Contents

Unit 9
The Link Layer and Local Area Network

Structure of the Unit

9.1 Unit Outcomes

After the successful completion of this unit, the student will be able to:

- Summarize several important link-layer concepts and technologies.
- Identify error detection and correction methods.
- Comprehend the need for Multiple Access Protocols
- Describe the switched LANs and wireless LANs

9.2 Introduction to Data Link Layer

This layer is the second layer or the layer above the physical layer in the OSI Reference Model. This layer performs various functions but the primary function is to transfer data on an individual link or is responsible for delivering data from node to node, hiding the hardware details of the physical layer which is below it to its upper layers.

Fig. 9.1 shows the same scenario discussed in Section 3.2 with appropriate changes showing the communication at the data link layer. In the communication path, there are five logical connections between the data link layers at Jay's computer, routers R2, R4, R5, R7, and Ram's computer.
We can see that the source and destination computers are connected to only one network, so only one data link layer is involved, whereas there are two data link layers involved at the routers, as they switch

data from one network to another.

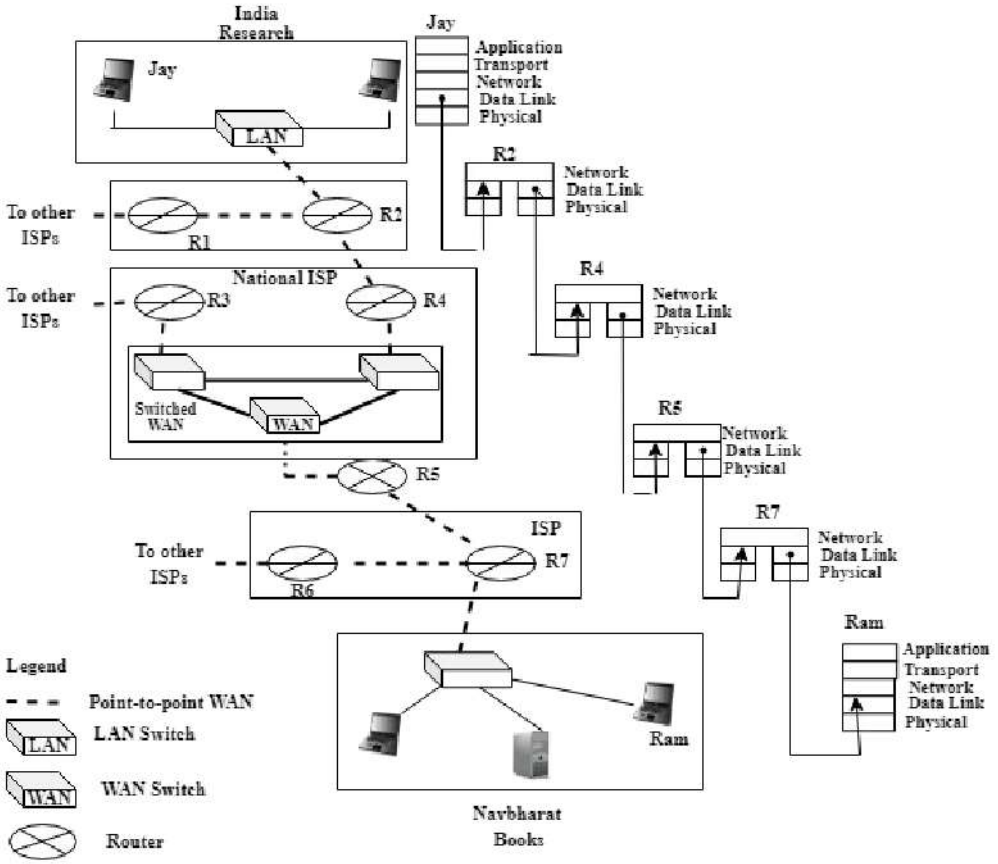

Fig. 9.1: Communication at the data-link layer

9.2.1 Nodes and Links

This layer operates between two nodes connected directly either in a broadcast mode or a point-to-point mode. One node may be connected to another node either by a wired or wireless medium.

Examples of point-to-point communication links are, where a user's computer is connected to an Ethernet switch in a LAN or two routers connect through a long-distance link.

Examples of broadcast links are where multiple nodes are connected in a wireless LAN, satellite networks, etc.

Fig.9.2 shows a representation of a small segment of the internet showing 3 links and 4 nodes. The first node (on the left in Fig. 9.2b) is the source host and the last node (on the right) is the destination host. The second and third nodes are routers connected in a point-to-point mode.

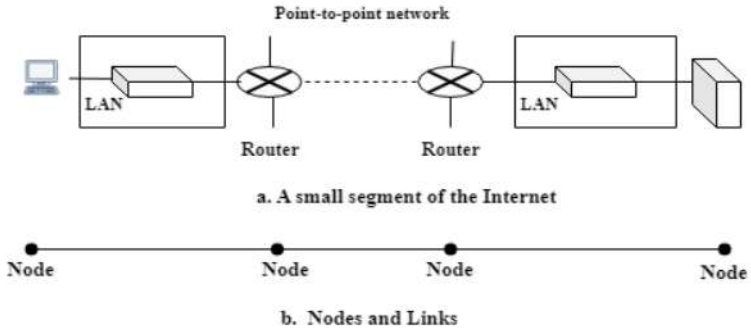

Fig. 9.2: Nodes and Links

9.2.2 Services provided by the Data Link Layer

Basically, this layer deals with the movement of data in and out of the physical layer at a node during data reception and transmission respectively. At the transmitter, this layer converts the stream of bits received from the top layer (Network Layer) into signals and transfers them across the hardware (the physical layer). At the receiver, this layer gathers the data from hardware which are in the form of electrical signals and then combines them together into a recognizable frame format. The frames are then passed to the network layer.

The important services provided by the data link layer are Link Access, Framing, Error Detection and Correction, and Reliable Delivery. To provide the above services, the data link layer uses a set of protocols to deal with addressing and framing, flow control, error detection, and correction.

Framing:

The network layer packets are encapsulated by the data link layer protocols within a frame before transmission. The data link layer maintains the connection between two devices on the same network As devices are identified by physical or MAC addresses, the source and destination MAC addresses are added in the header to construct a frame. A frame also contains a trailer part containing a frame check sequence for error correction at the receiver, and frame delimiters to identify the beginning and end of the frame. Fig. 9.3 demonstrates the functionality at the packet and frame level.

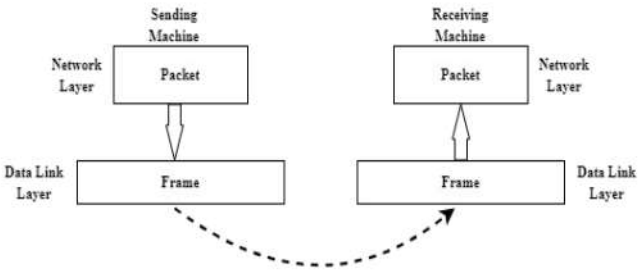

Fig.9.3: Conversion of Packet to frame at Data Link Layer

Link Access:
A media access control (MAC) protocol is used to transmit a frame on a link when the link is available. The protocol has two basic versions for controlling access to point-to-point links and broadcast links.

Reliable Delivery:
Reliability is a guaranteed transmission of a network layer data unit or a packet without any error across a link. This is achieved through acknowledgment from the receiver about its delivery or retransmissions.
Link layer reliability service is needed for links with high error rates like in a wireless link. Here errors in transmission can be detected and corrected locally on the link where errors occur and end-to-end retransmissions are not used by the transport or application layer protocols.

Error Detection and Correction:
Bit errors are introduced due to various factors, so there are link layer protocols to detect bit errors. This is implemented by adding error-detection bits in the frame format at the transmitting node and detecting errors at the receiving node through these bits.

9.2.3 Layered Implementation
All the above functions of the data link layer are implemented in two sub-layers: the data link control (DLC) and media access control (MAC).

1. The DLC identifies the device addresses, controls the data flow among different services and applications, and provides a data reception acknowledgment and error notification mechanism.
2. The MAC sublayer helps in providing access control to the physical media for transport and physical addressing of frames and controls the connection between the devices.

NOTE: The link layer is implemented in a network adapter also called a Network Interface Card, which is a chip (hardware).

NOTE: The two devices operating at the link layer are bridges and layer 2 switches.

In the following sections, the following topics are discussed:

1. Study of important services of the data link layer in detail,
   - Error Detection and Correction.
   - Accessing the physical media for transmission.
2. Importance of Switching in LANS
3. Architecture of Wireless LANs and their benefits

9.3 Data Link Layer and Error Detection
In data transmission, messages can get corrupted at any time and there are various factors that can change one or more bits of a message. Some of the applications like audio/video in television reception can tolerate small errors but in applications where textual messages are transferred, a high degree of

accuracy is needed.

9.3.1 Types of Errors

Whenever bits flow from one point to another, there may be changes in the shape of the signal due to interference. This results in two types of errors: Single-bit errors and Burst errors.

In single-bit error, only 1 bit of a given data unit (such as a byte, character, or packet) is altered from 0 to 1 or from 1 to 0.

In burst errors, there will be changes in 2 or more bits in the data unit. Errors in data occur due to the addition of noise to them and when the duration of the noise signal is longer than the duration of a bit, burst errors occur. It is found that Burst errors are more likely to occur than single-bit errors.

Fig.9.4 shows single-bit and burst error occurrences.

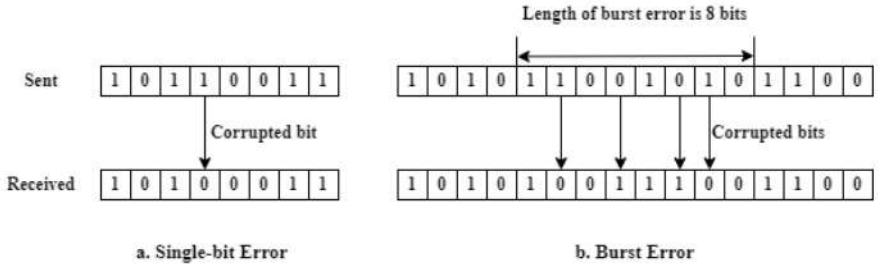

Fig.9.4: Single-bit Error and Burst Error

9.3.2 Error Detection

Error detection is achieved through Redundancy. Redundancy is the addition of extra bits to our data before sending and removing them when they are received. The redundant bits help the receiver detect and/or correct the corrupted bits. Redundancy can be achieved through various Coding schemes. Before we study these coding schemes let us understand the difference between error detection and correction by comparing them.

The process of error correction is more complex than its detection because it not only checks if bits are in error but also the number of bits in error and their location in the message.

9.3.3 Coding

In the context of networking, Coding refers to, performing some linear or complex algebraic operations on the user data to improve the network's efficiency, throughput, and scalability and reduce attacks and eavesdropping. It is also used to detect errors.

Coding is a process performed at the transmitting end. Here, redundant bits are added to the actual data to create a relationship between the new data and the actual data bits. To detect errors, the relationships between the two sets of bits are checked at the receiver.

The two important factors to be considered in the design of a coding scheme are:

- The ratio of redundant bits to data bits.

- The robustness of the process.

There are two broad categories of coding schemes: Block Coding and Convolution Coding. In the following sections, only Block Coding will be discussed.

9.3.3.1 Block Coding

In a block coding scheme, the message is first divided into k-bit blocks, called data words, and then r number of redundant bits are added to each block. This makes the length of the block n = k + r. The resulting n-bit blocks are called codewords. As n > k, the possible combinations of n are greater than k, and so the number of codewords is greater than data words.

This coding process is a one-to-one coding process where the same data word is encoded as a codeword. So $2^n - 2^k$ codewords are not used, and if these invalid words are received, the data words are thought to be corrupted during transmission.

Error Detection Using Block Coding:

If the following two conditions are met, a receiver can detect a change in the original codeword.

1. The receiver can find a list of valid codewords.
2. The original codeword has been modified to an invalid one.

The process of error detection is demonstrated in Fig. 9.5. At the transmitter, the generator process adds r extra bits to the k-bit data word to form n+k bits of codeword. At the receiver, the checker process extracts the data word and discards the extra bits.

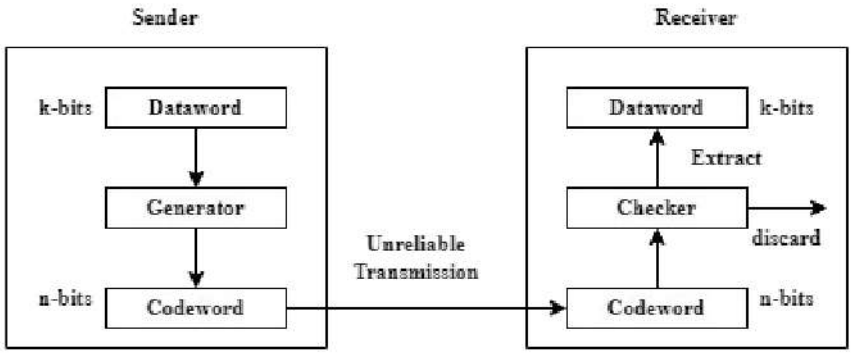

Fig. 9.5: Process of error-detection in block coding

NOTE: Any error detection code can detect only certain types of errors for which it is designed.

Hamming Distance: This is a concept used for error detection. This is the distance between two words (of the same size) and is given as the number of differences between corresponding bits. (total number of 1's).

Hamming Distance between the sent code word & received codeword is the number of bits that got corrupted during transmission. Let us understand it through examples.

Example 1: Find the Hamming distance between two words 000 and 011

Solution: The Hamming distance is found by the EX-OR operation between the given data words and counting the number of 1's in the result.

000 ⊕ 011 = 011. There are 2 numbers of 1's, so the Hamming distance is 2.

Example 2: Find the Hamming distance between two words 10101 and 11110
Solution: The Hamming distance is found by the EX-OR operation between the given data words and counting the number of 1's in the result.
10101 ⊕ 11110 = 01011. There are 3 numbers of 1's, so the Hamming distance is 3.

NOTE: If the Hamming Distance between two code words is not zero, then the code word has been corrupted during transmission.

Minimum Hamming Distance:
In a set of codewords, this is the smallest Hamming distance between all possible pairs of codewords. This distance is used to find the number of errors that are required to be detected.

If we assume that s errors may occur between the sent codeword and received codeword and these errors are to be detected, then the minimum Hamming distance between the valid codes is s +1, so that the received codeword does not match with the valid codeword.
For example, if the minimum distance for a coding scheme is 2, then we can detect only a single-bit error.

Types of Block Coding Schemes:
There are two types of Block Coding Schemes: Linear and Non-linear. As the theoretical analysis and implementation of non-linear schemes are difficult, only linear schemes are used today.

Parity Check Code:
A linear block code is a code in which the modulo-2 addition or exclusive OR () operation on two valid code words results in another valid codeword.
Parity Check Code is a very popular linear block coding scheme. Here, a k-bit data word is converted to an n-bit codeword, where n = k +1. The added extra bit is called the parity bit. If this bit makes the total number of 1's in the codeword even, then it is called even parity, else it is called odd parity.

Fig. 9.6 shows an Encoder and Decoder for a simple parity check code. The encoder at the transmitter uses the generator to calculate the parity bit r_0 using the modulo-2 addition or exclusive OR operation on the copy of the data bits (4 -bits) represented by (a_3, a_2, a_1, a_0) as shown below:
$r_0 = a_3 \oplus a_2 \oplus a_1 \oplus a_0$
If the number of 1s in the data is even, r_0 is 0 and if the number of 1s is odd, then r_0 is 1. So for even parity implementation, the parity bit appended is 0, else it is 0.
The sender sends the 5-bit codeword (a_3, a_2, a_1, a_0, r_0) on an unreliable medium and may get corrupted. The receiver receives a 5-bit word and uses the checker to generate the syndrome bit by doing the modulo-2 addition or exclusive OR operation on the copy of the codeword (b_3, b_2, b_1, b_0, q_0) as shown

below:

$s_0 = b_3 \oplus b_2 \oplus b_1 \oplus b_0 \oplus q_0$

The syndrome bit passes through the decision logic analyzer. If the syndrome bit is 0, there is no error in the received codeword and the data word is accepted. There is an error in the received codeword if the syndrome bit is 1, and the data word is then discarded.

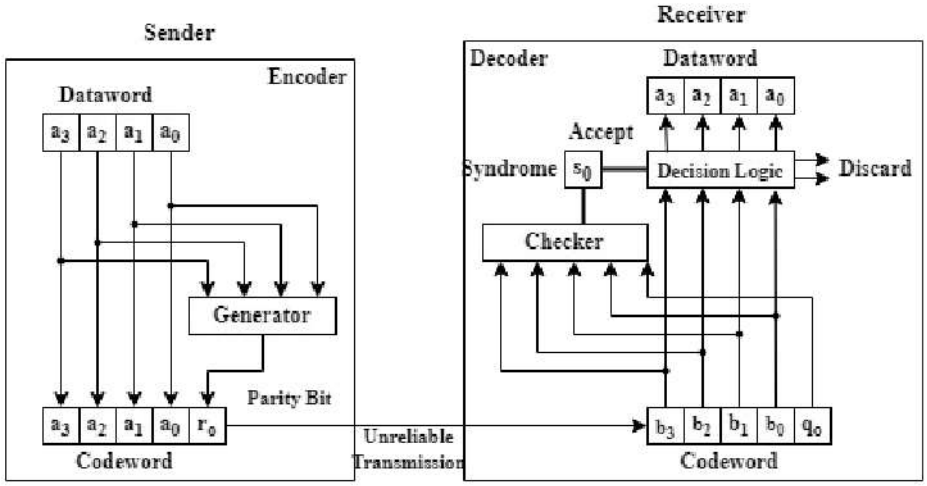

Fig. 9.6: Encoder and Decoder for simple parity-check code

NOTE: The minimum Hamming distance for this scheme is 2 and so the parity-check code can also detect a single-bit error.

9.3.3.2 Cyclic Codes

These are also linear block codes with a property that if a codeword is cyclically shifted (rotated), it results in another codeword.

If a 7-bit codeword is represented by, $a_6, a_5, a_4, a_3, a_2, a_1, a_0$, then we can shift the bits using $b_1=a_0, b_2=a_1, b_3=a_2, b_4=a_3, b_5=a_4, b_6=a_5, b_0=a_6$ to get the new codeword $b_6, b_5, b_4, b_3, b_2, b_1, b_0$.

For example, if 1011000 is a codeword and if it is cyclically left-shifted, then 0110001 is also a codeword.

Cyclic Redundancy Check (CRC):

Block coding techniques discussed in the previous section are useful for error detection only. But correcting errors after detection is also of prime importance for the error-free reception of data. Cyclic codes can be created to correct errors. In the following section, we will discuss only a subset of cyclic codes called the cyclic redundancy check (CRC), used in LANs and WANs.

Let us understand the concept with the help of Fig.9.7

In the encoder, the data word is of k-bits (4 bits) and the codeword is of n-bits (7 bits). Three bits of zeroes are appended to the data word and sent to the generator. The generator performs a modulo-2 division on the data word using a predefined divisor. The resulting quotient is discarded and the remainder is appended to the codeword and transmitted on an unreliable medium.

At the receiver, a copy of the codeword which is the replica of the generator is sent to the checker. It performs a modulo-2 division on the codeword copy with the same shared divisor. The quotient is discarded and the remainder is a syndrome that is passed to the decision logic analyzer. There is no error in the received codeword and the data word is accepted if the syndrome is 0, else there is an error and the data word is rejected.

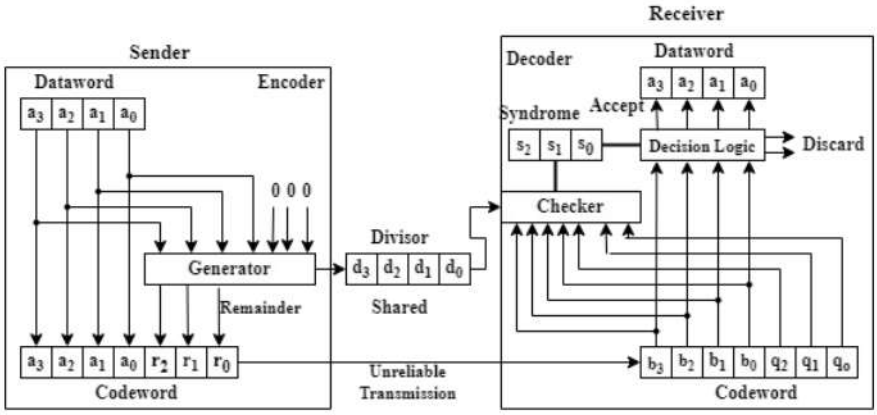

Fig. 9.7: CRC Encoder and Decoder

If the number of bits in the codeword is not provided and a generator polynomial is given, then the codeword length is calculated by using the steps demonstrated in the solution for Example 1.

Example 1: A data bit stream 100100 is to be transmitted using the standard CRC method. If the generator polynomial is x^3+x^2+1, find the actual encoded bit string transmitted. Also, if the fourth bit from the left is changed to 0 during transmission, show how the receiver detects this error.

Solution 1:

CRC Encoding at the transmitter:

In this example, the number of bits in the given data word 100100 is k = 6.

Here, the number of bits in the codeword will be calculated based on the given generator polynomial.

Step 1: The generator polynomial $G(X) = x^3+x^2+1$, so it consists of 4 bits and can be encoded in binary as , $1.\ x^3 + 1.\ x^2 + 0.\ x^1 + 1 = 1101 = m$

Step 2: The number of zeroes to be appended will be m-1 = 4-1 = 3.

So the code word will be of length, n = k + m = 6 + 3 = 9 and the augmented data word will be 100100**000**

Step 3: Perform the modulo-2 binary division of the augmented data word by the polynomial as shown in Fig. 9.8

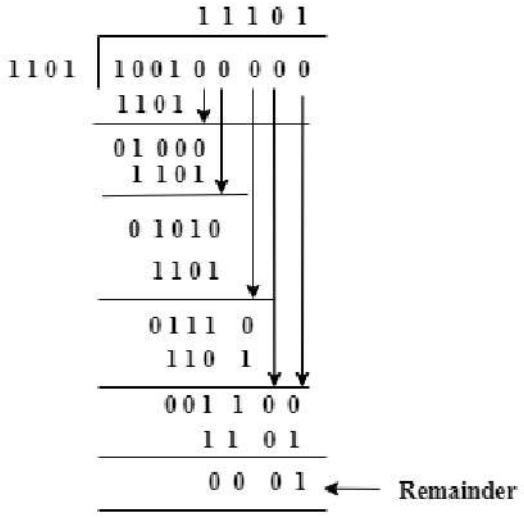

Fig: 9.8: Modulo-2 Binary Division at Encoder for Example 1

NOTE: In the modulo-2 division process, the subtraction operation is replaced by an EX-OR operation.

Step 4: The remainder which is the CRC is appended to the data word to form the codeword to be transmitted.

The encoded data word is obtained by replacing the last three bits of the augmented data word with the CRC, 100100 **001**

CRC Decoding at the receiver:

Step 1: The received bit stream is 100**0**0001

Step 2: Perform the modulo-2 binary division of the received data word by the same shared polynomial as shown in Fig.9.9

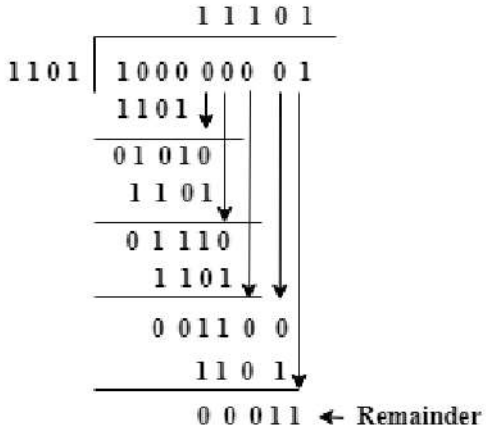

Fig: 9.9: Modulo-2 Binary Division at Decoder for Example 1

As the remainder is a non-zero value, the received code has a transmission error, which is detected by the receiver.

In case there is no transmission error, the decoding at the receiver will detect it with a remainder of zero as demonstrated in the division process as shown in Fig. 9.10

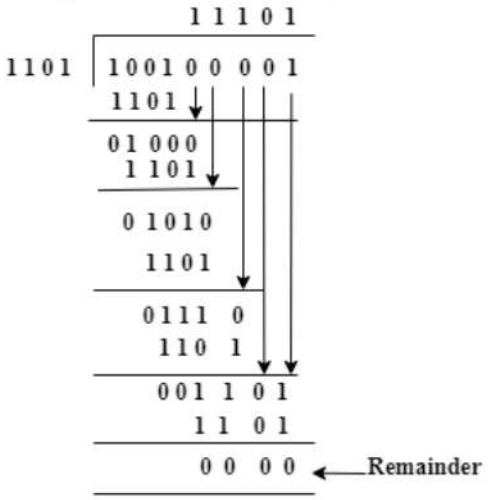

Fig. 9.10: Modulo-2 Binary Division at Decoder for Example 1

9.3.3.3 Checksum

The Checksum is an error detection technique that detects an error in a transmitted message of any length, by appending redundant bits to the message. It is used in the network and transport layer.

At the sender, the message is divided into m-bit blocks. The checksum generator generates an m-bit checksum and appends it to the transmitting message. At the receiver, the checker creates a new checksum on the whole message. If the new checksum is zero, then the message is accepted else it is discarded.

Example 2: Calculate the 8-bit checksum for the data given below.
10011001111000100010010010000100
Solution 2:
At the transmitter:
Step 1: The data is divided into 4, 8-bit blocks: 10011001 11100010 00100100 10000100
Step 2: These are added : 10011001 + 11100010 + 00100100 +10000100 = 1000100011
Step 3: As the result is 10 bits, the 2 most significant bits are wrapped around by adding them:
10 + 00100011= 00100101 (8-bits)
Step 4: The 1's complement of 00100101 which is 11011010 gives the checksum.
Step 5: The data along with the checksum is transmitted.

At the receiver:
Step 1: The data along with the checksum is divided into 8-bit blocks.
Step 2: All the blocks are added along with the checksum: 00100101 + 11011010 = 11111111
Step 3: The complement of the value obtained at step 2 = 00000000
As the result is zero, the receiver knows that there is no error and accepts the data.

9.4 Multiple Access Links and Protocols

Multiple Access Links are links shared by multiple nodes or stations. These are also called multipoint or broadcast links. Here when any of the nodes transmits a frame, all the other nodes receive a copy. Multiple access protocols help in coordinating the link access and allowing all the nodes to access the links fairly without data collision and loss. These protocols are implemented as a part of the MAC sublayer.

The three main objectives of multiple access protocols are:

- Minimization of collisions
- Avoidance of crosstalks
- Optimization of transmission time.

They are divided into three categories based on their implementation: Random access protocols, Controlled access protocols, and Channelization protocols.

Random access protocols:

This protocol assigns a uniform priority to all the connected nodes and any node can send data at any time on the transmission channel after checking the status of the link is idle. Also, there is no fixed time or fixed sequence given for data transmission.

Controlled access protocols:

As the name says, these protocols allow only one node to send data at any given time instance. Before beginning a transmission, the nodes consult each other to determine which station has the right to send. The nodes cannot send data until they are authorized by the other nodes. This avoids the collision of messages on the shared channel.
These are used in LANs.

Channelization protocols:

These protocols divide the available bandwidth of the transmission channel among the different nodes for parallel data transfer. These protocols are used in cellular telephony.

The sub-categories of the protocols are given in Fig. 9.11.

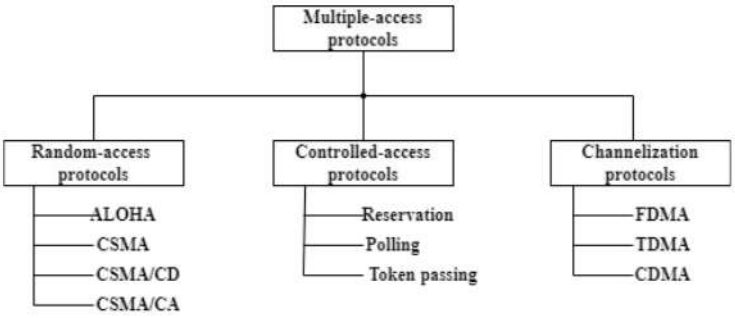

Fig. 9.11: Taxonomy of multiple-access protocols

Only the Random-access protocols are discussed in detail in the next section.

9.4.1 Random Access

Random access is also called contention, as there are no rules specifying the node to transmit next and all the nodes compete with one another to access the medium.

Here all the nodes have equal priority over the link access and no node is assigned control over another. At any time instance, a node willing to send data uses a protocol-defined procedure to decide whether to send the data or not depending on the state of the medium (idle or busy).

This access is called random access as all the nodes transmit randomly and there is no scheduled time for any station to transmit.

Random access methods are designed to solve the following issues,

1) The time when the station can access the medium.
2) The action a station should take if the link is busy.
3) Steps taken by a station to determine the success or failure of the transmission.
4) Steps taken by a station during an access conflict.

9.4.1.1 ALOHA

Pure ALOHA or ALOHA is the original ALOHA protocol. Initially, this protocol was used for ground-based radio broadcasting, but today it has been implemented in satellite communication systems.

The main idea on which this protocol is developed are:

1) A frame is sent by every node sends whenever it is ready with a frame.
2) As the link is shared, the frames sent from different nodes may collide.

Let us understand the concept with an example.

Example: There are 4 stations that are contending for access to the shared channel. Fig.9.12

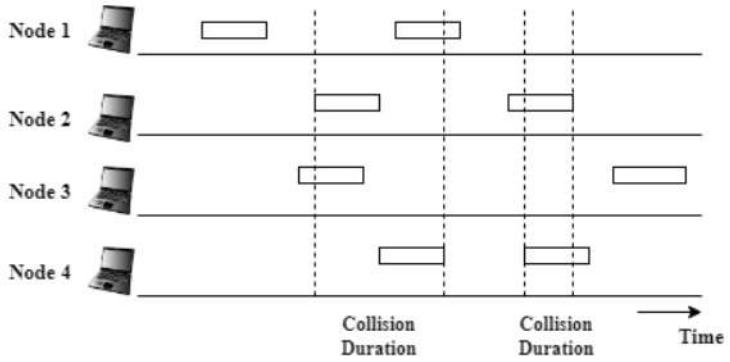

Fig. 9.12: Frames in a Pure ALOHA Network

Fig.9.12 shows the frames in a pure ALOHA network during a small time duration. Here,

- Each node sends two frames so there are 8 frames on the link.
- During contention for the shared channel, some of these frames collide. The first frame from node 1 and the second frame from node 3 survived the collision.
- Even if one bit of a frame coexists with one bit from another frame on the channel, there is a collision, and both frames will be destroyed and need to be resent.
- Pure ALOHA protocol relies on acknowledgment from the receiver and if the sending node does not receive back an acknowledgment within the time-out period, it assumes that frames have been destroyed and resends it.
- Whenever there is a collision involving two or more nodes, and all these stations resend frames, then there is collision again.
- To reduce the number of collisions, pure ALOHA dictates that each station resends the frames after the time-out period passes but waits for some random amount of time before doing it. This time is called Back-off time T_B.

Vulnerable Time:

This is the length of time when collision possibility exists. To understand this, let us assume that the nodes send fixed-sized frames. Let the frames take T_{fr} seconds to send. Fig. 9.13 shows the vulnerable time for node B.

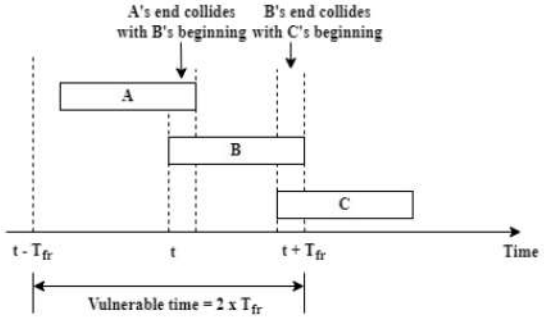

Fig. 9.13: Vulnerable time for pure ALOHA protocol

From Fig. 9.13, we observe that the vulnerable time for when the collision can occur is 2 times the frame transmission time T_{fr}.

The expression for finding the throughput S is given by, $S = G \times e^{-2G}$, where G is the average number

of frames generated during one frame transmission time.

Slotted ALOHA:

This version of the ALOHA protocol reduces the vulnerable time by dividing the time into slots of T_{fr} seconds. All the nodes are forced to send the frames only at the beginning of these slots and not later. If any node misses this time, it has to wait for the next slot. In Fig. 9.14, the time when it is more vulnerable for packets to collide for node B is shown and this is equal to the frame transmission time T_{fr}.

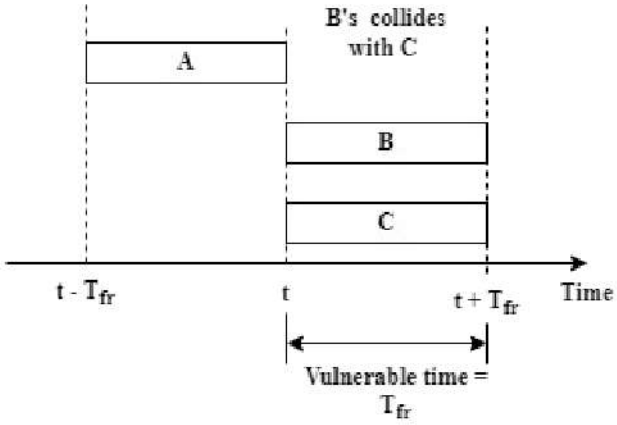

Fig. 9.14: Vulnerable time for slotted ALOHA protocol

The expression for finding the throughput S is given by, $S = G \times e^{-G}$, where G is the average number of frames generated during one frame transmission time.

9.4.1.2 Carrier-Sense Multiple Access (CSMA)

This protocol was developed to reduce the chances of collision and improve performance. Here every node senses the medium before transmitting. Due to propagation delay, a collision may occur even with this access method. When a frame is sent by a node, it takes time for the first bit to reach all the nodes, and one or more nodes can find the link idle and may transmit.

So the vulnerable time for this method has been found to be the propagation time T_{p}, which is the time required for a signal to propagate from one end of the link to another. Fig. 9.15 shows the vulnerable time for CSMA. If station A sends a frame at time t_1, it takes $t_1 + T_p$ to reach station D. In this case, if the first bit of the frame has not reached the end of the medium at points where B, C, and D, are connected, these stations can send frames and collision can occur.

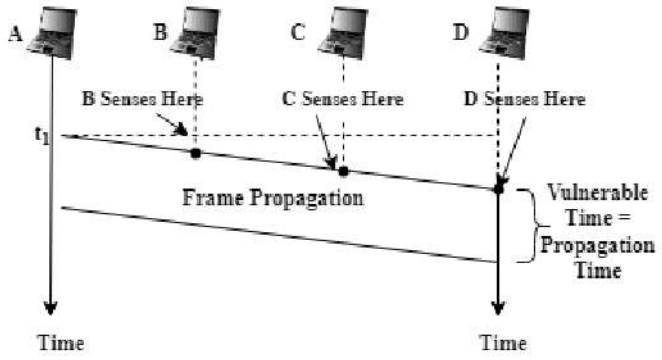

Fig. 9.15: Vulnerable Time for Carrier Sense Multiple Access

Persistence methods:

These are methods that the stations follow when the channel is busy. There are three persistent methods: I-Persistent, Nonpersistent, and p-Persistent.

1. I-persistent: Here the frames are sent by a station whenever it finds the line idle or sends the frames with a probability of 1 and the chances of collision are the highest in this method, as two or more stations send the frames simultaneously when the line is sensed idle.
2. Nonpersistent: Here, similar to the I-persistent method, frames are sent by a station whenever the line is idle but if the line is busy, the stations wait for a random amount of time before sending the frame. This way the chances of collision are reduced because all the stations wait for different random amounts of time. But the efficiency of the network reduces because the line can remain idle when stations are waiting to send.
3. p-Persistent: The time for sending frames is divided into time slots whose duration is greater than or equal to the maximum propagation time. The stations the following two steps after finding the line idle:
    1. The station sends the frames with probability p,
    2. The station waits for the start of the next time slot with a probability q = (1-p) and senses the line again.
        a. If the line is idle, it follows step 1, else it follows a backoff procedure as though the collision has occurred.

There are two versions of Carrier-Sense Multiple Access:

- Carrier-Sense Multiple Access with Collision Detection (CSMA/CD)
- Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)

In CSMA/CD, a node monitors the link using any one of the persistence methods after sending a frame. If no collision occurred, transmission is found to be successful, else a jamming signal is sent by the transmitting station to signal the other stations to not transmit their data immediately to avoid collision again. Then increment the retransmission counter. If the maximum number of transmission attempts is reached, abort the transmission, else calculate the random backoff time and wait for that time and start again from the main procedure.

Fig. 9.16 shows the flow diagram for the operation of CSMA/CD

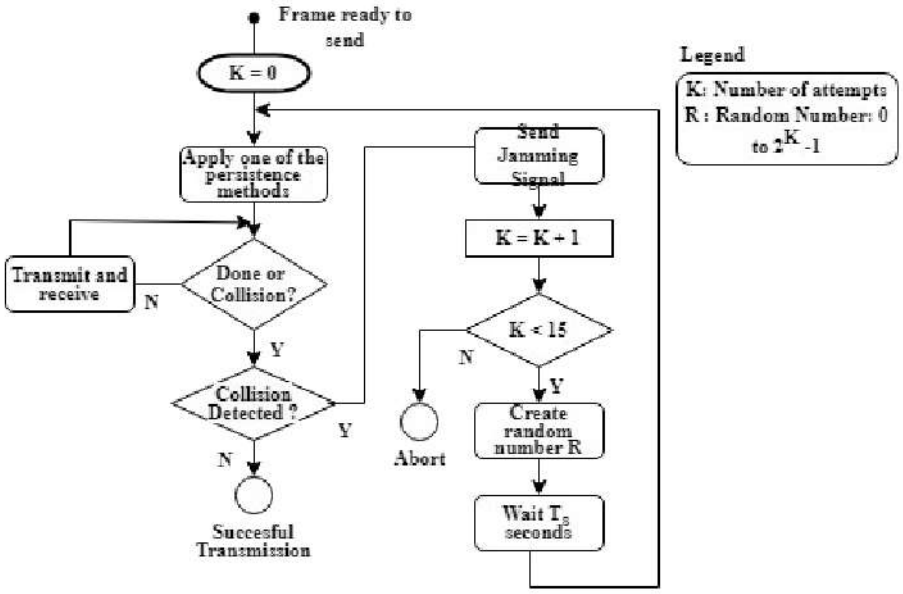

Fig. 9.16: Flow diagram for the CSMA/CD

In CSMA/CA, each station first senses the medium before transmitting a frame. If the medium is busy, the stations wait for a random amount of time and sense the medium again. A predefined backoff counter is used and is decremented until zero. If the channel becomes idle before the counter is reached zero, then the packet is transmitted, else the counter is reset to the predefined value and the process is repeated.

CSMA/CA waits for acknowledgments, so prevents collisions. The result is that no data is lost and it also avoids wasteful transmissions. This media access protocol is used for wireless transmissions.
There are three strategies used to avoid a collision:

- The interframe space (IFS)
- The contention window
- Acknowledgment

In IFS, nodes do not transmit immediately after sensing the link idle but wait for a period of time called IFS time to check if any node has already started transmission, and due to delay, the distance node's signal has not reached the other node. After this IFS time, the node can transmit.

In the contention window, a window of time is divided into slots, and nodes that are ready to transmit, choose a random number of slots to wait before transmitting. Also. the number of slots in the window varies according to the binary exponential backoff strategy. Here, if the link is not idle and the number of slots is one, then the slots get doubled if again the link is sensed idle. Also, the timer does not restart when for the first time a link is sensed idle, and this way priority is given to the node which has waited the longest.

The third protocol guarantees the reception of a frame through a positive acknowledgment from a receiver.

Fig. 9.17 shows the flow diagram for the operation of CSMA/CA with the IFS strategy used to avoid a collision.

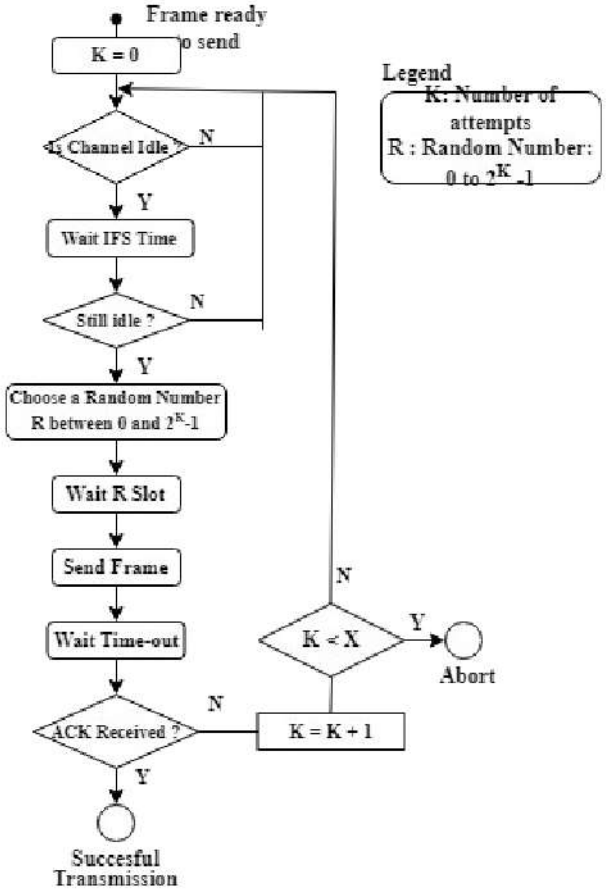

Fig. 9.17: Flow diagram for the IFS CSMA/CA

9.5 Switched Local Area Networks

Local Area Networks (LANs) are used to connect personal computers and workstations within a small area like a building or an office in order to exchange information or share resources such as printers, servers, etc. Examples are Home wifi networks and small business networks. Sometimes LANs can be large covering many buildings or a city. This classifies them into Wide Area Networks (WANs) and Metropolitan Area Networks (MANs).

LAN switching is a technology used to reduce the problem of network bandwidth when the number of users increases. Though switched LANs are scalable and users have better bandwidth performance, the cost of LAN setting is high.

Examples: Wired LAN - Ethernet, Hub, and Switch

Wireless LAN – Wifi.

9.5.1 Local Area Network

It uses a broadcast channel that is shared among many hosts. Any frame sent to a broadcast address reaches all the hosts in a LAN. LANs in the earlier days used bus topology, where all the frames were broadcast on the shared bus, and the hosts ignored the frames if not needed. But today LANs use a star topology, where the frames use the MAC address to send the frames to a specific device or host. There are six LAN technologies: Ethernet, 100Base-T, FDDI, token ring, ATM and 100VG-AnyLAN

Fig. 9.18 shows how a link layer switch carries frames between hosts and a router using MAC or physical address.

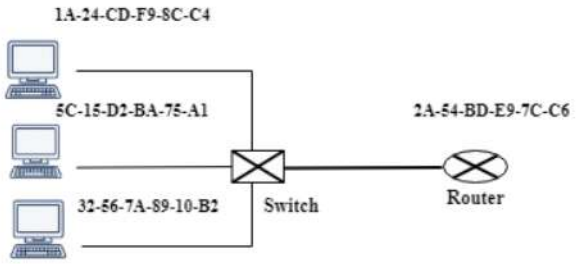

Fig. 9.18: Each Interface Connected to a LAN has a unique MAC address

MAC addresses are used to carry frames from one physical interface to another physically connected interface on the same network. These are 48 bits long or 12-digit Hexadecimal numbers. These are burned into the network adapter Read Only Memory (ROM). If the frame is to be broadcast, then the address used is FF-FF-FF-FF-FF-FF in 12-digit Hexadecimal format.
These addresses are unique globally and so they are portable. The Ethernet adapter or card can be moved from one LAN to another.

9.5.1.1 Address Resolution Protocol (ARP)

This is a request-response protocol and works between layers 2 and 3 of the OSI and Internet model. ARP is used by a host or a router to find the physical address of another host or router in a LAN.

All hosts in a network are identified by an IP address, which is a network layer logical address that changes over time and also from one network to another. But it is unique within a network. It is used by a router to route a packet from its source to its destination passing through different networks. This address is only used to locate a host in a network but to send data, a physical or MAC address is needed. All the devices in the network hold an ARP cache memory with a mapping of the MAC address to the IP address of all the machines in the LAN.

Whenever a new host is added to a network, its physical address is not known to the router or other hosts to which it is connected. When an incoming packet to this new host arrives at the router or other hosts, they use an ARP broadcast request to find out its physical or MAC address by providing its IP address (along with its own MAC and IP addresses). So all the machines match the IP address from the request packet, and the device with a match responds to the request and sends its MAC address to the

requested machine and the other devices drop the packet. The ARP cache in the requested and the responded router or host in the LAN gets updated. When the MAC address is received, the source host sends the packet to the destination host.

Reverse ARP or RARP is another protocol whose objective is also to complete the IP address to MAC address mapping, but using MAC address to find the IP address. Used by thin clients with limited resources. Fig. 9.19 demonstrates the functions of ARP and RARP.

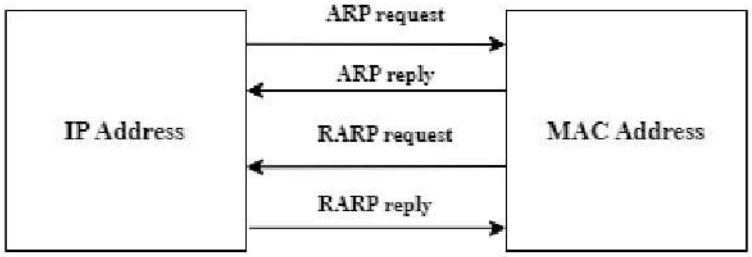

Fig. 9.19: ARP and RARP protocols

9.5.2 Ethernet

This is the most popular technology used for wired LAN, WAN, and MANs. It uses the IEEE 802.3 standard set of protocols for communication. Since its commercialization in 1983, it has been developed to provide higher bit rates, more nodes, and long-distance links. They are simpler and cheaper than Fiber distributed data interface (FDDI) and token ring. Provides data rates up to 10 Gbps. The physical topology used was Bus, but today Ethernet networks use star topology with Hub or Switch used to connect the nodes. Fig. 9.20 shows an Ethernet LAN with three nodes.

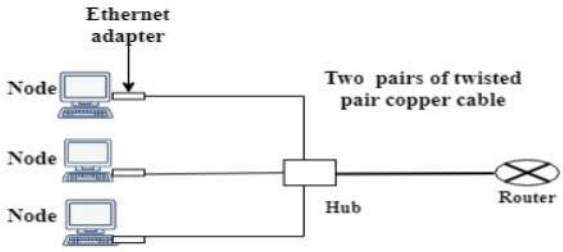

Fig. 9.20: Ethernet LAN

9.5.2.1 Ethernet Frame Format

The Ethernet frame carries the data over the Ethernet network. It helps in the successful transmission of data packets. Here the network layer IP packet is encapsulated at the transmitter and decapsulated at the receiver.

The Ethernet frame contains three fields: a header consisting of source and destination MAC addresses, the actual data, and a frame check sequence (FCS).

Fig. 9.21 shows the Ethernet frame format. The Ethernet frame size can vary from 64 bytes to a maximum of 1518 bytes.

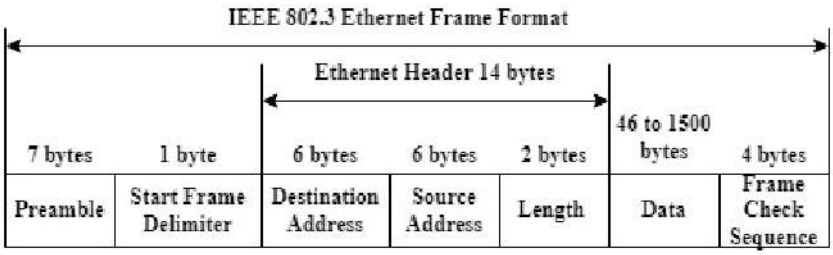

Fig. 9.21: Basic Ethernet Frame Format

- The Preamble field of 7 bytes of alternative 1's and 0's followed by one byte of 10101011 is used to synchronize the clock rates at the sender and receiver.
- The Start Frame Delimiter of 1 byte is used to indicate the start of the frame from the next byte in the frame.
- The Source and Destination (physical or MAC) address fields are 6 bytes each, identifying the sending and receiving systems.
- A Length field of 2 bytes specifies the network layer protocols used, either IPv4 or IPv6.
- Data contains the payload data and padding bytes if the data length is less than 46 bytes.
- The Frame Check Sequence consists of 4 bytes of 32-bit Cyclic Redundancy Check (CRC) code for error detection/correction.

Some of the features of today's Ethernet networks are:

- Fast Ethernet uses 10BaseT and 100BaseT physical media standards with 10 Mbps and 100Mbps data rates respectively with twisted pair cable as the medium.
- They use a star topology
- Maximum distance between node and hub is 100 meters.
- Hub is used to connect nodes. These serve as bit-level repeaters with no frame buffering
- Gigabit ethernet use point-to-point and shared links
- Media access protocol used is CSMA/CD only for shared links
- Transmission mode is full duplex at 10 Gbps for point-to-point links

9.6 Wireless LAN and IEEE 802.11

Wireless LANs are Local Area Networks using high-frequency radio waves for connecting devices. It is the last link in a network for the user giving mobility to them inside a building or a campus. The wireless link is connected to a wired cable-based backbone network.

Fig.9.22 shows a common wireless LAN topology.

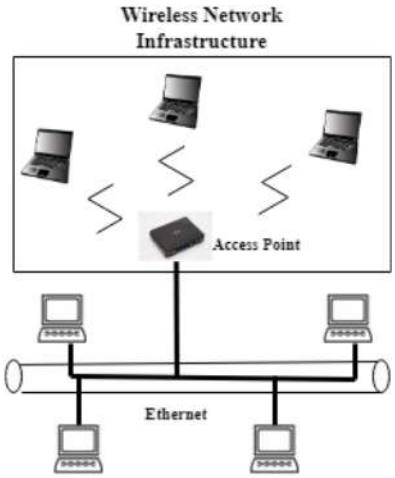

Fig. 9.22: Wireless LAN Topology

In the figure, the wireless LAN connects to a wired LAN through an access point, which bridges the traffic between the two LANs. It acts as a repeater increasing the possible distance between the nodes. The Wireless Network Infrastructure is also called the basic service set (BSS) where there are three wireless nodes and the central base station or access point. The access point can be connected to a switch or a router which can be connected to the Internet.

Scenarios, where wireless networks are used, are given below.
In a home network or small office network, wireless LANs link together laptop computers, smartphones, printers, smart TVs, and gaming devices with a wireless router.
Hotspots are provided by routers at hotels, restaurants, libraries, coffee shops, and airports. Consumers can use their portable wireless devices and access the internet through these hotspots.

Benefits of Wireless LANs:

- Provide Mobility and Flexibility
- Used where wired infrastructure is not available
- Low cost of deployment
- High scalability

Wireless LAN Technologies:
Almost all of the wireless LANs are based on the standard IEEE 802.11, also known as Wireless Fidelity (Wifi), which gives the architecture and specifications for these LANs covering both physical and data link layers. There are several standards of IEEE 802.11 WLANs specifying different data rates and modulation techniques suitable for different applications. The important standards used are 802.11, 802.11a, 802.11b, 802.11g, 802.11n, and 802.11p. All the above standards use carrier-sense multiple access with collision avoidance (CSMA/CA) link access. All these standards support both centralized base station-based (Fig. 9.22) and ad hoc networks (Fig. 9.23).

Fig. 9.23: An IEEE 802.11 ad hoc network

An ad hoc network is formed when mobile devices are brought in proximity to each other for communication and there is no network infrastructure found in that location.

9.7 Self-Assessment Questions

Q1. List and briefly describe the services provided by the data link layer. (10 marks, L2)
Q2. What are the different types of errors? (6 marks, L2)
Q3. How are error detection mechanisms implemented at the data link layer? (8 marks, L4)
Q4. What are the different coding schemes used for error detection? Describe them (8 marks, L3)
Q5. What is Hamming distance? What is the Hamming distance between 10101110 and 11001110? (4 marks, L3)
Q6. Describe Cyclic Redundancy Check. (6 marks, L3)
Q7. Explain any one Random Access Protocol (8 marks, L3)
Q8. Compare ALOHA with CSMA (4 marks, L4)
Q9. Explain the working of the Address Resolution Protocol. (8 marks, L3)
Q10. Explain the Ethernet Frame Format (6 marks, L3)
Q11. List the benefits of Wireless LANs.(4 marks, L2)

9.8 Multiple-Choice Questions

Q1. The services provided by the link layer is/are, [1 mark, L1]
   A. Framing
   B. Link Access
   C. Error detection
   D. All the above

Q2. The protocol used for random link access is/are, [1 mark, L1]
   A. ALOHA
   B. Polling
   C. Reservation
   D. CDMA

Q3. Data Link layer data is _____ [1 mark, L1]

A. Bits

B. Frames

C. Datagram

D. Messages

Q4. The Hamming distance between 1011 and 1001 is, [1 mark, L1]

A. 1

B. 2

C. 3

D. None of the above

Q5. Link Layer is responsible for, [1 mark, L1]

A. End-to-end delivery of data

B. Node-to-node delivery of data

C. Both A and B

D. Either A or B

Q6. Error detection and correction provides, [1 mark, L1]

A. Reliability

B. Security

C. Flow control

D. Routing

Q7. The protocol used for error detection and correction is, [1 mark, L1]

A. Slotted ALOHA

B. CSMA

C. CRC

D. None of the above

Q8. Random access is also called, [1 mark, L1]

A. Polling

B. Reservation

C. Contention

D. None of the above

Q9. Devices used at the link layer are.

A. Repeaters

B. Bridges

C. Routers

D. None of the above

Q10. The address fields in the Ethernet frame format are of size ___ bytes,

A. 4

B. 5

C. 6

D. None of the above

9.9 Keys to Multiple-Choice Questions

Q1. Provides all the services of Framing, Link Access, and Error detection (D)
Q2. ALOHA (A)
Q3. Frames (B)
Q4. 1011 ⊕ 1001 = 1 (A)
Q5. Node-to-node delivery (B)
Q6. Reliability (A)
Q7. For error detection and correction, Cyclic Redundancy Check is used (C)
Q8. Contention – as all the nodes contend for link access. (C)
Q9. Bridges (B)
Q10. MAC address is 6 bytes. (C)

9.10 Summary of The Unit

This unit covers four important topics: Services provided by the data link layer, error detection, multiple access protocols, and switched local area networks. The first section of this unit discussed the important services of the link layer such as Framing, Link Access, Reliable Delivery, and Error Detection. Also in the second and third sections, a brief description of the popular services such as Link Access and Error Detection is studied. The services at the link layer are implemented in two layers DLC and MAC sublayer. In order to provide services, many protocols are developed at these two sub-layers. The prominent ones at the MAC sublayer, ALOHA, and CSMA are studied. Today all businesses, corporates, homes, and public places rely on computer networks for their operations, LANs play an important role, so Ethernet architecture and Wireless LAN architectures are studied in the last section.

9.11 Recommended Learning Resources

[1] James F Kurose and Keith W Ross, Computer Networking, A Top-Down Approach, Sixth Edition, Pearson,2017.

[2] Behrouz A Forouzan, Data and Communications and Networking, Fifth Edition, McGraw Hill, Indian Edition

9.12 References

[1] https://data-flair.training/blogs/data-link-layer-of-osi-model/

[2] https://www.javatpoint.com/data-link-layer

[3] https://www.tutorialspoint.com/data_communication_computer_network/data_link_layer_introduction.htm#

[4] https://www.techtarget.com/searchnetworking/definition/Data-Link-layer#:~:text=The%20data%20link%20layer%20is%20Layer%202%20in%20the%20Open.the%20same%20LAN%20or%20WAN.

[5] https://www.pearsonitcertification.com/articles/article.aspx?p=438038&seqNum=4

[6] https://www.tutorialspoint.com/multiple-access-protocols-in-computer-networks#:~:text=Multiple%20access%20protocols%20can%20be,access%20protocols%20and%20channelization%20protocols.
[7] https://ecomputernotes.com/computernetworkingnotes/communication-networks/what-is-aloha
[8] https://www.youtube.com/watch?v=HNefQ1J4eFk
[9] https://cs460.byu.edu/static/lectures/winter-2015/switched-local-area-networks.pdf
[10] https://ipwithease.com/arp-vs-rarp/
[11] https://slideplayer.com/slide/12428171/