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.

DATA LINK LAYER DESIGN ISSUES

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

1. Providing a well-defined service interface to the network layer.
2. Dealing with transmission errors.
3. Regulating the flow of data

To accomplish these goals, the data link layer takes the packets it gets from the network layer and encapsulates them into **frames** for transmission. Each frame contains a frame header, a payload field for holding the packet, and a frame trailer.

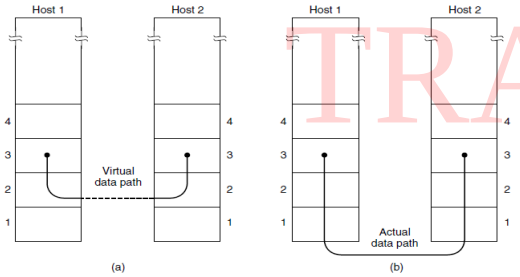
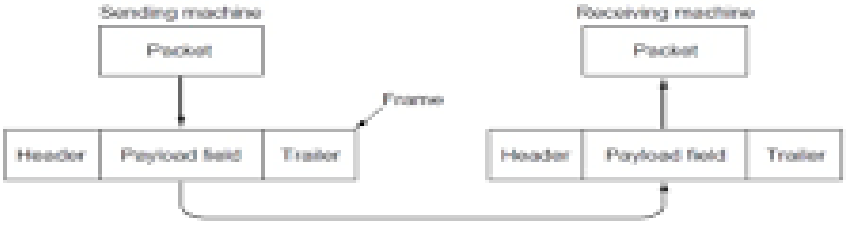


Figure 3-2. (a) Virtual communication. (b) Actual communication.

Packets and Frames

Relationship between packets and frames.



Services Provided to the Network Layer

The function of the data link layer is to provide services to the network layer. The principal service is transferring data from the network layer on the source machine to the network layer on the destination machine. The job of the data link layer is to transmit the bits to the destination machine so they can be handed over to the network layer.

The data link layer can be designed to offer various services.

1. Unacknowledged connectionless service.
2. Acknowledged connectionless service.
3. Acknowledged connection-oriented service.

Unacknowledged connectionless service consists of having the source machine send independent frames to the destination machine without having the destination machine acknowledge them. Ethernet is a good example of a data link layer that provides this class of service. No logical connection is established. If a frame is lost due to noise on the line, no attempt is made to detect the loss or recover from it in the data link layer.

The next step up in terms of reliability is acknowledged connectionless service. When this service is offered, there are still no logical connections used, but each frame sent is individually acknowledged. In this way, the sender knows whether a frame has arrived correctly or been lost. If it has not arrived within a specified time interval, it can be sent again. This service is useful over unreliable channels, such as wireless systems. 802.11 (WiFi) is a good example of this class of service.

The most sophisticated service the data link layer can provide to the network layer is connection-oriented service. With this service, the source and destination machines establish a connection before any data are transferred. Each frame sent over the connection is numbered, and the data link layer guarantees that each frame sent is indeed received. Furthermore, it guarantees that each frame is received exactly once and that all frames are received in the right order. Connection-oriented service thus provides the network layer processes with the equivalent of a reliable bit stream. It is appropriate over long, unreliable links such as a satellite channel or a long-distance telephone circuit.

Framing

The data link layer breaks up the bit stream into discrete frames, compute a short token called a checksum for each frame, and include the checksum in the frame when it is transmitted. When a frame arrives at the destination, the checksum is recomputed. If the newly computed checksum is different from the one contained in the frame, the data link layer knows that an error has occurred and takes steps to deal with it (e.g., discarding the bad frame and possibly also sending back an error report).

A good design must make it easy for a receiver to find the start of new frames while using little of the channel bandwidth. The four methods are:

1. Byte count.(Charcter count)
2. Flag bytes with byte stuffing.
3. Flag bits with bit stuffing.

Byte count

The first framing method uses a field in the header to specify the number of bytes in the frame. When the data link layer at the destination sees the byte count, it knows how many bytes follow and hence where the end of the frame is.The trouble with this algorithm is that the count can be changed by a transmission error. As a result the destination will get out of synchronization. It will then be unable to locate the correct start of the next frame.

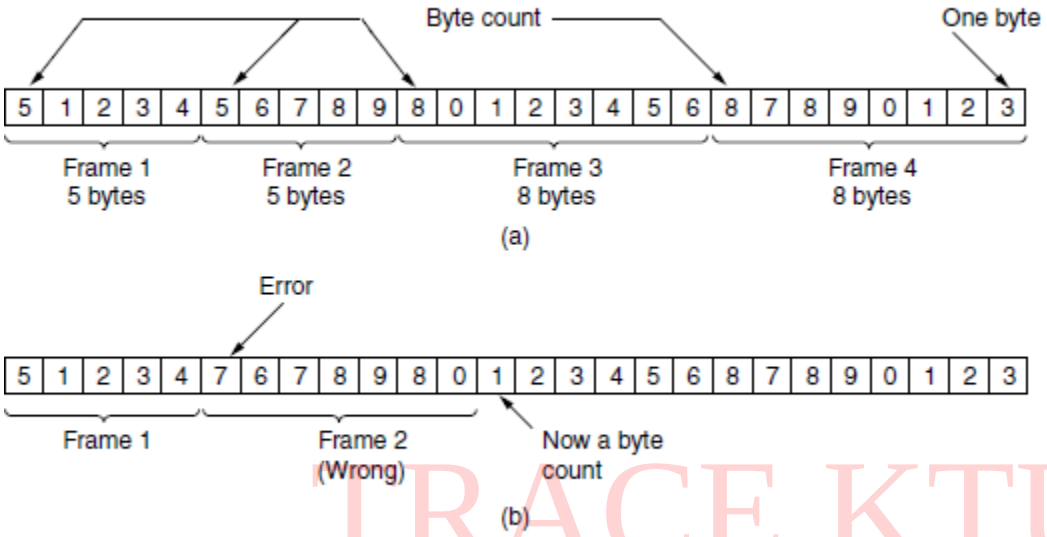
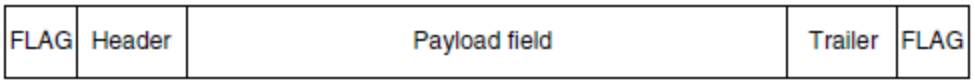


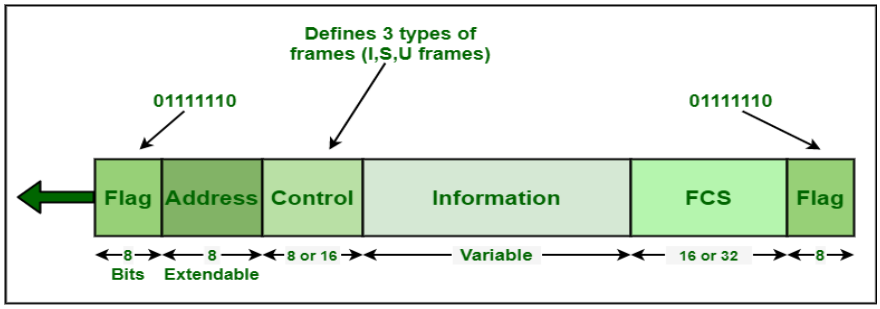
Figure 3-3. A byte stream. (a) Without errors. (b) With one error.

Byte stuffing

The second framing method gets around the problem of resynchronization after an error by having each frame start and end with special bytes. Often the same byte, called a **flag byte**, is used as both the starting and ending delimiter. Two consecutive flag bytes indicate the end of one frame and the start of the next. Thus, if the receiver ever loses synchronization it can just search for two flag bytes to find the end of the current frame and the start of the next frame.



HDLC (**Highlevel Data Link Control**) protocol



Basic Frame Structure

Flag(01111110)- Beginning and ending sequence
Address- identify the destination
Control-used for sequence numbers, ACKs etc
Information- Data to send
FCS(Checksum)- Error detection

Each frame begins and ends with a special bit pattern, 01111110 or 0x7E in hexadecimal. This pattern is a flag byte. Whenever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a 0 bit into the outgoing bit stream. It also ensures a minimum density of transitions that help the physical layer maintain synchronization.

When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit,it automatically destuffs (i.e., deletes) the 0 bit. Just as byte stuffing is completely transparent to the network layer in both computers, so is bit stuffing. If the user data contain the flag pattern, 01111110, this flag is transmitted as 011111010 but stored in the receiver's memory as 01111110.

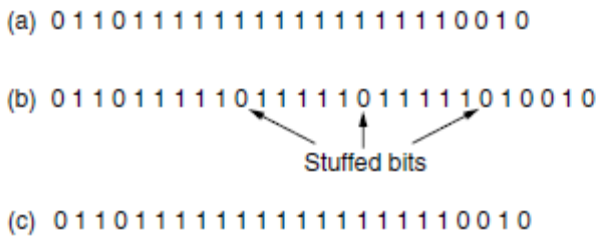


Figure 3-5. Bit stuffing. (a) The original data. (b) The data as they appear on the line. (c) The data as they are stored in the receiver's memory after destuffing.

The last method of framing is to use a shortcut from the physical layer. It is easy to find the start and end of frames and there is no need to stuff the data.

ERROR CONTROL

To ensure reliable delivery of data

- Use ACKs for reliable connections. Two ACKs positive and negative ACKs. For correct delivery positive ACK is used and incorrect delivery negative ACK is used.

- If there is a hardware failure, the sender will wait indefinitely for the ACKs. To avoid that timers are used.
- When the sender transmits a frame, it generally also starts a timer. The timer is set to expire after an interval long enough for the frame to reach the destination, be processed there, and have the acknowledgement propagate back to the sender.

FLOW CONTROL

Flow problem occurs if a sender that systematically wants to transmit frames faster than the receiver can accept them. This situation can occur when the sender is running on a fast, powerful computer and the receiver is running on a slow, low-end machine.

Two approaches are commonly used.

feedback-based flow control, the 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.

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

ERROR CORRECTION

Error Correction codes are used to detect and correct the errors when data is transmitted from the sender to the receiver.

Error Correction can be handled in two ways:

- **Backward error correction:** Once the error is discovered, the receiver requests the sender to retransmit the entire data unit.
- **Forward error correction:** In this case, the receiver uses the error-correcting code which automatically corrects the errors.

A single additional bit can detect the error, but cannot correct it.

For correcting the errors, one has to know the exact position of the error. For example, If we want to calculate a single-bit error, the error correction code will determine which one of seven bits is in error. To achieve this, we have to add some additional redundant bits.

Suppose r is the number of redundant bits and d is the total number of the data bits. The number of redundant bits r can be calculated by using the formula:

$2^r >= d+r+1$

The value of r is calculated by using the above formula. For example, if the value of d is 4, then the possible smallest value that satisfies the above relation would be 3.

To determine the position of the bit which is in error, a technique developed by R.W Hamming is Hamming code which can be applied to any length of the data unit and uses the relationship between data units and redundant units.

Hamming Code

Parity bits: The bit which is appended to the original data of binary bits so that the total number of 1s is even or odd.

Even parity: To check for even parity, if the total number of 1s is even, then the value of the parity bit is 0. If the total number of 1s occurrences is odd, then the value of the parity bit is 1.

Odd Parity: To check for odd parity, if the total number of 1s is even, then the value of parity bit is 1. If the total number of 1s is odd, then the value of parity bit is 0.

Algorithm of Hamming code:

- An information of 'd' bits are added to the redundant bits 'r' to form d+r.
- The location of each of the (d+r) digits is assigned a decimal value.
- The 'r' bits are placed in the positions 1,2,.....2^{k-1}.
- At the receiving end, the parity bits are recalculated. The decimal value of the parity bits determines the position of an error.

Total number of data bits 'd' = 4

Number of redundant bits r : $2^r >= d+r+1$

$2^r >= 4+r+1$

Therefore, the value of r is 3 that satisfies the above relation.

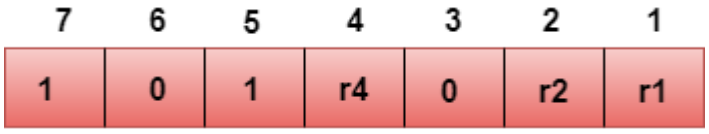
Total number of bits = d+r = 4+3 = 7;

- Determining the position of the redundant bits

The number of redundant bits is 3. The three bits are represented by r1, r2, r4. The position of the redundant bits is calculated with corresponds to the raised power of 2. Therefore, their corresponding positions are **1, 2^1, 2^2**.

1. The position of r1 = 1
2. The position of r2 = 2
3. The position of r4 = 4

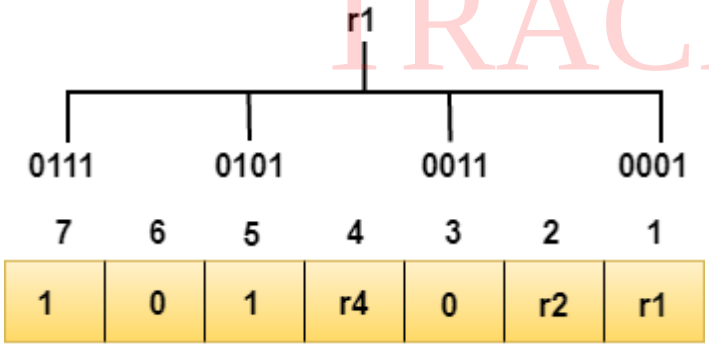
Representation of Data on the addition of parity bits:



- Determining the Parity bits

Determining the r1 bit

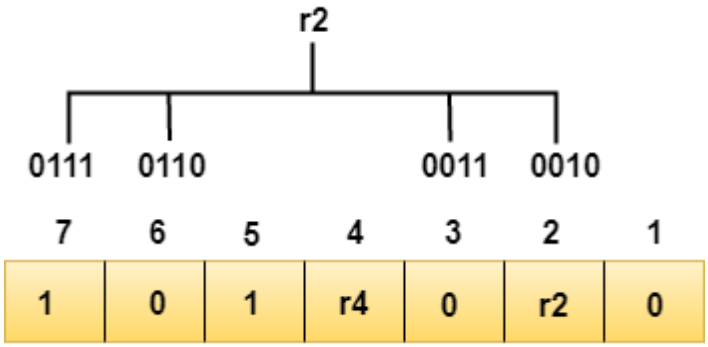
The r1 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the first position.



We observe from the above figure that the bit positions that includes 1 in the first position are 1, 3, 5, 7. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r1 is **even, therefore, the value of the r1 bit is 0**.

Determining r2 bit

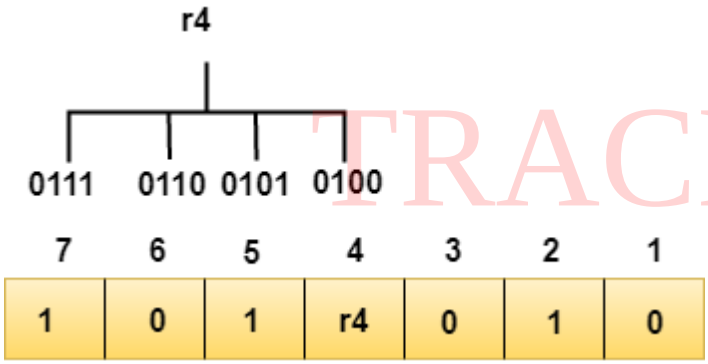
The r2 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the second position.



We observe from the above figure that the bit positions that includes 1 in the second position are **2, 3, 6, 7**. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r2 is **odd, therefore, the value of the r2 bit is 1**.

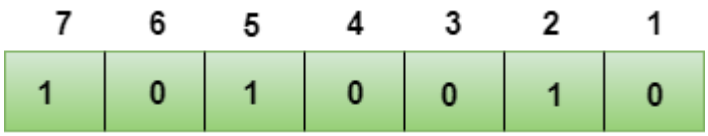
Determining r4 bit

The r4 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the third position.



We observe from the above figure that the bit positions that includes 1 in the third position are **4, 5, 6, 7**. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r4 is **even, therefore, the value of the r4 bit is 0**.

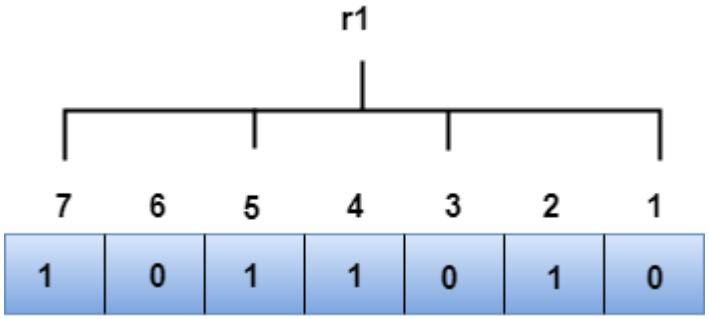
Data transferred is given below:



Suppose the 4th bit is changed from 0 to 1 at the receiving end, then parity bits are recalculated.

R1 bit

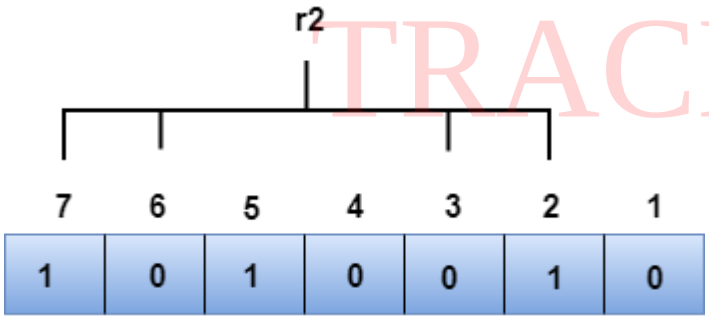
The bit positions of the r1 bit are 1,3,5,7



We observe from the above figure that the binary representation of r1 is 1100. Now, we perform the even-parity check, the total number of 1s appearing in the r1 bit is an even number. Therefore, the value of r1 is 0.

R2 bit

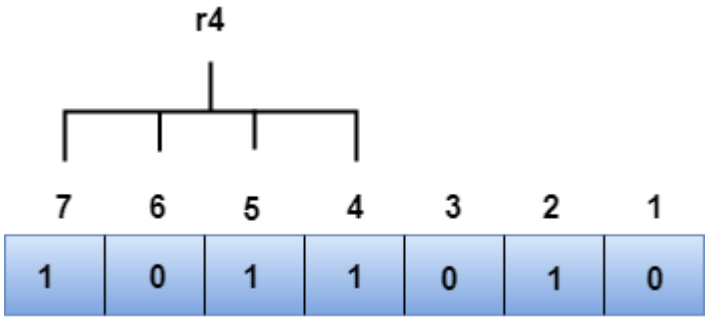
The bit positions of r2 bit are 2,3,6,7.



We observe from the above figure that the binary representation of r2 is 1001. Now, we perform the even-parity check, the total number of 1s appearing in the r2 bit is an even number. Therefore, the value of r2 is 0.

R4 bit

The bit positions of r4 bit are 4,5,6,7.



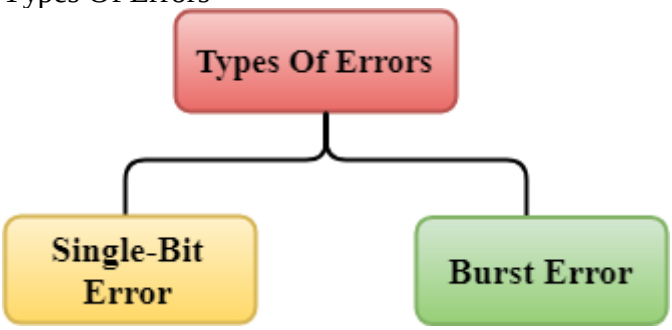
We observe from the above figure that the binary representation of r4 is 1011. Now, we perform the even-parity check, the total number of 1s appearing in the r4 bit is an odd number. Therefore, the value of r4 is 1.

- *The binary representation of redundant bits, i.e., r4r2r1 is 100, and its corresponding decimal value is 4. Therefore, the error occurs in a 4th bit position. The bit value must be changed from 1 to 0 to correct the error.*

ERROR DETECTION

When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device. An Error is a situation when the message received at the receiver end is not identical to the message transmitted.

Types Of Errors

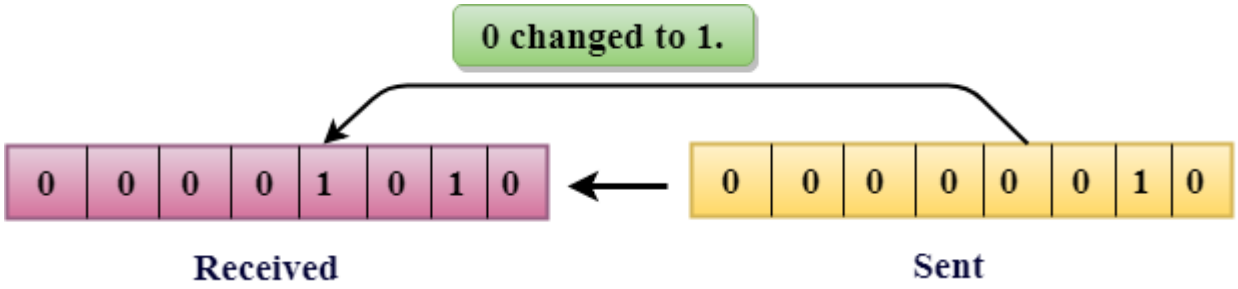


Errors can be classified into two categories:

- Single-Bit Error
- Burst Error

Single-Bit Error:

The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



In the above figure, the message which is sent is corrupted as single-bit, i.e., 0 bit is changed to 1.

Single-Bit Error does not appear more likely in Serial Data Transmission. For example, Sender sends the data at 10 Mbps, this means that the bit lasts only for 1 ?s and for a single-bit error to occurred, a noise must be more than 1 ?s.

Single-Bit Error mainly occurs in Parallel Data Transmission. For example, if eight wires are used to send the eight bits of a byte, if one of the wire is noisy, then single-bit is corrupted per byte.

Burst Error:

The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.

Error Detecting Techniques:

- Checksum
- Cyclic redundancy check

Cyclic Redundancy Check (CRC)

CRC is a redundancy error technique used to determine the error.

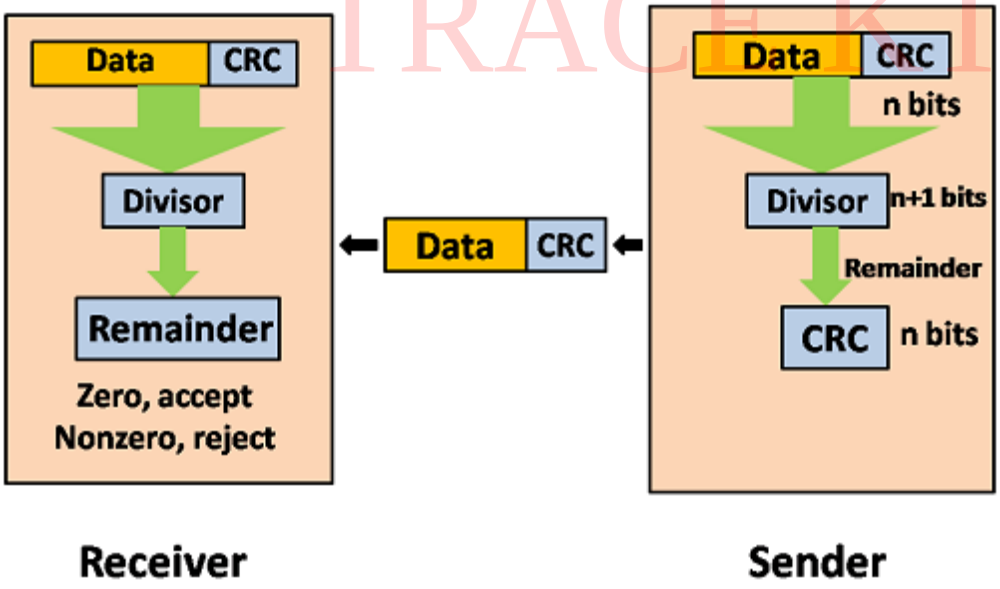
Following are the steps used in CRC for error detection:

- In CRC technique, a string of n 0s is appended to the data unit, and this n number is less than the number of bits in a predetermined number, known as division which is n+1 bits.

- Secondly, the newly extended data is divided by a divisor using a process is known as binary division. The remainder generated from this division is known as CRC remainder.
- Thirdly, the CRC remainder replaces the appended 0s at the end of the original data. This newly generated unit is sent to the receiver.
- The receiver receives the data followed by the CRC remainder. The receiver will treat this whole unit as a single unit, and it is divided by the same divisor that was used to find the CRC remainder.

If the resultant of this division is zero which means that it has no error, and the data is accepted.

If the resultant of this division is not zero which means that the data consists of an error. Therefore, the data is discarded.

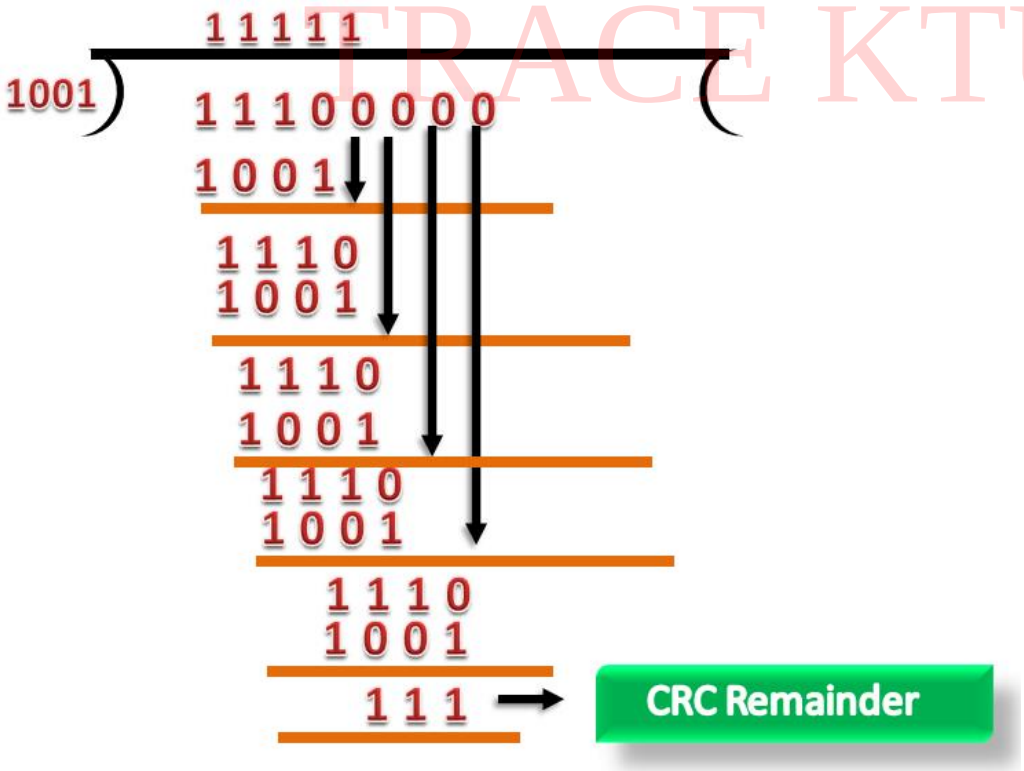


Let's understand this concept through an example:

Suppose the original data is 11100 and divisor is 1001.

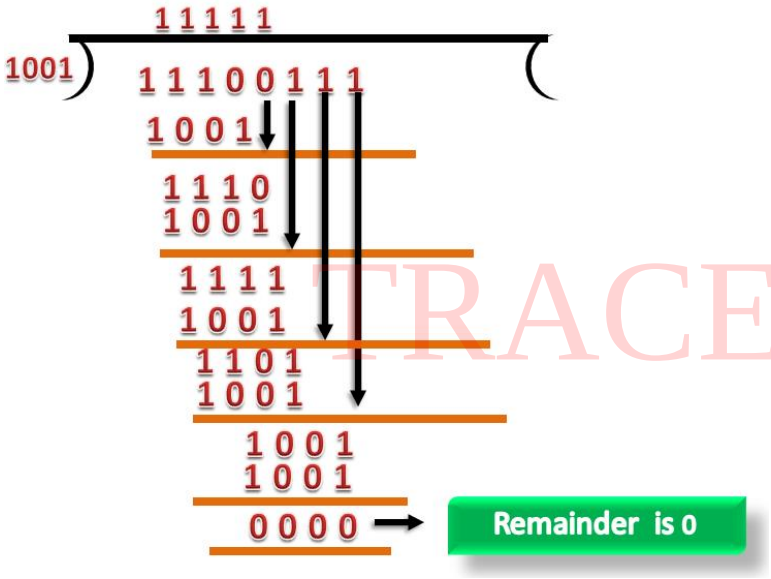
CRC Generator

- A CRC generator uses a modulo-2 division. Firstly, three zeroes are appended at the end of the data as the length of the divisor is 4 and we know that the length of the string 0s to be appended is always one less than the length of the divisor.
- Now, the string becomes 11100000, and the resultant string is divided by the divisor 1001.
- The remainder generated from the binary division is known as CRC remainder. The generated value of the CRC remainder is 111.
- CRC remainder replaces the appended string of 0s at the end of the data unit, and the final string would be 11100111 which is sent across the network.



CRC Checker

- The functionality of the CRC checker is similar to the CRC generator.
- When the string 11100111 is received at the receiving end, then CRC checker performs the modulo-2 division.
- A string is divided by the same divisor, i.e., 1001.
- In this case, CRC checker generates the remainder of zero. Therefore, the data is accepted.



Example 2

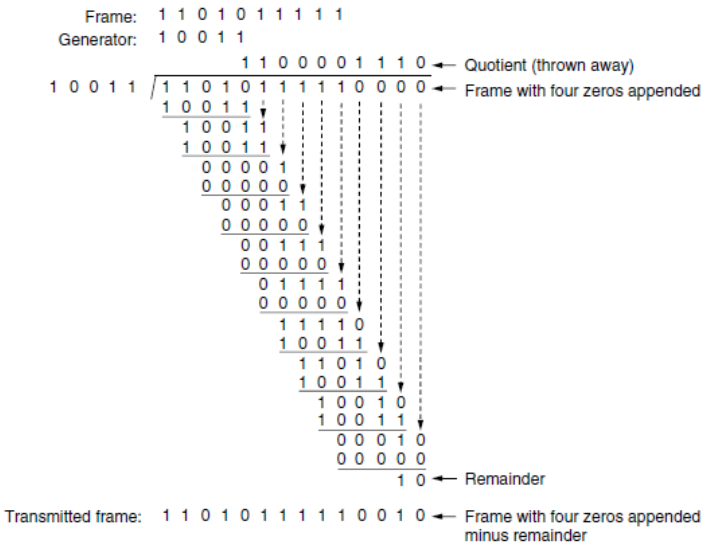
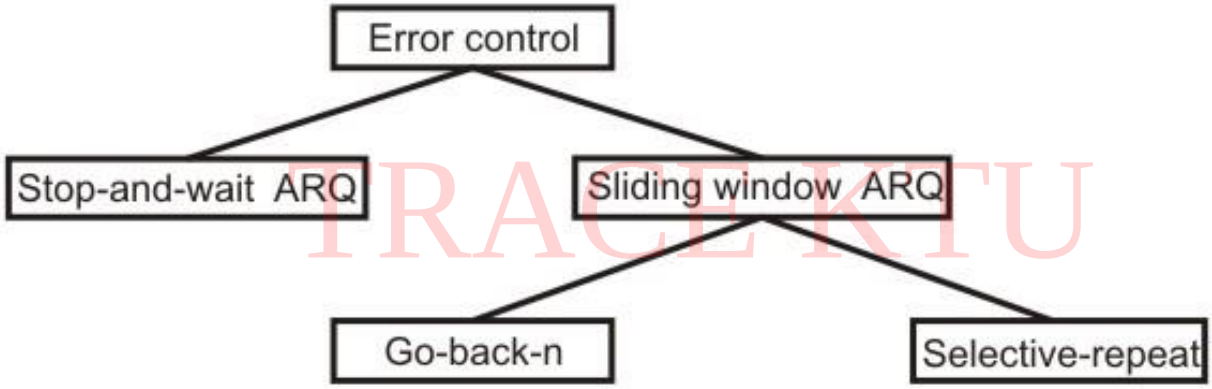


Figure 3-9. Example calculation of the CRC.



Stop and wait

- The simplest ARQ scheme is the stop-and-wait algorithm.
- The idea of stop-and-wait is:- After transmitting one frame, the sender waits for an acknowledgment before transmitting the next frame. If the acknowledgment does not arrive after a certain period of time, the sender times out and retransmit the original frame.

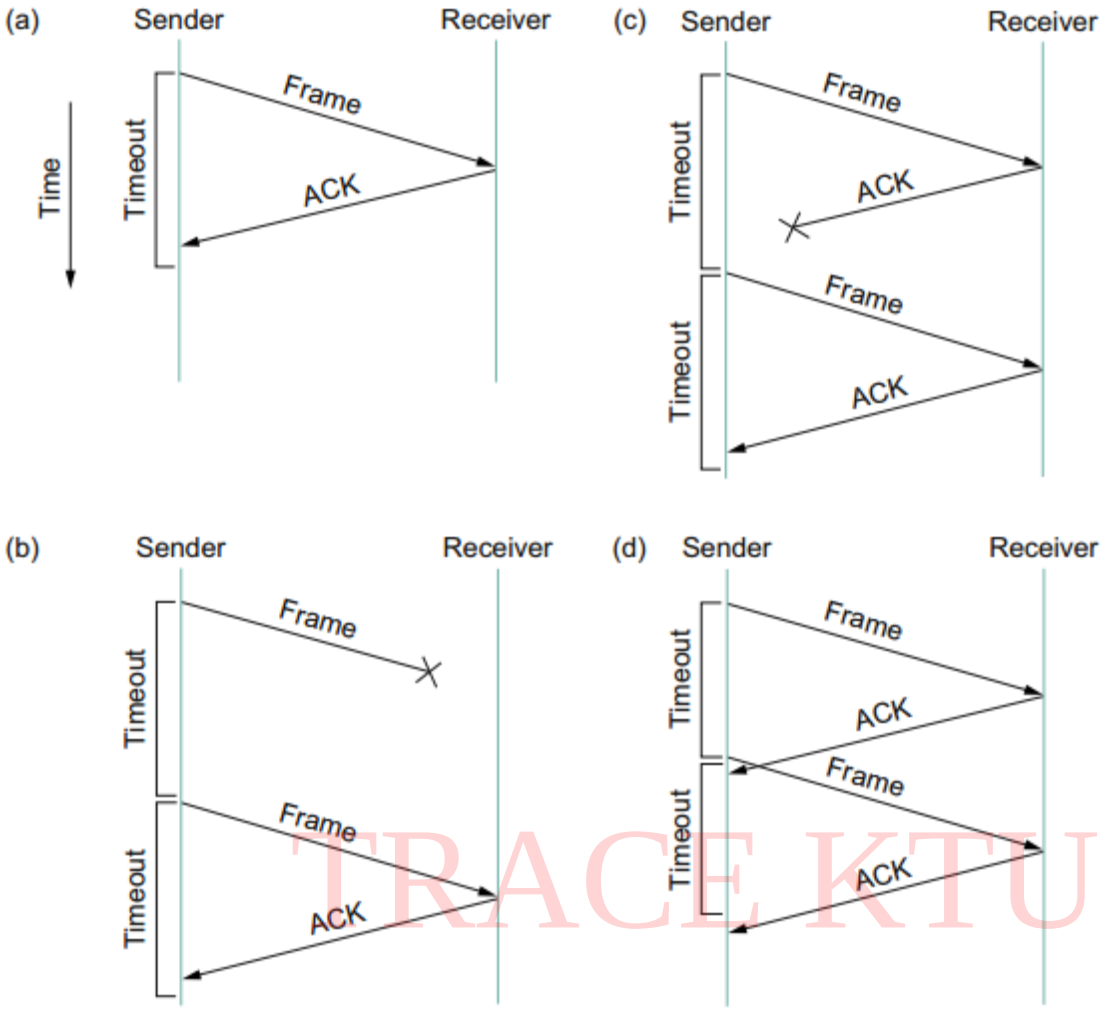
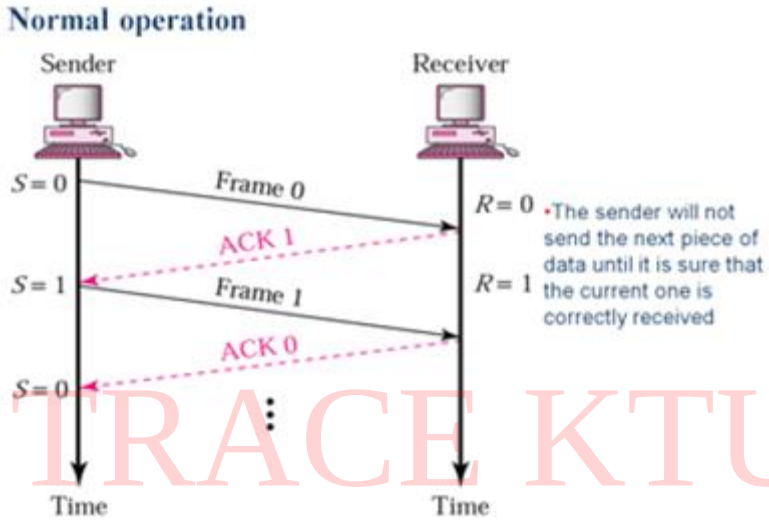


Fig (a) shows the simple ARQ mechanism. Fig (b) shows that the ACK is lost in between the transmission, here the sender will retransmit the data after timeout (**lost acknowledgement**). Here the receiver gets duplicate data frame. Fig (c) indicates **lost frame**. The sender will wait for an ACK, but after timeout it will resend the frame. Fig (d) shows **delayed acknowledgment**. The sender receives the ACK only after the timeout. But the sender will resend the frame before the delayed ACK, in this case also the receiver will get duplicate data frame.

In order to address the problem with lost ACK and delayed ACK, stop-and-wait protocol usually includes a 1-bit sequence number—that is, the sequence number can take on the values 0 and 1—and the sequence numbers used for each frame alternatively. (The protocol specifies that frames need to be numbered. This is done by using sequence numbers. A field is added to the data frame to hold the sequence number of that frame.)

When the sender retransmits frame 0, the receiver can determine that it is seeing a second copy of frame 0 rather than the first copy of frame 1 and therefore can ignore it (the receiver still acknowledges it, in case the first ACK was lost).

The acknowledgment numbers always announce the sequence number of the next frame expected by the receiver. For example, if frame 0 has arrived safe and sound, the receiver sends an ACK frame with acknowledgment 1 (meaning frame 1 is expected next). If frame 1 has arrived safe and sound, the receiver sends an ACK frame with acknowledgment 0 (meaning frame 0 is expected).



The main shortcoming of the stop-and-wait algorithm is that it allows the sender to have only one outstanding frame on the link at a time.

Sequence number

Frames from a sending station are numbered sequentially. However we need to include the sequence number of each frame in the header, we need to set a limit. If the header of the frame allows m bits for the sequence number, the sequence numbers range from 0 to 2^m - 1. For example, if m is 4, the only sequence numbers are 0 through 15 inclusive. However, we can repeat the sequence. So the sequence numbers are 0, 1,2,3,4,5,6, 7,8,9, 10, 11, 12, 13, 14, 15,0, 1,2,3,4,5,6,7,8,9,10, 11, ... In other words, the sequence numbers are modulo-2m.

SLIDING WINDOW PROTOCOL

The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol)

In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

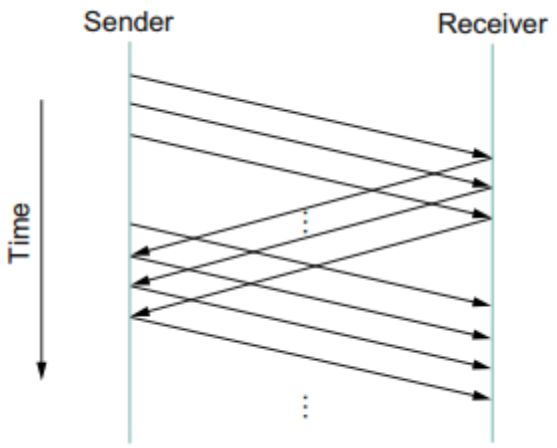
There is a finite size buffer on the **sender side** as well as on the **receiver side**. The buffer on the **sending side** is also known as **sending window** while the buffer on the **receiving side** is known as **receiving window**.

There is the specific size of the window, where the frames are numbered modulo- n, which simply means frames are numbered from **0 to n-1**. For e.g. if **n = 10**, the frames are numbered 0, 1,2,3,4,5,6, 7,8,9, 0, 1,2,3,4,5,6, 7, 8,9,0, 1, ….

Whenever the receiver sends an acknowledgment (ACK)it also includes the number of the next frame that it expects to receive. For example, in the order to acknowledge the group of frames that ends in frame 6, the receiver needs to send the ACK that contains the number 7. When the sender sees an ACK with the number 7, then the sender comes to know that all the frames up to number 6 have been successfully received.

Mainly the size of the sending window is used to determines the sequence number of the outbound frames.

- In this protocol (and the next), the sliding window is an abstract concept that defines the range of sequence numbers that is the concern of the sender and receiver. In other words, the sender and receiver need to deal with only part of the possible sequence numbers. The range which is the concern of the sender is called the send sliding window; the range that is the concern of the receiver is called the receiver sliding window.
- The send window is an imaginary box covering the sequence numbers of the data frames which can be in transit. In each window position, some of these sequence numbers define the frames that have been sent; others define those that can be sent. The maximum size of the window is $2^m - 1$

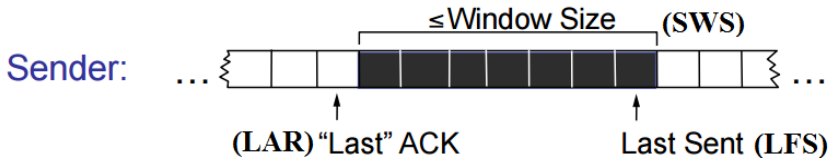


The sliding window algorithm works as follows. First, the sender assigns a sequence number, denoted **SeqNum**, to each frame. The sender maintains three variables:

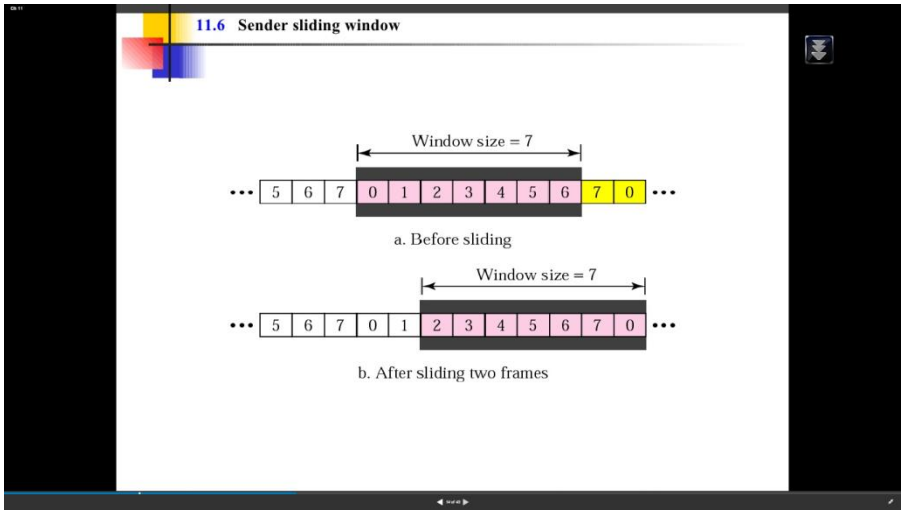
- The **send window size**, denoted **SWS**, gives the upper bound on the number of outstanding (unacknowledged) frames that the sender can transmit;
- **LAR** denotes the sequence number of the last acknowledgment received;
- **LFS** denotes the sequence number of the last frame sent.

The sender also maintains the following invariant:

$$LFS - LAR \leq SWS$$



When an acknowledgment arrives, the sender moves LAR to the right, thereby allowing the sender to transmit another frame. Also, the sender associates a timer with each frame it transmits, and it retransmits the frame should the timer expire before an ACK is received.

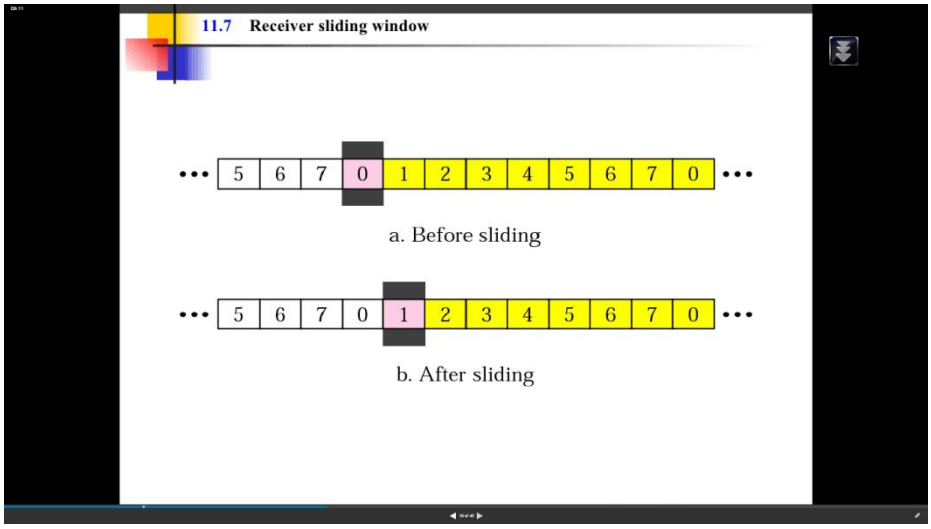


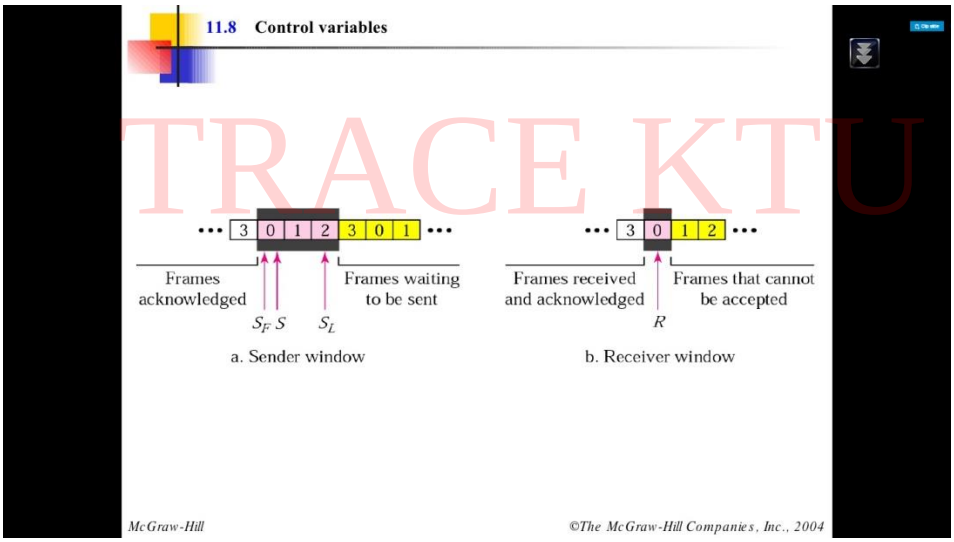
The receiver maintains the following three variables:

- The receive window size, denoted RWS, gives the upper bound on the number of out of-order frames that the receiver is willing to accept;
- LAF denotes the sequence number of the largest acceptable frame;
- LFR denotes the sequence number of the last frame received.

The receiver also maintains the following invariant:

$$LAF - LFR \leq RWS$$





When a frame with sequence number SeqNum arrives, the receiver takes the following action. If SeqNum ≤ LFR or SeqNum > LAF, then the frame is outside the receiver's window and it is discarded.

If LFR < SeqNum ≤ LAF, then the frame is within the receiver's window and it is accepted. Now the receiver needs to decide whether or not to send an ACK. Let SeqNumToAck denote the largest sequence number not yet acknowledged, such that all frames with sequence numbers less than or equal to SeqNumToAck have been received. The receiver acknowledges the receipt of SeqNumToAck, even

if higher numbered packets have been received. This acknowledgment is said to be cumulative. It then sets LFR = SeqNumToAck and adjusts LAF = LFR+RWS.

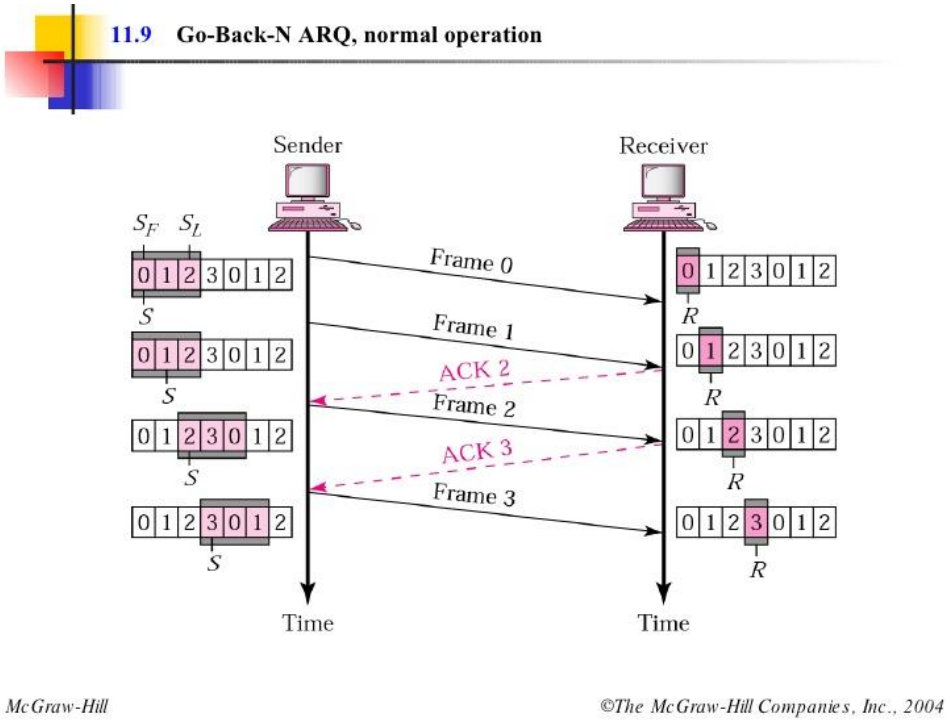
Types

Sliding window protocol has two types:

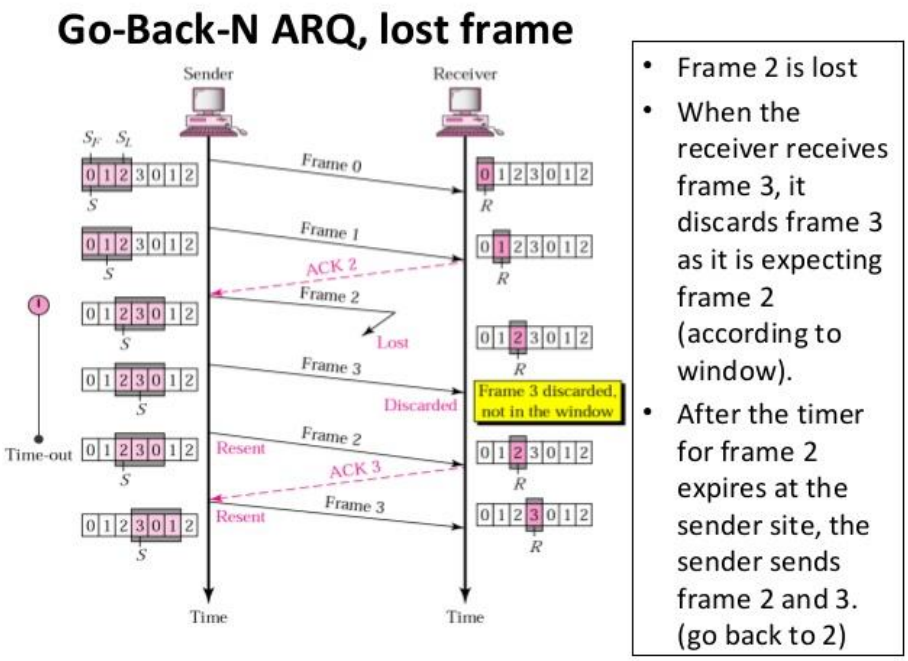
1. Go-Back-N ARQ
2. Selective Repeat ARQ

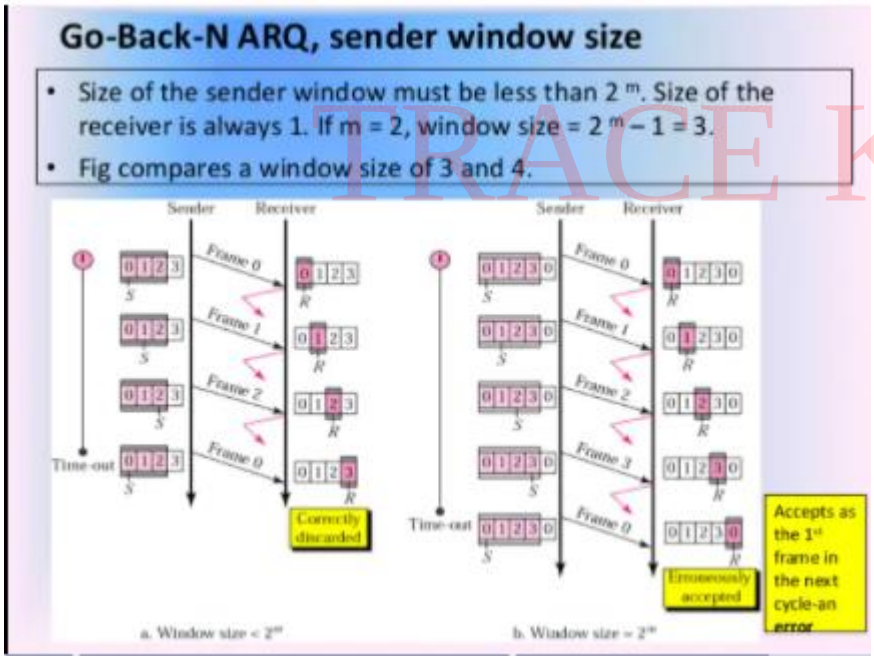
Go-Back-N Automatic Repeat Request

- To improve the efficiency of transmission (filling the pipe), multiple frames must be in transition while waiting for acknowledgment. In other words, we need to let more than one frame be outstanding to keep the channel busy while the sender is waiting for acknowledgment. In this protocol we can send several frames before receiving acknowledgments; we keep a copy of these frames until the acknowledgments arrive.
- In go-back-N ARQ the receiver window size is 1.
- It uses cumulative acknowledgement that is ACK N indicates that the receiver received N-1 frames and expecting N^{th} frame. Frames must be accepted in the order they were sent and Out of order packets are discarded.



As the receiver receives the frames, it keeps on sending ACKs or a NACK, in case a frame is incorrectly received. When the sender receives a NACK, it retransmits the frame in error plus all the succeeding frames. Hence, the name of the protocol is go-back-N ARQ. If a frame is lost, the receiver sends NAK after receiving the next frame. In case there is long delay before sending the NAK, the sender will resend the lost frame after its timer times out. If the ACK frame sent by the receiver is lost, the sender resends the frames after its timer times out.

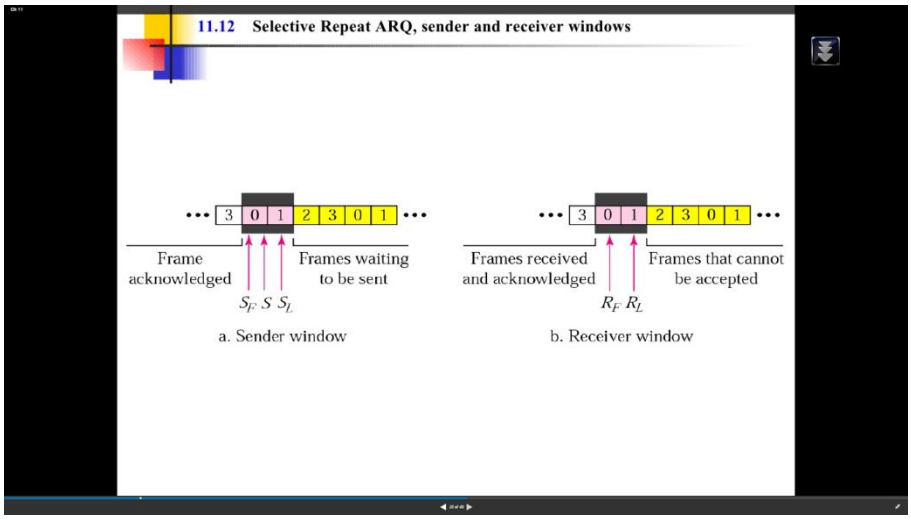




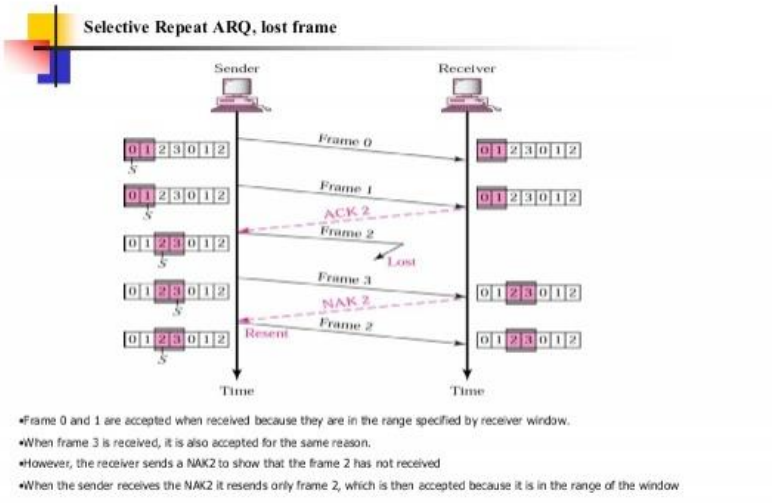
If an ACK is damaged/lost, we can have two situations: • If the next ACK arrives before the expiration of any timer, there is no need for retransmission of frames because ACKs are cumulative in this protocol. • If ACK1, ACK2, and ACk3 are lost, ACK4 covers them if it arrives before the timer expires. • If ACK4 arrives after time-out, the last frame and all the frames after that are resent. • Receiver never resends an ACK. • A delayed ACK also triggers the resending of frames

Selective request ARQ

Selective Repeat attempts to retransmit only those packets that are actually lost (due to errors). The sender and receiver window size is at most half of 2^m



The selective-repetitive ARQ scheme retransmits only those for which NAKs are received or for which timer has expired. This is the most efficient among the ARQ schemes, but the sender must be more complex so that it can send out-of-order frames. The receiver also must have storage space to store the post NAK frames and processing power to reinsert frames in proper sequence.

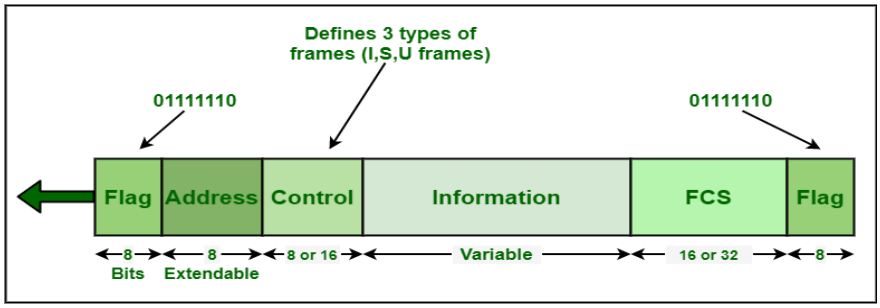


High Level Data Link Control(Bit Oriented)

High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes. Since it is a data link protocol, data is organized into frames.

A frame is transmitted via the network to the destination that verifies its successful arrival.

It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications



Basic Frame Structure

HDLC Frame

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

- **Flag** − It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** − It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent by the secondary station, it contains the address of the primary station. The address field may be from 1 byte to several bytes.
- **Control** − It is 1 or 2 bytes containing flow and error control information.
- **Payload** − This carries the data from the network layer. Its length may vary from one network to another.
- **FCS** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)

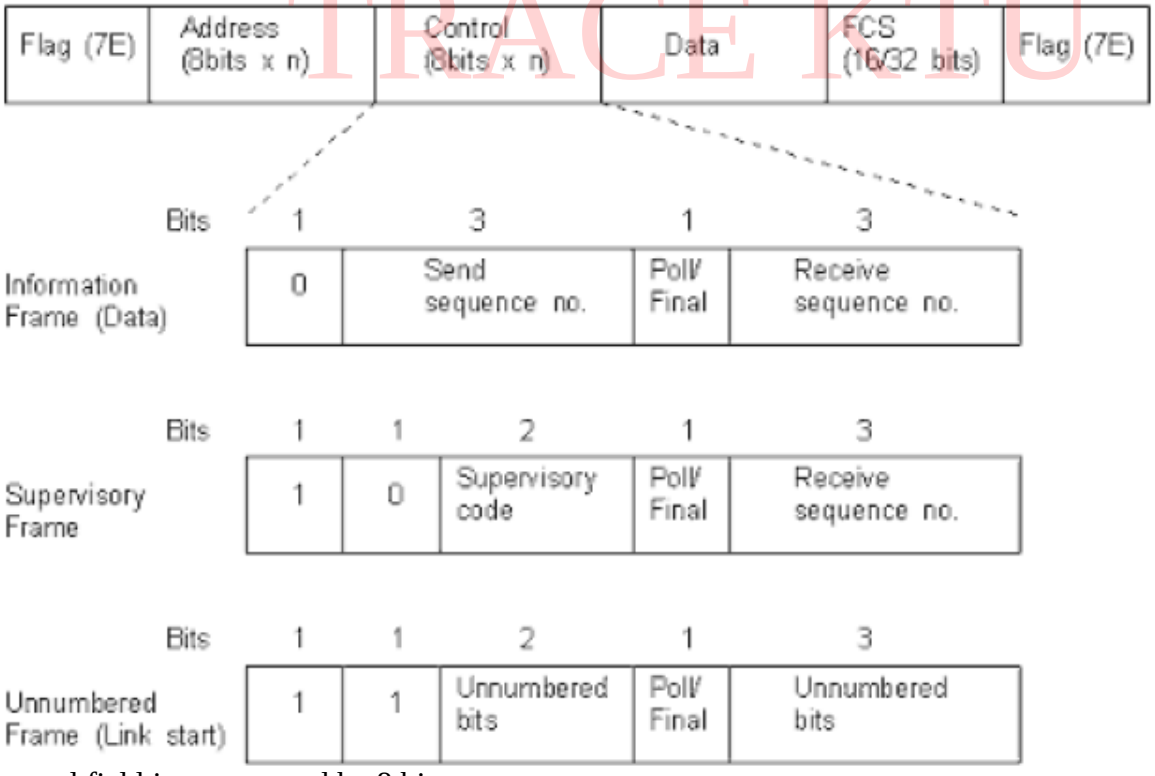
. Types of HDLC Frames

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

- **I-frame** − I-frames or Information frames carry user data from the network layer. They also include flow and error control information that is piggybacked on user data. The first bit of control field of I-frame is 0.
- **S-frame** − S-frames or Supervisory frames do not contain information field. They are used for flow and error control when piggybacking is not required. The first two bits of control field of S-frame is 10.
- **U-frame** − U-frames or Un-numbered frames are used for myriad miscellaneous functions, like link management. It may contain an information field, if required. The first two bits of control field of U-frame is 11.

Flag	Address Field	Control	User information	FCS	Flag

Flag is used to indicate the beginning and ending of the frame
Address field represents where the data must be send.
Control is used to store the control information.
User information: users information is send.
Fcs (Frame check sequence):It is used to check whether there is an error in the sequence.



Control field is represented by 8 bit.

Control frame in I frame

0				P/F			

Sequence no

Acknowledgment no

Sequence number is 3 bit-0 to 7.Acknowledgment numner is used to check whether acknowledgment is received or not.

P/F=1(Poll/Final) :Primary section is sending data

P/F=0(Poll/Final) :secondary section is sending data

2) Supervisory Frame or S frame

It is used to pass only control information

Flag	Address	control	FCS	flag

Control frame in S frame

1	0	S1	S2	P/F			

To indicate s-frame

Acknowledgment no

Value of s1 & s2 will decide which status is provided.

S1	S2	Status
0	0	Receiver ready
0	1	Receiver not ready
1	0	Send –ve acknowledgment
1	1	In selective repeat retransmission is specified.which numner is transmitted is specified in ACK no

3) Unnumbered Frame or u-frame

In this instead of user information we will send system management information.

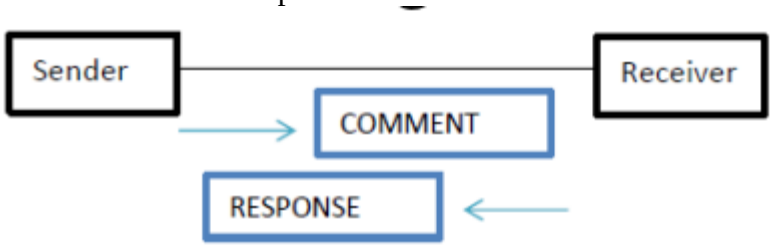
Flag	address	Control	System management information field	FCS	flag

Control frame in u-frame

1	1			P/F			

To indicate U-frame

T**hree types of stations** have been defined in HDLC:-
1. Primary station
2. Secondary station
3.Combined Station
1.**Primary station:** The Primary station has a responsibility of connecting and disconnecting the data link. The frame send by a primary station are called commands.
2.**Secondary Station:** It operates under the control of a primary station. The frame sent by the secondary station are called Response.
3.**Combined Station:** A combined station can act as a primary as well as secondary station. It can issue both command and response.



HDLC Operational Modes
A mode in HDLC is the relationship between two devices involved in an exchange; the mode describes who controls the link. Exchanges over unbalanced configurations are always conducted in normal response mode. Exchanges over symmetric or balanced configurations can be set to specific mode using a frame design to deliver the command. HDLC offers three different modes of operation. These three **modes of operations** are:
• Normal Response Mode (NRM)
• Asynchronous Response Mode (ARM)
• Asynchronous Balanced Mode (ABM)

Normal Response Mode
This is the mode in which the primary station initiates transfers to the secondary station. The secondary station can only transmit a response when, and only when, it is instructed to do so by the primary station. In other words, the secondary station must receive explicit permission from the primary station to transfer a response. After receiving permission from the primary station, the secondary station initiates its transmission. This transmission from the secondary station to the primary station may be much more than just an acknowledgment of a frame. It may in fact be more than one information frame. Once the last frame is transmitted by the secondary station, it must wait once again from explicit permission to transfer anything, from the primary station. Normal Response Mode is only used within an unbalanced configuration.
It is used most frequently in multi-point lines, where the primary station controls the link.

Asynchronous Response Mode
In this mode, the primary station doesn't initiate transfers to the secondary station. In fact, the secondary station does not have to wait to receive explicit permission from the primary station to transfer any frames. The frames may be more than just acknowledgment frames. They may contain data, or control information regarding the status of the secondary station. This mode can reduce

overhead on the link, as no frames need to be transferred in order to give the secondary station permission to initiate a transfer. However, some limitations do exist. Due to the fact that this mode is asynchronous, the secondary station must wait until it detects and idle channel before it can transfer any frames. This is when the ARM link is operating at half-duplex. If the ARM link is operating at full duplex, the secondary station can transmit at any time. In this mode, the primary station still retains responsibilityfor error recovery, link setup, and link disconnection.
It is better for point-to-point links, as it reduces overhead

ASynchronous Balanced Mode .

This mode is used in case of combined stations. There is no need for permission on the part of any station in this mode. This is because combined stations do not require any sort of instructions to perform any task on the link.

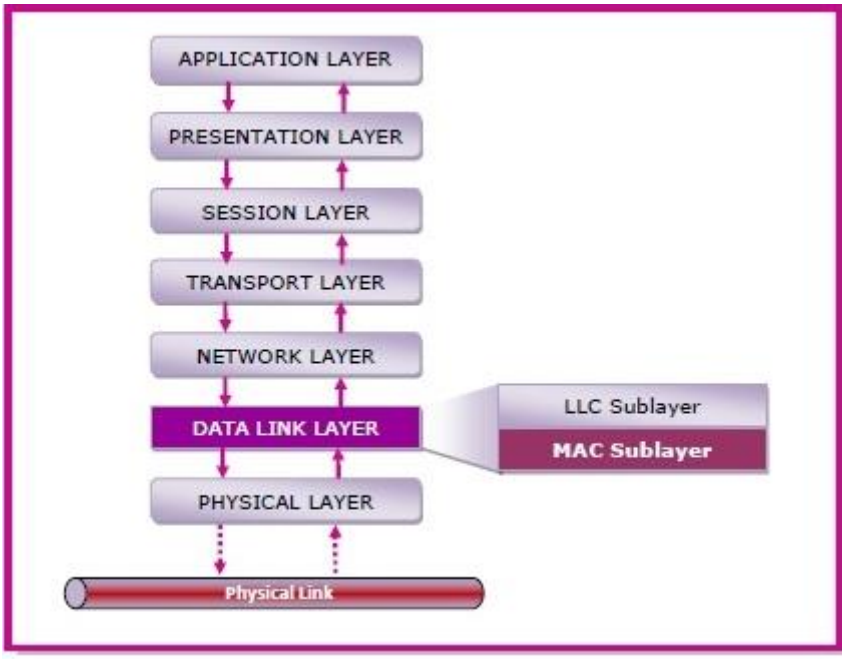
Medium Access control (MAC)

The medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.

MAC Layer in the OSI Model

The Open System Interconnections (OSI) model is a layered networking framework that conceptualizes how communications should be done between heterogeneous systems. The data link layer is the second lowest layer. It is divided into two sublayers −

- The logical link control (LLC) sublayer
- The medium access control (MAC) sublayer



The MAC layer is the "low" part of the second OSI layer, the layer of the "data link". In fact, the IEEE divided this layerinto two layers "above" is the control layer the logical connection
(Logical Link Control, LLC) and "down" the control layer the mediumaccess (MAC).
The LLC layer is standardized by the IEEE as the 802.2 since the beginning 1980 Its purpose is to allow level 3 network protocols (for eg IP) to be based on a single layer (the LLC layer) regardless underlying protocol used, including WiFi , Ethernet or Token Ring, for example. All WiFi data packets so carry a pack LLC, which contains itself packets from the upper network layers. The header of a packet LLC indicates the type of layer 3 protocol in it: most of the time, it is IP protocol, but it could be another protocol, such as IPX (Internet Packet Exchange) for example. Thanks to the LLC layer, it is possible to have at the same time, on the same network, multiple Layer 3protocols.
In LAN nodes uses the same communication channel for transmission. The MAC sub-layer has two primary responsibilities: Data encapsulation, including frame assembly before transmission, and frame parsing/error detection during and after reception. Media access control, including initiation of frame transmission and recovery from transmission failure.

MAC Addresses

MAC address or media access control address is a unique identifier allotted to a network interface controller (NIC) of a device. It is used as a network address for data transmission within a network segment like Ethernet, Wi-Fi, and Bluetooth.

MAC address is assigned to a network adapter at the time of manufacturing. It is hardwired or hard-coded in the network interface card (NIC). A MAC address comprises of six groups of two hexadecimal digits, separated by hyphens, colons, or no separators. An example of a MAC address is 00:0A:89:5B:F0:11.

Channel Allocation Schemes

Channel Allocation may be done using two schemes −

- Static Channel Allocation
- Dynamic Channel Allocation

Static Channel Allocation

In static channel allocation scheme, a fixed portion of the frequency channel is allotted to each user. For N competing users, the bandwidth is divided into N channels using frequency division multiplexing (FDM), and each portion is assigned to one user.

This scheme is also referred as fixed channel allocation or fixed channel assignment.

In this allocation scheme, there is no interference between the users since each user is assigned a fixed channel. However, it is not suitable in case of a large number of users with variable bandwidth requirements.

Dynamic Channel Allocation

In dynamic channel allocation scheme, frequency bands are not permanently assigned to the users. Instead channels are allotted to users dynamically as needed, from a central pool. The allocation is done considering a number of parameters so that transmission interference is minimized.

This allocation scheme optimises bandwidth usage and results is faster transmissions.

Following Protocols are used by Medium Access Layer :

ALOHA : ALOHA is a system for coordinating and arbitrating access to a shared communication channel. It was developed in the 1970s at the University of Hawaii. The original system used terrestrial radio
broadcasting, but the system has been implemented in satellite communication systems. A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time.

In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.

Carrier Sensed Multiple Access (CSMA) :

CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network. Devices attached to the network cable listen (carrier sense) before transmitting. If the channel is in use, devices wait before transmitting. MA (Multiple Access) indicates that many devices can connect to and share the same network. All devices have equal access to use the network when it is clear. Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time. On large networks, the transmission time between one end of the cable and another is enough that one station may access the cable even though another has already just accessed it.

Persistent and Non-persistent CSMA are two different types.

1-persistent CSM A

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. If a collision occurs, the station waits a random amount of time and starts all over again.

The propagation delay has an important effect on the performance of the protocol. There is a small chance that just after a station begins sending, another station will become ready to send and sense the channel. If the first station's signal has not yet reached the second one, the latter will sense an idle channel and will also begin sending, resulting in a collision.

Even if the propagation delay is zero, there will still be collisions. If two stations become ready in the middle of the a third station's transmission, both will wait until the transmission ends and then both will began transmitting simultaneously, resulting in a collision.

Nonpersistent CSMA:

In this protocol, a conscious attempt is made to be less greedy than in the previous one. Before sending, a station senses the channel. If no one else is sending, the station begins doing so itself.

If the channel is already in use, the station does not continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission. Instead, it waits a random period of time and then repeats the algorithm.

p-persistent CSMA

It applies to slotted channels and works as follows.

When a station becomes ready to send, it senses the channel. If it is idle, it transmits with a probability of p. With a probability q = 1 - p it defers until the next slot. If that slot is also idle, it either transmits of defers again, with probabilities p and q.

This process is repeated until either the frame has been transmitted or another station has begun transmitting.

There are two methods for avoiding these so-called collisions, listed here :

CSMA/CD (Carrier Sense Multiple Access/Collision Detection):

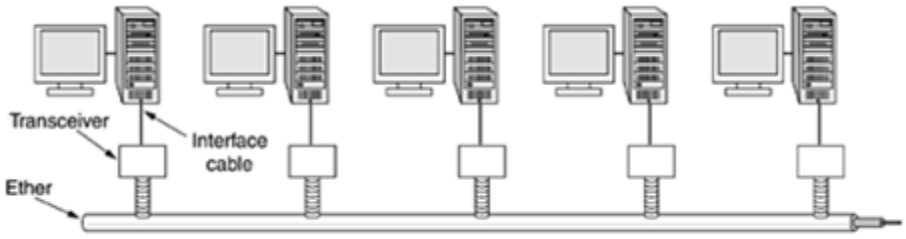
CD (collision detection) defines what happens when two devices sense a clear channel, then attempt to transmit at the same time. A collision occurs, and both devices stop transmission, wait for a random amount of time, and then retransmit. This is the technique used to access the 802.3 Ethernet network channel.

This method handles collisions as they occur, but if the bus is constantly busy, collisions can occur so often that performance drops drastically. It is estimated that network traffic must be less than 40 percent of the bus capacity for the network to operate efficiently. If distances are long, time lags occur that may result in inappropriate carrier sensing, and hence collisions.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance):

In CA collision avoidance), collisions are avoided because each node signals its intent to transmit before actually doing so. This method is not popular because it requires excessive overhead that reduces performance.

IEEE802.3(Ethernet):



IEEE802.3 is a working group and a collection of Institute of Electrical and Electronics Engineers(IEEE)standards produced by the working group defining the physical layer and data link layer's media access control(MAC)of wired Ethernet.

- This is generally a Local area network(LAN)technology with some wide area network(WAN)applications.

- Physical connections are made between nodes and or infrastructure devices(hubs, switches, routers)by various types of copper or fibre cable.802.3is a technology that supports the IEEE802.1network architecture.
- 802.3also defines LAN access method using CSMA/CD.
- The IEEE 802.3 is for 1 persistent CSMA/CD (Carrier sense multiple access with collision detection) LAN. Here when a station wants to transmit it listens to the cable. If the cable is busy, the station waits until it goes ideal, otherwise it transmits immediately. If 2 or more stations simultaneously begin transmitting on an ideal cable, they will collide. All colliding stations then terminate their transmission, wait a random time, and repeat the whole process all over again. So when data is send when the carrier is free. Since the name "Ethernet" refers to the cable, two types of coaxial cables are used.

Algorithm of CSMA/CD

Step 1) When a frame is ready, the transmitting station checks whether the channel is idle or busy.

Step 2) If the channel is busy, the station waits until the channel becomes idle.

Step 3) If the channel is idle, the station starts transmitting and continually monitors the channel to detect collision.

Step 4) If a collision is detected, the station starts the binary exponential backoff algorithm.

Step 5) The station resets the retransmission counters and completes frame transmission.

Binary Exponential Backoff Algorithm in case of Collision

Step 1) The station continues transmission of the current frame for a specified time along with a jam signal, to ensure that all the other stations detect collision.

Step 2) The station increments the retransmission counter, c, that denote the number of collisions.

Step 3) The station selects a random number of slot times in the range 0 and 2^c-1. For example, after the first collision (i.e. c = 1), the station will wait for either 0 or 1 slot times. After the second collision (i.e. c = 2), the station will wait anything between 0 to 3 slot times. After the third collision (i.e. c = 3), the station will wait anything between 0 to 7 slot times, and so forth.

Step 4) If the station selects a number k in the range 0 and 2^c-1, then

*Back_off_time = k * Time slot,*

where a time slot is equal to round trip time (RTT)(approx 51.2micro sec)

Step 5) And the end of the backoff time, the station attempts retransmission by continuing with the CSMA/CD algorithm.

Step 6) If the maximum number of retransmission attempts is reached, then the station aborts transmission.

Ethernet Cabling

Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings

Four types of cabling are commonly used.

• **10Base5 cabling, thick Ethernet,**

- It resembles a yellow garden hose, with markings every 2.5 meters to show where the taps go. (The 802.3 standard does not actually require the cable to be yellow, but it does suggest it.) Connections to it are generally made using vampire taps, in which a pin is very carefully forced halfway into the coaxial cable's core.
- The notation 10Base5 means that it operates at 10 Mbps, uses baseband signaling, and can support segments of up to 500 meters.

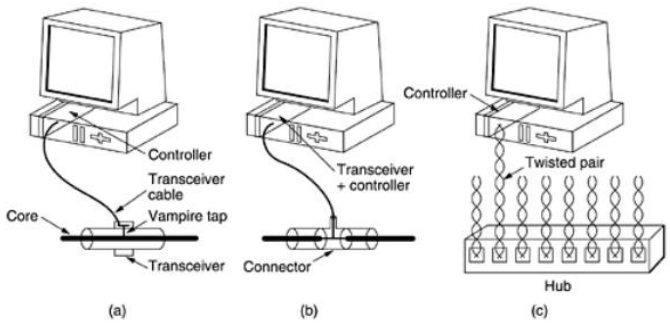
• **10Base2, or thin Ethernet,**

- It bends easily.
- Connections to it are made using industry standard BNC connectors to form T junctions, rather than using vampire taps. BNC connectors are easier to use and more reliable.
- Thin Ethernet is much cheaper and easier to install, but it can run for only 185 meters per segment, each of which can handle only 30 machines.
- **10Base-T.**
- The problems associated with finding cable breaks drove systems toward a different kind of wiring pattern, in which all stations have a cable running to a central hub in which they are all connected electrically (as if they were soldered together). Usually, these wires are telephone company twisted pairs, since most office buildings are already wired this way, and normally plenty of spare pairs are available.
- Hubs do not buffer incoming traffic.

10Base-F,

which uses fiber optics. This alternative is expensive due to the cost of the connectors and terminators, but it has excellent noise immunity and is the method of choice when running between buildings or widely-separated hubs. Runs of up to km are allowed. It also offers good security since wiretapping fiber is much more difficult than wiretapping copper wire.

Figure 4-14. Three kinds of Ethernet cabling. (a) 10Base5. (b) 10Base2. (c) 10Base-T.



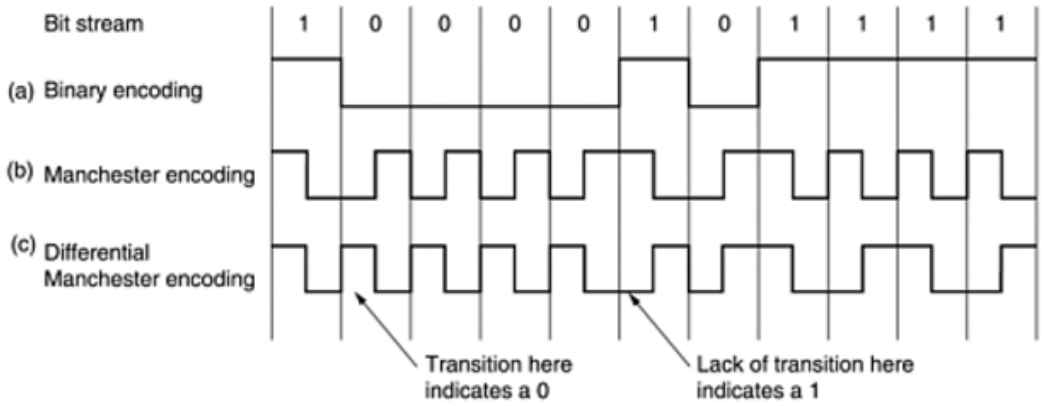
Frame Format

7	1	6	6	2	0-1500	0-46	4
preamble	SFD	Dest address	Source address	Length of data	Data field	padding	FCS

- Preamble:used for synchronization ,that is synchronization of receiver's clock with sender's ,7bytes
- SFD(Start frame delimit):used to show the start of the frame. Destination address & Source address :used to denote the destination & source of the data .There is group address which sends data to multiple stations. Sending data to group of stations is known as multicast. The address consisting of all 1 bits is reserved for broadcast.
- Length of data & Data field:Tells how many bytes of data are present\ in the data field, from a minimum of 0 to maximum of 1500.while a data field of 0 byte is illegal.it causes problem.When transceiver detects collision,it truncates current frame due to this stray bits and pieces of frame appear on the cable.
- Min size of Ethernet frame =64 bytes

- Padding: used to fill out frame to min size-etc 0's added to data.If the data send is 12 bit we make it 2 byte by adding 4 0's.The data field send must be small then min size must be specified ,else conjetion frame or runt frame.
- FCS(Frame check sequence): used to check errors.

802.3 Coding:



None of the versions of Ethernet uses straight binary encoding with 0 bvolts for a 0 bit and 5volts for a 1 bit because it leads to ambiguities. 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 and -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. Different clock speeds can cause the receiver and sender to get out of

synchronization about where the bit boundaries are, especially after a long run of consecutive 0s or a long run of consecutive 1s. What is needed is a way for receivers to unambiguously determine the start, end, or middle of each bit without reference to an external clock.
Two such approaches are called **Manchester** encoding and **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 is that it requires twice as much bandwidth as straight binary encoding because the pulses are half the width.
  - **Manchester encoding:**0- low to high,1 - high to low

Differential Manchester encoding:
0- beginning transition present,1:no transition in beginning.

Fast ethernet

It is the Successor of 10-Base-T Ethernet. It is more popular than Gigabit Ethernet because its configuration and implementation is simple. It is faster than its successors. Its variants are:

- 100Base-T4: signaling speed of 25 MHz and requires four twisted pairs
- 100Base-Tx:is simpler because the wires can handle clock rates of 125 MHz. Only two twisted pairs per station are used, one to the hub and one from it.
- The 100Base-TX system is full duplex; stations can transmit at 100 Mbps and receive at 100 Mbps at the same time.
- **100Base-Fx:** uses two strands of multimode fiber, one for each direction, so it, too, is full duplex with 100 Mbps in each direction. In addition, the distance between a station and the hub can be up to 2 km

Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps (Cat 5 UTP)
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

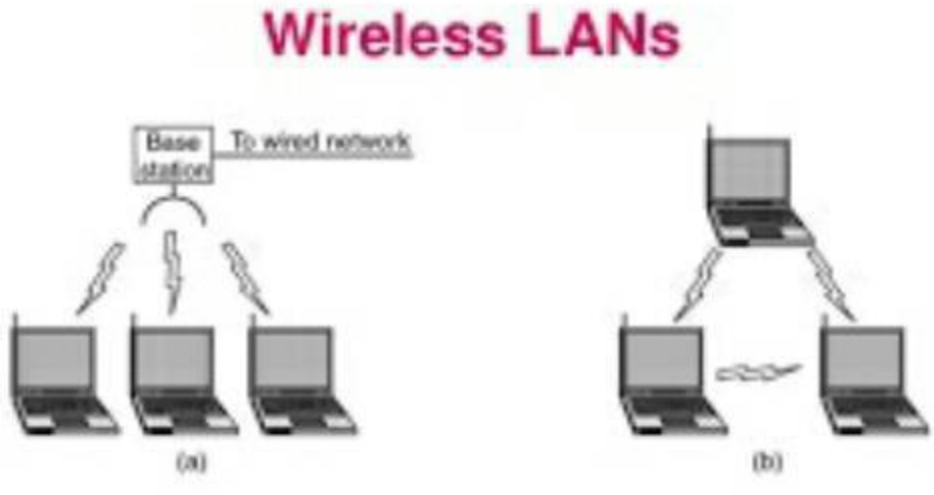
Gigabit Ethernet

- It the successor of Fast Ethernet. It can produces upto 1 Gbps speed. It is less popular than Fast Ethernet because its configuration and implementation is complicated than Fast Ethernet. The coverage limit of Gigabit Ethernet is up to 70km.

- Gigabit Ethernet had to provide service with both unicast and broadcast using the same 48-bit address scheme and also maintaining the same frame format. All configurations of gigabit Ethernet must use point-to-point links
- Gigabit Ethernet supports both copper and fiber cabling as shown in table 1. When sending signals at the speed of 1 Gbps then it requires encoding and at every nanosecond, a bit must be sent.
- Gigabit Ethernet supports two different modes of operation: full-duplex mode and half-duplex mode. The "normal" mode is full-duplex mode, which allows traffic in both directions at the same time. This mode is used when there is a central switch connected to computers (or other switches) on the periphery.

Name	Cable	Max. Segment	Advantages
1000Base-SX	Fiber optics	550m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000m	Single(10 μ) or multimode(50, 62.5 μ)
1000Base-CX	2 pairs of STP	25m	Shielded twisted pair
1000Base-T	4 pairs of UTP	100m	Standard category 5 UTP

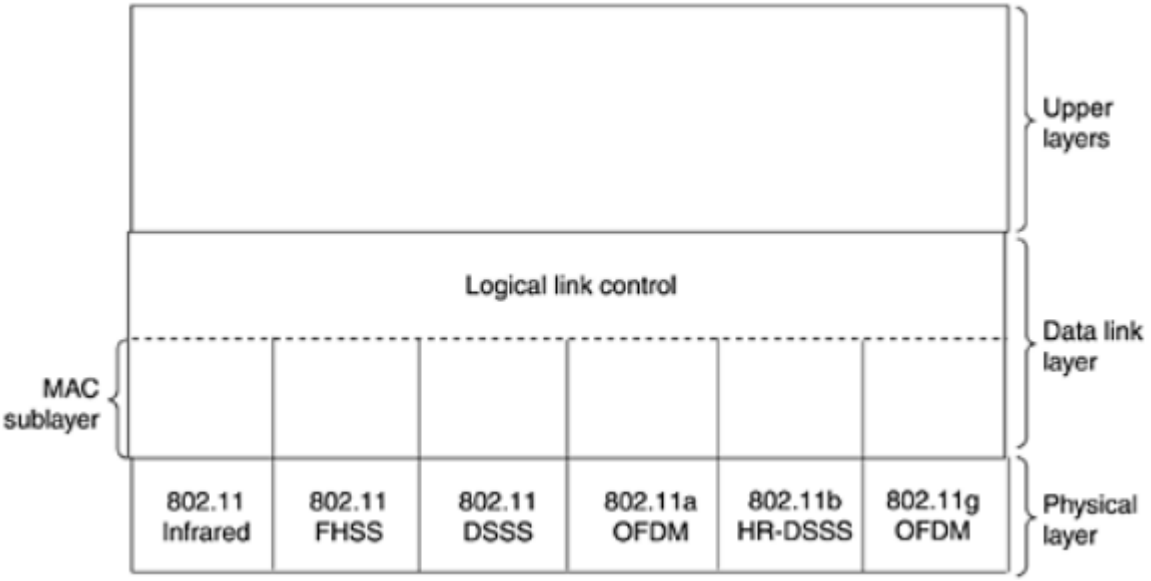
WIRELESS LANs



(a) Wireless networking with a base station. (b) Ad hoc networking.

- A wireless local area network (WLAN)is a wireless computer network that links two or More devices using wireless communication within a limited are a such as a home, school, computer laboratory, or office building.
- This gives users the ability to move around within a local coverage area and yet still be connected to the network. Through a gateway, a WLAN can also provide a connection to the wider Internet.
- Most modern WLANs are based on IEEE802.11 standards and are marketed under the **Wi-Fi brand name.**
- A wireless LAN (or WLAN, for wireless local area network, sometimes referred to as LAWN, for local area wireless network) is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection.
- The IEEE 802.11 group of standards specify the technologies for wireless LANs. 802.11 standards
- operate in one of two configurations
  - Infrastructure mode
  - Ad-hoc mode.
- Infrastructure mode
- Each client is associated with an **AP** (**Access Point**) 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.
- clients can send frames to other clients via their APs.
- **Ad hoc network**
- 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
- use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing and include an encryption method, the Wired Equivalent Privacy algorithm.
- 802.11 only supported a maximum network bandwidth of 2 Mbps – too slow for most applications. For this reason, ordinary 802.11 wireless products are no longer manufactured.

The 802.11 Protocol Stack



- The physical layer corresponds to the OSI physical layer fairly well,
- 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.

The 802.11 Physical Layer

- **802.11 standard specifies three groups of transmission techniques allowed in the physical layer.**

1) **Infrared method (1 technique)**
2) **Short – range radio method (2 techniques)**
3) **Higher bandwidth method(2+1 techniques)**

- **Each of the five permitted transmission techniques makes it possible to send a MAC frame from one station to another.**

They differ, however, in the technology used and speeds achievable

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**
- **FHSS (Frequency Hopping Spread Spectrum) uses 79 channels, each 1-MHz wide, starting at the low end of the 2.4-GHz ISM**
- **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**

802.11b

- IEEE expanded on the original 802.11 standard in July 1999, creating the *802.11b*specification. 802.11b supports bandwidth up to 11 Mbps, comparable to traditional Ethernet. 802.11b uses the same *unregulated* radio signaling frequency (2.4 GHz) as the original 802.11 standard. Vendors often prefer using these frequencies to lower their production costs.

- **HR-DSSS (High Rate Direct Sequence Spread Spectrum**), another spread spectrum technique, which uses 11 million chips/sec to achieve 11 Mbps in the 2.4-GHz band.
- Being unregulated, 802.11b gear can incur interference from microwave ovens, cordless phones, and other appliances using the same 2.4 GHz range. However, by installing 802.11b gear a reasonable distance from other appliances, interference can easily be avoided.

• **Pros of 802.11b** - Lowest cost; signal range is good and not easily obstructed

• **Cons of 802.11b** - Slowest maximum speed; home appliances may interfere on the unregulated frequency band

802.11a

- While 802.11b was in development, IEEE created a second extension to the original 802.11 standard called *802.11a*. Because 802.11b gained in popularity much faster than did 802.11a, some folks believe that 802.11a was created after 802.11b. In fact, 802.11a was created at the same time.
- Due to its higher cost, 802.11a is usually found on business networks whereas 802.11b better serves the home market.
- Uses **OFDM (Orthogonal Frequency Division Multiplexing**) to deliver up to 54 Mbps
- 802.11a supports bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz. This higher frequency compared to 802.11b shortens the range of 802.11a networks.
- The higher frequency also means 802.11a signals have more difficulty penetrating walls and other obstructions.
- Because 802.11a and 802.11b utilize different frequencies, the two technologies are incompatible with each other. Some vendors offer hybrid *802.11a/b* network gear, but these products merely implement the two standards side by side (each connected devices must use one or the other).

• **Pros of 802.11a** - Fast maximum speed; regulated frequencies prevent signal interference from other devices.

• **Cons of 802.11a** - Highest cost; shorter range signal that is more easily obstructed.

802.11g

- In 2002 and 2003, WLAN products supporting a newer standard called *802.11g*emerged on the market. 802.11g attempts to combine the best of both 802.11a and 802.11b.
- It uses the **OFDM modulation metho**d 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.
- 802.11g supports bandwidth up to 54 Mbps, and it uses the 2.4 GHz frequency for greater range. 802.11g is backward compatible with 802.11b, meaning that 802.11g access points will work with 802.11b wireless network adapters and vice versa.

• **Pros of 802.11g** - Fast maximum speed; signal range is good and not easily obstructed.

• **Cons of 802.11g** - Costs more than 802.11b; appliances may interfere on the unregulated signal frequency.

802.11n

- *802.11n* (also sometimes known as Wireless N) was designed to improve on 802.11g in the amount of bandwidth supported by utilizing multiple wireless signals and antennas (called *MIMO* technology) instead of one.
- Industry standards groups ratified 802.11n in 2009 with specifications providing for up to 300 Mbps of network bandwidth. 802.11n also offers somewhat better range over earlier Wi-Fi standards due to its increased signal intensity, and it is backward-compatible with 802.11b/g gear.

• **Pros of 802.11n** - Fastest maximum speed and best signal range; more resistant to signal interference from outside sources.
• **Cons of 802.11n** - Standard is not yet finalized; costs more than 802.11g; the use of multiple signals may greatly interfere with nearby 802.11b/g based networks.

The 802.11 MAC Sublayer Protocol

CSMA/CA (MACA for wireless LAN)

Hidden station problem

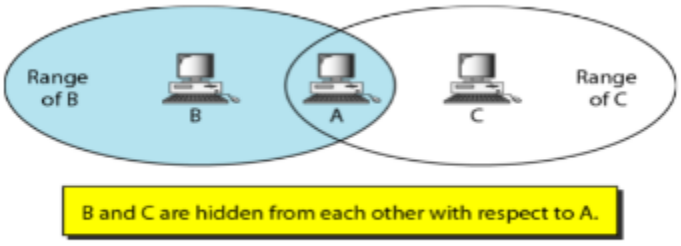
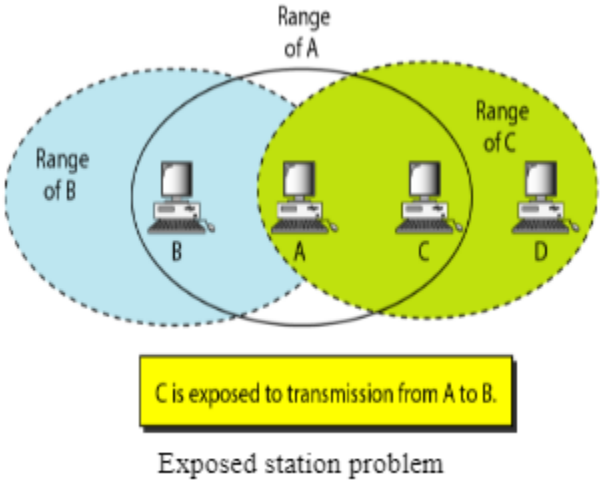


Fig. Hidden station problem

When A is transmitting to B

If C senses the medium, it will not hear A because A is out of range, and thus falsely conclude that it can transmit to B.
If C does start transmitting, it will interfere at B, wiping out the frame from A.
The problem of a station not being able to detect a potential competitor for the medium because the competitor is too far away is called the **hidden station problem**.

Exposed station problem



Exposed station problem

When B transmitting to A (previous figure part b)

If C senses the medium, it will hear an ongoing transmission and falsely conclude that it may not send to D, when in fact such a transmission would cause bad reception only in the zone between B and C, where neither of the intended receivers is located.
This is called the **exposed station problem**.

The problem is that before starting a transmission, a station really wants to know whether there is activity around the receiver.

An early protocol designed for wireless LANs is **MACA (Multiple Access with Collision Avoidance)** (Karn, 1990).

The basic idea behind it is for the sender to stimulate the receiver into outputting a short frame, so stations nearby can detect this transmission and avoid transmitting for the duration of the upcoming (large) data frame.

Let us now consider how A sends a frame to B.

- A starts by sending an RTS (Request To Send) frame to B. This short frame (30 bytes) contains the length of the data frame that will eventually follow.
- Then B replies with a CTS (Clear to Send) frame. The CTS frame contains the data length (copied from the RTS frame). Upon receipt of the CTS frame, A begins transmission.

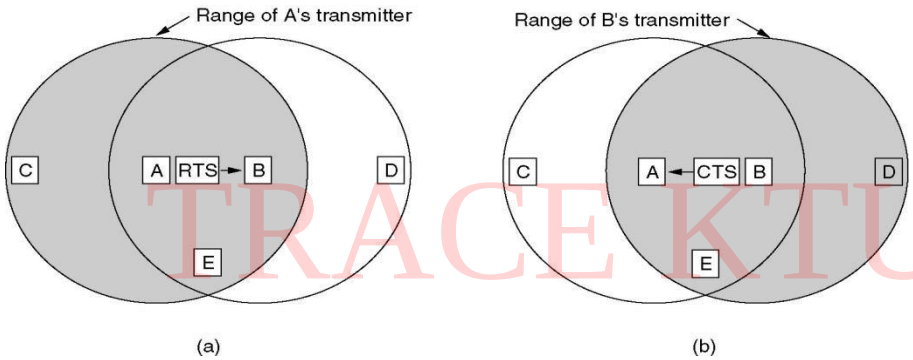


Fig. The MACA protocol. (a) A sending an RTS to B. (b) B responding with a CTS to A.

- Any station hearing the RTS is clearly close to A and *must remain silent* ***long enough*** for the CTS to be transmitted back to A without conflict.
- Any station hearing the CTS is clearly close to B and *must remain silent* ***during*** the upcoming data transmission, whose length it can tell by examining the CTS frame.
- C is within range of A but not within range of B. Therefore, it hears the RTS from A but not the CTS from B. As long as it does not interfere with the CTS, it is *free to transmit* while the data frame is being sent.
- D is within range of B but not A. It does not hear the RTS but does hear the CTS. Hearing the CTS tips it off that it is close to a station that is about to receive a frame, so it *defers sending* anything until that frame is expected to be finished.
- E hears both control messages and, like D, must be silent until the data frame is complete.
- Collisions can still occur:

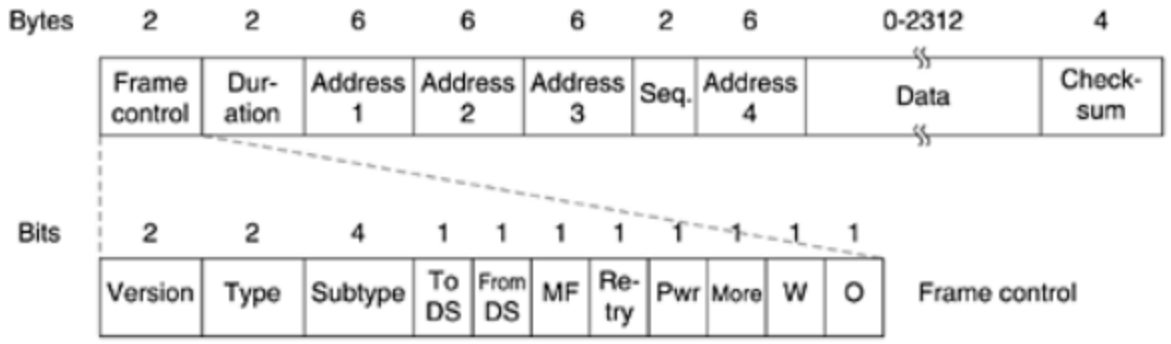
For example, B and C could both send RTS frames to A at the same time. These will collide and be lost. In the event of a collision, an unsuccessful transmitter (i.e., one that does not hear a CTS within the expected time interval) waits a random amount of time and tries again later.

- New improvements have been made to MACA to improve its performance and the new protocol named MACAW (MACA for Wireless).

The 802.11 Frame Structure

The 802.11 standard defines three different classes of frames on the wire: data, control, and management.

The format of the data frame



Frame Control field.

- It itself has 11 subfields.
- The first of these is the *Protocol version*, which allows two versions of the protocol to operate at the same time in the same cell.
- *Type* (data, control, or management) and *Subtype* fields (e.g., RTS or CTS).
- The *To DS* and *From DS* bits indicate the frame is going to or coming from the intercell distribution system (e.g., Ethernet).
- The *MF* bit means that more fragments will follow.
- The *Retry* bit marks a retransmission of a frame sent earlier.
- The *Power management* bit is used by the base station to put the receiver into sleep state or take it out of sleep state.
- The *More* bit indicates that the sender has additional frames for the receiver.
- The *W* bit specifies that the frame body has been encrypted using the **WEP** (**Wired Equivalent Privacy**) algorithm.
- The *O* bit tells the receiver that a sequence of frames with this bit on must be processed strictly in order.

***Duration* field**, tells how long the frame and its acknowledgement will occupy the channel. This field is also present in the control frames

The frame header contains four addresses,The source and destination and source and destination base stations for intercell traffic.

The *Sequence* field allows fragments to be numbered. Of the 16 bits available, 12 identify the frame and 4 identify the fragment.

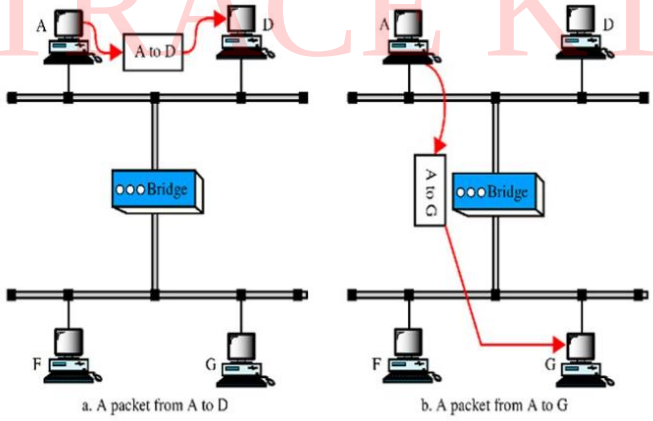
The ***Data*** field contains the payload, up to 2312 bytes, followed by the usual ***Checksum*.**

- **Management frames** have a format similar to that of data frames, except without one of the base station addresses, because management frames are restricted to a single cell.

- **Control frames** are shorter still, having only one or two addresses, no *Data* field, and no *Sequence* field. The key information here is in the *Subtype* field, usually RTS, CTS, or ACK.

BRIDGES:-

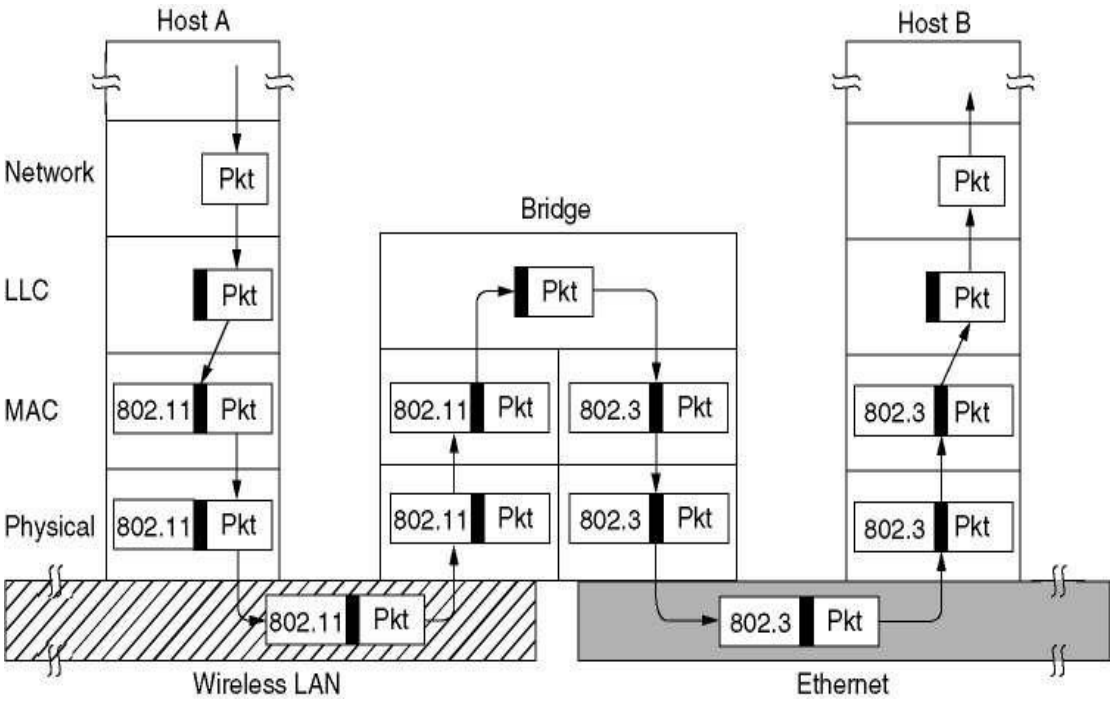
- A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segment. This function is called **network bridging.**
- The bridge is one of the tools to join divided LANS.
- Secondly a LAN(for example Ethernet)can be limited in its transmission distance. We Can eliminate this problem using bridges as repeaters, so that we can connect a Geographically extensive network within the building or campus using bridges.
- Third, the network administrator can control the amount of traffic going through bridges sent across the expensive network media.
- Fourth, the bridge is plug and play devices other is no need to configure the bridge. And suppose any machine was taken out from the network then there is no need for the Network administrator to update the bridge configuration information as bridges are self configured. And also it provide easiness for the transfer of Data.



a. A packet from A to D b. A packet from A to G

Bridges from 802.x to 802.y

- 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.
- 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
- Note that a bridge connecting k different LANs will have k different MAC sublayers and k different physical layers, one for each type.



Host A has a packet to send. The packet descends into the LLC sublayer and acquires an LLC header. Then it passes into the MAC sublayer and an 802.11 header is prepended to it .This unit goes out onto the cable and eventually is passed up to the MAC sublayers in the bridge, where the 802.11 header is stripped off. The bare packet is then headed off to the LLC sublayer in the bridge. In this example ,the packet is destined for an 802.3 subnet connected to the bridge, so it works its way down the 802.3 side of the bridge and off it goes.

Types of Bridges:-

- Source routing bridge
- Transparent learning bridge

The Transparent Learning Bridge

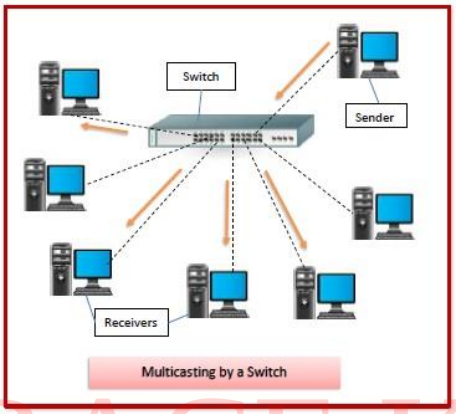
- The transparent bridge finds the location of user using the source and destination address.
- When the frame is received at the bridge it checks its source address and the Destination address.
- The destination address is stored if it was not found in a routing table.
- Then the frame sent to all LAN excluding the LAN from which it came.
- The source Address is also stored in the routing table. If another frame is arrived in which the Previous source address is now its destination address then it is forwarded to that port.
- Build a table of MAC addresses as frames arrive.
- Ethernet networks use transparent bridge
- Duties are : Filtering frames, forwarding and blocking

Source Routing Bridge

- A communication protocol in which the sending station is aware of all the bridges in the network and predetermines the complete route to the destination station before transmitting.
- Used in Token Ring networks
- Frame contains not only the source and destination address but also the bridge addresses.

SWITCHES:

- A network switch(also called switching hub, bridging hub) is a computer networking device that connects devices together on a computer network by using packet switching to receive,process and
- forward data to the destination device.
- Switches are networking devices operating at layer 2 or a data link layer of the OSI model.
- They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.
- A switch has many ports, to which computers are plugged in.
- When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s).
- It supports unicast, multicast as well as broadcast communications.



Features of Switches

- A switch operates in the layer 2, i.e. data link layer of the OSI model.
- It is an intelligent network device that can be conceived as a multiport network bridge.
- It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.
- It uses packet switching technique to receive and forward data packets from the source to the destination device.
- It is supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.
- Transmission mode is full duplex, i.e. communication in the channel occurs in both the directions at the same time. Due to this, collisions do not occur.
- Switches are active devices, equipped with network software and network management capabilities.
- Switches can perform some error checking before forwarding data to the destined port.