Why does a data link layer protocol generally doesn't handle error correction?

Data Link Layer focuses on smooth local network communication, leaving error correction to the Transport Layer for better overall performance and flexibility.

Write eight differences between circuit switched and packet switched networks.

Circuit Switched Network	Packet Switched Network
A dedicated path is created between two points	A dedicated path is not created. Only the virtual circuit exists.
Requires simple protocols for delivery.	Requires complex protocols for delivery.
Low installation cost	High installation cost
Fixed Bandwidth	Variable Bandwidth
Fixed route is followed by packets	Variable route is followed by packets
Call setup is required.	Call setup is not required.
Congestion can occur at set up time.	Congestion can occur on every packet.
More reliable	Less reliable

Explain different types of noises.

- **Thermal noise:** is generated due to the random motion of electrons in a wire. It can be reduced by reducing the temperature.
- **Induced noise:** is generated in a circuit by a varying magnetic or electrostatic field produced by another circuit. It can be reduced by using twisted pair cable
- **Crosstalk:** happens when *signal in one wire affects the signal in the other wire.* It can be reduced by using twisted pair cable
- **Impulse**: is a signal with high energy.

What do you mean by transmission mode? Explain different transmission modes.

The way in which data is transmitted from one device to another device is called **transmission mode**.

There are three types of transmission mode:

1. **Simplex Mode**: In Simplex mode, the communication is unidirectional. Only one of the two devices on a link can transmit, the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction. Example: Keyboard and traditional monitors.
2. **Half-Duplex Mode:** In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time. The entire capacity of the channel can be utilized for each direction.
   Example: Walkie-talkie
   Channel capacity=Bandwidth * Propagation Delay

3. **Full-Duplex Mode**: In full-duplex mode, both stations can transmit and receive simultaneously. It is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.
   Example: Telephone Network

   Channel Capacity=2* Bandwidth*propagation Delay

Explain KARN's algorithm.

KARN's Algorithm provide accurate RTT (Round-Trip Time) estimates for reliable data transfer and congestion control.

KARN's Algorithm

1. **Initial RTT:** Measure RTT for a segment successfully transmitted without retransmissions.
2. **Retransmission Dilemma:** If a segment is retransmitted, don't update RTT based on its timing (ambiguity).
3. **Delayed RTT Update:** Upon acknowledgment for a retransmitted segment, delay RTT update until a new segment is successfully transmitted without retransmission. Use that segment's timing for the update.

Explain tunnelling a packet in a WAN.

1. **Encapsulation:** The original packet is wrapped inside a new packet header, forming a "tunnel packet." This header contains information for tunneling, such as routing instructions and security measures.

2. **Transmission:** The tunnel packet is sent through the WAN, using the tunneling protocol's routing mechanisms. The WAN only sees the outer header, keeping the original packet's contents hidden.

3. **Decapsulation:** Upon reaching the destination, the tunnel packet is unwrapped, removing the outer header. The original packet is extracted and delivered to its intended recipient.

What are the advantages of IPv6 over IPv4.

1. IPv6 has 128-bit address space compared to IPv4's 32-bit space.
2. IPv6 has a simpler header compared to IPv4, reducing processing overhead and improving network efficiency.
3. IPv6 utilizes hierarchical addressing, making routing tables smaller and more efficient.

4. IPv6 has security features at the protocol level
5. IPv6 provides built-in support for Quality of Service features

Explain the Go Back N ARQ protocol with the help of windows

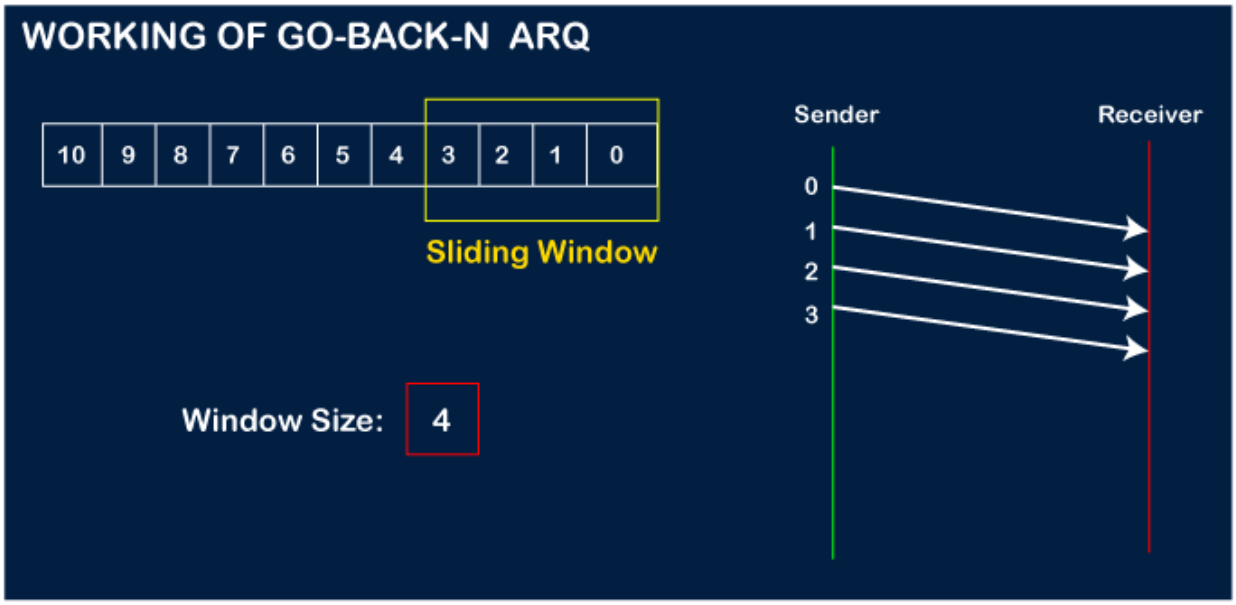
In Go-Back-N ARQ, **N** is the sender's window size. Suppose we say that Go-Back-3, which means that the three frames can be sent at a time before expecting the acknowledgment from the receiver.

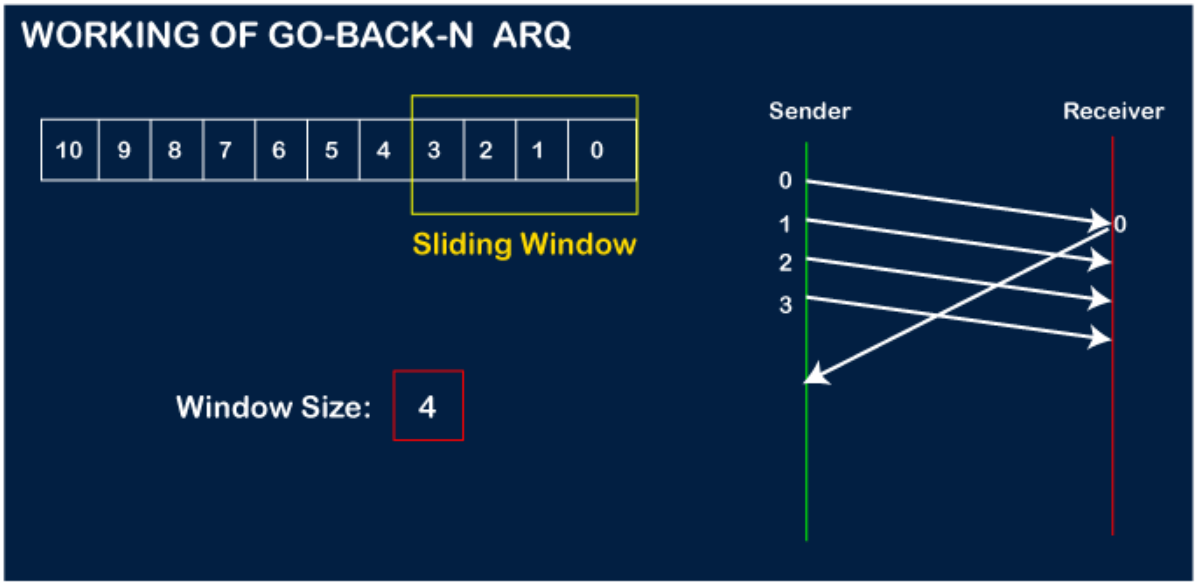
It uses the principle of protocol pipelining in which the multiple frames can be sent before receiving the acknowledgment of the first frame.

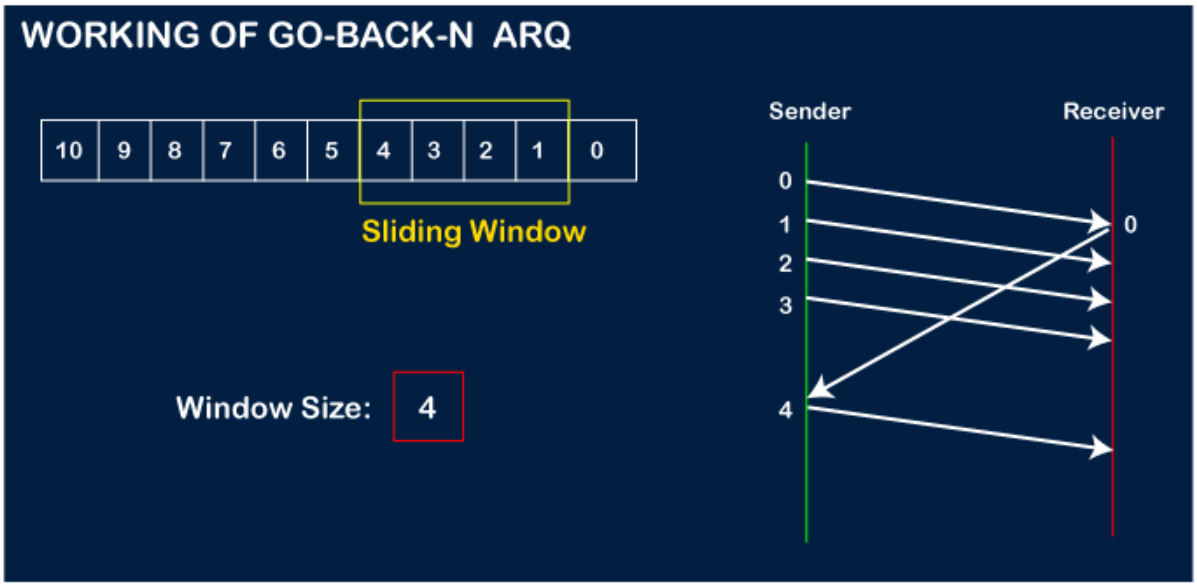
If the acknowledgment of a frame is not received within an agreed-upon time period, then all the frames available in the current window will be retransmitted.

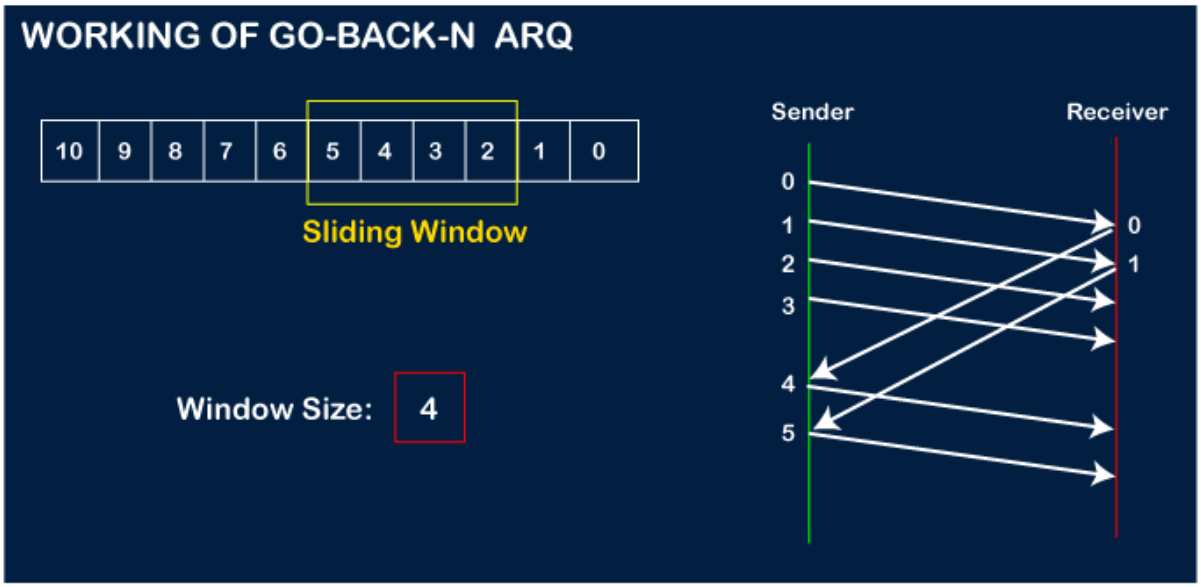
Example:

Suppose there are a sender and a receiver, and let's assume that there are 11 frames to be sent. These frames are represented as 0,1,2,3,4,5,6,7,8,9,10. Let's consider the window size as 4, which means that the four frames can be sent at a time before expecting the acknowledgment of the first frame.

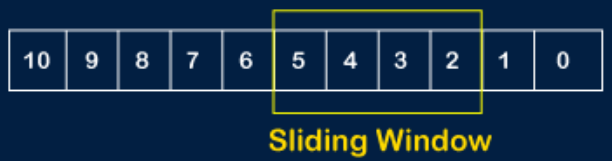



WORKING OF GO-BACK-N ARQ
10 9 8 7 6 5 4 3 2 1 0
Sliding Window
Window Size: 4
Sender
Receiver
0
1
2
3
0

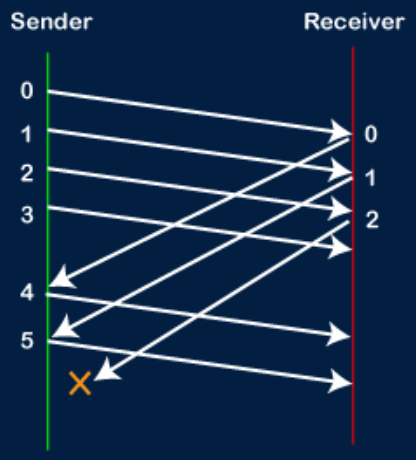

WORKING OF GO-BACK-N ARQ
10 9 8 7 6 5 4 3 2 1 0
Sliding Window
Window Size: 4
Sender
Receiver
0
1
2
3
4
0


WORKING OF GO-BACK-N ARQ
10 9 8 7 6 5 4 3 2 1 0
Sliding Window
Window Size: 4
Sender
Receiver
0
1
2
3
4
5
0
1

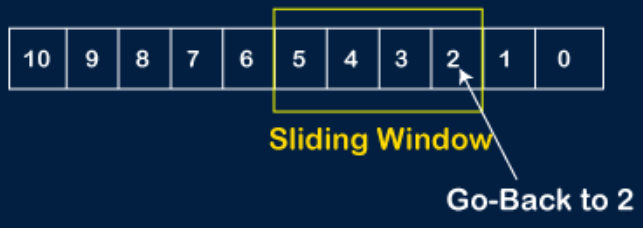
WORKING OF GO-BACK-N ARQ



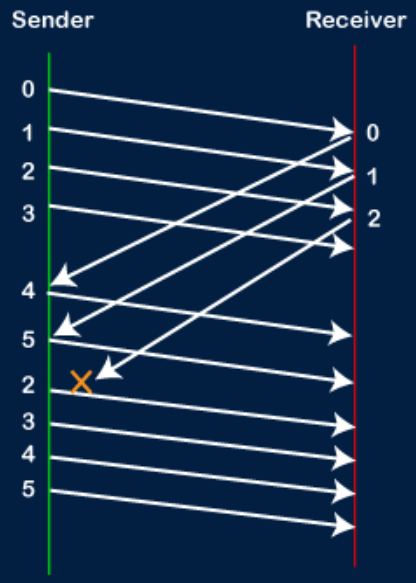
Window Size: 4



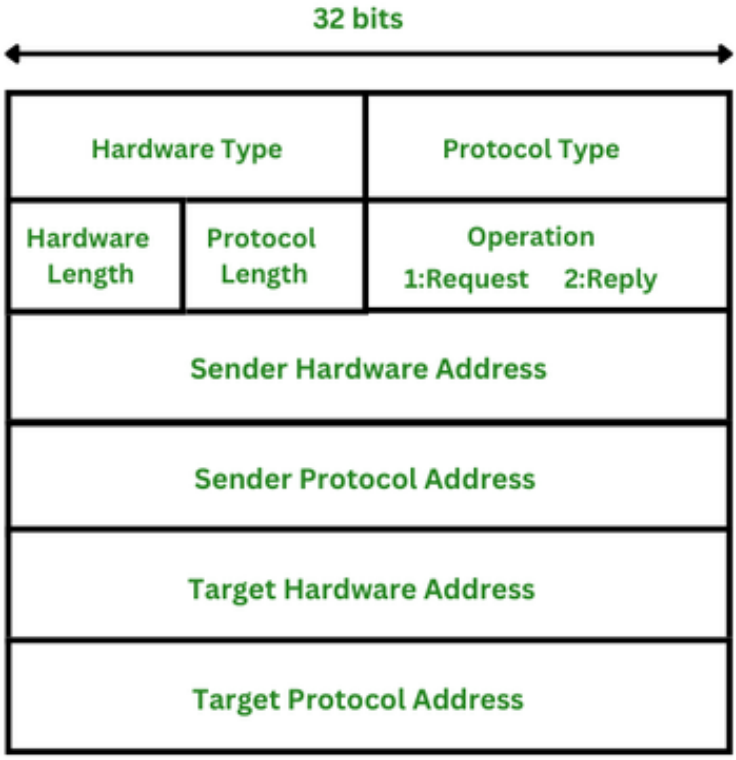
WORKING OF GO-BACK-N ARQ



Window Size: 4



Draw ARP packet format.



Hardware type: This is 16 bits field defining the type of the network on which ARP is running.

Protocol type: This is 16 bits field defining the protocol.

Hardware length: This is an 8 bits field defining the length of the physical address in bytes.

Protocol length: This is an 8 bits field defining the length of the logical address in bytes.

Operation (**request or reply):** This is a 16 bits field defining the type of packet.

Sender hardware address: This is a variable length field defining the physical address of the sender.

Sender protocol address: This is also a variable length field defining the logical address of the sender

Target hardware address: This is a variable length field defining the physical address of the target.

Target protocol address: This is also a variable length field defining the logical address of the target.

Draw flow diagram for stop and wait ARQ protocol and explain

Sender side

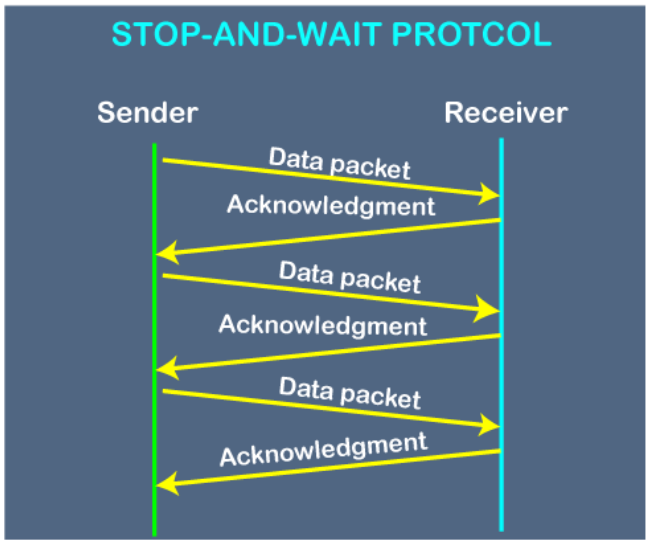
Rule 1: Sender sends one data packet at a time.

Rule 2: Sender sends the next packet only when it receives the acknowledgment of the previous packet.

Receiver side

Rule 1: Receive and then consume the data packet.

Rule 2: When the data packet is consumed, receiver sends the acknowledgment to the sender.



Problems in Stop and Wait ARQ protocol

1. If the data is lost
   i. Sender waits for an infinite amount of time for an acknowledgment.
   ii. Receiver waits for an infinite amount of time for a data.
2. If acknowledgement is lost, sender waits for an infinite amount of time for an acknowledgment.
3. If the acknowledgement is delayed, acknowledgment is wrongly considered as the acknowledgment of some other data packet.

Explain congestion control in TCP in detail.

1. **Slow Start Phase (Exponential increment)**: In this phase after every RTT the congestion window size increments exponentially.

   Example:- If the initial congestion window size is 1 segment, and the first segment is successfully acknowledged, the congestion window size becomes 2 segments. If the next transmission is also acknowledged, the congestion window size doubles to 4 segments.

2. **Congestion Avoidance Phase (Additive increment):** This phase starts after the threshold value. The size of congestion window increases additive.

   Example:- if the congestion window size is 20 segments and all 20 segments are successfully acknowledged within an RTT, the congestion window size would be increased to 21 segments in the next RTT.

3. **Congestion Detection Phase (Multiplicative decrement):** If congestion occurs, the congestion window size is decreased.

   Retransmission can occur in one of two cases:
   Case 1: Retransmission due to Timeout – In this case, the congestion possibility is high.
   Case 2: Retransmission due to 3 Acknowledgement Duplicates – The congestion possibility is less.

Differentiate between UDP and TCP. What are present in TCP header but not present in the UDP header? Discuss their significance and reasons for not being there in UDP header.

Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
Connection-oriented protocol.	Datagram-oriented protocol.
Reliable	Not reliable
Provides extensive error-checking mechanisms.	Provides basic error-checking mechanism
Acknowledgment segment is present.	Acknowledgment segment is absent.
Slower	Faster
Retransmission of lost packets is possible	Retransmission of lost packets is impossible
Doesn’t support Broadcasting.	Supports Broadcasting.
(20-60) bytes variable length header.	8 bytes fixed-length header.
Connection is a byte stream.	Connection is a message stream.

1. **Sequence Number:**

- Significance: Ensures in-order delivery of data
- Reason for Absence in UDP: It doesn't require in-order delivery.

2. **Acknowledgment Number:**

- Significance: Acknowledges receipt of successful data packets, enabling retransmission of lost or corrupted ones.
- Reason for Absence in UDP: UDP applications often tolerate some data loss or handle it at higher layers

3. **Window Size:**

- Significance: Controls the flow of data
- Reason for Absence in UDP: UDP considers flow control less essential.

Why do we need a DNS when we can directly use an IP address? To find the IP address of a destination we need the service of DNS. DNS need the services of UDP or TCP. UDP or TCP need the services of IP. IP need an IP destination address. Is this a vicious cycle here? If not, who breaks this cycle and how?

Need of DNS

1. DNS translates human-readable domain names into machine-readable IP addresses
2. DNS allows us to use meaningful domain names that are easy to remember
3. DNS servers maintain a hierarchical database of domain names and IP addresses

Breaking the Cycle: Local Knowledge and Caching:

1. **Initial Bootstrapping:** When a device first connects to a network, it receives essential IP configuration information, including the IP addresses of DNS servers to use.
2. **Caching:** Once a DNS server resolves a domain name, it stores the IP address in its cache for a certain period. Subsequent requests for the same domain can be answered directly from the cache.
3. **Local Host Files:** Operating systems can maintain a local "hosts" file that maps domain names to IP addresses, bypassing DNS lookups for known destinations.

Differentiate in between public and private key cryptography. Illustrate through an example.

Private Key Cryptography	Public Key Cryptography
Same key is used to encrypt and decrypt the message.	Two keys are used, one for encryption, and other for decryption.
It is faster	It is slower
The key is kept a secret.	One of the two keys is kept a secret.
It is Symmetrical	It is Asymmetrical
It is efficient	It is inefficient
It is used for large messages	It is used for short messages
It is used to protect data storage devices.	It is used to secure web sessions and emails.

Example of private key cryptography:

- Alice and Bob share a secret key.
- Alice encrypts a message using the shared key.
- Bob decrypts the message using the same shared key.

Example of public key cryptography:

- Alice wants to send a secure message to Bob.
- Bob shares his public key with Alice.
- Alice encrypts the message using Bob's public key.
- Only Bob, with his private key, can decrypt the message.