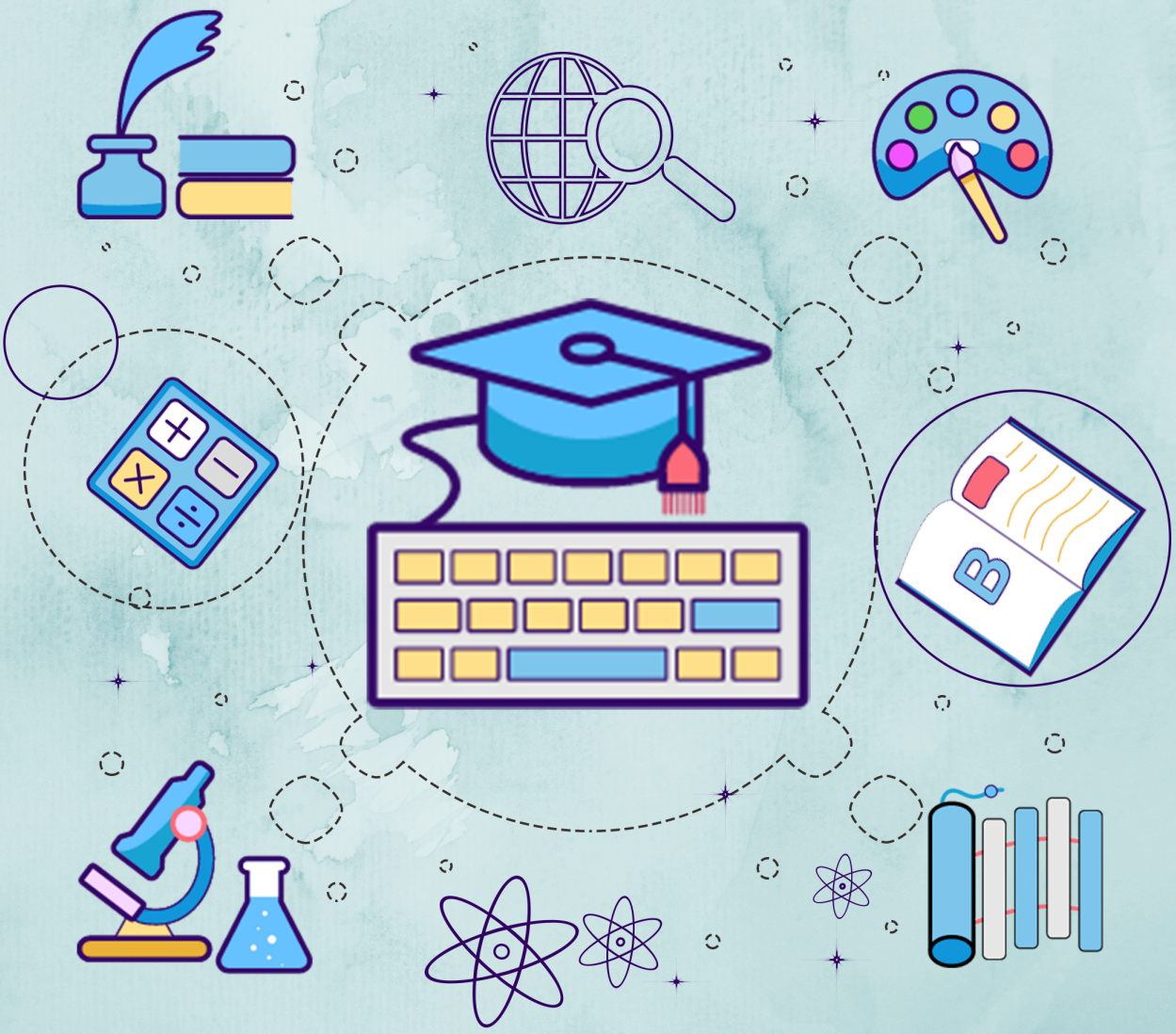
APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

KeralaNotes



SYLLABUS | STUDY MATERIALS | TEXTBOOK

PDF | SOLVED QUESTION PAPERS

www.keralanotes.com

KeralaNotes

KTU STUDY MATERIALS

COMPUTER NETWORKS

CST 303

Module 2

Related Link :

- KTU S5 STUDY MATERIALS
- KTU S5 NOTES
- KTU S5 SYLLABUS
- KTU S5 TEXTBOOK PDF
- KTU S5 PREVIOUS YEAR SOLVED QUESTION PAPER

KTU S5 Computer Science

Computer Networks

Module 2

Module - 2 (Data Link Layer)

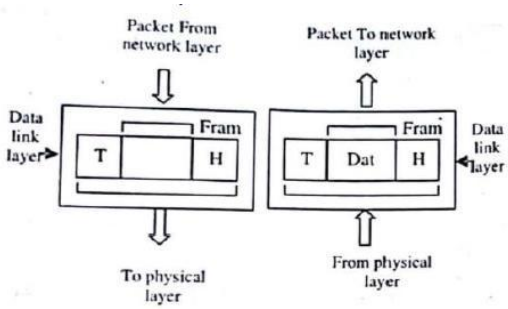
Data link layer - Data link layer design issues, Error detection and correction, Sliding window protocols, High-Level Data Link Control(HDLC)protocol. Medium Access Control (MAC) sublayer –Channel allocation problem, Multiple access protocols, Ethernet, Wireless LANs - 802.11, Bridges & switches - Bridges from 802.x to 802.y, Repeaters, Hubs, Bridges, Switches, Routers and Gateways.

Neethu Mathew , CSE Dept. EKCTC

DATA LINK LAYER

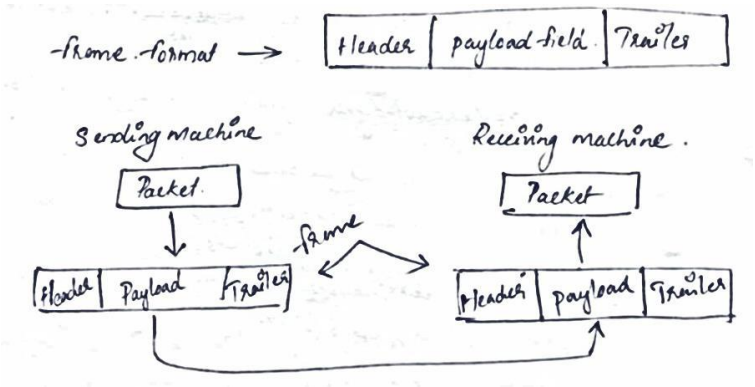
- data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- The data link layer adds a header to the frame to define the addresses of the sender and receiver of the frame.
- If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
- The data link layer also adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged, duplicate, or lost frames.
- Provide well defined service interface to the network layer
- Determining how the bits of the physical layer are grouped into frames
- Specific responsibilities of the data link layer include framing, addressing, flow control, error control etc

- data link layer is responsible for error free transfer of data frames.
- Purpose of data link layer is to Transfer blocks of data without error between 2 adjacent devices



Each Frame contains:

H-Header
Data
T-trailer



Design issues for data link layer : Functions of data link layer

1. Services Provides to Network Layer
2. Framing
3. Flow control
4. Error control
5. Addressing etc

1. Services Provides to Network Layer

- Principle service is transferring data from the network layer on the source machine to the Network layer on the destination machine.
- The job of data link layer is to Transmit the bits to the destination machine, so they can be handed over to the network layer.
- The actual transmission follows the path but its easier to think in terms of two data link layer processes communicating using a data link protocol
- Data link layer offer different types of services:
    i. Unacknowledged Connectionless Service
    ii. Acknowledged Connectionless Service
    iii. Acknowledged Connection-Oriented Service

i. Unacknowledged Connectionless Service

- In this service, destination machine do not send back any acknowledgement of receiving frames.
- It's a Connectionless service. Therefore no connection is established before communication or after it is over
- If a frame is lost due to noise, then no attempt is made to recover it.

ii. Acknowledged Connectionless Service

- In this type of service, there are no connection used but for each frame receive, the receiver sends an acknowledgement to the sender
- If a frame is not received within specified time, then the sender will retransmit it.

iii. Acknowledged Connection-Oriented Service

- Most sophisticated one.
- The source & destination machine establish a connection before transferring the data.
- A specific number is given to each frame being sent & data link layer guarantees that each transmitted frame is received.
- All the frames are guaranteed to be received in the same order as the order of transmission
- data transfer takes place by 3 phases : i)connection is established, ii)frames transmitted, iii)connection is released

2. Framing

- Data link layer pack bits into frames, each frame is distinguishable from another.
- Framing is the function of the data link layer that separates from other messages to other destinations 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.
- In order to guarantee that the bit stream is error free, the checksum(detect whether there was an error in transmission) of each frame is computed. when a frame is received, data link there , recomputes the checksum. If it is different from the checksum present in the frame , then data link layer knows that an error has occurred. It then discards the bad frame& send back a request for retransmission.
- Framing methods : character count, physical layer coding violations, character stuffing etc
- 2 types of framing

    *Fixed-Size Framing: there is no need for defining the boundaries

    *Variable-Size Framing: one needs a way to define the end of the frame and the beginning of the next

3. Error control

- Provides error detection and correction
- Make sure that all frames delivered to destination in proper order
- Generally receiver sends back some feedback (positive or negative) to convey the information about whether it has received a frame or not
- A positive acknowledgement(feedback) indicates a successful & error free delivery of frames
- A negative acknowledgement means that something has gone wrong and that frame need to be retransmitted.

❑ error detection and correction

When transmission of digital signals takes place between 2 systems, the signal get contaminated due to the addition of noise to it. The noise can introduce an error in the binary bits travelling from one system to other. This means that a 0 may change to 1 or 1 may change to 0

Redundancy

- The central concept in detecting or correcting errors is redundancy.
- To be able to detect or correct errors, we need to send some **extra (redundant) bits** with our data. These redundant bits are added by the sender and removed by the receiver. Their presence allows the receiver to detect or correct corrupted bits.

Detection Versus Correction

- In **error detection**, we are looking only to see if any error has occurred. The answer is a simple yes or no. We are not even interested in the number of errors.
- In **error correction**, we need to know the exact number of bits that are corrupted and more importantly, their location in the message

Forward Error Correction Versus Retransmission - 2 main methods of error correction.

- **Forward error correction** is the process in which the receiver tries to guess the message by using redundant bits. This is possible, if the number of errors is small.
- Correction by **retransmission** is a technique in which the receiver detects the occurrence of an error and asks the sender to resend the message. Resending is repeated until a message arrives that the receiver believes is error-free (usually, not all errors can be detected).

5.6.1. Types of Errors

Basically, whenever the received data differs from the transmitted data, an error is said to have occurred. Errors can occur due to various reasons. The errors introduced in the data bits during their transmission can be categorized as :

(i) Content errors

(ii) Flow integrity errors.

The content errors are nothing but errors in the content of a message e.g. a 0 may be received as 1 or vice versa. Such errors are introduced due to noise added into the data signal during its transmission. Flow integrity errors means missing blocks of data. It is possible that a data block may be lost in the network as it has been delivered to a wrong destination. Depending on the number of bits in error we can classify into two types as under

(i) Single bit error and

(ii) Burst errors.

1. Single bit error

The term signal bit error suggest that only one bit in the given data unit such as byte is in error. This means that only one bit will change from 1 to 0 or 0 to 1, as shown in figure 5.13.

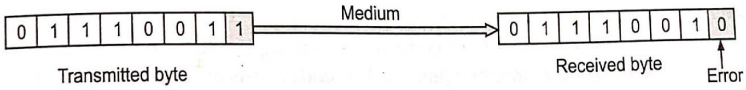


Fig. 5.13. Single bit error

2. Burst errors

If two or more bits from a data unit such as a byte change from 1 to 0 or from 0 to 1 then burst errors are said to have occurred. The length of the burst is measured from the first corrupted bit to the last corrupted bit. Some of the bits in between may not have been corrupted. Burst errors are illustrated in figure 5.14.

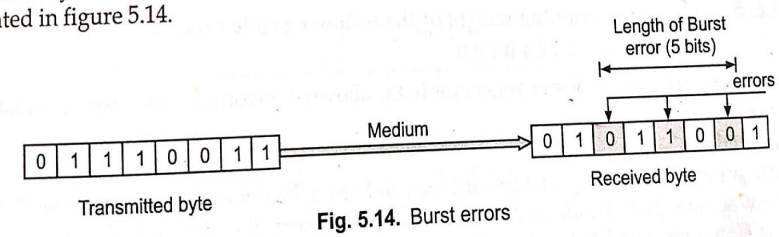


Fig. 5.14. Burst errors

Cyclic Redundancy Check (CRC)

- The CRC is more reliable error detection method.
- The method is a mathematical division process.
- The entire string of bits in a block of data is divided by some preselected constant.
- The remainder is known as CRC.
- The CRC code is appended to the data stream.
- The receiver reads in the data plus the CRC bytes and performs division by same divisor.
- The remainder will be zero if there were no errors in transmission.

CRC generation at sender side
1)Find the length of the divisor L
2)Append L-1 Bits to the original message
3)Perform binary division (X0R) Operation
4)Remainder of the division=CRC
CRC will add with original message and sent

A	B	X0R
0	0	0
0	1	1
1	0	1
1	1	0

Problem) **Find the CRC for the data block 100100 with divisor 1101 .**

Or

Problem) **Find the CRC for the data block 100100 The generator polynomial is $x^3+ x^2$ +1. verify the result**

Ex: Polynomial --- divisor
x^3+ x+1 is 1011
x^2+1 is 101
x^3 + 1 is 1001
$x^3+ x^2$ +1 is 1101

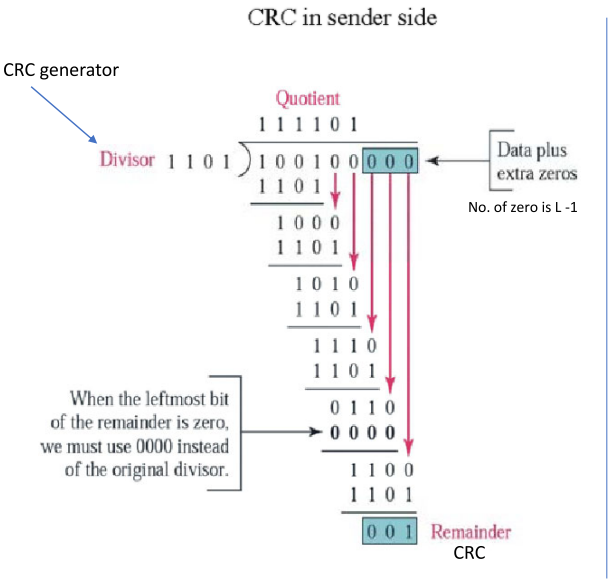
Here generator polynomial / Divisor is $x^3+ x^2$ +1

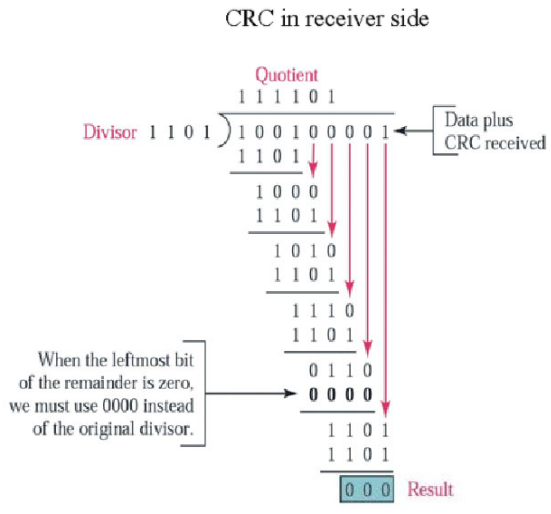
ie,

$x^3+ x^2$ +1 => $1x^3+ 1x^2+ 0x^1+1\ x^0$ => ie, **1101**

Answer) Length of divisor (L) is 4. So Append L-1 bits to the original message.

L-1=3 .so 3 zeros appended with original message (data block) 100100 and is **100100 000**

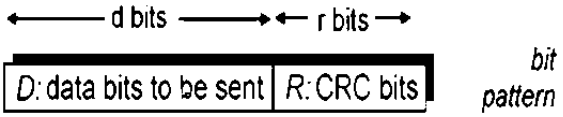




Here remainder is all zeros
Hence data received has No error
Data is accepted

If remainder is non zero….indicates error occurred

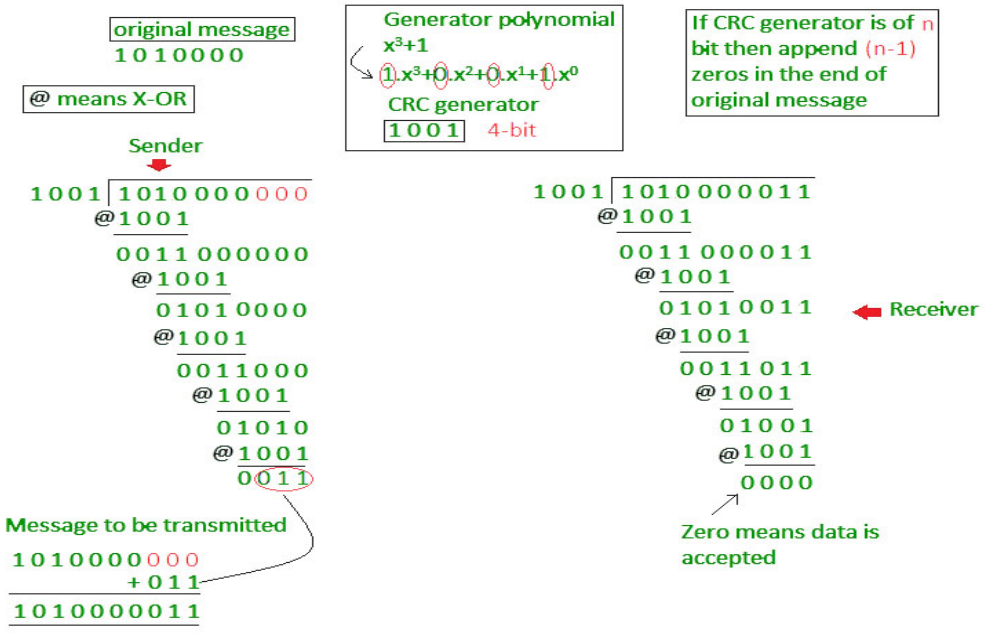
codeword =dataword+ remainder
Check receiver side
data (100100) plus CRC received (001) is codeword(**100100 001)**
Divisor is same 1101



Operation:

- Consider the d-bit piece of data, D.
- The sender and receiver must first agree on an r+1 bit pattern, known as generator, which is denoted as G. The most significant bit of G must be a 1.
- For a given piece of data, D, the sender will choose r additional bits, R, and append them to D such that the resulting d+r bit pattern is exactly divisible by G using modulo-2 arithmetic.
- The receiver divides the d+r received bits by G. If the remainder is non-zero, the receiver knows that an error has occurred; otherwise the data is accepted as being correct.

Q) bit stream transmitted is 1010000 . The generator polynomial is $x^3 + 1$. Use CRC method



Q. Calculate CRC for the message D = 101110, generator G = 1001 and reminder length r=3. And verify the result with and without error

Step 1:Add r zeros at the end of the message D to get T=101110000

Step 2: Divide T by G

Step 3: Message to be transmitted: 101110011

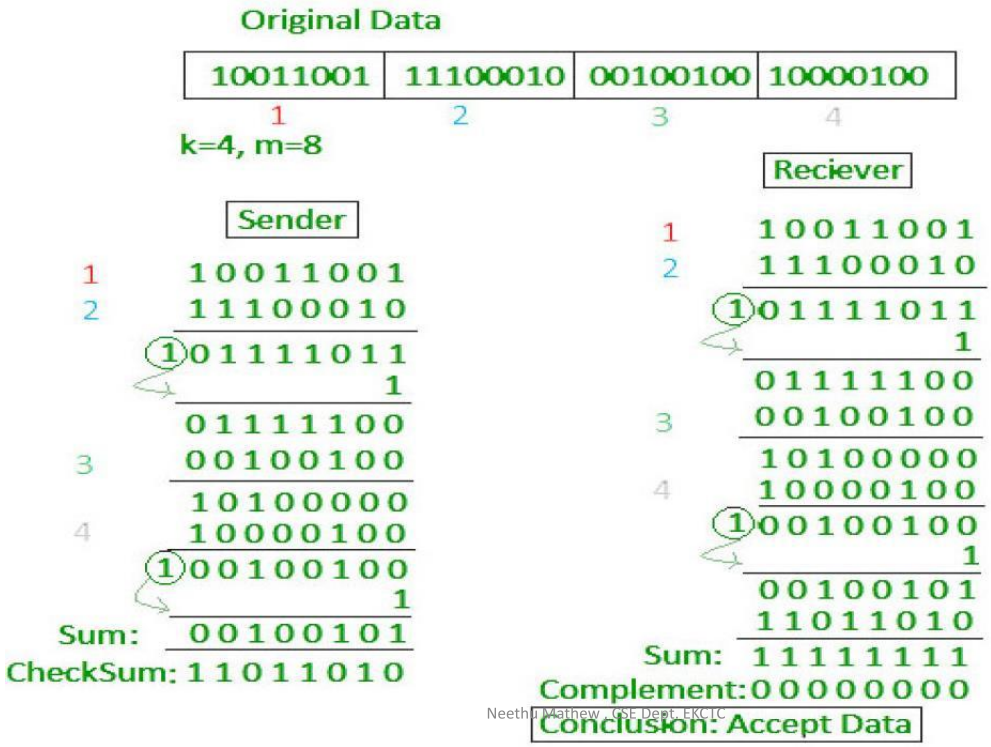
Verification without error:

Divide received message T by G

```
          101011
      ------------
1001 | 101110011
       1001
       ----
        101
        000
        ---
        1010
        1001
        ----
         110
         000
         ---
         1101
         1001
         ----
          1001
          1001
          ----
             0   <------- Remainder
```


Checksum

- In **checksum error detection scheme**, the data is divided into k segments each of m bits.
- In the sender's end the segments are added using 1's complement arithmetic to get the sum.
- The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.
- At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum.
- The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.



4. Flow Control

- If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
- It is a Set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver.
- The flow of data must not be allowed to overwhelm the receiver.
- Any receiving device has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data.
- 2 approaches

1: Feedback-Based Flow Control:

- receiver sends back information to the sender giving it permission to send more data or at least telling the sender how the receiver is doing.

2: Rate-Based Flow Control:

- In this the protocol has a built-in mechanism that limits the rate at which senders may transmit data, without using feedback from the receiver.

Categories Of Flow Control protocols

1. Stop-and-Wait Protocol

- source sends a packet and only after receiving the acknowledgment from the destination, it sends next packet.
- It's a simple protocol but results in lots of delay, and the bandwidth is not used efficiently.
  - Source (sender A) sends the first packet to the destination(B) and wait for the acknowledgement (ACK), then B sends an acknowledgement packet
  - Then A sends the second packet & B sends the acknowledgement.
  - A repeat this process until sender A transmit an end of transmission frame (EOT).

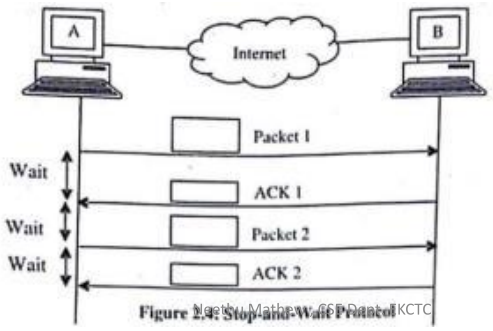


Figure 2.4: Stop-and-Wait Protocol

- Stop & wait is a data link layer protocol used for transmitting data over the noiseless channels
- Provides unidirectional data transmission(either sending / receiving of data will takes place at a time)

✓ Advantages

- It is a very simple protocol of flow control.

✓ Disadvantages

- Loss of data packet
- Loss of acknowledgement

2. Sliding Window Protocol:

- Improves the efficiency of stop and wait protocol by allowing multiple frames to be transmitted before receiving an acknowledgment.
- Ie, several frames can be transmit at a time
- Both the sender and the receiver has finite sized buffers called windows. (sending window and receiving window)
- The sender and the receiver agrees upon the number of frames to be sent based upon the buffer size.
- The sender maintains information about:
  - *Size of sender window
  - *Last frame sent
  - *Last acknowledgement received
- Receiver holds information about
  - *Receiver window size,
  - *Large acceptable frame,
  - *Last frame received

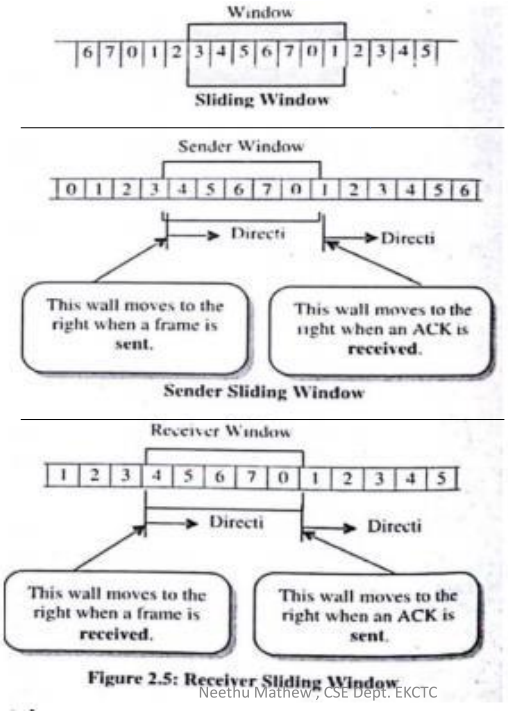
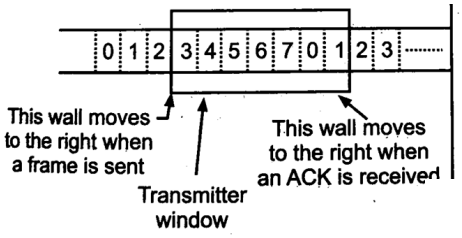
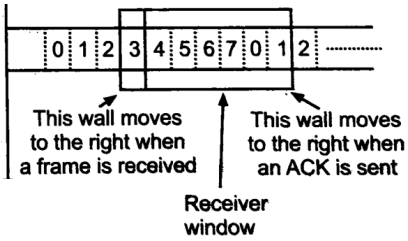


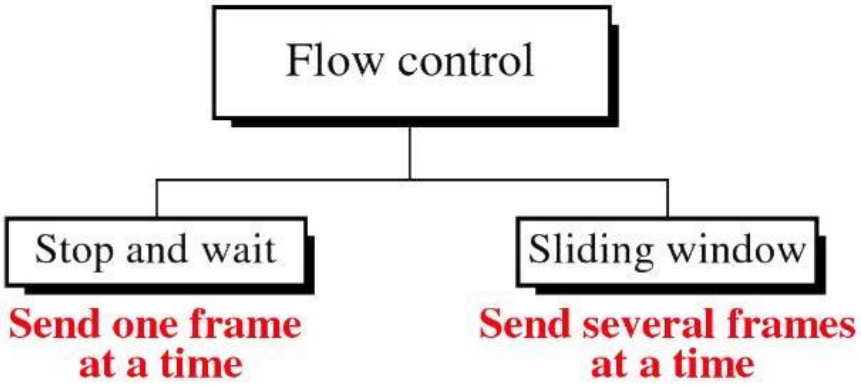
Figure 2.5: Receiver Sliding Window



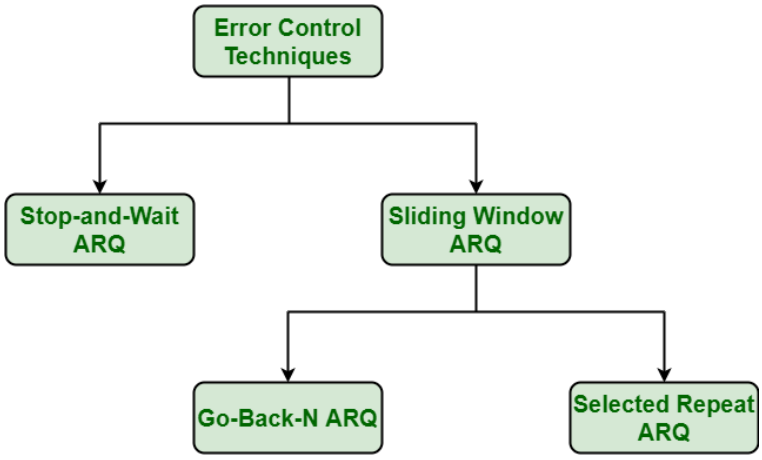


✓ **Advantages**
- Network Utilization
- Data can be transmitted in both directions.
- Several frames can be in transit at a time.

✓ **Disadvantages**
- complexity and hardware capacity



Error control mechanism



Error control mechanism

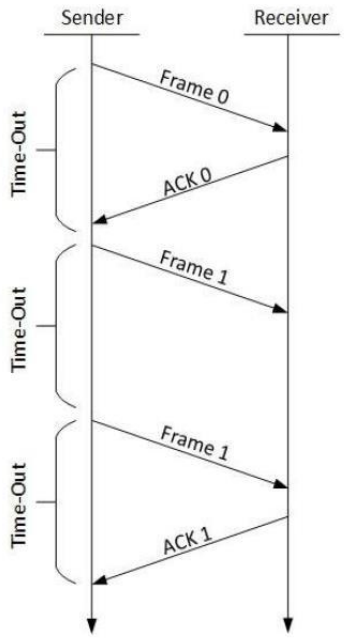
Automatic Repeat Query / Automatic Repeat Request (ARQ)

- ARQ is an error-control method for data transmission that uses acknowledgements (messages sent by the receiver indicating that it has correctly received a data frame or packet) & timeouts (specified periods of time allowed to elapse before an acknowledgment is to be received)
- If the sender does not receive an acknowledgment before the timeout, it usually re-transmits the frame/packet until the sender receives an acknowledgment

Types of ARQ Techniques

1. **Stop-and-Wait ARQ:**

- The sender maintains a timeout counter.
- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
- If a negative acknowledgement (NAK) is received, the sender retransmits the frame



- Stop -and-Wait ARQ provides unidirectional data transmission
- It is also known as ABP(Alternating Bit Protocol).

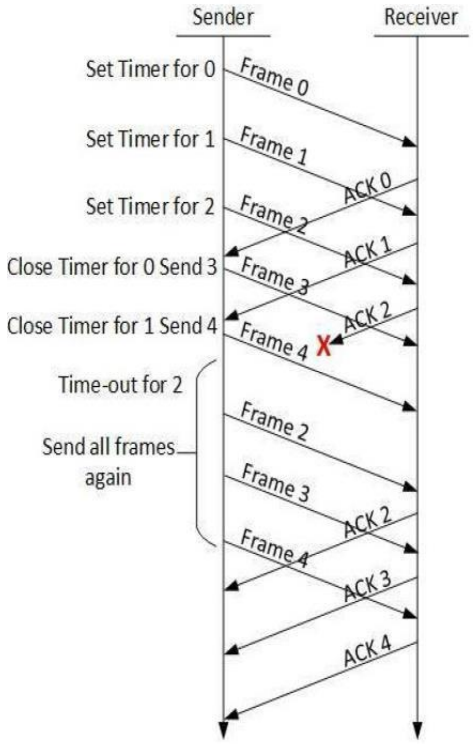
- For retransmission , four features are added to the basic flow control mechanism:

1. The sending device keeps a copy of the last frame transmitted until it receives an acknowledgment for that frame. Keeping a copy allows the sender to retransmit lost or damaged frames until they are received correctly.
2. For identification purposes. both data frames and ACK frames are numbered and numbering allows for identification of data frames in case of duplicate transmission
3. If an error is discovered in a data frame, indicating that it has been corrupted in transit, a negative acknowledgement (NAK) frame is returned. NAK frames, tell the sender to retransmit the last frame sent
4. The sending device is equipped with a timer. If an expected acknowledgment is not received within an allotted time period, the sender assumes that the last data frame was lost in transit and sends it again

2. Sliding Window ARQ:

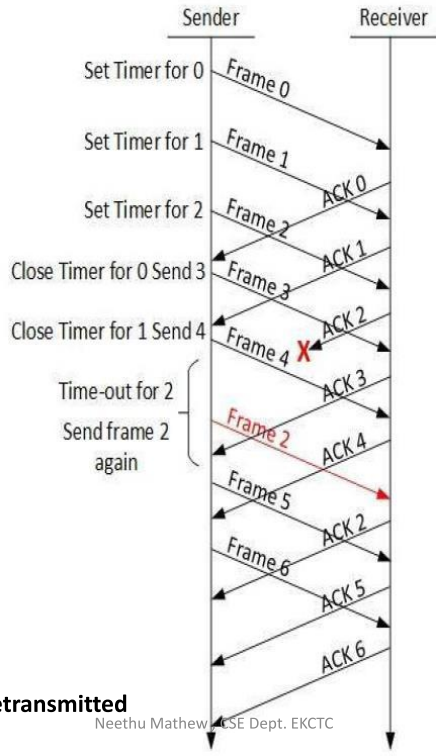
1. Go-Back-n ARQ:

- If the acknowledgement of a frame is not received within the time period, all frames starting from that frame are retransmitted.
- In Go-Back-N ARQ method, both sender and receiver maintain a window. The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them.The receiver keeps track of incoming frame's sequence number.



- When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement.
- If all frames are positively acknowledged, the sender sends next set of frames.
- If sender finds that it has received NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK

2. Selective Repeat ARQ



only the erroneous or lost frames are retransmitted

- Selective Repeat ARQ provides for sending multiple frames before receiving the acknowledgement for the first frame. only the erroneous or lost frames are retransmitted, while the good frames are received and buffered. Sender sends a number of frames specified by a window size even without the need to wait for individual ACK .receiver sends ACK for each frame individually, receiver accepts out-of-order frames and buffers them. The sender individually retransmits frames that have timed out. In selective-repeat ARQ, only the specific damaged or lost frame is retransmitted. If a frame is corrupted in transit, a NAK is returned and the frame is resent out of sequence.

Advantages of Selective-Repeat ARQ

i) Similar to Go-Back-N ARQ. However, the sender only retransmits frames for which a NAK is received.

ii) Fewer retransmission

Disadvantages of Selective-Repeat ARQ

i) More complexity at sender and receiver

ii) Each frame must be acknowledged individually

iii) Receiver may receive frames out of sequence

High-level Data Link Control (HDLC)

- HDLC is a bit-oriented data link control protocol
- It offers high level of flexibility,adaptability,reliability and efficiency of operation
- It implements the ARQ (automatic repeat request) mechanisms
- To make HDLC protocol applicable to various network configurations, HDLC defines 3 types of stations :

1. Primary station

- Responsibility of connecting & disconnecting data link(in the event of communication b/w primary & secondary station)
- Data link management
- Frames sent by primary station are called commands

2. Secondary station

- It operates under the control of primary station
- Frames sent by secondary station are called responses

3. Combined station

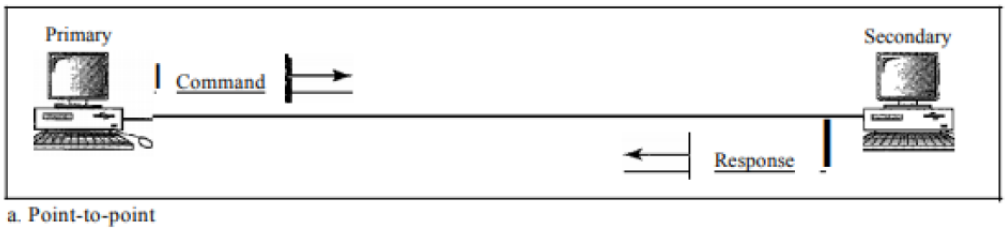
- It act as primary as well as secondary station. So it can issue both commands and responses

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

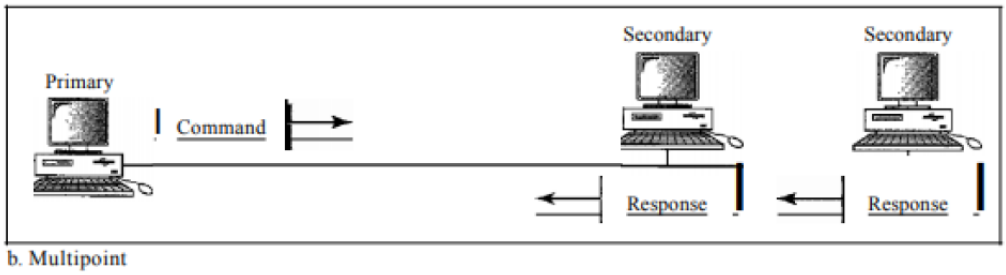
❑ **Normal Response Mode**

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

Normal response mode



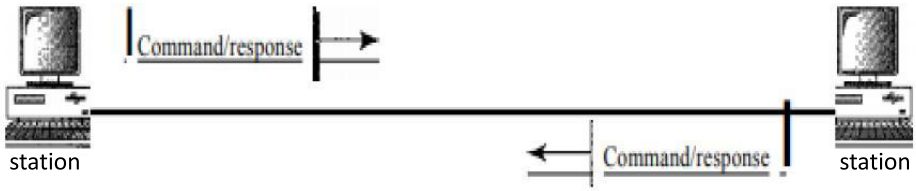
a. Point-to-point



b. Multipoint

❑ **Asynchronous Balanced Mode** (ABM)

- configuration is balanced.
- The link is point-to-point, and each station can function as a primary and a secondary
- Frames can be transmitted in full duplex manner



frame types in HDLC

- HDLC defines three types of frames:
  - Information frames (I-frames),
  - supervisory frames (S-frames),
  - unnumbered frames (U-frames).

• I-frames are used to transport user data and control information relating to user data .

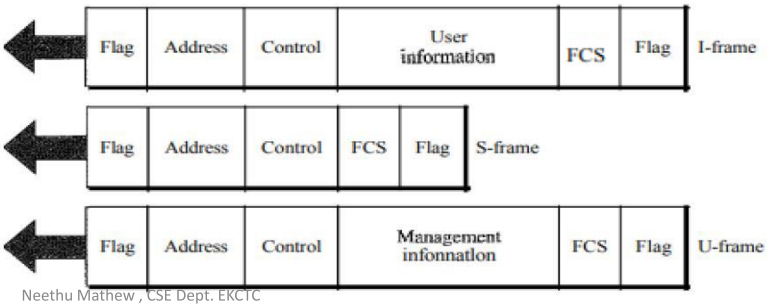
• S-frames are used only to transport control information. These are used for error and flow control

• U-frames are reserved for system management. Information carried by U-frames is intended for managing the link itself

Frame format/structure of HDLC

Each frame in HDLC may contain up to six fields:

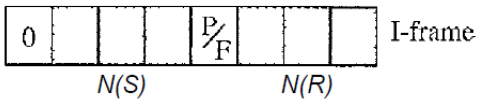
- a beginning flag field,
- an address field,
- a control field,
- an information field,
- a frame check sequence (FCS) field,
- and an ending flag field.



- **Flag field:** The flag field of an HDLC frame is an 8-bit sequence with the bit pattern 01111110 that identifies both the beginning and the end of a frame
- **Address field:** The second field of an HDLC frame contains the address of the secondary station. If a primary station created the frame, it contains a to address. If a secondary creates the frame, it contains a from address. An address field can be 1 byte or several bytes long, depending on the needs of the network.(extendable)
- **Information field:** The information field contains the user's data from the network layer or management information. Its length can vary from one network to another.
- **FCS field:** The frame check sequence (FCS) is the HDLC error detection field.
- **Control field:** The control field is a 1or 2-byte segment , used for flow and error control.

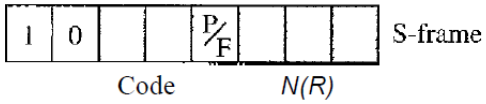
Control field format for the different frame types

Control Field for I-Frames



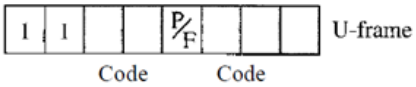
- The first bit defines the type. If the first bit of the control field is 0, this means the frame is an I-frame.
- The next 3 bits, called N(S), define the sequence number of the frame.
- The last 3 bits, called N(R), correspond to the acknowledgment number.
- The single bit between N(S) and N(R) is called the P/F bit (poll or final). It means poll when the frame is sent by a primary station to a secondary (when the address field contains the address of the receiver). It means final when the frame is sent by a secondary to a primary (when the address field contains the address of the sender).

Control Field for S-Frame



- S-frames do not have information fields.
- If the first 2 bits of the control field is 1 0, this means the frame is an S-frame.
- The last 3 bits, called N(R), corresponds to the acknowledgment number (ACK) or negative acknowledgment number (NAK) depending on the type of S-frame.
- The 2 bits called code is used to define the type of S-frame itself. With 2 bits, we can have four types of S-frames, as described below:
  - If the value of the code subfield is **00**, it is an Receive ready (RR) S-frame.
  - If the value of the code subfield is **10**, it is an Receive not ready (RNR) S-frame
  - If the value of the code subfield is **01**, it is a Reject (REJ) S-frame
  - If the value of the code subfield is **11**, it is an Selective reject (SREJ) S-frame.

Control Field for U-Frame



- 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. Together, these two segments (5 bits) can be used to create up to 32 different types of U-frames

  ex: 00 001 → SNRM (Set normal response mode)Command

  11 001 → RSET (Reset) command

  etc

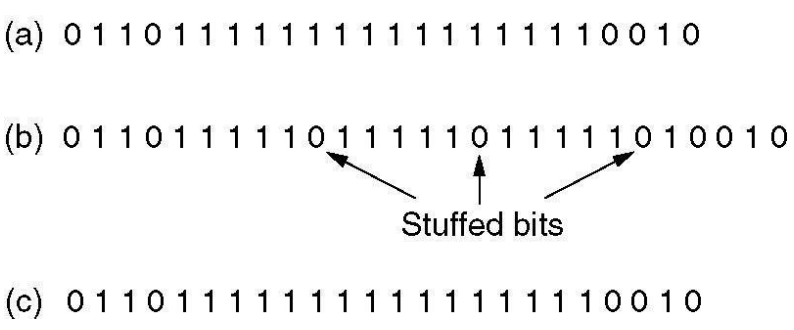
Table 11.1 *U-frame control command and response*

Code	*Command*	*Response*	*Meaning*
00 001	SNRM		Set normal response mode
11 011	SNRME		Set normal response mode, extended
11 100	SABM	DM	Set asynchronous balanced mode or disconnect mode
11110	SABME		Set asynchronous balanced mode, extended
00 000	UI	UI	Unnumbered information
00 110		UA	Unnumbered acknowledgment
00 010	DISC	RD	Disconnect or request disconnect
10 000	SIM	RIM	Set initialization mode or request information mode
00 100	UP		Unnumbered poll
11 001	RSET		Reset
11 101	XID	XID	Exchange ID
10 001	FRMR	FRMR	Frame reject

Bit stuffing

- In data transmission and telecommunication, it is the insertion of non information bits into data.(It is the process of adding one extra 0 after the data-1)
- In the data a 0 bit is automatically stuffed into the outgoing bit stream whenever the sender's data link layer finds five consecutive 1s
- Bit stuffing is merely a way of attempting to ensure that the transmission starts and ends at the correct places
- Bit stuffing is used for various purposes, such as for bringing bit streams that do not necessarily have the same or rationally related bit rates up to a common rate, or to fill buffers or frames.
- The location of the stuffing bits is communicated to the receiving end of the data link, where these extra bits are removed to return the bit streams to their original bit rates or form.

- When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automatically destuffs (i.e., deletes) the 0 bit. The figure1 below gives an example of bit stuffing.



a) Original data.

b) Data as they appear on the transmission line

c) Data as they are stored in receivers memory after destuffing

Fig: Bit stuffing

Medium Access Control (MAC) sublayer

Network –

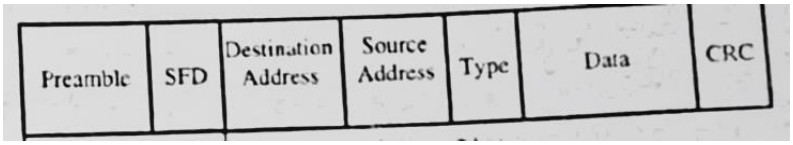
2 categories - Point to point & broadcast

- Broadcast channels are sometimes referred to as multiaccess channels or random access channels
- Data link layer is divided into two sublayers:
  - ❑ logical link control (LLC) - responsible for flow and error control
  - ❑ Media access control (MAC)
- IEEE made this division for LAN
- In the broadcast network, the most important point is the criteria to determine who is allowed to use the channel when more than one users want to use it. A protocol is used to make this decision. such a protocol belong to sublayer of data link layer called the **MAC sublayer**
- MAC (Medium Access Control) Sub layer deals with broadcast networks and their protocols.
- MAC sublayer is especially important in LAN

MAC layer functions
- Detection of errors
- To perform the control of access to media

Basic format for all MAC implementation is defined in IEEE 802.3 standard

Structure of MAC



- Preamble: used for bit synchronization, contains 7 bytes of alternating 0s and 1s
- Start frame delimiter (SFD) : The SFD warns the station or stations that this is the last chance for synchronization. It alerts the receiver that the next field is the destination address
- Destination address (DA):contains address of the destination station or stations to receive the packet.
- Source address (SA): address of the sender of the packet.
- Length or type: This field is defined as a type field or length field. length field to define the number of bytes in the data field.
- Data : This field carries data encapsulated. It is a minimum of 46 and a maximum of 1500 bytes.
- CRC: The last field contains error detection information

Channel allocation problem

- In broadcast network, several stations share a single communication channel. This channel can be allocated to only one transmitting user at a time
- Two different methods/schemes of channel allocation:
  - ❑ static channel allocation
  - ❑ Dynamic channel allocation

Static Channel Allocations

- FDM & TDM are the examples of static channel allocations
- In this method, either a fixed frequency or a fixed time slot is assigned to each user

•FDM (Frequency Division Multiplexing) - In FDM, fixed frequency is assigned to each user

•TDM (Time Division Multiplexing) ,whereas, in TDM, fixed time slot is assigned to each user.

- The problem in these methods is that if all the N number of users are not using the channel, the channel bandwidth is wasted and if there are more than N users who want to use the channel they cannot do so for the lack of bandwidth.
- When the number of senders is large and continuously varying or the traffic is bursty, FDM presents some problems.
- static channel allocation has a poor performance with bursty traffic and hence generally dynamic channel allocation is used

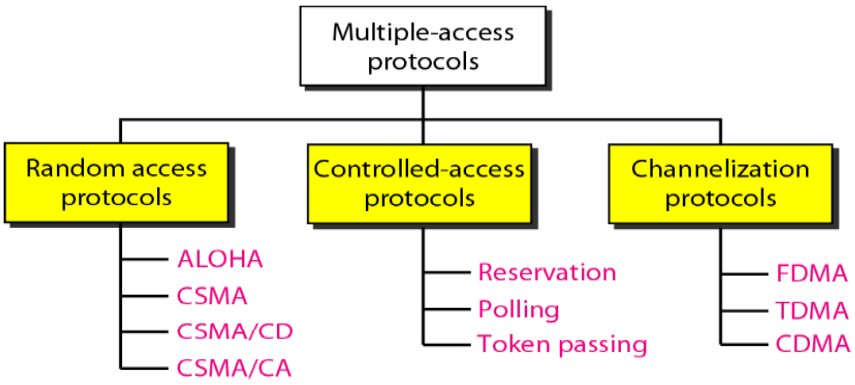
Dynamic Channel Allocation

- In this method, no user is assigned fixed frequency or fixed time slot.
- All users are dynamically assigned frequency or time slot, depending upon the requirements of the user
- Based on 5 key assumptions:
  - Static model :-consists of N independent stations each with a program or user that generates frames for transmission
  - Single channel:- A single channel is available for all communication
  - Collision :- If frames are transmitted at the same time by two or more stations, there is an overlap in time and the resulting signal is garbled. This event is called a collision
  - Continuous or Slotted Time :- Time may be assumed continuous, in which case frame transmission can begin at any instant. Frame transmissions must then begin at the start of a slot
  - Carrier Sense or No Carrier Sense:- With the carrier sense assumption, stations can tell if the channel is in use before trying to use it. No station will attempt to use the channel while it is sensed as busy. If there is no carrier sense, stations cannot sense the channel before trying to use it. They just go ahead and transmit

Multiple Access Links

- Broadcast : networks have a single channel that is shared by all the machines in the network.
- When nodes or stations are connected and use a common link, called a multipoint or broadcast link (or network), we need a **Multiple Access Protocol** to coordinate access to the link.
- Many protocols has been defined to handle the access to shared link
- These protocols divided into 3 different groups

Multiple Access Protocol



A. Random Access Protocols

- In random access method no station is superior to another station and no one is assigned the control over another
- Two features give this method its name.
  - – Transmission is random among the stations (there is no scheduled time for a station to transmit) That is why these methods are called random access.
  - – No rules specify which station should send next. Stations compete with one another to access the medium. That is why these methods are also called **contention methods**.
- if more than one station tries to send, there is an access conflict-collision- and the frames will be either destroyed or modified.

Types :

- ALOHA
- CSMA (Carrier Sense Multiple Access)
- CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

I) ALOHA

It was used for ground based radio broadcasting. In this method, stations share a common channel. When two stations transmit simultaneously, collision occurs and frames are lost. There are two different versions of ALOHA:

- Pure ALOHA
- Slotted ALOHA

Pure ALOHA:

- In pure ALOHA, stations transmit frames whenever they have data to send.
- When two stations transmit simultaneously, there is collision and frames are lost.
- In pure ALOHA, whenever any station transmits a frame, it expects an acknowledgement from the receiver.
- If acknowledgement is not received within specified time, the station assumes that the frame has been lost.
- **If the frame is lost, station waits for a random amount of time and sends it again**.
- This waiting time must be random, otherwise, same frames will collide again and again.
- Whenever two frames try to occupy the channel at the same time, there will be collision and both the frames will be lost. If first bit of a new frame overlaps with the last bit of a frame almost finished, both frames will be lost and both will have to be transmitted.

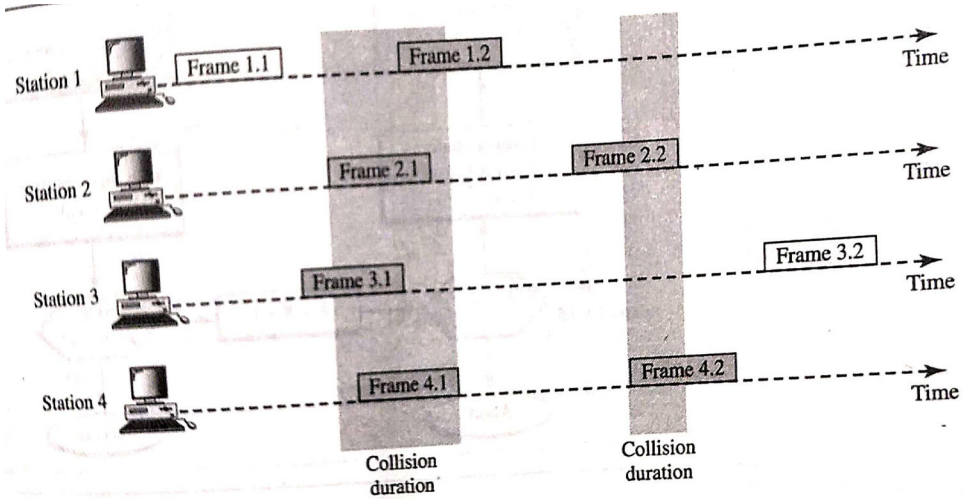
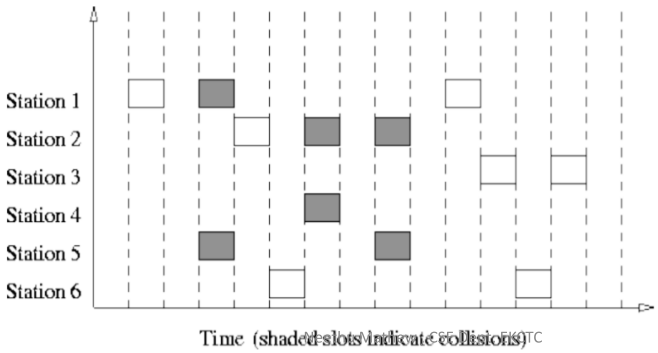


Fig : Frames in pure ALOHA

2. Slotted ALOHA :

- Slotted ALOHA was invented to improve the efficiency of pure ALOHA.
- In slotted ALOHA, time of the channel is divided into intervals called slots.
- The station can send a frame only at the beginning of the slot and only one frame is sent in each slot.
- If any station is not able to place the frame onto the channel at the beginning of the slot, it has to wait until the next time slot.
- There is still a possibility of collision if two stations try to send at the beginning of the same time slot.
- Method for doubling the capacity of an ALOHA system



II) Carrier Sense Multiple Access (CSMA) Protocols

- CSMA was developed to overcome the problems of ALOHA
- i.e. to minimize the chances of collision.
- CSMA is based on the principle of "carrier sense". The station sense the carrier or channel before transmitting a frame. It means the station checks whether the channel is idle or busy. The chances of collision reduces to a great extent if a station checks the channel before trying to use it.
- Principle : sense before transmit or listen before talk
- The chances of collision still exists because of propagation delay. The frame transmitted by one station takes some time to reach the other station. In the meantime, other station may sense the channel to be idle and transmit its frames. This results in the collision.
- There are three different types of CSMA protocols:
  - 1-Persistent CSMA
  - Non-Persistent CSMA
  - P-Persistent CSMA

- **1-Persistent CSMA:** When a station has data to send, it first listens to the channel to see if anyone else is transmitting at that moment. If the channel is busy, the station waits until it becomes idle. When the station detects an idle channel, it transmits a frame immediately (with a probability of 1). This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.
- **Non-Persistent CSMA:** A station that has a frame to send senses the channel. If the channel is idle, it sends immediately. If the channel is busy, it waits a random amount of time and then senses the channel again. It reduces the chance of collision because the stations wait for a random amount of time. It is unlikely that two or more stations will wait for the same amount of time and will retransmit at the same time.
- **P-Persistent CSMA:** In this method, the channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time. When a station is ready to send, it senses the channel. If the channel is busy, station waits until next slot. If the channel is idle, it transmits the frame. It reduces the chance of collision and improves the efficiency of the network.

- p-persistent CSMA applies to slotted channels
- When a station becomes ready to send, it senses the channel.
- If it is idle, it transmits frame with a probability p.
- With a probability q = 1 - p, it waits until the next slot.
- If that slot is also idle, it either transmits or defers again, with probabilities p and q.
- This process is repeated until either the frame has been transmitted or another station has begun transmitting
- If the station initially senses the channel busy, it waits until the next slot and applies the above algorithm

III) CSMA with Collision Detection (CSMA/CD)

- Additional feature in CSMA/CD is that the stations can detect collisions.
- The stations abort their transmission as soon as they detect collision. This feature is not present in CSMA. The stations continue to transmit even though they find that collision has occurred.
- In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, there is a collision, the frame is sent again
- Advantage: saves time and bandwidth
- widely used on LANs in the MAC sublayer
- CSMA/CD is specified in the IEEE 802.3 standard.
- In CSMA/CD protocol, the station senses the channel before transmitting the frame. If the channel is busy, the station waits.

CSMA/CD is Carrier Sense Multiple Access / Collision Detection :

- Carrier Sense – the ability of a network card to sense or detect communication on the network
- Multiple Access – states that in that network there are multiple stations that could access the network at the same time
- Collision Detection – the method needed for detecting a collision

Carrier Sense Multiple Access/Collision Detection (CSMA/CD) is the protocol for carrier transmission access in Ethernet networks. Carrier-sense multiple access with collision detection describes how the Ethernet protocol regulates communication among nodes

IV) Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

- This is a CSMA protocol with collision avoidance
- We need to avoid collisions on wireless networks because they cannot be detected. Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for this network
- Collisions are avoided through the use of CSMA/CA's 3 strategies:
    - interframe space
    - contention window
    - acknowledgments

Interframe Space (IFS):

- 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. If after the IFS time the channel is still idle, the station can sed , but it still needs to wait a time – contention time

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 back-off 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.
- This is very similar to the p-persistent method except that a random outcome defines the number of slots taken by the waiting station. One interesting point about the contention window is that the station needs to sense the channel after each time slot. However, if the station finds the channel busy, it does not restart the process; it just stops the timer and restarts it when the channel is sensed as idle. This gives priority to the station with the longest waiting time.

Acknowledgment :

- With all these precautions, there still may be a collision resulting in destroyed data. 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.

B. CONTROLLED ACCESS PROTOCOLS

- In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations. We discuss three popular controlled-access methods

1. Reservation :

- In the reservation method, a station needs to make a reservation before sending data.
- Time is divided into intervals.
- In each interval, a reservation frame precedes the data frames sent in that interval.
- If there are N stations in the system, there are exactly N reservation minislots in the reservation frame. Each minislot belongs to a station.
- When a station needs to send a data frame, it makes a reservation in its own minislot. The stations that have made reservations can send their data frames after the reservation frame

2. Polling :

- Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations. All data exchanges must be made through the primary device even when the ultimate destination is a secondary device.

- The primary device controls the link; the secondary devices follow its instructions. It is up to the primary device to determine which device is allowed to use the channel at a given time. The primary device, therefore, is always the initiator of a session.
- If the primary wants to receive data, it asks the secondaries if they have anything to send; this is called **poll** function. If the primary wants to send data, it tells the secondary to get ready to receive; this is called **select** function. The poll function is used by the primary device to solicit transmissions from the secondary devices. When the primary is ready to receive data, it must ask (poll) each device in turn if it has anything to send.

3. Token Passing :

- In the token-passing method, the stations in a network are organized in a logical ring.
- for each station, there is a predecessor and a successor. The predecessor is the station which is logically before the station in the ring; the successor is the station which is after the station in the ring. The current station is the one that is accessing the channel now.

- In this method, a special packet called a token circulates through the ring. The possession of the token gives the station the right to access the channel and send its data.
- When a station has some data to send, it waits until it receives the token from its predecessor. It then holds the token and sends its data. When the station has no more data to send, it releases the token, passing it to the next logical station in the ring.
- The station cannot send data until it receives the token again in the next round. In this process, when a station receives the token and has no data to send, it just passes the data to the next station.
- Token management is needed for this access method.
- The token must be monitored to ensure it has not been lost or destroyed. For example, if a station that is holding the token fails, the token will disappear from the network.
- Another function of token management is to assign priorities to the stations and to the types of data being transmitted. And finally, token management is needed to make low-priority stations release the token to high priority stations

C. CHANNELIZATION

- Channelization(channel partition) is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations.
- 3 channelization protocols: **FDMA, TDMA, and CDMA**.

1. Frequency-Division Multiple Access (FDMA)

- The available bandwidth is divided into frequency band. Each station is allocated a band to send its data
- The available channel (medium) bandwidth is shared by all the station.so each station uses its allocated frequency band to send its data.
- Each band is reserved for a specific station and it belongs to the station all the time
- To prevent station interferences, the allocated bands are separated from one another by small guard bands
- Stream data can be used with FDMA
- FDMA used in cellular telephone phones systems
- Advantage : all stations can operate all 24 hours without having to wait for their turn to come
  : no synchronization is necessary
- Disadvantage : adjacent channel interference
  : each station use only a part of the total bandwidth

2. Time-Division Multiple Access (TDMA)

- The entire bandwidth can be used by every user(station) but not simultaneously
- A station can use entire bandwidth only for the allotted time
- each station is allocated a time slot during which it can send its data
- Each station transmits its data in its assigned time slot
- FDMA used in cellular phones and satellite networks
- TDMA needs synchronization which makes it more complicated as compared to FDMA

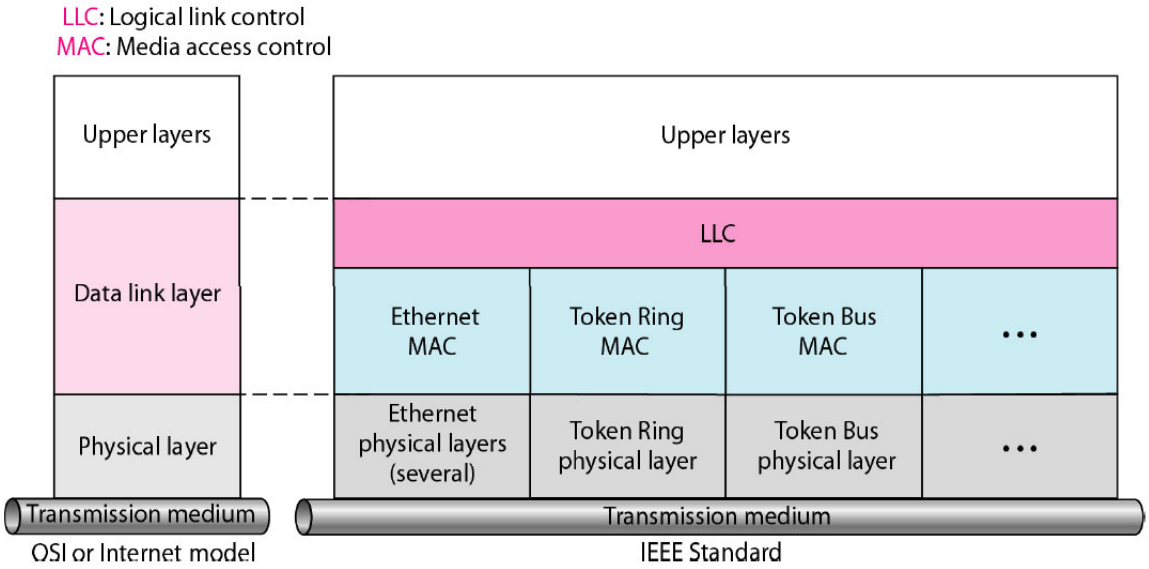
3. Code-Division Multiple Access (CDMA)

- In CDMA, one channel carries all transmissions simultaneously
- CDMA simply means communication with different codes
- Synchronization is not necessary
- Interferences will be present

Ethernet - Wired LAN

- Computer Society of the IEEE(Institution Of Electrical And Electronics Engineers) started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers.
- Project 802 specifying functions of the physical layer and the datalink layer of major LAN protocols.
- The IEEE has subdivided the data-link layer into two sublayers: logical link control (LLC) and media access control (MAC).
- IEEE has also created several physical-layer standards for different LAN protocols.
- IEEE 802 standards are
  - 802.3 (Ethernet)- CSMA/CD
  - 802.4 (Token bus)
  - 802.5 (Token ring)
  - 802.11 (wireless LAN)
  - 802.15 (Bluetooth)
  - 802.16 (wireless MAN) etc

IEEE Standards for LANs



❑ **Logical Link Control (LLC)**

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

❑ **Media Access Control (MAC)**

- IEEE Project 802 has created a sublayer called media access control that defines the specific access method for each LAN.
- For example, it defines CSMA/CD as the media access method for Ethernet LANs , and defines the token-passing method for Token Ring and Token Bus LANs.
- A part of the framing function is also handled by the MAC layer.

Generations:

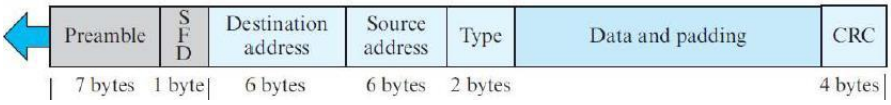
1. Standard Ethernet (10 Mbps)
2. Fast Ethernet (100 Mbps)
3. Gigabit Ethernet (1 Gbps)
4. 10 Gigabit Ethernet (10 Gbps)

1. Standard Ethernet

- We refer to the original Ethernet technology with the data rate of 10 Mbps as the Standard Ethernet.

Frame Format

- The Ethernet frame contains seven fields



- Preamble: This field contains 7 bytes (56 bits) of alternating 0s and 1s that alert the receiving system to the coming frame
- Start frame delimiter (SFD): This field is actually a flag that defines the beginning of the frame
- Destination address :contains address of the destination station or stations to receive the packet.
- Source address : address of the sender of the packet.
- Length or type: length field to define the number of bytes in the data field.
- Data/padding: This field carries data encapsulated. It is a minimum of 46 and a maximum of 1500 bytes. If its less than 46 bytes , it needs to be padded with extra 0's
- CRC: The last field contains error detection information

- Standard Ethernet- in the nomenclature 10 Base X

  Number defines the data rate(10Mbps)

  Base means baseband (digital) signal

  X defines maximum size of the cable

- The standard ethernet uses a baseband signal, which means that the bits are changed to digital signal and directly sent on the line
- All implementations use a Manchester Encoding
  - Ethernet refers to the cable (the ether)
  - Four types of cabling are commonly used

max length

Name	Cable	Max. seg.	Nodes/seg.
10Base5	Thick coax	500 m	100
10Base2	Thin coax	185 m	30
10Base-T	Twisted pair	100 m	1024
10Base-F	Fiber optics	2000 m	1024

Fig: most common kinds of Ethernet cabling

✓ **10Base5 cabling**

- popularly called thick Ethernet
- resembles a yellow garden hose
- Connections to it are generally made using vampire taps.
- 10Base5 means that it operates at 10 Mbps, uses baseband signaling, and can support segments of up to 500 meters.

✓ **10Base2, or thin Ethernet**

- bends easily
- Connections to it are made using industry-standard BNC connectors to form T junctions
- Adv:
  - BNC connectors are easier to use and more reliable.
  - Thin Ethernet is much cheaper and easier to install
- Limitation:
  - it can run for only 185 meters per segment, each of which can handle only 30 machines.
- Major problem with 10Base5 & 10Base2
  - Detecting cable breaks, excessive length, bad taps, or loose connectors is difficult

✓ **10Base-T**

- Problems associated with finding cable breaks introduced different kind of wiring pattern, in which all stations have a cable running to a central hub where they are all connected electrically
- these wires are telephone company twisted pairs

✓ **10Base-F**

- Uses fiber optics
- Expensive
- Excellent noise immunity
- Offers good security

Two kinds of Ethernet exist:

Classic Ethernet : Classic Ethernet is the original form and ran at rates from 3 to 10 Mbps

Switched Ethernet :

- Devices called switches are used to connect different computers. Switched Ethernet is runs at 100, 1000, and 10,000 Mbps, in forms called fast Ethernet, gigabit Ethernet, and 10 gigabit Ethernet.

2. Fast Ethernet

- 100 Mbps speed
- Traditional ethernet can operate only upto 10Mbps
- Hence for higher data rates, fast ethernet has been developed
- In the evolution of ethernet, care has been taken to keep the MAC sublayer untouched.
- Frame format is remain untouched. Same as that of Traditional ethernet
- max & min frame length also remain untouched

3. Gigabit Ethernet (1 Gbps)

- Support the data rates upto 1000 Mbps
- IEEE calls the standard 802.3z
- The goals of gigabit ethernet were to upgrade the data rate to 1 Gbps,use the same frame format, keep the same min and max frame length etc
- Operating in either half duplex or full duplex modes , almost follow full duplex ,in full duplex mode of Gigabit there is no collision

Name	Cable	Max. segment
1000Base-SX	Fiber optics	550 m
1000Base-LX	Fiber optics	5000 m
1000Base-CX	2 Pairs of STP	25 m
1000Base-T	4 Pairs of UTP	100 m

Fig: Gigabit Ethernet cabling.

4. 10 Gigabit Ethernet (10 Gbps)

- Maximum data rate is 10 Gbps
- IEEE created and called it standard 802.3ae
- Used in LAN,MAN,WAN
- The goals of gigabit ethernet were to use the same frame format, keep the same min and max frame length etc
- Use fiber-optic technology
- Most common 4 implementations are 10GBase –S, 10GBase –L, 10GBase –E, 10GBase –X4

Manchester Encoding - introduction

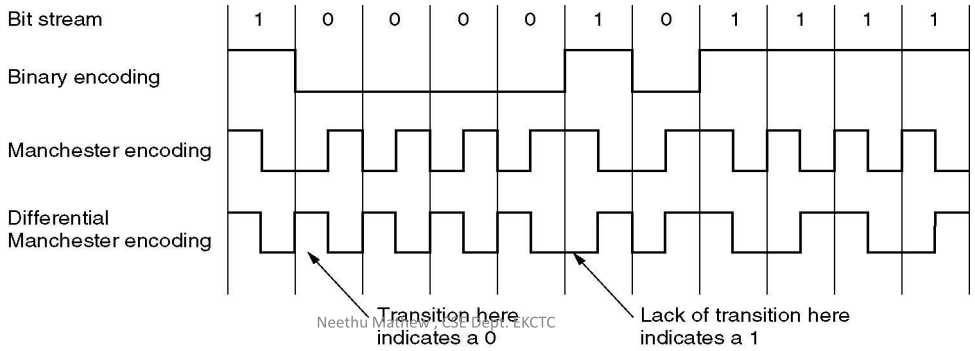
- None of the versions of Ethernet uses straight binary encoding with 0 volts for a 0 bit and 5 volts for a 1 bit because it leads to ambiguities (uncertainty).
- If one station sends the bit string 0001000, others might falsely interpret it as 10000000 or 01000000 because they cannot tell the difference between an idle sender (0 volts) and a 0 bit (0 volts). This problem can be solved by using +1 volts for a 1 & -1 volts for a 0, but there is still the problem of a receiver sampling the signal at a slightly different frequency than the sender used to generate it.

- A way is needed for receivers to unambiguously determine the start, end, or middle of each bit without reference to an external clock.

Two such approaches

- **Manchester encoding**
- **differential Manchester encoding.**

- **Manchester encoding**
  - each bit period is divided into two equal intervals.
  - A binary 1 bit is sent by having the voltage set high during the first interval and low in the second one.
  - A binary 0 is just the reverse: first low and then high.
  - This scheme ensures that every bit period has a transition in the middle, making it easy for the receiver to synchronize with the sender.
- A disadvantage of Manchester encoding
  - it requires twice as much bandwidth as straight binary encoding because the pulses are half the width.
  - For example, to send data at 10 Mbps, the signal has to change 20 million times/sec.
- Manchester encoding is shown below



- **Differential Manchester encoding**
  - A variation of basic Manchester encoding.
  - A 1 bit is indicated by the absence of a transition at the start of the interval.
  - A 0 bit is indicated by the presence of a transition at the start of the interval.
  - In both cases, there is a transition in the middle as well.
  - Disadv: requires more complex equipment
  - Adv: offers better noise immunity.
- All Ethernet systems use Manchester encoding due to its simplicity.
- The high signal is + 0.85 volts and the low signal is - 0.85 volts, giving a DC value of 0 volts.
- Ethernet does not use differential Manchester encoding
- but other LANs (e.g., the 802.5 token ring) do use it.

Wired LAN - 802.11

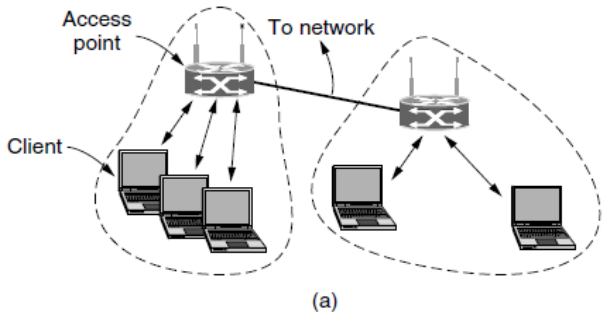
(802.11 protocol stack, Physical layer, MAC Sublayer protocol, Frame structure.)

- IEEE has defined the specification for a wireless LAN , called IEEE 802.11 ,which covers the physical & data link layers
- the public uses the term WiFi (short for wireless fidelity) as a synonym for wireless LAN.

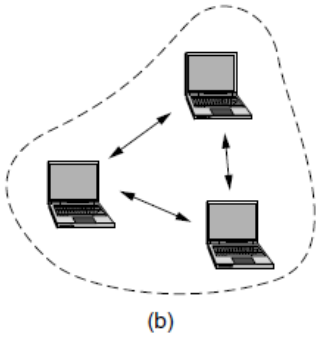
802.11 Architecture

- operate in one of two configurations : Infrastructure mode & Ad-hoc mode.
  - **Infrastructure mode** –
    - The most popular mode is to connect clients, such as laptops and smart phones, to another network, such as a company intranet or the Internet.
    - In infrastructure mode, each client is associated with an Access Point - AP (central base station) that is in turn connected to the other network. The client sends and receives its packets via the AP. Several access points may be connected together, typically by a wired network called a distribution system, to form an extended 802.11 network. In this case, clients can send frames to other clients via their APs.
  - **Ad hoc mode** - This mode is a collection of computers that are associated so that they can directly send frames to each other. There is no access point (AP)

Neethu Mathew , CSE Dept. EKCTC



infrastructure mode

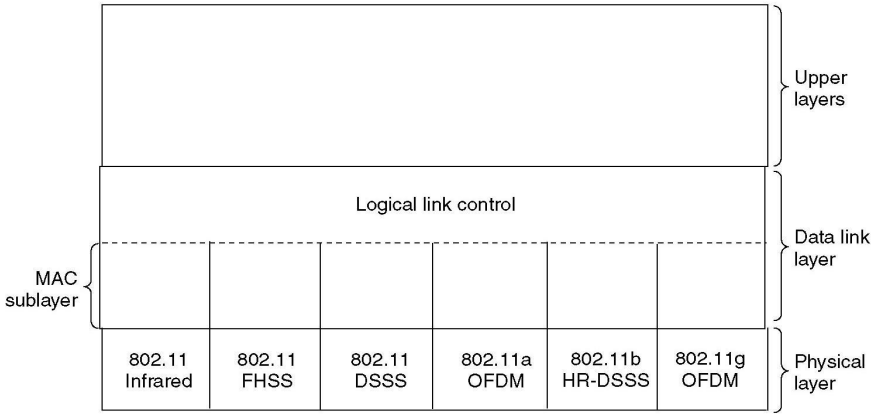


Ad hoc mode

- The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS)
- A BSS is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP). The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture. A BSS with an AP referred to as an infrastructure BSS
- 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

802.11 protocol stack

A partial view of the 802.11 protocol stack is given



- The physical layer corresponds to the OSI physical layer.
- The data link layer in all the 802 protocols is split into two or more sublayers.
- In 802.11, the MAC (Medium Access Control) sublayer determines how the channel is allocated, that is, who gets to transmit next.
- Above it is the LLC (Logical Link Control) sublayer, whose job it is to hide the differences between the different 802 variants and make them indistinguishable as far as the network layer is concerned.

802.11 Physical Layer

- The 802.11 standard specifies 3 transmission techniques allowed in the physical layer.

1) Infrared method

- This method uses much the same technology as television remote controls do.
- The infrared option uses diffused (i.e., not line of sight) transmission at 0.85 or 0.95 microns.
- Two speeds are permitted: 1 Mbps and 2 Mbps

2) short-range radio Method

- using techniques called FHSS and DSSS
- Both of these (FHSS and DSSS) use a part of the spectrum that does not require licensing (the 2.4-GHz ISM band).

a) FHSS (Frequency Hopping Spread Spectrum)

- uses 79 channels, each 1-MHz wide, starting at the low end of the 2.4-GHz ISM (Industrial, Scientific, Medical) band.
- A pseudorandom number generator is used to produce the sequence of frequencies hopped to.

b) DSSS (Direct Sequence Spread Spectrum), is also restricted to 1 or 2 Mbps.

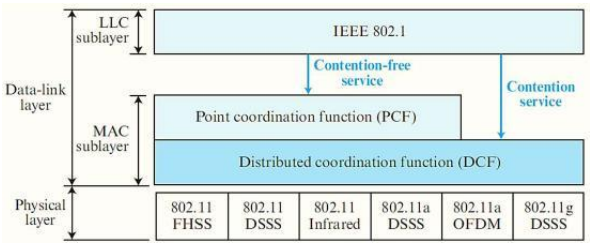
- The scheme used has some similarities to the CDMA (Code Division Multiple Access) system.
- Each bit is transmitted as 11 chips, using what is called a Barker Sequence.

3) Higher bandwidth method

- **a) 802.11a**, OFDM (Orthogonal Frequency Division Multiplexing) is used to deliver up to 54 Mbps in the wider 5 GHz ISM band. Splitting the signal into many narrow bands has some key advantages over using a single wide band, including better immunity to narrowband interference
- **b) 802.11b**, HR-DSSS (High Rate Direct Sequence Spread Spectrum) uses 11 million chips/sec to achieve 11 Mbps in the 2.4- GHz band. Although 802.11b is slower than 802.11a, its range is about 7 times greater, which is more important in many situations
- **c) 802.11g** is an enhanced version of 802.11b. It uses the OFDM (Orthogonal Frequency Division Multiplexing) modulation method of 802.11a but operates in the narrow 2.4-GHz ISM band along with 802.11b. In theory it can operate at up to 54 Mbps. It is not yet clear whether this speed will be realized in practice.

802.11 MAC Sublayer Protocol

- IEEE 802.11 defines two MAC sublayers:
  - Distributed Coordination Function (DCF)
  - Point Coordination Function (PCF)



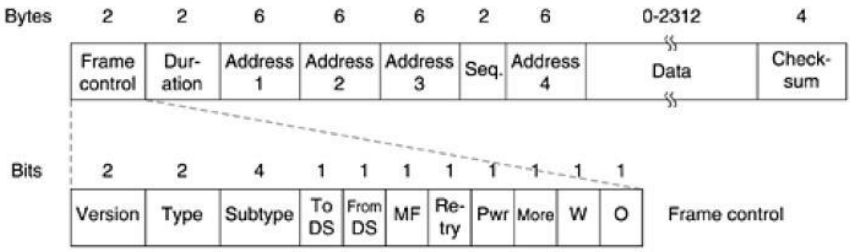
Distributed Coordination Function(DCF)

- It is a protocol defined by IEEE at the MAC sublayer
- DCF uses CSMA/CA as the access method

Point Coordination Function (PCF)

- The point coordination function (PCF) is an optional access method that can be implemented in an infrastructure network (not in an ad hoc network).
- It is implemented on top of DCF & is used mostly for time-sensitive transmission.
- PCF has a centralized, contention-free polling access method.
- The AP performs polling for stations that are capable of being polled. The stations are polled one after another, sending any data they have to the AP.

802.11 Frame Structure



The MAC layer frame consist of 9 fields as shown in figure.

- **Frame Control (FC) field:**
  - It defines the type of frame & some control information
  - It has 11 subfields.
  - first - the Protocol version, which allows two versions of the protocol to operate at the same time in the same cell.

- Then come the Type (data, control, or management) and Subtype fields (e.g., RTS or CTS).
- To DS and From DS bits indicate the frame is going to or coming from the intercell distribution system (e.g., Ethernet).
- MF(more flag) bit means that more fragments .
- Retry bit marks a retransmission of a frame sent earlier.
- pwr: power management mode: The Power management bit is used by the base station to put the receiver into sleep state or take it out of sleep state.
- More bit indicates that the sender has more data to send
- W bit specifies that the frame body has been encrypted using the WEP (Wired Equivalent Privacy) algorithm.
- Finally, the O bit tells the receiver that a sequence of frames with this bit on must be processed strictly in order.

- **Duration field (D):** defines the duration of the transmission that is used to set the value of NAV (network allocation vector -used for collision avoidance).
- **Addresses :** contains 4 addresses. The meaning of each address field depend on value of To DS & From DS subfields
- **Sequence field :** allows fragments to be numbered. It defines the sequence number of the frame
- **Data**
- **Checksum :** error detection

Bridges

- Multiple LANs can be connected by devices called bridges. ie, Bridges connect two or more LANs
- A bridge operates at data link layer
- It has a single input and single output port, thus making it a 2 port device.
- Bridges examine the data layer link addresses to do routing. Since they are not supposed to examine the payload field of the frames they route, they can transport any kinds of packets.
- Bridge performs filtering. Bridge can check the destination address and decide whether the packet is to be forwarded or dropped.
- Bridges are of four types:

1. routing bridges / source routing bridges
2. transparent bridges
3. Spanning Tree Bridges
4. Remote bridges

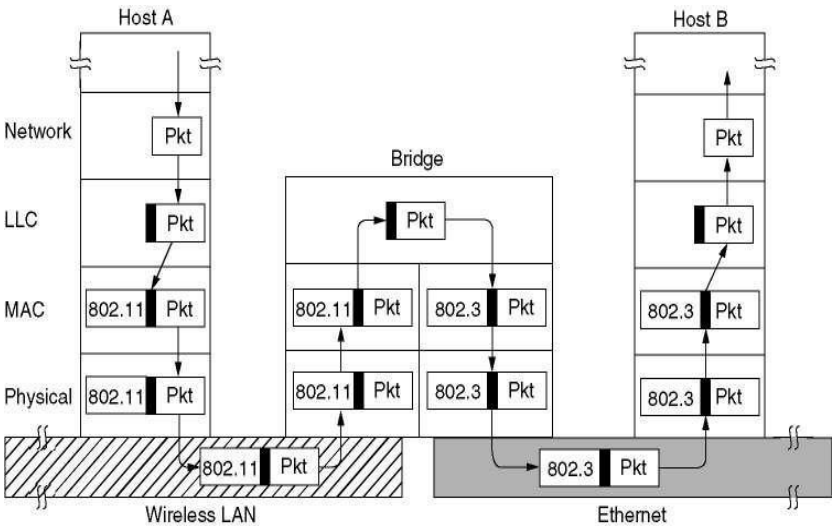
- A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination.
- It is also used for interconnecting two LANs working on the same protocol.

Why bridges?

- By joining multiple LAN ,bridges help in multiplying network capacity of a single LAN
- the organization may be geographically spread over several buildings separated by considerable distances. It may be cheaper to have separate LANs in each building and connect them with bridges.
- it may be necessary to split what is logically a single LAN into separate LANs to accommodate the load.
- Using bridges, the total physical distance covered can be increased.
- there is the matter of reliability.
- bridges can contribute to the organization's security

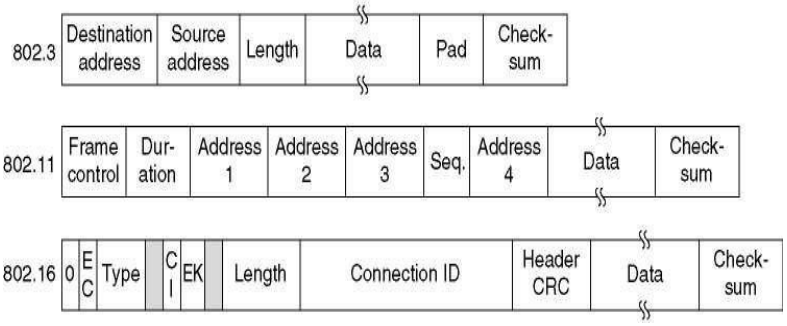
Bridges from 802.x to 802.y

- Bridges are a data link layer device and can connect to different networks as well as connect different networks of different types.
- Bridges from 802.x to 802.y where x & y may both be Ethernet or one can be Ethernet and other may be a token ring, etc.
- Following figure illustrates the operation of a simple two-port bridge.
- Host A on a wireless (802.11) LAN has a packet to send to a fixed host, B, on an (802.3) Ethernet to which the wireless LAN is connected.
- Note that a bridge connecting k different LANs will have k different MAC sublayers and k different physical layers, one for each type.



Operation of a LAN bridge from 802.11 to 802.3.

- There are many difficulties that one encounters when trying to build a bridge between the various 802 LANs (and MANs)
- Each of the LANs uses a different frame format



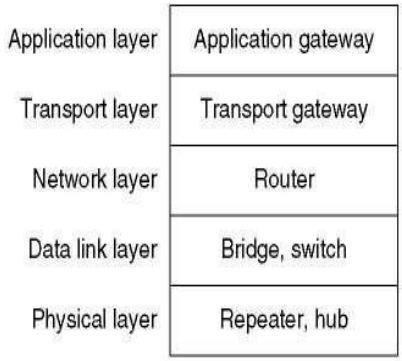
The IEEE 802 frame formats.
The drawing is not to scale.

Some problems are :

- data rate problem
- different 802 LANs have different maximum frame lengths.
- security problem
- Frame format
- Bit order
- quality of service.

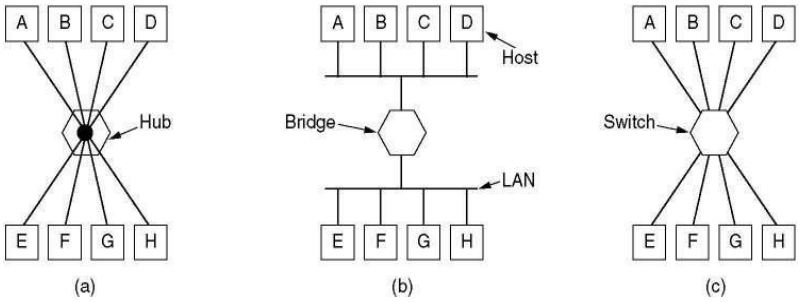
Repeaters, Hubs, Bridges, Switches, Routers and Gateways

These devices operate in different layers



(a)

Which device is in which layer.



hub bridge. switch.

Switches

- Switch is data link layer device.
- Switch act as multiport bridge to connect devices in LAN
- A switch is a device which provides bridging functionality with greater efficiency
- Switches are similar to bridges in that both route on frame addresses.
- In fact, many people uses the terms interchangeably. The main difference is that a switch is most often used to connect individual computers, as shown in Fig. (c).
- A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number of ports imply less traffic) and performance.
- Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.
- 2 Types-
  - 2 layer switch : it's a bridge with many ports. It performs at physical & data link layer
  - 3 layer switch : used at network layer

Repeater

- Network device
- A repeater operates at the physical layer.
- Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.
- repeaters do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.
- It is a 2 port device.

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. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.
- 3 types : active, passive,intelligent

Router:

- Router is mainly a Network Layer device.
- A router is a device like a switch that routes data packets based on their IP addresses.
- Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets.
- Router divide broadcast domains of hosts connected through it.
- When a packet comes into a router, the frame header and trailer are stripped off and the packet located in the frame's payload field is passed to the routing software. This software uses the packet header to choose an output line.

Gateway

- A gateway, is a passage to connect two networks together that may work upon different networking models.
- They 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 and can operate at any network layer.
- Gateways are generally more complex than switch or router.
- Transport gateways connect two computers that use different connection – oriented transport protocols. The transport gateway can copy the packets from one connection to the other, reformatting them as need be.
- Application gateways understand the format and contents of the data and translate messages from one format to another.