DATA LINK LAYER

Multiple Choice Type Questions

1. In selective repeat sliding window protocol, the receiver window size is [WBUT 2015]
   a) greater than one b) one
   c) two d) none of these
Answer: (a)

2. The Hamming code is used for [WBUT 2015]
   a) error detection b) error correction
   c) error encapsulation d) both (a) and (b)
Answer: (d)

3. Which channel access method is used in Ethernet network? [WBUT 2015]
   a) CSMA/CD b) token bus c) token ring d) all of these
Answer: (a)

4. Which error detection method uses ones complement arithmetic? [WBUT 2016]
   a) Parity check b) Checksum c) CRC d) None of these
Answer: (b)

5. Pure ALOHA has a maximum efficiency of [WBUT 2016]
   a) 10% b) 37% c) 18% d) none of these
Answer: (c)

6. If the data unit is 111111, the divisor 1010 and remainder 110, what is the dividend at the receiver? [WBUT 2016]
   a) 111111011 b) 111111110 c) 111111101 d) 1111111110
Answer: (b)

7. Each frame must contain [WBUT 2017]
   a) only source address b) only destination address
   c) source and destination address d) source or destination address
Answer: (c)

8. Which of the following IP Network addresses is a reserved address? [WBUT 2018]
   a) 127.0.0.0 b) 130.50.0.0 c) 4.0.0.0 d) None of these
Answer: (a)

9. Which Layer is responsible for Congestion Control? [WBUT 2018]
   a) Network Layer b) Datalink Layer
   c) Transport layer d) Application Layer
Answer: (c)

10. In the "Go-Back-N" ARQ mechanism, the maximum window size for a k-bit sequence number field in information frames is [WBUT 2018]

a) k + 1 b) 2k c) 2k – 1 d) None of these

Answer: (c)

11. Pure ALOHA has a maximum throughput of _____. [WBUT 2018]

a) 16.4% b) 18.4% c) 7.4% d) 1%

Answer: (b)

12. The special address 'THIS HOST' is referred to as _____. [WBUT 2018]

a) 0.0.0.0 b) 0.0.14.98

c) 127.0.0.127 d) 255.255.255.255

Answer: (a)

Short Answer Type Questions

1. Explain the principle of Go-back-N ARQ. [WBUT 2013]

Answer:

Go-Back-N ARQ

- Receiver sends Ack for the correctly received frame
- An Acknowledgement field has a meaning of "next expected sequence number" (Example: Ack 2 means "next expected packet sequence number is 2 and all packets up to 2(0, 1) are received)
- Sender keeps on sending frames (limited to the Window-size) and receiver keeps on acknowledging.
- When a frame is damaged, receiver sends a Reject control packet(Nak)
- Sender goes back to the Rejected frame and sends all the frames starting with the rejected one even if those frames are already sent to the receiver
- Sender's buffer size = Window size
- Receiver's buffer size = 1

2. How CRC detect the error in a bit stream? Explain with example. [WBUT 2013]

Answer:

A cyclic redundancy check (CRC) or polynomial code checksum is a hash function designed to detect accidental changes to raw computer data and is commonly used in digital networks and storage devices such as hard disk drives. A CRC-enabled device calculates a short, fixed-length binary sequence, known as the CRC code or just CRC, for each block of data and sends or stores them both together. When a block is read or received the device repeats the calculation; if the new CRC does not match the one calculated earlier, then the block contains a data error and the device may take corrective action such as rereading or requesting the block be sent again, otherwise the data is assumed to be error free.

Applying the CRC algorithm, here we determine the transmitted frame for the data 11010111 and for the generator polynomial $x^3 + x^2 + 1$.

We append 000 (since highest power of generator polynomial is 3) to get 11010111000.

```
1101) 1101 01110 00(10000 10 1
          1101
          ------
            1110
            1101
            ------
              1100
              1101
              ------
                001 ← Remainder
```

So, transmitted string is 11010111001

When the received string is again divided by 1001, we get remainder 000 as shown below:

```
1001) 1010 00 0 1 1 1 1 (10 1 10 1 1 1
          1001
       ------
           1100
           1001
          -------
           1010
           1001
           ------
             1111
             1001
             ------
               1101
               1001
               ------
                 1001
                 1001
                 ------
                   000 ← Remainder
```

3. Explain the property of flow control. **[WBUT 2013]**

Answer:

Ethernet Flow Control

1. Flow control operates at a lower layer than TCP or IP, and thus is independent of them. Put another way, flow control is capable of being used regardless of what higher-level protocols are put on top of it. An important side-effect of this is that neither TCP nor IP know what Ethernet's flow control is doing; they operate under the assumption that there is no flow control other than what they may or may not provide themselves.
2. Flow control functions between two directly connected network devices, and flow control frames are never forwarded between links. Thus, two computers that are connected via a switch will never send pause frames to each other, but could send

pause frames to the switch itself (and vice versa: the switch can send pause frames to the two computers).

3. Pause frames have a limited duration; they will automatically "expire" after a certain amount of time. The expiration time is set by the device that transmits the pause frame.
4. A paused link is not a discriminator of protocols; it will prevent **any** data from being passed across the link other than more pause frames.

For the purpose of proper handshaking between two peer data link layers, a packet that the data link layer receives from the network layer is encapsulated in a "frame".

A frame consists of:

A **Sequence Number** field: A small number of few bits used to number frames in a small group of frames.

An **Acknowledge** field: Used by the receiver to acknowledge receipt of a frame.

A **Type** field: Depending upon the protocol used, a frame can be one of several types. This field is used to disambiguate among them.

The **Data** field: Contains the packet data.

When the sender data link layer has sent a frame, it is not sure that it will reach the destination error-free or in order. Hence, it must "buffer" the frame temporarily. Actually, depending upon the protocol used, several frames need to be kept buffered. A frame is de-buffered only when its error-free delivery is established. The receiver data link layer similarly maintains a buffer of frames received so that the sequence of the frames supplied to the network layer is maintained.

4. Given a 10 bit sequence 1010011110 and a divisor of 1011. Find the CRC and check your answer. **[WBUT 2014, 2015]**

Answer:

Since divisor is 1101, we append from 0-s to the data and divide.

```
        100100011
    ____________
1011|1010011110 0000
    1011
    ----
      1011
      1011
      ----
        1100
        1011
        ----
         1110
         1011
         ----
          1010
          1011
          ----
Remainder →  0010
```

∴ Data with CRC is 1010 0111 1000 10

5. What is piggybacking? **[WBUT 2015]**

Answer:

Piggybacking is a bi-directional data transmission technique in the network layer (OSI model). It makes the most of the sent data frames from receiver to emitter, adding the confirmation that the data frame sent by the sender was received successfully (ACK acknowledge). This practically means, that instead of sending an acknowledgement in an individual frame it is piggy-backed on the data frame.

6. What are the differences between Flow Control and Error Control? [WBUT 2015]

Answer:

Flow control is the management of data flow between computers or devices or between nodes in a network so that the data can be handled at an efficient pace. Too much data arriving before a device can handle it causes data overflow, meaning the data is either lost or must be retransmitted.

In information theory and coding theory with applications in computer science and telecommunication, error detection and correction or error control are techniques that enable reliable delivery of digital data over unreliable communication channels.

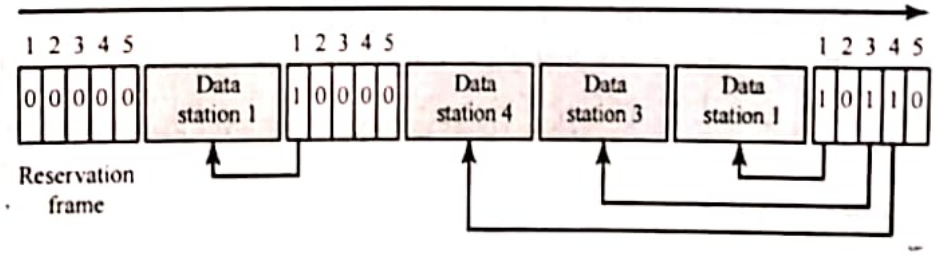
7. Describe reservation in controlled access mechanism. **[WBUT 2016]**

Answer:

In the reservation method, a station needs to make a reservation before sending data. Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval.

If there are N stations in the system, there are exactly N reservation mini slots in the reservation frame. Each mini slot belongs to a station. When a station needs to send a data frame, it makes a reservation in its own mini slot. The stations that have made reservations can send their data frames after the reservation frame.

The following figure shows a situation with five stations and a five-minislot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.



8. Describe pure ALOHA. **[WBUT 2016]**

Answer:

In pure ALOHA, a user transmits a new information packet at the moment it is presented to (or arrives at) that user. If during the transmission of a packet there is no other overlapping (partial or complete) packet transmissions from other senders, then the

packet is received successfully and the sender receives an ACK on the feedback channel. Otherwise, there is a collision, which is assumed to destroy completely all overlapping packets, regardless of whether they overlap partially or completely. The senders of colliding packets interpret the absence of an ACK on the feedback channel as the signal their packets were destroyed. When a collision occurs, the packets involved must be retransmitted. To avoid continually repeating the same collision, the pure ALOHA algorithm specifies that each user involved in a collision independently and randomly selects a waiting time after which he again retransmits his packet.

In analyzing pure ALOHA, Abramson used the term throughput to describe the "rate of occurrence of those packets which are received correctly" and showed that the maximum throughout for pure ALOHA is $\frac{1}{2e} \approx 0.184$ packets/slot. To obtain this result, Abramson assumed a statistical equilibrium in which not only do the transmission times of new packets form a stationary Poisson process with intensity λ packets/slot but the retransmission times of packets previously transmitted unsuccessfully do also form a stationary Poisson process with intensity λ_r packets/slot that is independent of the new packet process. Because the superposition of two independent stationary Poisson processes is again a stationary Poisson process, the totality of transmission times on the channel is also a stationary Poisson process with intensity $\lambda + \lambda_r$ packets/slot.

Consider now a particular chosen transmitted packet. This chosen packet will be received successfully if and only if there is no other packet whose transmission starting time lies strictly within the time interval that begins one slot prior to the starting time of the chosen packet and that ends with the end of the slot that contains the chosen packet. Thus, successful transmission of the chosen packet specifies a forbidden interval of length two slots for the starting times of other packets. The probability that the chosen packet will not suffer a collision is the probability that a Poisson random variable with mean $2(\lambda + \lambda_r)$ packets takes on the value 0, which is $e^{-2(\lambda+\lambda_r)}$. Because packets are transmitted on the channel at a total rate of $(\lambda + \lambda_r)$ packets/slot, it follows that packets are received correctly at a rate of

$S = (\lambda + \lambda_r)e^{-2(\lambda+\lambda_r)}$ packets/slot,

which is the throughput equation for pure ALOHA in statistical equilibrium. Differentiation on the right shows that the throughput S is maximized by the total transmission rate $\lambda + \lambda_r = \frac{1}{2}$ packets/slot. The resulting maximum throughput is indeed

$$S_{max} = \frac{1}{2e} \approx 0.184 \text{ packets/slot}$$

9. What do you mean by ARQ? Explain selective repeat ARQ. **[WBUT 2016]**

Answer:

1st Part:

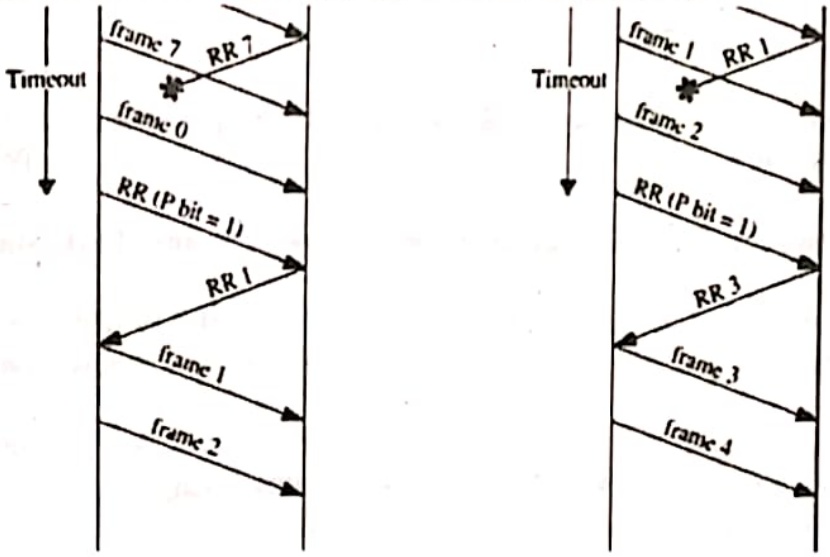
Automatic Repeat ReQuest (ARQ), also called Automatic Repeat Query, is an error-control protocol that automatically initiates a call to retransmit any data packet or frame

after receiving flawed or incorrect data. When the transmitting device fails to receive an acknowledgement signal to confirm the data has been received, it usually retransmits the data after a predefined timeout and repeats the process a predetermined number of times until the transmitting device receives the acknowledgement.

2nd Part:

Selective-Repeat ARQ

- Same as the Go-Back-N ARQ except when the receiver receives a frame which is out of sequence, then
- Sender retransmits only the rejected packet and continues with other packets
- More efficient than Go-Back-N
- Sender's buffer size = Receiver's buffer size=Window size



(a) Go-back-N ARQ (b) Selective-reject ARQ

10. What do you mean by flow control in data link layer? What is error control in data link layer? [WBUT 2017]

Answer:

Flow control is the management of data flow between computers or devices or between nodes in a network so that the data can be handled at an efficient pace. Flow control observes the proper flow of the data from sender to receiver. Feedback-based flow control and rate-based flow control are the approaches to achieve the proper flow control. It avoid overrunning of receivers buffer the data loss.

Error control is the control mechanism at data link layer. It is meant for delivering the error-free data to the receiver. Parity checking, Cyclic Redundancy Code (CRC) and checksum are the approaches to detect the error in data. Hamming code, Binary Convolution codes, Reed-Solomon code, Low-Density Parity Check codes are the approaches to correct the error in data. It detects and correct the error occurred in the data.

11. Explain why CSMA/CD protocol cannot be used in wireless LAN? [WBUT 2018]

Answer:

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) is a protocol for carrier transmission in 802.11 networks. Unlike CSMA/CD (Carrier Sense Multiple Access/Collision Detect) which deals with transmissions after a collision has occurred, CSMA/CA acts to prevent collisions before they happen.

In CSMA/CD the sender senses the medium(eg wire) if the medium is free it starts sending the data if in between any other sender sends data at same time collision occurs and this collision can be detected by all the devices in that network hence the sending device stops sending the data and waits untill the medium becomes free.

This works well for wired network but in case of wireless network this fails since the collision occurs at receiver side and this collision can't be detected by sender and sender feels that the sent packets are received by sender without collision and continues sending. In this case we use CSMA/CA.

12. What is difference between Distance Vector Routing Protocols and Link State Routing Protocols? **[WBUT 2018]**

Answer:

Difference between Distance vector Routing Protocols and Link state Routing Protocols:

Distance vector routing protocol like RIP, the routing table is forwarded by each router to neighboring routers. Here, the router's don't know the topology i.e. how other routers are interconnected.

Link state routing protocol like OSPF, routers first exchange information about connections within the network and build a topology table. Then each router calculate the best route to each destination by using Dijkstra's algorithm.

Unique hardware address from the interface card and send an RARP request (a broadcast frame on the network) asking for someone to reply with the diskless system's IP address (in an RARP reply).

13. a) What are the problems of providing redundant path in a bridged network?
b) How does a transparent bridge solution to those problems?

[MODEL QUESTION]

Answer:

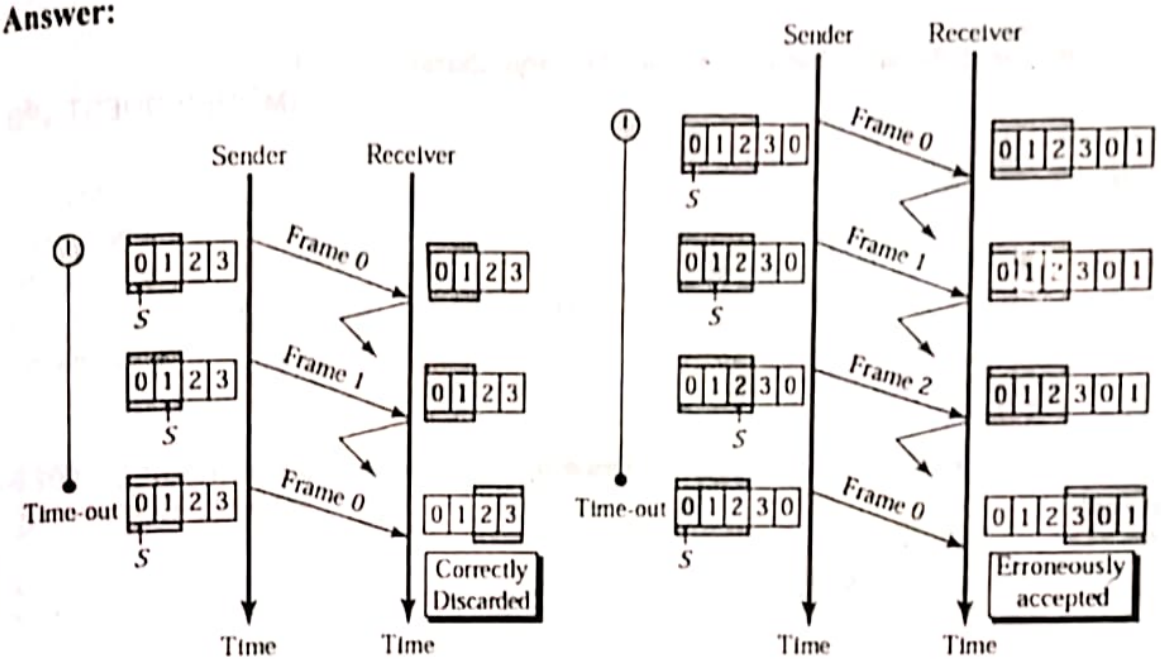
a) In a bridged network, no correspondence is required between addresses and paths. Put another way, addresses don't imply anything about where hosts are physically attached to the network. Any address can appear at any location. In contrast, routing requires more thoughtful address assignment, corresponding to physical placement.

Bridging relies heavily on broadcasting. Since a packet may contain no information other than the destination address, and that implies nothing about the path that should be used, the only option may be to send the packet everywhere! This is one of bridging's most severe limitations, since this is a very inefficient method of data delivery, and can trigger broadcast storms. In networks with low speed links, this can introduce crippling overhead.

b) Transparent bridging, the type used in Ethernet and documented in IEEE 802.1, is based on the concept of a spanning tree. This is a tree of Ethernet links and bridges, spanning the entire bridged network. The tree originates at a root bridge, which is determined by election, based either on Ethernet addresses or engineer-defined preference. The tree expands outward from there. Any bridge interfaces that would cause loops to form are shut down. If several interfaces could be deactivated, the one farthest from the root is chosen. This process continues until the entire network has been transversed, and every bridge interface is either assigned a role in the tree, or deactivated.

14. In Selective Reject ARQ the size of the sender and receiver window must be at most one half of 2^m, explain it. **[MODEL QUESTION]**

Answer:



Size of the sender and receiver windows must be at most one-half of 2 m. If m = 2, window size should be 2 ^m /2 = 2. Fig compares a window size of 2 with a window size of 3. Window size is 3 and all ACKs are lost, sender sends duplicate of frame 0, window of the receiver expect to receive frame 0 (part of the window), so accepts frame 0, as the 1st frame of the next cycle – an error.

15. Suppose a system uses Stop and Wait protocol with propagation delay 20 ms. If the frame size is 160 bits and band width is 4kbps then calculate channel utilization or efficiency. **[MODEL QUESTION]**

Answer:

At a transmission rate of 4bits/ms, 160 bits takes 20ms+20ms =40 ms. So, after transmitting a 160 bits frame in 160/4=160ms, the sending system has to wait another 40ms to get the ACK. Thus it takes 20+20=80ms for a frame of which transmission happens for 40 ms.

So, efficiency = 40/80=50% for round trip propagation delay.

16. Suppose a system uses Go Back N protocol with window size 3. If a sender wants to transmit 6 frames and every 4th frame is error then calculate how many number of extra frames to be transmitted to the receiver. [MODEL QUESTION]

Answer:

Given: Frames 40 send=6

N=window size= 3.

Every 4th frame is erroneously transmitted.

Hence, 4th frame out of 6 had error.

NAK received after 6th frame.

Action – Retransmit 4th frame which now goes through without error.

So, System needs to transmit 1 extra frame i.e. 7 frames total.

17. Write the difference between bit stuffing and character stuffing. [MODEL QUESTION]

Answer:

Both bit and character stuffing are used to distinguish the start and end of frames. In character stuffing, some special (usually three) characters are used to mark the beginning and end of frames. In bit-stuffing, a special flag pattern "01111110" is send at the beginning to indicate the start of a frame. All subsequent data is literally treated as a stream of bits. However, if five consecutive '1'-s have been pumped out, a '0' is ignored by the receiver.

18. Discuss the IEEE 802.5 protocol. Draw the lower two layers of the IEEE 802.5 protocol. [MODEL QUESTION]

Answer:

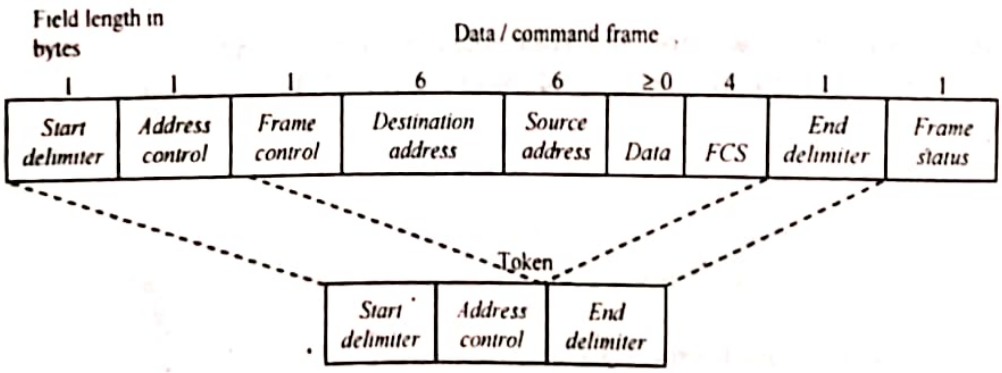
Token Ring and IEEE 802.5 support two basic frame types

- Tokens
- Data/command frames.

Tokens are 3 bytes in length and consist of a start delimiter, an access control byte, and an end delimiter.

Data/command frames vary in size, depending on the size of the Information field. Data frames carry information for upper-layer protocols, while command frames contain control information and have no data for upper-layer protocols.

Both formats are shown in Figure below.



Tokens:

Start delimiter: Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.

Access-control byte: Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).

End delimiter: Signals the end of the token or data/command frame. This field also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.

Data/Command Frame

Data/command frames have the same three fields as Token Frames, plus several others:

Start delimiter: Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.

Access-control byte: Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).

Frame-control bytes: Indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.

Destination and source addresses: Consists of two 6-byte address fields that identify the destination and source station addresses.

Data: Indicates that the length of field is limited by the ring token holding time, which defines the maximum time a station can hold the token.

Frame-check sequence (FCS): Is filed by the source station with a calculated value dependent on the frame contents. The destination station recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.

End Delimiter: Signals the end of the token or data/command frame. The end delimiter also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.

Frame Status: Is a 1-byte field terminating a command/data frame. The Frame Status field includes the address-recognized indicator and frame-copied indicator.

Long Answer Type Questions

1. How you correct a single bit error of a sending bit stream? Explain with proper example. [WBUT 2013]

Answer:

In digital world, error correction can be done in two ways:

Backward Error Correction:

When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.

Forward Error Correction:

When the receiver detects some error in the data received, it uses an error-correcting code, which helps it to auto-recover and correct some kinds of errors.

The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive, for example fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, Forward Error Correction is used.

To correct the error in data frame, the receiver must know which bit (location of the bit in the frame) is corrupted. To locate the bit in error, redundant bits are used as parity bits for error detection. If for example, we take ASCII words (7 bits data), then there could be 8 kind of information we need. Up to seven information to tell us which bit is in error and one more to tell that there is no error.

For m data bits, r redundant bits are used. r bits can provide 2r combinations of information. In m+r bit codeword, there is possibility that the r bits themselves may get corrupted. So the number of r bits used must inform about m+r bit locations plus no-error information, i.e. m+r+1.

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

The key to the Hamming Code is the use of extra parity bits to allow the identification of a single error. Create the code word as follows:

1. Mark all bit positions that are powers of two as parity bits. (positions 1, 2, 4, 8, 16, 32, 64, etc.)
2. All other bit positions are for the data to be encoded. (positions 3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17, etc.)
3. Each parity bit calculates the parity for some of the bits in the code word. The position of the parity bit determines the sequence of bits that it alternately checks and skips.
   Position 1: check 1 bit, skip 1 bit, check 1 bit, skip 1 bit, etc. (1,3,5,7,9,11,13,15,...)
   Position 2: check 2 bits, skip 2 bits, check 2 bits, skip 2 bits, etc. (2,3,6,7,10,11,14,15,...)
   Position 4: check 4 bits, skip 4 bits, check 4 bits, skip 4 bits, etc. (4,5,6,7,12,13,14,15,20,21,22,23,...)
   Position 8: check 8 bits, skip 8 bits, check 8 bits, skip 8 bits, etc. (8-15,24-31,40-47,...)

Position 16: check 16 bits, skip 16 bits, check 16 bits, skip 16 bits, etc. (16-31,48-63,80-95,...)
Position 32: check 32 bits, skip 32 bits, check 32 bits, skip 32 bits, etc. (32-63,96-127,160-191,...)
etc.

4. Set a parity bit to 1 if the total number of ones in the positions it checks is odd.
   Set a parity bit to 0 if the total number of ones in the positions it checks is even.

Here is an example:
A byte of data: 10011010
Create the data word, leaving spaces for the parity bits: _ _ 1 _ 0 0 1 _ 1 0 1 0
Calculate the parity for each parity bit (a ? represents the bit position being set):

- Position 1 checks bits 1,3,5,7,9,11:
  ? _ 1 _ 0 0 1 _ 1 0 1 0. Even parity so set position 1 to a 0: 0 _ 1 _ 0 0 1 _ 1 0 1 0
- Position 2 checks bits 2,3,6,7,10,11:
  0 ? 1 _ 0 0 1 _ 1 0 1 0. Odd parity so set position 2 to a 1: 0 1 1 _ 0 0 1 _ 1 0 1 0
- Position 4 checks bits 4,5,6,7,12:
  0 1 1 ? 0 0 1 _ 1 0 1 0. Odd parity so set position 4 to a 1: 0 1 1 1 0 0 1 _ 1 0 1 0
- Position 8 checks bits 8,9,10,11,12:
  0 1 1 1 0 0 1 ? 1 0 1 0. Even parity so set position 8 to a 0: 0 1 1 1 0 0 1 0 1 0 1 0
- Code word: 011100101010.

Finding and fixing a bad bit
The above example created a code word of 011100101010. Suppose the word that was received was 011100101110 instead. Then the receiver could calculate which bit was wrong and correct it. The method is to verify each check bit. Write down all the incorrect parity bits. Doing so, we will discover that parity bits 2 and 8 are incorrect. It is not an accident that 2 + 8 = 10, and that bit position 10 is the location of the bad bit. In general, check each parity bit, and add the positions that are wrong, this will give us the location of the bad bit.

2. a) Host A sends a datagram to host B. Host B never receives the datagram, and host A never receives notification of failure. Give two different explanations of what might happened. **[WBUT 2014]**

Answer:
Host A sends a datagram to host B. Host B never receives the datagram, and host A never receives notification of failure.

First explanation:
When Host B doesn't receive the expected datagram it sends a negative acknowledgement to Host A. But unfortunately it also lost in the way: So as Host A neither gets any acknowledgement nor any negative acknowledgement it will re-send the frame when the timer fires.

Second explanation:

The sender may fail to get the ACK in proper sequence expected. This will cause a timeout (if the receiver simply does not send an ACK) or a quick knowledge of the failure (if the receiver sends an NACK). Either way, the sender would come to know about the failure after sending m frames. The best it can do is sliding the window back by m and resume.

The receiver on its parts goes on discarding frames till it gets the frame just after the last correctly received frame. But if the receiver doesn't get the frame and the sender, the NACK, then Host A can do the same i.e. sliding the window back by m and resume. And Host B will do nothing as it did not receive any new frame.

b) What are the advantages of Go-Back-N ARQ over Stop-and-Wait ARQ? **[WBUT 2014]**

Answer:

In Stop and Wait ARQ, the sender needs to stop and wait for acknowledgement to each data frame that it has sent to the receiver when the sender sends a data frame to the receiver it starts timer. If the frame that the sender has sent is damaged. The receiver will not get any frame received so, it doesn't send any acknowledgement to that frame. By then, if the timer expires, the sender will resend that frame. In this protocol, sender has to set the timer every time it sends a frame. How ever in Go Back n ARQ, the sender need not wait for the acknowledgement of the first frame it has sent. Sender can send multiple frames while waiting for acknowledgement. Several frames can be sent before we receive news about the previous frames. This saves time. A task has begun before the previous task has ended. Here the task is sending all the subsequent frames after sending the first frame before getting the acknowledgement for the first frame. So eventually multiple frames are to be put in transition while waiting for acknowledgement. This is called Pipelining. This improves the efficiency of the transmission.

3. a) Explain about error detection or method of error detection (Parity check, Cyclic Redundancy Check (CRC) & Check sum) with proper example. [WBUT 2017]

Answer:

Error: A condition when the receiver's information does not matches with the sender's information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0.

Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the message.

Basic approach used for error detection is the use of redundancy bits, where additional bits are added to facilitate detection of errors.

Some popular techniques for error detection are:

1. SimpleParitycheck
2. Two-dimensional Parity check

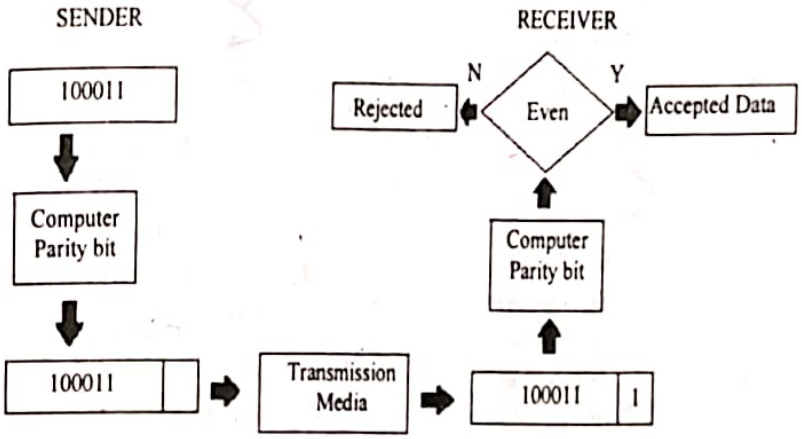
3. Checksum
4. Cyclicredundancycheck

1. SimpleParitycheck

Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of :

- 1 is added to the block if it contains odd number of 1's, and
- 0 is added if it contains even number of 1's

This scheme makes the total number of 1's even, that is why it is called even parity checking.



2. Two-dimensional Parity check

Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end these are compared with the parity bits calculated on the received data.

3. Checksum

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

Original Data

10011001	11100010	00100100	10000100
1	2	3	4

K=4, m=8

Sender

1	10011001	
2	11100010	
	01111011	carry 1
	01111100	
3	00100100	
	10100000	
4	10000100	
	00100100	carry 1
Sum:	00100101	
CheckSum:	11011010	

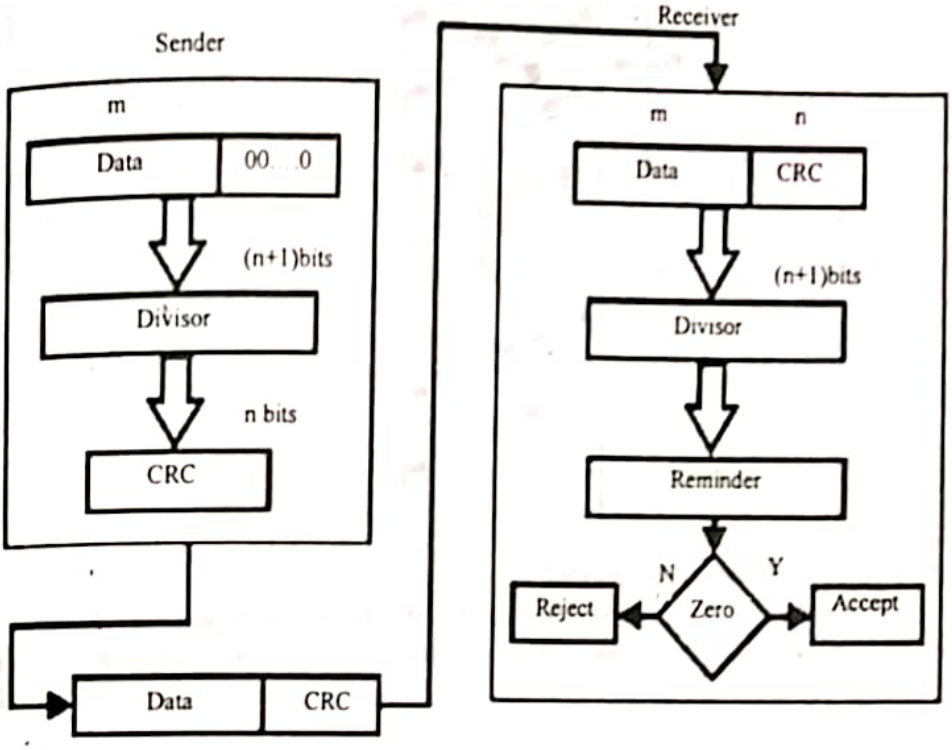
Receiver

1	10011001	
2	11100010	
	01111011	carry 1
	01111100	
3	00100100	
	10100000	
4	10000100	
	00100100	carry 1
Sum:	00100101	
Complement:	11011010	
	11111111	
	00000000	

Conclusion: Accept Data

Cyclic redundancy check (CRC)

- 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.



b) Given a 10-bit sequence 1010011110 and a divisor of 1011. Find the CRC. **[WBUT 2017]**

Answer:

Refer to Question No. 4 of Short Answer Type Questions.

4. Describe Stop-and-wait ARQ, Go-Bank-N ARQ, with the help of diagram. Find the error and correct 1011101011001010110 using Hamming code. **[WBUT 2017]**

Answer:

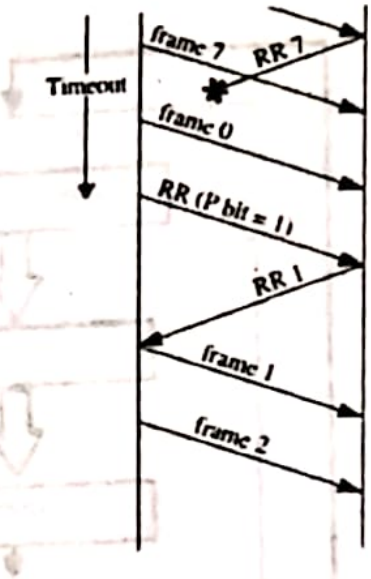
1st part:

Stop-and-wait ARQ:

Refer to Question No. 6(b) of Long Answer Type Questions.

Go-Back-N ARQ

- Receiver sends Ack for the correctly received frame.
- An Acknowledgement field has a meaning of "next expected sequence number" (Example: Ack 2 means "next expected packet sequence number is 2 and all packets up to 2(0, 1) are received).
- Sender keeps on sending frames (limited to the Window size) and receiver keeps on acknowledging.
- When a frame is damaged, receiver sends a Reject control packet (Nak).
- Sender goes back to the Rejected frame and sends all the frames starting with the rejected one even if those frames are already sent to the receiver.
- Sender's buffer size = Window size
- Receiver's buffer size = 1



5. a) What is a cyclic redundancy check?
b) Classify the errors that a CRC method will always detect and will not detect.
c) What are the major differences between the go-back-n and select repeat protocols? [WBUT 2018]

Answer:

a) & b) ***Refer to Question No. 2 of Short Answer Type Questions.***

c) ***Refer to Question No. 8(a) of Long Answer Type Questions.***

6. Write short notes on the following:

a) HDLC [WBUT 2016]
b) Stop-and-wait ARQ [WBUT 2016]
c) IEEE 802.11 [WBUT 2015, 2018]
d) Piggybacking [WBUT 2018]

Answer:

a) HDLC:

The High-Level Data-Link Control (HDLC) protocol ISO-standard, bit-oriented, Data Link layer protocol. It specifies an encapsulation method for data on synchronous serial data links using frame characters and checksums. HDLC is a point-to-point protocol used on leased lines. No authentication can be used with HDLC.

In byte-oriented protocols, controls information is encoded using entire bytes. On the other hand, bit-oriented protocols use single bits to represent the control information. Some common bit-oriented protocols include SDLC, LLC, HDLC, TCP, and IP.

HDLC is the default encapsulation used by Cisco routers over synchronous serial links. And Cisco's HDLC is proprietary – it won't communicate with any other vendor's HDLC implementation. But don't give Cisco grief for it – everyone's HDLC implementation is proprietary. Figure below shows the Cisco HDLC format.

Cisco HDLC

Flag	Address	Control	Proprietary	Data	FCS	Flag

Fig: Cisco HDLC frame format

Each vendor's HDLC has a proprietary data field to support multiprotocol environments.

HDLC

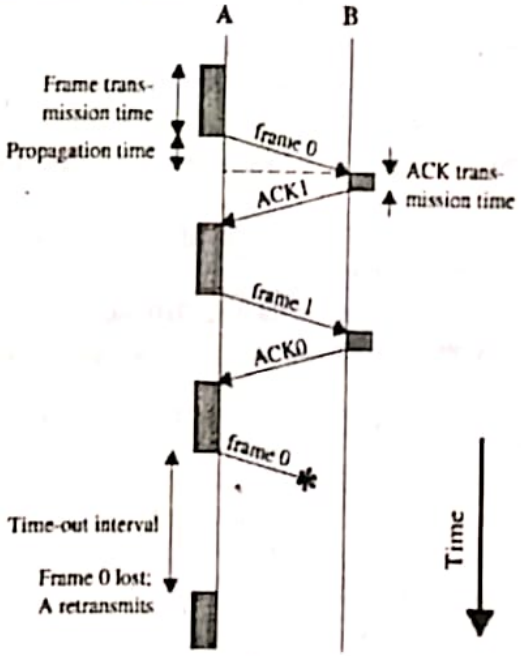
Flag	Address	Control	Data	FCS	Flag

Supports only single-protocol environments

As shown in the figure, the reason that every vendor has a proprietary HDLC encapsulation method is that each vendor has a different way for the HDLC protocol to encapsulate multiple Network layer protocols. If the vendors didn't have a way for HDLC to communicate the different layer 3 protocols, then HDLC would only be able to carry one protocol. This proprietary header is placed in the data field of the HDLC encapsulation.

b) Stop-and-wait ARQ:

Stop-and-wait ARQ is a method used to send information between two connected devices. It ensures that information is not lost due to dropped packets and that packets are received in the correct order. It is the simplest kind of automatic repeat-request (ARQ) method. A stop-and-wait ARQ sender sends one frame at a time; it is a special case of the general sliding window protocol with both transmit and receive window sizes equal to 1. After sending each frame, the sender doesn't send any further frames until it receives an acknowledgement (ACK) signal. After receiving a good frame, the receiver sends an ACK. If the ACK does not reach the sender before a certain time, known as the timeout, the sender sends the same frame again.



c) IEEE 802.11:

Refer to Question No. 15 of Short Answer Type Questions.

d) Piggybacking:

Refer to Question No. 5 of Short Answer Type Questions.

7. a) What is the disadvantage of character stuffing? [MODEL QUESTION]
b) Calculate the probability of single bit error in a massage of size n where the probability of a bit in error is P.
c) What is the minimum window size required for selective-repeat ARQ protocol and how?
d) If the received string is 110110111011 them calculate the actual data string. The data is encoded by 1 bit error correcting code (Hamming code).
e) Why acknowledgement is numbered in stop and wait protocol? Discuss a situation when unnumbered acknowledgements can create confusion in the sender and receiver end.

Answer:

a) The main disadvantage of character stuffing is that it is closely tied to 8-bit characters in general and the ASCII character code in particular. As networks grow, this disadvantage of embedding the character code in framing mechanism becomes more.

b) P(error in a bit) = p
Hence P(no error in bit) = 1 - p
P (There is error in i-th bit and no error in other bits) = $p * (1 - p)^{n-1}$
But error can be any of the n bits and each such event is mutually exclusive.
Hence required probability = $n * p * (1 - p)^{n-1}$

c) The size of the sending and receiving windows must be equal and half the maximum sequence number (assuming that sequence numbers are numbered from 0 to n–1) to avoid miscommunication in all cases of packets being dropped. To understand this, consider the case when all ACKs are destroyed.
If the receiving window is larger than half the maximum sequence number, some, possibly even all, of the packages that are resent after timeouts are duplicates that are not recognized as such. The sender moves its window for every packet that is acknowledged.

d) In hamming code of 12-bits, there must be 4 parity bits at positions 1, 2, 4 and 8 from the left. The remaining bits are data bits.
For the given code, parity bits = 1111 and data bits: 01011011.

Bit-pos	Bit	Checked by P1	Checked by P2	Checked by P3	Checked by P4
1	1	Y	N	N	N
2	1	N	Y	N	N
3	0	Y	Y	N	N
4	1	N	N	Y	N
5	1	Y	N	Y	N
6	0	N	Y	Y	N
7	1	Y	Y	Y	N
8	1	N	N	N	Y
9	1	Y	N	N	Y
10	0	N	Y	N	Y
11	1	Y	Y	N	Y
12	1	N	N	Y	Y
		P(101111) = 1	P(100101) = 1	P(11011) = 0	P(11011) = 0

The decimal number given by P4-P3-P2-P1 is 3. Hence bit-3 has been flipped.
So, correct string is: **111110111011**. So correct data is: **11011011**

e) The frame/ACK number field in Stop and Wait protocol is used in the receiver to distinguish between a new frame and a frame received earlier.
Suppose frames of succeeding packets are framed with frame numbers 0, 1, 0, 1, and so on (i.e., 0 and 1 repeating alternately).
The receiver keeps a local copy of the frame number that it expects to receive. If the arriving frame has a different frame number, it is silently discarded. On other cases, the receiver sets the ACK frame's frame-number with the received frames frame number and alters its expected frame number appropriately (0 to 1 or 1 to 0, as the case may be).
At the sender side, the last-sent frame is considered delivered correctly only if its frame number matches that of an ACK frame received.
Suppose frames and ACK-s are not numbered and a frame is sent and arrives error free on the receiver. It is delivered to the network layer and an unnumbered ACK is sent. Suppose the ACK itself gets corrupted on its way. The sender never gets the ACK and by the Stop and Wait algorithm, when the timer fires, it re-sends the frame. The receiver may receive this frame error-free. Since it has no inkling that the ACK it had sent earlier got lost, it will accept the frame and deliver the packet. In essence, the packet gets delivered twice and hence the sequence assumption is clearly broken.

8. a) What is the difference between Go-back-N ARQ and Selective Repeat ARQ?
b) What is the remainder obtained by dividing x^7+x^5+1 by the generator polynomial x^3+1?
c) What is polling?
d) How a new station is introduced in token bus? **[MODEL QUESTION]**

Answer:

a)

Go-Back-N ARQ	Selective Repeat ARQ
Retransmission begins with the last unacknowledged frame even if subsequent frames have arrived correctly duplicate frames are discarded. Go-back-n ARQ -- Receiver must get Frames in correct order.	Only the unacknowledged frame is retransmitted. It may be (slightly) more efficient than Go-back-n ARQ, but also much more complicated. Selective repeat ARQ – correctly - received out-of-order Frames are stored at Receiver until they can be re-assembled into correct order.

b) dividing x^7+x^5+1 by x^3+1 we get the remainder x^2+x+1
hence 110 is required remainder.

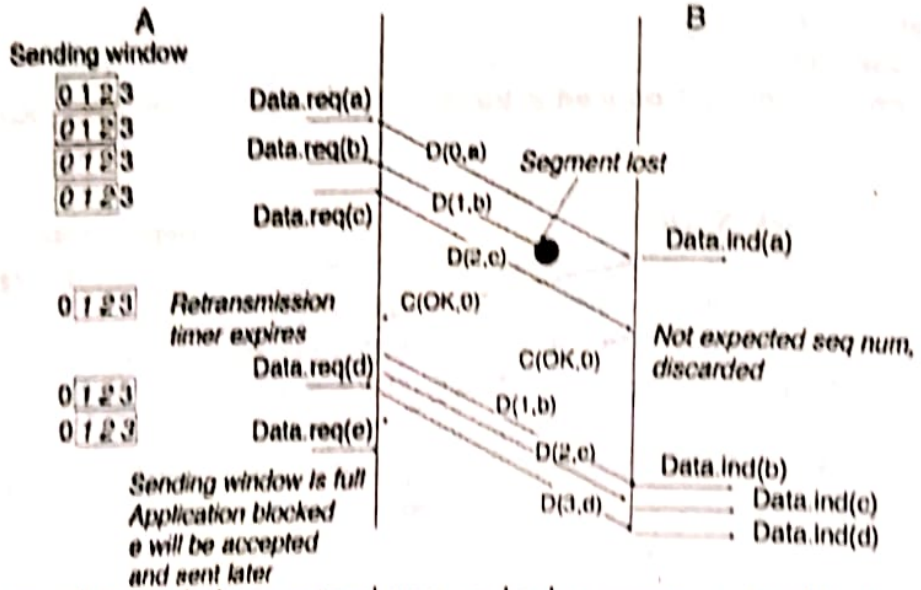
c) Computer network Polling is where a client server or Network Hub polls each computer for data. Data can only be sent when the particular computer is polled. If the computer has data to send but is not polled at that time, the data has to be stored until it can be sent.

d) Token Bus was a 4 Mbps Local Area Networking technology created by IBM to connect their terminals to IBM mainframes. Token bus utilized a copper coaxial cable to connect multiple end stations (terminals, workstations, shared printers etc.) to the mainframe. The coaxial cable served as a common communication bus and a token was created by the Token Bus protocol to manage or 'arbitrate' access to the bus. Any station that holds the token packet has permission to transmit data. The station releases the token when it is done communicating or when a higher priority device needs to transmit (such as the mainframe). This keeps two or more devices from transmitting information on the bus at the same time and accidentally destroying the transmitted data.

Token Bus suffered from two limitations. Any failure in the bus caused all the devices beyond the failure to be unable to communicate with the rest of the network. Second, adding more stations to the bus was somewhat difficult. Any new station that was improperly attached was unlikely to be able to communicate and all devices beyond it were also affected. Thus, token bus networks were seen as somewhat unreliable and difficult to expand and upgrade.

9. Explain with diagram, how the lost frame, delayed and lost acknowledgements are handled in Go-Back-N ARQ. [MODEL QUESTION]

Answer:



The simplest sliding window protocol uses go-back-n recovery. Intuitively, go-back-n operates as follows. A go-back-n receiver is as simple as possible. It only accepts the segments that arrive in-sequence. A go-back-n receiver discards any out-of-sequence segment that it receives. When a go-back-n receives a data segment, it always returns an acknowledgement that contains the sequence number of the last in-sequence segment that it received. This acknowledgement is said to be cumulative. When a go-back-n receiver

send an acknowledgement for sequence number x, it implicitly acknowledges the reception of all segments whose sequence number is earlier than x. A key advantage of these cumulative acknowledgements is that it is easy to receive from the loss of an acknowledgement. Consider for example a go-back-n receiver that received segments 1, 2 and 3. It sent OK1, OK2 and OK3. Unfortunately, OK1 and OK2 were lost. Thanks to the cumulative acknowledgements, when the receiver receives OK3, it knows that all three segments have been correctly received.

10. a) Applying CRC algorithm, determine the checksum and the transmitted frame for the frame 11010111 and for the generator polynominal $x^3 + x^2 + 1$.
b) How are a lost acknowledgement and a lost frame handled in Stop-and-Wait ARQ? **[MODEL QUESTION]**

Answer:

a) Frame: 11010111

Generator G(x) of degree 3, $x^3 + x^2 + 1$: 1101
T(x) is the frame with 3 attached 0-bits: 11010111000
Divide T(x) by G(x) by using XOR,

```
1101|11010111000|1000010
    1101
    ----
    0000
        01110
         1101
         ----
         000110 → Remainder
```

The remainder R(x)= 110. The Transferred frame: 11010111 **110**

b)

- If the sender receives a damaged ACK, it discards it.
- When the timer of the sender expires, the sender retransmits frame 1.
- Receiver has already received frame 1 and expecting to receive frame 0 (R=0). Therefore it discards the second copy of frame 1.