Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Information Technology

Session 2018-2019 (Even Semester)

Sixth Semester **Subject: Computer Networks**

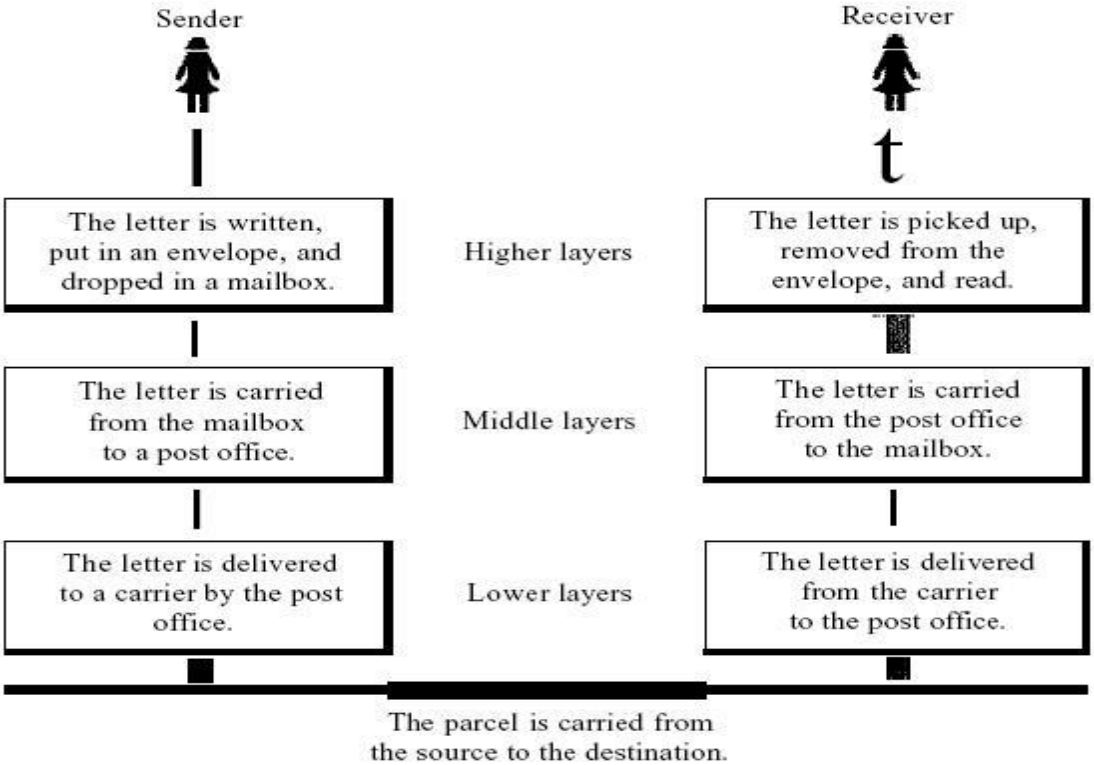
Unit – I

Syllabus

Computer networks & Internet, Network architecture, layered approach, OSI reference model, TCP/IP protocol suite, performance issues in networks, throughput, delay, latency, jitter, packet delivery ratio, packet loss rate, reliability, Introduction to Wireless Networks, IEEE 802.11, Bluetooth and WiMAX, wireless transmission, infrared transmission

Q 1) What are the reasons for using layered protocols? [5M]

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail. The process of sending a letter to a friend would be complex if there were no services available from the post office. Below Figure shows the steps in this task.



Sender, Receiver, and Carrier

In Figure we have a sender, a receiver, and a carrier that transports the letter. There is a hierarchy of tasks.

At the Sender Site

Let us first describe, in order, the activities that take place at the sender site.

o Higher layer. The sender writes the letter, inserts the letter in an envelope, writes the sender and receiver addresses, and drops the letter in a mailbox.

o Middle layer. The letter is picked up by a letter carrier and delivered to the post office.

o Lower layer. The letter is sorted at the post office; a carrier transports the letter.

0n the Way: The letter is then on its way to the recipient. On the way to the recipient's local post office, the letter may actually go through a central office. In addition, it may be transported by truck, train, airplane, boat, or a combination of these.

Q 2) What is the principal difference between connectionless communication and connection oriented communication? [4]

Ans: Layers can offer two different types of service to the layers above them: connection-oriented and connectionless.

Connection -oriented service (modeled after the telephone system): to use it, the service user first establishes a connection, uses the connection, and then releases the connection. The essential aspect of a connection is that it acts like a tube: the sender pushes objects (bits) in at one end, and the receiver takes them out in the same order at the other end.

Connectionless service (modeled after the postal system): Each message carries the full destination address, and each one is routed through the system independent of all the others. Order of the messages is not preserved.

Quality of service - some services are reliable in the sense that they never lose data. Reliability is usually implemented by having the receiver acknowledge the receipt of each message. The acknowledgment process is often worth but introduces sometimes undesirable overheads and delays.

Reliable connection-oriented service has two minor variation:

- message sequences - the message boundaries are preserved.
- byte streams - the connection is simply a stream of bytes, with no message boundaries.

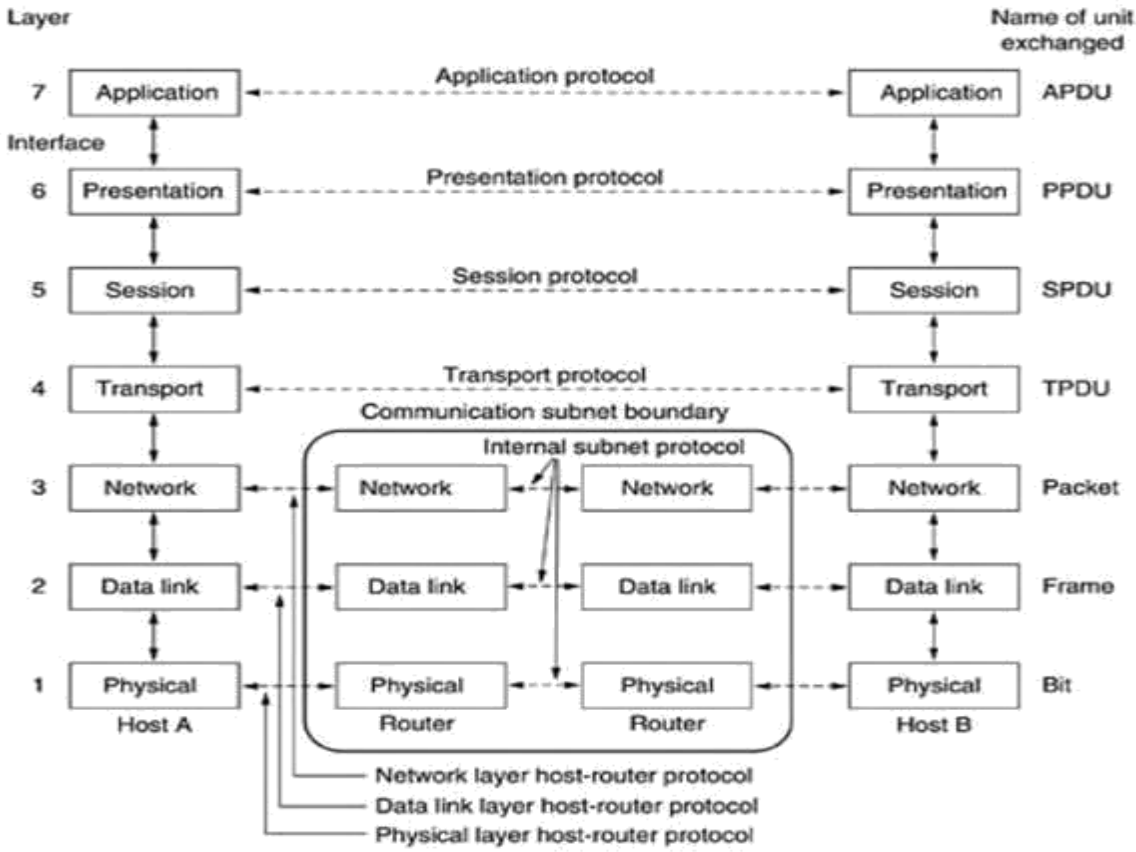
Applications where delays introduced by acknowledgment are unacceptable:

· digitized voice traffic,
· video film transmission.

The use of connectionles service

- electronic junk mail (third class mail as advertisements) - this service is moreover unreliable (meaning not acknowledged). Such connectionless services are often called datagram services.
- acknowledged datagram services - connectionless datagram services with acknowledgment.
- request-reply service - the sender transmits a single datagram containing a request. The reply contains the answer. Request-reply is commonly used to implement communication in the client-server model.

Q. 3) Enumerate the functions of seven layers of ISO-OSI reference model with the help of block diagram. [8M]
Ans:



The OSI reference model

The Physical Layer:

The physical layer is concerned with transmitting raw bits over a communication channel. The

design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit.

The Data Link Layer:

The main task of the data link layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer. It accomplishes this task by having the sender break up the input data into data frames (typically a few hundred or a few thousand bytes) and transmits the frames sequentially. If the service is reliable, the receiver confirms correct receipt of each frame by sending back an acknowledgement frame.

Another issue that arises in the data link layer (and most of the higher layers as well) is how to keep a fast transmitter from drowning a slow receiver in data. Some traffic regulation mechanism is often needed to let the transmitter know how much buffer space the receiver has at the moment. Frequently, this flow regulation and the error handling are integrated.

The Network Layer:

The network layer controls the operation of the subnet. A key design issue is determining how packets are routed from source to destination. Routes can be based on static tables that are "wired into" the network and rarely changed. They can also be determined at the start of each conversation, for example, a terminal session (e.g., a login to a remote machine). Finally, they can be highly dynamic, being determined anew for each packet, to reflect the current network load.

If too many packets are present in the subnet at the same time, they will get in one another's way, forming bottlenecks. The control of such congestion also belongs to the network layer. More generally, the quality of service provided (delay, transit time, jitter, etc.) is also a network layer issue.

When a packet has to travel from one network to another to get to its destination, many problems can arise. The addressing used by the second network may be different from the first one. The second one may not accept the packet at all because it is too large. The protocols may differ, and so on. It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected. In broadcast networks, the routing problem is simple, so the network layer is often thin or even nonexistent.

The Transport Layer:

The basic function of the transport layer is to accept data from above, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end. Furthermore, all this must be done efficiently and in a way that isolates the upper layers from the inevitable changes in the hardware technology. The transport layer also determines what type of service to provide to the session layer, and, ultimately, to the users of the network. The most popular type of transport connection is an error-free point-to-point channel that delivers messages or bytes in the order in which they were sent. However, other possible kinds of transport service are the transporting of isolated messages, with no guarantee about the order of delivery, and the broadcasting of messages to multiple destinations. The type of service is determined when the connection is established.

The transport layer is a true end-to-end layer, all the way from the source to the destination. In other words, a program on the source machine carries on a conversation with a similar program on the destination machine, using the message headers and control messages. In the lower layers, the protocols are between each machine and its immediate neighbours, and not between the ultimate source and destination machines, which may be separated by many routers.

The Session Layer:

The session layer allows users on different machines to establish sessions between them. Sessions offer various services, including dialog control (keeping track of whose turn it is to transmit), token management (preventing two parties from attempting the same critical operation at the same time), and synchronization (check pointing long transmissions to allow them to continue from where they were after a crash).

The Presentation Layer:

The presentation layer is concerned with the syntax and semantics of the information transmitted. In order to make it possible for computers with different data representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used "on the wire." The presentation layer manages these abstract data structures and allows higher-level data structures (e.g., banking records), to be defined and exchanged.

The Application Layer:

The application layer contains a variety of protocols that are commonly needed by users. One widely-used application protocol is HTTP (Hypertext Transfer Protocol), which is the basis for the World Wide Web. When a browser wants a Web page, it sends the name of the page it wants to the server using HTTP. The server then sends the page back. Other application protocols are

used for file transfer, electronic mail, and network news.

Q. 4) Which of the OSI layers handle each of the following :

(i) Dividing the transmitted bit streams into frames

Ans: DataLink layer

(ii) Determine which route through the subnet to use?

Ans: Transport Layer

Q. 5) Differentiate between OSI model and TCP / IP model. [4M]
Ans:

OSI Model:

1)It has 7 layers
2)Transport layer gurantees delivery of packets
3)Horizontal approach
4)Separate presentation layer
5)Separate session layer
6)Network layer provides both connectionless and connection oriented services
7)It defines the services,interfaces and protocols very clearly and makes a clear distinction between them
8)The protocol are better hidden and can be easily replaced as the technology changes
9)OSI truly is a general model
10)It has a problem of protocol filtering into a model

TCP/IP Model:

1)Has 4 layers
2)Transport layer does not gurantees delivery of packets
3)Vertical approach
4)No session layer, characteristics are provided by transport layer
5)No presentation layer, characteristics are provided by application layer
6)Network layer provides only connection less services
7)It does not clearly distinguishes between service interface and protocols
8)It is not easy to replace the protocols
9)TCP/IP can not be used for any other application
10)The model does not fit any protocol stack.

Q. 6) Define following terms with formula if any. [10M]
1) Jitter 2) Latency 3) Throughput
4) Packet loss rate 5) Packet delivery ratio.

Ans:

1) Jitter:

- The variation (i.e., standard deviation) in the delay or packet arrival times is called jitter.
- The sending side transmits packets in a continuous stream and spaces them evenly apart.
- Because of network congestion, improper queuing, or configuration errors, the delay between packets can vary instead of remaining constant.
- This variation causes problems for audio playback at the receiving end. Playback may experience gaps while waiting for the arrival of variable delayed packets.

2) Latency:

Latency is the amount of time a message takes to traverse a system. In a **computer network**, it is an expression of how much time it takes for a packet of data to get from one designated point to another. It is sometimes measured as the time required for a packet to be returned to its sender.

3) Throughput:

throughput is the amount of data moved successfully from one place to another in a given time period, and typically measured in bits per second (bps), as in megabits per second (Mbps) or gigabits per second (Gbps).

4) Packet loss rate:

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is typically caused by network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent.

5) Packet delivery ratio:

Packet Delivery ratio is the ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender.

Q. 7) Describe following Transmission medium. [4M]

1) Infrared transmission. 2) Radio Transmission. 3) Bluetooth.

Ans:

1) Infrared transmission:

- Infrared signals, with frequencies from 300 GHz to 400 THz can be used for short-range communication.
- Infrared signals cannot penetrate walls. This advantageous characteristic prevents interference between one system and another: a short-range communication system in one room cannot be affected by another system in the next room.
- When we use our infrared remote control, we do not interfere with the use of the remote by our neighbors. This characteristic makes infrared signals useless for long-distance communication.

- We cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.
- No licensing is required for infrared signals, that is, no frequency allocation issues with infrared signals

Infrared (or milimeter) waves characteristics :

- Used by remote controls for TV, VCRs, etc.
- Cheap and easy to build.
- Straight line, no obstacles - even more so than microwaves.
- Used for wireless LANs within a room.

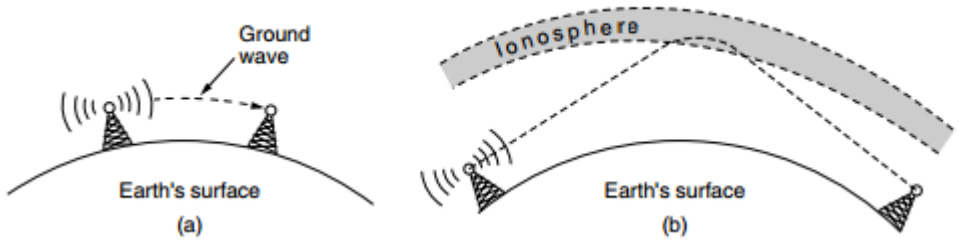
- **Applications of Infrared**
  - Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.
  - The infrared band, almost 400 THz, has an excellent potential for data transmission.
  - The Infrared Data Association (IrDA), an association for sponsoring the use of infrared waves, has established standard for using these signals for communications between devices such as keyboards, mice, PCs, and printers.
  - For example, some manufactures provide a special port called the IrDA port that allows a wireless keyboard to communicate with a PC.

2) Radio Transmission:

Ans:

- Radio frequency (RF) waves are easy to generate, can travel long distances, and can penetrate buildings easily, so they are widely used for communication, both indoors and outdoors.

- Radio waves also are omnidirectional, meaning that they travel in all directions from the source, so the transmitter and receiver do not have to be carefully aligned physically.
- The properties of radio waves are frequency dependent.
- At low frequencies, radio waves pass through obstacles well, but the power falls off sharply with distance from the source—at least as fast as 1/r 2 in air—as the signal energy is spread more thinly over a larger surface. This attenuation is called path loss.
- At high frequencies, radio waves tend to travel in straight lines and bounce off obstacles.
- Path loss still reduces power, though the received signal can depend strongly on reflections as well.
- High-frequency radio waves are also absorbed by rain and other obstacles to a larger extent than are low-frequency ones.
- At all frequencies, radio waves are subject to interference from motors and other electrical equipment.
- In the VLF, LF, and MF bands, radio waves follow the ground, as illustrated in Fig. 2-12(a). These waves can be detected for perhaps 1000 km at the lower frequencies, less at the higher ones.
- AM radio broadcasting uses the MF band, which is why the ground waves from Boston AM radio stations cannot be heard easily in New York.
- Radio waves in these bands pass through buildings easily, which is why portable radios work indoors.
- The main problem with using these bands for data communication is their low bandwidth.



- In the HF and VHF bands, the ground waves tend to be absorbed by the earth. However, the waves that reach the ionosphere, a layer of charged particles circling the earth at a height of 100 to 500 km, are refracted by it and sent back to earth, as shown in Fig. 2-12(b).
- Under certain atmospheric conditions, the signals can bounce several times. Amateur radio operators (hams) use these bands to talk long distance.
- The military also communicate in the HF and VHF bands.

3) Bluetooth:

Bluetooth is a wireless LAN technology designed to connect devices of different functions such

as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, and so on. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet. A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability. A Bluetooth LAN, by nature, cannot be large. If there are many gadgets that try to connect, there is chaos.

Bluetooth technology has several applications. Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology. Monitoring devices can communicate with sensor devices in a small health care center. Home security devices can use this technology to connect different sensors to the main security controller. Conference attendees can synchronize their laptop computers at a conference.

Bluetooth was originally started as a project by the Ericsson Company. It is named for Harald Blaatand, the king of Denmark (940-981) who united Denmark and Norway. *Blaatand* translates to *Bluetooth* in English.

Today, Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard. The standard defines a wireless personal-area network (PAN) operable in an area the size of a room or a hall.

Q. 8)Differentiate between Bluetooth & WiMAX.

Ans: 1.“WiMAX” stands for “Worldwide Interoperability for Microwave Access”; “Wi-Fi” stands for “Wireless Fidelity.”

2.WiMAX provides wireless broadband connectivity for long ranges; Wi-Fi provides short-range, wireless broadband connectivity mostly within an office or home.

3.WiMAX is more controlled and requires a licensed spectrum; the service is deployed by the service providers. Wi-Fi can work in a less controlled environment; it works in an unlicensed environment and is less controlled. Moreover, the end users have to buy the devices.

4.WiMAX uses MAC protocol which is connection oriented; Wi-Fi uses connection-based or connectionless protocol called CSMA/CA.

Q. 8)Discuss about IEEE 802.11 and its architecture.

The IEEE 802.11 standard defines two kinds of services: the Basic Service Set (BSS) and the Extended Service Set (ESS) [1, 6]. The BSS is the basic building block of a wireless LAN. A BSS consists of stationary or mobile wireless stations and possibly a central base station (e.g., an AP). When a station is in the BSS, it can communicate with the other members of the BSS.

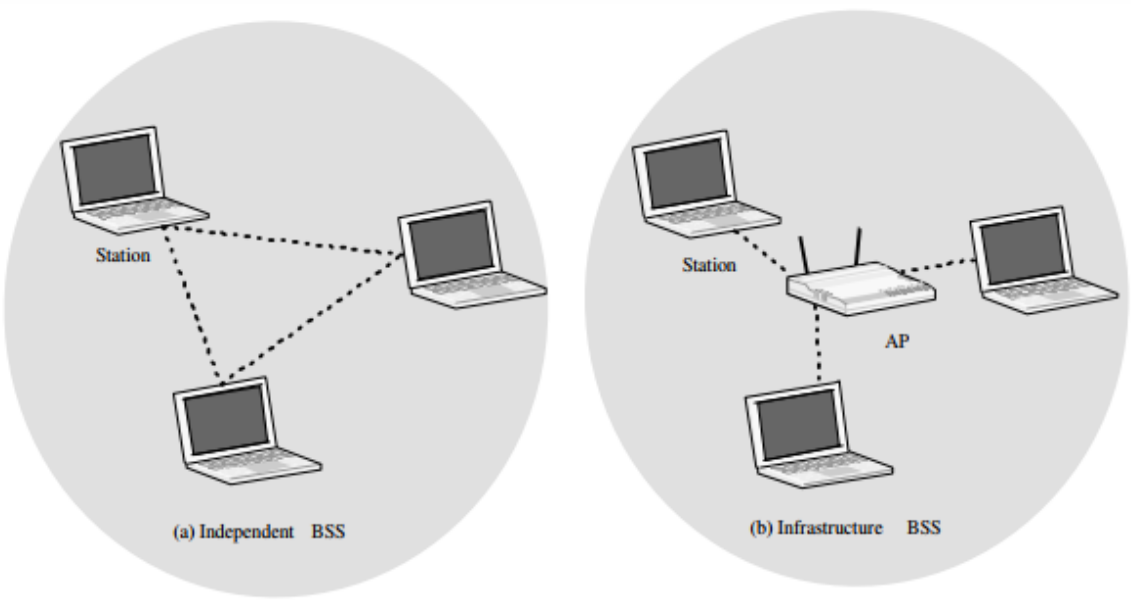


Figure 3: Independent and Infrastructure Basic Service Sets

The BSS without an AP is a stand-alone network and cannot send data to other BSSs. Such BSSs are called Independent BSSs (IBSS). Typically, IBSSs involve a small number of stations set up for a specific purpose and for a short period of time (e.g., creating a short-lived network to support a single meeting in a conference room). IBSSs are also referred to as ad hoc networks.

Infrastructure BSSs are distinguished from ad hoc networks by the use of an AP. APs are used for all communications in an infrastructure BSS, including communication between mobile nodes in the same service set. An infrastructure BSS is bounded by the coverage distance from the AP. The coverage area of a single AP is called a cell. All mobile stations are required to be within reach of the AP.

802.11 allows wireless networks of arbitrarily large size to be created by linking BSSs into an ESS. An ESS is created by chaining BSSs together with a backbone network. All the APs in an ESS are given the same Service Set Identifier (SSID), which serves as a network name for its users. APs in an ESS operate in a manner such that the outside world can use the station's MAC address to talk to a station without worrying about its location in the ESS.

Figure 4 shows three BSSs corresponding to three APs. There is an equal level of overlap between BSS 1 and BSS 2, and between BSS 2 and BSS 3. Such overlap is necessary to provide

stations with seamless connectivity if they move from one BSS to another. In the figure, the router uses the station's MAC address as the destination to deliver frames to a station; only the AP with which that station is associated delivers the frame.

Usually, mobility support is the primary motivation for deploying an 802.11 network. IEEE 802.11 allows mobility between BSSs at the link layer. However, it is not aware of anything that happens above the link layer. When stations move between BSSs, they will find and attempt to associate with an AP with the strongest signal and the least network traffic.This way, a mobile station can transition seamlessly from one AP in the network to another, without losing connectivity. This event is often referred to as roaming.

Tulsiramji Gaikwad-Patil College of Engineering and Technology
Wardha Road, Nagpur-441 108
NAAC Accredited

Department of Information Technology

Session 2018-2019 (Even Semester)

Sixth Semester **Subject: Computer Networks**

Unit – II

Syllabus

Design issues, framing, error control, flow control, error-correcting and detecting codes, Data link protocols, unrestricted simplex protocol, simplex stop-and-wait protocol, onebit sliding window protocol, Go Back N ARQ protocol, selective repeat ARQ protocol, static and dynamic channel allocation, ALOHA, CSMA/CD, CSMA/CA

Q.1 Explain various Framing Methods in Datalink layer.

Ans:

Framing:

Breaking the bit stream up into frames is called as framing. Following are the framing methods:

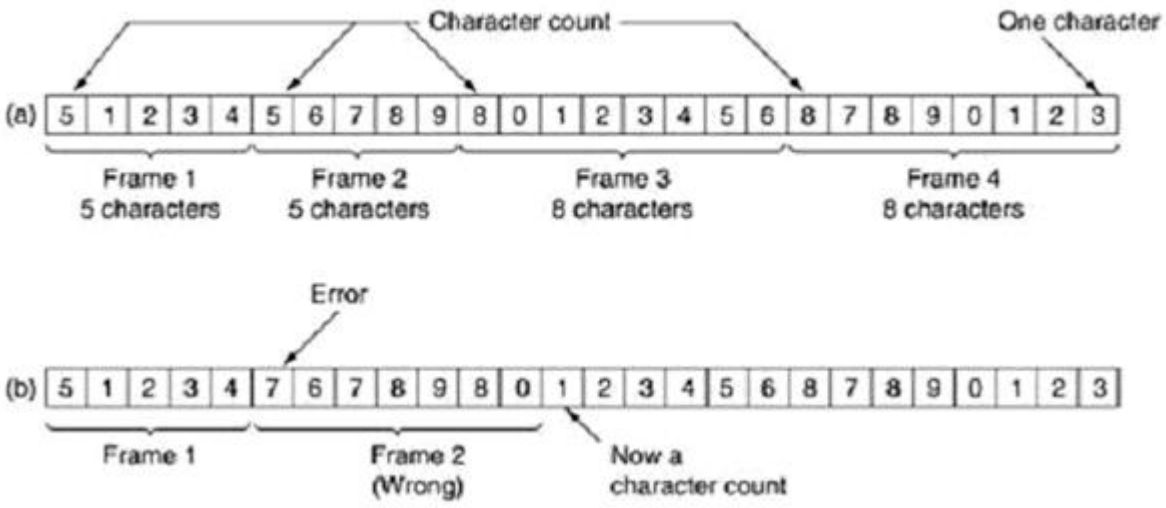
1. Character count.
2. Flag bytes with byte stuffing.
3. Starting and ending flags, with bit stuffing.
4. Physical layer coding violations.

1. Character count:

- This method uses a field in the header to specify the number of characters in the frame.
- When the data link layer at the destination sees the character count, it knows how many characters follow and hence where the end of the frame is. This technique is shown in Fig.3.1(a) for four frames of sizes 5, 5, 8, and 8 characters, respectively.
- The trouble with this algorithm is that the count can be garbled by a transmission

error.

- For example, if the character count of 5 in the second frame of Fig. 3.1(b) becomes a 7, the destination will get out of synchronization and will be unable to locate the start of the next frame.
- Even if the checksum is incorrect so the destination knows that the frame is bad, it still has no way of telling where the next frame starts.
- Sending a frame back to the source asking for a retransmission does not help either, since the destination does not know how many characters to skip over to get to the start of the retransmission. For this reason, the character count method is rarely used anymore.



2. Flag bytes with 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.
    - In the past, the starting and ending bytes were different, but in recent years most protocols have used the same byte, called a flag byte, as both the starting and ending delimiter, as shown in Fig.(a) as FLAG.
    - In this way, if the receiver ever loses synchronization, it can just search for the flag byte to find the end of the current frame.
    - Two consecutive flag bytes indicate the end of one frame and start of the next one.

- A serious problem occurs with this method when binary data, such as object programs or floating-point numbers, are being transmitted.
- It may easily happen that the flag byte's bit pattern occurs in the data. This situation will usually interfere with the framing.
- One way to solve this problem is to have the sender's data link layer insert a special escape byte (ESC) just before each "accidental" flag byte in the data.
- The data link layer on the receiving end removes the escape byte before the data are given to the network layer.
- This technique is called byte stuffing or character stuffing. Thus, a framing flag byte can be distinguished from one in the data by the absence or presence of an escape byte before it.
- If an escape byte occurs in the middle of the data, the it, too, is stuffed with an escape byte. Thus, any single escape byte is part of an escape sequence, whereas a doubled one indicates that a single escape occurred naturally in the data.
- Some examples are shown in Fig. 3.3(b). In all cases, the byte sequence delivered after de stuffing is exactly the same as the original byte sequence.

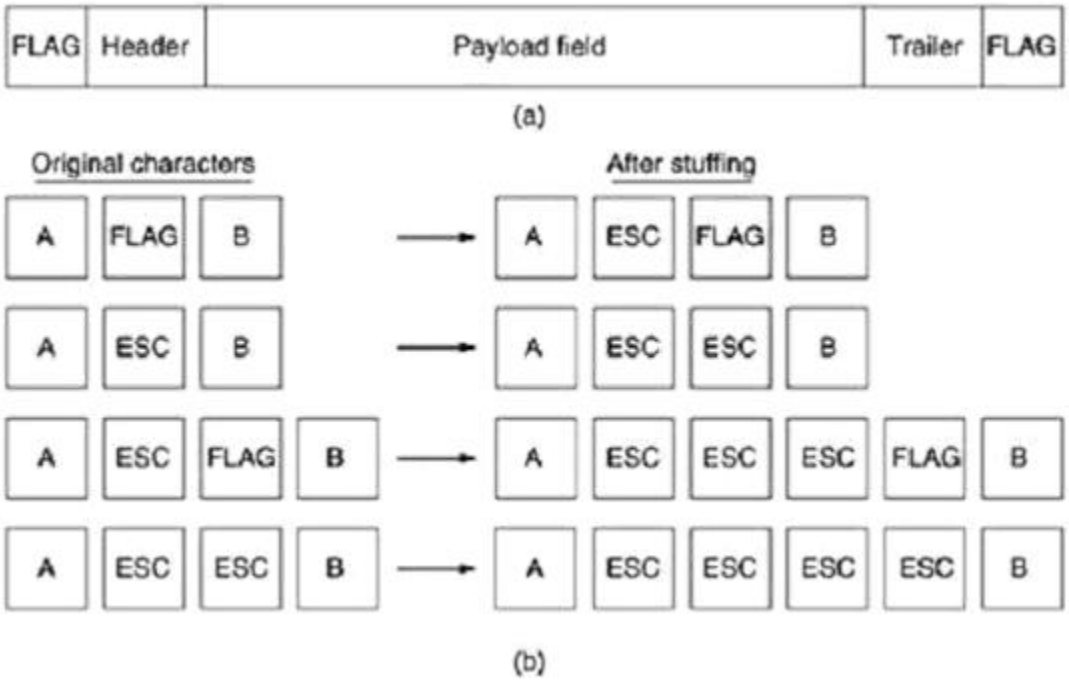


Fig. (a) A frame delimited by flag bytes (b) Four examples of byte sequences before and after byte stuffing

3. Starting and ending flags, with bit stuffing.
    - The new technique allows data frames to contain an arbitrary number of bits and allows character codes with an arbitrary number of bits per character.
    - Each frame begins and ends with a special bit pattern, 01111110 (in fact, 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. This bit stuffing is analogous to byte stuffing, in which an escape byte is stuffed into the outgoing character stream before a flag byte in the data.
    - When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automatically de stuffs (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.
    - With bit stuffing, the boundary between two frames can be unambiguously recognized by the flag pattern. Thus, if the receiver loses track of where it is, all it has to do is scan the input for flag sequences, since they can only occur at frame boundaries and never within the data.

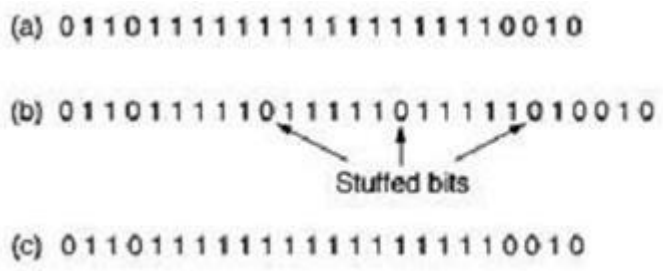


Figure 3.3 Bit stuffing. (a) The original data. (b) The data as they appear on the line. (c) The data as they are stored in the receiver's memory after destuffing.

4. Physical layer coding violations.
    - The last method of framing is only applicable to networks in which the encoding on the physical medium contains some redundancy. For example, some LANs encode 1 bit of data by using 2 physical bits.
    - Normally, a 1 bit is a high-low pair and a 0 bit is a low-high pair.
    - The scheme means that every data bit has a transition in the middle, making it easy for the receiver to locate the bit boundaries. The combinations high-high and low-low

are not used for data but are used for delimiting frames in some protocols.

Q. Explain the error control and flow control mechanism. How the flow control mechanism is implemented by data link layer ? [6M]

Ans:

Flow Control: Flow control coordinates that amount of data that can be sent before receiving acknowledgement.

- It is one of the most important duties of the data link layer.
- Flow control tells the sender how much data to send.
- It makes the sender wait for some sort of an acknowledgment (ACK) before continuing to send more data.
- *Flow Control Techniques: Stop-and-wait, and Sliding Window*

Error Control: Error control in the data link layer is based on ARQ (automatic repeat request), which is the retransmission of data.

- The term error control refers to methods of error detection and retransmission.
- Anytime an error is detected in an exchange, specified frames are retransmitted. This process is called ARQ.

To ensure reliable communication, there needs to exist flow control (managing the amount of data the sender sends), and error control (that data arrives at the destination error free).

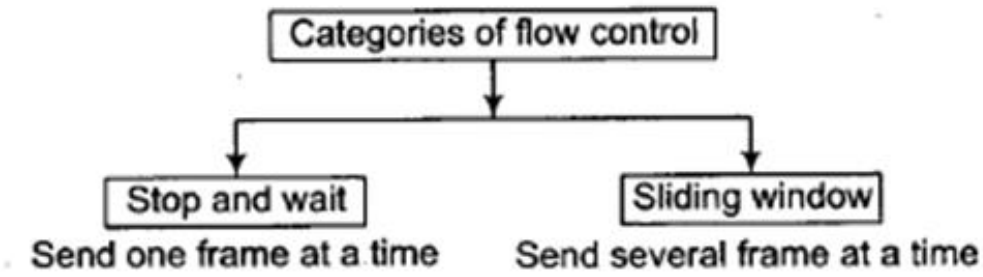
- Flow and error control needs to be done at several layers.
- For node-to-node links, flow and error control is carried out in the data-link layer.
- For end-point to end-point, flow and error control is carried out in the transport layer.

Flow & Error control:

- Error Detection and ARQ (error detection with retransmissions) must be combined with methods that intelligently limit the number of 'outstanding' (unACKed) frames.
- *Flow & Error control techniques: Stop-and-Wait ARQ, Go-Back-N ARQ, and Selective Repeat ARQ*

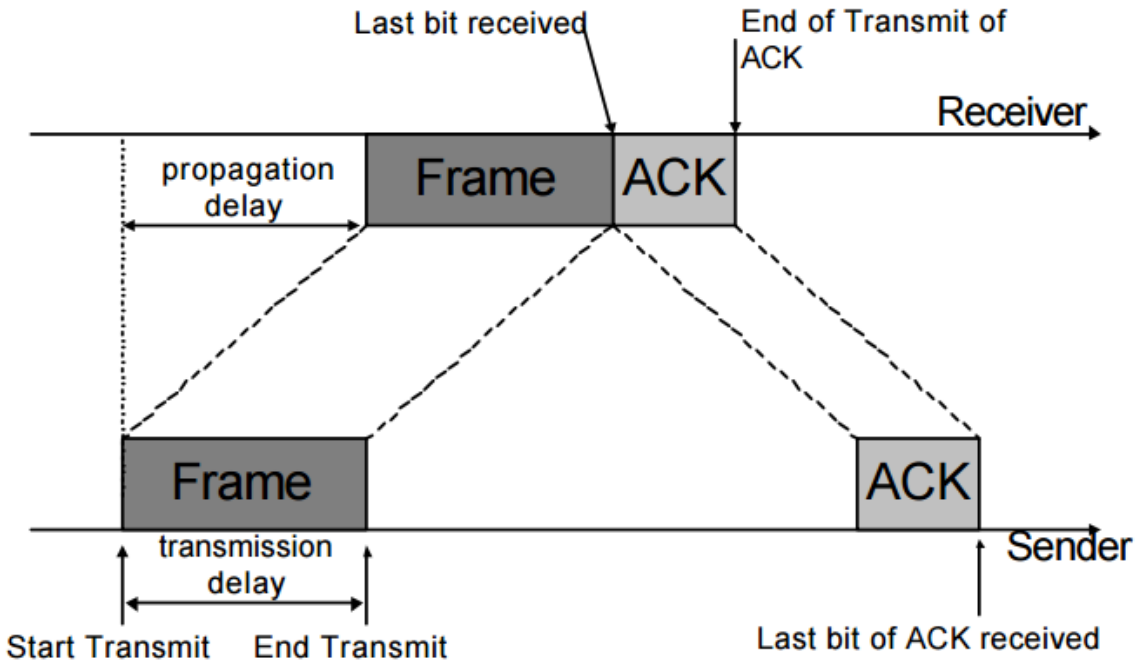
Flow Control Techniques:

- One important aspect of data link layer is flow control.
- Flow control refers to a set of procedures used to restrict the amount of data the sender can send before waiting for acknowledgement.



Stop and Wait Flow control:

- The sender has to wait for an acknowledgment of every frame that it sends.
- Only when a acknowledgment has been received is the next frame sent. This process continues until the sender transmits an End of Transmission (EOT) frame.
- In Stop-and-Wait flow control, the receiver indicates its readiness to receive data for each frame.



- For every frame that is sent, there needs to be an acknowledgment, which takes a similar amount of propagation time to get back to the sender.
- Only one frame can be in transmission at a time. This leads to inefficiency if propagation delay is much longer than the transmission delay
- **Advantages of Stop and Wait:**
  - It's simple and each frame is checked and acknowledged well.
- **Disadvantages of Stop and Wait:**
  - Only one frame can be in transmission at a time.
  - It is inefficient, if the distance between devices is long. Reason is propagation delay is much longer than the transmission delay.
  - The time spent for waiting acknowledgements between each frame can add significant amount to the total transmission time.

Sliding Window Flow Control:

- It works by having the sender and receiver have a "window" of frames.
- Each frame has to be numbered in relation to the sliding window. For a window of size n, frames get a number from 0 to n - 1. Subsequent frames get a number mod n.
- The sender can send as many frames as would fit into a window.
- The receiver, upon receiving enough frames, will respond with an acknowledgment of all frames up to a certain point in the window. It is called slide.
- This window can hold frames at either end and provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgement.
- For example, if n = 8, the frames are numbered 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4, 5, 6, 7, 0, 1...so on. The size of the window is (n -1) = 7.
- When the receiver sends an ACK, it includes the number of the next frame it expects to receive. When the receiver sends an ACK containing the number 5, it means all frames upto number 4 have been received.
- If the window size is sufficiently large the sender can continuously transmit packets:
    - If W >= (2a+1), sender can transmit continuously. **(Efficiency =1)**
    - If W < (2a+1), sender can transmit W frames every (2a+1) time units. **(Efficiency = W/(1+2a))**

Q. Explain Simplex stop-and-wait protocol.

Stop & Wait Protocol

• In this method of flow control, the sender sends a single frame to receiver & waits for an acknowledgment.

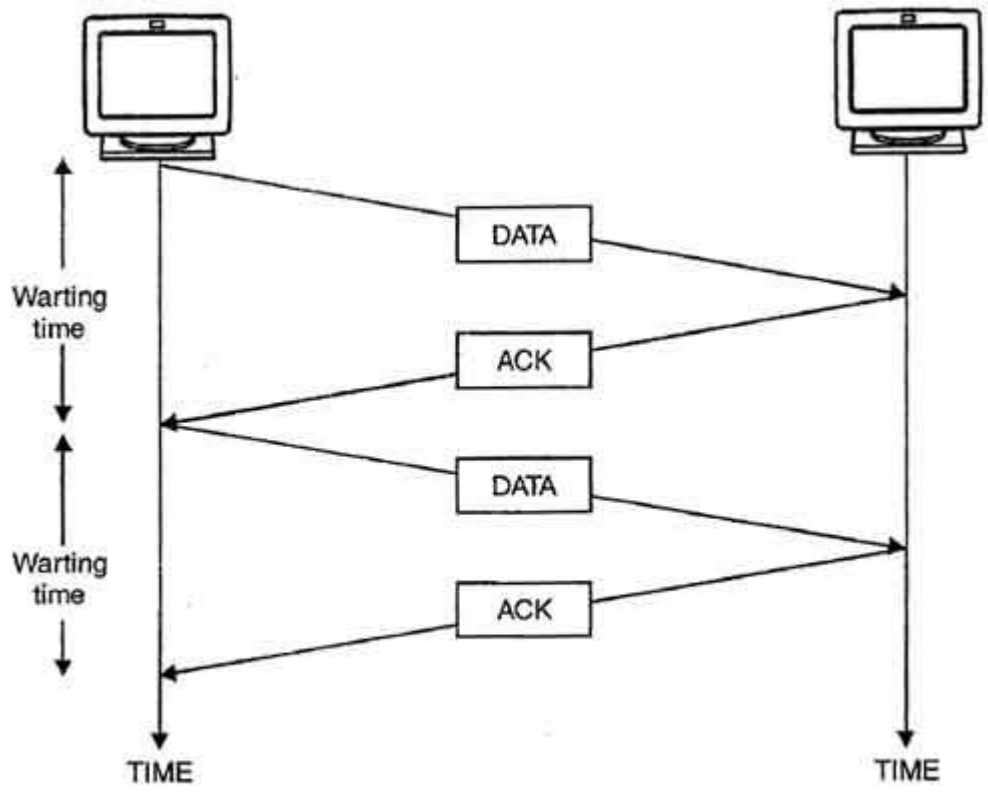
• The next frame is sent by sender only when acknowledgment of previous frame is received.

• This process of sending a frame & waiting for an acknowledgment continues as long as the sender has data to send.

• To end up the transmission sender transmits end of transmission (EOT) frame.

• The main advantage of stop & wait protocols is its accuracy. Next frame is transmitted only when the first frame is acknowledged. So there is no chance of frame being lost.

• The main disadvantage of this method is that it is inefficient. It makes the transmission process slow. In this method single frame travels from source to destination and single acknowledgment travels from destination to source. As a result each frame sent and received uses the entire time needed to traverse the link. Moreover, if two devices are distance apart, a lot of time is wasted waiting for ACKs that leads to increase in total transmission time.

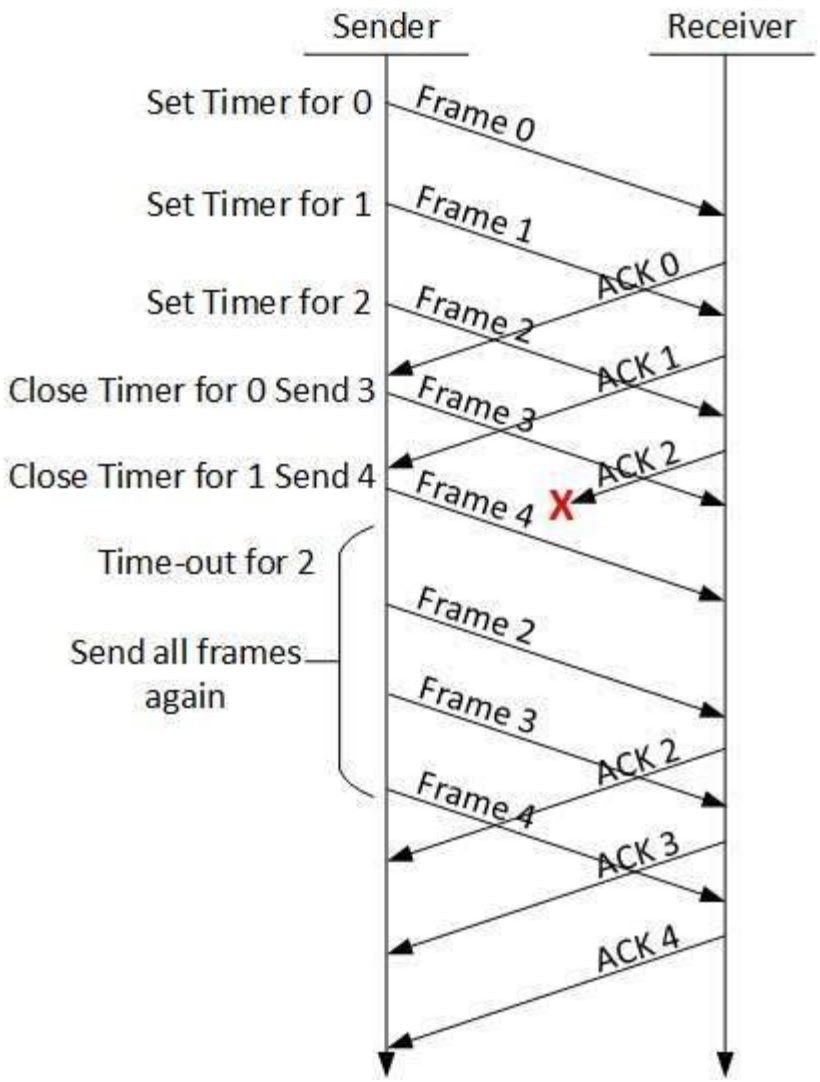


Stop & Wait Method.

Q. Write a short note on Go back N ARQ protocol.

Ans: Go-Back-N ARQ Protocol:

- 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.

Q. Explain One bit sliding window protocol.

Ans:

Q. Define piggybacking & its benefit. [3M]
Ans:

In two way communication, Whenever a data frame is received, the received waits and does not send the control frame (acknowledgement) back to the sender immediately.

The receiver waits until its network layer passes in the next data packet. The delayed acknowledgement is then attached to this outgoing data frame.

This technique of temporarily delaying the acknowledgement so that it can be hooked with next outgoing data frame is known as piggybacking.

• The major advantage of piggybacking is better use of available channel bandwidth.

Q. Explain 1-persistence, non-persistence & P-persistence CSMA protocol. [6M]

Ans:

(i) I-persistent CSMA

• In this method, station that wants to transmit data continuously senses the channel to check whether the channel is idle or busy.

• If the channel is busy, the station waits until it becomes idle.

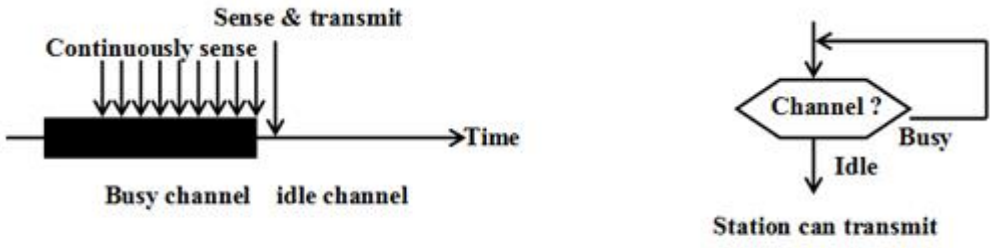
• When the station detects an idle-channel, it immediately transmits the frame with probability 1. Hence it is called I-persistent CSMA.

• This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.

• When the collision occurs, the stations wait a random amount of time and start allover again.

Drawback of I-persistent

• The propagation delay time greatly affects this protocol. Let us suppose, just after the station I begins its transmission, station 2 also became ready to send its data and senses the channel. If the station I signal has not yet reached station 2, station 2 will sense the channel to be idle and will begin its transmission. This will result in collision.



1-persistent CSMA

Even if propagation delay time is zero, collision will still occur. If two stations became .ready in the middle of third station's transmission, both stations will wait until the transmission of first station ends and then both will begin their transmission exactly simultaneously. This will also result in collision.

(ii) Non-persistent CSMA

• In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval oftime.
• After this time, it again checks the status of the channel and if the channel is.free it will transmit.

• A station that has a frame to send senses the channel.

• If the channel is idle, it sends immediately.

• If the channel is busy, it waits a random amount of time and then senses the channel again.

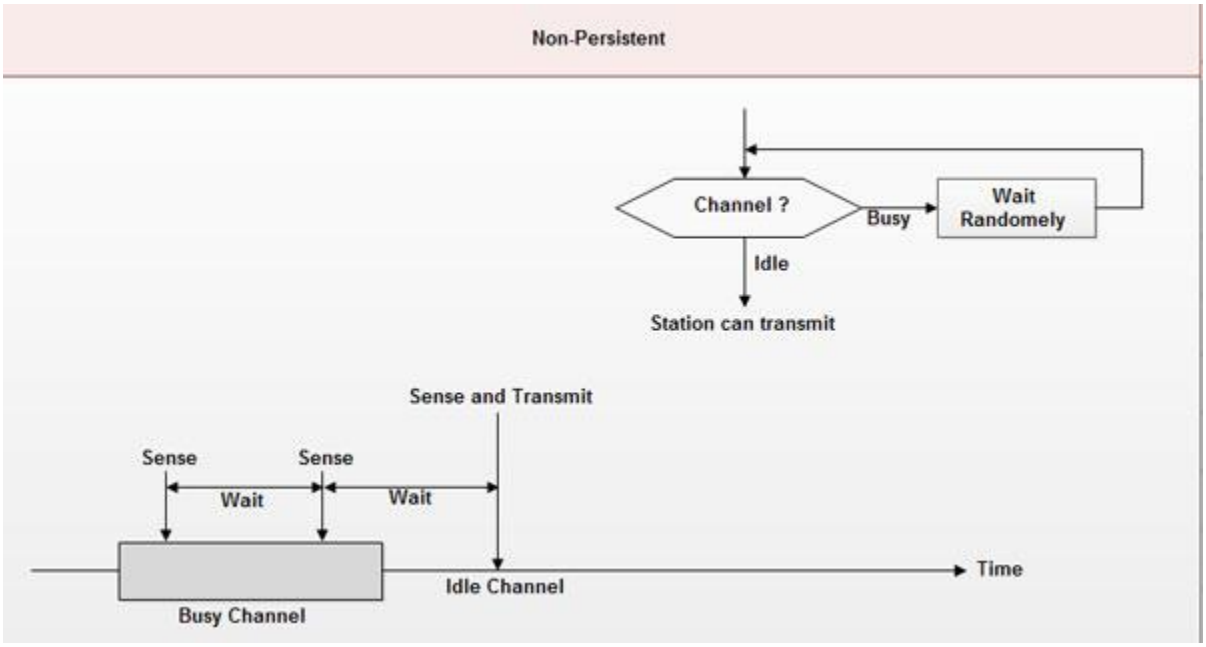
• In non-persistent CSMA the station does not continuously sense the channel for the purpose of capturing it when it detects the end of previous transmission.

Advantage of non-persistent

• It reduces the chance of collision because the stations wait a random amount of time. It is unlikely that two or more stations will wait for same amount of time and will retransmit at the same time.

Disadvantage of non-persistent

• It reduces the efficiency of network because the channel remains idle when there may be stations with frames to send. This is due to the fact that the stations wait a random amount of time after the collision.



(iii) p-persistent CSMA

• This method is used when channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time.

• Whenever a station becomes ready to send, it senses the channel.

• If channel is busy, station waits until next slot.

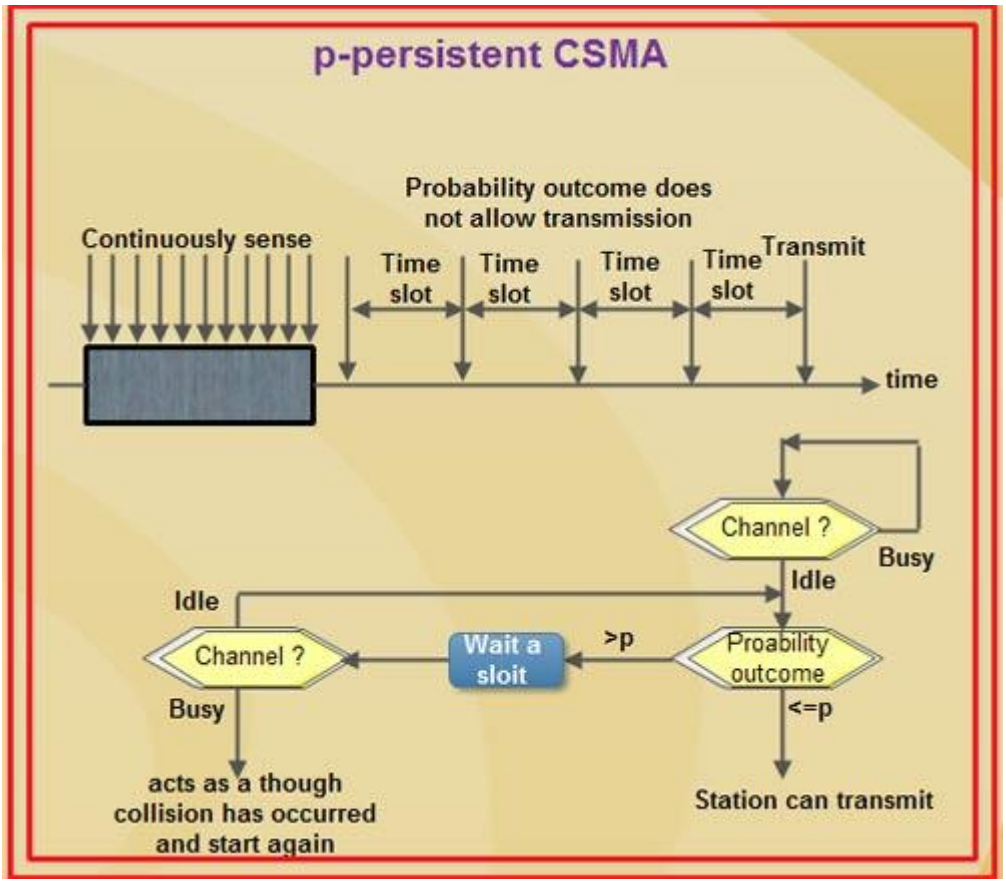
• If channel is idle, it transmits with a probability p.

• With the probability q=l-p, the station then waits for the beginning of the next time slot.

• If the next slot is also idle, it either transmits or waits again with probabilities p and q.

• This process is repeated till either frame has been transmitted or another station has begun transmitting.

• In case of the transmission by another station, the station acts as though a collision has occurred and it waits a random amount of time and starts again.



Advantage of p-persistent

• It reduces the chance of collision and improves the efficiency of the network.

Q. There is no acknowledgement mechanism in CSMA/CD, but we need this mechanism in CSMA/CA. Explain the reason. [3M]

Ans:

In CSMA/CD, the lack of detecting collision before the last bit of the frame is sentout is interpreted as an acknowledgment. In CSMA/CA, the sender cannot sense collision; there is a need for explicit acknowledgments.

Q. 4 c) With respect to data-link-layer what is the meaning of following term. [4M]
i) Framing ii) Pipe lining
iii) Piggy backing iv) Virtual bit pipe.

Ans:

i) Framing : Breaking the bit stream into discrete frames

ii) Pipe lining:

allowing the sender to transmit multiple contiguous frames (say up to w frames) before it receives an acknowledgement. This technique is known as pipelining.

iii) Piggy backing :In two way communication, Whenever a data frame is received, the receiver waits and does not send the control frame (acknowledgement) back to the sender immediately.

The receiver waits until its network layer passes in the next data packet. The delayed acknowledgement is then attached to this outgoing data frame.

This technique of temporarily delaying the acknowledgement so that it can be hooked with next outgoing data frame is known as piggybacking.

iv) Virtual bit pipe:
The function of the physical layer is to provide a virtual link for transmitting a sequence of bits between any pair of nodes (or any node and external site) joined by a physical communication channel. Such a virtual link is called a virtual bit pipe.

Q. Explain ALOHA system in detail.

Ans:

ALOHA:

In the 1970s, Norman Abramson and his colleagues at the University of Hawaii devised a new and elegant method to solve the channel allocation problem. Their work has been extended by many researchers since then (Abramson, 1985).

Although Abramson's work, called the ALOHA system, used ground-based radio broadcasting, the basic idea is applicable to any system in which uncoordinated users are competing for the use of a single shared channel. There are two versions of ALOHA: pure and slotted. They differ with respect to whether time is divided into discrete slots into which all frames must fit. Pure ALOHA does not require global time synchronization; slotted ALOHA does.

Pure ALOHA:

In pure ALOHA, the stations transmit frames whenever they have data to send.

• When two or more stations transmit simultaneously, there is collision and the frames are destroyed.

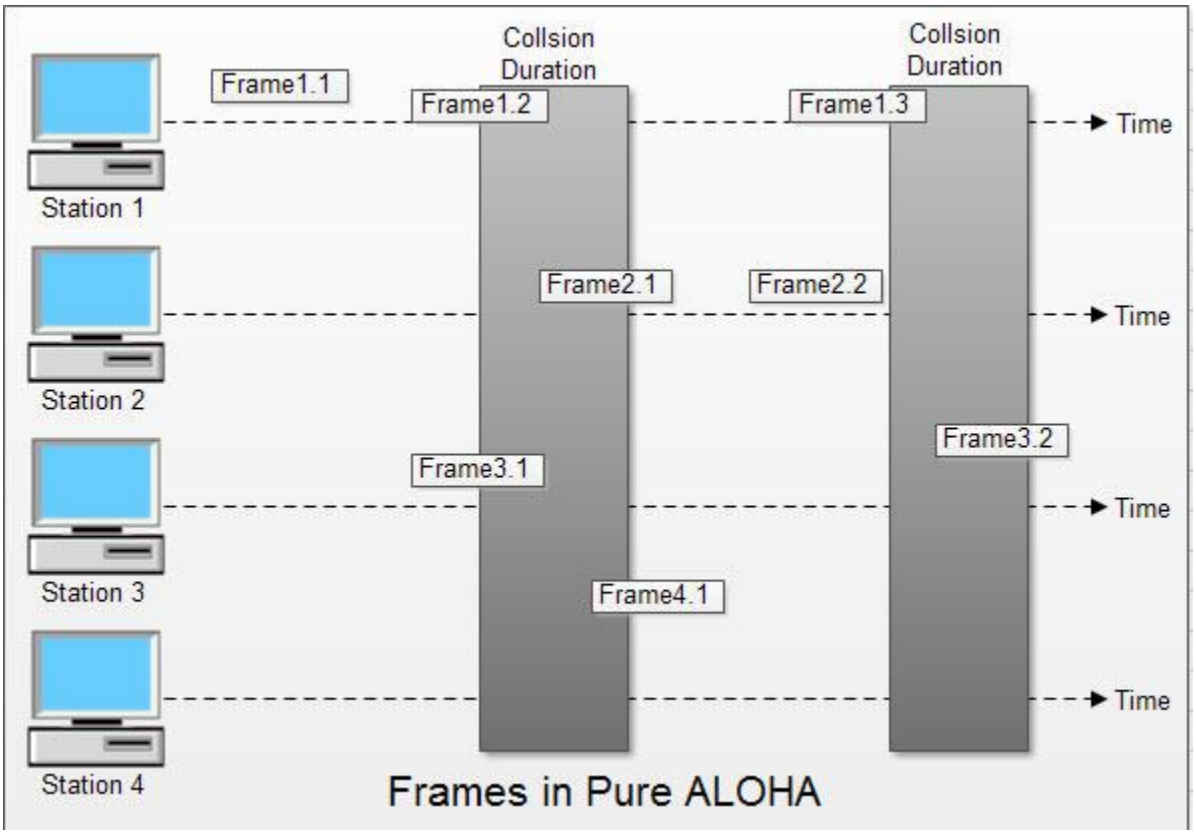
• In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.

• If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.

• If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.

• Therefore pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help avoid more collisions.

• Figure shows an example of frame collisions in pure ALOHA.



• In fig there are four stations that .contended with one another for access to shared channel. All these stations are transmitting frames. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames, frame 1.1 and frame 2.2 survive. All other frames are destroyed.

• Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged. If first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted