CMR INSTITUTE OF TECHNOLOGY	USN	□□□□□□□□□□	CELEBRATING 25 YEARS CMRIT CMR INSTITUTE OF TECHNOLOGY, BENGALURU. ACCREDITED WITH A+ GRADE BY NAAC

Internal Assesment Test – I Answer Key

Subject : Computer Networks				Code : 18MCA24
Date : 16/04/2019	Duration : 90 mins	Max Marks : 50	Sem : II	Branch : MCA

			OBE	
	Answer ANY FIVE FULL Questions	Marks	CO	RBT
1	Explain Requirements of Computer Networks.	10	CO1	L1

- We have established an ambitious goal for ourselves: to understand how to build a computer network from the ground up.
- it is important to recognize the underlying concepts because networks are constantly changing as the technology evolves and new applications are invented.
- It is our experience that once you understand the fundamental ideas, any new protocol that you are confronted with will be relatively easy to digest.
- 1.2.1 **Perspectives**
  - we also want to cover the perspectives of two additional groups that are of increasing importance: those who develop networked applications and those who manage or operate networks.
  - Let's consider how these three groups might list their requirements for a network:
  - **An application programmer** would list the services that his or her application needs—for example, a guarantee that each message the application sends will be delivered without error within a certain amount of time or the ability to switch gracefully among different connections to the network as the user moves around.
- A network operator would list the characteristics of a system that is easy to administer and manage—for example, in which faults can be easily isolated, new devices can be added to the network and configured correctly, and it is easy to account for usage.
- A network designer would list the properties of a cost-effective design—for example, that network resources are efficiently utilized and fairly allocated to different users. Issues of performance are also likely to be important.
- 1.2.2 **Scalable Connectivity**
- A network must provide connectivity among a set of computers. Sometimes it is enough to build a limited network that connects only a few select machines. In fact, for reasons of privacy and security, many private (corporate) networks have the explicit goal of limiting the set of machines that are connected.
- A system that is designed to support growth to an arbitrarily large size is said to scale.
- Links, Nodes, and Clouds
- To understand the requirements of connectivity more fully, we need to take a closer look at how computers are connected in a network. Connectivity occurs at many different levels.
- At the lowest level, a network can consist of two or more computers directly connected by some physical medium, such as a coaxial cable or an optical fibber. We call such a physical medium a link, and we often refer to the computers it connects as nodes. (Sometimes a node is a more specialized piece of hardware rather than a computer.
- in Figure 1.2, physical links are sometimes limited to a pair of nodes (such a link is said to be point-to-point), while in other cases more than two nodes may share a single physical link (such a link is said to be multiple-access).
- 1.2.3 **Cost-Effective Resource Sharing**
- Given a collection of nodes indirectly connected by a nesting of networks, it is possible for any pair of hosts to send messages to each other across a sequence of links and nodes. Of course, we want to do more than support just one pair of communicating hosts—we want to provide all pairs of hosts with the ability to exchange messages.

	○ *multiplexing, which means that a system resource i*s shared among multiple users. multiplexing can be explained by analogy to a timesharing computer system, where a single physical processor is shared (multiplexed) among multiple jobs, each of which believes it has its own private processor. Similarly, data being sent by multiple users can be multiplexed over the physical links that make up a network. ○ **1.2.4 Support for Common Services** ○ It is more accurate to think of a network as providing the means for a set of application processes that are distributed over those computers to communicate. In other words, the next requirement of a computer network is that the application programs running on the hosts connected to the network must be able to communicate in a meaningful way. ○ When two application programs need to communicate with each other, a lot of complicated things must happen beyond simply sending a message from one host to another. ○ One option would be for application designers to build all that complicated functionality into each application program. However, since many applications need common services, it is much more logical to implement those common services once and then to let the application designer build the application using those services. ○ The challenge for a network designer is to identify the right set of common services. The goal is to hide the complexity of the network from the application without overly constraining the application designer.			
2	**Performance issues in Computer Networks.** ➢ **1.5.1 Bandwidth and Latency** Network performance is measured in two fundamental ways: bandwidth (also called throughput) and latency (also called delay). The bandwidth of a network is given by the number of bits that can be transmitted over the network in a certain period of time. For example, a network might have a bandwidth of 10 million bits/second (Mbps), meaning that it is able to deliver 10million bits every second. latency, corresponds to how long it takes a message to travel from one end of a network to the other. Latency is measured strictly in terms of time. For example, a transcontinental network might have a latency of 24 milliseconds (ms); that is, it takes a message 24 ms to travel from one coast of North America to the other. There are many situations in which it is more important to know how long it takes to send a message from one end of a network to the other and back, rather than the one-way latency. We call this the round-trip time (RTT) of the network. RRT:-is the length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgement of that signal to be received. We often think of latency as having three components. First, there is the speed-of-light propagation delay. This delay occurs because nothing, including a bit on a wire, can travel faster than the speed of light. Second, there is the amount of time it takes to transmit a unit of data. This is a function of the network bandwidth and the size of the packet in which the data is carried. Third, there may be queuing delays inside the network, since packet switches generally need to store packets for some time before forwarding them on an outbound link. Latency = Propagation + Transmit + Queue Propagation = Distance/SpeedOfLight Transmit = Size/Bandwidth Distance is the length of the wire over which the data will travel, SpeedOfLight is the effective speed of light over that wire, Size is the size of the packet, and Bandwidth is the bandwidth at which the packet is transmitted. Note that if the message contains only one bit and we are talking about a single link (as opposed to a whole network), then the Transmit and Queue terms are not relevant, and latency corresponds to the propagation delay only. ➢ **1.5.2 Delay × Bandwidth Product** It is also useful to talk about the product of these two metrics, often called the delay × bandwidth product.	10	CO2	L2

if we think of a channel between a pair of processes as a hollow pipe where the latency corresponds to the length of the pipe and the bandwidth gives the diameter of the pipe, then the delay × bandwidth product gives the volume of the pipe—the maximum number of bits that could be in transit through the pipe at any given instant Said another way, if latency (measured in time) corresponds to the length of the pipe, then given the width of each bit (also measured in time) you can calculate how many bits fit in the pipe.

1.5.3 High-Speed Networks

The bandwidths available on today's networks are increasing at a dramatic rate, and there is eternal optimism that network bandwidth will continue to improve. This causes network designers to start thinking about what happens in the limit or, stated another way, what is the impact on network design of having infinite bandwidth available.

To appreciate the significance of ever-increasing bandwidth in the face of fixed latency, consider what is required to transmit a 1-MB file over a 1-Mbps network versus over a 1-Gbps network, both of which have an RTT of 100 ms. In the case of the 1-Mbps network, it takes 80 round-trip times to transmit the file; during each RTT, 1.25% of the file is sent. In contrast, the same 1-MB file doesn't even come close to filling 1 RTT's worth of the 1-Gbps link, which has a delay × bandwidth product of 12.5 MB.

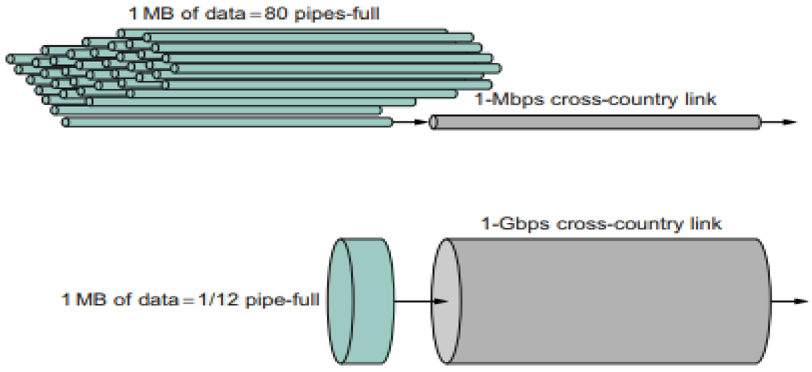

1 MB of data = 80 pipes-full
1-Mbps cross-country link
1-Gbps cross-country link
1 MB of data = 1/12 pipe-full

FIGURE 1.19 Relationship between bandwidth and latency. A 1-MB file would fill the 1-Mbps link 80 times but only fill the 1-Gbps link 1/12 of one time.

1.5.4 Application Performance Needs

The unstated assumption has been that application programs have simple needs—they want as much bandwidth as the network can provide. This is certainly true of the aforementioned digital library program that is retrieving a 25-MB image; the more bandwidth that is available, the faster the program will be able to return the image to the user.

some applications are able to state an upper limit on how much bandwidth they need. Video applications are a prime example. Suppose one wants to stream a video that is one quarter the size of a standard TV screen; that is, it has a resolution of 352 by 240 pixels. If each pixel is represented by 24 bits of information, as would be the case for 24-bit color.

Consider the situation in which the source sends a packet once every 33 ms, as would be the case for a video application transmitting frames 30 times a second. If the packets arrive at the destination spaced out exactly 33 ms apart, then we can deduce that the delay experienced by each packet in the network was exactly the same. If the spacing between when packets arrive at the destination—sometimes called the inter-packet gap—is variable, however, then the delay experienced by the sequence of packets must have also been variable, and the network is said to have introduced jitter into the packet stream.

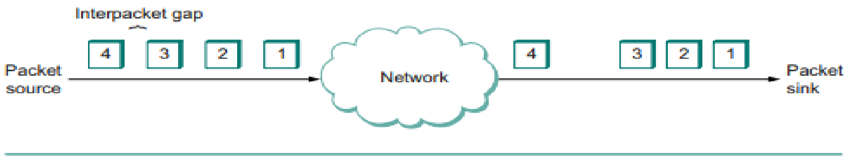
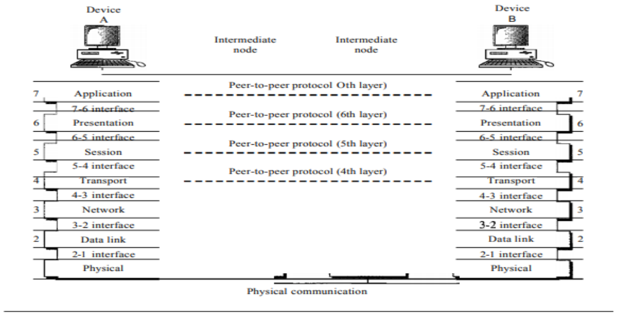


FIGURE 1.20 Network-induced jitter.

3 **Draw the OSI network architecture. Explain each layer in detail.** [10] CO4 L2

the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model. It was first introduced in the late 1970s.

The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network



LAYERS IN THE OSI MODEL

1) Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium.
It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to Occur.

Representation of bits. The physical layer data consists of a stream of bits (sequence of Os or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how Os and Is are changed to signals).

Data rate. The transmission rate-the number of bits sent each second-is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.
Synchronization of bits. The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.
Physical topology. The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology (every device is connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), a bus topology (every device is on a common link), or a hybrid topology (this is a combination of two or more topologies).

Transmission mode. The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex. In simplex mode, only one device can send; the other can only receive. The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

2) **Data Link Layer**

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the

physical layer appear error-free to the upper layer (network layer).
Other responsibilities of the data link layer include the following:
Framing. The data link layer divides the stream of bits received from the network layer into manageable data units called frames. The data link layer is responsible for moving frames from one hop (node) to the next.

Physical addressing. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.

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.

Error control. The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.
Access control. When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time

3)**Network Layer**
The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.

If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery. Figure shows the relationship of the network layer to the data link and transport layers.

Logical addressing. The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
Routing. When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

4)**Transport Layer**
The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.
Service-point addressing.

Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address).
The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.
Segmentation and reassembly.

A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.
Connection control.

The transport layer can be either connectionless or connection oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.

flow control.
at this layer is performed end to end rather than across a single link.

error control
at this layer is performed process-to process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

5)Session Layer
The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems. The session layer is responsible for dialog control and synchronization.

Specific responsibilities of the session layer include the following:
Dialog control. The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.

Synchronization. The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

6) Presentation Layer
The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.
Translation. The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods.
Encryption. To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
Compression. Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

7). Application Layer
The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
In Figure shows the relationship of the application layer to the user and the presentation layer. Of the many application services available, the figure shows only three: XAOO (message-handling services), X.500

(directory services), and file transfer, access, and management (FTAM). The user in this example employs XAOO to send an e-mail message.

Specific services provided by the application layer include the following:

Network virtual terminal. A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.

File transfer, access, and management. This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

Mail services. This application provides the basis for e-mail forwarding and storage.

Directory services. This application provides distributed database sources and access for global information about various objects and services.

4 **What is Framing? Explain Byte-Oriented Protocols.** [10] CO2 L3

FRAMING

we have seen how to transmit a sequence of bits over a point-to-point link—from adaptor to adaptor.

t blocks of data (called frames at this level), not bit streams, are exchanged between nodes. It is the network adaptor that enables the nodes to exchange frames.

When node A wishes to transmit a frame to node B, it tells its adaptor to transmit a frame from the node's memory.

This results in a sequence of bits being sent over the link. The adaptor on node B then collects together the sequence of bits arriving on the link and deposits the corresponding frame in B's memory.

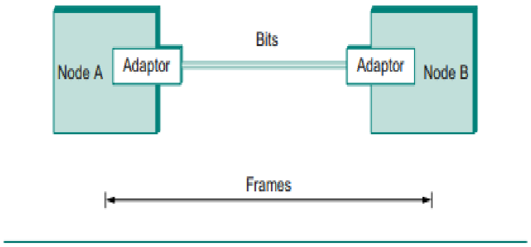


FIGURE 2.6 Bits flow between adaptors, frames between hosts.

(1) Byte-Oriented Protocols(BISYNC,PPP,DDCMP):-

BISYNC:-

a byte-oriented approach is exemplified by older protocols such as the Binary Synchronous Communication (BISYNC) protocol developed by IBM in the late 1960s.

Sentinel-Based Approaches:-

BISYNC uses special characters known as sentinel characters to indicate where frames start and end. The beginning of a frame is denoted by sending a special SYN (synchronization) character.

The data portion of the frame is then contained between two more special characters: STX (start of text) and ETX (end of text).

The SOH (start of header) field serves much the same purpose as the STX field. The problem with the sentinel approach, of course, is that the ETX character might appear in the data portion of the frame.

BISYNC overcomes this problem by "escaping" the ETX character by preceding it with a DLE (data-link-escape) character whenever it appears in the body of a frame.

the DLE character is also escaped (by preceding it with an extra DLE) in the frame body.

This approach is often called **character stuffing** because extra characters are inserted in the data portion of the frame.

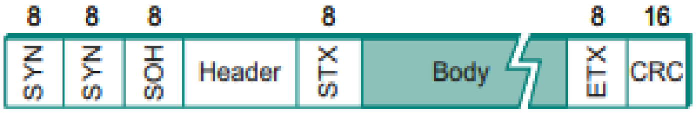


FIGURE 2.7 BISYNC frame format.

The frame format also includes a field labeled CRC (cyclic redundancy check), which is used to detect **transmission errors.**

PPP:-

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

Services Provided by PPP

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

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

Components of PPP

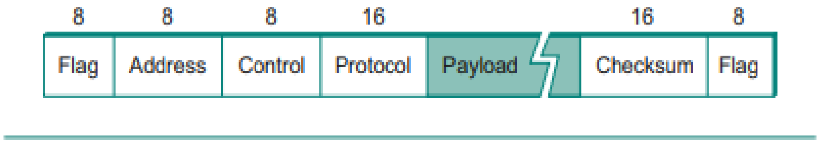
Point - to - Point Protocol is a layered protocol having three components −

- **Encapsulation Component** − It encapsulates the datagram so that it can be transmitted over the specified physical layer.
- **Link Control Protocol (LCP)** − It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also imparts negotiation for set up of options and use of features by the two endpoints of the links.

PPP Frame

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

- **Flag** − 1 byte that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** − 1 byte which is set to 11111111 in case of broadcast.
- **Control** − 1 byte set to a constant value of 11000000.
- **Protocol** − 1 or 2 bytes that define the type of data contained in the payload field.
- **Payload** − This carries the data from the network layer. The maximum length of the payload field is 1500 bytes. However, this may be negotiated between the endpoints of communication.
- **CHECKSUM** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)



■ FIGURE 2.8 PPP frame format.

DDCMP :-

An alternative to detect end-of-frame is to include number of bytes in the frame body as part of the frame header.

Digital Data Communication Message Protocol (DDCMP) uses the count approach. The Count Field specifies how many bytes are contained in the frame's body.

If Count Field is corrupted, then it is known as framing error. The receiver comes to know of it when it comes across the SYN field of the next frame.

5 **Explain CRC for Error Detection.** [10] CO2 L4

This Cyclic Redundancy Check is the most powerful and easy to implement technique. Unlike checksum scheme, which is based on addition, CRC is based on binary division.

In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.

At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted. A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.

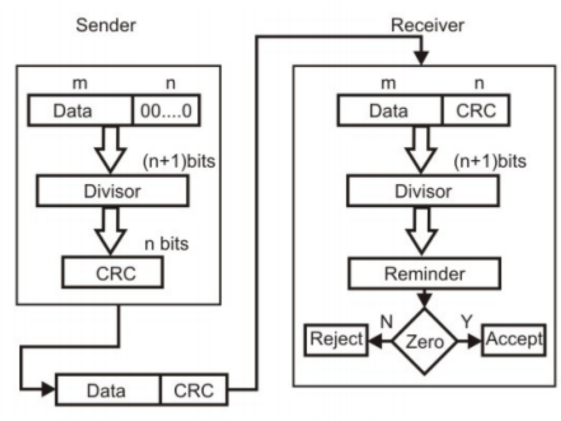


Figure 3.2.6 Basic scheme for Cyclic Redundancy Checking

CRC developed by IBM uses the concept of finite fields.

¬ A 'n' bit message is represented as a polynomial of degree n - 1.

¬ The message M(x) is represented as a polynomial by using the value of each bit in the message as coefficient for each term.

¬ For eg, 10011010 represents x7 + x4 + x3 + x

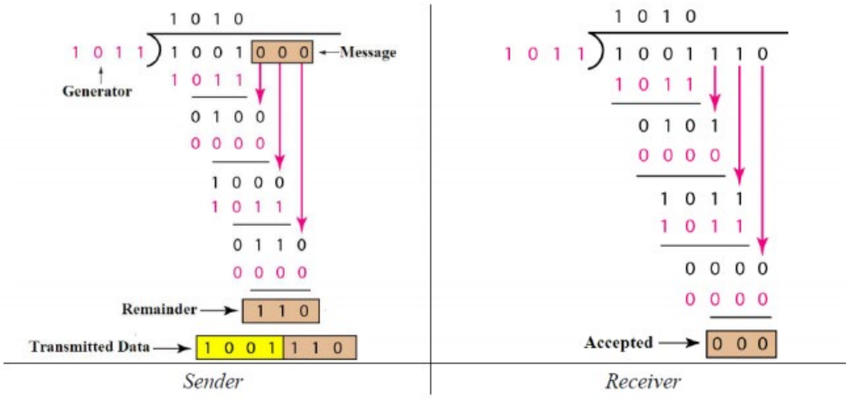
¬ For calculating a CRC, sender and receiver agree on a divisor polynomial, C(x) of degree k such that k< n – 1.

SENDER

Multiply M(x) by x k i.e., append k zeroes. Let the modified poly be M'(x).

¬ Divide M'(x) by C(x) using XOR operation. The remainder has k bits.

¬ Subtract the remainder from M'(x) using XOR, say T(x) and transmit T(x) with n + k bits.



RECEIVER

¬ Divide the received polynomial T(x) by C(x) as done in sender.

¬ If the remainder is non-zero then discard the frame.

¬ If zero, then no errors and redundant bits are removed to obtain data.

6 **What is sliding window? Explain Types of Sliding Window.** [10] CO3 L3

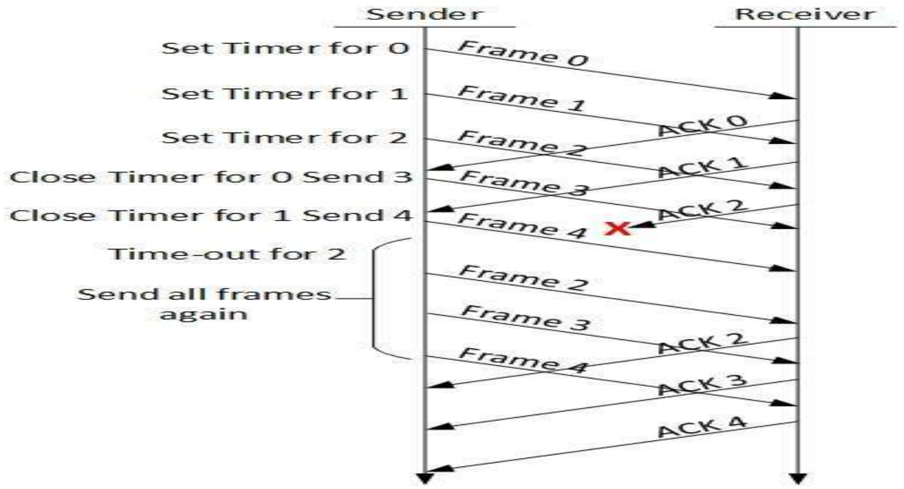
data frames were transmitted in one direction only. In most practical situations, there is a need to transmit data in both directions. One way of achieving full-duplex data transmission is to run two instances of one of the previous protocols, each using a separate link for simplex data traffic (in different directions). Each link is then comprised of a ‘‘forward’’ channel (for data) and a ‘‘reverse’’ channel (for acknowledgements). In both cases the capacity of the reverse channel is almost entirely wasted.

A better idea is to use the same link for data in both directions. After all, in protocols 2 and 3 it was already being used to transmit frames both ways, and the reverse channel normally has the same capacity as the forward channel. In this model the data frames from A to B are intermixed with the acknowledgement frames from A to B. By looking at the kind field in the header of an incoming frame, the receiver can tell whether the frame is data or an acknowledgement.

Types of Sliding window:-

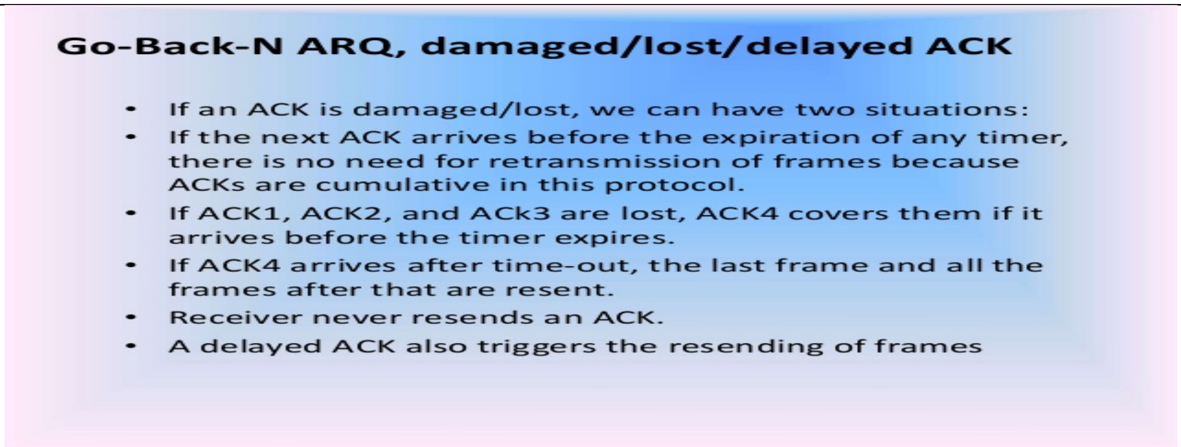
1)GO-BACK-N

Stop and wait ARQ mechanism does not utilize the resources at their best.When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window.



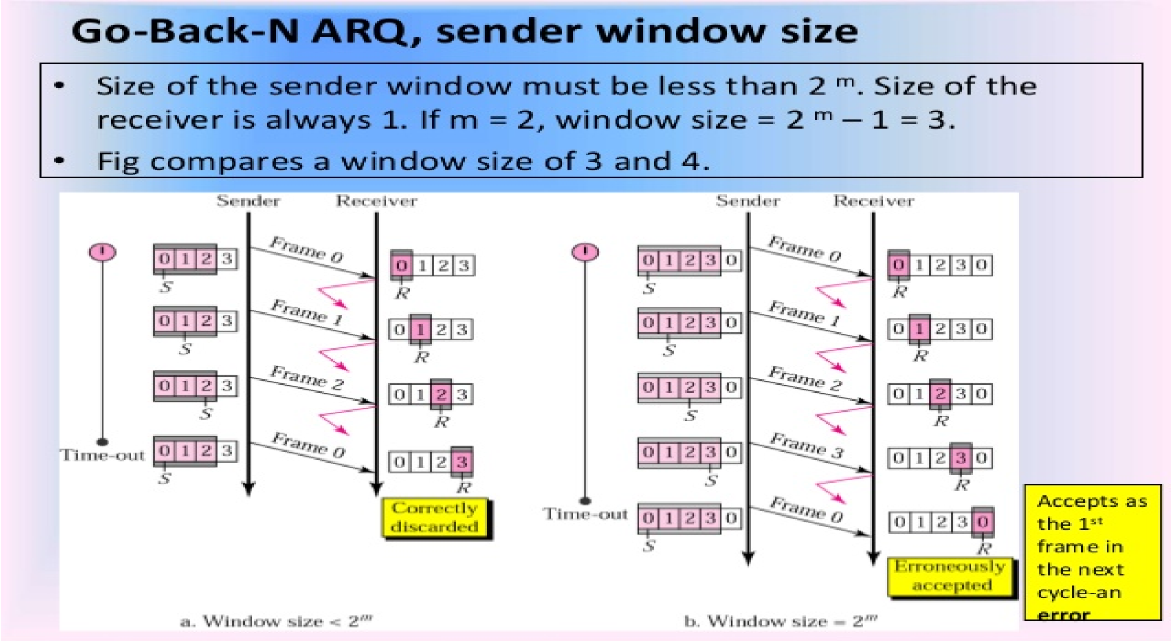
The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame’s sequence number.

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.



Go-Back-N ARQ, damaged/lost/delayed ACK

- 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



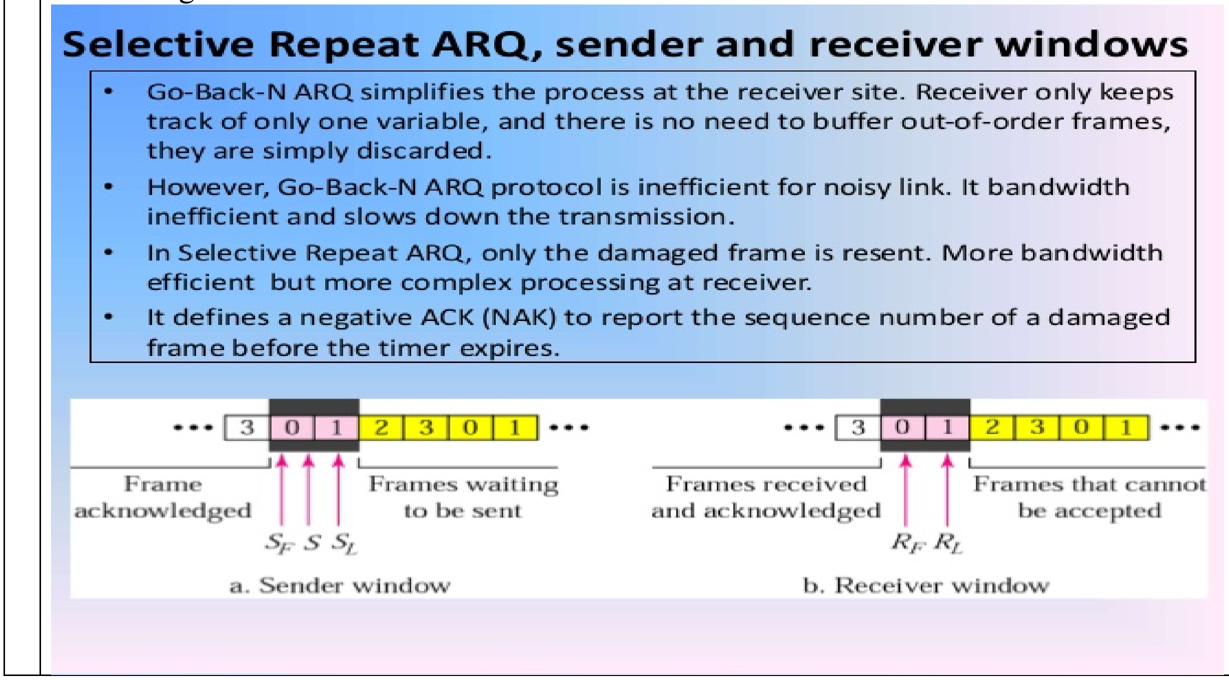
Go-Back-N ARQ, sender window size

- Size of the sender window must be less than 2 m. Size of the receiver is always 1. If m = 2, window size = 2 m – 1 = 3.
- Fig compares a window size of 3 and 4.

Accepts as the 1st frame in the next cycle-an error

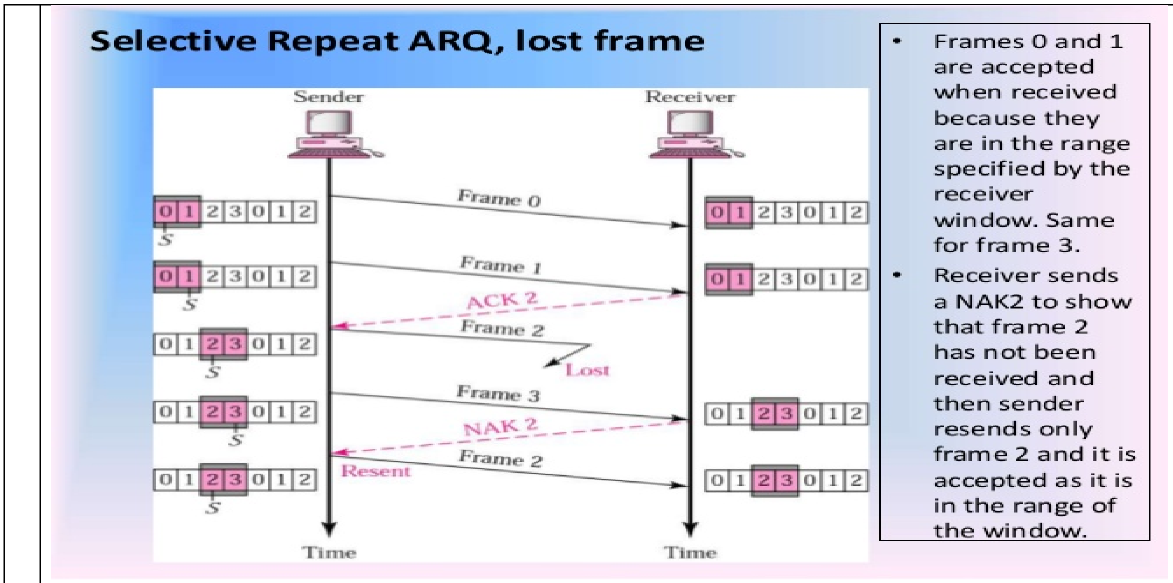
2) Selective Repeat ARQ

In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.



Selective Repeat ARQ, sender and receiver windows

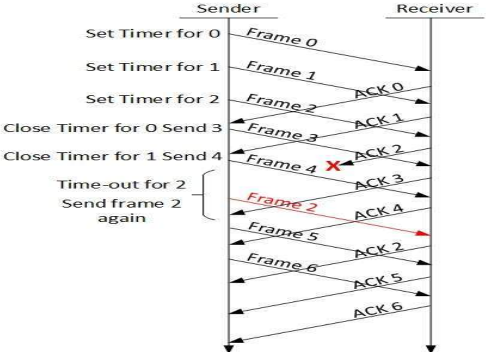
- Go-Back-N ARQ simplifies the process at the receiver site. Receiver only keeps track of only one variable, and there is no need to buffer out-of-order frames, they are simply discarded.
- However, Go-Back-N ARQ protocol is inefficient for noisy link. It bandwidth inefficient and slows down the transmission.
- In Selective Repeat ARQ, only the damaged frame is resent. More bandwidth efficient but more complex processing at receiver.
- It defines a negative ACK (NAK) to report the sequence number of a damaged frame before the timer expires.



Selective Repeat ARQ, lost frame

- Frames 0 and 1 are accepted when received because they are in the range specified by the receiver window. Same for frame 3.
- Receiver sends a NAK2 to show that frame 2 has not been received and then sender resends only frame 2 and it is accepted as it is in the range of the window.

In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged.



The sender in this case, sends only packet for which NACK is received.

7 **Explain Ethernet and Multiple Access Networks(802.3).** [10] CO2 L2

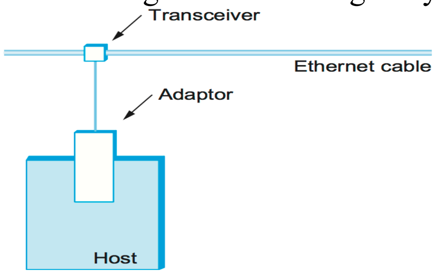
Developed in the mid-1970s by researchers at the Xerox Palo Alto Research Center (PARC), the Ethernet eventually became the dominant local area networking technology,e merging from a pack of competing technologies.

The more general name for the technology behind the Ethernet is Carrier Sense, Multiple Access with Collision Detect (CSMA/CD). As indicated by the CSMA name, the Ethernet is a multiple-access network, meaning that a set of nodes sends and receives frames over a shared link. You can, therefore, think of an Ethernet as being like a bus that has multiple stations plugged into it. The "carrier sense" in CSMA/CD means that all the nodes can distinguish between an idle and a busy link, and "collision detect" means that a node listens as it transmits and can therefore detect when a frame it is transmitting has interfered (collided) with a frame transmitted by another node.

Ethernet standard in 1978. This standard then formed the basis for IEEE standard 802.3, which additionally defines a much wider collection of physical media over which an Ethernet can operate, including 100-Mbps, 1-Gbps, 10-Gbps, 40-Gbps, and 100-Gbps versions.

Physical Properties

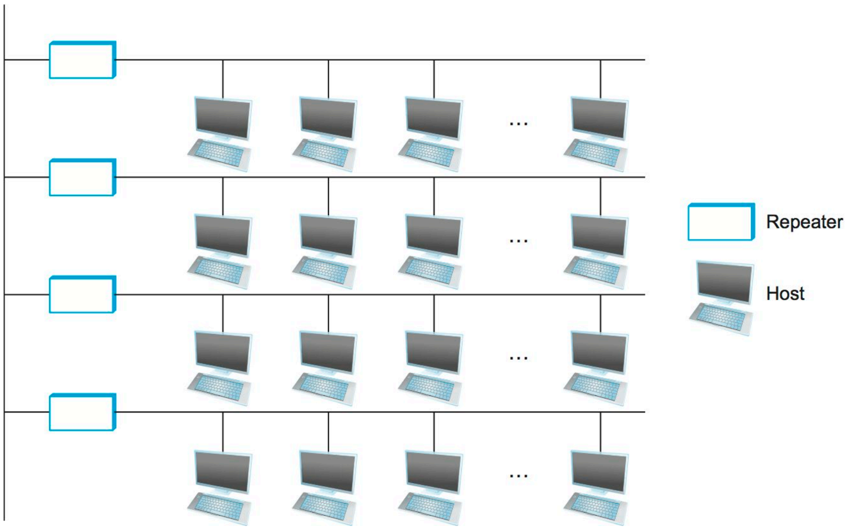
- **Ethernet transceiver and adaptor**
- Ethernet segments were originally implemented using coaxial cable of length up to 500 m.



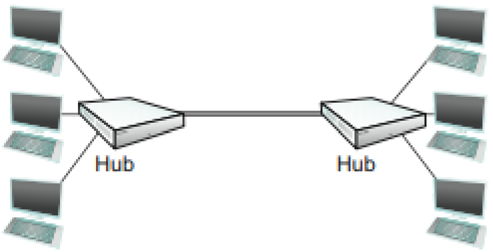
-
- A transceiver, a small device directly attached to the tap, detected when the line was idle and drove

the signal when the host was transmitting.

- The transceiver, in turn, connected to an Ethernet adaptor, which was plugged into the host.
- **Ethernet Repeater**
- Multiple Ethernet segments can be joined together by repeaters.



- A repeater is a device that forwards digital signals, much like an amplifier forwards analog signals; repeaters do not understand bits or frames.
- For example, using just two repeaters between any pair of hosts supports a configuration similar to the one illustrated in Figure. —that is, a segment running down the spine of a building with a segment on each floor.
- **Ethernet hub**
- Like a repeater, a hub just repeats whatever signals it hears on one port out all its other ports.
- The important thing about hubs is that they can be used to connect node to a shared Ethernet without using a tap.
- the link can be implemented in fiber or twisted pair copper, and not a coax cable.
- This is necessary to achieve the higher Ethernet performance levels.



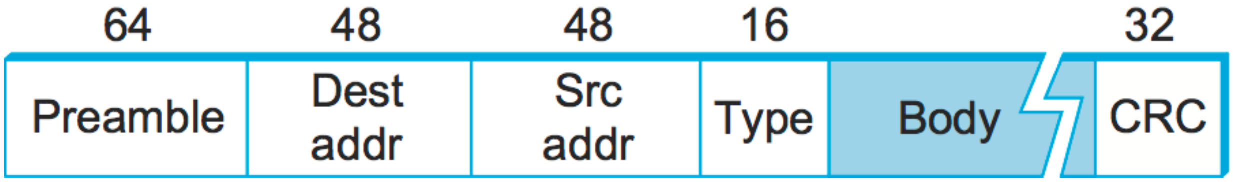
■ FIGURE 2.24 Ethernet hub.

- Any signal placed on the Ethernet by a host is broadcast over the entire network; that is, the signal is propagated in both directions, and repeaters and hubs forward the signal on all outgoing segments.
- It is important to understand that whether a given Ethernet spans a single segment, a linear sequence of segments connected by repeaters, or multiple segments connected in a star configuration by a hub, data transmitted by any one host on that Ethernet reaches all the other hosts. This is the good news.
- The bad news is that all these hosts are competing for access to the same link, and, as a consequence, they are said to be in the same collision domain. The multi-access part of the Ethernet is all about dealing with the competition for the link that arises in a collision domain.

Access Protocol

- This algorithm is commonly called the Ethernet's media access control (MAC). It is typically implemented in hardware on the network adaptor. We will not describe the hardware per se, but instead focus on the algorithm it implements. First, however, we describe the Ethernet's frame format and addresses.

- **Frame Format:-**

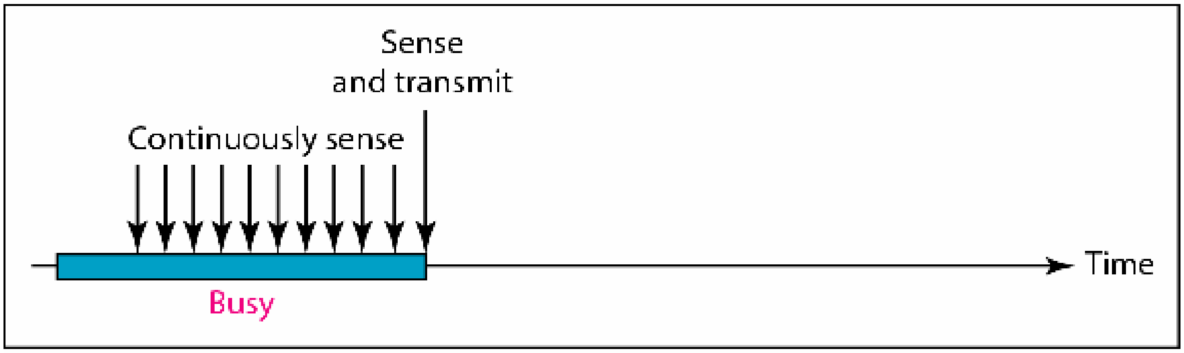


- The 64-bit preamble allows the receiver to synchronize with the signal; it is a sequence of alternating 0s and 1s.
- Both the source and destination hosts are identified with a 48-bit address.
- The packet type field serves as the demultiplexing key; it identifies to which of possibly many higher-level protocols this frame should be delivered.
- a frame must contain at least 46 bytes of data, even if this means the host has to pad the frame before transmitting it. The reason for this minimum frame size is that the frame must be long enough to detect a collision.
- each frame includes a 32-bit CRC. Like the HDLC protocol described in an earlier section, the Ethernet is a bit-oriented framing protocol.
- an Ethernet frame has a 14-byte header: two 6-byte addresses and a 2-byte type field. The sending adaptor attaches the preamble and CRC before transmitting, and the receiving adaptor removes them.
- **Addresses**
- every Ethernet host in the world— has a unique Ethernet address. Technically, the address belongs to the adaptor, not the host; it is usually burned into ROM.
- Ethernet addresses are typically printed in a form humans can read as a sequence of six numbers separated by colons.
- Each number corresponds to 1 byte of the 6-byte e address and is given by a pair of hexadecimal digits, one for each of the 4-bit nibbles in the byte; leading 0s are dropped.
- For example, 8:0:2b:e4:b1:2 is the human-readable representation of Ethernet address
- 00001000 00000000 00101011 11100100 10110001 00000010
- Each frame transmitted on an Ethernet is received by every adaptor connected to that Ethernet. Each adaptor recognizes those frames addressed to its address and passes only those frames on to the host.
- **Transmitter Algorithm**
- When the adaptor has a frame to send and the line is idle, it transmits the frame immediately; there is no negotiation with the other adaptors.
- CSMA/CD (Collision Detection):-
- ***CSMA (all previous methods) has an inefficiency:***
- If a collision has occurred, the channel is **unstable** until colliding packets have **<u>been fully transmitted</u>** ***CSMA/CD*** *(Carrier Sense Multiple Access with Collision Detection)* ***overcomes this as follows:***
- While transmitting, the sender is **listening to medium** for collisions.
- Sender **stops transmission** if collision has occurred **reducing channel wastage** .
- CSMA/CD is Widely used for **bus topology LANs** (IEEE 802.3, Ethernet).
- Types of CSMA Protocols

    Non-Persistent CSMA
    1-Persistent CSMA
    p-Persistent CSMA

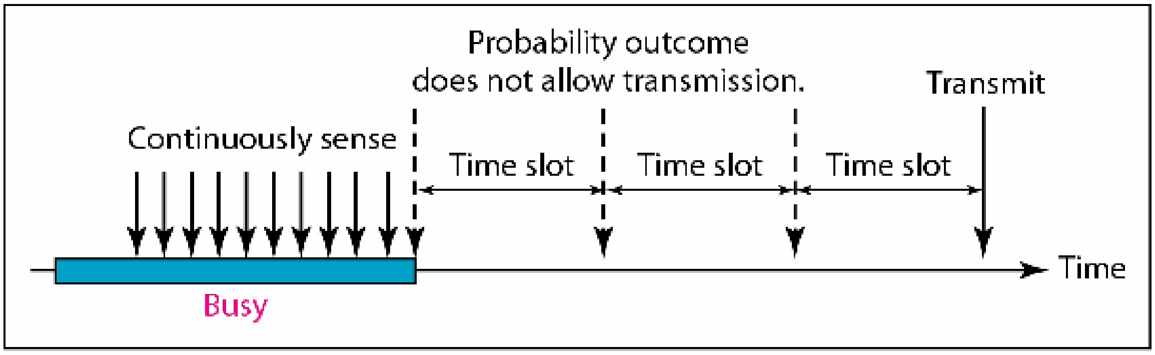
- **1-persistent CSMA**
- To avoid idle channel time, 1-persistent protocol used Station wishing to transmit listens to the medium:
- If medium idle, **transmit** immediately;
- If medium busy, **continuously listen** until medium becomes idle; then transmit immediately with probability 1
- **Performance**

- 1-persistent stations are **selfish** If two or more stations becomes ready at the same time, **collision guaranteed.**



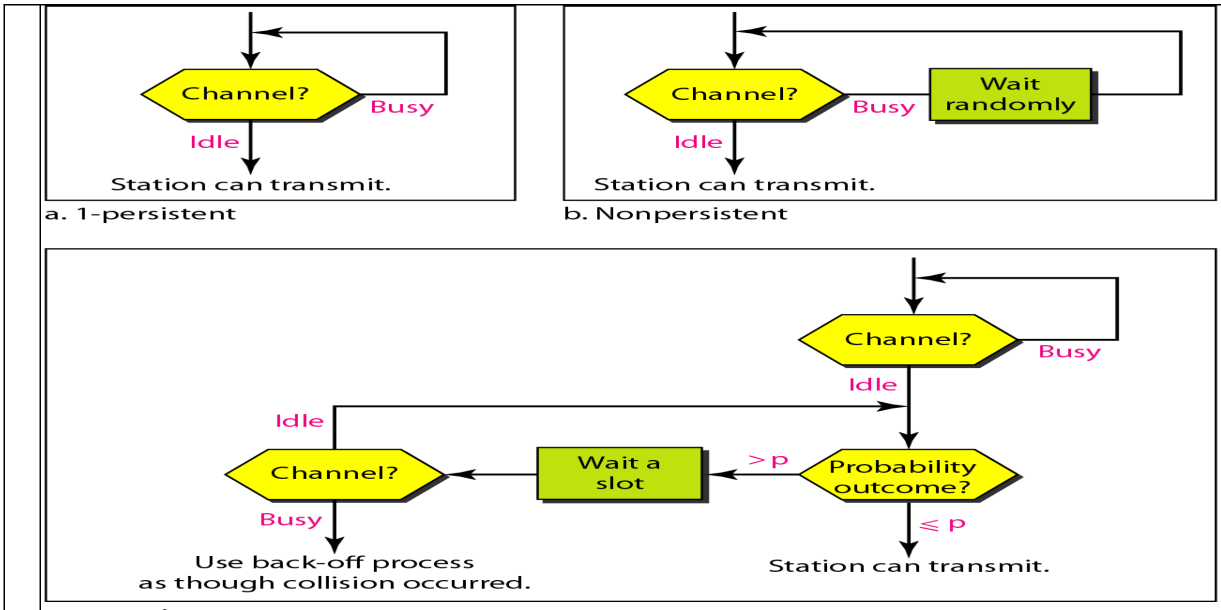
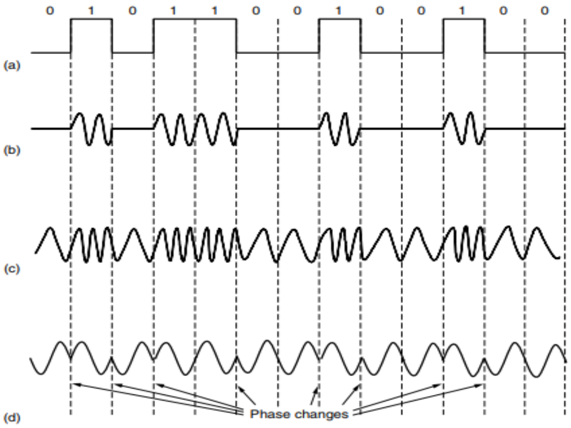
- a. 1-persistent

- **P-persistent CSMA**
- Time is divided to slots where each Time unit (slot) typically equals maximum propagation delay Station wishing to transmit listens to the medium:
- If medium idle, transmit with probability (p), OR wait one time unit (slot) with probability (1 – p), then repeat 1.
- If medium busy, continuously listen until idle and repeat step 1
- **Performance**
- Reduces the possibility of collisions like non persistent Reduces channel idle time like 1-persistent.
-



c. p-persistent

- **Non persistent CSMA**
- A station with frames to be sent, should sense the medium
- If medium is idle, **transmit**; otherwise, go to 2
- If medium is busy, (**backoff**) wait a ***random*** **amount of time** and repeat **1**
- Non-persistent Stations are **deferential (respect others)**
- **Performance:**
- Random delays reduces probability of collisions because two stations with data to be transmitted will wait for different amount of times.
- Bandwidth is **wasted** if waiting time (backoff) is large because medium will remain idle following end of transmission even if one or more stations have frames to send

	 Channel? Busy Idle Station can transmit. Channel? Busy Wait randomly Idle Station can transmit. Channel? Busy Idle Idle Channel? Busy Use back-off process as though collision occurred. Wait a slot > p Probability outcome? ≤ p Station can transmit.a. 1-persistent b. Nonpersistent c. p-persistent			
8	**Show the NRZ,NRZI and Manchester encoding for the bits pattern 0101100100100.**  0 1 0 1 1 0 0 1 0 0 1 0 0 (a) (b) (c) (d) Phase changes	[10]	CO3	L4