables that have to be kept up-to-date, and it is easy to add a new host to the network.

It is *inexpensive*: Cable is cheap, and the only other cost is the network adaptor on each host.

9. WIRELESS LAN (IEEE 802.11)

Wireless communication is one of the fastest-growing technologies.

The demand for connecting devices without the use of cables is increasing everywhere.

Wireless LANs can be found on college campuses, in office buildings, and in many public areas.

ADVANTAGES OF WLAN / 802.11

1. **Flexibility**: Within radio coverage, nodes can access each other as radio waves can penetrate even partition walls.
2. **Planning** : No prior planning is required for connectivity as long as devices follow standard convention
3. **Design** : Allows to design and develop mobile devices.
4. **Robustness** : Wireless network can survive disaster. If the devices survive, communication can still be established.

DISADVANTAGES OF WLAN / 802.11

1. **Quality of Service** : Low bandwidth (1 – 10 Mbps), higher error rates due to interference, delay due to error correction and detection.
2. **Cost** : Wireless LAN adapters are costly compared to wired adapters.
3. **Proprietary Solution** : Due to slow standardization process, many solution are proprietary that limit the homogeneity of operation.
4. **Restriction** : Individual countries have their own radio spectral policies. This restricts the development of the technology
5. **Safety and Security** : Wireless Radio waves may interfere with other devices. Eg; In a hospital, radio waves may interfere with high-tech equipment.

TECHNOLOGY USED IN WLAN / 802.11

WLAN's uses Spread Spectrum (SS) technology.

The idea behind Spread spectrum technique is to spread the signal over a wider frequency band than normal, so as to minimize the impact of interference from other devices.

There are two types of Spread Spectrum:

- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)

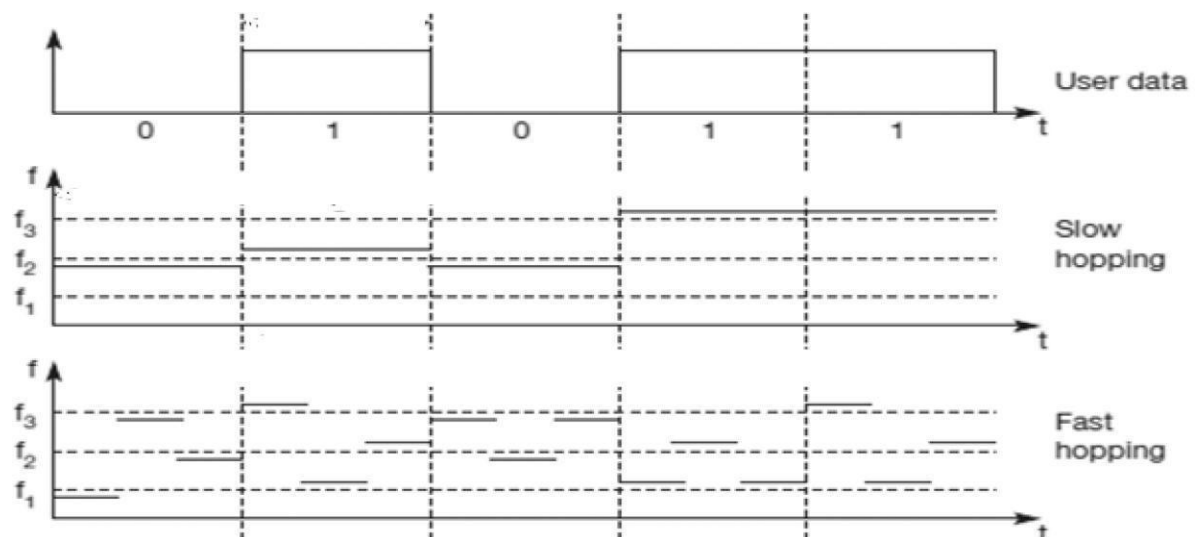
Frequency Hopping Spread Spectrum (FHSS)

Frequency hopping is a spread spectrum technique that involves transmitting the signal over a random sequence of frequencies.

That is, first transmitting at one frequency, then a second, then a third, and so on.

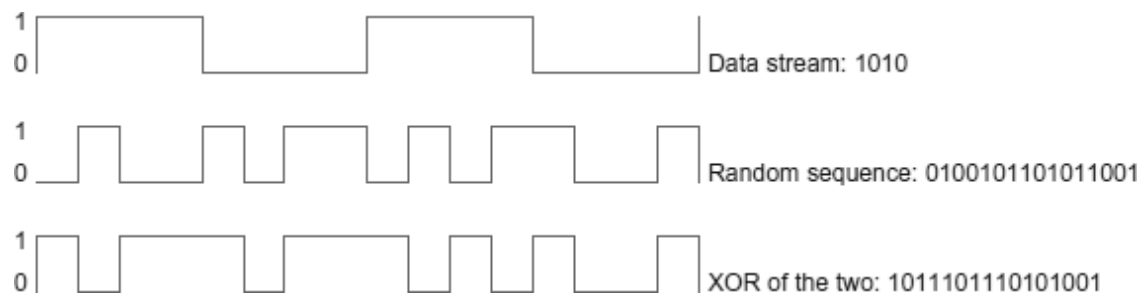
The random sequence of frequencies is computed by a pseudorandom number generator.

The receiver uses the same algorithm as the sender and initializes it with the same seed and hence is able to hop frequencies in sync with the transmitter to correctly receive the frame.

**Direct Sequence Spread Spectrum (DSSS)**

Each bit of data is represented by multiple bits in the transmitted signal. DSSS takes a user data stream and performs an XOR operation with a pseudo-random number.

This pseudo random number is called as *chipping sequence*.

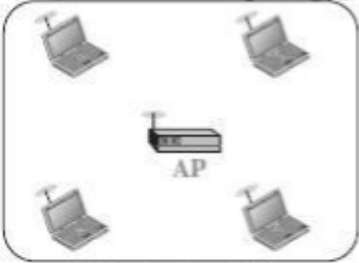



TOPOLOGY IN WLAN / 802.11

WLANs can be built with either of the following two topologies /architecture:

Infra-Structure Network Topology

Ad Hoc Network Topology

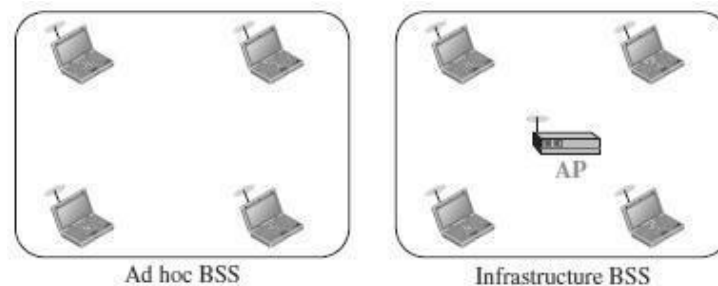
<u>Infra-Structure Topology</u>	<u>Ad-Hoc Topology</u>
<p data-bbox="389 1010 695 1046">(AP based Topology)</p>  <p data-bbox="427 1312 614 1339">Infrastructure BSS</p>	<p data-bbox="1011 976 1270 1012">Ad-Hoc Topology</p> <p data-bbox="963 1043 1318 1079">(Peer-to-Peer Topology)</p>  <p data-bbox="1082 1312 1204 1339">Ad hoc BSS</p>
<ul style="list-style-type: none"> • An infrastructure network is the network architecture for providing communication between wireless clients and wired network resources. • The transition of data from the wireless to wired medium occurs via a Base Station called AP(Access Point). • An AP and its associated wireless clients define the coverage area. 	<ul style="list-style-type: none"> • An adhoc network is the architecture that is used to support mutual communication between wireless clients. • Typically, an ad- hoc network is created spontaneously and does not support access to wired networks. • An adhoc network does not require an AP.

ARCHITECTURE OF WLAN / 802.11

- The standard defines two kinds of services: the Basic Service Set (BSS) and the Extended Service Set (ESS).

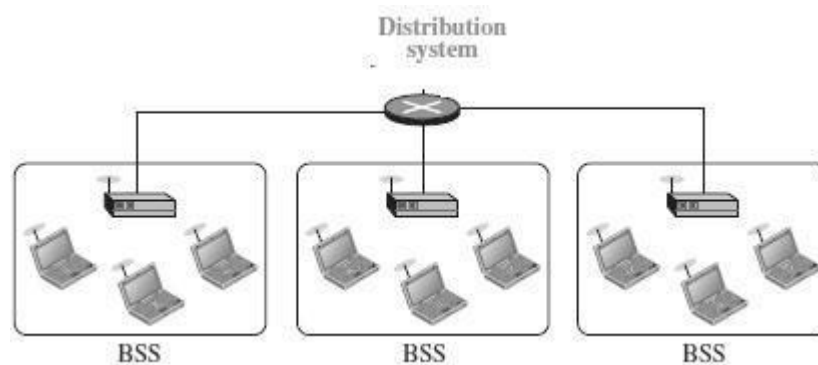
Basic Service Set (BSS)

- IEEE 802.11 defines the **basic service set (BSS)** as the building blocks 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)*.



Extended Service Set (ESS)

- An extended service set (ESS) is made up of two or more BSSs with APs.
- In this case, the BSSs are connected through a *distribution system*, which is a wired or a wireless network.
- The distribution system connects the APs in the BSSs. The extended service set uses two types of stations: mobile and stationary.
- The mobile stations are normal stations inside a BSS.
- The stationary stations are AP stations that are part of a wired LAN.



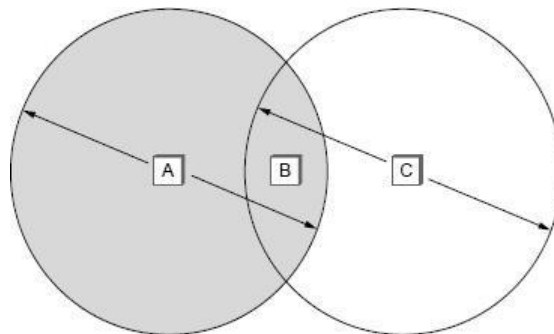
Station Types

IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN:

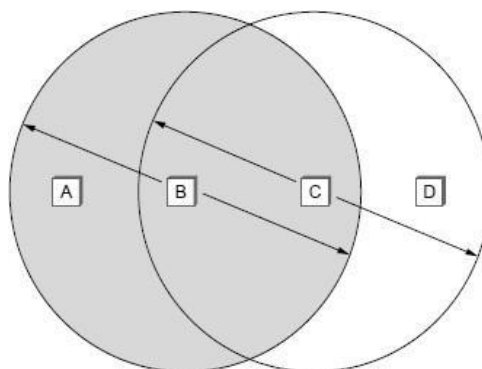
1. **No-transition** - A station with no-transition mobility is either stationary (not moving) or moving only inside a BSS.
2. **BSS-transition** - A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS
- ESS-transition** - A station with ESS-transition mobility can move from one ESS to another.

COLLISION AVOIDANCE IN WLAN / 802.11

Wireless protocol would follow exactly the same algorithm as the Ethernet—Wait until the link becomes idle before transmitting and back off should a collision occur.

Hidden Node Problem

- Consider the situation shown in the Figure.
- Here A and C are both within range of B but not with each other.
- Suppose both A and C want to communicate with B and so they each send a frame to B.
- A and C are unaware of each other since their signals do not carry that far.
- These two frames collide with each other at B, but neither A nor C is aware of this collision.
- A and C are said to be *hidden nodes* with respect to each other.

Exposed Node Problem

- Each of the four nodes is able to send and receive signals that reach just the nodes to its immediate left and right.
- For example, B can exchange frames with A and C but it cannot reach D, while C can reach B and D but not A.

- Suppose B is sending to A. Node C is aware of this communication because it hears B's transmission.
- If at the same time, C wants to transmit to node D.
- It would be a mistake, however, for C to conclude that it cannot transmit to anyone just because it can hear B's transmission.
- This is not a problem since C's transmission to D will not interfere with A's ability to receive from B.
- This is called exposed problem.
- Although B and C are exposed to each other's signals, there is no interference if B transmits to A while C transmits to D.

MULTIPLE ACCESS WITH COLLISION AVOIDANCE (MACA)

MACA is used to avoid collisions caused by the hidden terminal problem and exposed terminal problem.

MACA uses short **signaling packets** called **RTS** and **CTS** for collision avoidance.

The RTS and CTS signals helps us to determine who else is in the transmission range or who is busy.

When a sender wants to transmit, it sends a signal called **Request-To-Send (RTS)**.

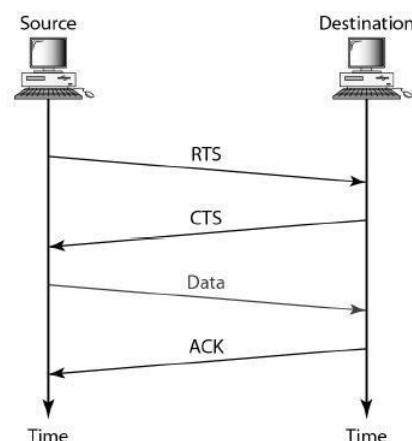
If the receiver allows the transmission, it replies to the sender a signal called **Clear-To-Send (CTS)**.

Any node that sees the CTS frame knows that it is close to the receiver, and therefore cannot transmit for the period of time.

Any node that sees the RTS frame but not the CTS frame is not close enough to the receiver to interfere with it, and so is free to transmit.

The Signaling packets RTS and CTS contains information such as

- ☐ sender address
- ☐ receiver address
- ☐ length of the data to be sent/received



The receiver sends an ACK to the sender after successfully receiving a frame.

All nodes must wait for this ACK before trying to transmit.

When two or more nodes detect an idle link and try to transmit an RTS frame at the same time, their RTS frames will collide with each other.

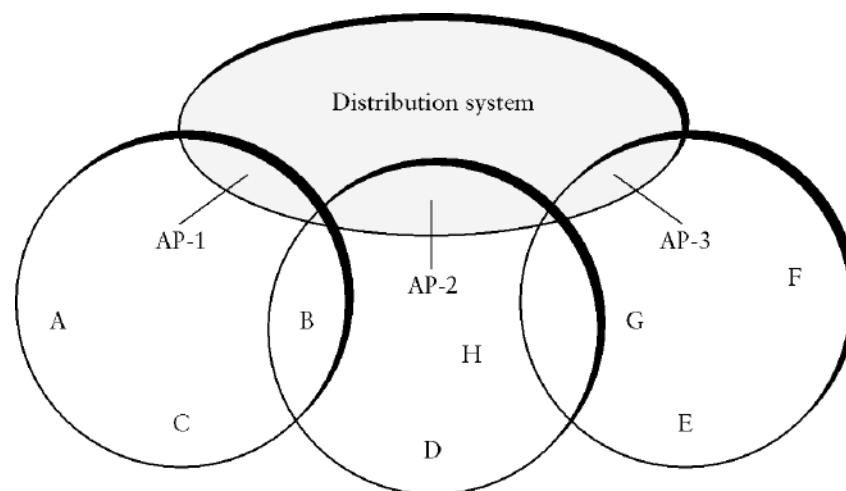
802.11 do not support collision detection, but instead, the senders realize the collision has happened when they do not receive the CTS frame after a period of time.

Each node waits for a random amount of time before trying again.

The amount of time a given node delays is defined by exponential back-off algorithm.

DISTRIBUTION SYSTEM IN WLAN / 802.11

In wireless network, nodes can move freely. Some nodes are allowed to roam and some are connected to a wired network infrastructure called **access points (AP)**, and they are connected to each other by a so-called **distribution system**.



Two nodes can communicate directly with each other if they are within reach of each other,

When the nodes are at different range, for example when node A wish to communicate with node E, A first sends a frame to its access point (AP-1), which forwards the frame across the distribution system to AP-3, which finally transmits the frame to E.

Scanning Process in Distribution System

- The *technique for selecting an Access Point* is called **scanning**.
- Scanning will take place whenever a node joins the network as well as when it is not satisfied with the current access point signal.
- It involves the following four steps:

The node sends a **Probe Request** frame.

All AP's within reach reply with a **Probe Response** frame.

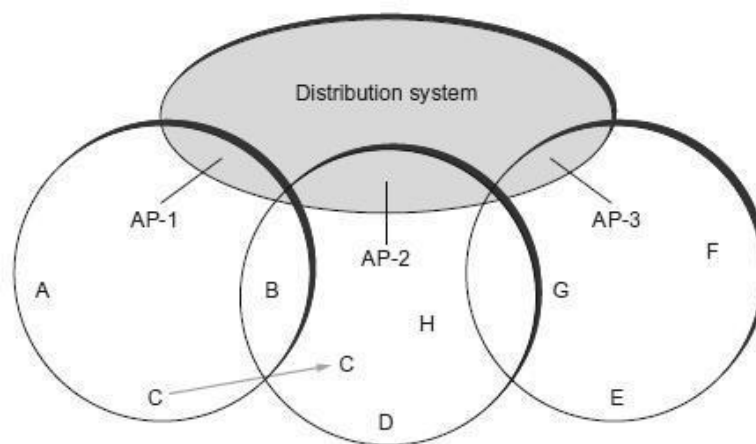
The node selects one of the access points and sends that AP an **Association Request** frame.

The AP replies with an **Association Response** frame.

- There are two types of Scanning. They are
 1. Active Scanning
 2. Passive Scanning

Active Scanning

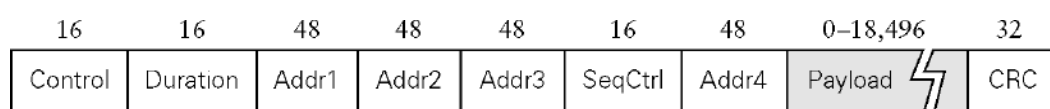
When node C moves from the cell serviced by AP-1 to the cell serviced by AP-2. As it moves, it sends Probe frames, which eventually result in Probe Response. Since the *node is actively searching for an access point* it is called active scanning.



Passive Scanning

AP's periodically send a Beacon frame to the nodes that advertises the capabilities of the access point which includes the transmission rates supported by the AP. This is called passive scanning and a node can change to this AP based on the Beacon frame simply by sending it an Association Request frame back to the access point.

FRAME FORMAT OF WLAN / 802.11



Control field - contains three subfields :

- **Type field** - Indicates whether the frame carries data, RTS or CTS frame
- **To DS** - Data frame sent to DS
- **From DS** - ACK sent from DS

When both the DS bits are set to 0, it indicates that one node is sending directly to another. Addr 1 identifies the target node and Addr2 identifies the source node.

When both the DS bits are set to 1, it indicates that one node is sending the message to another indirectly using the distribution system.

Duration - contains the duration of time the medium is occupied by the nodes.

Addr 1 - identifies the final original destination

Addr 2 - identifies the immediate sender (the one that forwarded the frame from the distribution system to the ultimate destination)

Addr 3 - identifies the intermediate destination (the one that accepted the frame from a wireless node and forwarded it across the distribution system)

Addr 4 - identifies the original source

Sequence Control - to avoid duplication of frames sequence number is assigned to each frame

Payload - Data from sender to receiver

CRC - used for Error detection of the frame.

10. BLUETOOTH (IEEE 802.15.1)

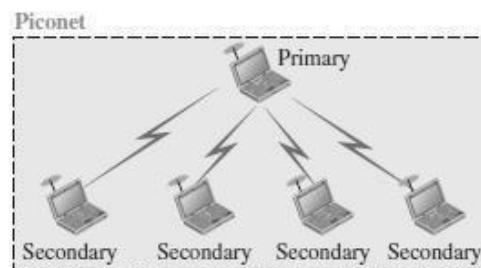
- A Bluetooth is an ad hoc network, which means that the network is formed spontaneously.
- Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, when they are at a short distance from each other.
- Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard.
- The standard defines a wireless personal-area network (PAN)
- Bluetooth operates in the 2.4 GHz Unlicensed ISM band.
- The range for Bluetooth communication is 0-30 feet (10 meters).
- This distance can be increased to 100 meters by amplifying the power.
- Bluetooth links have typical bandwidths around 1 to 3 Mbps.
- Bluetooth is specified by an industry consortium called the Bluetooth Special Interest Group.
- Upto eight devices can be connected through Bluetooth.
- One device will function as a Master and the other seven devices will function as slaves.
- Bluetooth uses Frequency Hopping Spread Spectrum (FHSS) to avoid any interference.
- Bluetooth supports two kinds of links:
 - Asynchronous Connectionless (ACL) links - for data
 - Synchronous Connection oriented (SCO) links - for audio/voice

BLUETOOTH ARCHITECTURE

Bluetooth defines two types of networks: Piconet and Scatternet.

PICONET

- The basic Bluetooth network configuration is called a Piconet
- A Piconet is a collection of eight bluetooth devices which are synchronized.
- One device in the piconet can act as **Primary (Master)**, all other devices connected to the master act as **Secondary (Slaves)**.
- All the secondary stations synchronize their clocks and hopping sequence with the primary.



- Any communication is between the primary/master and a secondary/slave.
- The communication between the primary and secondary stations can be one-to-one or one-to-many.
- The slaves do not communicate directly with each other.
- The devices in a piconet can be in any one of the three types/states.
- They are

□ Active Device / State

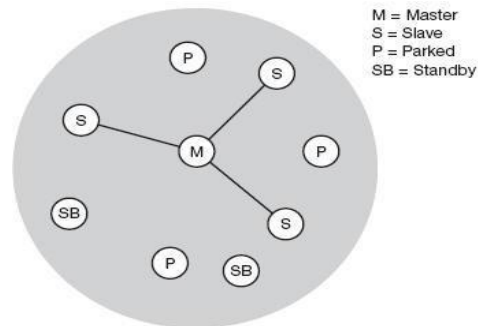
1. Connected to the piconet and participates in the communication.
2. Can be a Master or a Slave device.
3. All active devices are assigned a 3-bit address (AMA).

□ Parked Device / State

1. Connected to the piconet, but does not actively participate in the communication.
2. More than 200 devices can be parked.
3. All parked devices use an 8-bit parked member address (PMA).

□ Stand-by Device / State

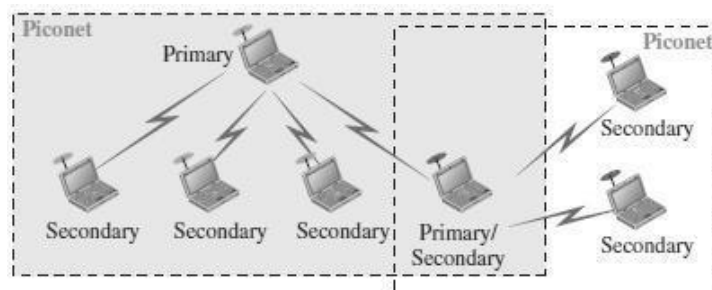
1. Not connected to the piconet.
2. They do not participate in the piconet currently but may take part at a later time.
3. Devices in stand-by do not need an address.



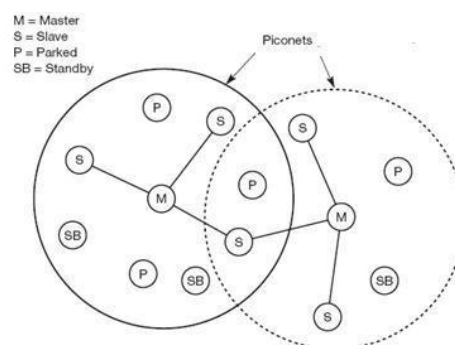
- If a parked device wants to communicate and there are already seven active slaves, one slave has to switch to park state to allow the parked device to switch to active state.

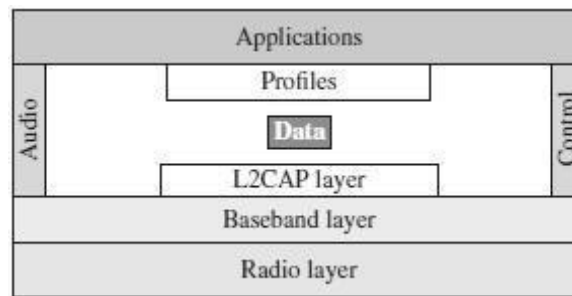
SCATTERNET

- Piconets can be combined to form what is called a **scatternet**.
- Many piconets with overlapping coverage can exist simultaneously, called 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.



- In the example given below, there are two piconets, in which one slave participates in two different piconets.
- Master of one piconet cannot act as the master of another piconet.
- But the Master of one piconet can act as a Slave in another piconet



BLUETOOTH LAYERS**Radio Layer**

- The radio layer is roughly equivalent to the physical layer of the Internet model.
- 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, which means that each device changes its modulation frequency 1600 times per second.
- To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK.

Baseband Layer

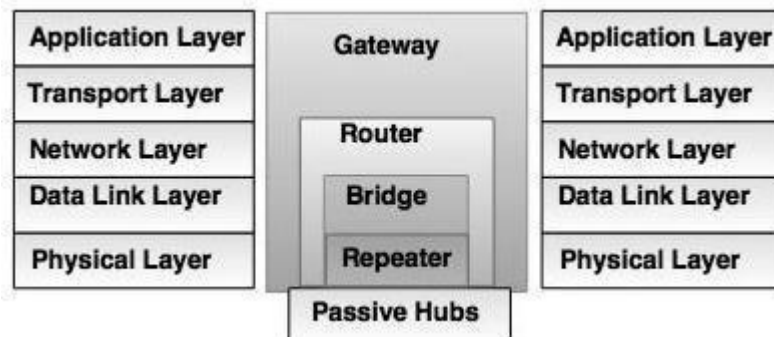
- The baseband layer is roughly equivalent to the MAC sublayer in LANs.
- The access method is TDMA.
- The primary and secondary stations communicate with each other using time slots. The length of a time slot is exactly 625 μ s.
- During that time, a primary sends a frame to a secondary, or a secondary sends a frame to the primary.

L2CAP

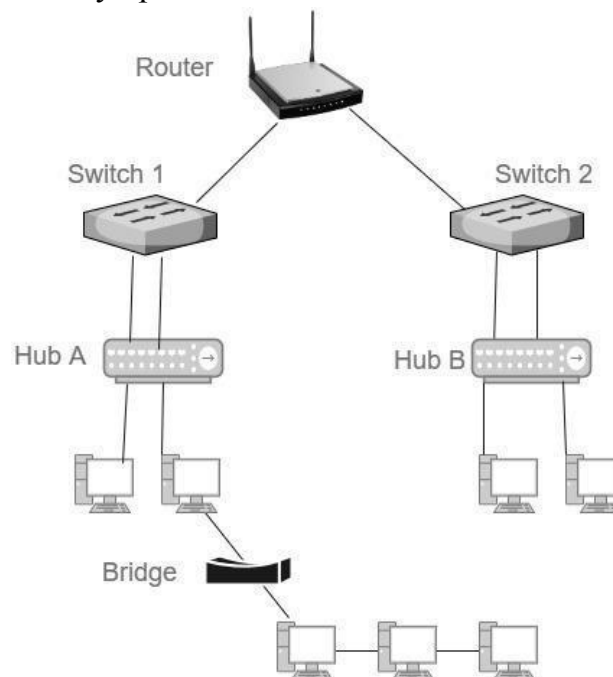
- The **Logical Link Control and Adaptation Protocol**, or **L2CAP** (L2 here means LL) is equivalent to the LLC sublayer in LANs.
 - It is used for data exchange on an ACL link.
 - SCO channels do not use L2CAP.
 - The L2CAP functions are : multiplexing, segmentation and reassembly, quality of service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

11. CONNECTING DEVICES

- Connecting devices are used to connect hosts together to make a network or to connect networks together to make an internet.
- Connecting devices can operate in different layers of the Internet model.



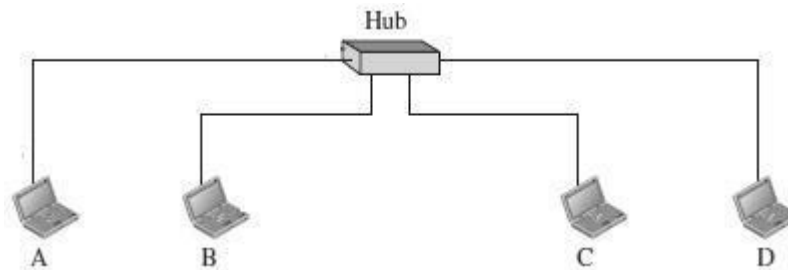
- Connecting devices are divided into five different categories on the basis of layers in which they operate in the network.



1. Devices which operate below the physical layer - **Passive hub**.
2. Devices which operate at the physical layer - **Repeater**.
3. Devices which operate at the physical and data link layers - **Bridge**.
4. Devices which operate at the physical layer, data link layer and network layer – **Router**.
5. Devices which operate at all five layers - **Gateway**.

1. HUBS

- Several networks need a central location to connect media segments together. These central locations are called as hubs.
- The hub organizes the cables and transmits incoming signals to the other media segments.



The three types of hubs are:

i) Passive hub

- It is a connector, which connects wires coming from the different branches.
- By using passive hub, each computer can receive the signal which is sent from all other computers connected in the hub.

ii) Active Hub

- It is a multiport repeater, which can regenerate the signal.
- It is used to create connections between two or more stations in a physical star topology.

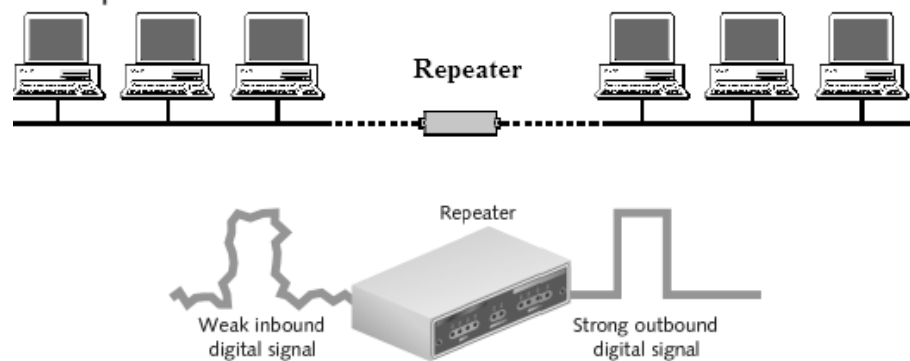
iii) Intelligent Hub

- Intelligent hub contains a program of network management and intelligent path selection.

2. REPEATERS

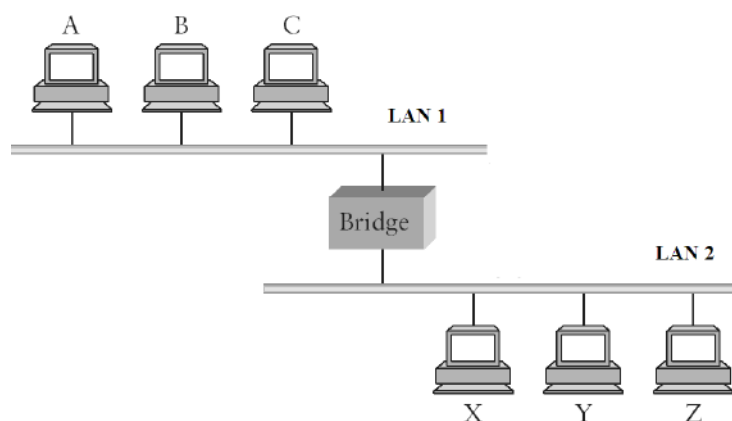
- A repeater receives the signal and it regenerates the signal in original bit pattern before the signal gets too weak or corrupted.
- It is used to extend the physical distance of LAN.
- Repeater works on physical layer.
- A repeater has no filtering capability.
- A repeater is implemented in computer networks to expand the coverage area of the network, repropagate a weak or broken signal and or service remote nodes.
- Repeaters amplify the received/input signal to a higher frequency domain so that it is reusable, scalable and available.

- Repeaters are also known as **signal boosters** or **range extender**.
- A repeater cannot connect two LANs, but it connects two segments of the same LAN.



3.BRIDGES

- Bridges operate in physical layer as well as data link layer.
- As a physical layer device, they regenerate the receive signal.
- As a data link layer, the bridge checks the physical (MAC) address (of the source and the destination) contained in the frame.
- The bridge has a filtering feature.
- It can check the destination address of a frame and decides, if the frame should be forwarded or dropped.
- Bridges are used to connect two or LANs working on the same protocol.



Types of Bridges :

Transparent Bridges

These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network , reconfiguration of the stations is unnecessary.

□ Source Routing Bridges

In these bridges, routing operation is performed by source station and the frame specifies which route to follow.

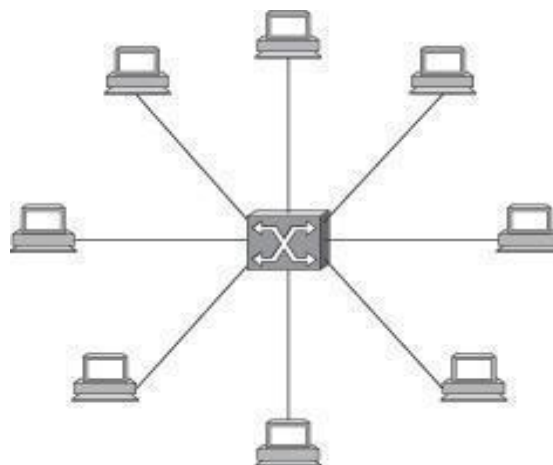
□ Translation Bridges

These bridges connect networks with different architectures, such as Ethernet and Token Ring. These bridges appear as:

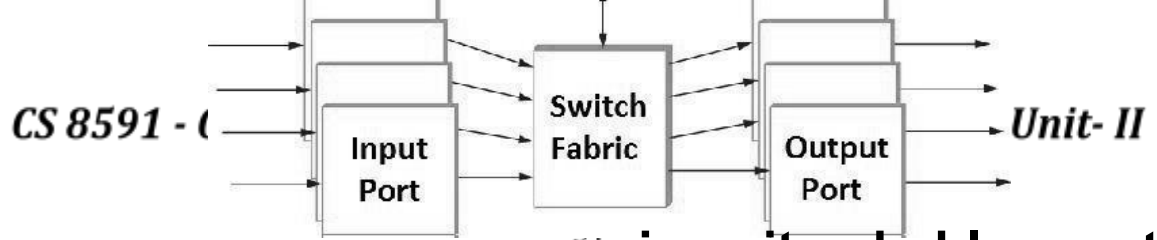
- Transparent bridges to an Ethernet host
- Source-routing bridges to a Token Ring host

4. SWITCHES

- A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).
- A switch is a mechanism that allows us to interconnect links to form a large network.



- Switch is data link layer device.
- A switch is a multi port bridge with a buffer .
- Switches are used to forward the packets based on MAC addresses.
- It is operated in full duplex mode.
- Packet collision is minimum as it directly communicates between source and destination.
- It does not broadcast the message as it works with limited bandwidth.
- A switch's primary job is to receive incoming packets on one of its links and to transmit them on some other link.
- A Switch is used to transfer the data only to the device that has been addressed.



annauniversityedu.blogspot.com

- Input ports receive stream of packets, analyzes the header, determines the output port and passes the packet onto the fabric.
- Ports contain buffers to hold packets before it is forwarded.
- If buffer space is unavailable, then packets are dropped.
- If packets at several input ports queue for a single output port, then only one of them is forwarded.

Types of Switch

i) Two- Layer Switch

- The two-layer switch performs at the physical and the data link layer.
- It is a bridge with many ports and design allows faster performs.
- A bridge is used to connect different LANs together.
- The two- layer switch can make a filtering decision bases on the MAC address of the received frame. However, two- layer switch has a buffer which holds the frame for processing.

ii) Three- Layer Switch

- The three-layer switch is a router.
- The switching fabric in a three-layer allows a faster table lookup and forwarding mechanism.

5.ROUTERS

A router is a three-layer device.

It operates in the physical, data-link, and network layers.

As a physical-layer device, it regenerates the signal it receives.

As a link-layer device, the router checks the physical addresses (source and destination) contained in the packet.

As a network-layer device, a router checks the network-layer addresses.

A router is a device like a switch that routes data packets based on their IP addresses.

A router can connect networks. A router connects the LANs and WANs on the internet.

A router is an internetworking device.

It connects independent networks to form an internetwork.



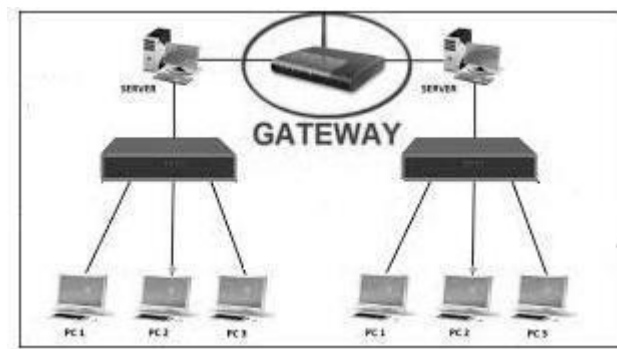
The key function of the router is to determine the shortest path to the destination.

Router has a routing table, which is used to make decision on selecting the route.

The routing table is updated dynamically based on which they make decisions on routing the data packets.

6.GATEWAY

- A gateway is a device, which operates in all five layers of the internet or seven layers of OSI model.
- It is usually a combination of hardware and software.
- Gateway connects two independent networks.



- Gateways are generally more complex than switch or router.
- Gateways basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system.
- Gateways are also called protocol converters
- A gateway accepts a packet formatted for one protocol and converts it to a packet formatted to another protocol before forwarding it.
- The gateway must adjust the data rate, size and data format.

7.BROUTER

- Brouter is a hybrid device. It combines the features of both bridge and router.
 - Brouter is a combination of Bridge and Router.
 - Functions as a bridge for nonroutable protocols and a router for routable protocols.
 - As a router, it is capable of routing packets across networks.
 - As a bridge, it is capable of filtering local area network traffic.
 - Provides the best attributes of both a bridge and a router
 - Operates at both the Data Link and Network layers and can replace separate bridges and routers.
-