Module 2[Computer networks]

Part-B
Rajeshwari and PriyaNandini

1.Compare and contrast Go back N and the selective Repeat?

A.) Both Go-Back-N Protocol and Selective Repeat Protocol are the types of sliding window protocols.

The main difference between these two protocols is that after finding the suspect or damage in sent frames go-back-n protocol re-transmits all the frames whereas selective repeat protocol re-transmits only that frame which is damaged.

Now, we shall see the difference between them:

S.NO	Go-Back-N Protocol	Selective Repeat Protocol
1.	In Go-Back-N Protocol, if the sent frame is found suspected then all the frames are re-transmitted from the lost packet to the last packet transmitted.	In selective Repeat protocol, only those frames are re-transmitted which are found suspected.
2.	Sender window size of Go-Back-N Protocol is N.	Sender window size of the selective Repeat protocol is also N.
3.	Receiver window size of Go-Back-N Protocol is 1.	Receiver window size of the selective Repeat protocol is N.

4.	The Go-Back-N Protocol is less complex.	Selective Repeat protocol is more complex.
5.	In Go-Back-N Protocol, neither sender nor receiver need sorting.	In selective Repeat protocol, the receiver side needs sorting to sort the frames.
6.	In Go-Back-N Protocol, type of Acknowledgement is cumulative.	In selective Repeat protocol, type of Acknowledgement is individual.
7.	In Go-Back-N Protocol, Out-of-Order packets are NOT Accepted (discarded) and the entire window is re-transmitted.	In selective Repeat protocol, Out-of-Order packets are Accepted.
8..	In Go-Back-N Protocol, if Receive receives a corrupt packet, then also, the entire window is re-transmitted.	In selective Repeat protocol, if Receive receives a corrupt packet, it immediately sends a negative acknowledgement and hence only the selective packet is retransmitted.
9.	Efficiency of Go-Back-N Protocol is	Efficiency of selective Repeat protocol is also

N/(1+2*a)	N/(1+2*a)

2.)List and briefly discuss the two different basic transmission technologies.

A.)**Types of Transmission Technology :**

Transmission media is basically divided into two categories: Broadcast Networks, Point-to-Point Networks. These are explained below.

1. Broadcast Networks :

Broadcast networks are also known as terrestrial networks. It is basically a group of radio stations, television stations, or any other electronic media outlets that simply generate agreement to air, or broadcast, content generally from a centralised source.

In this network, a message that is sent by a node is received by all the other nodes connected to the network and share a common medium of communication. Broadcast networks also avoid procedures of complex routing of switched networks by simply confirming and ensuring that each transmission of nodes is basically received by all the other nodes in the network. This is the reason why the broadcast network has a single communications channel.

2. Point-to-Point Networks :

Point-to-Point Networks or Point-to-Point Connection is a type of private data connection that is connecting securely two or more locations for private data services. It might also be configured to usually carry voice, internet, and data services together all over the same point-to-point network. It simply refers to the type of communication connection among two endpoints or nodes of communication. It is a connection among pairs of machines. Transmission from point-to-point with one sender and receiver is commonly known as unicasting.

This network is generally used for two locations that are required to securely send data that is very sensitive and confidential among each of the locations. A point-to-point or P2P (Data Link) also gives or provides a path from one point that is fixed to another point being fixed. It is a very closed network data transport service that does not travel through the public Internet. This network includes various connections among individual pairs of machines. A packet present on these types of networks might be needed to go through intermediate computers before they reach the desired or destination computer. The packets also need to follow multiple routes of different length sizes.

3.)What is pure ALOHA and slotted ALOHA. Consider the delay of both at low load. Which one is less? Justify your answer.

A.)Statistically pure ALOHA is supposed to be less efficient than slotted ALOHA, that means, at normal load or when collisions occur in a contention channel.

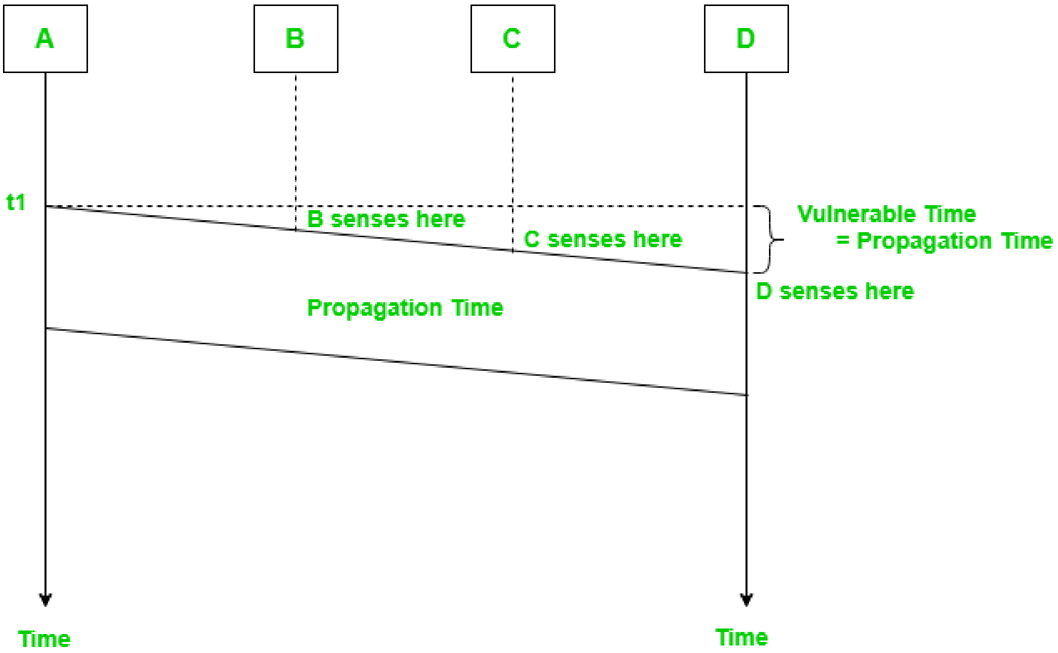
However, if the load is low, then pure ALOHA is supposed to be as efficient as slotted ALOHA (statistically). But if we consider the delay of sending the packet in a slotted time as in the slotted ALOHA protocol, then we can say that slotted ALOHA's delay is more than the one in pure ALOHA protocol, which sends the packet immediately.

4.)Summarise the working of carrier sense multiple access protocol?

A.)This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the data link layer. Carrier Sense multiple access requires that each station **first check the state of the medium** before sending.

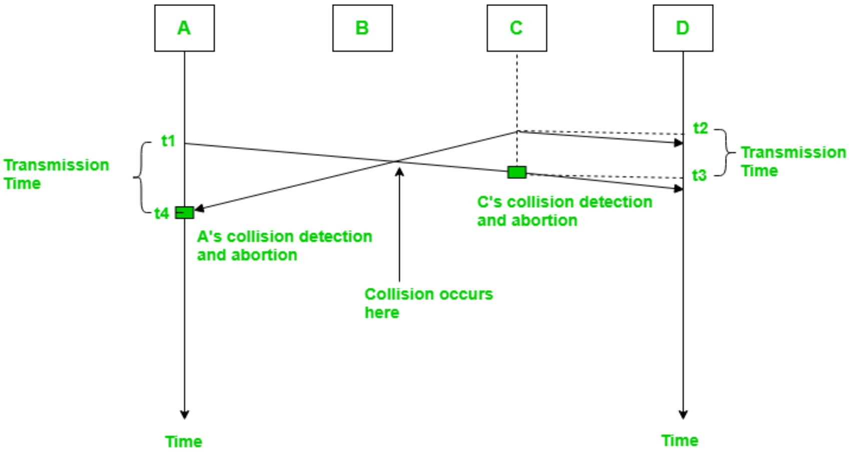
Vulnerable Time –

```
Vulnerable time = Propagation time (Tp)
```



1. Carrier Sense Multiple Access with Collision Detection (CSMA/CD) –

In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If successful, the station is finished, if not, the frame is sent again.



In the diagram, A starts sending the first bit of its frame at t1 and since C sees the channel idle at t2, starts sending its frame at t2. C detects A's frame at t3 and aborts transmission. A detects C's frame at t4 and aborts its transmission. Transmission time for C's frame is, therefore, t3-t2 and for A's frame is t4-t1.

So, the **frame transmission time (Tfr) should be at least twice the maximum propagation time (Tp)**. This can be deduced when the two stations involved in a collision are a maximum distance apart.

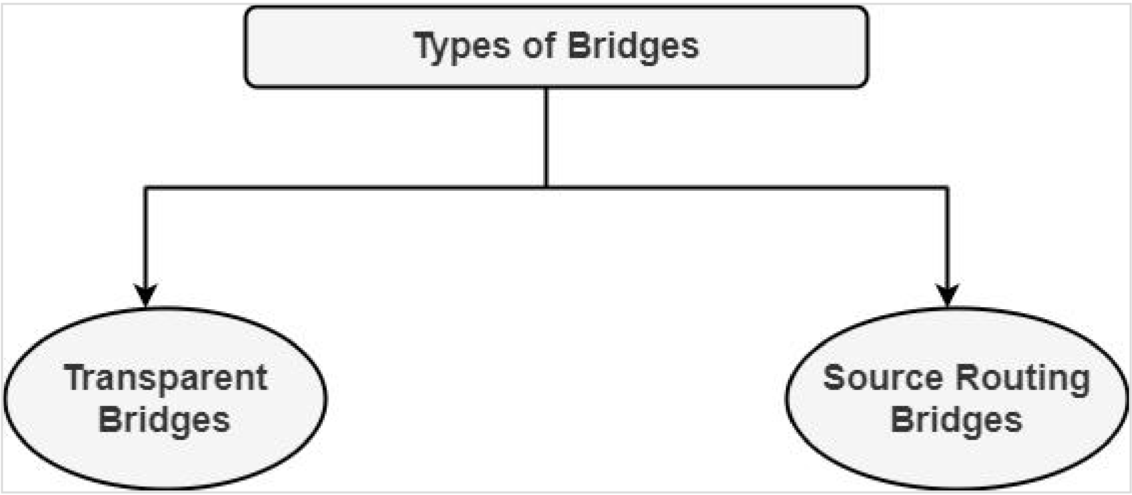
5.)Explain the back-off time of PURE ALOHA protocol

A.)http://www.myreadingroom.co.in/notes-and-studymaterial/68-dcn/819-aloha-protocols.html#:~:text=Pure%20ALOHA%20dictates%20that%20when,the%20channel%20with%20retransmitted%20frames.

6.)Describe in detail the types of bridges.

A.Types of Bridges

There are generally two types of bridges which are as follows −



Transparent Bridges

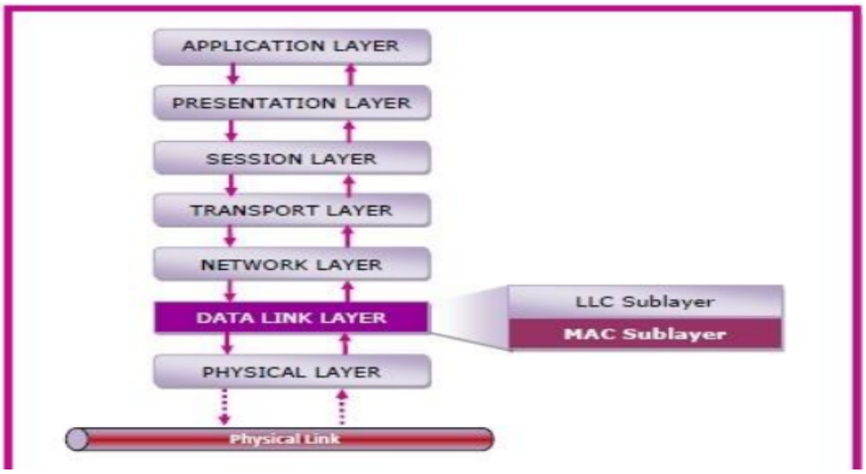
It is also called learning bridges. Bridge constructs its table of terminal addresses on its own as it implements connecting two LANs. It facilitates the source location to create its table. It is self-updating. It is a plug and play bridge.

Source Routing Bridge

This sending terminal means the bridges that the frames should stay. This type of bridge is used to prevent looping problems.

7.)Explain the functions of MAC.

A.MAC Layer in the OSI Model The Open System Interconnections (OSI) model is a layered networking framework that conceptualises 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 following diagram depicts the position of the MAC layer.



Functions of MAC Layer

• It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.

• It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.

• It resolves the addressing of source station as well as the destination station, or groups of destination stations.

• It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.

• It also performs collision resolution and initiating retransmission in case of collisions.

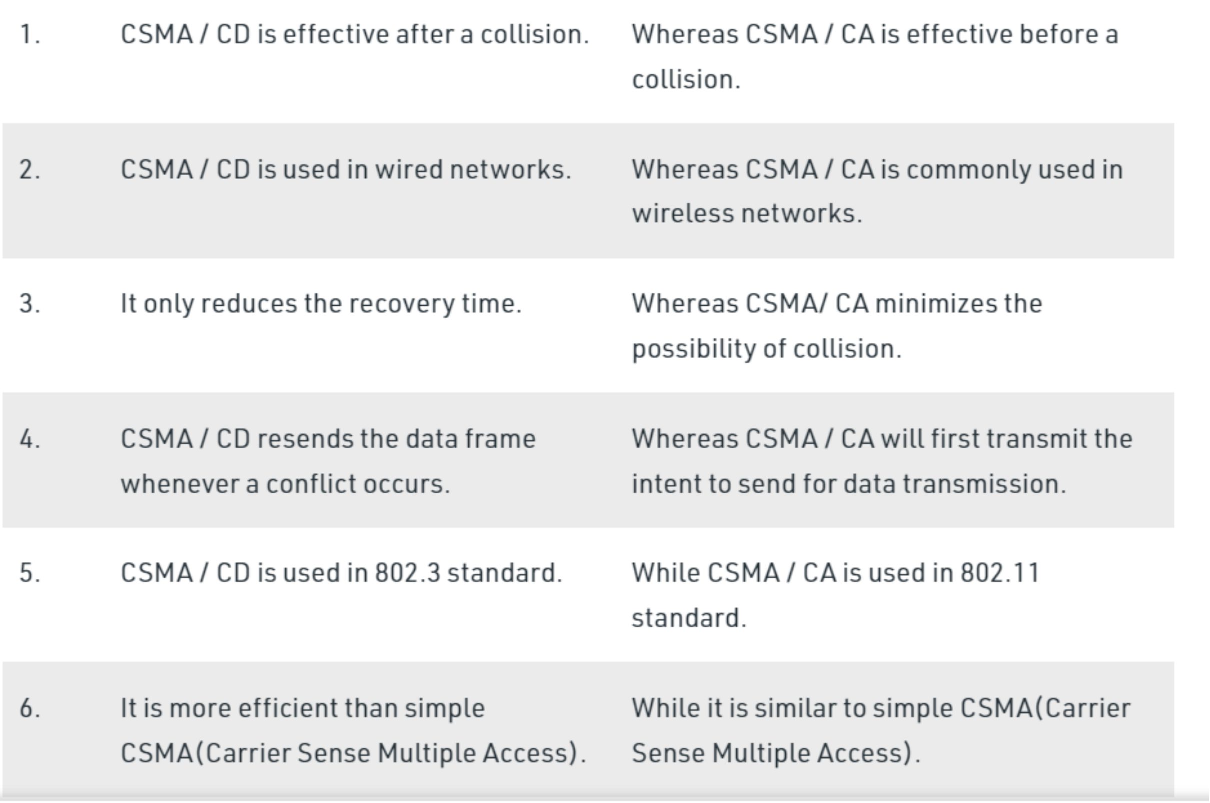
• It generates the frame check sequences and thus contributes to protection against transmission errors.

8.)How performance is improved in CSMA/CD protocol compared to CSMA protocol Explain.

A.In CSMA scheme, a station monitors the channel before sending a packet. Whenever a collision is detected, it does not stop transmission leading to some wastage of time. On the other hand, in the CSMA/CD scheme, whenever a station detects a collision, it sends a jamming signal by which another station comes to know that a collision occurs. As a result, wastage of time is reduced leading to improvement in performance.

9.)How CSMA/CA differs from CSMA/CD. Explain in brief

A.



S.NO	CSMA/CD	CSMA/CA
1.	CSMA / CD is effective after a collision.	Whereas CSMA / CA is effective before a collision.
2.	CSMA / CD is used in wired networks.	Whereas CSMA / CA is commonly used in wireless networks.
3.	It only reduces the recovery time.	Whereas CSMA/ CA minimizes the possibility of collision.
4.	CSMA / CD resends the data frame whenever a conflict occurs.	Whereas CSMA / CA will first transmit the intent to send for data transmission.
5.	CSMA / CD is used in 802.3 standard.	While CSMA / CA is used in 802.11 standard.
6.	It is more efficient than simple CSMA(Carrier Sense Multiple Access).	While it is similar to simple CSMA(Carrier Sense Multiple Access).

10.)What is the purpose of the timer at the sender site?

A.The sender starts a timer when it sends a frame. If an acknowledgment is not received within an allotted time period, the sender assumes that the frame was lost or damaged and resends it.

11.)Explain Error Control & Flow Control.

A. Flow control

For most of the protocols, flow control is a set of procedures that mainly tells the sender how much data the sender can send before it must wait for an acknowledgment from the receiver.

- The data flow must not be allowed to overwhelmFlow Control mainly coordinates with the amount of data that can be sent before receiving an acknowledgment from the receiver and it is one of the major duties of the data link layer.
- the receiver; because any receiving device has a very limited speed at which the device can process the incoming data and the limited amount of memory to store the incoming data.
- The processing rate is slower than the transmission rate; due to this reason each receiving device has a block of memory that is commonly known as buffer, that is used to store the incoming data until this data will be processed. In case the buffer begins to fill up then the receiver must be able to tell the sender to halt the transmission until once again the receiver becomes able to receive.

Thus the flow control makes the sender; wait for the acknowledgment from the receiver before continuing to send more data to the receiver.

Some of the common flow control techniques are: Stop-and-Wait and sliding window technique.

Error Control

contains both error detection and error correction. It mainly allows the receiver to inform the sender about any damaged or lost frames during the transmission and then it coordinates with the retransmission of those frames by the sender.

The term Error control in the data link layer mainly refers to the methods of error detection and retransmission. Error control is mainly implemented in a simple way and that is whenever there is an error detected during the exchange, then specified frames are retransmitted and this process is also referred to as Automatic Repeat request(ARQ).

12.)What if we need a multiple access protocol when we use the local loop of the telephone company to access the internet? Explain.

…………………….

13)Explain about ALOHA and CDMA

REFER PART B 20th qn

14)What is the need for bridges? Explain the working of 802.x to 802.y bridges in detail?

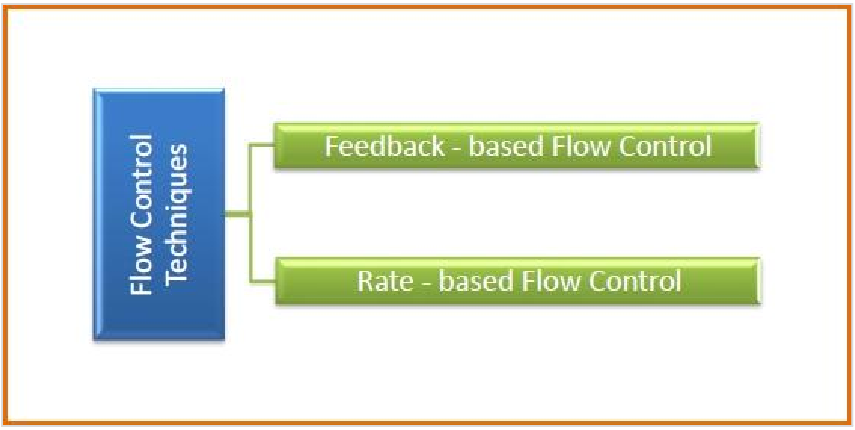
....

15)What is the need of Flow control? Explain the common approaches for flow control in data link layer

Flow control is a technique that allows two stations working at different speeds to communicate with each other. It is a set of measures taken to regulate the amount of data that a sender sends so that a fast sender does not overwhelm a slow receiver. In data link layer, flow control restricts the number of frames the sender can send before it waits for an acknowledgment from the receiver.

Approaches of Flow Control

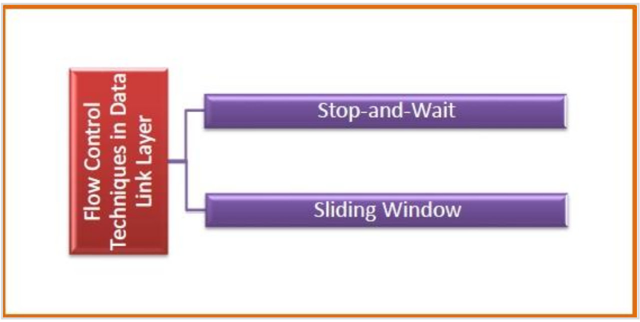
Flow control can be broadly classified into two categories −



- **Feedback based Flow Control** In these protocols, the sender sends frames after it has received acknowledgments from the user. This is used in the data link layer.
- **Rate based Flow Control** These protocols have built in mechanisms to restrict the rate of transmission of data without requiring acknowledgment from the receiver. This is used in the network layer and the transport layer.

Flow Control Techniques in Data Link Layer

Data link layer uses feedback based flow control mechanisms. There are two main techniques



Stop and Wait

This protocol involves the following transitions −

- The sender sends a frame and waits for acknowledgment.
- Once the receiver receives the frame, it sends an acknowledgment frame back to the sender.
- On receiving the acknowledgment frame, the sender understands that the receiver is ready to accept the next frame. So it sender the next frame in the queue.

Sliding Window

This protocol improves the efficiency of stop and wait protocol by allowing multiple frames to be transmitted before receiving an acknowledgment.

The working principle of this protocol can be described as follows −

- Both the sender and the receiver has finite sized buffers called windows. The sender and the receiver agrees upon the number of frames to be sent based upon the buffer size.
- The sender sends multiple frames in a sequence, without waiting for acknowledgment. When its sending window is filled, it waits for acknowledgement. On receiving acknowledgment, it advances the window and transmits the next frames, according to the number of acknowledgments received.

16)Explain how slotted ALOHA solves the problem of Channel allocation

In 1970, The channel allocation problem was solved by Norman Abramson and his colleagues at the University of Hawaii. This method is one of the most primitive and elegant methods and that is known as Aloha in Networking. The basic objective of Aloha is that ground-based radio communication. The idea can be extended in the case where a single channel is shared by several computing nodes. There are two types of Aloha in Networking are used:

Pure ALOHA
Slotted ALOHA

Pure ALOHA

In this system, the users are allowed to transmit whenever they are ready with data. Due to the feedback property of any broadcasting system, if during transmission users listen to any collision then the users wait for a random amount of time and then start all over again. If listening during transmitting isn't possible then the acknowledgement system must be there for the detection of any collision. This type of system in which multiple users share a common channel to exchange data that may lead to a collision is known as a Contention System.

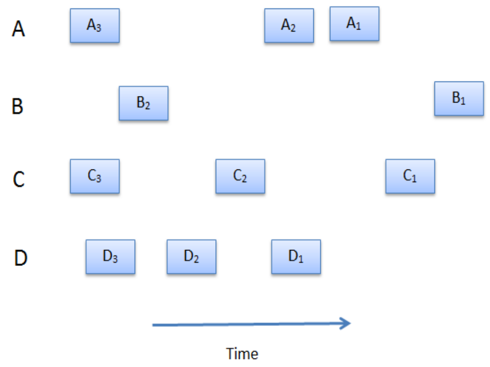


Fig: Pure ALOHA

Slotted ALOHA

In 1972, another method was proposed by Roberts to improve the efficiency of the channel utilisation factor that is known as Slotted ALOHA. According to his proposal, time is divided into discrete intervals. A station can transmit only at the start of a time frame. To achieve synchronisation, a special station transmits a beep at the starting of a frame time which acts as a clock for all the stations.

In this system, a station ready with data can't send it during a running frame time, rather it will have to wait for the starting of the next time

17)Explain classful and classless addressing schemes with an example?

A.Classful Address

The first addressing system to be implemented as part of the Internet Protocol was Classful Addressing. In the year 1981, the Classful addressing network architecture was first used on the Internet. The Classful addressing system was superseded by a Classless addressing scheme with the introduction of Classless Inter-Domain Routing (CIDR) in 1993.

Types of Classful Address

Class A, Class B, Class C, Class D, and Class E are the five varieties of Classful addresses. In IPv4, this classification is known as Classful addressing or IP address classes.

- The first three classes, Class A, B, and C, are used for "public addressing", in which communication is always one-to-one between source and destination. It implies that when data is transmitted from a source, it will only be sent to a single network host.
- The reserved categories include Class D and Class E, with Class D being utilized for multicast and Class E being saved for future usage exclusively.

- In IPv4, the Network ID is the first part of Class A, B, and C, while the Host ID is the remaining second portion.
- The Host ID always indicates the number of hosts or nodes in a certain network, whereas the Network ID always identifies the network in a specific place.
- In Class A, B, and C, the address space is split into a certain number of IP address blocks. It also specifies the maximum number of hosts in a network.

Network and Host part in Classful Addressing

The first octet or byte of an IP address is part of the network ID (short for Net-ID), while the next three octets or three bytes are part of the host ID in Class A. (in short, host-ID).

- The network ID takes up the first two octets or two bytes in Class B, whereas the host ID takes up the remaining two octets or two bytes.
- In Class C, the first three octets or bytes are dedicated to the network ID, while the last octet or byte is dedicated to the host ID.

Classless Addressing

Classless Inter-Domain Routing (CIDR) is another name for classless addressing. This addressing type aids in the more efficient allocation of IP addresses. This technique assigns a block of IP addresses based on specified conditions when the user demands a specific amount of IP addresses. This block is known as a "CIDR block", and it contains the necessary number of IP addresses.

When allocating a block, classless addressing is concerned with the following three rules.

- **Rule 1** − The CIDR block's IP addresses must all be contiguous.
- **Rule 2** − The block size must be a power of two to be attractive. Furthermore, the block's size is equal to the number of IP addresses in the block.
- **Rule 3** − The block's first IP address must be divisible by the block size.

For example, assume the classless address is 192.168.1.35/27.

- The network component has a bit count of 27, whereas the host portion has a bit count of 5. (32-27)
- The binary representation of the address is: (00100011 . 11000000 . 10101000 . 00000001).
- (11000000.10101000.00000001.00100000) is the first IP address (assigns 0 to all host bits), that is, 192.168.1.32
- (11000000.10101000.00000001.00111111) is the most recent IP address (assigns 1 to all host bits), that is, 192.168.1.63
- The IP address range is 192.168.1.32 to 192.168.1.63.

Difference Between Classful and Classless Addressing

- Classful addressing is a technique of allocating IP addresses that divides them into five categories. Classless addressing is a technique of allocating IP addresses that is intended to replace classful addressing in order to reduce IP address depletion.
- The utility of classful and classless addressing is another distinction. Addressing without a class is more practical and helpful than addressing with a class.
- The network ID and host ID change based on the classes in classful addressing. In classless addressing, however, there is no distinction between network ID and host ID. As a result, another distinction between classful and classless addressing may be made.

18)Explain error detection and correction methods in detail.

A.) https://www.javatpoint.com/computer-network-error-detection

19)Explain the services provided by the data link layer in detail?

A.The primary service of the data link layer is to support error-free transmission. The physical layer sends the data from the sender’s hub to the receiver’s hub as raw bits. The data link layer should recognize and correct some errors in the communicated data.

- **Unacknowledged connectionless service** − This contains separate frames from the source host to the destination host without some acknowledgment structure. It does not have any link established or launched. It does not manage with frame recovery due to channel noise.

- **Acknowledged connectionless service** − The transmission medium is more error-prone. This requires acceptance service for each frame shared between two hosts to provide that the frame has occurred correctly.

- **Acknowledged connection-oriented service** − This layer supports this service to the network layer by settling a link between the source and destination hosts before any information removal occurs.

- **Framing** − In this layer, it receives a raw bitstream from the physical layer that cannot be bug-free. The data link layer divides the bitstreams into frames to provide a frequent change of bitstreams to the network layer.

- **Error Control** − It includes sequencing frames and sending control frames for acceptance. A noisy channel can avoid scanning of bits, falling bits from a frame, introducing specific bits in the frame, frames final sinking, etc.
-
- **Flow Control** − There is another fundamental problem in the data link design to regulate the cost of data communication between two source and destination hosts. If the conflict among the source and destination hosts data sending and receiving speed, it will create packets to drop at the receiver end.

- **Sequence Integrity** − The data link layer supports the data bits sequence and sends them to the physical layer in the similar sequence as received from the network layer. It supports a reliable share of data link service data unit (DLSDU) over the data link connections.

20)Explain random access protocols in detail?

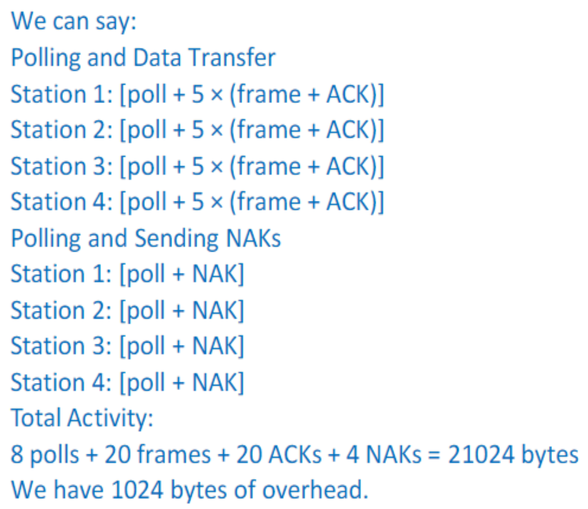
A.https://www.studytonight.com/post/random-access-protocols-aloha-csma-csmaca-and-csmacd

PART-A

1.)Demonstrate the Laplace transform of the message delay in FDMA in which every message contains a random number of packets. Compare the expected message delay with that of TDMA

2.)Illustrate a network with one primary and four secondary stations uses polling. The size of a data frame is 1000 bytes. The size of the poll, ACK and NAK frames are 32 bytes each. Each station has 5 frames to send. How many total bytes are exchanged if there is no limitation on the

number of frames a station can send in response to a poll?



We can say:

Polling and Data Transfer

Station 1: [poll + 5 × (frame + ACK)]

Station 2: [poll + 5 × (frame + ACK)]

Station 3: [poll + 5 × (frame + ACK)]

Station 4: [poll + 5 × (frame + ACK)]

Polling and Sending NAKs

Station 1: [poll + NAK]

Station 2: [poll + NAK]

Station 3: [poll + NAK]

Station 4: [poll + NAK]

Total Activity:

8 polls + 20 frames + 20 ACKs + 4 NAKs = 21024 bytes

We have 1024 bytes of overhead.

3.)Find CRC for P = 110011 and M = 1100011

A.) P = 110011 and M = 1100011

To Find:

CRC

Step by step Explanation:

CRC Stands for *Cyclic Redundancy Check*. CRC is an error identifying method. It is mostly used in digital networks and storage devices to detect accidental error changes to raw data.

M Stand for *Message*

P stand for *Pattern*

Message (M) = 1100011 (8 bits)

Pattern (P) = 110011 (6 bits)

First to find n, we can get n from P

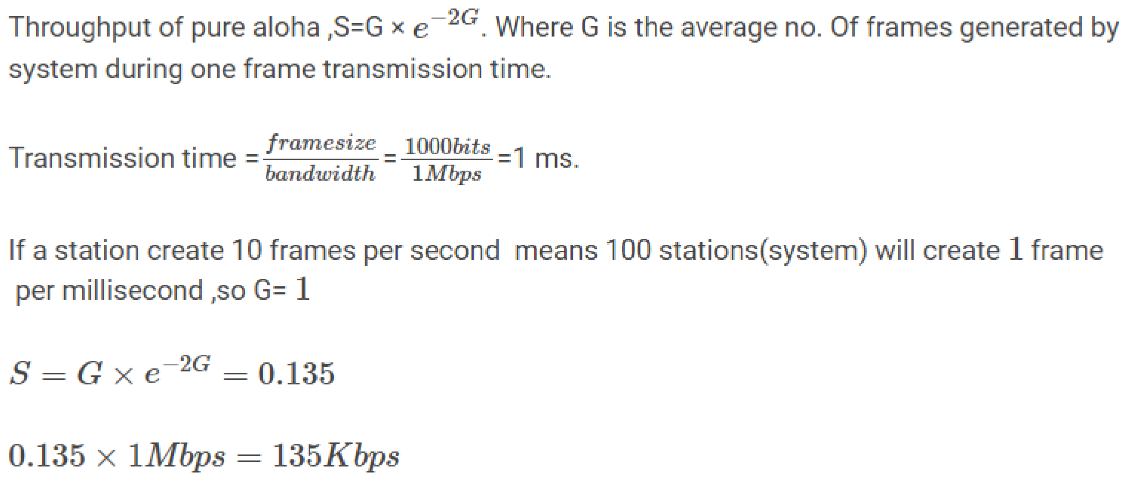
where, P is *(n+1)*

In our problem P has 6 bits , so n= 5

There are 5 bits, the message will be multiplied by 2^5 . Append the *5 zeros* at the end of the message. Finally, the message will become 1110001100000

CRC is 1110001100000

4.)One hundred stations on a pure ALOHA network share a 1- Mbps channel. If frames are 1000 bits long, find the throughput if each station is sending 10 frames/sec?



Throughput of pure aloha ,S=G × e^{-2G}. Where G is the average no. Of frames generated by system during one frame transmission time.

Transmission time =$\frac{framesize}{bandwidth}$=$\frac{1000bits}{1Mbps}$=1 ms.

If a station create 10 frames per second means 100 stations(system) will create 1 frame per millisecond ,so G= 1

$$S = G \times e^{-2G} = 0.135$$

$$0.135 \times 1Mbps = 135Kbps$$

5.)Calculate the hamming distance for each of the following code words
i. d(10000,01000)
ii. d(10101, 10010)
iii. d(1111,1111)
iv. d(0000,0000)

6.) Exclusive-OR (XOR) is one of the most used operations in the calculation of codewords. Apply the exclusive-OR operation on the following pairs of patterns. Interpret the results
a.(10001),(10001)
b. (11100),(00000)
c. (10011),(11111)

7.)Assuming even parity, find the parity bit for each of the following data units.

a. 1001011

b. 0001100

c. 1000000

d. 1110111

8.)Given the dataword 101001111 and the divisor 10111, show the generation of the CRC codeword at the sender site (using binary division).

9.)A category of error detecting (and correcting) code, called the Hamming code, is a code in which dmin = 3. This code can detect up to two errors (or correct one single error). In this code, the values of n, k, and r are related as Find the number of bits in the dataword and the codewords if r is 3

Let n = code word bits
r = redundant bits
k = data word
n = 2^r -1
k=n-r
r=3
n=2^3 -1
n= 8-1
n=7
k =7-3 = 4
hence data word bits = 4
code word bits = 7

10.)A slotted ALOHA network transmits 200-bit frames using a shared channel with a 200-kbps bandwidth. Find the throughput if the system (all stations together) produces

a. 1000 frames per second.

b. 500 frames per second.

c. 250 frames per second

a.)G =1 S=G×e−G=0.368 (36.8%)

Throughput = 1000 × 0.0368 = 368 frames.

b.)G =1 $S=G\times e-G=0.368$ (36.8%)
Throughput = 500 × 0.0368 = 184 frames.

c.)G =1 $S=G\times e-G=0.368$ (36.8%)
Throughput = 250 × 0.0368 = 92 frames.