DATALINK LAYER

Contents

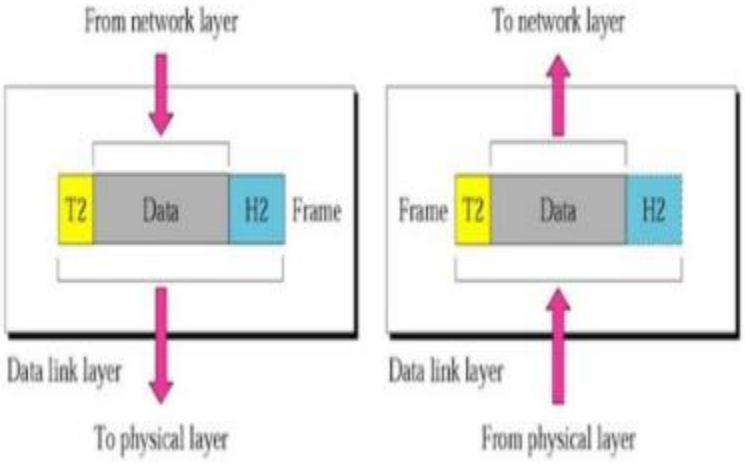
INTRODUCTION

- The data-link layer is responsible for transferring a datagram that comes from the network layer across an individual link.

• A link is the communication channels that connect two adjacent hosts routers.

• In order to move a datagram from source host to destination host, the datagram must be moved over each of the individual links in the path.

• Its responsibilities include framing data into frames, addressing, flow control manage data rates between sender and receiver, error control to ensure reliability, and media access control in shared networks.



Functions

Framing: Divides the bit stream from the network layer into manageable data units called frames.

Physical Addressing: Adds a header to frames to specify sender and/ receiver addresses. If the frame needs to be forwarded outside the sender's network, the receiver address is the device connecting to the next network.

Flow Control: Regulates data flow between sender and receiver to prevent overwhelming the receiver. Ensures that data are transmitted at a rate that the receiver can handle.

Error Control: Enhances reliability by detecting and retransmitting damaged or lost frames. Uses mechanisms like checksums or CRC (Cyclic Redundancy Check) in a frame trailer to detect errors. Includes mechanisms to manage duplicate frame detection.

Access Control: Manages access to shared communication channels when multiple devices are connected. Implements protocols to determine which device can transmit data on the link at any given time, ensuring orderly communication.

Logical Link Control (LLC) and Media Access Control (MAC)

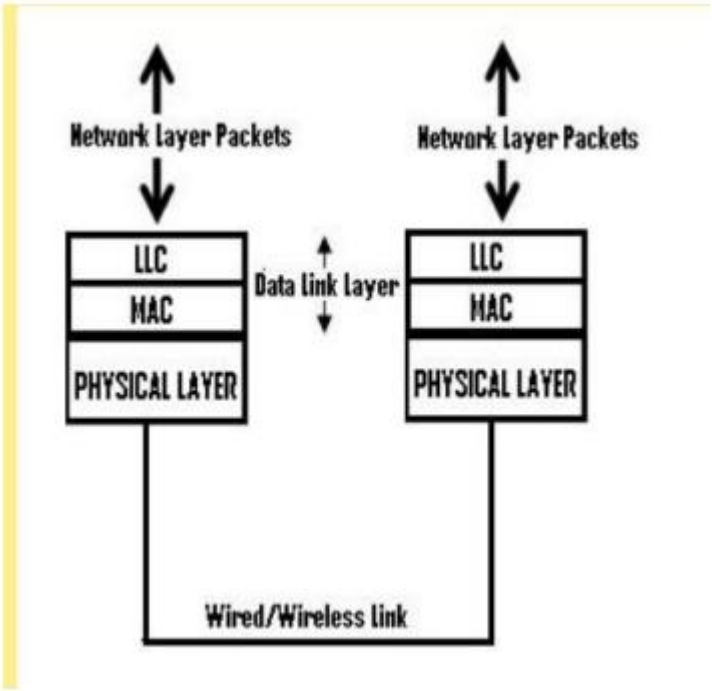
The data link layer is made up of two sublayers:

LLC (Logical Link Control)Layer

MAC(Media Access Control)Layer

• Both of these two sublayers are responsible for different functions for the data link layer.

• LLC interacts with the network layer above and the lower sub-layer, termed as MAC, that interacts with the physical layer below.



LLC (Logical Link Control)

• The LLC (Logical Link Control) is responsible for managing multiple Layer 3 protocols (multiplexing and de-multiplexing) and providing link services such as reliability and flow control.

The key functions of the LLC include:

• Multiplexing protocols that operate on top of the data link layer.

• Optionally offering flow control, acknowledgment, and error recovery.

• Providing addressing and control over the data link, specifying mechanisms for stations over the transmission medium and managing data exchange between the sender and receiver

MAC(Media Access Control)Layer

• The MAC sublayer provides control for accessing the transmission medium.

• It is responsible for moving data packets from one network interface card (NIC) to another across a shared transmission medium.

• Physical addressing is managed at the MAC sublayer. This involves determining the method used to allocate network access to devices and prevent simultaneous transmissions that could cause data collisions.

Common MAC methods include:

• Carrier Sense Multiple Access/Collision Detection (CSMA/CD), used by Ethernet networks.

• Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), used by AppleTalk networks.

• Token passing, used by Token Ring and Fiber Distributed Data Interface (FDDI) networks.

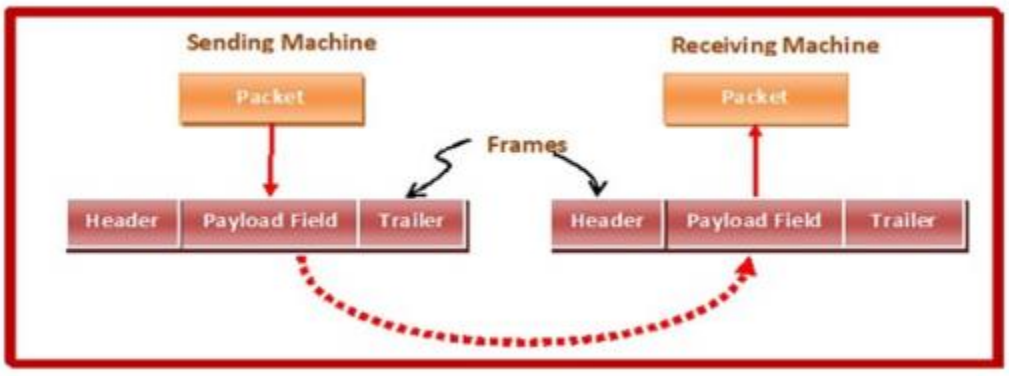
FRAMING

Framing is the process of dividing data into manageable blocks called frames for transmission between two devices.

It ensures that the bits sent by the sender are understood correctly by the receiver.

Each frame has a structure, often including a header with important information like error-checking codes.

This function is managed by the data link layer, and various technologies like Ethernet and token ring use different frame structures.



In the physical layer, data transmission involves the synchronized transmission of bits from the source to the destination. The data link layer packs these bits into frames

The data link layer takes packets from the network layer and encapsulates them into frames. If the frame size becomes too large, the packet may be divided into smaller frames. Smaller frames improve the efficiency of flow control and error control.

The data link layer then sends each frame bit-by-bit on the hardware. At the receiver's end, the data link layer picks up signals from the hardware and reassembles them into frames.

Parts of Frame

Frame Header – It contains the source and the destination addresses of the frame.

Payload field – It contains the message to be delivered.

Trailer – It contains the error detection and error correction bits.

Flag – It marks the beginning and end of the frame

Types of Framing

Fixed-Sized Framing:

•Frames have a fixed size, so the frame length itself acts as a delimiter.

•No additional boundary bits are needed to identify the start and end of frame.

•Example: ATM (Asynchronous Transfer Mode) cells.

Variable-Sized Framing:

•Frames can be of different sizes.

•Additional mechanisms are used to mark the end of one frame and the beginning of the next.

•Commonly used in local area networks (LANs)

Flow Control

•Flow control in the data link layer manages the rate at which data is sent from sender to receiver.

•It ensures the sender doesn't overwhelm the receiver by regulating how much data can be sent before receiving acknowledgment.

•This coordination prevents data loss and ensures efficient transmission over shared networks.

•Flow Control coordinates that amount of data that can be sent before receiving acknowledgement.

•It makes the sender wait for some sort of an ACK before continuing to send more data.

•Flow control tells the sender how much data to be sent

FLOW CONTROL TECHNIQUE

1) STOP AND WAIT
2) SLIDDING WINDOW

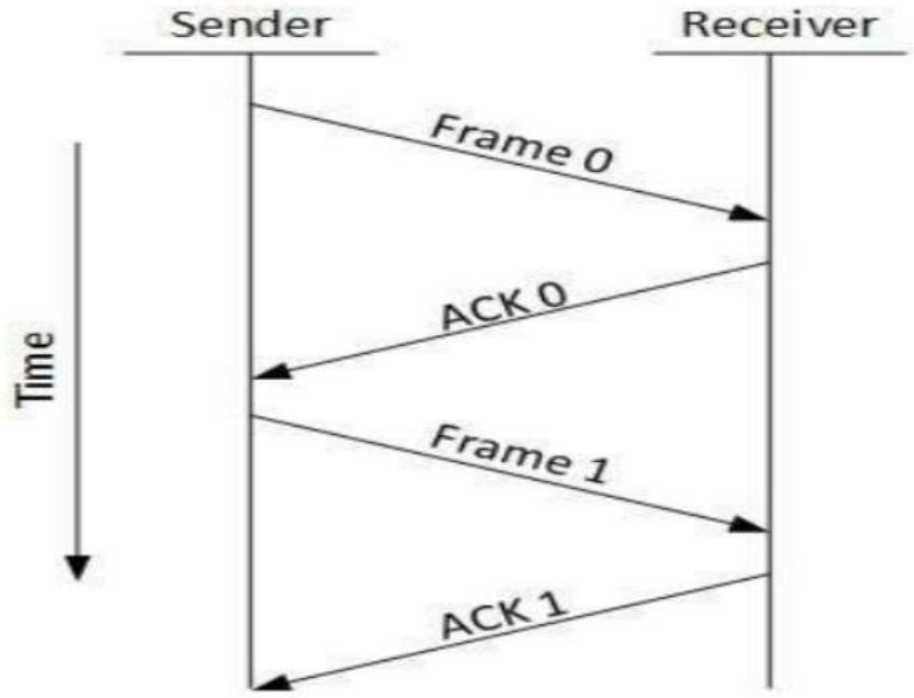
Stop and Wait

•Sends one frame at the time.

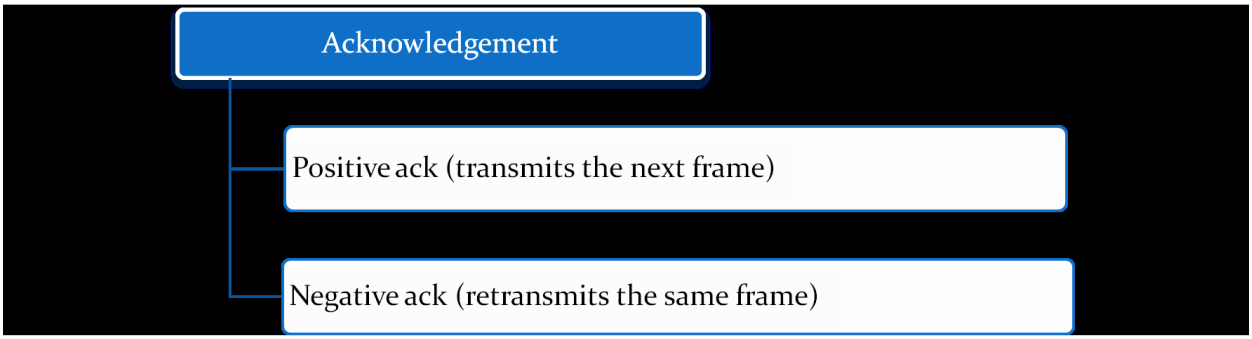
•The sender waits for acknowledgement of every frame that it sends.

•The receiver indicates its willingness to accept another frame by sending acknowledgement of the frame that it receives.

•Only when acknowledgement has been received next frame is sent.



Positive ACK – When the receiver receives a correct frame, it should acknowledge it.
Negative ACK – When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.
•The receiver can thus stop flow of data by just withholding the acknowledgement.



Advantages

•Each frame is transmitted only after first frame is acknowledged.

•Data frame is not lost.

Disadvantages

•Inefficient, only one frame can be in transmission at a time.

•The time spent for waiting acknowledgment between each frame add significant amount to total transmission time.

Sliding Window

•In sliding window, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent.

•Sends multiple packets or frames without waiting for acknowledgment.

•Frames can be sent one right after another and it's capacity can be used effectively.

•The receiver acknowledges only some of the frames using single ACK to confirm receipt of multiple data frames.

•Sender and receiver have a window which can hold frames.

•The sender can send as many frames that would fit into a window.

•For each window of size n, frames get numbered from 0 to n-1.

•If n=8 the frames are numbered 0,1,2,3,4,5,6,7. (the size of the window is n)

•When the receiver sends ACK it includes the number of the next frame it expects to receive.

•When the sender sees an ACK with the number 5, it knows that all frames up through number 4 have been received.

What is Error?

•When bits are transmitted over the computer network, they are subject to get corrupted due to interference and network problems.

•The corrupted bits leads to spurious data being received by the destination and are called errors.

•Condition where sender's info doesn't match receiver's info are Errors

Types of Errors:

•Single Bit Error

•Multiple Bits Error

•Burst Error

- **Single bit error**

In a frame, there is only one bit, anywhere though, which is corrupt.

- **Multiple bits error**

Frame is received with more than one bits in corrupted state.

- **Burst error**

Frame contains more than1 consecutive bits corrupted.

Error Control

•Error control includes both error detection and error correction.

•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.

•Error control in the data link layer is based on automatic repeat request (ARQ). Whenever an error is detected, specified frames are retransmitted.

Two ways of Error control :

•**Error Detection**: This involves checking whether any errors have occurred. The number of error bits and the type of error do not matter.

•**Error Correction**: This involves determining the exact number of corrupted bits and the location of these corrupted bits.

Requirements for error control mechanism

•**Error Detection**: The sender and receiver, either both or individually, must ensure that there is no error during transit.

•**Positive ACK**: When the receiver receives a correct frame, it should acknowledge it.

•**Negative ACK**: When the receiver receives a damaged or duplicate frame, it sends a NACK back to the sender, and the sender must retransmit the correct frame.

•**Retransmission**: The sender maintains a clock and sets a timeout period. If an acknowledgment of a previously transmitted data frame does not arrive before the timeout, the sender retransmits the frame, assuming that the frame or its acknowledgment was lost in transit.

Error Detection: This involves identifying errors in the transmitted data. Common techniques include:

•**Parity Check**: Adding a parity bit to the data. If the number of bits with a value of 1 is odd or even (depending on whether odd or even parity is used), the parity bit is set accordingly. If a single bit error occurs, the parity will be incorrect, signaling an error.

•**Checksums**: Summing the data segments and sending this sum along with the data. The receiver performs the same summing operation and checks if the sums match.

•**Cyclic Redundancy Check (CRC)**: A more robust method where a polynomial division is performed on the data, and the remainder is sent along with the data. The receiver performs the same division and checks the remainder to detect errors.

Parity Check

•Parity check involves adding a parity bit to data to ensure a specific number of 1s (even or odd).

•During frame creation, the sender calculates the number of 1s in the data:

oFor even parity, the parity bit is 0 if the count of 1s is even, and 1 if odd.

oFor odd parity, the parity bit is 0 if the count of 1s is odd, and 1 if even.

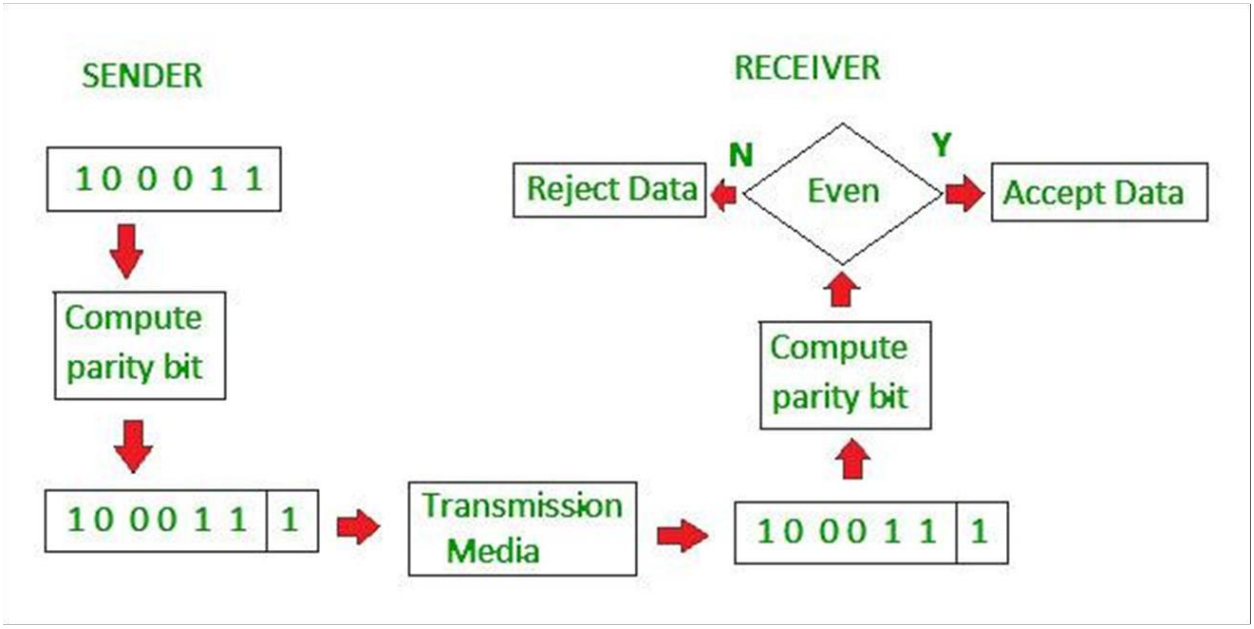
•Upon receiving a frame, the receiver counts the 1s:

oFor even parity, the frame is accepted if the count of 1s is even; otherwise, it's rejected.

oFor odd parity, acceptance occurs if the count of 1s is odd; otherwise, it's rejected.

•Parity check effectively detects single-bit errors but has limitations beyond this scope.

Simple Parity Check

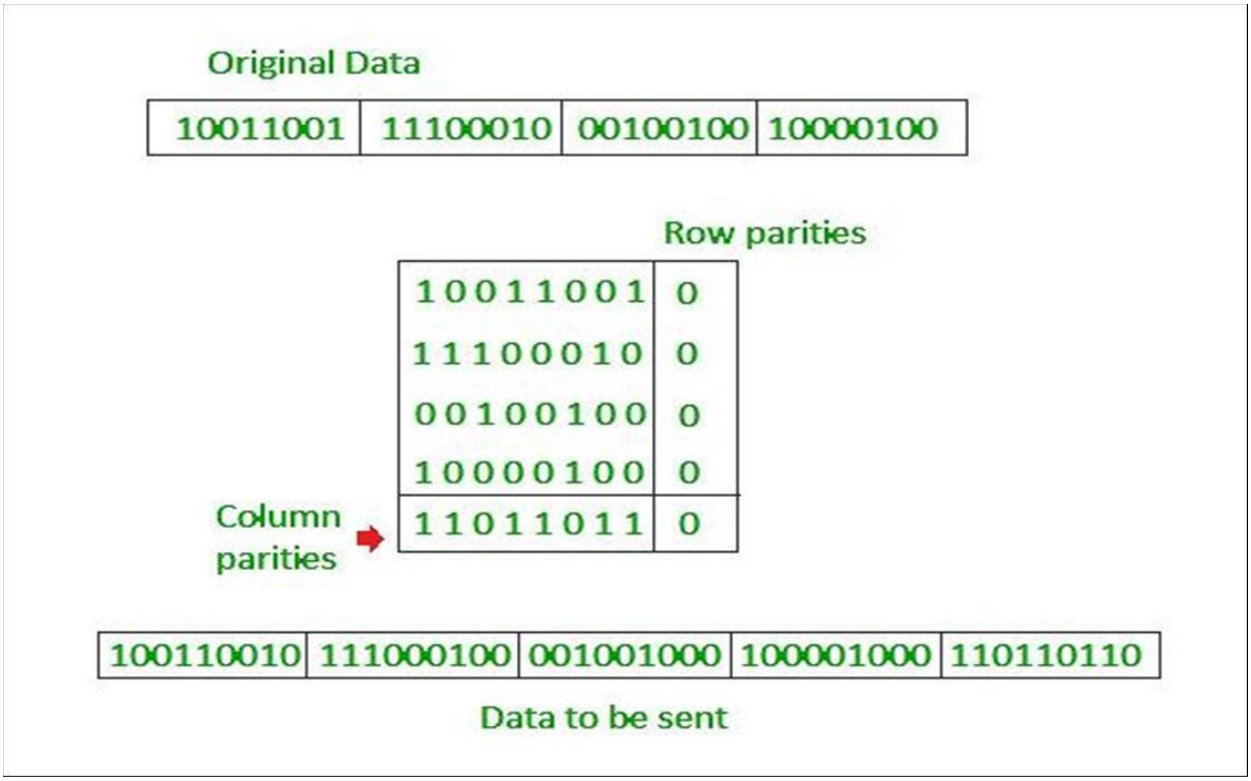


Two Dimensional Parity Check

•Parity check bits are calculated for each row which is equivalent simple parity check bit

•Parity check bits are also calculated for all columns, then both are sent along with data

•At the receiving end these are compared with parity bits calculated on the received data



Checksum

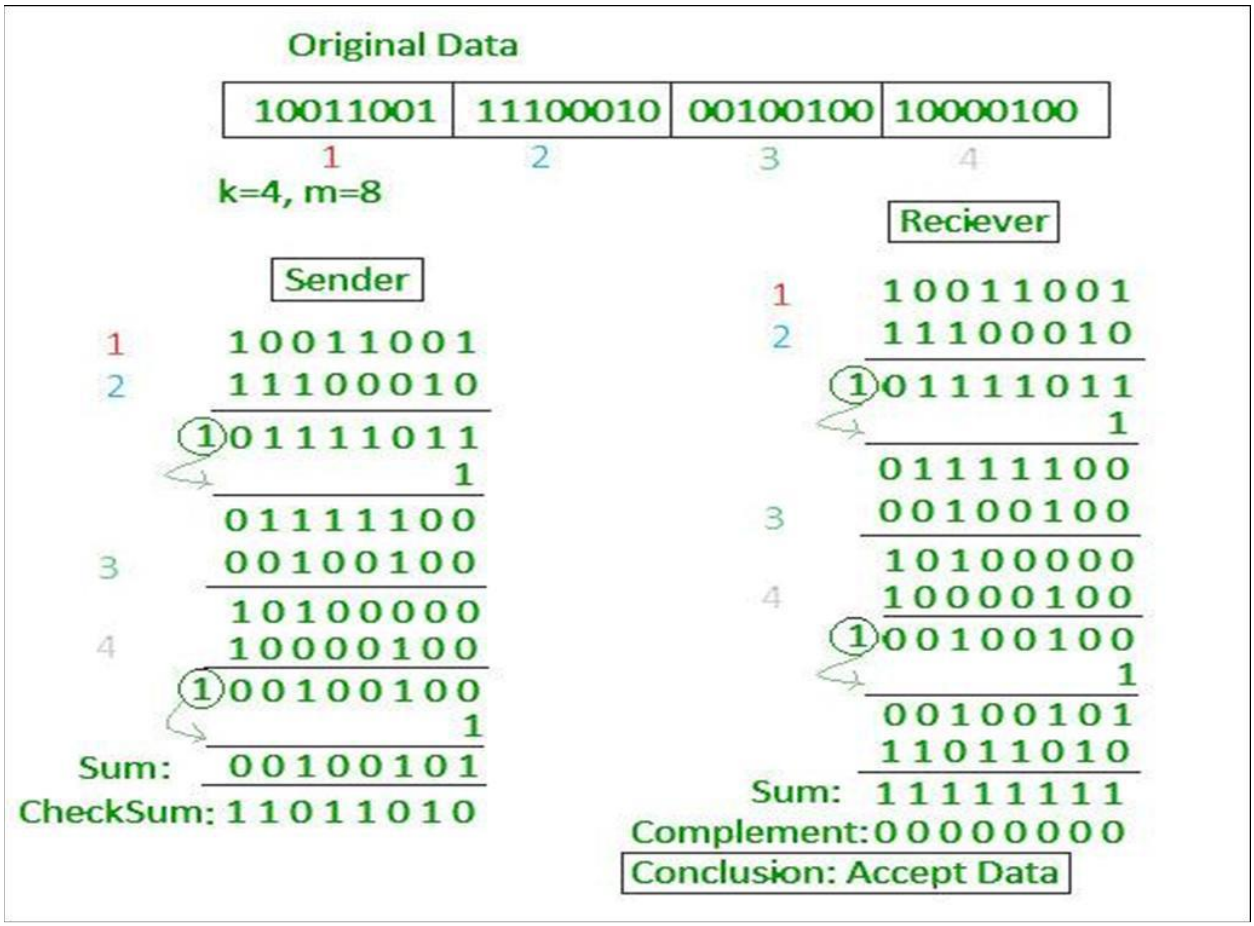
Data is segmented into fixed-sized frames or segments.

•The sender computes the checksum by summing up the segments using 1's complement arithmetic. It then complements this sum to obtain the checksum, which is sent along with the data frames.

•Upon receiving the data frames, the receiver computes the sum of the segments along with the received checksum using 1's complement arithmetic.

•The receiver then complements the sum obtained.

•If the resulting sum is zero, indicating no errors, the frames are accepted. Otherwise, they are discarded due to detected errors.



Cyclic Redundancy Check (CRC)

•Cyclic Redundancy Check (CRC) is a robust error detection scheme used in data communication.

•It is a powerful algorithm that is used for error control in the data link layer.

•Data is segmented into fixed-sized frames or blocks.

•The sender generates a CRC by performing polynomial division on the data using a predefined generator polynomial.

•The resulting CRC, a remainder of this division, is appended to the data frames before transmission.

•Upon receiving the frames, the receiver performs the same polynomial division using the generator polynomial.

•If the remainder obtained matches a predefined constant (usually zero), no errors are detected, and the frames are accepted.

•Any deviation indicates an error, leading to the rejection of the frames.

Cyclic Redundancy Check

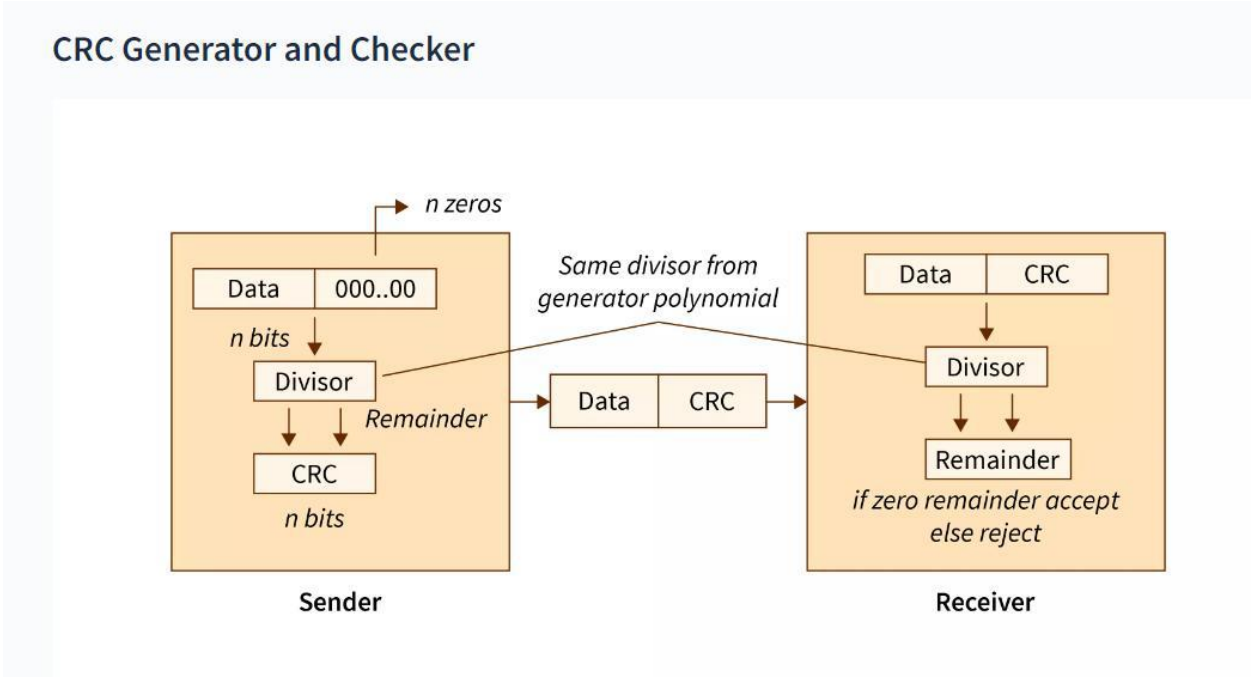
Let M(x) be the **message polynomial**

Let P(x) be the **generator polynomial**

o P(x) is fixed for a given CRC scheme

o P(x) is known both by sender and receiver

Create a block polynomial F(x) based on M(x) and P(x) such that F(x) is divisible by P(x)



Sending

1.Multiply M(x) by xn

2.Divide xnM(x) by P(x)

3.Ignore the quotient and keep the reminder C(x)

4.Form and send F(x) = xnM(x)+C(x)

Receiving

1.Receive F'(x)

2.Divide F'(x) by P(x)

3.Accept if remainder is 0, reject otherwise

Cyclic Redundancy Check

Let us assume *k* message bits and n bits of redundancy

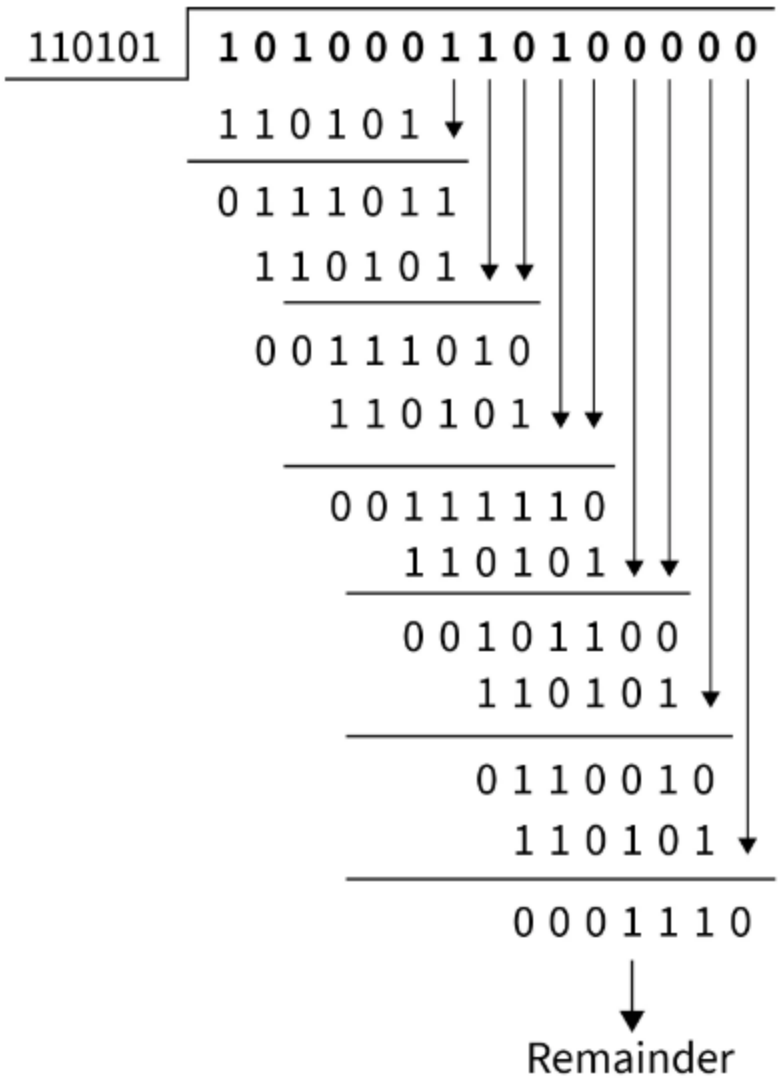
Xxxxxxxx yyyy block of length k+n

Associate bits with coefficients of a polynomial 1 0 1 1 0 1 1 1x6+0x5+1x4+1x3+0x2+1x+1 = x6+x4+x3+x+1

AT THE SENDER END

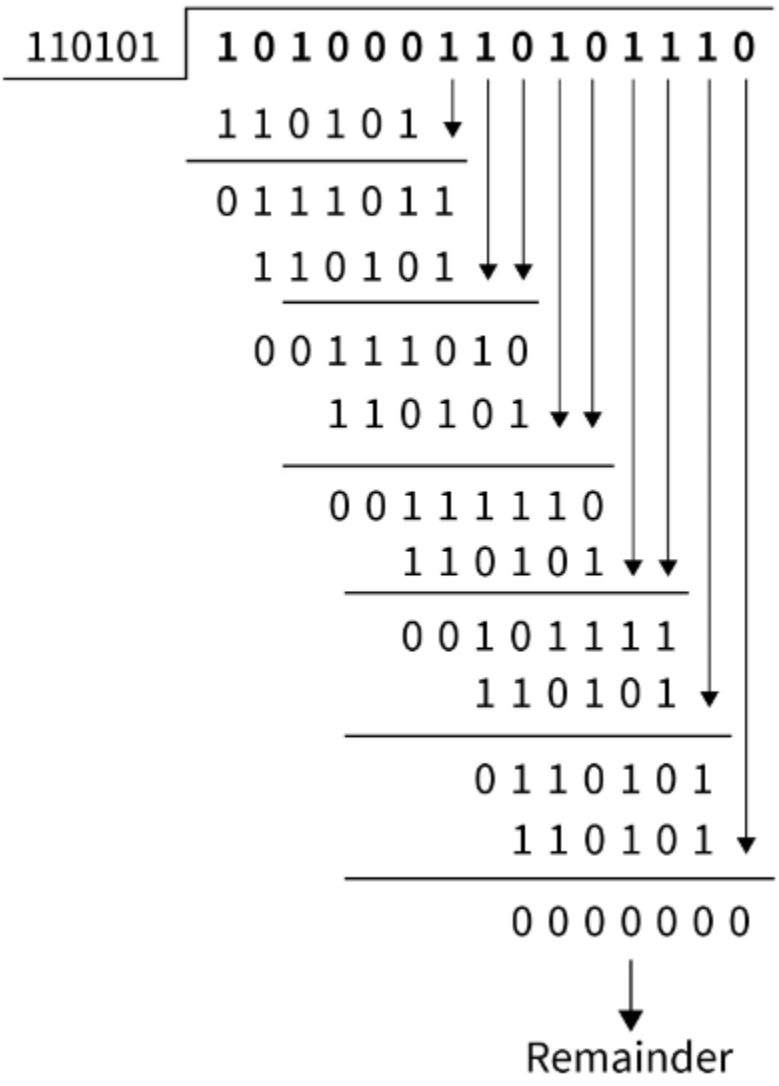
Example: Consider the message sender wants to send is 1010001101, and the generator polynomial is $x5+x4+x2+1$. Find the message transmitted by the sender. If the receiver receives the message, check if the receiver receives the correct message or not.

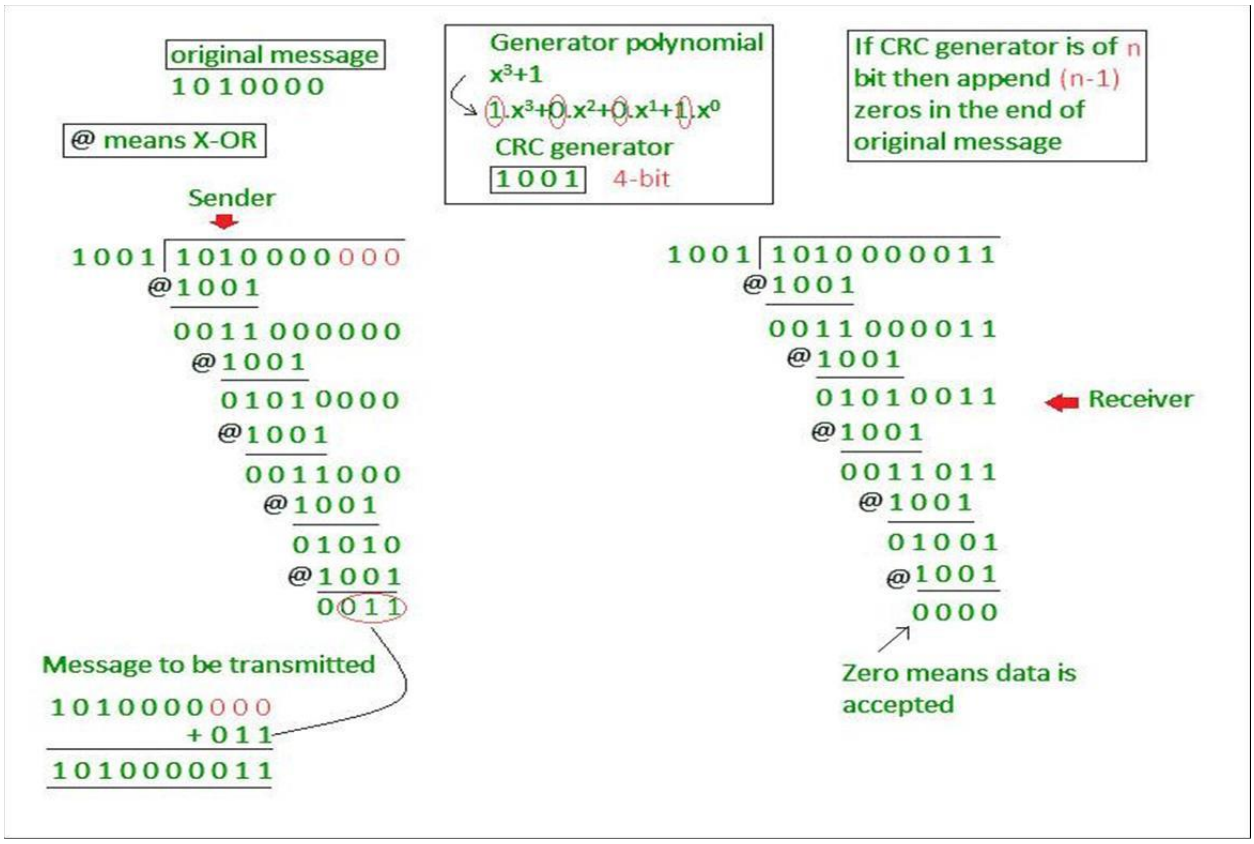
- The generator polynomial is $x5+x4+x2+1$; therefore, the divisor is 110101. The dividend will become 1010001101 + 0000 (number of bits(n) = highest degree of polynomial).
- Therefore the dividend = 101000110100000. Now, let us calculate the remainder by performing an XOR operation between bits.


110101
1 0 1 0 0 0 1 1 0 1 0 0 0 0
1 1 0 1 0 1
0 1 1 1 0 1 1
1 1 0 1 0 1
0 0 1 1 1 0 1 0
1 1 0 1 0 1
0 0 1 1 1 1 1 0
1 1 0 1 0 1
0 0 1 0 1 1 0 0
1 1 0 1 0 1
0 1 1 0 0 1 0
1 1 0 1 0 1
0 0 0 1 1 1 0
Remainder

AT THE RECEIVER END

As we can see the remainder is 0, which means that the receiver receives the correct data





- Send
  - M(x) = 11001 → x^5+x^4+x+1 (6 bits)
  - P(x) = 11001 → x^4+x^3+1 (5 bits, n = 4) → 4 bits of redundancy
  - Form $x^n M(x)$ → 11001 0000 → $x^9+x^8+x^5+x^4$
  - Divide $x^n M(x)$ by P(x) to find C(x)

```
          100001
11001 | 1100110000
        11001
        -----
        10000
        11001
        -----
         1001   = C(x)
```

Send the block 11001 1001

- Receive

```
11001 | 1100111001
        11001
        -----
            11001
            11001
            -----
            00000
```

No remainder → Accept

Error Correction: Once an error is detected, error correction techniques are used to recover the original data. Techniques include:

•**Stop-and-Wait ARQ**: The sender transmits a frame and waits for an acknowledgment before sending the next frame. If no acknowledgment is received, the sender retransmits the frame.

•**Go-Back-N ARQ**: The sender can send multiple frames before needing an acknowledgment, but if an error is detected, it goes back and retransmits the erroneous frame and all subsequent frames.

•**Selective Repeat ARQ**: The sender retransmits only the frames that were received in error, not the entire sequence of frames.

ARQ (Automatic Repeat reQuest)

ARQ (Automatic Repeat reQuest) protocols offer the following services:

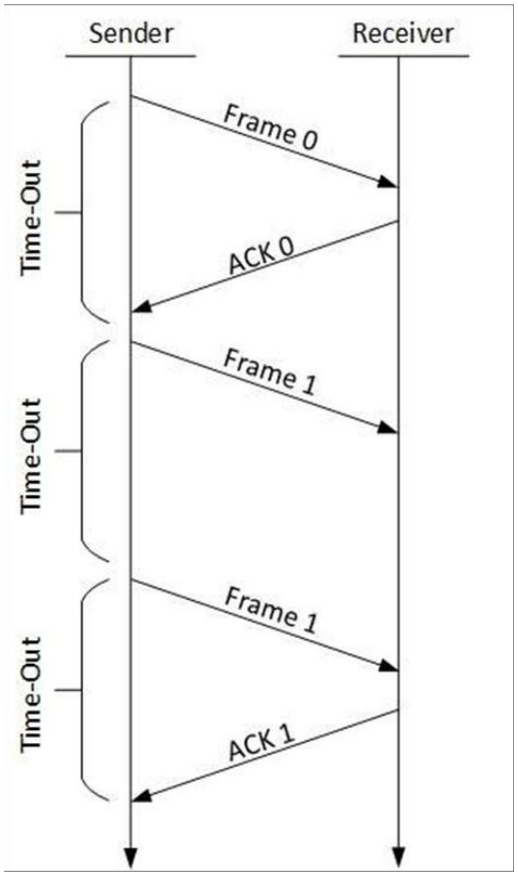
•**Packet Ordering**: Packets are delivered in the same order they are sent.

•**Loss-Free Delivery**: Packets are delivered without any losses.

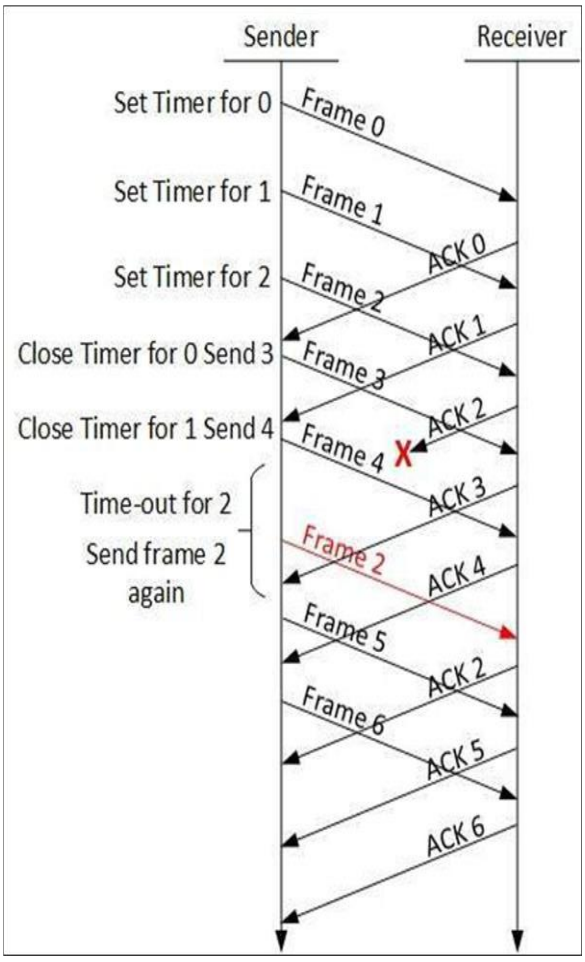
•**Error-Free Delivery**: Packets are guaranteed to be delivered without errors.

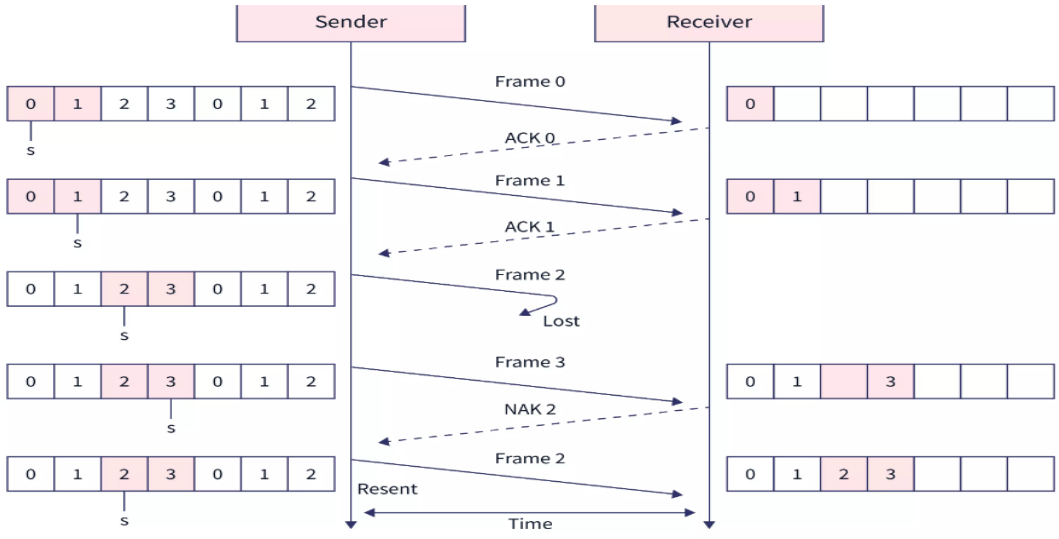
•ARQ protocols are based on retransmission. For example, in a conversation, you either let the speaker know you received the message with positive acknowledgment (e.g., "OK") or that you missed the message and want it repeated with negative acknowledgment (e.g., "Please repeat that.").

Stop-and-Wait ARQ:



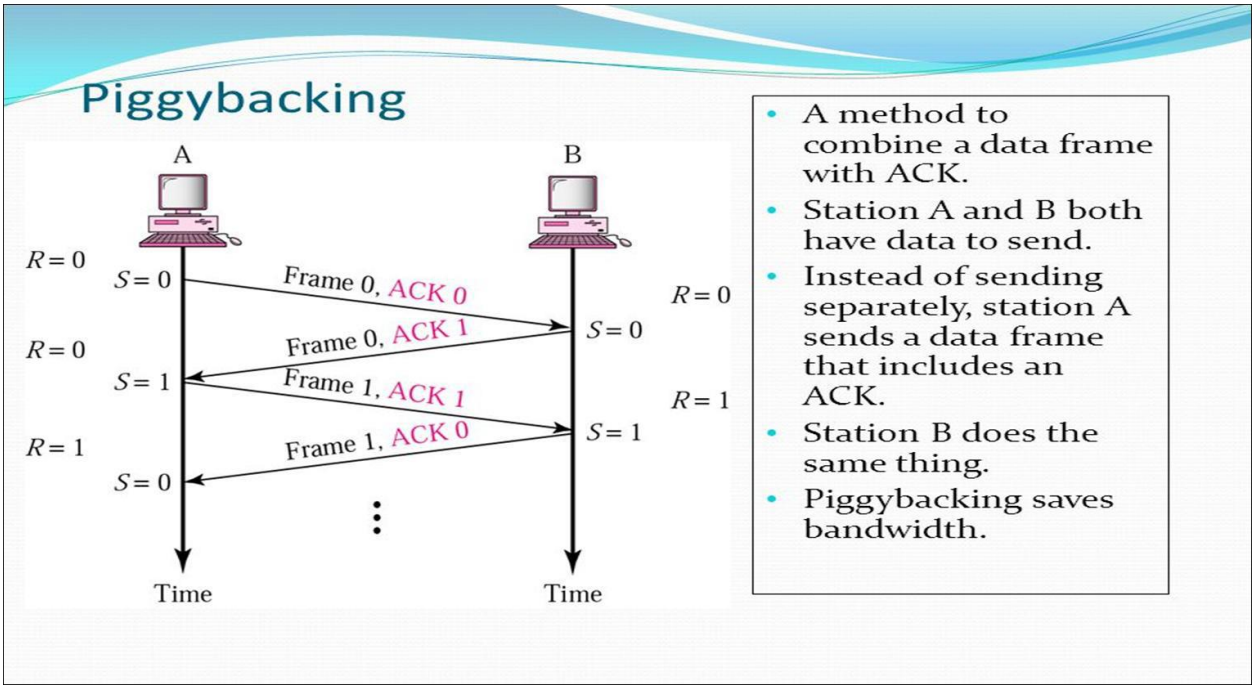
Go-Back-N ARQ:





Selective Repeat ARQ

Piggybacking



- Piggybacking is a process of attaching the acknowledgment with the data packet to be sent.

•Suppose there is two-way communication between two devices A and B. When the data frame is sent by A to B, then device B will not send the acknowledgment to A until B does not have the next frame to transmit. And the delayed acknowledgment is sent by the B with the data frame.

•The method of attaching the delayed acknowledgment with sending the data frame is known as piggybacking.

Channel Allocation Techniques

•Channel allocation techniques in the Data Link Layer are used to manage how multiple devices share a common communication medium.

•Multiple-access protocols are techniques used to allow multiple devices to share a communication channel efficiently.

•Multiple access protocols regulate how nodes transmit data onto a shared broadcast channel. Additionally, the coordination of these transmissions also utilizes the channel.

• A multiple access protocol employs a distributed algorithm to determine how stations share the channel, specifically deciding when a station can transmit.

•This communication about channel sharing also uses the channel itself.

Key aspects to consider in multiple access protocols include:

•Synchronous or asynchronous operation

•Information needed about other stations

•Robustness (e.g., resistance to channel errors)

•Performance

RANDOM ACCESS PROTOCOLS

- In a random access protocol, all stations have equal priority to send data over a channel.
- Each station independently decides to transmit based on whether the channel is idle or busy.
- If multiple stations transmit simultaneously, a collision can occur, leading to data loss or corruption, preventing the receiver from getting the data correctly.

ALOHA

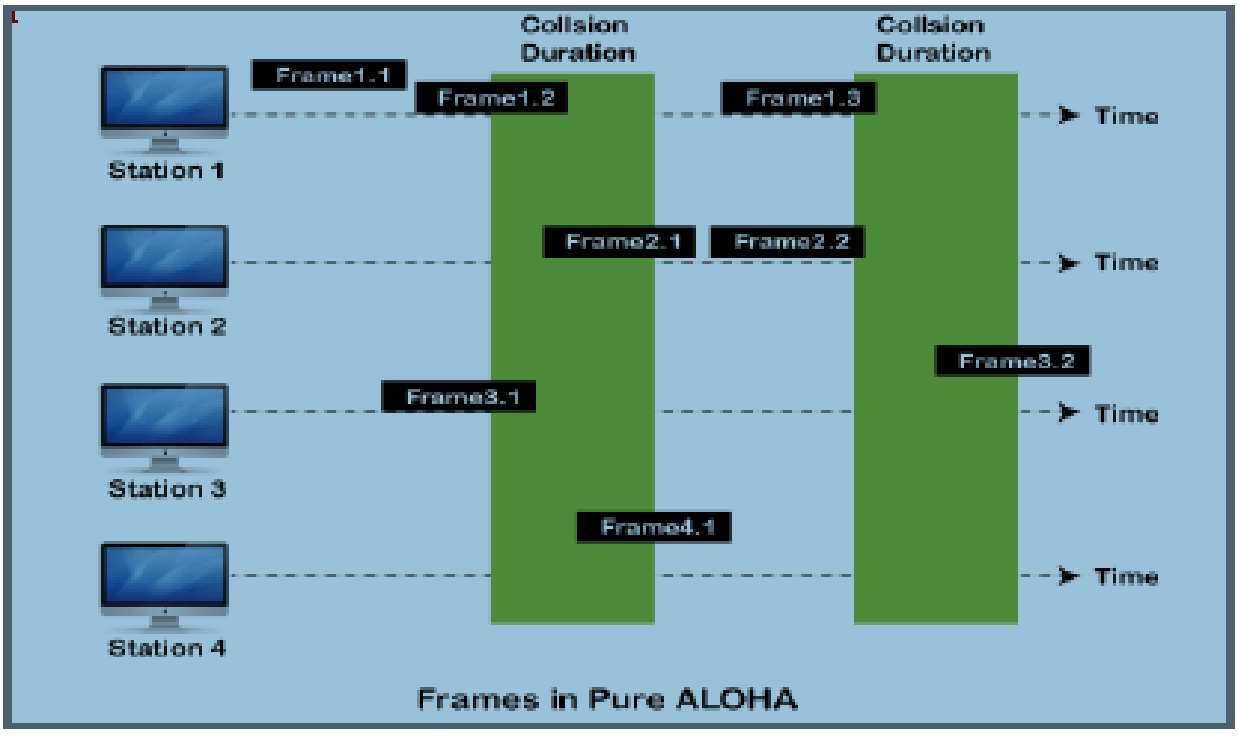
ALOHA, the earliest random access method, was developed at the University of Hawaii in the early 1970s.

Originally designed for a radio (wireless) LAN, it can be used on any shared medium.

Collisions are a potential issue in this arrangement, as the medium is shared among stations. When one station sends data, another station may attempt to transmit simultaneously, causing their data to collide and become corrupted.

Types: Pure ALOHA and Slotted ALOHA

PURE ALOHA



Sends a frame whenever it has data to transmit, leading to potential collisions since they all share a single channel.

with four stations, each sending two frames, collisions occur when multiple frames try to use the shared channel at the same two out of eight frames might successfully transmit without collision.

collisions happen, the frames need to be resent. Pure ALOHA relies on acknowledgments from the receiver.

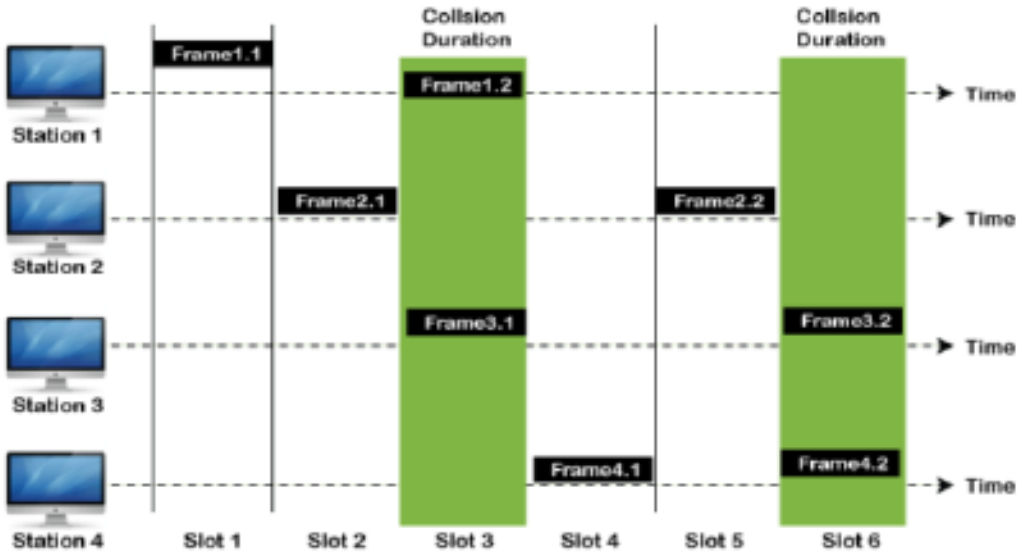
doesn't receive an acknowledgment after a timeout period, it resends the frame.

repeated collisions, each station waits a random amount of time before attempting to resend, known as the back-off time (TB).

channel congestion with retransmissions, Pure ALOHA limits the number of resend attempts.

reaching a maximum number of attempts (Kmax), a station will stop trying and wait before resending later. This approach helps network traffic and reduces persistent collisions.

SLOTTED ALOHA



Frames in Slotted ALOHA

•Slotted ALOHA was developed to improve the efficiency of Pure ALOHA, where collision chances are very high.

•In Slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.

•Stations can send a frame only at the beginning of a slot, with only one frame sent per slot.

•If a station misses the beginning of a slot, it must wait until the start of the next slot to send its frame.

•Although collisions can still occur if two stations transmit at the beginning of the same time slot, the probability of collision is reduced.

•Slotted ALOHA has an advantage over Pure ALOHA, as the chances of collision are reduced by half.

•This efficiency makes Slotted ALOHA a more effective protocol for managing network traffic.

CSMA

•CSMA (Carrier Sense Multiple Access) works by checking if the communication channel is free before sending data:

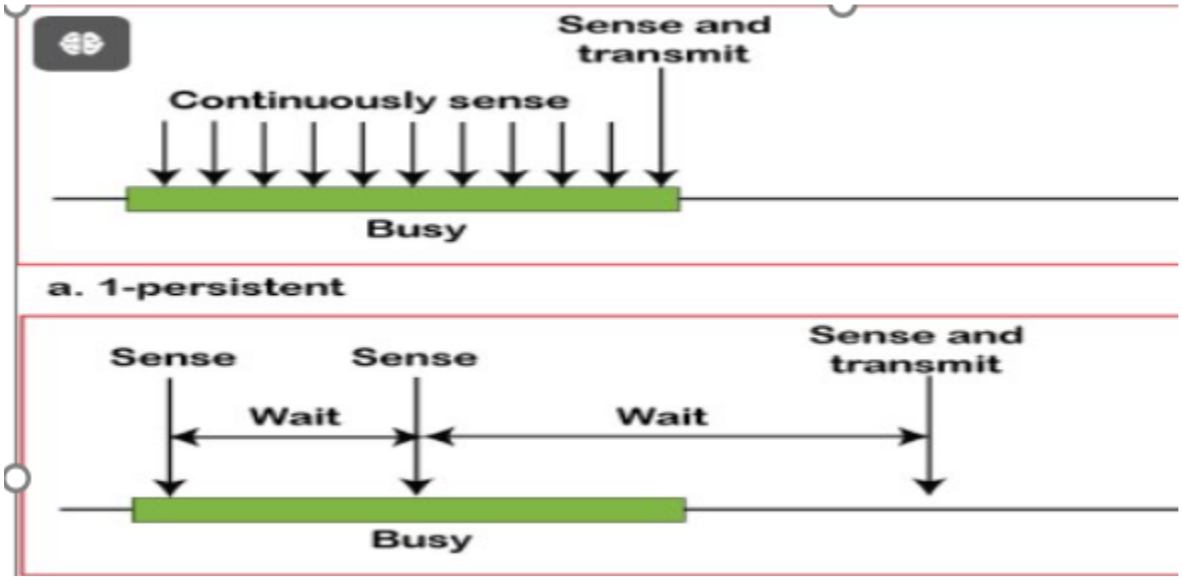
•**If the channel is idle:** You can send your entire message right away.

•**If the channel is busy:** Wait until it's free before sending to avoid interruptions and collisions.

Types of CSMA:

•**Persistent CSMA:** This approach involves retrying transmission immediately when the channel becomes idle. There's a probability p associated with retrying, which can lead to potential instability or increased collisions if many devices retry simultaneously.

•**Non-Persistent CSMA:** Here, after sensing the channel as busy, the device waits for a random period before attempting to transmit again. This random interval helps reduce collisions that might occur if multiple devices try to transmit at the same time after a busy period



CSMA/CD

CSMA/CD is a network protocol used to transmit data frames. It operates at the medium access control layer. Here's how it works:

Sensing the Channel: Before sending data, CSMA/CD checks if the channel is free.

Transmitting Data: If the channel is clear, it sends a data frame. After sending, it checks if the transmission was successful. **Handling Collisions:** If a collision occurs (when two stations send data simultaneously), CSMA/CD sends a stop

signal to halt transmission and then waits for a random time before trying again.

This protocol ensures efficient and collision-free communication over shared network channels.

CSMA/CA

•CSMA/CA is a network protocol used for transmitting data frames over a carrier. It operates at the medium access control layer. Here's how it works:

•**Sending Data Frames:** When a station sends a data frame to the channel, it waits for an acknowledgment to confirm if the channel is clear.

•**Acknowledgment Process:**

–If the station receives a single acknowledgment (its own), it confirms successful transmission to the receiver.

–If it receives two acknowledgments (its own and another due to a collision), it detects a frame collision on the shared channel.

This protocol helps manage data transmission efficiently by avoiding collisions and ensuring reliable communication over shared network channels.

Controlled Access Protocols

In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations.

Authorization Process:

•**Consultation Between Stations:** Stations communicate with each other to determine which one has the right to transmit.

•**Permission Requirement:** A station cannot initiate transmission unless it receives authorization from other stations or follows a specific protocol-defined sequence.

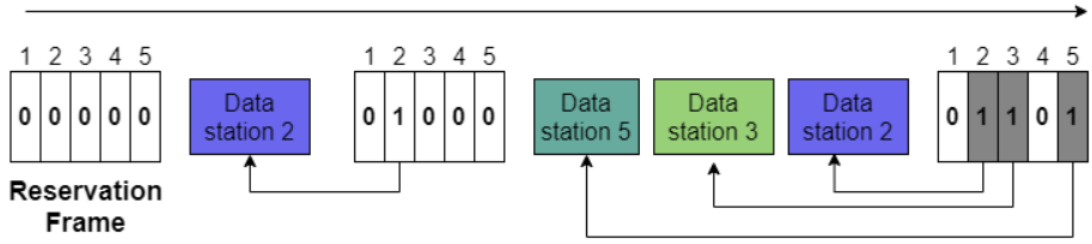
Examples

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

•**Token Passing:** Stations pass a token (a special control frame) to grant permission to transmit. Only the station holding the token can send data.

•**Polling:** A central controller (like a master station) polls individual stations to determine if they have data to send. Stations respond when polled, and only one station transmits at a time.

Reservation



•In this method, a station needs to make a reservation before sending the data.

•Time is mainly divided into intervals.

•Also, in each interval, a reservation frame precedes the data frame that is sent in that interval.

•Suppose if there are **'N'** stations in the system in that case there are exactly **'N'** reservation minislots in the reservation frame; where each minislot belongs to a station.

•Whenever a station needs to send the data frame, then the station makes a reservation in its own minislot.

•Then the stations that have made reservations can send their data after the reservation frame.

Example

•Let us take an example of 5 stations and a 5-minislot reservation frame. In the first interval, the station 2,3 and 5 have made the reservations. While in the second interval only station 2 has made the reservations.

Polling

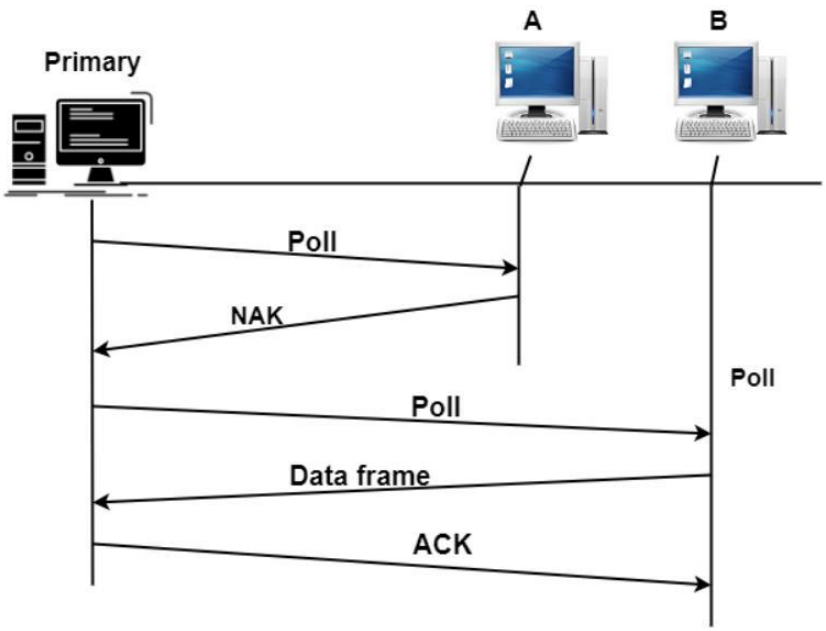
•Polling operates in network topologies where one device acts as the primary station and others as secondary stations.

•In a polling setup, a primary station controls communication among secondary stations in a network topology.

•All data exchanges, even those intended for secondary devices, must go through the primary device.

•The primary station dictates when each secondary device can use the channel, ensuring orderly access.

•Consequently, the primary station always initiates communication sessions.



Token Passing

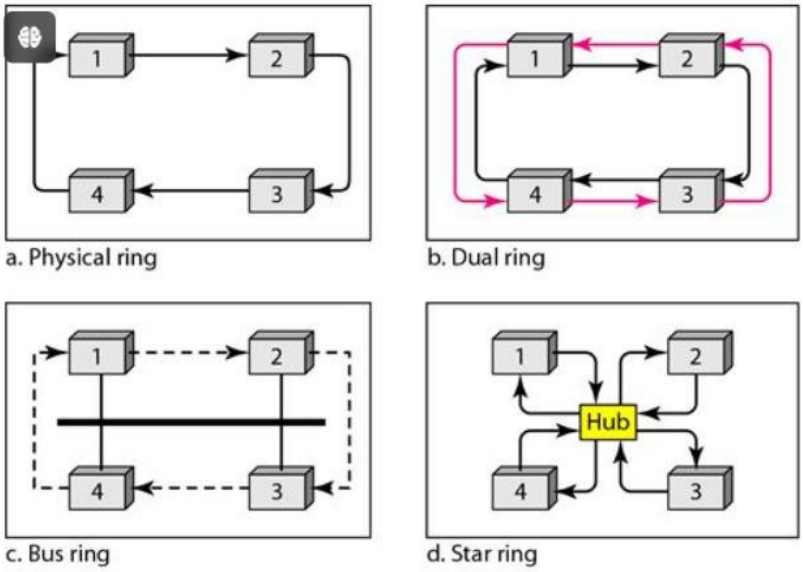
•In token passing, network stations are arranged in a logical ring where each station has a predecessor and a successor.

•The current station accessing the channel receives the right to do so from its predecessor via a circulating token packet.

•Possessing the token grants a station permission to send data. When a station has data to transmit, it waits to receive the token from its predecessor, sends its data, and then passes the token to the next station in the ring when finished.

• Stations without data simply pass the token along to the next station until needed again in the next cycle.

•Token management regulates token possession time, ensures token integrity, and assigns priorities among stations and data



Channelization

•Channelization is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations.

• Three channelization protocols are:

•FDMA(Frequency-Division Multiple Access)

•TDMA(Time-Division Multiple Access)

•CDMA(Code-Division Multiple Access)

Ethernet Standards

•Ethernet standards are defined by IEEE under the IEEE 802 standard, is the most popular local area network (LAN) technology in use today.

•It specifies the number of conductors required for connections, sets performance expectations, and provides a framework for data transmission.

Ethernet standards are expressed by using the following terminology.:

•Transmission speed, type of transmission, and length or type of cabling

The term **'100BaseT'** describes the following: -

•**100**: - The number *100* indicates that the standard data transmission speed of this media type is 100Mbps.

•**Base**: - The *'Base'* indicates that the media uses a baseband technology for transmission.

•**T**: - The letter *'T'* indicates that the media uses twisted-pair cabling.

•**10Base-T (IEEE 802.3)** – 10 Mbps with category 3 unshielded twisted pair (UTP) wiring, up to 100 meters long.

•**100Base-TX (IEEE 802.3u)** – known as Fast Ethernet, uses category 5, 5E, or 6 UTP wiring, up to 100 meters long.

•**100Base-FX (IEEE 802.3u)** – a version of Fast Ethernet that uses multi-mode optical fiber. Up to 412 meters long.

•**1000Base-CX (IEEE 802.3z)** – uses copper twisted-pair cabling. Up to 25 meters long.

•**1000Base-T (IEEE 802.3ab)** – Gigabit Ethernet that uses Category 5 UTP wiring. Up to 100 meters long.

•**1000Base-SX (IEEE 802.3z)** – 1 Gigabit Ethernet running over multimode fiber-optic cable.

•**1000Base-LX (IEEE 802.3z)** – 1 Gigabit Ethernet running over single-mode fiber.

•**10GBase-T (802.3.an)** – 10 Gbps connections over category 5e, 6, and 7 UTP cables.

Wireless LAN

•A Wireless Local Area Network (WLAN) is a type of local area network that uses wireless communication technology to connect devices within a limited area, such as a home, office, or campus.

•Unlike wired networks that use cables to connect devices, WLANs use radio waves to transmit data between devices and a central point, typically a wireless router or access point.

•**Standards:** Governed by the IEEE 802.11 family of standards : 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax, each with different characteristics and data rates.

•**Frequency Bands:** Typically operates in the 2.4 GHz and 5 GHz frequency bands.

•**Security:** Includes various security protocols to protect the network, such as WEP, WPA, WPA2, and WPA3. Ensures data privacy and prevents unauthorized access.

Virtual Circuit

•Virtual circuit is a communication method used in packet-switched networks to establish a logical path between two network devices, simulating a direct and dedicated connection.

• This path, though not a continuous physical link, allows for consistent and reliable data transmission as if the devices were directly connected.

•A virtual circuit creates a logical pathway through the network from the source device to the destination device.

•This pathway is maintained throughout the duration of the communication session, ensuring a consistent route for data packets.

Examples Virtual Circuit :

X.25: An early packet-switched network technology using virtual circuits for reliable, error-corrected communication over long distances.

Frame Relay:A high-speed packet-switched network technology that uses virtual circuits to handle bursty traffic patterns efficiently.

Asynchronous Transfer Mode (ATM):A cell-based network technology that uses small, fixed-size packets (cells) and virtual circuits for high-speed, QoS-enabled data transfer.

Frame Relay

•Frame Relay is a high-performance, cost-efficient, packet-switched wide area network (WAN) technology designed for transmitting data over long distances.

•It operates at the Data Link Layer (Layer 2) of the OSI model and is used to connect local area networks (LANs) and transfer data across WANs.

•Frame Relay is particularly suited for bursty data traffic and provides an efficient way to handle network traffic with minimal latency.

•FR originally was designed for use across Integrated Service Digital Network (ISDN) interfaces.

•Today, it is used over a variety of other network interfaces as well.

•FR is an example of a packet-switched technology.

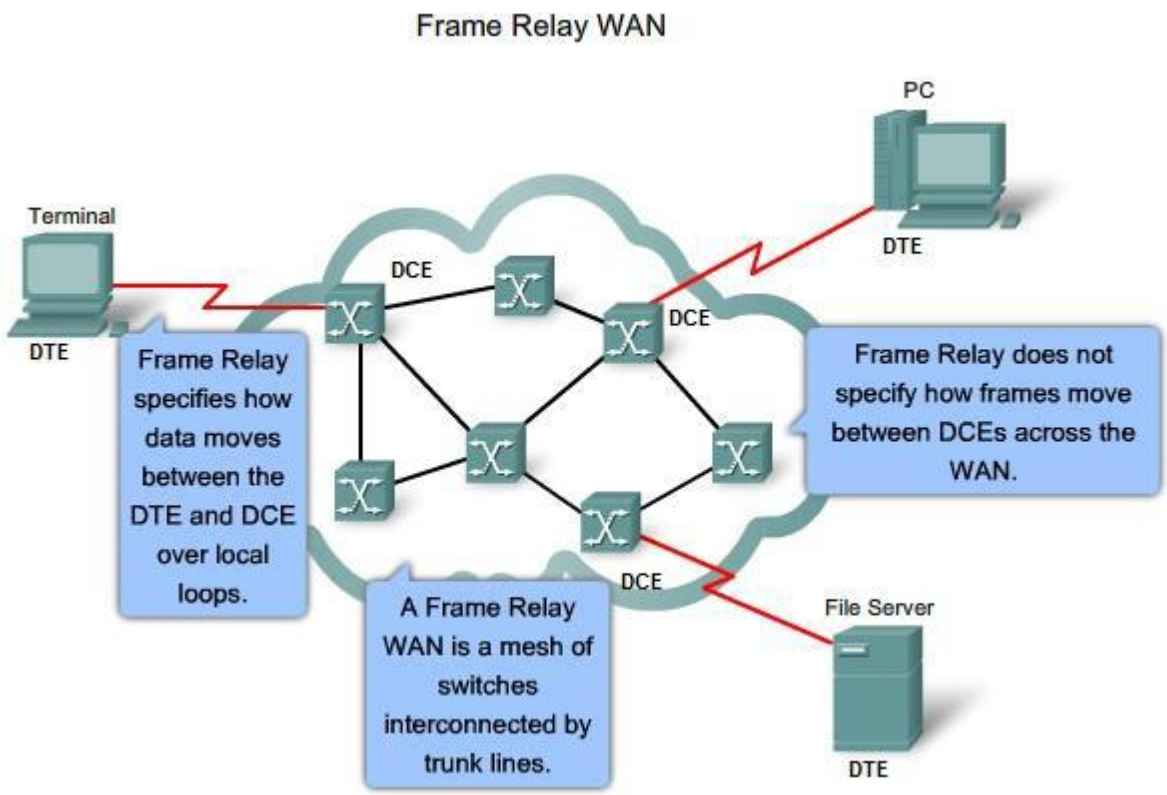
•Packet-switched networks enable end

How Frame Relay Works?

•The operation of Frame Relay involves the encapsulation of data into frames before transmission over the network.

•These frames are relayed from the source to the destination using fast packet-switching technology.

•The network relies on the endpoints to ensure data integrity, thus allowing the core network to maintain high speeds.



Frame Relay Devices

•Devices attached to a Frame Relay WAN fall into the following two general categories:

Data terminal equipment (DTE)

•DTEs generally are considered to be terminating equipment for a specific network and typically are located on the premises of a customer.

•Example of DTE devices are terminals, personal computers, routers, and bridges.

Data circuit-terminating equipment (DCE)

•DCEs are carrier-owned internetworking devices.

•The purpose of DCE equipments is to provide clocking and switching services in a network, which are the devices that actually transmit data through the WAN

ADVANTAGES

•**High-Speed Data Transfer**: Enables rapid information transmission.

•**Cost Efficiency**: Reduces need for dedicated physical connections.

•**Scalability**: Easily adjusts network capacity based on demand.

•**Reliability**: Ensures data integrity with error detection.

•**Improved Bandwidth Utilization**: Enhances data flow and reduces latency.

DISADVANTAGES

•**Unreliable Service**: It does not guarantee reliable delivery of packets.

•**Packet Order Not Maintained**: The order of arriving packets may not be preserved.

•**Dropped Erroneous Packets**: Erroneous packets are dropped without notification.

•**No Flow Control**: Frame Relay does not offer any flow control mechanisms.

•**Lack of Acknowledgement and Retransmission**: There is no provision for acknowledging received packets or controlling the retransmission of frames.

ATM

ATM stands for Asynchronous Transfer Mode.

It is a switching technique developed by integrating features from both telecommunications and computer networks. ATM uses cells to transfer various forms of information, such as voice, data, and video.

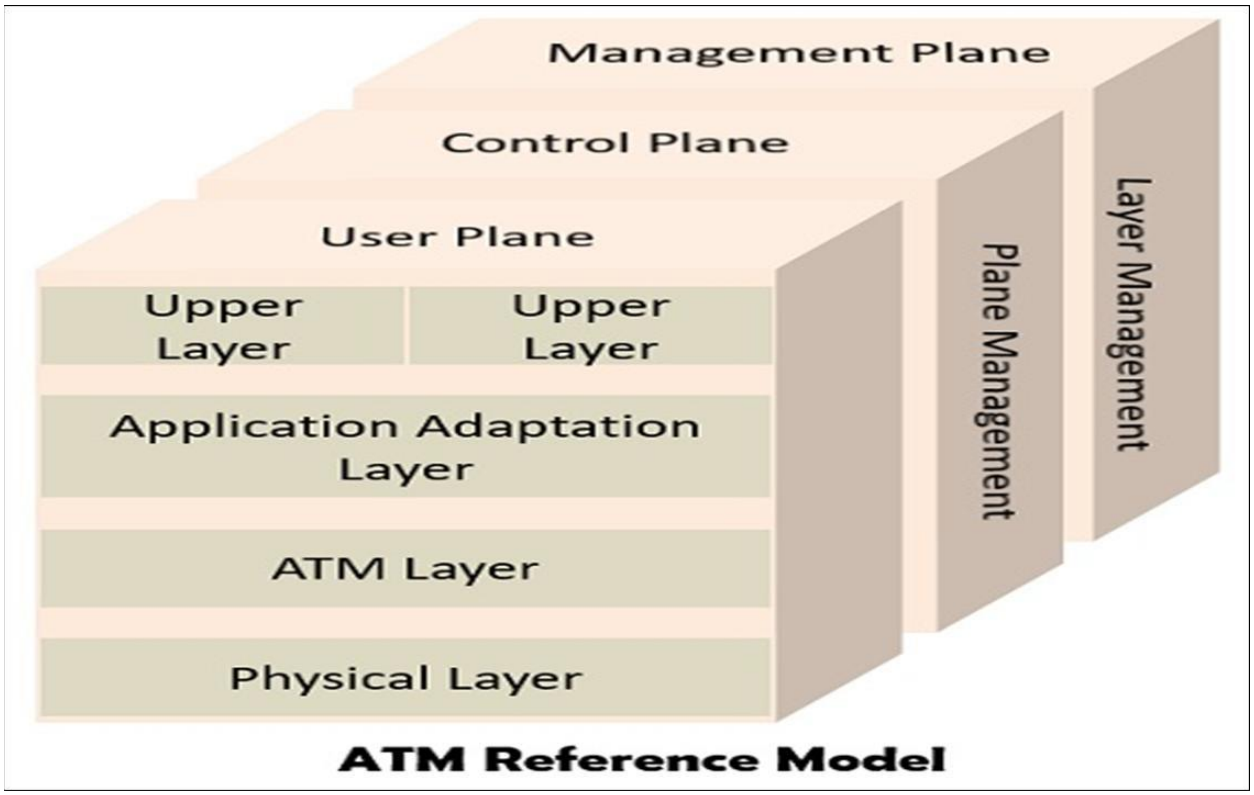
These cells are encoded using asynchronous time division multiplexing. By combining multiplexing and switching, ATM enables communication between devices operating at variable speeds and is well-suited for handling bursty traffic.

These cells are essentially collections of fixed-size packets.

These cells are transmitted asynchronously, and the network operates in a connection-oriented manner.

ATM Architecture

The ATM reference model consists of layers and planes as shown in the diagram. There are three basic layers in the ATM- physical, ATM and ATM AAL layer. Physical Layer: This layer of the ATM handles the medium dependent transmissions. ATM Layer: The ATM layer is similar to data link layer which enables the sharing of virtual circuits between the different users and transmission of the cells over the virtual circuit. Application Adaptation Layer (AAL): The AAL is responsible for hiding the ATM implementation details form the higher layers. It also transforms the data into 48 bit cell payloads.



Different Plane in ATM

Control: The main function of this plane is to produce and manage the signalling request.

User: This plane handles the transfer of the data.

Management: Layer related functions such as failure detection, problems regarding protocols are governed by this plane. It also involves the functions related to the complete system.

DISADVANTAGES

•Costly Equipment: Switching devices are expensive.

•Header Overhead: Significant overhead from cell headers.

•Complex QoS: Setting up Quality of Service (QoS) can be challenging.

ADVANTAGES

Compatibility: Easily interfaces with PSTN, ISDN, and operates over SONET (Synchronous Optical Network) and SDH (Synchronous Digital Hierarchy)

Versatility: Seamlessly integrates across LAN, MAN, and WAN networks.

Efficient Resource Use: Optimizes network resources for effective performance.

Noise Resistance: Less susceptible to signal degradation.

High Bandwidth: Provides ample bandwidth for high-speed data, voice, and video.

DLL Protocols:

•DLL (Data Link Layer) protocols are responsible for managing data transmission between two directly connected devices.

•They handle error detection, flow control, and framing of data packets.

DLL Protocols

•Ethernet

•Wi-Fi (IEEE 802.11)

•Token Ring

•FDDI (Fiber Distributed Data Interface)

•PPP (Point-to-Point Protocol)

•HDLC (High-Level Data Link Control)

•ATM (Asynchronous Transfer Mode)

•Frame Relay

•MPLS (Multiprotocol Label Switching)

•SLIP (Serial Line Internet Protocol)

HDLC

Frame format for HDLC protocol

•**HDLC (High-level Data Link Control)** is a WAN protocol intended to perform the encapsulation of the data in the data link layer. The encapsulation of the data means to change the format of the of the data.

•HDLC protocol follows the bit-oriented concept and uses bit stuffing for achieving data transparency. Here bit oriented approach signifies that the single bit is used to present the control information. The frame structure of HDLC contains the address, control, data, checksum and flag fields.

•The default encapsulation protocol in the Cisco devices is the HDLC. The Cisco proprietary HDLC only works when the devices in both of the ends of the link are of cisco. Standard HDLC can have different devices in the ends

Format of HDLC:

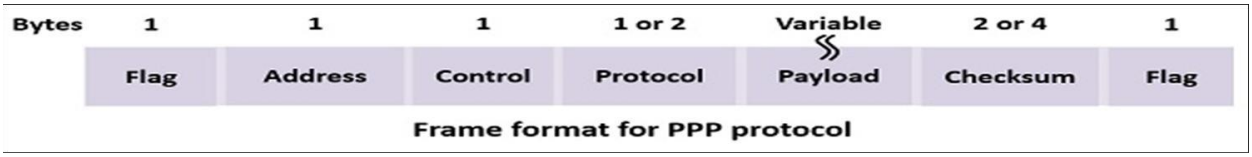
•**Address field** – It is used to describe the terminal.

•Control field – The bits in the control field is intended for the sequence number and acknowledgements.

•**Data field** – This field is used to hold the information.

•**Checksum field** -In this field, the bits are reserved for the performing the cyclic redundancy code.

PPP



Frame format for PPP protocol

PPP (Point-to-Point Protocol) is also a WAN protocol, but there are several enhancements made in the PPP protocol after HDLC.
• Priorily, the PPP protocol is not proprietary, which means that it can be used with two different type of devices without committing changes over the format of the data. All of the links collaboratively treated as single, independent IP network which is having its own frame format, hardware addressing method, and data link protocol.

• A point-to-point connection is obtained without assigning multiple IP addresses to the tangible wires, and it just needs the IP network number.

•The PPP frame contains two flag fields, a **protocol** filed to determine the type of packet residing in the **payload**, and a payload field which can variate. However, the rest of the fields are the same as the HDLC protocol.

•**Address field** – It is used to describe the terminal.

•**Control field** – The bits in the control field is intended for the sequence number and acknowledgements.

•**Data field** – This field is used to hold the information.

•**Checksum field** -In this field, the bits are reserved for the performing the cyclic redundancy code.