UNIT II : DATA-LINK LAYER & MEDIA ACCESS

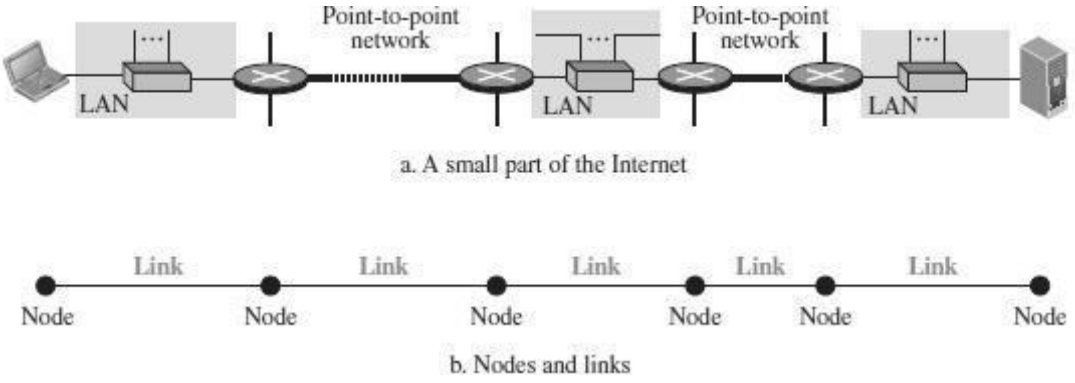
•Introduction • Transmission Media • Data Link Layer • Error, Detection and Correction methods (Parity, LRC, CRC, Hamming Code) • Ethernet Frame(format) •Random Access Protocol

1. INTRODUCTION

- In the OSI model, the data link layer is the 2nd layer from the bottom.
- It is responsible for **transmitting frames from one node to next node**.
- The main responsibility of the Data Link Layer is to transfer the datagram across an individual link.
- An important characteristic of a Data Link Layer is that datagram can be handled by different link layer protocols on different links in a path.
- The other responsibilities of this layer are
    - **Framing -** Divides the stream of bits received into data units called frames.
    - **Physical addressing** – If frames are to be distributed to different systems on the same network, data link layer adds a header to the frame to define the sender and receiver.
    - **Flow control**- If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender ,the Data link layer imposes a flow control mechanism.
    - **Error control**- Used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.
    - **Medium Access control** - Used to determine which device has control over the link at any given time.

Nodes and Links

- Communication at the data-link layer is node-to-node.
- The communication channel that connects the adjacent nodes is known as links, and in order to move the datagram from source to the destination, the datagram must be moved across an individual link.
- A data unit from one point in the Internet needs to pass through many networks (LAN and WAN) to reach another point.
- Theses LANs and WANs are connected by routers.
- The two end hosts and the routers are ***nodes*** and the networks in- between are ***links*.**



- The first node is the source host; the last node is the destination host.
- The other four nodes are four routers.
- The first, the third, and the fifth links represent the three LANs; the second and the fourth links represent the two WANs.

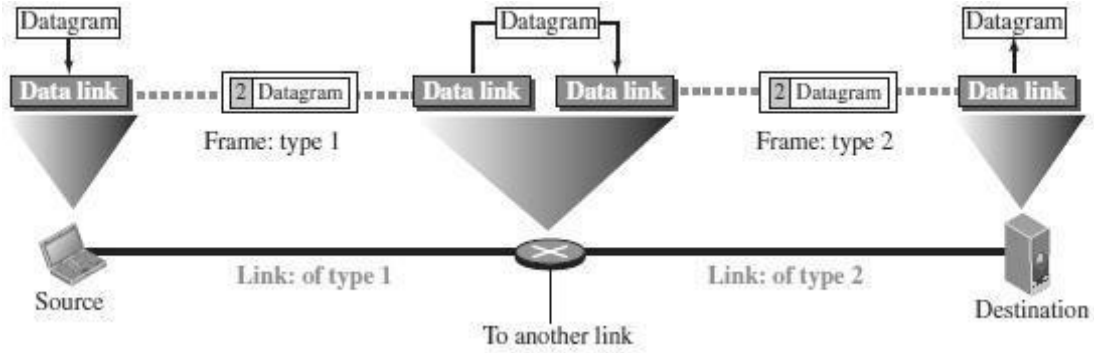
Two Categories of Links

Point-to-Point link and Broadcast link.

- In a point-to-point link, the link is dedicated to the two devices
- In a broadcast link, the link is shared between several pairs of devices.

Data Link Layer Services

- The data-link layer is located between the physical and the network layers.
- The data link layer provides services to the network layer; it receives services from the physical layer.
- When a packet is travelling, the data-link layer of a node (host or router) is responsible for delivering a datagram to the next node in the path.
- For this purpose, the data-link layer of the sending node needs to encapsulate the datagram and the data-link layer of the receiving node needs to decapsulate the datagram.



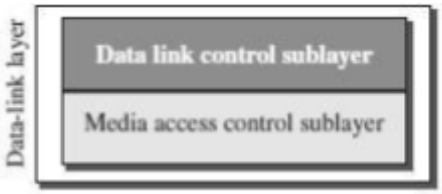
- The datagram received by the data-link layer of the source host is

encapsulated in a frame.

- The frame is logically transported from the source host to the router.
- The frame is decapsulated at the data-link layer of the router and encapsulated at another frame.
- The new frame is logically transported from the router to the destination host.

Sublayers in the Data Link layer

- We can divide the data-link layer into two sublayers: **data link control (DLC)** and **media access control (MAC).**
- The data link control sublayer deals with all issues common to both point-to-point and broadcast links
- The media access control sublayer deals only with issues specific to broadcast links.



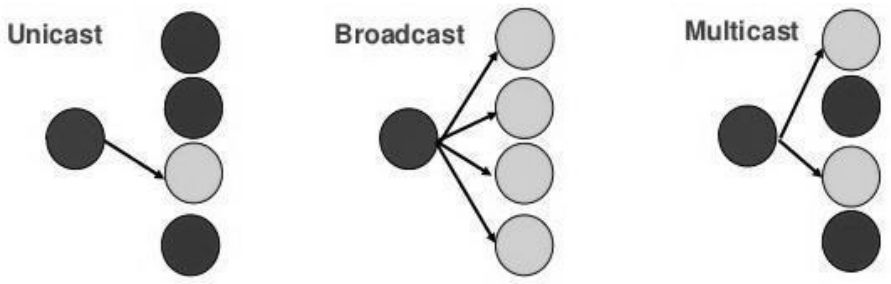
---

2. LINK-LAYER ADDRESSING

- A link-layer address is sometimes called a link address, sometimes a physical address, and sometimes a MAC address.
- Since a link is controlled at the data-link layer, the addresses need to belong to the data-link layer.
- When a datagram passes from the network layer to the data-link layer, the datagram will be encapsulated in a frame and two data-link addresses are added to the frame header.
- These two addresses are changed every time the frame moves from one link to another.

THREE TYPES OF ADDRESSES

The link-layer protocols define three types of addresses: unicast, multicast, and broadcast.



Unicast Address :

Each host or each interface of a router is assigned a unicast address. Unicasting means one-to-one communication. A frame with a unicast address destination is destined only for one entity in the link.

Multicast Address :

Link-layer protocols define multicast addresses. Multicasting means one-to-many Communication but not all.

Broadcast Address :

Link-layer protocols define a broadcast address. Broadcasting means one-to-all communication. A frame with a destination broadcast address is sent to all entities in the link.

MAC Addressing

MAC (Media Access Control) Addressing is a unique identifier assigned to network interfaces for communication on the data link layer of the OSI model. It is used for identifying devices in local networks and ensuring proper communication between them.

Key Concepts:

1. **MAC Address Format**:
   - A MAC address is a 48-bit (6-byte) address represented in hexadecimal format.
   - Typically written as: `XX:XX:XX:XX:XX:XX`, where `XX` represents hexadecimal digits (0-9, A-F).
   - Example: `00:1A:2B:3C:4D:5E`.
2. **MAC Address Components**:
   - The first 3 bytes (24 bits) represent the **Organizationally Unique Identifier (OUI)**, which is assigned by the IEEE to a manufacturer. This identifies the device's maker.
   - The last 3 bytes (24 bits) are assigned by the manufacturer and serve as a unique identifier for the device.
3. **Types of MAC Addresses**:
   - **Unicast**: A unique MAC address assigned to a single device. It's used for one-to-one communication.
   - **Broadcast**: A special MAC address `FF:FF:FF:FF:FF:FF`, used to send data to all devices in the network.
   - **Multicast**: A MAC address used to send data to a specific group of devices. Multicast MAC addresses fall within the range `01:00:5E`.
4. **Static vs Dynamic MAC Addresses**:
   - **Static**: The MAC address is burned into the hardware and cannot be changed (e.g., NICs in computers).
   - **Dynamic**: Some systems (e.g., virtual machines) can dynamically assign or change MAC addresses for specific purposes.

Role of MAC Addresses:

- **Identification**: Every device on a network has a unique MAC address that helps in identifying it, making it crucial for local network communication.
- **Data Link Layer Communication**: In Ethernet and other data link protocols, devices use MAC addresses to send and receive frames within the same network or subnet.
- **Address Resolution Protocol (ARP)**: ARP is used to map an IP address to its corresponding MAC address in local networks.

Functions of MAC Addressing:

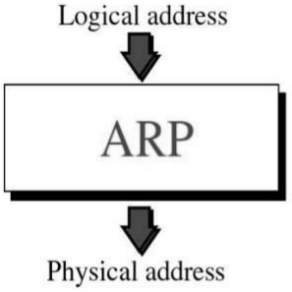
1. **Local Communication**: MAC addresses help devices communicate within a local area network (LAN) or between devices on the same subnet.
2. **Frame Delivery**: In Ethernet networks, data frames are sent with the destination MAC address, ensuring they reach the correct device.
3. **Network Security**: MAC filtering is used in Wi-Fi networks for security, allowing only devices with specified MAC addresses to connect.

MAC Address Table (Ethernet Switches):

- **Ethernet Switches** maintain a MAC address table (or forwarding table) to map MAC addresses to the respective ports. This helps in efficiently forwarding data frames to the correct device on the network.

ADDRESS RESOLUTION PROTOCOL (ARP)

- ARP stands for Address Resolution Protocol.
- ARP is the most important protocol in the data link layer.
- ARP is a network layer protocol used to **convert an IP address (Network/Logical address) into a MAC Address (Hardware /Physical address).**



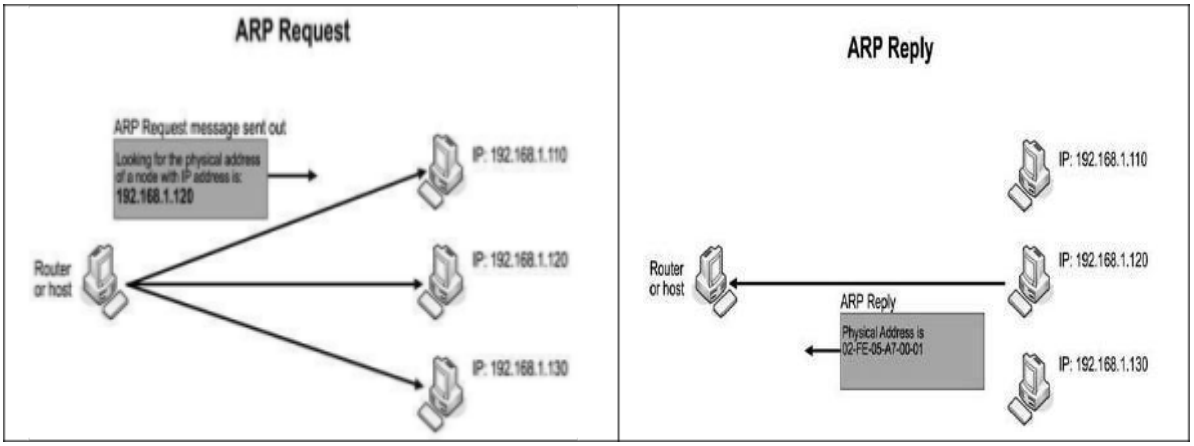
- The computer programs/applications use logical address (IP address) to send/receive messages, however the actual communication happens over the physical address (MAC address).
- To send a datagram over a network, we need both the logical and physical address.
- IP addresses are made up of 32 bits whereas MAC addresses are made up of 48 bits.
- ARP enables each host to build a table of IP addresses and corresponding physical addresses.
- ARP relies on broadcast support from physical networks.
- The Address Resolution Protocol is a request and response protocol.
- The types of ARP messages are:

1. ARP request
2. ARP reply

ARP Operation

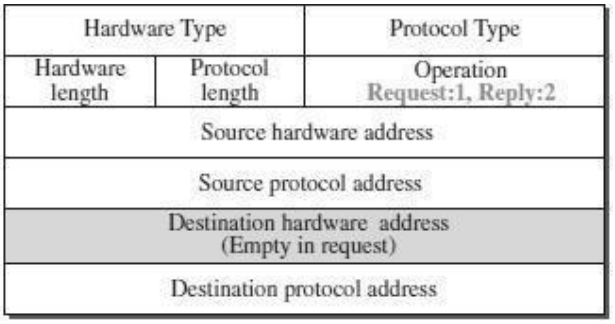
- ARP maintains a cache table in which MAC addresses are mapped to IP addresses.
- If a host wants to send an IP datagram to a host, it first checks for a mapping in the cache table.
- If no mapping is found, the Address Resolution Protocol needs to be invoked over the network.
- It does this by broadcasting an ARP query onto the network.
- This query contains the target IP address.
- Each host receives the query and checks to see if it matches its IP address.
- If it does match, the host sends a response message that contains its link-layer address (MAC Address) back to the originator of the query.
- The originator adds the information contained in this response to its ARP table.
- For example,

  To determine system B's physical (MAC) address, system A broadcasts an ARP request containing B's IP address to all machines on its network.



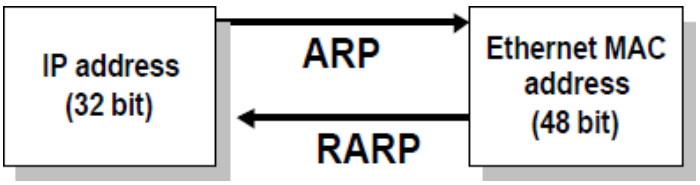
- All nodes except the destination discard the packet but update their ARP table.
- The destination host (System B)constructs an ARP Response packet
- ARP Response is unicast and sent back to the source host (System A).
- Source stores target Logical & Physical address pairs in its ARP table from ARP Response.
- If the target node does not exist on the same network, an ARP request is sent to the default router.

ARP Packet



RARP – Reverse ARP

- Reverse Address Resolution Protocol (RARP) allows a host to convert its MAC address to the corresponding IP address.



Transmission Media refers to the physical materials or means used to transfer data signals between devices on a network. Transmission media serve as the pathway for data to travel in the form of electrical, optical, or radio signals, making them essential to network communication.

Types of Transmission Media

Transmission media are generally classified into two categories: **guided (wired)** and **unguided (wireless)** media.

1. Guided Media (Wired)

Guided media use physical cables to direct the transmission of signals between devices. The three main types of guided media are:

- **Twisted Pair Cable**
  - **Description**: Comprises pairs of insulated copper wires twisted together. The twists reduce electromagnetic interference from other pairs and external sources.
  - **Types**:
    - *Unshielded Twisted Pair (UTP)*: Commonly used in Ethernet networks.
    - *Shielded Twisted Pair (STP)*: Adds a shielding layer to reduce interference, used in environments with high interference.
  - **Applications**: Telephony, Ethernet LANs, DSL.
  - **Pros and Cons**: Twisted pairs are cost-effective but have limited bandwidth and are more susceptible to interference than fiber optics.
- **Coaxial Cable**
  - **Description**: Has a central conductor surrounded by insulation, a metal shield, and

an outer cover, making it resistant to interference.
    - **Applications**: Cable TV, older Ethernet networks (10Base2, 10Base5).
    - **Pros and Cons**: Coaxial cables offer good resistance to interference and moderate bandwidth but are bulkier and more expensive than twisted pair.
- **Fiber Optic Cable**
    - **Description**: Uses light signals to transmit data through a core made of glass or plastic fibers, with an outer cladding to reflect the light.
    - **Types**:
        - *Single-mode*: Thin core, allows only one light mode; used for long distances.
        - *Multi-mode*: Thicker core, multiple light modes; used for shorter distances.
    - **Applications**: High-speed data transmission over long distances, backbone network infrastructure, and high-speed internet connections.
    - **Pros and Cons**: Fiber optic cables provide high bandwidth and immunity to electromagnetic interference but are more expensive and fragile compared to copper cables.

2. Unguided Media (Wireless)

Unguided media transmit data wirelessly through electromagnetic waves. This type of media does not require a physical pathway, making it ideal for mobility and flexible communication. Key types include:

- **Radio Waves**
    - **Range**: Can cover a few meters to several kilometers, depending on power and frequency.
    - **Applications**: Wi-Fi, Bluetooth, mobile networks, and AM/FM radio.
    - **Pros and Cons**: Radio waves enable wireless communication over large areas and can penetrate buildings, but they are susceptible to interference from other devices and weather conditions.
- **Microwave Transmission**
    - **Range**: Line-of-sight transmission, typically up to 50 kilometers between towers.
    - **Applications**: Cellular networks, satellite communication, point-to-point connections.
    - **Pros and Cons**: Microwaves can handle high bandwidth but require line-of-sight and are affected by environmental factors such as rain (rain fade).
- **Infrared (IR)**
    - **Range**: Typically limited to a few meters.
    - **Applications**: Remote controls, short-range communication like IrDA (Infrared Data Association).
    - **Pros and Cons**: Infrared is used for low-speed, short-range applications and requires line-of-sight. It's susceptible to interference from sunlight or other IR sources.
- **Satellite Communication**
    - **Description**: Satellites in orbit relay signals between ground stations, covering large geographic areas.
    - **Applications**: Global communication, television broadcasting, GPS, internet for remote locations.
    - **Pros and Cons**: Satellite provides coverage to remote areas and is useful for global

broadcasting but has high latency and is costly to deploy and maintain.

Role of Transmission Media in the Data Link Layer

The Data Link layer is responsible for error detection, data framing, and ensuring the reliable transmission of frames between nodes on the same network. Transmission media directly affect the **performance, bandwidth, and reliability** of data transmission, impacting the overall efficiency and quality of communication. The Data Link layer works closely with the Physical layer to optimize data transmission over these media by handling errors, framing, and managing access to shared media through protocols like Ethernet.

Factors to consider for designing transmission media:

1. **Bandwidth**: Ensure the media supports required data transmission speeds.
2. **Distance & Attenuation**: Choose media that maintains signal strength over the necessary distance.
3. **Interference & Noise**: Use shielded or fiber optics in high-interference environments.
4. **Cost**: Balance performance needs with budget constraints.
5. **Security**: Fiber optics offer better security; wireless and unshielded media may be more vulnerable.
6. **Installation & Maintenance**: Consider ease of installation and required maintenance effort.
7. **Environmental Conditions**: Choose media durable for environmental factors like moisture or temperature.
8. **Scalability**: Select media that can support future growth and higher data needs.
9. **Latency**: Opt for low-latency media if real-time data transfer is essential.
10. **Data Rate**: Ensure the media supports the necessary data rate and throughput for applications.

---

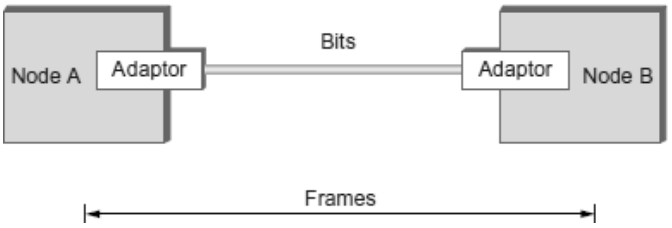
3. DLC SERVICES

- The data link control (DLC) deals with procedures for communication between two adjacent nodes—node-to-node communication—no matter whether the link is dedicated or broadcast.
- Data link control service include

(1) Framing (2) Flow Control (3) Error Control

1. FRAMING

- The data-link layer packs the bits of a message into frames, so that each frame is distinguishable from another.



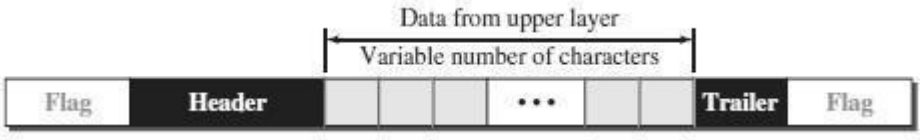
- Although the whole message could be packed in one frame, that is not normally done.
- One reason is that a frame can be very large, making flow and error control very inefficient.
- When a message is carried in one very large frame, even a single-bit error would require the retransmission of the whole frame.
- When a message is divided into smaller frames, a single-bit error affects only that small frame.
- Framing in the data-link layer separates a message from one source to a destination by adding a sender address and a destination address.
- The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

Frame Size

- Frames can be of fixed or variable size.
- Frames of fixed size are called cells. In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter.
- In variable-size framing, we need a way to define the end of one frame and the beginning of the next. Two approaches were used for this purpose: a character-oriented approach and a bit-oriented approach.

Character-Oriented Framing

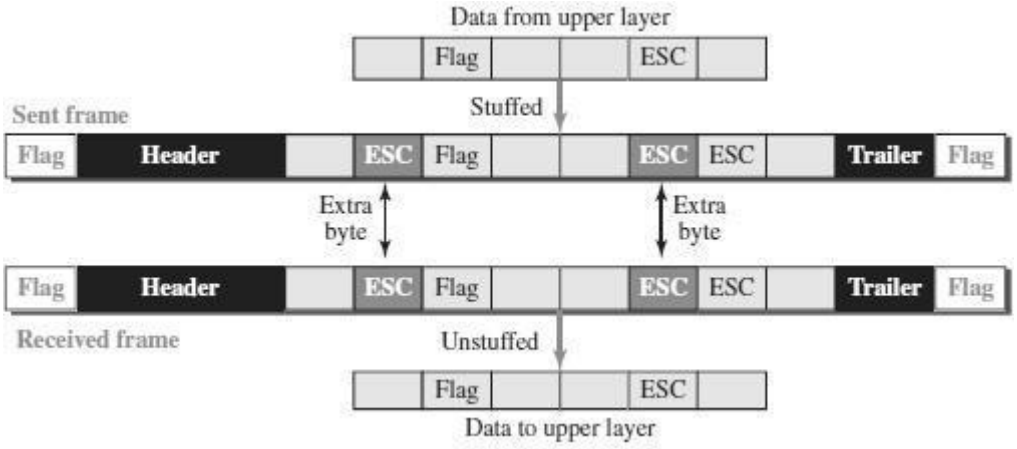
- In character-oriented (or byte-oriented) framing, data to be carried are 8-bit characters.
- To separate one frame from the next, an 8-bit (1-byte) flag is added at the beginning and the end of a frame.
- The flag, composed of protocol-dependent special characters, signals the start or end of a frame.



- Any character used for the flag could also be part of the information.
- If this happens, when it encounters this pattern in the middle of the data, the receiver thinks it has reached the end of the frame.
- To fix this problem, a **byte-stuffing** strategy was added to character-oriented framing.

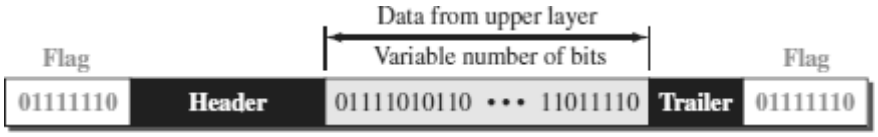
Byte Stuffing (or) Character Stuffing

- **Byte stuffing is the process of adding one extra byte whenever there is a flag or escape character in the text.**
- In byte stuffing, a special byte is added to the data section of the frame when there is a character with the same pattern as the flag.
- The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC) and has a predefined bit pattern.
- Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not as a delimiting flag.



Bit-Oriented Framing

- In bit-oriented framing, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on.
- In addition to headers and trailers), we still need a delimiter to separate one frame from the other.
- Most protocols use a special 8-bit pattern flag, 01111110, as the delimiter to define the beginning and the end of the frame

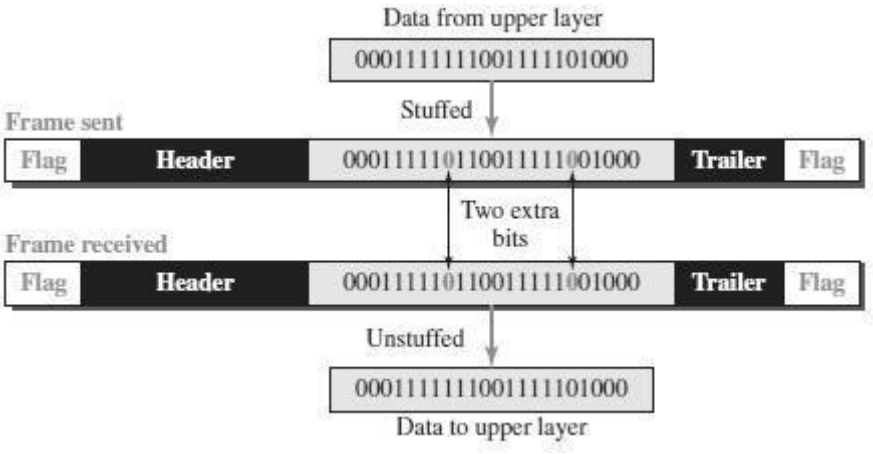


- If the flag pattern appears in the data, the receiver must be informed that this is not the end of the frame.
- This is done by stuffing 1 single bit (instead of 1 byte) to prevent the pattern from looking like a flag. The strategy is called **bit stuffing.**

Bit Stuffing

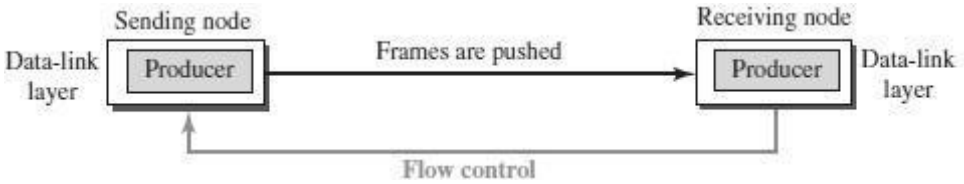
- **Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow a 0 in the data so that the receiver does not mistake the pattern 0111110 for a flag.**
- In bit stuffing, if a 0 and five consecutive 1 bits are encountered, an extra 0 is added.

- The receiver eventually removes this extra stuffed bit from the data.
- The extra bit is added after one 0 followed by five 1's regardless of the value of the next bit.
- This guarantees that the flag field sequence does not inadvertently appear in the frame.



2. FLOW CONTROL

- **Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.**
- The receiving device has limited speed and limited memory to store the data.
- Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.
- It requires a buffer, a block of memory for storing the information until they are processed.



Two methods have been developed to control the flow of data:(Discussed earlier syllabus)

- Stop-and-Wait
- Sliding Window

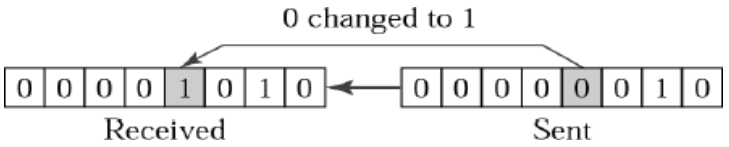
3. ERROR CONTROL

Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected. Error Control is a technique of error detection and retransmission.

TYPES OF ERRORS

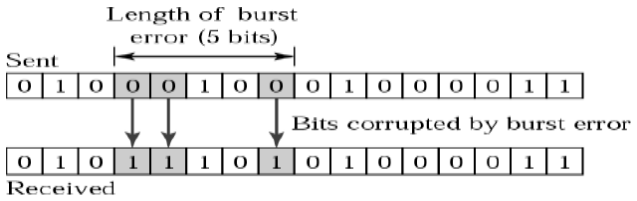
SINGLE-BIT ERROR

The term Single-bit error means that only one bit of a given data unit (such as byte, character, data unit or packet) is changed from 1 to 0 or from 0 to 1.



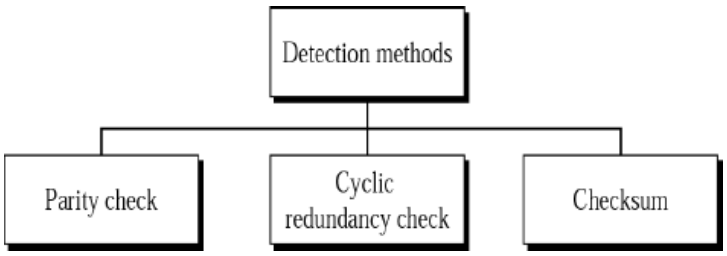
BURST ERROR

The term Burst Error means that two or more bits in the data unit have changed from 1 to 0 or from 0 to 1.



ERROR DETECTION TECHNIQUES / METHODS

The basic idea behind any error detection scheme is to add additional information to a frame that can be used to determine if errors have been introduced.



PARITY CHECK

- One bit, called the parity bit is added to every data unit so that the total number of 1's in the data unit becomes even (or) odd.
- The source then transmits this data via a link, and bits are checked and

verified at the destination.

- Data is considered accurate if the number of bits (even or odd) matches the number transmitted from the source.
- This technique is the most common and least complex method.

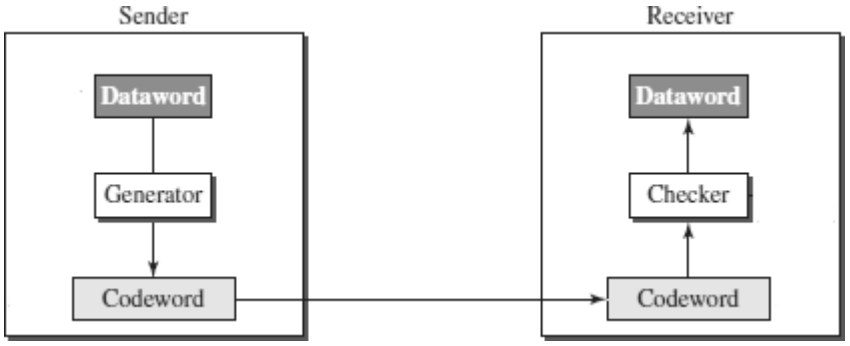
1. ***Even parity*** – Maintain even number of 1s E.g., 1011 → 1011 **1**
2. ***Odd parity*** – Maintain odd number of 1s E.g., 1011 → 1011 **0**

CYCLIC REDUNDANCY CHECK

- Cyclic codes refer to encoding messages by adding a fixed-length check value.
- CRCs are popular because they are simple to implement, easy to analyze mathematically, and particularly good at detecting common errors caused in transmission channels.

Steps Involved:

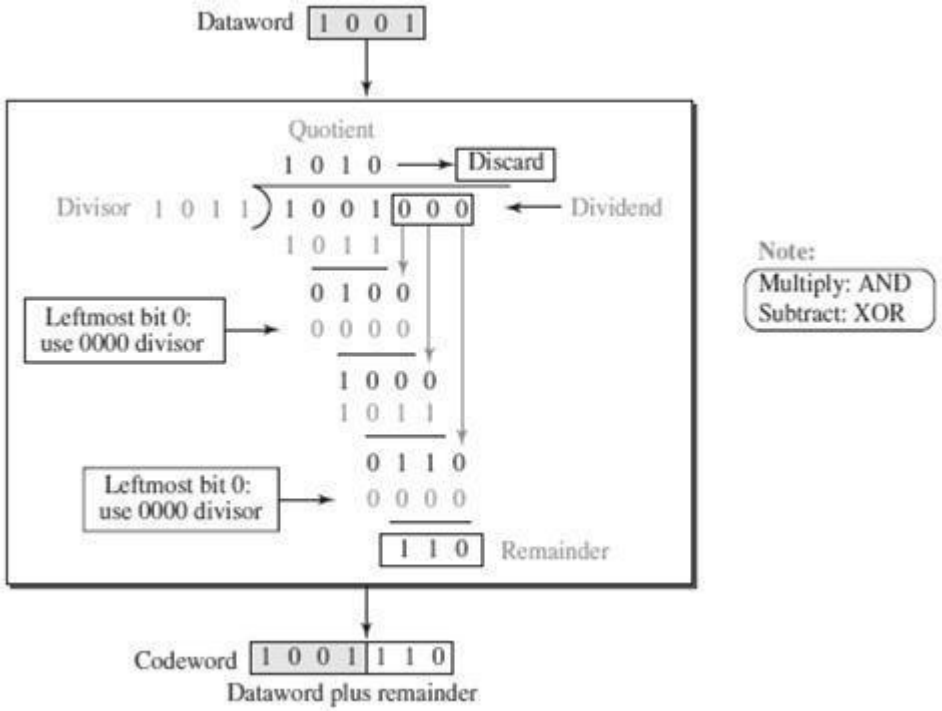
- Consider the original message (data word) as M(x) consisting of 'k' bits and the divisor as C(x) consists of 'n+1' bits.
- The original message M(x) is appended by 'n' bits of zero's. Let us call this zero-extended message as T(x).
- Divide T(x) by C(x) and find the remainder.
- The division operation is performed using XOR operation.
- The resultant remainder is appended to the original message M(x) as CRC and sent by the sender (code word).



Example 1:

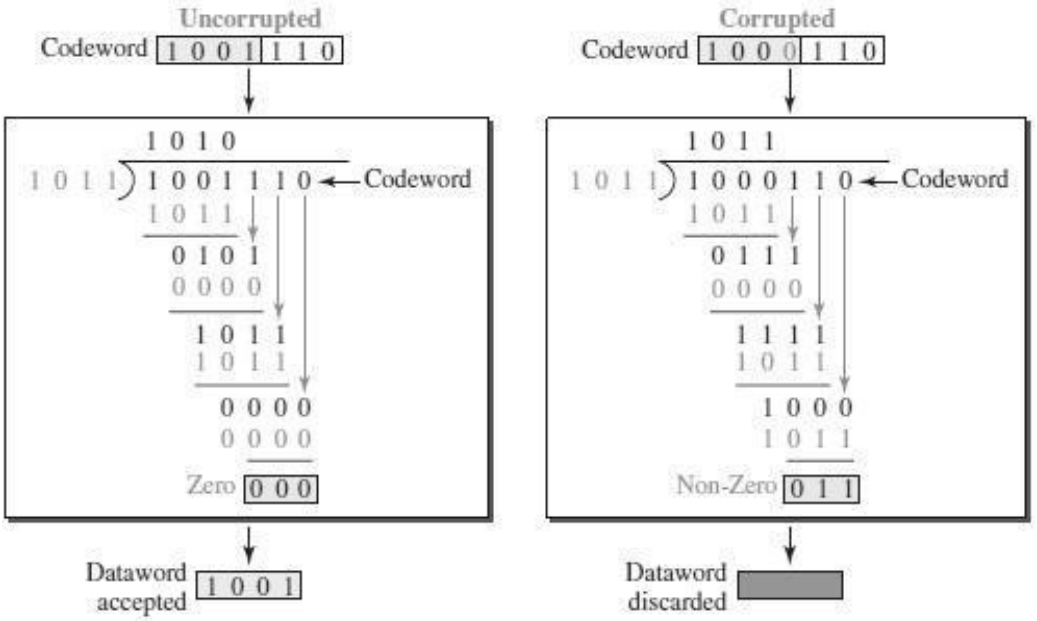
- Consider the Data word / Message M(x) = 1001
- Divisor C(x) = 1011 (n+1=4)
- Appending 'n' zeros to the original Message M(x).
- The resultant messages are called T(x) = 1001 **000.** (here n=3)
- Divide T(x) by the divisor C(x) using the XOR operation.

Sender Side:



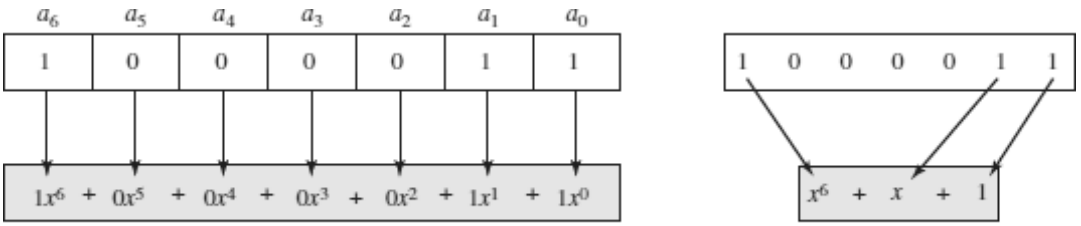
Receiver Side:

(For Both Cases – Without Error and with Error)



Polynomials

- A pattern of 0s and 1s can be represented as a **polynomial** with coefficients of 0 and 1.
- The power of each term shows the position of the bit; the coefficient shows the value of the bit.



Hamming Code - Detailed Explanation

Hamming Code is an error-correcting code used to detect and correct single-bit errors in data. It is widely used in digital communication systems to enhance data integrity.

Key Concepts

- **Parity Bits:** Hamming code uses multiple parity bits that allow not only detection but also correction of single-bit errors.
- **Positions of Parity Bits:** Parity bits are placed in positions that are powers of 2 (i.e., positions 1, 2, 4, 8, etc.).
- **Data Bits and Parity Bits:** The parity bits are determined based on specific data bits and their positions.

Step-by-Step Guide for Calculating Hamming Code

1. **Determine the Number of Parity Bits (r):**
   To find the required number of parity bits, use the formula:

   $2^r \geq m+r+1$

   where m is the number of data bits and r is the number of parity bits. This formula ensures that enough parity bits are available to cover all data bits and enable error correction.
2. **Positioning Parity Bits:**
   Parity bits are placed at positions that are powers of 2 (1, 2, 4, 8, etc.). These positions will be reserved for parity bits, while other positions will hold the data bits.
3. **Determine Each Parity Bit's Value:**
   Each parity bit is responsible for a set of specific bit positions in the combined data + parity bit sequence. The value of each parity bit (0 or 1) is calculated to ensure that the bits it checks have even (or odd) parity, depending on the system.
   In Hamming Code:

   - **Parity bit p1:** Checks positions 1, 3, 5, 7, 9, etc.
   - **Parity bit p2:** Checks positions 2, 3, 6, 7, 10, etc.

- **Parity bit p3:** Checks positions 4, 5, 6, 7, 12, etc.
- Continue this pattern for additional parity bits as necessary.

4. **Construct the Hamming Code Sequence:**
   After calculating each parity bit, combine the data and parity bits to get the final code sequence.
5. **Error Detection and Correction:**
   When a Hamming Code sequence is received, the parity bits are re-evaluated. If there's no error, all parity checks will pass. If there is a single-bit error, the failing parity bits will indicate the position of the error, allowing it to be corrected.

Example: Generating Hamming Code for 4-Bit Data with Even Parity

Let's encode the data 1011 using Hamming Code with even parity.

Step 1: Determine the Number of Parity Bits

For 4 data bits, let's calculate r using:

$2^r \geq m+r+1$

For $m= 4$

$2^3 \geq 4+3+1$

So, 3 parity bits are required.

Step 2: Arrange Data and Parity Bits

We'll place the data and parity bits in the following positions:

Position	1 (p1)	2 (p2)	3	4 (p4)	5	6	7
Bits	p1	p2	1	p4	0	1	1

Step 3: Calculate Parity Bits

Using **even parity** (ensuring that each group has an even number of 1's):

1. **Parity bit p1:** Covers positions 1, 3, 5, and 7.
   - Bits: 1,1,0,1 → Total 1's = 3 (odd).
   - To make it even, set p1=1.
2. **Parity bit p2:** Covers positions 2, 3, 6, and 7.
   - Bits: 0,1,1,1 → Total 1's = 3 (odd).
   - To make it even, set p2=1.
3. **Parity bit p4:** Covers positions 4, 5, 6, and 7.
   - Bits: 0,0,1,11 → Total 1's = 2 (even).
   - p4 remains 0.

Step 4: Complete Hamming Code

Now we have all the bits to construct the final Hamming code:

Position	1 (p1)	2 (p2)	3	4 (p4)	5	6	7
Bits	1	1	1	0	0	1	1

So, the encoded data with parity is `1110011`.

Error Detection and Correction Example

Assume the received code is `1110111`.

1. Recalculate each parity bit:
   - **Parity bit** p_1: Checks 1, 3, 5, 7 → $1, 1, 0, 1$: Total 1's = 3 (odd). Parity check fails.
   - **Parity bit** p_2: Checks 2, 3, 6, 7 → $1, 1, 1, 1$: Total 1's = 4 (even). Parity check passes.
   - **Parity bit** p_4: Checks 4, 5, 6, 7 → $0, 0, 1, 1$: Total 1's = 2 (even). Parity check passes.
2. **Identify Error Position:** Only p_1 failed, indicating an error at position 1.
3. **Correct the Error:** Flip bit at position 1 from `1` to `0`.

Corrected code: `0110011`.

Practice Question

Encode the data 1101 using Hamming Code with even parity.

Hamming Distance is a measure of the difference between two binary strings of equal length. It is calculated by counting the number of bit positions in which the two strings differ. In error detection and correction, the Hamming Distance helps determine the minimum number of bit changes required to transform one code into another.

Key Points:

- **Error Detection**: Hamming Distance of 2 can detect single-bit errors.
- **Error Correction**: Hamming Distance of 3 or more is required to correct single-bit errors.
- **Applications**: Used in coding theory for reliable data transmission, including Hamming Code.

For example, the Hamming Distance between 1101 and 1001 is 1 (only the second bit differs).

Hamming Distance is the number of bit positions in which two binary strings differ.

Example:

Find the Hamming Distance between `1011101` and `1001001`.

`1011101`

`1001001`

1. Align the bits:
2. Compare each bit:
    - Bits 3 and 5 differ.
3. **Result**: The Hamming Distance is **2**.

Longitudinal Redundancy Check (LRC)

Longitudinal Redundancy Check (LRC) is a simple error-detection method where data is arranged in a matrix format (with rows and columns), and a parity bit is calculated for each column. An extra row (parity row) is added to the matrix, containing parity bits for each column, creating a **checksum** that can help detect errors.

Steps to Solve LRC

1. **Arrange Data in Rows**: Divide the data into a matrix format where each row contains one data unit (typically a byte, but it can vary).
2. **Calculate Column Parity**: For each column, count the number of 1's in that column across all rows. For even parity, the parity bit is set to 1 if the count of 1's is odd, making the total count even. For odd parity, the parity bit is set to 1 if the count of 1's is even, making it odd.
3. **Construct Parity Row**: Place the calculated parity bit for each column in an extra row (parity row) beneath the data rows. This parity row represents the LRC checksum.
4. **Transmit Data with Parity Row**: The data matrix along with the parity row is transmitted. During transmission or storage, if any error occurs, the parity row can help detect errors by checking the parity of each column.

Solved Example

Let's take an example where we have three 8-bit data units (bytes) and we want to calculate the LRC

using even parity.

Data Bytes:
Byte 1: 11001100
Byte 2: 10101010
Byte 3: 11110000

Step 1: Arrange Data in Matrix Form

Arrange each byte in a column-wise matrix format

Byte Position	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7	Bit 8
Byte 1	1	1	0	0	1	1	0	0
Byte 2	1	0	1	0	1	0	1	0
Byte 3	1	1	1	1	0	0	0	0

Step 2: Calculate Column Parity for Even Parity

Let's go through each column and calculate the parity bit for even parity:

Bit Position	1	2	3	4	5	6	7	8
Column 1	3 ones (odd) → parity 1							
Column 2	2 ones (even) → parity 0							
Column 3	2 ones (even) → parity 0							
Column 4	2 ones (even) → parity 0							
Column 5	2 ones (even) → parity 0							
Column 6	1 one (odd) → parity 1							
Column 7	1 one (odd) → parity 1							
Column 8	0 ones (even) → parity 0							

Parity Row (Checksum Row)

Based on the calculated parity bits for each column, we get the parity row (LRC):

Parity Row: 11000010

Step 3: Construct the Final Matrix with Parity Row

Now, combine the data bytes with the calculated parity row:

Now, combine the data bytes with the calculated parity row:

Byte Position	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7	Bit 8
Byte 1	1	1	0	0	1	1	0	0
Byte 2	1	0	1	0	1	0	1	0
Byte 3	1	1	1	1	0	0	0	0
Parity Row	1	1	0	0	0	0	1	0

Step 4: Transmit Data

The final data with LRC is transmitted as follows:

Data Bytes: 11001100, 10101010, 11110000

LRC (Parity Row): 11000010

Note: If the data is received with a single-bit error, the parity row can help detect the error. If any of the column parities don't match upon recalculating, this indicates a column error. LRC can detect single-bit and some multi-bit errors but may not correct them.

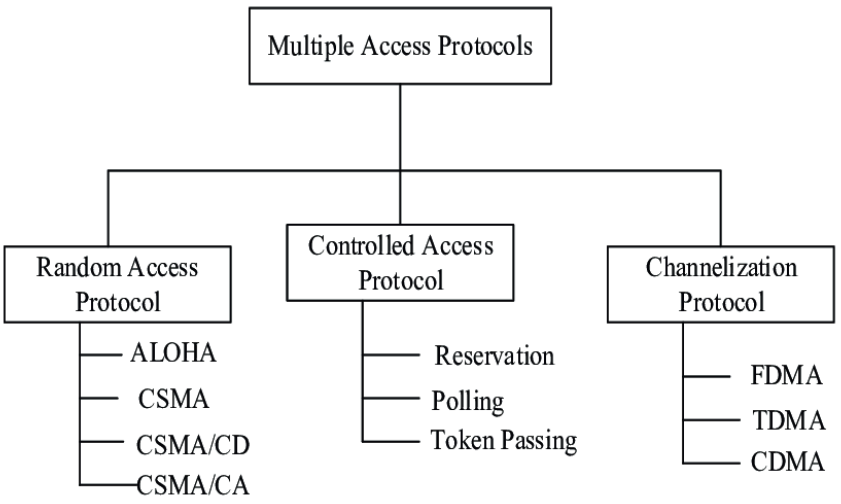
ERROR CONTROL

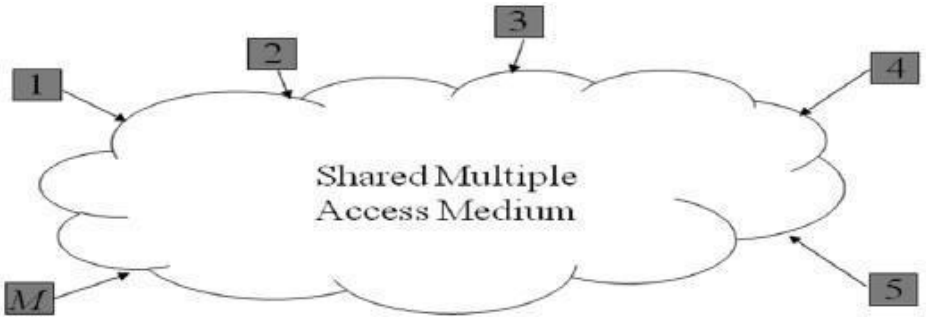
- Error control includes both error detection and error correction.
- Whenever an error is detected, specified frames are retransmitted
- It allows the receiver to inform the sender if a frame is lost or damaged during transmission and coordinates the retransmission of those frames by the sender.
- Includes the following actions:
    - **Error detection**
    - Positive Acknowledgement (**ACK**): if the frame arrived with no errors
    - Negative Acknowledgement (**NAK**): if the frame arrived with errors
    - Retransmissions after **Timeou**t: Frame is retransmitted after certain amount of time if no acknowledgement was received
- Error control in the data link layer is based on automatic repeat request (ARQ).

---

7. MEDIA ACCESS CONTROL (MAC)

- When two or more nodes transmit data at the same time, their frames will collide and the link bandwidth is wasted during collision.
- To coordinate the access of multiple sending/receiving nodes to the shared link, we need a protocol to coordinate the transmission.
- These protocols are called Medium or Multiple Access Control (MAC) Protocols. MAC belongs to the data link layer of OSI model
- MAC defines rules for orderly access to the shared medium. It tries to ensure that no two nodes are interfering with each other's transmissions, and deals with the situation when they do.



- 

Issues involved in MAC

The key issues involved are –

- ***Where*** the control is exercised - refers to whether the control is exercised in a centralized or distributed manner
- ***How*** the control is exercised - refers to in what manner the control is exercised

Goals of MAC

1. Fairness in sharing
2. Efficient sharing of bandwidth
3. Need to avoid packet collisions at the receiver due to interference

MAC Management

- Medium allocation (collision avoidance)
- Contention resolution (collision handling)

MAC Types

- **Round-Robin :** – Each station is given opportunity to transmit in turns. Either a central controller polls a station to permit to go, or stations can coordinate among themselves.
- **Reservation : -** Station wishing to transmit makes reservations for time slots in advance. (Centralized or distributed).

- **Contention (Random Access)** : - No control on who tries; If collision‖ occurs, retransmission takes place.

MECHANISMS USED

- Wired Networks :
    - CSMA / CD – Carrier Sense Multiple Access / Collision Detection
- Wireless Networks :
    - CSMA / CA – Carrier Sense Multiple Access / Collision Avoidance

1. RANDOM ACCESS PROTOCOL:

Aloha Protocols

Aloha is a protocol for managing random access in shared communication channels. There are two main versions of Aloha:

- **Pure Aloha**
- **Slotted Aloha**

The protocol is simple, allowing stations to transmit data at any time, but collisions may occur if two or more stations transmit simultaneously. To handle these collisions, Aloha uses retransmission strategies. Below is a deeper look at the two versions, including vulnerable time and efficiency.

1. Pure Aloha

Transmission Process:

- **Data Transmission:** Stations can transmit their data at any time.
- **Acknowledgment (ACK):** After sending a data packet, the transmitting station waits for an acknowledgment (ACK) from the receiver.
    - **If ACK is received:** The transmission is considered successful.
    - **If no ACK is received:** The transmission is considered unsuccessful. The station then backs off for a random time before retransmitting the data. This process repeats until the transmission succeeds or the backoff limit is reached.

Vulnerable Time in Pure Aloha:

- **Vulnerable Time:** The time during which a collision can occur if another station starts transmitting.
    - For Pure Aloha, the **vulnerable time** is $2 \times Tt$, where Tt is the time required to

send a data packet.
    - This is because, for a successful transmission, the other station must not transmit during the time the packet is being sent and for a short period afterward (due to propagation delay).
    - **Collision Scenario:**
        - If another station transmits a packet that overlaps with the first one during transmission or just before/after, a collision occurs.

Efficiency Formula:

The efficiency of Pure Aloha is given by:

$$\eta = G \times e^{-2G}$$

Where:

- G is the average number of stations trying to transmit at any given time.

Maximum Efficiency:

- To find the maximum efficiency, we calculate the point where the derivative of the efficiency formula η with respect to G is zero:

$$\frac{d\eta}{dG} = 0$$

- The maximum efficiency occurs at $G = \frac{1}{2}$.
- Substituting $G = \frac{1}{2}$ into the formula:

$$\eta = \frac{1}{2} \times e^{-2\times\frac{1}{2}} = \frac{1}{2e} = 0.184$$

Maximum Efficiency of Pure Aloha = 18.4%.

This low efficiency is due to frequent collisions, as the stations transmit at any time without synchronization.

2. Slotted Aloha

Transmission Process:

- **Time Slots:** In Slotted Aloha, time is divided into equal-sized slots. Stations must wait for the beginning of the next time slot to start transmission.
- **Transmission Starts at Slot Boundaries:** If a station misses the beginning of a time slot,

it must wait until the next time slot.

- **Collision Handling:** If two stations transmit during the same time slot, a collision occurs, and both stations must retry transmission.

Vulnerable Time in Slotted Aloha:

- **Vulnerable Time:** In Slotted Aloha, the vulnerable time is reduced to Tt , which is the time required to send one data packet.
    - Since stations are synchronized to time slots, the only possible collision can occur if two stations choose the same time slot to transmit.
    - If no overlap occurs between time slots, there will be no collision.

Efficiency Formula:

The efficiency of Slotted Aloha is given by:

$$\eta = G \times e^{-G}$$

Where:

- G is the average number of stations trying to transmit at the beginning of the time slot.

Maximum Efficiency:

- The maximum efficiency occurs when $G = 1$. Substituting $G = 1$ into the efficiency formula:

$$\eta = 1 \times e^{-1} = \frac{1}{e} = 0.368$$

Maximum Efficiency of Slotted Aloha = 36.8%.

Compared to Pure Aloha, Slotted Aloha has a higher efficiency due to reduced collisions.

Differences Between Pure Aloha and Slotted Aloha

Feature	Pure Aloha	Slotted Aloha
Transmission Time	Any time	Must start at the beginning of a time slot
Time Synchronization	Continuous, not globally synchronized	Discrete, globally synchronized
Vulnerable Time	$2 \times T_t$	T_t
Probability of Successful Transmission	$G \times e^{-2G}$	$G \times e^{-G}$
Maximum Efficiency	18.4%	36.8%
Collision Rate	Higher, due to unsynchronized transmission	Lower, due to time slot synchronization
Advantages	Simple to implement	Higher efficiency, reduced collisions

Problem: A group of N stations shares a 100 Kbps slotted ALOHA channel. Each station sends a 500-bit frame every 5000 ms, even if the previous one hasn't been sent. What is the required value of N?

Solution:

1. **Throughput of One Station:**

$$\text{Throughput of each station} = \frac{500 \text{ bits}}{5000 \text{ ms}} = \frac{500}{5000 \times 10^{-3}} = 100 \text{ bits/sec}$$

2. **Throughput of Slotted Aloha:**

$$\text{Throughput of slotted aloha} = \eta \times \text{Bandwidth} = 0.368 \times 100 \text{ Kbps} = 36.8 \text{ Kbps}$$

3. **Total Number of Stations:**

$$\text{Throughput of slotted aloha} = N \times \text{Throughput of each station}$$

$$36.8 \text{ Kbps} = N \times 100 \text{ bits/sec}$$

$$N = \frac{36.8 \times 10^3}{100} = 368$$

Q. A slotted ALOHA network transmits 200-bit frames using a shared channel with a 200- kbps bandwidth. Find the throughput if the system (all stations together) produces a. 1000 frames per second b. 500 frames per second c. 250 frames per second

Ans:

Given Data:

- Frame size = 200 bits
- Channel bandwidth = 200 Kbps (kilobits per second)
- **Efficiency of Slotted Aloha (η) formula:**

$$\eta = G \times e^{-G}$$

Where:

- G is the average number of frame transmission attempts per time slot.
- The throughput of Slotted Aloha = $\eta \times \text{Bandwidth}$

Step 1: Calculate Frame Transmission Time

The time it takes to transmit one frame (i.e., frame duration) is calculated by:

$$T_{\text{frame}} = \frac{\text{Frame size}}{\text{Bandwidth}}$$

$$T_{\text{frame}} = \frac{200\,\text{bits}}{200,000\,\text{bits/sec}} = 1\,\text{ms}$$

Step 2: Calculate G (Average Number of Attempts Per Slot)

The average number of frame transmission attempts G is determined by the number of frames produced per second by all stations, and the time slot duration is equal to the frame time for Slotted Aloha.

For each second:

- The system produces Frames per second total frame attempts.
- The time slot duration is **1 ms**, which is the time to send one frame.

So, G is the total number of frames transmitted per second divided by the number of slots (which is 1000 slots per second since each slot is 1 ms):

$$G = \frac{\text{Frames per second}}{1000}$$

Step 3: Calculate Throughput for Different Cases

a. 1000 frames per second

For 1000 frames per second, we calculate G as:

$$G = \frac{1000}{1000} = 1$$

Substitute $G = 1$ into the efficiency formula:

$$\eta = 1 \times e^{-1} \approx 0.368$$

Now, calculate the throughput:

$$\text{Throughput} = \eta \times \text{Bandwidth} = 0.368 \times 200,000\,\text{bps} = 73,600\,\text{bps} = 73.6\,\text{Kbps}$$

Thus, the throughput when producing 1000 frames per second is **73.6 Kbps**.

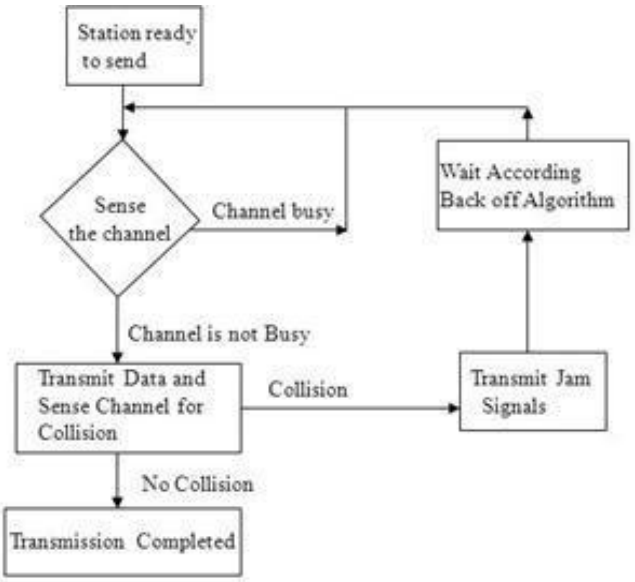
Refer example of text book page 92,93,94 (on pure and slotted aloha)

CARRIER SENSE MULTIPLE ACCESS / COLLISION DETECTION (CSMA / CD)

- **Carrier Sense** in CSMA/CD means that all the nodes sense the medium to check whether it is idle or busy.
  - If the carrier sensed is idle, then the node transmits the entire frame.
  - If the carrier sensed is busy, the transmission is postponed.

- **Collision Detect** means that a node listens as it transmits and can therefore detect when a frame it is transmitting has collided with a frame transmitted by another node.

Flowchart of CSMA/CD Operation

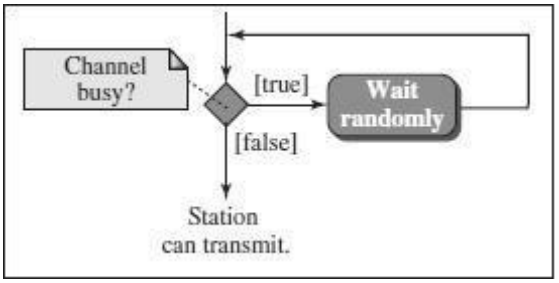

Station ready to send
Sense the channel
Channel busy
Wait According Back off Algorithm
Channel is not Busy
Transmit Data and Sense Channel for Collision
Collision
Transmit Jam Signals
No Collision
Transmission Completed

Transmitter Algorithm in CSMA/CD

- Transmitter Algorithm defines the procedures for a node that senses a busy medium.
- Three types of Transmitter Algorithm exist**.**
- They are
  1. Non-Persistent Strategy
  2. Persistent Strategy : 1-Persistent & P-Persistent

Non-Persistent Strategy

- In the non-persistent method, a station that has a frame to send senses the line.
- If the line is idle, it sends immediately.
- If the line is not idle, it waits a random amount of time and then senses the line again.

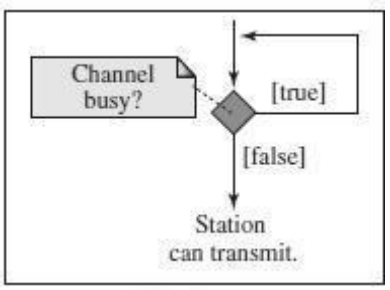


- The non-persistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.
- However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

Persistent Strategy

1- ***Persistent :***

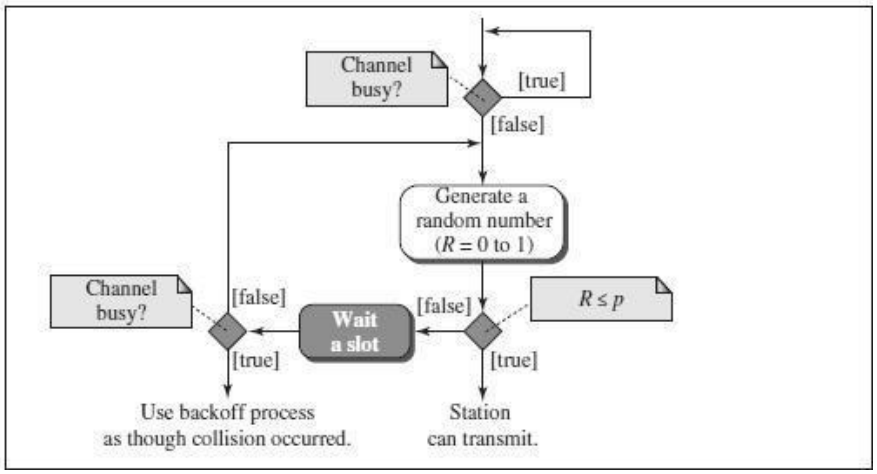
- The 1-persistent method is simple and straightforward.
- In this method, after the station finds the line idle, it sends its frame immediately (with probability 1).



- This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

P-Persistent :

- In this method, after the station finds the line idle it follows these steps:
- With probability *p*, the station sends its frame.
- With probability $q = 1 - p$, the station waits for the beginning of the next time slot and checks the line again.

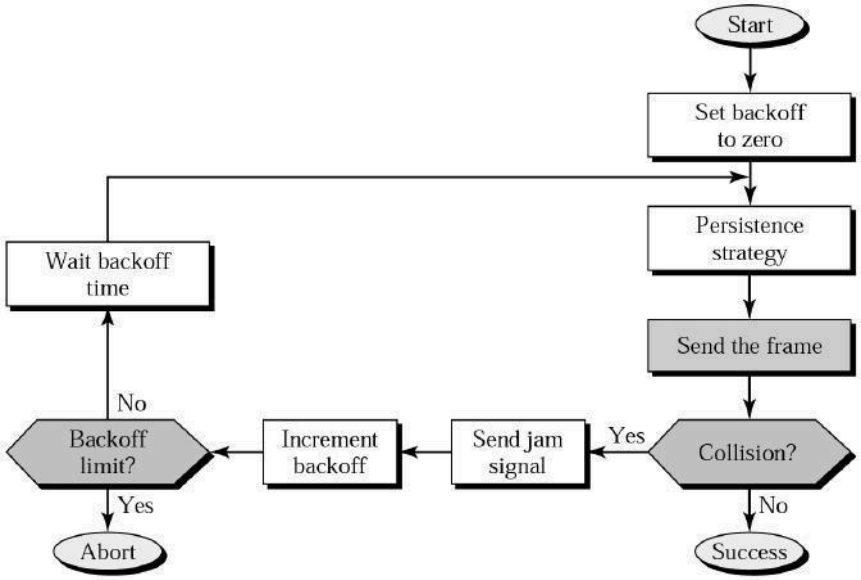


- The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time.
- The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency.

.

EXPONENTIAL BACK-OFF

- Once an adaptor has detected a collision and stopped its transmission, it waits a certain amount of time and tries again.
- Each time it tries to transmit but fails, the adaptor doubles the amount of time it waits before trying again.
- This strategy of doubling the delay interval between each retransmission attempt is a general technique known as **exponential back-off.**



FORMULAS TO REMEBER (IGNORE DERIVATAION)

[expect short question on it]

1.Transmission delay >= 2 x Propagation delay

2.

$$\text{Efficiency } (\eta) = \frac{T_t}{e \times 2 \times T_p + T_t + T_p}$$

OR

$$\text{Efficiency } (\eta) = \frac{T_t}{T_t + 6.44 \times T_p}$$

OR

$$\text{Efficiency } (\eta) = \frac{1}{1 + 6.44 \times a}, \text{ where } a = T_p / T_t$$

Example:

Let's assume the following values for the CSMA/CD network:

- **Bandwidth (B)** = 10 Mbps (10,000,000 bits per second).
- **Propagation Delay (d)** = 10 microseconds (10×10^{-6} seconds).

We can now calculate the minimum frame size.

Step 1: Calculate the minimum frame size (L):

$$L \geq 2 \times \text{Propagation Delay} \times \text{Bandwidth}$$

$$L \geq 2 \times (10 \times 10^{-6}\,\text{s}) \times (10,000,000\,\text{bits/sec})$$

$$L \geq 2 \times 10^{-6} \times 10^{7}$$

$$L \geq 20,000\,\text{bits}$$

Thus, the **minimum frame size** L is **20,000 bits**.

Step 2: Convert to bytes:

$$\text{Frame Size in bytes} = \frac{20,000\,\text{bits}}{8} = 2,500\,\text{bytes}$$

Thus, the **minimum frame size** is **2,500 bytes**.

Example Calculation:

Using the previous example where:

- **Bandwidth (B)** = 10 Mbps = 10^7 bits/sec.
- **Propagation Delay (one-way)** = 10 microseconds = 10×10^{-6} seconds.
- **Frame Size (L)** = 2000 bits (for example).

Step 1: Calculate Transmission Time (T):

$$T = \frac{L}{B} = \frac{2000\,\text{bits}}{10 \times 10^6\,\text{bits/sec}} = 0.0002\,\text{seconds} = 200\,\text{microseconds}$$

Step 2: Calculate Round-Trip Propagation Delay (d):

$$d = 2 \times 10 \times 10^{-6} = 20 \times 10^{-6}\,\text{seconds} = 20\,\mu\text{s}$$

Step 3: Calculate Efficiency (η):

$$\eta = \frac{1}{1 + 6.4 \times \frac{d}{L}} = \frac{1}{1 + 6.4 \times \frac{20 \times 10^{-6}}{2000}} = \frac{1}{1 + 6.4 \times 10^{-5}}$$

$$\eta \approx \frac{1}{1 + 0.000064} \approx \frac{1}{1.000064} \approx 0.999936$$

CARRIER SENSE MULTIPLE ACCESS / COLLISION AVOIDANCE (CSMA/CA)

- Carrier sense multiple access with collision avoidance (CSMA/CA) was

invented for wireless networks.

- Wireless protocol would follow exactly the same algorithm as the Ethernet—Wait until the link becomes idle before transmitting and back off should a collision occur.
- Collisions are avoided through the use of CSMA/CA's three strategies: the interframe space, the contention window, and acknowledgments

Interframe Space (IFS) - First, collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period of time called the ***interframe space*** or ***IFS.***

Contention Window - The **contention window** is an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time. The number of slots in the window changes according to the binary exponential backoff strategy. This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.

Acknowledgment - In addition, the data may be corrupted during the transmission.The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.

Comparison of Efficiency

Feature	CSMA/CD (Wired)	CSMA/CA (Wireless)
Collision Handling	Collision Detection	Collision Avoidance
Efficiency at Low Traffic	High	High
Efficiency at High Traffic	Low (due to collisions)	Moderate (due to RTS/CTS overhead)
Backoff Mechanism	Random backoff after collision	Random backoff + RTS/CTS
Overhead	Low	High (due to RTS/CTS)
Best Use Case	Wired networks (Ethernet)	Wireless networks (Wi-Fi)

Controlled Access in Data Link Layer

Controlled access is a method used in the data link layer to manage how multiple devices share the same communication channel. It helps to avoid collisions and ensures fair access to the medium. The three main controlled access mechanisms are **Polling**, **Reservation**, and **Token Passing**.

1. Polling:

Polling is a method in which a central device (master) controls and coordinates the access to the shared communication medium. In polling, the master device asks each station (in a round-robin or sequential manner) if it has data to send. Only the station that gets polled can transmit, while others wait for their turn.

Types of Polling:

- **Unidirectional Polling:** The central device sends a polling request to each device one by one.
- **Bidirectional Polling:** Stations can also send polling requests to the central device.

Working:

- The master device sends a polling signal to each station.
- The station responds with either a "Yes" (if it has data to send) or a "No" (if it has no data).
- If a station has data, it is allowed to transmit; otherwise, the polling continues to the next station.

Advantages:

- Simple to implement.
- Fair access as the master controls the polling sequence.

Disadvantages:

- Overhead increases as the number of stations increases.
- Master device can become a bottleneck.

2. Reservation:

In the reservation method, stations "reserve" a time slot in advance for transmission. The reservation is done by signaling the central controller or a shared control channel, allowing stations to guarantee time for transmission. Reservation is typically used in systems like **Reservation-based ALOHA** or **TDMA**.

Working:

- Stations make reservations in advance to transmit during a specific time slot.
- The reservation process ensures that each station can transmit without causing a collision.

Advantages:

- Predictable and efficient as stations have fixed transmission times.
- Reduces collisions as each station has its reserved time.

Disadvantages:

- It may lead to inefficient use of bandwidth if some stations do not need their reserved slots.
- Complex setup and maintenance of reservations.

3. Token Passing:

In token passing, a special data packet called the **token** is passed around the network. Only the station holding the token is allowed to transmit. This method eliminates the need for a central controller and is widely used in ring topologies (e.g., **Token Ring**).

Working:

- A special token (packet) circulates through the network.
- A station can only send data if it holds the token.
- After sending the data, the station passes the token to the next station in the sequence.
- If a station does not need to transmit, it simply passes the token along.

Advantages:

- No central controller is required.
- Fair access to the medium, as only the token holder can transmit.
- Scalable and flexible for large networks.

Disadvantages:

- If the token is lost, no station can transmit.
- Overhead in managing the token's circulation.

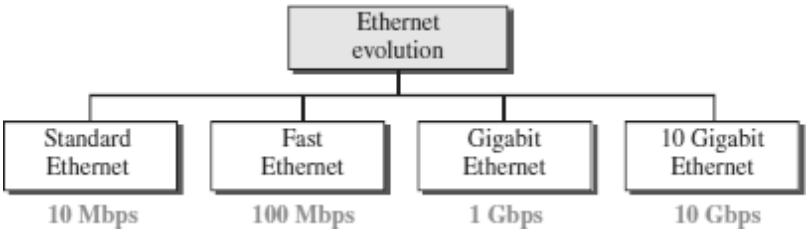
Comparison of Polling, Reservation, and Token Passing:

Feature	Polling	Reservation	Token Passing
Central Control	Yes, master controls access	Yes, control is managed centrally	No, decentralized (token circulates)
Access Method	Master polls stations one by one	Stations reserve specific time slots	Only token holder can transmit
Efficiency	Low (due to overhead of polling)	High (predictable, dedicated time slots)	Moderate (overhead in passing the token)
Fairness	Fair, as all stations get a turn	Fair, as each station has a reserved slot	Fair, as token is passed in a loop
Scalability	Less scalable as network grows	Scalable, but overhead in managing slots	Scalable and flexible in large networks
Collisions	Occurs if stations transmit between polls	Low, as each station has reserved time	No collisions as only token holder transmits
Implementation	Simple, easy to implement	More complex, requires slot management	Moderate, requires token management

8. WIRED LAN : ETHERNET (IEEE 802.3)

- Ethernet was developed in the mid-1970's at the Xerox Palo Alto Research Center (PARC),
- IEEE controls the Ethernet standards.
- The Ethernet is the most successful local area networking technology, that uses bus topology.
- The Ethernet is **multiple-access networks** that is set of nodes send and receive frames over a shared link.
- Ethernet uses the **CSMA / CD (C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection) mechanism.

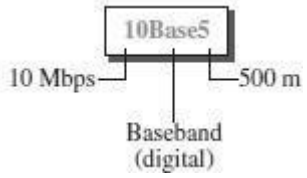
EVOLUTION OF ETHERNET

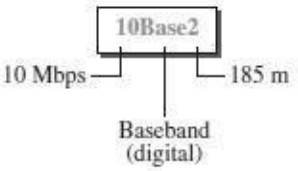


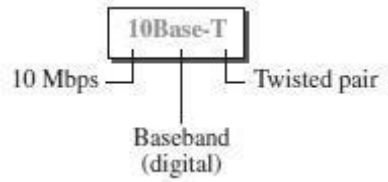
Standard Ethernet (10 Mbps)

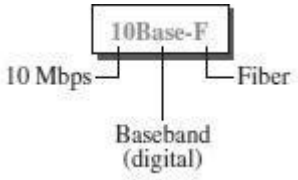
The original Ethernet technology with the data rate of 10 Mbps as the Standard Ethernet.
Standard Ethernet types are

1. 10Base5: Thick Ethernet,
2. 10Base2: Thin Ethernet ,
3. 10Base-T: Twisted-Pair Ethernet
4. 10Base-F: Fiber Ethernet.

<table>
<tr>
<td><u>10Base5: Thick Ethernet</u>
 

● The first implementation is called 10Base5, thick Ethernet, or Thicknet.
● 10Base5 was the first Ethernet specification to use a bus topology with an external transceiver(transmitter/receiver) connected via a tap to a thick coaxial cable.</td>
<td><u>10Base2: Thin Ethernet</u>
 

● The second implementation is called 10Base2, thin Ethernet, or Cheapernet.
● 10Base2 also uses a bus topology, but the cable is much thinner and more flexible.
● In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.</td>
</tr>
<tr>
<td><u>10Base-T: Twisted-Pair Ethernet</u>
 

● The third implementation is called 10Base-T or twisted-pair Ethernet.
● 10Base-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable.</td>
<td><u>10Base-F: Fiber Ethernet</u>
 

● Although there are several types of optical fiber 10-Mbps Ethernet, the most common is called 10Base-F.
● 10Base-F uses a star topology to connect stations to a hub.
● The stations are connected to the hub using two fiber-optic cables.</td>
</tr>
</table>

Fast Ethernet (100 Mbps)

Fast Ethernet or 100BASE-T provides transmission speeds up to 100 megabits per second and is typically used for LAN backbone systems.

The 100BASE-T standard consists of three different component specifications –

1. 100 BASE-TX
2. 100BASE-T4
3. 100BASE-FX

100 BASE-TX	**100BASE-T4**	**100BASE-FX**
100Base-TX uses two pairs of twisted-pair cable either UTP or STP. A 100Base-TX network can provide a data rate of 100 Mbps.	A new standard, called ***100Base-T4,*** was designed to use four pairs of UTP for transmitting 100 Mbps.	**100Base-FX** uses two pairs of fiber-optic cables. Optical fiber can easily handle high bandwidth requirements.

Gigabit Ethernet (1 Gbps)

- The Gigabit Ethernet upgrades the data rate to 1 Gbps(1000 Mbps).
- Gigabit Ethernet can be categorized as either a two-wire or a four-wire implementation.
- The two-wire implementations use fiber-optic cable (**1000Base-SX,** short-wave, or **1000Base-LX,** long-wave), or STP (**1000Base-CX**).
- The four-wire version uses category 5 twisted-pair cable (**1000Base-T**).

10 Gigabit Ethernet(10 Gbps)

- 10 Gigabit Ethernet is an upcoming Ethernet technology that transmits at 10 Gbps.
- 10 Gigabit Ethernet enables a familiar network technology to be used in LAN, MAN and WAN architectures.
- 10 Gigabit Ethernet uses multimode optical fiber up to 300 meters and single mode fiber up to 40 kilometers.
- Four implementations are the most common: **10GBase-SR, 10GBase-LR, 10GBase-EW, and 10GBase-X4.**

ACCESS METHOD/ PROTOCOL OF ETHERNET

The access method of Ethernet is CSMA/CD.

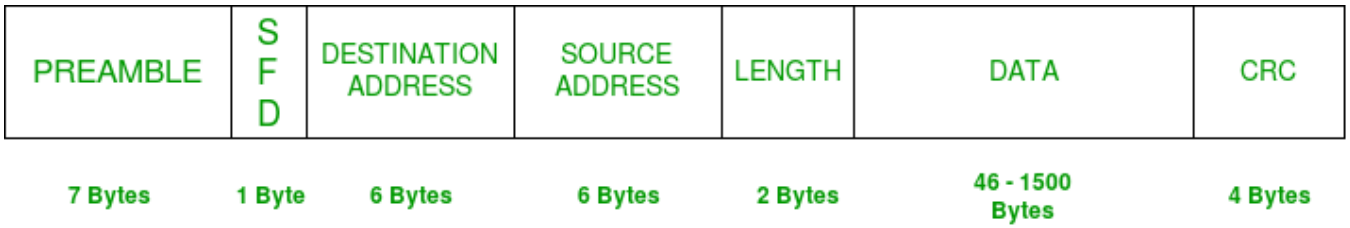
Note: Refer CSMA/CD from MAC

COLLISION DETECTION IN ETHERNET

- As the Ethernet supports collision detection, senders are able to determine a collision.
- At the moment an adaptor detects that its frame is colliding with another, it first makes sure to transmit a **32-bit jamming sequence** along with the **64-bit preamble** (totally 96 bits) and then stops the transmission.
- These **96 bits** are sometimes called **Runt Frame.**

FRAME FORMAT OF ETHERNET

The Ethernet frame is defined by the format given in the Fig.



IEEE 802.3 ETHERNET Frame Format

- The 64-bit ***preamble*** allows the receiver to synchronize with the signal; it is a sequence of alternating 0's and 1's.
- Both the ***source and destination*** hosts are identified with a 48-bit ***address.***
- The packet ***type*** field serves as the demultiplexing key.
- Each frame contains up to 1500 bytes of ***data(Body).***
- ***CRC*** is used for Error detection

Ethernet Addresses

- Every Ethernet host has a unique Ethernet address (48 bits – 6 bytes).
- Ethernet address is represented by sequence of six numbers separated by colons.
- Each number corresponds to 1 byte of the 6 byte address and is given by

pair of hexadecimal digits.

- **Eg: 8:0:2b:e4:b1:2** is the representation of
  00001000 00000000 00101011 11100100 10110001 00000010
- Each frame transmitted on an Ethernet is received by every adaptor connected to the Ethernet.
- In addition to ***unicast*** addresses an Ethernet address consisting of ***all 1s*** is treated as ***broadcast*** address.
- Similarly the address that has the ***first bit set to 1*** but it is not the broadcast address is called ***multicast*** address.

Ethernet Frame Format

An Ethernet frame is the basic unit of data transmission on Ethernet networks. The frame structure allows for precise data transfer and error-checking to ensure that data arrives intact at its destination. Below is a breakdown of each component in an Ethernet frame.

1. Preamble (7 Bytes)

- Pattern: Composed of a repetitive sequence of alternating 0's and 1's.
- Function: The preamble signals the beginning of a new frame and establishes bit synchronization between the sender and receiver. This sequence allows devices on the network to "lock onto" the frame, ensuring they are prepared to read the data accurately.
- Historical Note: Originally introduced to compensate for signal delays on older, slower networks, it is less critical on modern, high-speed Ethernet. However, it is still part of the Ethernet standard to maintain backward compatibility with older Ethernet devices and protocols.

2. Start of Frame Delimiter (SFD) (1 Byte)

- Pattern: Always set to 10101011.
- Function: The SFD marks the actual start of the frame data following the preamble and indicates that the frame's destination address follows next.
- Additional Note: The SFD is sometimes considered part of the preamble, making it seem like the preamble is 8 bytes. However, it's technically distinct and warns receiving stations that this is the last bit pattern for synchronization.

3. Destination Address (6 Bytes)

- Content: Contains the 48-bit (6-byte) MAC address of the receiving device or devices. This address can be:
  - Unicast: For a specific destination device.
  - Multicast: For a group of devices in a multicast group.
  - Broadcast: For all devices on the network (using the address FF:FF:FF:FF:FF:FF).
- Function: This field directs the frame to the intended recipient(s) within the network. The destination MAC address ensures that only the designated receiver(s) will process the frame.

4. Source Address (6 Bytes)

- Content: Holds the MAC address of the frame's sender.
- Function: Identifies the sender device to the recipient, allowing the recipient to recognize where the data originated from. This address is always a unicast address.
- Details: The least significant bit of the first byte is always 0, denoting a unique (unicast) address, differentiating it from multicast addresses (where this bit is set to 1).

5. Length / Type Field (2 Bytes)

- Purpose: This field can serve one of two functions depending on its value:
    - Length: Specifies the size of the payload (Data field), up to a maximum of 1500 bytes. Values up to 1500 denote the length.
    - Type: If the value is 1536 (0x0600) or higher, it indicates the type of protocol encapsulated in the payload, e.g., 0x0800 for IP and 0x0806 for ARP.
- Function: The Type field helps the receiving device understand how to process the data in the payload.

6. Data / Payload (46–1500 Bytes)

- Content: Contains the actual data being transferred over the network. This could be an IP packet, ARP message, or any other protocol data.
- Minimum Length: To meet the Ethernet frame's minimum length requirements, padding is added if the data is less than 46 bytes.
- Maximum Length: Standard Ethernet frames limit this field to 1500 bytes.
- Additional Details: If IP is used, the Data field includes the IP header along with the actual data. For encapsulating higher-level protocols, Ethernet frames may include fields from TCP, UDP, etc., in the payload section.

7. Cyclic Redundancy Check (CRC) (4 Bytes)

- Content: A 32-bit checksum generated by running a CRC algorithm on the frame's contents, including the destination address, source address, Length/Type, and Data fields.
- Function: Helps ensure data integrity by allowing the receiving device to detect transmission errors. If the calculated CRC at the destination doesn’t match the transmitted CRC, the frame is considered corrupted, and it may be discarded or retransmitted.

8. Optional Fields in Ethernet Frames

- VLAN Tagging (4 Bytes):
    - Purpose: Allows for logical network segmentation. Each VLAN tag includes a VLAN ID, which can be used to segregate network traffic, giving each VLAN its virtual subnet.
    - Content: A VLAN tag contains information about priority and VLAN ID, allowing devices to differentiate between various virtual networks.
- Jumbo Frames:
    - Definition: Frames larger than the standard Ethernet frame size of 1518 bytes, often with payload sizes up to 9000 bytes or more.
    - Purpose: Used in specific network environments (like data centers) to improve throughput by reducing the need to send many small frames, thus reducing overhead.

9. EtherType Field (2 Bytes)

- Function: Identifies the protocol type encapsulated within the Ethernet frame payload.
- Examples:
    - 0x0800 for IPv4
    - 0x0806 for ARP (Address Resolution Protocol)
    - 0x86DD for IPv6
- Importance: Helps the receiving device know how to handle the frame's payload. For instance, an IP frame can be directed to the IP processing stack.

10. Frame Types: Unicast, Multicast, and Broadcast Frames

- Unicast Frames: Directed to a single destination MAC address.
- Multicast Frames: Sent to multiple devices within a designated multicast group, often for streaming or conferencing applications.
- Broadcast Frames: Sent to all devices on the network using the special MAC address FF:FF:FF:FF:FF:FF.

11. Collision Detection and CSMA/CD Protocol

- Protocol: Ethernet networks, especially half-duplex ones, use Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to prevent and handle frame collisions.
- How it Works:
    - Devices listen to the network before transmitting data to avoid collisions.
    - If two devices transmit at the same time, a collision occurs, detected by the CSMA/CD protocol.
    - Both devices wait a random period before retrying, reducing the chance of repeated collisions.
- Note: With modern Ethernet (full-duplex and switched networks), collisions are rare, as each device has its dedicated channel.

Summary of Ethernet Frame Components

Field	Size	Purpose & Notes
Preamble	7 bytes	Synchronization between sender and receiver.
SFD	1 byte	Marks the beginning of the frame.
Destination Address	6 bytes	MAC address of the destination device(s).
Source Address	6 bytes	MAC address of the sending device.
Length / Type	2 bytes	Indicates data length or protocol type.
Data / Payload	46-1500 bytes	Contains actual data or padding.
CRC	4 bytes	Provides error-checking.

ADVANTAGES OF ETHERNET

Ethernets are successful because

- It is extremely ***easy to administer and maintain.*** There are no switches that can fail, no routing or configuration tables that have to be kept up-to-date, and it is easy to add a new host to the network.

- It is ***inexpensive:*** Cable is cheap, and the only other cost is the network adaptor on each host.
