UNIT 3 PHYSICAL AND DATA LINK LAYER

Structure **Page Nos.**

3.0 INTRODUCTION

As you have studied earlier that the physical layer provides an electrical, mechanical, and functional interface to the transmission medium also the data link layer together with physical layer provide a data link connection for reliable transfer of data bits over an imperfect physical connection, between two adjacent nodes. In this unit, we will study about design of Data Link Layer and its Medium Access Control Sublayer. This includes various protocols for achieving reliable, efficient communication. It also covers the study of nature of errors, causes and how they can be detected and corrected. The MAC sublayer contains protocols which determine what goes next on a multi-access channel. In the end of this unit you will learn about working of ARP and RARP protocols.

3.1 OBJECTIVES

After going through this unit, you should be able to:

- Know the services of physical and data link layer
- Understand the concept of framing
- Understand various error handling methods;
- Know the Retransmission Strategies at data link layer
- Understand various flow control methods,
- Understand the working of MAC sub-layer protocols
- Differentiate between CSMA/CD, Polling and Token Passing.
- Understand the working of ARP and RARP

3.2 PHYSICAL AND DATA LINK LAYER SERVICES

To exchange digital information between devices A and B, we require an interconnecting transmission medium to carry the electrical signals; a standard interface and the physical layer to convert bits into electrical signals and vice-versa.

This is an elementary layer below the logical data structures of the higher level functions in a network. The physical layer deals with transmitting raw bits rather than logical data packets over a physical network. The bit stream may be grouped into code words or symbols and converted to an electrical signal that is transmitted over a hardware transmission medium.
The physical layer provides an electrical, mechanical, and functional interface to the transmission medium. This layer has certain limitations, for example assume:

- If the electrical signal gets impaired due to the encountered interference with other signals or electromagnetic waves from external sources, errors may be introduced in the data bits.
- Errors can also be introduced if the receiving device is not ready for the incoming signal, hence resulting in the loss of some information.

The data link layer constitutes the second layer of the hierarchical OSI Model. The Data Link layer together with physical layer provide a data link connection for reliable transfer of data bits over an imperfect physical connection, between two adjacent nodes. It accomplishes this task by having the sender break the input data into data frames, transmit the frames sequentially and process the acknowledgement frames sent back by the receiver. Remember, like other layers of OSI model this layer also create its own protocol data unit. Data link layer add some control bits to the protocol data unit received from network layer and convert into different protocol data unit called frames. The data link layer creates and recognises frame boundaries too.

Another issue that arises in data link layer is how to keep a fast transmitter from overflowing a slow receiver in data. The data link layer (Figure 1) incorporates certain processes, which carry out error control, flow control and the associated link management functions. The data block along with the control bits is called a frame.

Data link layer (Figure 1) is divided into two sublayers:

Logical Link Control (LLC) concerned with providing a reliable communication part between two devices. It is also involved with flow control and sequencing. The LLC is non-architecture-specific and is the same for all IEEE defined LANs.

Medium Access Control (MAC) focuses on methods of sharing a single transmission medium.

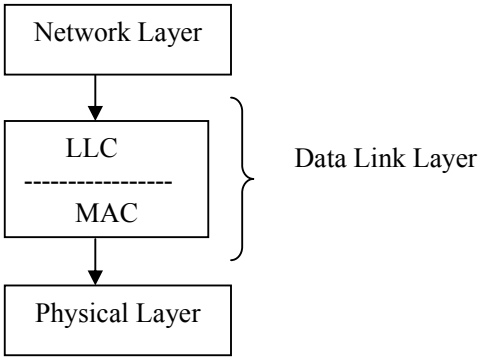


Figure 1: Division of Data Link Layer

The data link layer provides the functional means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the physical layer. Following are some of the main services provided by data

Link layer:

1. **Framing:** Encapsulation of network layer data packets into frames, and Frame synchronization
2. **Flow Control:** Flow control deals with how to keep the fast sender from overflowing a slow receiver by buffering and acknowledgement procedures. This flow control at data link layer is provided in addition to the one provided on the transport layer.
3. **Error detection and correction codes:** Various methods used for error-detection and corrections are – Parity bit, cyclic redundancy check, checksum, Hamming code, etc.
4. Multiple access protocols for channel-access control
5. Physical addressing (MAC addressing)
6. Quality of Service (QoS) control

3.3 ERROR DETECTION AND CORRECTION

Data that is either transmitted over communication channel or stored in memory is not completely error free. Transmission Errors may be caused by many reasons like Signal distortion or attenuation, synchronization problems, distorted channel, etc. Error detection and corrections are two different but related thing, error detection is the ability to detect errors but the error correction has an additional feature that enables identification and correction of the errors. Error detection always precedes error correction. Both can be achieved by having extra/ redundant/check bits in addition to data deduce that there is an error.

Error Detection

In the following section parity bit and CRC methods for error detection are discussed.

Parity bits Method

Parity bit method is very simple error detection method in the digital communication. A binary digit called “parity” is used to indicate whether the number of bits with “1” in a given set of bits is even or odd. The parity bit is then attached to original bits. In this method sender adds the parity bit to existing data bits before transmission. At the receiver side, it checks for the expected parity, if wrong parity found, the received data is discarded and retransmission is requested. It is a very simple scheme that can be used to detect single or any other odd/even number of errors in the output.

The parity bit is only suitable for detecting errors; it cannot correct any errors, as there is no way to determine which particular bit is corrupted. The data must be discarded entirely, and re-transmitted from scratch. Following are some of the examples for parity bit methods:

Assume, sender wants to send some bit streams like 001 0101 and 101 0011. If we are using even parity bit method, we will add “0” with the bit steam having even number of 1’s otherwise add “1”. So our bit steams will be changed after adding parity bit as **1**001 0101and **0**101 0011. At the receiver again the number of 1’s are counted in the original message, if the parity bit is mismatched we can say an error has occurred in the message. Just like the even parity we may have odd parity bit method. Parity bit method has many limitations, like it cannot identify the error if more than one bit has been changed or parity bit itself has been changed during the transmission. Further it cannot determine which bit position has a problem.

Cyclic redundancy checks (CRCs)

A cyclic redundancy check (CRC) is an error-detecting code commonly used in digital networks and storage devices to detect transmission error.

When n-bits of message M(x) is transmitted from sender to receiver, first the n- bits of message is converted in such a way that when a selected k-bits divisor code G(k) (so-called generator polynomial) is divided with the x+k-bits message M(x+k) the remainder is zero.

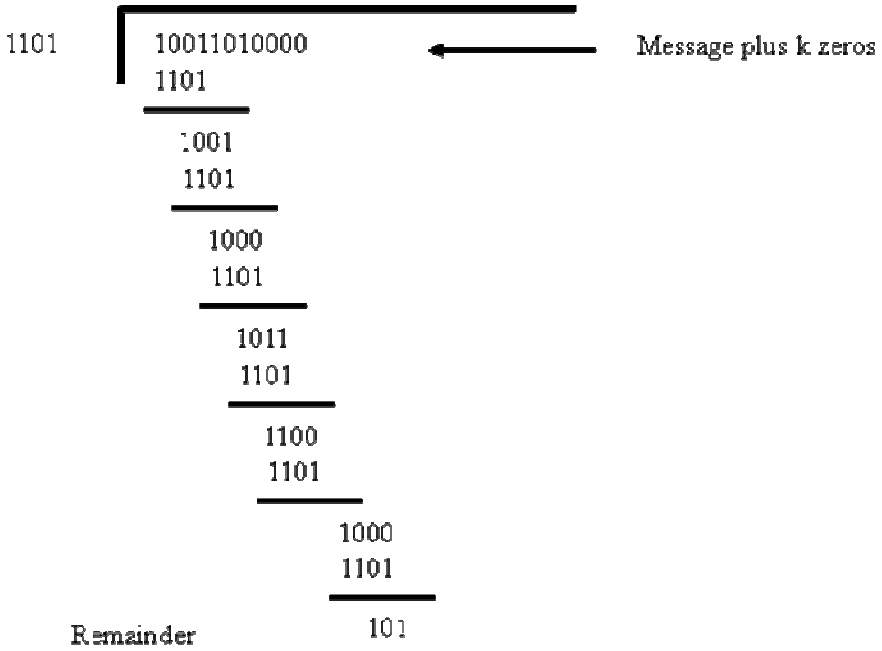
Than the modified message M(x+k) is sent along with the k-bits divisor code to the receiver through channel. The receiver will divide this M(x+k) bits with G(k) bits, if the remainder is zero receiver can say there is no error in the message. Finally the original message M(x) is separated from the modified message M(x+k).

Let us take assume an example for simple decimal numbers, if you want to send some number say 10 and divisor code is 3. First, make all legal messages divisible by 3. For that you need to multiply by 4 to get 40 and add 2 to make it divisible by 3 = 42. When the data is received and divided by 3, and if there is no remainder, it means there is no error. If no error, divide by 4 and separate it by 2 to get sent message. If we receive 43, 44, 41, 40, we can say there is an error. But if 45 is received, we will not be able to recognize as an error.

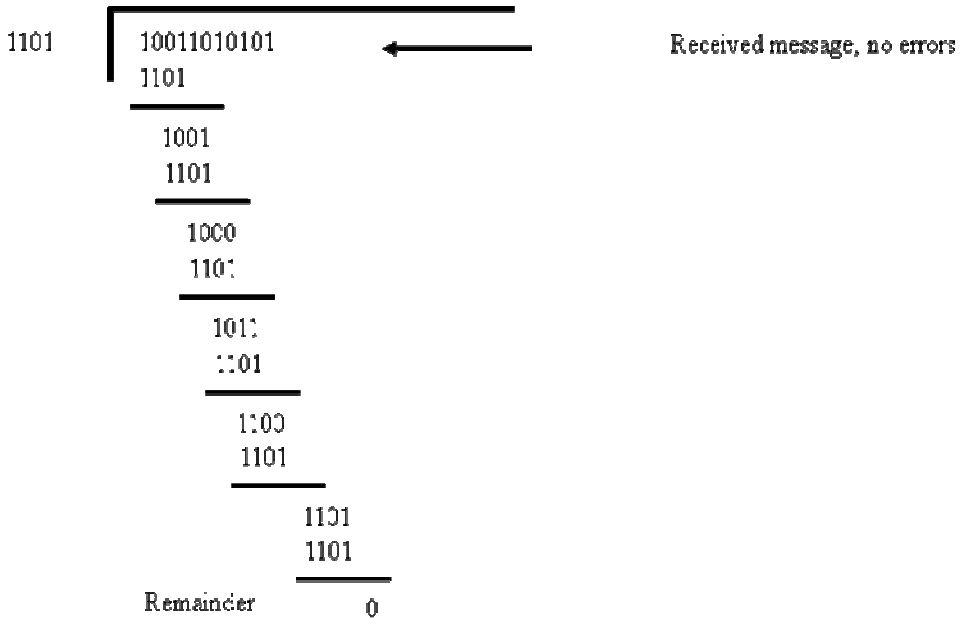
We can represent n-bit message as an n-1 degree polynomial; e.g., M=10011010 corresponds to M(x) = x7+ x4 + x3 + x1.

Add k bits of extra data to an n-bit message.
Let k be the degree of some divisor polynomial G(k); e.g., G(k) = x3+ x2 + 1.

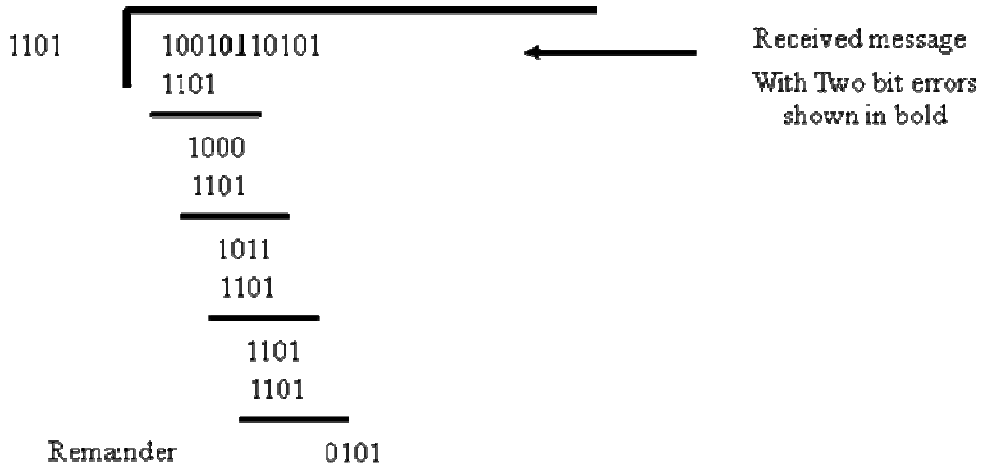
Multiply M(x) = x7+ x4 + x3 + x1 by x^k; for our example, we get
x10 + x7 + x6 + x4 (10011010000);divide result by G(k) (1101);



Send 10011010000 + 101 = 10011010101, since this must be exactly divisible by G(k);



Now, assume if receiver will receive a message with errors, for example receiver has received a message 10010110101.



Cyclic codes have favorable properties in that they are well suited for detecting burst errors. CRCs are particularly easy to implement in hardware, and are therefore commonly used in digital networks and storage devices such as hard disk drives.

Error correction

Mainly, we have two error correction mechanisms one is Automatic Repeat request and another approach is of using some error correction codes like hamming code.

Automatic Repeat Request

It is an error control method for data transmission that makes use of error-detection codes, acknowledgment and/or negative acknowledgment messages, and timeouts to get reliable data transmission. Generally, when the sender does not receive the acknowledgment before the timeout occurs, it retransmits the frame until it is either correctly received or the error persists beyond a predetermined number of retransmissions. Three types of ARQ protocols are Stop-and-wait ARQ, Go-Back-N ARQ, and Selective Repeat ARQ, these mechanisms we will study further in this unit.

Error-correcting codes

Any error-correcting code can be used for error correction. An error-correcting code is a system of adding redundant data, or parity data, to a message, such that it can be recovered by a receiver even when a number of errors were introduced, either during the process of transmission, or on storage. Since the receiver does not have to request the sender for retransmission of the data, a back-channel is not required in forward error correction, and it is therefore suitable for simplex communication such as broadcasting. Error-correcting codes are often used in lower layers of OSI like data link layer and physical layer.

Error-correcting codes can be classified into two type's convolutional codes which processed on a bit-by-bit basis and block codes that processed on a block-by-block basis. Convolutional codes are suitable for implementation in hardware. However, block codes are error correction in data communication. Hamming code is an example of block codes. Hamming codes are code words formed by adding redundant check bits, or parity bits, to a data word. The Hamming distance between two code words is the number of bits in which two code words differ. For an example 10001001 and 10110001 bytes has a Hamming distance of 3. The minimum Hamming distance for a code is the smallest Hamming distance between all pairs of words in the code. The minimum Hamming distance for a code, D(min), determines its error detecting and error correcting capability. Hamming codes can *detect* D(min) - 1 errors and correct (D(min) - 1)/2 errors.

☛ Check Your Progress 1

1. What are the sub-layers of data link layer? Explain.

   ……

   ……

   ……

   ……

2. List the services of data link layer.

   ……

   ……

   ……

   ……

3. What is parity bit method? Explain its use with the help of an example.

   ……

   ……

   ……

4. Explain the use of Automatic Repeat Request in error correction.

   ……

   ……

   ……

3.4 FLOW AND ERROR CONTROL

Packets can be lost and/or corrupted during transmission due to Bit level errors and loss due to congestion. We use checksums to detect bit level errors, and to maintain reliability into the data transmission stage we use *acknowledgements* and *timeouts* to signal lost or corrupt frame. An acknowledgement (ACK) is a packet sent by one host in response to a packet it has received. A timeout is a signal that an ACK to a packet that was sent has not yet been received within a specified timeframe. In this section we will discuss several retransmission strategies, which are also considered as a flow control and error control mechanism.

Stop and Wait

The sender allows one message to be transmitted, checked for errors and an appropriate ACK (Positive Acknowledgement) or NAK (Negative Acknowledgement) returned to the sending station. No other data messages can be transmitted until the receiving station sends back a reply, thus the name STOP and WAIT is derived from the originating station sending a message, stopping further transmission and waiting for a reply. This scheme is also shown in figure 2 given below.

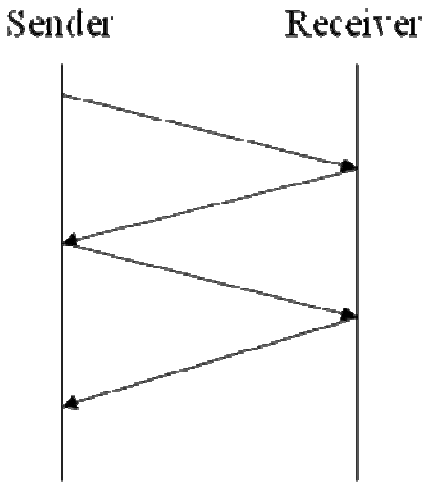


Figure 2: Stop and Wait Protocol

Its major drawback is the idle line time that results when the stations are in the waiting period. If the ACK is lost then the sending station retransmits the same message to the receiver side. The redundant transmission could possibly create a duplicate frame. A typical approach to solve this problem is the provision for a sequence number in the header of the message. The receiver can then check for the sequence number to determine if the message is a duplicate. The Stop and Wait mechanism requires a very small sequence Number, since only one message is outstanding at any time. The sending and receiving station only use a one bit alternating sequence of 0 and 1 to maintain the relationship of the transmitted message and its ACK/NAK status.

Sliding Window

Here data and control frames flow from sender to receiver in a more continuous manner and several frames can be outstanding at any one time as depicted in figure 3. Allow multiple outstanding (un-ACKed) frames. Upper bound on un-ACKed frames, called window. Sender needs to buffer data so that if data is lost, it can be resent.
Receiver needs to buffer data so that if data is received out of order, it can be held until all packets are received in Flow control Next,
How can we prevent sender overflowing receiver's buffer?
Receiver tells sender its buffer size during connection setup.

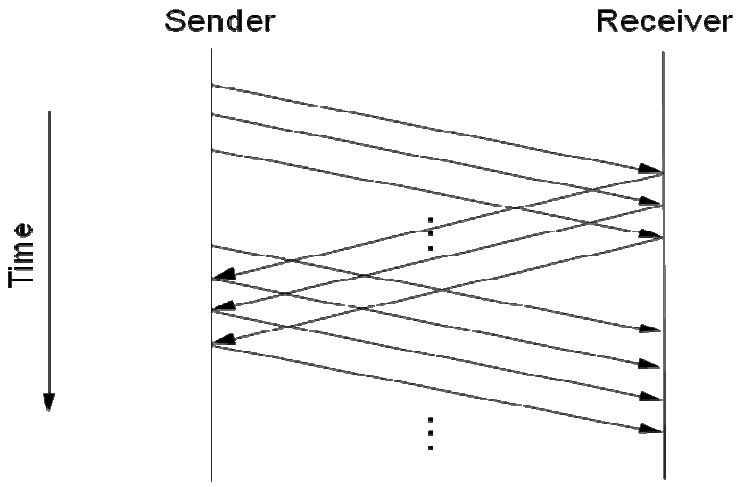


Figure 3: Simple Sliding Window Scheme

The transmitting station maintains a sending window that maintains the number of frames it is permitted to send to the receiving station and the receiving station also maintains a receiving window that performs complementary functions. The two sides use the window to coordinate the flow of frames between each other. The window wrap around is used to reuse the same set of numbers for different frames. There are sliding window techniques:

1. Go Back N
2. Selective Repeat

Go Back N

This is a sliding window technique as shown in figure 4. It allows data and control messages to be
transmitted continuously without waiting for its acknowledgement from the receiver. In the event of error detection at the receiving side, the erroneous message is retransmitted, as well as all other frames that were transmitted after the erroneous message.

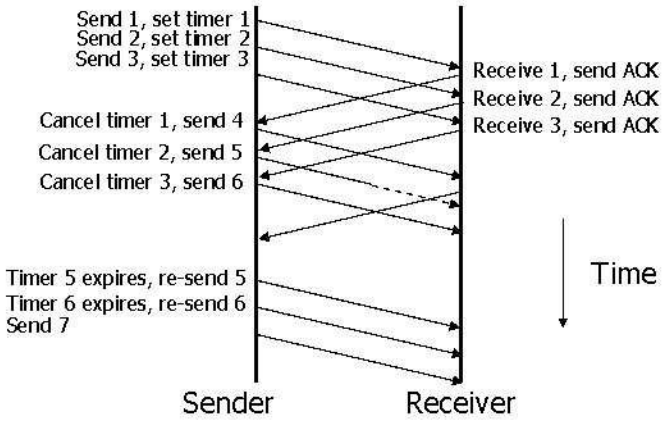


Figure 4: Go Back N Scheme

Sender has to buffer all unacknowledged packets, because they may require retransmission. Receiver may be able to accept out-of-order packets, but only up to its buffer limits. The sender needs to set timers in order to know when to retransmit a packet that may have been lost

Selective Repeat

This method provides for a more refined approach. In contrast to the Go back N, the only messages retransmitted are those for which negative acknowledgement is received. In this the sending process continues to send a number of frames specified by a window size even after a frame loss. Unlike Go-Back-N, the receiving process will continue to accept and acknowledge frames sent after an initial error; this is the general case of the sliding window protocol with both transmit and receive window sizes greater than 1.

The receiver process keeps track of the sequence number of the earliest frame it has not received, and sends that number with every acknowledgement (ACK) it sends. If a frame from the sender does not reach the receiver, the sender continues to send subsequent frames until it has emptied its window. The receiver continues to fill its receiving window with the subsequent frames, replying each time with an ACK containing the sequence number of the earliest missing frame. Once the sender has sent all the frames in its window, it re-sends the frame number given by the ACKs, and then continues where it left off.

Now if we compare Selective Repeat behaves in the same way like Go-Back-N , it accepts when the receiver receives a frame which is out of sequence, it sends a SREJ(Selective Reject) message. Sender retransmits only the rejected packet and continues with other packets. Here in Selective Repeat method the both the Sender's and Receiver's buffer size are equal to the window size.

In the following figure 5, you can see that the difference between Go Back N and Selective Repeat, because of the buffer frame 5 and Frame 6 are stored and selectively the reject message is sent only for frame 4 (which was lost in transmission) however in Go back N the reject message is sent for all 4, 5 and 6 frames.

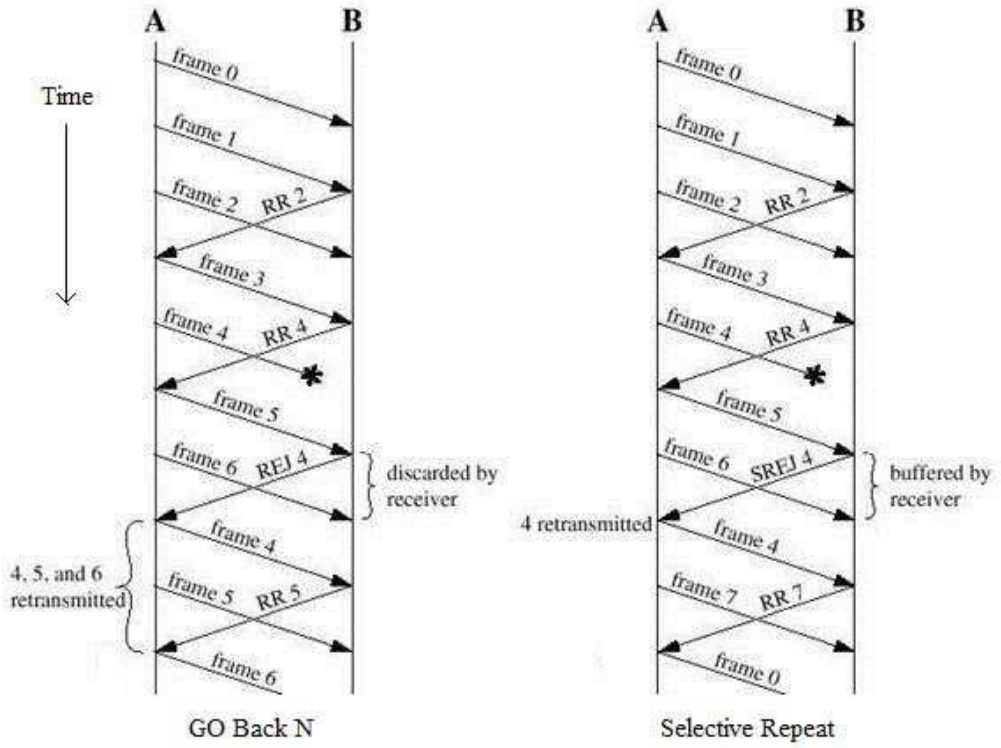


Figure 5: Comparison between the Go Back N and Selective Repeat method

Studies reveal that the selective repeat mechanism produces greater throughput than the Go Back N. Selective Repeat mechanism requires additional logic to maintain the sequence of the recent message and merge it into the proper place as the queue at the receiver end.

☞ Check Your Progress 2

1. Explain the importance of Sliding Window protocol. Also, List the types of sliding window techniques.

   ……

   ……

   ……

   ……

2. Discuss the working of selective Repeat method. Also, compare it with GO Back N.

   ……

   ……

   ……

   ……

3.5 MEDIUM ACCESS CONTROL (MAC) SUBLAYER

In any broadcast network, key issue is how to determine who gets to use the channel when there is competition for it. The protocols used to determine who goes next on a multi-access channel belong to a sub-layer of a Data Link Layer called MAC sublayer.

3.5.1 Contention Based Media Access Protocols

Contention is what happens at a staff meeting when several people start to speak at the same time. In contention protocol, no one controls usage of the communication channel.

All workstations on a contention network share a common transmission channel. Messages are broadcasted on that channel and may be overheard by all attached workstations. A workstation responds only to message with its address. Message intended for other nodes are ignored.

Message to be transmitted are converted to packets and are sent when ready, without verifying the availability of the channel. When transmission of a station overlaps with that of another, collision occurs. Colliding packets with their messages are destroyed.

3.5.2 Random Access Protocols

In random access approach, any station is not superior to another station and none is assigned the control over another. A station with a frame to be transmitted can use the link directly based on a procedure defined by the protocol to make a decision on whether or not to send.

Pure ALOHA

It is based on simple principles that if you have data to send, send the data immediately. If the message collides with another transmission, after some random time wait, we can resend it message. In this, all frames from any station are of fixed length size and produce frames with equal frame lengths. A station that has data can transmit at any time, after transmitting a frame, the sender waits for an acknowledgment for an amount of time. If ACK was not received, sender assumes that the frame or ACK has been destroyed and resends that frame after it waits for a random amount of time.

Slotted ALOHA

Slotted ALOHA is an improvement over pure ALOHA, which has discrete timeslots. A station is allowed to send the message only at the beginning of a timeslot, due to time the possibility of collisions are reduced. If a station misses the beginning of a slot, it has to wait until the beginning of the next time slot. A central clock or station informs all stations about the start of an each slot.

Channel utilization or efficiency or Throughput is the percentage of the transmitted frames that arrive successfully (without collisions) or the percentage of the channel bandwidth that will be used for transmitting frames without collisions.

The throughput (S) for pure ALOHA is $S = G \times e^{-2G}$. The maximum throughput is $S_{max} = 0.184$ when G= (1/2). Where, G is equal to the traffic load. In case of Slotted ALOHA the throughput is $S = G \times e^{-G}$ and the maximum throughput is $S_{max} = 0.368$ when G = 1. The following figure 6 shows the different between pure and slotted ALOHA based on the traffic load and throughput.

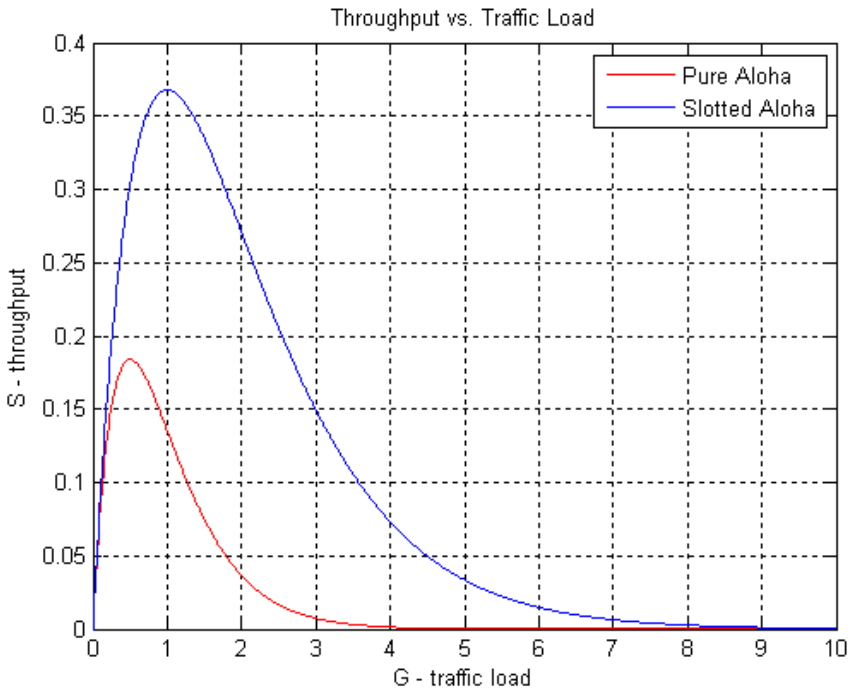


Figure 6: Different between pure and slotted ALOHA (source wikipedia.org)

CSMA/CD

Before discussing about CSMA/CD (Carrier Sense Multiple Access with Collision Detection), let us first discuss about simple CSMA. Carrier Sense Multiple Access

(CSMA) is a MAC layer protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium. Here, the Carrier Sense means the fact that a transmitter uses feedback from a receiver before trying to send any message. If a carrier is sensed, the station waits for the transmission in progress to finish before initiating its own transmission. And the Multiple Access means that multiple stations are sending and receiving on the same medium. Based on different situations of medium like medium busy or idle different CSMA protocols has been designed like non-Persistent CSMA, 1-Persistent CSMA and p-Persistent CSMA. All these types of CSMA have inefficiency in term of collision detection. Assume that a collision has occurred, than the channel is unstable until colliding packets have been fully transmitted. A standards and rules need to be created for stations like when they could send data and when they could not.

This standard in CSMA is Carrier Sense Multiple Access with Collision Detection, referred to as CSMA/CD.

To avoid collision, CSMA/CD compel stations to "listen" to the channel before sending in order to make sure that no other host on the wire is sending. When the channel is not busy, station may send its data. The sender will then continue to listen, to make sure that sending the data have not caused a collision. If a collision is heard, senders will send a jam signal over the network. This jam signal indicates to all other devices on the network segment that there has been a collision, and they should not send data onto the channel. After sending the jam signal, each of the senders will wait a random amount of time before beginning the entire process over. CSMA/CD (Carrier Sense Multiple Access with Collision Detection) While reducing channel wastage. It is widely used for bus topology LANs (IEEE 802.3, Ethernet).

3.5.3 Polling based MAC Protocols

Polling involves the channel control of all workstations in a network. The primary workstation which acts like a teacher going down the rows of the class room asking each student for homework. When one student has answered, the next is given a chance to respond. A polling network contains two classes of workstations, the primary workstation and the multiple secondary workstations connected to it. A buffer that can temporarily store messages is associated with each secondary workstation. When a workstation has information to transmit, the data is passed to the buffer. The frames are held until the central controller polls the workstation.

Following are two possibilities for the path of a message from some to destination workstation:

- All messages may be required to pass to the central workstation, which route them to their destination.
- Messages may be sent directly.

Polling technique can be said to maintain a tight control over the network resources than do contention based protocols.

Token Passing

The network continuously circulates a special bit pattern known as a token among all the nodes in the network.

Each token contains network information, comprising of a header, a data field and a trailer. Any node willing to send a frame has to grab a token first. After a node has captured a token it transmits its frame. The frame is relayed by all intermediate nodes till it reaches destination, when it is copied. Now let us talk about some standards.

3.5.4 IEEE Standard 802.3 and Ethernet

It uses CSMA/CD mechanism Expand (carrier Seen Multiple Access/Collision Detect). When station wants to transmit, it listens to the cable. If the cable is busy, the station waits until it goes idle, otherwise it transmits immediately. If two or more stations simultaneously begin transmitting on an idle cable they will collide. All colliding stations then terminate their transmissions, wait a random time and repeat the whole process all over again.

3.5.5 IEEE Standard 802.4 Token Bus

Token bus combines features of Ethernet and token ring (discussed in the next section). It combines the physical configuration of Ethernet (bus topology) and collision free (predictable delay) feature of token ring. Token bus is a physical bus that operates as logical ring using tokens.

It is a linear cable onto which the stations are attached. When the logical ring is initialised, the highest numbered station may send the first frame after it is done, it passes permission to its immediate neighbour by sending the neighbour a special control frame called a token.

The token propagates around the logical ring with only the token holder being permitted to transmit frames. Since only one station at a time holds the token, collisions do not occur.

3.5.6 IEEE Standard 802.5 Token Ring

In a token ring, the token circulates around the ring whenever all stations are idle. When a station wants to transmit a frame, it is required to seize the token and remove it from the ring before transmitting. This action is done by inverting a single bit in the 3-byte token which instantly changes it into the first 3 bytes of a normal data frame. Because there is only one token, only one station can transmit at a given instant, thus solving the channel access problem.

3.5.7 Address Resolution Protocol (ARP)

We have seen that IP address makes the addressing uniform on the Internet. Routing of packets is done using the IP addresses of the packet. However, communication in a local network is broadcast, which is done using physical address. Therefore, when the packet reaches the destined network, there must be a process of obtaining the physical address corresponding to its IP address, of a computer in order to finally deliver the datagram to the destined computer. The physical address corresponding to an IP address is resolved by using address resolution protocol (ARP). ARP maps given IP address to a physical address as shown in the Figure 7. It takes host's IP address as input and gives its physical address as output.

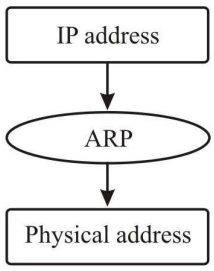


Figure 7: ARP maps the IP address to the physical address

ARP assumes that every host knows its IP address and physical address. Any time a host needs to know the physical address of another host on the network, it creates an ARP packet that includes the IP address X of the destination host asking–Are you the one whose IP address is X? If yes, please send back your physical address. This packet is then broadcasted over the local network. The computer, whose IP address matches X, sends an ARP reply packet, with its physical address. All the other hosts ignore the broadcast. Next time the host needs to send a datagram to the same destination, it need not broadcast an ARP query datagram; instead it can look up in its ARP cache. If the mapping is not found in the cache, then only the broadcast message is sent.

3.5.8 Reverse Address Resolution Protocol (RARP)

This protocol performs the job exactly opposite to ARP. It maps a physical address to its IP address as shown in Figure 8. Where is this needed? A node is supposed to have its IP address stored on its hard disk. However, there are situations when the host may not have hard disk at all, for example a diskless workstation. But also, when a host is being connected to the network for the first time, at all such times, and a host does not know its IP address. In that case, RARP find out the IP address, this process is shown in Figure 8.

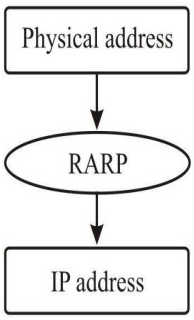


Figure 8: RARP maps the physical address to the IP address

☞ Check Your Progress 3

1. Compare the Throughput of pure and slotted ALOHA.

   ……

   ……

   ……

2. Explain the need of RARP.

   ……

   ……

3.6 SUMMARY

After studying this unit, we are sure that you understood the services and protocol of data link layer. Essentially it provides the functional means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the physical layer. We have briefly discussed various methods used for error-detection and corrections are – Parity bit, cyclic redundancy check, Hamming code, etc. In this unit you have studied some flow control and error control mechanism to ensure the reliability of communication. In this unit you have studied sliding window mechanisms mainly used for flow control at data link layer. As you know that the key issue is how to determine who gets to use the channel when there is

competition for it. In this unit, we have studied the protocols used to determine who goes next on a multi-access channel. In the end of this unit we have studied address resolution protocols to map between IP addresses and the physical addresses of the machines.

3.7 REFERENCES/FURTHER READING

1. *Computer Networks*, A. S. *Tanenbaum* 4th Edition, Practice Hall of India, New Delhi. 2003.
2. *Introduction to Data Communication & Networking,* 3rd Edition, Behrouz Forouzan, Tata McGraw Hill.
3. *Computer Networking*, J.F. Kurose & K.W. Ross, A Top Down Approach Featuring the Internet, Pearson Edition, 2003.
4. *Communications Networks*, Leon Garcia, and Widjaja, Tata McGraw Hill, 2000.
5. *Data and Computer Communications,* Willian Stallings, 6th Edition, Pearson Education, New Delhi.
6. www. wikipedia.org
7. Larry L. Peterson, *Computer Networks*: A Systems Approach, 3rd Edition (The Morgan Kaufmann Series in Networking).

3.8 SOLUTIONS/ANSWERS

☞ Check Your Progress 1

1. Data link layer is divided into two sublayers LLC and MAC. **Logical Link Control** (LLC) concerned with providing a reliable communication part between two devices. It is also involved with flow control and sequencing. The LLC is non-architecture-specific and is the same for all IEEE defined LANs. **Medium Access Control (MAC)** focuses on methods of sharing a single transmission medium.

2. Following are services provided by data link layer:
   - i) **Framing:** Encapsulation of network layer data packets into frames, and Frame synchronization
   - ii) **Flow Control:** Flow control deals with how to keep the fast sender from overflowing a slow receiver by buffering and acknowledgement procedures. This flow control at data link layer is provided in addition to the one provided on the transport layer.
   - iii) **Error detection and correction codes:** Various methods used for error-detection and corrections are – Parity bit, cyclic redundancy check, checksum, Hamming code, etc.
   - iv) Multiple access protocols for channel-access control
   - v) Physical addressing (MAC addressing)
   - vi) Quality of Service (QoS) control

3. Parity bit method is very simple error detection method in the digital communication. A binary digit called "parity" is used to indicate whether the number of bits with "1" in a given set of bits is even or odd. The parity bit is then attached to original bits. Assume sender want to send some bit streams like 001 0101 and 101 0011. If we are using even parity bit method, we will add "0" with

the bit steam having even number of 1's otherwise add "1". So our bit steams will be changed after adding parity bit as **1**001 0101and **0**101 0011. At the receiver again the number of 1's are counted in the original message, if the parity bit is mismatched we can say an error has occurred in the message. Just like the even parity we may have odd parity bit method.

4. It is an error control method for data transmission that makes use of error-detection codes, acknowledgment and/or negative acknowledgment messages, and timeouts to get reliable data transmission. Generally, when the sender does not receive the acknowledgment before the timeout occurs, it retransmits the frame until it is either correctly received or the error persists beyond a predetermined number of retransmissions. Three types of ARQ protocols are Stop-and-wait ARQ, Go-Back-N ARQ, and Selective Repeat ARQ, these mechanisms we will study further in this unit.

☞ Check Your Progress 2

1. In Sliding Window data and control frames flow from sender to receiver in a more continuous manner and several frames can be outstanding at any one time. Allow multiple outstanding (un-ACKed) frames. Upper bound on un-ACKed frames, called window. Sender needs to buffer data so that if data is lost, it can be resent. Receiver needs to buffer data so that if data is received out of order, it can be held until all packets are received Flow control. The transmitting station maintains a sending window that maintains the number of frames it is permitted to send to the receiving station and the receiving station also maintains a receiving window that performs complementary functions. The two sides use the window to coordinate the flow of frames between each other. The window wrap around is used to reuse the same set of numbers for different frames.

   There are sliding window techniques:

   Go Back N
   Selective Repeat

2. This method provides for a more refined approach. In contrast to the Go back N, the only messages retransmitted are those for which negative acknowledgement is received. In this the sending process continues to send a number of frames specified by a window size even after a frame loss. Unlike Go-Back-N, the receiving process will continue to accept and acknowledge frames sent after an initial error; this is the general case of the sliding window protocol with both transmit and receive window sizes greater than 1.

   The receiver process keeps track of the sequence number of the earliest frame it has not received, and sends that number with every acknowledgement (ACK) it sends. If a frame from the sender does not reach the receiver, the sender continues to send subsequent frames until it has emptied its window. The receiver continues to fill its receiving window with the subsequent frames, replying each time with an ACK containing the sequence number of the earliest missing frame. Once the sender has sent all the frames in its window, it re-sends the frame number given by the ACKs, and then continues where it left off.

   Now if we compare Selective Repeat behaves in the same way like Go-Back-N , it except when the receiver receives a frame which is out of sequence, it sends a SREJ(Selective Reject) message. Sender retransmits only the rejected packet and continues with other packets. Here in Selective Repeat method the both the

   Sender's and Receiver's buffer size are equal to the window size.

☞ Check Your Progress 3

1. Throughput is the percentage of the transmitted frames that arrive successfully (without collisions) or the percentage of the channel bandwidth that will be used for transmitting frames without collisions. The throughput (S) for pure ALOHA is $S = G \times e^{-2G}$. The maximum throughput is $S_{max} = 0.184$ when G= (1/2). Where, G is equal to the traffic load. In case of Slotted ALOHA the throughput is $S = G \times e^{-G}$ and the maximum throughput is $S_{max} = 0.368$ when G = 1.
2. RARP maps a physical address to its IP address. Where is this needed? A node is supposed to have its IP address stored on its hard-disk. However, there are situations when the host may not have hard disk at all, for example a diskless workstation. But also when a host is being connected to the network for the first time, at all such times, a host does not know its IP address. In that case RARP find out the IP address.