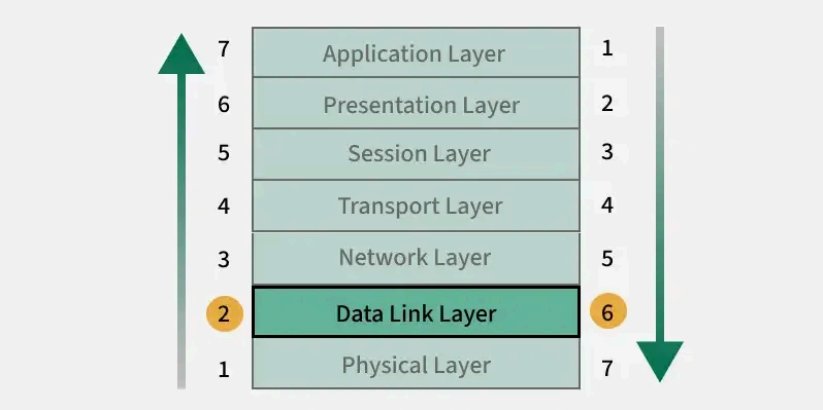
Data Link Layer in OSI Model

Last Updated : 31 Jan, 2025

The data link layer is the second layer from the bottom in the OSI (Open System Interconnection) network architecture model. It is responsible for the node-to-node delivery of data within the same local network. Its major role is to ensure error-free transmission of information. DLL is also responsible for encoding, decoding, and organizing the outgoing and incoming data.

This is considered the most complex layer of the OSI model as it hides all the underlying complexities of the hardware from the other above layers. In this article, we will discuss Data Link Layer in Detail along with its functions, and sub-layers.



Data Link Layer in OSI Model

Sub-Layers of The Data Link Layer

The data link layer is further divided into two sub-layers, which are as follows:

Logical Link Control (LLC)

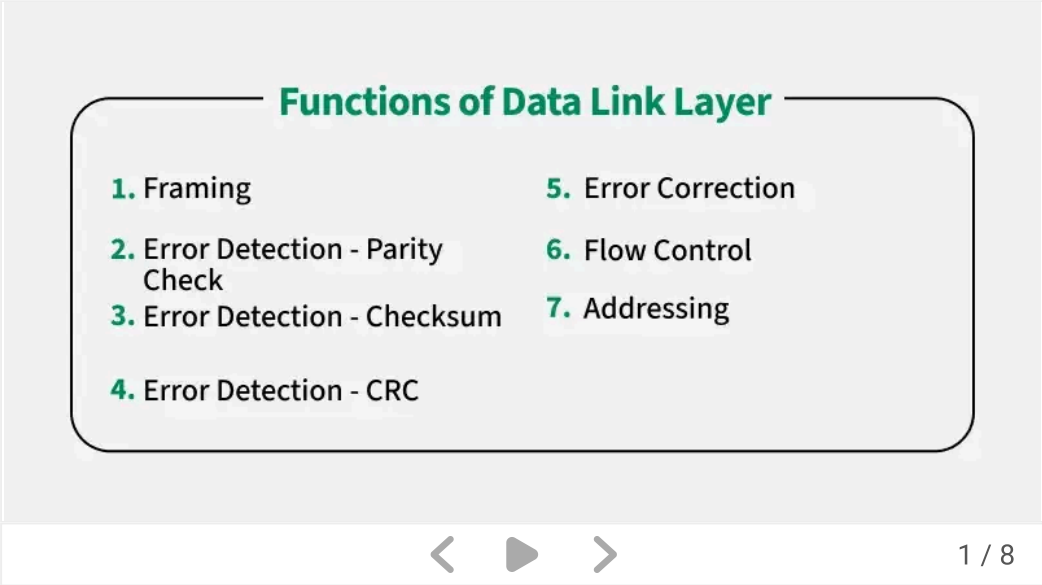
This sublayer of the data link layer deals with multiplexing, the flow of data among applications and other services, and LLC is responsible for providing error messages and acknowledgments as well.

Media Access Control (MAC)

MAC sublayer manages the device's interaction, responsible for addressing frames, and also controls physical media access. The data link layer receives the information in the form of packets from the Network layer, it divides packets into frames and sends those frames bit-by-bit to the underlying physical layer.

Functions of The Data-link Layer

There are various benefits of data link layers s let's look into it.



To read in detail about services offered by this layer, refer to Data Link Layer Services.

Protocols in Data link layer

There are various protocols in the data link layer, which are as follows:

- Synchronous Data Link Protocol (SDLC)
- High-Level Data Link Protocol (HDLC)
- Serial Line Interface Protocol (SLIP)
- Point to Point Protocol (PPP)
- Link Access Procedure (LAP)
- Link Control Protocol (LCP)
- Network Control Protocol (NCP)

Devices Operating at the Data Link Layer

1.Switch

- A switch is a key device in the Data Link Layer.
- It uses **MAC addresses** to forward data frames to the correct device within a network.
- Works in **local area networks (LANs)** to connect multiple devices.

2. Bridge

- A bridge connects two or more LANs, creating a single, unified network.
- Operates at the Data Link Layer by forwarding frames based on **MAC addresses**.
- Used to reduce network traffic and segment a network.

3. Network Interface Card (NIC)

- A NIC is a hardware component in devices like computers and printers.
- Responsible for adding the **MAC address** to frames and ensuring proper communication with the network.
- Operates at the Data Link Layer by preparing and sending frames over the physical medium.

4. Wireless Access Point (WAP)

- A WAP allows wireless devices to connect to a wired network.
- Operates at the Data Link Layer by managing **wireless MAC addresses**.
- Uses protocols like Wi-Fi (IEEE 802.11) to communicate with devices.

5. Layer 2 Switches

- These are specialized switches that only operate at Layer 2, unlike multi-layer switches.

- Responsible for **frame forwarding** using MAC address tables.

Limitations of Data Link Layer

- **Limited Scope**: It operates only within a local network and cannot handle end-to-end communication across different networks.
- **Increased Overhead**: Adding headers, trailers, and redundant data (for error correction) increases the size of transmitted data.
- **Error Handling Dependency**: While it can detect and correct some errors, it relies on upper layers for handling more complex issues.
- **No Routing Capability**: The Data Link Layer cannot make routing decisions. It only ensures delivery within the same network segment.
- **Resource Usage**: Flow control and error correction mechanisms may consume extra processing power and memory

Applications of Data Link Layer

- **Local Area Networks (LANs)**: Enables reliable communication between devices within a local network using protocols like Ethernet (IEEE 802.3).
- **Wireless Networks (Wi-Fi)**: Manages communication between devices in wireless networks via protocols like IEEE 802.11 hence, handling media access and error control.
- **Switches and MAC Addressing**: Facilitates the operation of switches by using MAC addresses to forward data frames to the correct device within the network.
- **Point-to-Point Connections**: Used in protocols like PPP (Point-to-Point Protocol) to establish and manage direct communication between two nodes.

Below questions have been asked in previous GATE exam on above topic:

GATE | GATE-CS-2003 | Question 90

GATE | GATE-CS-2005 | Question 74

GATE | GATE CS 2013 | Question 65

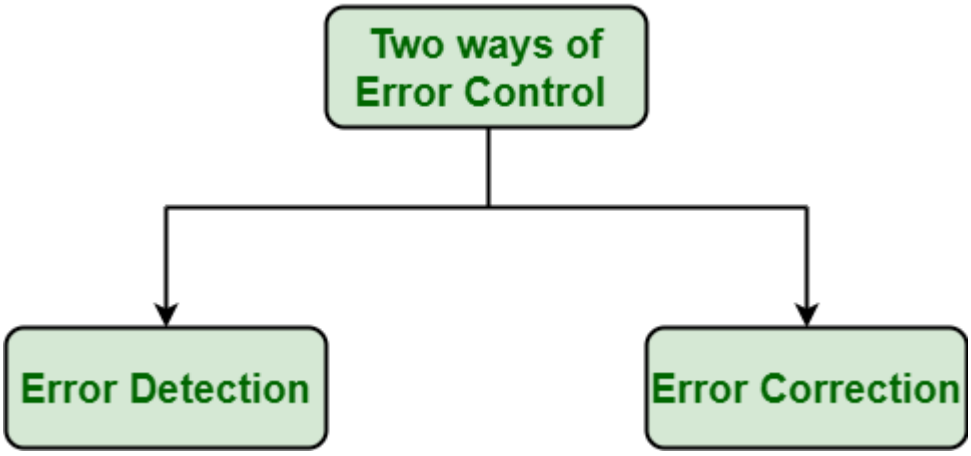
GATE | GATE CS 2015 Set 3 | Question 65

Error Control in Data Link Layer

Last Updated : 28 Dec, 2024

Data-link layer uses the techniques of error control simply to ensure and confirm that all the data frames or packets, i.e. bit streams of data, are transmitted or transferred from sender to receiver with certain accuracy. Using or providing error control at this data link layer is an optimization, it was never a requirement. Error control is basically process in data link layer of detecting or identifying and re-transmitting data frames that might be lost or corrupted during transmission. In both of these cases, receiver or destination does not receive correct data frame and sender or source does not even know anything about any such loss regarding data frames. Therefore, in such type of cases, both sender and receiver are provided with some essential protocols that are required to detect or identify such types of errors as loss of data frames. The Data-link layer follows a technique known as re-transmission of frames to detect or identify transit errors and also to take necessary actions that are required to reduce or remove such errors. Each and every time an error is detected during transmission, particular data frames are retransmitted and this process is known as ARQ (Automatic Repeat Request).

Ways of doing Error Control : There are basically two ways of doing Error control as given below :



Ways of Error Control

1. **Error Detection :** Error detection, as the name suggests, simply means detection or identification of errors. These errors may occur due to noise or any other impairments during transmission from transmitter to the receiver, in communication system. It is a class of techniques for detecting garbled i.e. unclear and distorted data or messages.
2. **Error Correction :** Error correction, as the name suggests, simply means correction or solving or fixing of errors. It simply means reconstruction and rehabilitation of original data that is error-free. But error correction method is very costly and very hard.

Various Techniques for Error Control : There are various techniques of error control as given below :

1. Stop-and-Wait ARQ : Stop-and-Wait ARQ is also known as alternating bit protocol. It is one of the simplest flow and error control techniques or mechanisms. This mechanism is generally required in telecommunications to transmit data or information between two connected devices. Receiver simply indicates its readiness to receive data for each frame. In these, sender sends information or data packets to receiver. Sender then stops and waits for ACK (Acknowledgment) from receiver. Further, if ACK does not arrive within given time period i.e., time-out, sender then again resends frame and waits for ACK. But, if sender receives ACK, then it will transmit the next data packet to receiver and then again wait for ACK from receiver. This process to stop and wait continues until sender has no data frame or packet to send.

2. Sliding Window ARQ : This is generally used for

continuous transmission error control. It is further categorized into two categories as given below :

- **Go-Back-N ARQ :** Go-Back-N ARQ is form of ARQ protocol in which transmission process continues to send or transmit total number of frames that are specified by window size even without receiving an ACK (Acknowledgement) packet from the receiver. It uses sliding window flow control protocol. If no errors occur, then operation is identical to sliding window.
- **Selective Repeat ARQ :** Selective Repeat ARQ is also form of ARQ protocol in which only suspected or damaged or lost data frames are only retransmitted. This technique is similar to Go-Back-N ARQ though much more efficient than the Go-Back-N ARQ technique due to reason that it reduces number of retransmission. In this, the sender only retransmits frames for which NAK is received. But this technique is used less because of more complexity between sender and receiver and each frame must be needed to be acknowledged individually.

The main difference between Go Back ARQ and Selective Repeat ARQ is that in Go Back ARQ, the sender has to retransmit the whole window of frame again if any of the frame is lost but in Selective Repeat ARQ only the data frame that is lost is retransmitted.

Next Article

Flow Control in Data Link Layer

Error Detection in Computer Networks

Last Updated : 31 Jan, 2025

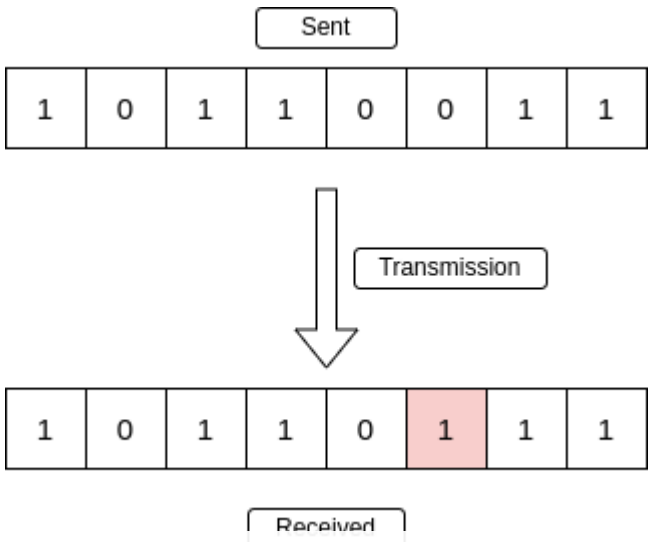
Error is a condition when the receiver's information does not match the sender's. Digital signals suffer from noise during transmission that can introduce errors in the binary bits traveling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0.

Data (Implemented either at the Data link layer or Transport Layer of the OSI Model) may get scrambled by noise or get corrupted whenever a message is transmitted. To prevent such errors, error-detection codes are added as extra data to digital messages. This helps in detecting any errors that may have occurred during message transmission.

Types of Errors

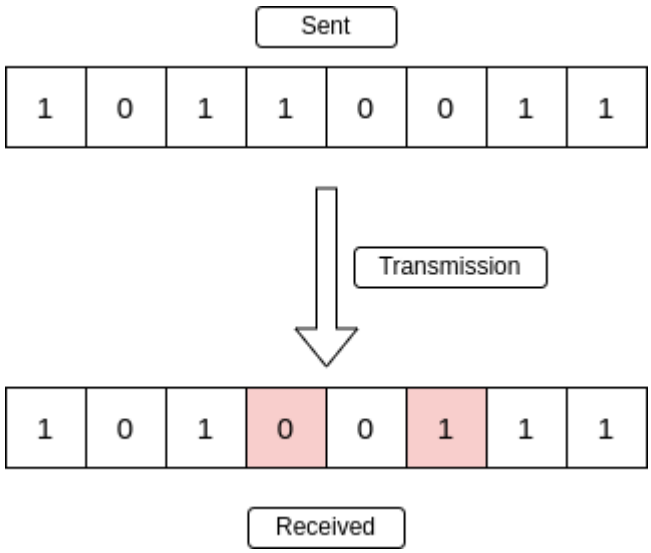
Single-Bit Error

A single-bit error refers to a type of data transmission error that occurs when one bit (i.e., a single binary digit) of a transmitted data unit is altered during transmission, resulting in an incorrect or corrupted data unit.



Multiple-Bit Error

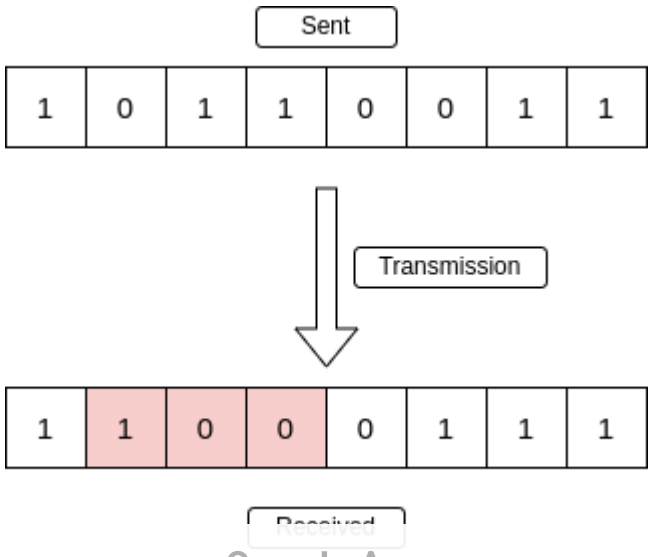
A multiple-bit error is an error type that arises when more than one bit in a data transmission is affected. Although multiple-bit errors are relatively rare when compared to single-bit errors, they can still occur, particularly in high-noise or high-interference digital environments.



Multiple-Bit Error

Burst Error

When several consecutive bits are flipped mistakenly in digital transmission, it creates a burst error. This error causes a sequence of consecutive incorrect values.



Error Detection Methods

To detect errors, a common technique is to introduce redundancy bits that provide additional information. Various techniques for error detection include:

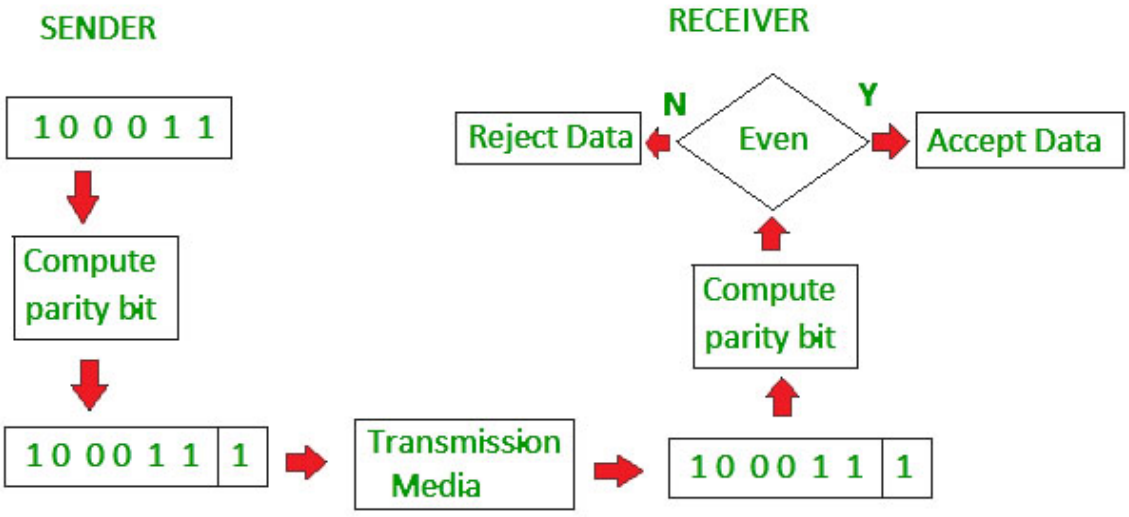
- Simple Parity Check
- Two-Dimensional Parity Check
- Checksum
- Cyclic Redundancy Check (CRC)

Simple Parity Check

Simple-bit parity is a simple error detection method that involves adding an extra bit to a data transmission. It works as:

- 1 is added to the block if it contains an odd number of 1's, and
- 0 is added if it contains an even number of 1's

This scheme makes the total number of 1's even, that is why it is called even parity checking.



Advantages of Simple Parity Check

- Simple parity check can detect all single bit error.
- Simple parity check can detect an odd number of errors

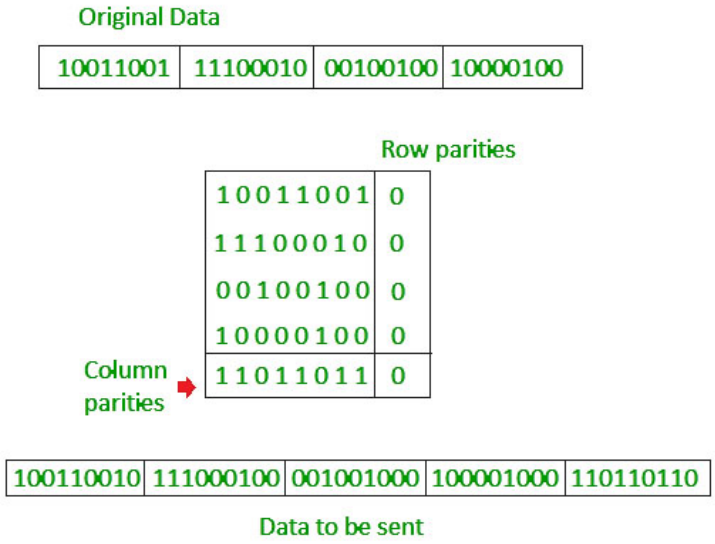
- **Implementation**: Simple Parity Check is easy to implement in both hardware and software.
- **Minimal Extra Data**: Only one additional bit (the parity bit) is added per data unit (e.g., per byte).
- **Fast Error Detection**: The process of calculating and checking the parity bit is quick, which allows for rapid error detection without significant delay in data processing or communication.
- **Single-Bit Error Detection**: It can effectively detect single-bit errors within a data unit, providing a basic level of error detection for relatively low-error environments.

Disadvantages of Simple Parity Check

- Single Parity check is not able to detect even no. of bit error.
- **For example,** the Data to be transmitted is **101010**. Codeword transmitted to the receiver is 1010101 (we have used even parity). Let's assume that during transmission, two of the bits of code word flipped to 1111101.
  On receiving the code word, the receiver finds the no. of ones to be even and hence **no error,** which is a wrong assumption.

Two-Dimensional Parity Check

Two-dimensional Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end, these are compared with the parity bits calculated on the received data.



Advantages of Two-Dimensional Parity Check

- Two-Dimensional Parity Check can detect and correct all single bit error.
- Two-Dimensional Parity Check can detect two or three bit error that occur any where in the matrix.

Disadvantages of Two-Dimensional Parity Check

- Two-Dimensional Parity Check can not correct two or three bit error. It can only detect two or three bit error.
- If we have a error in the parity bit then this scheme will not work.

Checksum

Checksum error detection is a method used to identify errors in transmitted data. The process involves dividing the data into equally sized segments and using a 1's complement to calculate the sum of these segments. The calculated sum is then sent along with the data to the receiver. At the receiver's end, the same process is repeated and if all zeroes are obtained in the sum, it means that the data is correct.

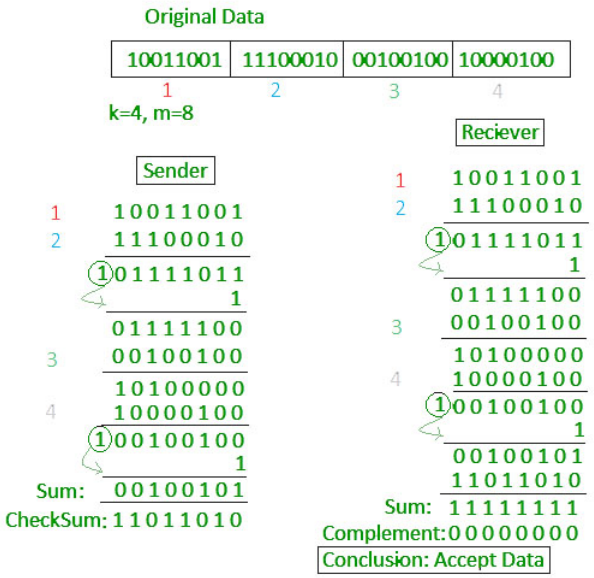
Checksum – Operation at Sender's Side

- Firstly, the data is divided into k segments each of m bits.

- On the sender's end, the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.

Checksum – Operation at Receiver's Side

- At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.

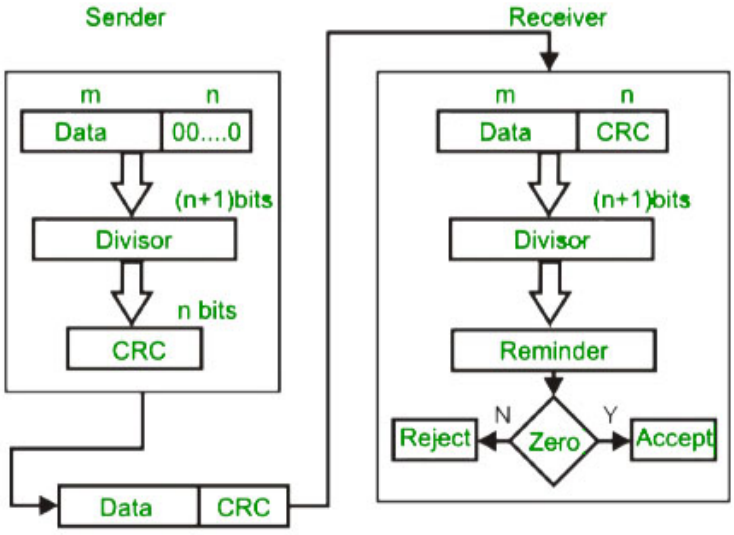


Read more about Checksum

Cyclic Redundancy Check (CRC)

- Unlike the checksum scheme, which is based on addition, CRC is based on binary division.
- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of the data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
- At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.

- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.



CRC Working

We have given dataword of length n and divisor of length k.

Step 1: Append (k-1) zero's to the original message

Step 2: Perform modulo 2 division

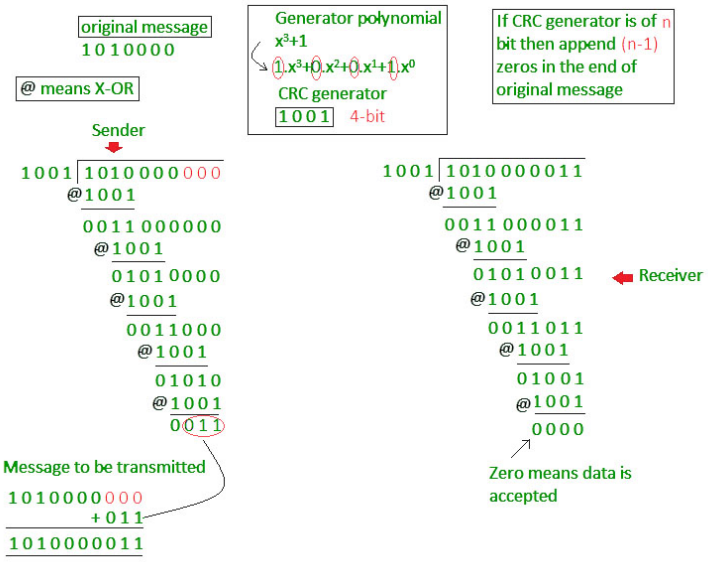
Step 3: Remainder of division = CRC

Step 4: Code word = Data with append k-1 zero's + CRC

Note:

- CRC must be k-1 bits
- Length of Code word = n+k-1 bits

Example: Let's data to be send is 1010000 and divisor in the form of polynomial is x^3+1. CRC method discussed below.



Read in detail about [Cyclic Redundancy Check(CRC)]

Previous year GATE questions based on error detection: [GATE CS 2009 Question 48] [GATE CS 2007 Question 68].

Advantages of Error Detection

- **Increased Data Reliability:** Error detection ensures that the data transmitted over the network is reliable, accurate, and free from errors. This ensures that the recipient receives the same data that was transmitted by the sender.
- **Improved Network Performance:** Error detection mechanisms can help to identify and isolate network issues that are causing errors. This can help to improve the overall performance of the network and reduce downtime.
- **Enhanced Data Security:** Error detection can also help to ensure that the data transmitted over the network is secure and has not been tampered with.

Disadvantages of Error Detection

- **Overhead**: Error detection requires additional resources and processing power, which can lead to increased overhead on the network. This can result in slower network performance and increased latency.
- **False Positives:** Error detection mechanisms can sometimes generate false positives, which can result in unnecessary

retransmission of data. This can further increase the overhead on the network.

- **Limited Error Correction:** Error detection can only identify errors but cannot correct them. This means that the recipient must rely on the sender to retransmit the data, which can lead to further delays and increased network overhead.

Frequently Asked Questions on Error Detection – FAQs

How many types of error detection are there?

There are several types of error detection methods commonly used in computer networks. Some common error detection methods are:

- *Simple Parity Check*
- *Two-Dimensional Parity Check*
- *Checksum*
- *Cyclic Redundancy Check (CRC)*

Which is the best method of error detection?

Cyclic Redundancy Check (CRC) is often considered one of the best and most widely used methods due to its high effectiveness and efficiency.

How many types of computer errors are there?

There are three types of error in transferring the data. These are:

- *Single bit error*
- *Multiple bit error*

Multiple Access Protocols in Computer Network

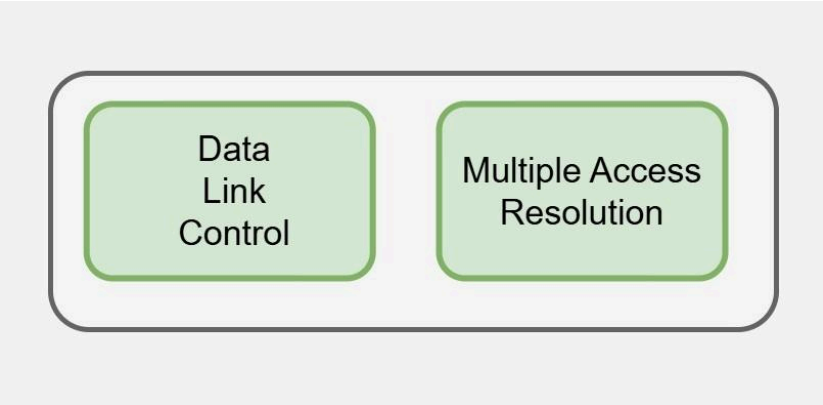
Last Updated : 07 Feb, 2025

Multiple Access Protocols are methods used in computer networks to control how data is transmitted when multiple devices are trying to communicate over the same network. These protocols ensure that data packets are sent and received efficiently, without collisions or interference. They help manage the network traffic so that all devices can share the communication channel smoothly and effectively.

Who is Responsible for the Transmission of Data?

The **Data Link Layer** is responsible for the transmission of data between two nodes. Its main functions are:

- Data Link Control
- Multiple Access Control



Data Link Layer Functions

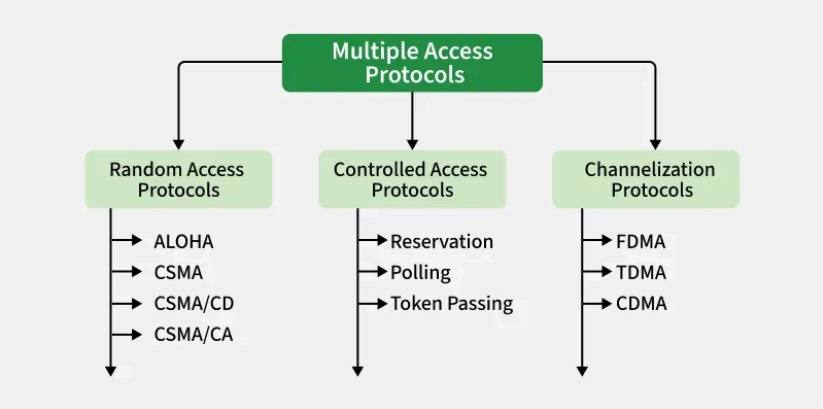
Data Link Control

The data link control is responsible for the reliable transmission of messages over transmission channels by using techniques like framing, error control and flow control. For Data link control refer to – Stop and Wait ARQ

Multiple Access Control

If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk. For example, in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (send data at same time) then a lot of chaos is created(data overlap or data lost) then it is the job of the teacher (multiple access protocols) to manage the students and make them answer one at a time.

Thus, protocols are required for sharing data on non dedicated channels. Multiple access protocols can be subdivided further as



1. Random Access Protocol

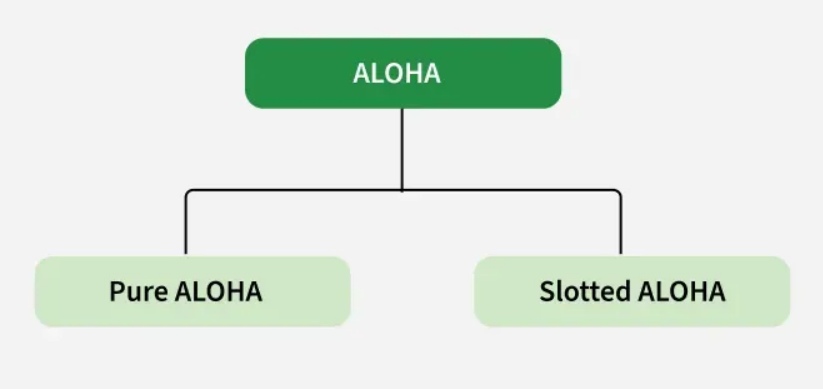
In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state(idle or busy). It has two features:

- There is no fixed time for sending data
- There is no fixed sequence of stations sending data

The Random access protocols are further subdivided as:

ALOHA

It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

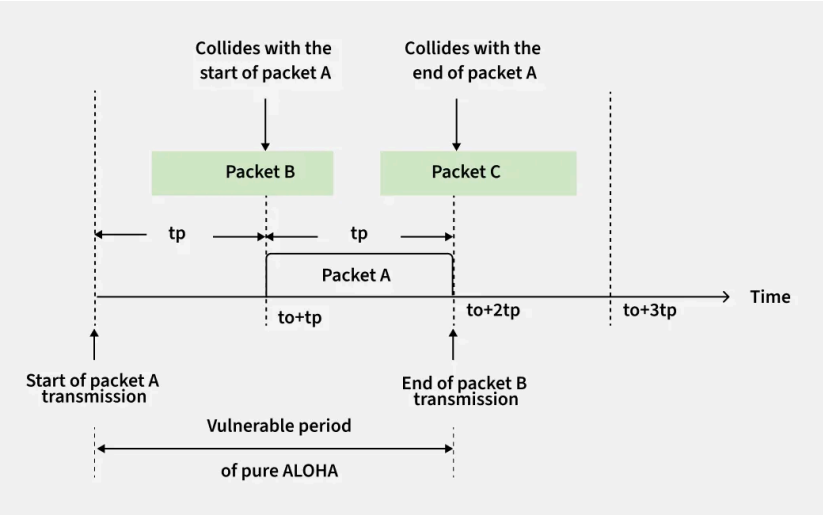


ALOHA

Pure ALOHA

When a station sends data it waits for an acknowledgement. If the acknowledgement doesn't come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data. Since different stations wait for different amount of time, the probability of further collision decreases.

```
Vulnerable Time = 2* Frame transmission time
Throughput =  G exp{-2*G}
Maximum throughput = 0.184 for G=0.5
```

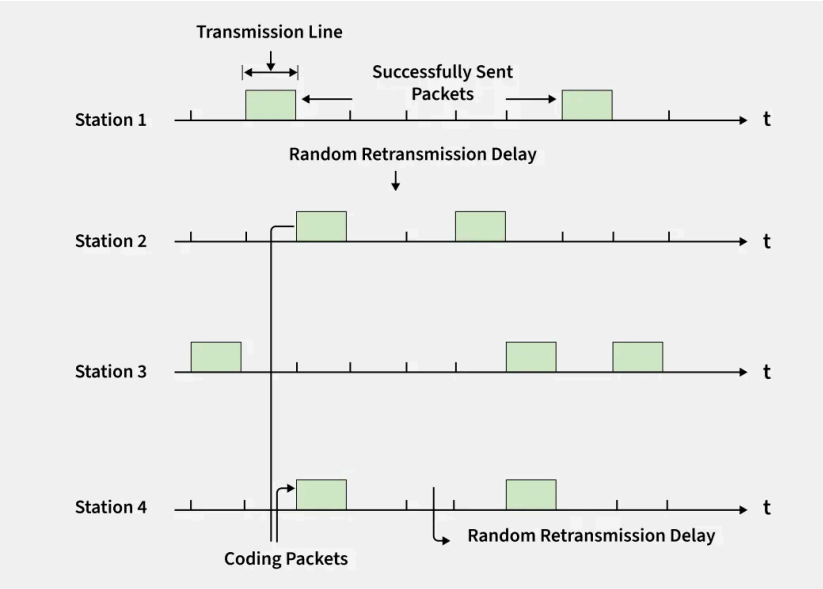


Pure ALOHA

Slotted ALOHA

It is similar to pure aloha, except that we divide time into slots and sending of data is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

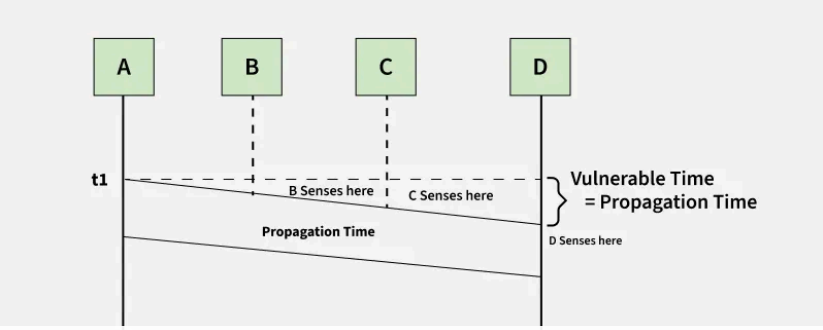
```
Vulnerable Time =  Frame transmission time
Throughput =  G exp{-*G}
Maximum throughput = 0.368 for G=1
```



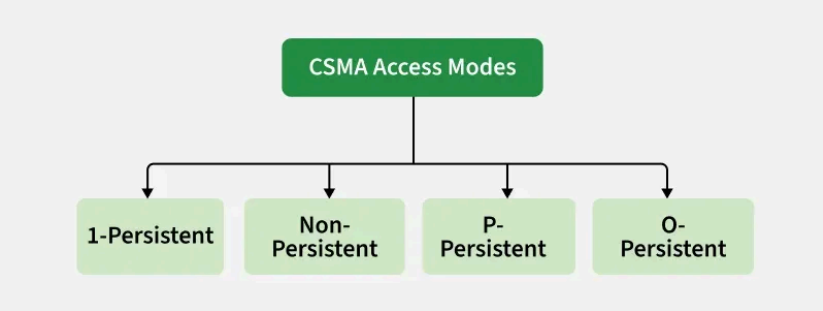
Slotted ALOHA

CSMA

Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium. If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.



CSMA Access Modes



CSMA Access Modes

- **1-Persistent:** The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally(with 1 probability) as soon as the channel gets idle.
- **Non-Persistent:** The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
- **P-Persistent:** The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wifi and packet radio systems.
- **O-Persistent:** Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

CSMA/CD

Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected. For more details refer – Efficiency of CSMA/CD.

CSMA/CA

Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal(its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. However it is not so in wired networks, so CSMA/CA is used in this case.

CSMA/CA Avoids Collision

- **Interframe Space:** Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time it again checks the medium for being idle. The IFS duration depends on the priority of station.
- **Contention Window:** It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.
- **Acknowledgement:** The sender re-transmits the data if acknowledgement is not received before time-out.

2. Controlled Access

Controlled access protocols ensure that only one device uses the network at a time. Think of it like taking turns in a conversation so everyone can speak without talking over each other.

In this, the data is sent by that station which is approved by all other stations. For further details refer – Controlled Access Protocols.

3. Channelization

In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

- **Frequency Division Multiple Access (FDMA) –** The available bandwidth is divided into equal bands so that each station can be

allocated its own band. Guard bands are also added so that no two bands overlap to avoid crosstalk and noise.

- **Time Division Multiple Access (TDMA) –** In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However there is a overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by addition of guard bands. For more details refer – Circuit Switching
- **Code Division Multiple Access (CDMA) –** One channel carries all transmissions simultaneously. There is neither division of bandwidth nor division of time. For example, if there are many people in a room all speaking at the same time, then also perfect reception of data is possible if only two person speak the same language. Similarly, data from different stations can be transmitted simultaneously in different code languages.
- **Orthogonal Frequency Division Multiple Access (OFDMA) –** In OFDMA the available bandwidth is divided into small subcarriers in order to increase the overall performance, Now the data is transmitted through these small subcarriers. it is widely used in the 5G technology.

Advantages of OFDMA

- High data rates
- Good for multimedia traffic
- Increase in efficiency

Disadvantages OFDMA

- Complex to implement
- High peak to power ratio

- **Spatial Division Multiple Access (SDMA) –** SDMA uses multiple antennas at the transmitter and receiver to separate the signals of

multiple users that are located in different spatial directions. This technique is commonly used in MIMO (Multiple-Input, Multiple-Output) wireless communication systems.

Advantages SDMA

- Frequency band uses effectively
- The overall signal quality will be improved
- The overall data rate will be increased

Disadvantages SDMA

- It is complex to implement
- It require the accurate information about the channel

Features of Multiple Access Protocols

- **Contention-Based Access:** Multiple access protocols are typically contention-based, meaning that multiple devices compete for access to the communication channel. This can lead to collisions if two or more devices transmit at the same time, which can result in data loss and decreased network performance.
- **Carrier Sense Multiple Access (CSMA):** CSMA is a widely used multiple access protocol in which devices listen for carrier signals on the communication channel before transmitting. If a carrier signal is detected, the device waits for a random amount of time before attempting to transmit to reduce the likelihood of collisions.
- **Collision Detection (CD):** CD is a feature of some multiple access protocols that allows devices to detect when a collision has occurred and take appropriate action, such as backing off and retrying the transmission.
- **Collision Avoidance (CA):** CA is a feature of some multiple access protocols that attempts to avoid collisions by assigning time slots to devices for transmission.
- **Token Passing:** Token passing is a multiple access protocol in which devices pass a special token between each other to gain access to

the communication channel. Devices can only transmit data when they hold the token, which ensures that only one device can transmit at a time.

- **Bandwidth Utilization:** Multiple access protocols can affect the overall bandwidth utilization of a network. For example, contention-based protocols may result in lower bandwidth utilization due to collisions, while token passing protocols may result in higher bandwidth utilization due to the controlled access to the communication channel.

Frequently Asked Questions on Multiple Access Protocols – FAQs

Why are Multiple Access Protocols important?

Multiple Access Protocols is important because, they ensure data is sent and received efficiently without collisions or interference.

How do Multiple Access Protocols work?

Multiple Access Protocols manage network traffic by organizing how and when each device can send data.

What are some common Multiple Access Protocols?

common Multiple Access Protocols include CSMA/CD (used in Ethernet), CSMA/CA (used in Wi-Fi), and TDMA (used in cellular networks).

What is CSMA/CD?

Sliding Window Protocol | Set 3 (Selective Repeat)

Last Updated : 31 Aug, 2023

Prerequisite : Sliding Window Protocol – Set 1 (Sender Side), Set 2 (Receiver Side) **Why Selective Repeat Protocol?** The go-back-n protocol works well if errors are less, but if the line is poor it wastes a lot of bandwidth on retransmitted frames. An alternative strategy, the selective repeat protocol, is to allow the receiver to accept and buffer the frames following a damaged or lost one. Selective Repeat attempts to retransmit only those packets that are actually lost (due to errors) :

- Receiver must be able to accept packets out of order.
- Since receiver must release packets to higher layer in order, the receiver must be able to buffer some packets.

Retransmission requests :

- **Implicit –** The receiver acknowledges every good packet, packets that are not ACKed before a time-out are assumed lost or in error.Notice that this approach must be used to be sure that every packet is eventually received.
- **Explicit –** An explicit NAK (selective reject) can request retransmission of just one packet. This approach can expedite the retransmission but is not strictly needed.
- One or both approaches are used in practice.

Selective Repeat Protocol (SRP) : This protocol(SRP) is mostly identical to GBN protocol, except that buffers are used and the receiver, and the sender, each maintains a window of size. SRP works better when the link is very unreliable. Because in this case, retransmission tends to happen more frequently, selectively retransmitting frames is

more efficient than retransmitting all of them. SRP also requires full-duplex link. backward acknowledgements are also in progress.

- Sender's Windows (Ws) = Receiver's Windows (Wr).
- Window size should be less than or equal to half the sequence number in SR protocol. This is to avoid packets being recognized incorrectly. If the size of the window is greater than half the sequence number space, then if an ACK is lost, the sender may send new packets that the receiver believes are retransmissions.
- Sender can transmit new packets as long as their number is with W of all unACKed packets.
- Sender retransmit un-ACKed packets after a timeout – Or upon a NAK if NAK is employed.
- Receiver ACKs all correct packets.
- Receiver stores correct packets until they can be delivered in order to the higher layer.
- In Selective Repeat ARQ, the size of the sender and receiver window must be at most one-half of 2^m.

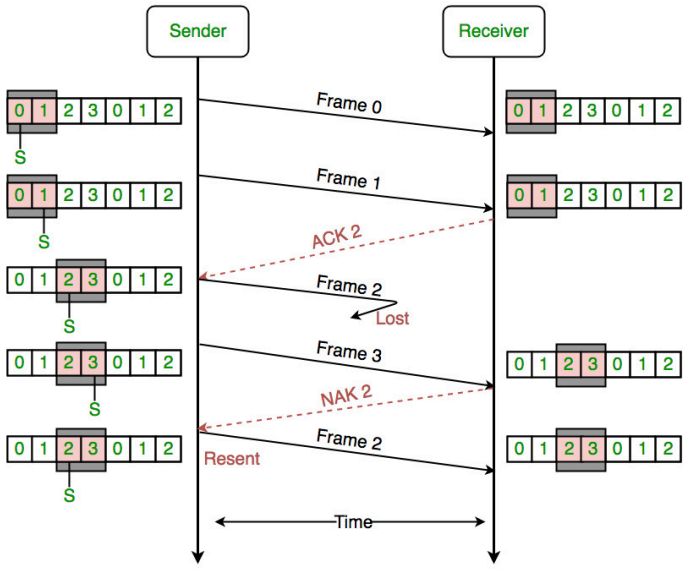


Figure – the sender only retransmits frames, for which a NAK is receivedEfficiency of Selective Repeat Protocol (SRP) is same as GO-Back-N's efficiency :

```
Efficiency = N/(1+2a)
Where a = Propagation delay / Transmission delay
Buffers = N + N
```

```
Sequence number  = N(sender side)  + N  ( Receiver Side)
```

if Tt(ack) :Transmission delay for acknowledgment , Tq: Queuing delay and Tpro: Processing delay is mention

We know that the Efficiency (?),

=Useful time / Total cycle time

=Tt(data) /Tt(data) + 2*Tp + Tq + Tpro + Tt(ack)

```
Tt(data) : Transmission delay for Data packet
Tp : propagation delay for Data packet
Tq: Queuing delay
Tpro: Processing delay
Tt(ack): Transmission delay for acknowledgment
```

Above formula is applicable for any condition, if any of the things are not given we assume it to be 0.

References – Slideshare Youtube MIT article<

Next Article

Piggybacking in Computer Networks

Similar Reads

Difference Between Go-Back-N and Selective Repeat Protocol

Both the Go-Back-N Protocol and Selective Repeat Protocol are the types of sliding window protocols. The main difference between these two...

Sliding Window Protocol – Go Back N (GBN)

Last Updated : 03 Oct, 2024

The **Sliding Window Protocol** is a method used in computer networks to manage the flow of data between two devices, ensuring that data is sent and received in the correct order. There are two types of sliding window protocol **Go-Back-N (GBN)**, and Selective Repeat (SR).

In **Go-Back-N**, the sender can send multiple data packets without waiting for an acknowledgement for each one. However, it can only send a certain number of packets (this is called the “window size”). If one packet is lost or not acknowledged, the sender must go back and resend that packet *and* all the packets that followed it, even if they were received correctly. For example, if packets 1, 2, 3, 4, and 5 are sent and packet 3 gets lost, the sender will have to resend packets 3, 4, and 5, even if 4 and 5 were received. In this article, we will discuss the Go-Back-N (GBN) protocol in detail.

What is the Go Back N (GBN) Protocol?

The Go-Back-N (GBN) protocol is a sliding window protocol used in networking for reliable data transmission. It is part of the Automatic Repeat reQuest (ARQ) protocols, which ensure that data is correctly received and that any lost or corrupted packets are retransmitted.

The three main characteristic features of GBN are:

1. Sender Window Size (W_R)

It is N itself. If we say the protocol is GB10, then Ws = 10. N should be always greater than 1 in order to implement pipelining. For N = 1, it reduces to the Stop and Wait protocol.

```
Efficiency Of GBN = N/(1+2a)
where a = Tp/Tt
Tp=Propogation Delay
Tt=Transmission Delay of sender
```

What will be the efficiency if processing delay, queuing delay and transmission delay of acknowledgement is not zero.

Efficiency= N*(Useful time)/(Total Time)

where, useful time=Tt

Total time=Tt+2*Tp+Pr+Pq+Tt(ack)

where,

***Tt**=Transmission delay of sender side*

***Tp**=Propogation Delay*

***Pr=**Processing Delay*

***Pq=**Queuing Delay*

***Tt(ack)**=Transmission Delay of Acknowledgement*

If B is the bandwidth of the channel, then

```
Effective Bandwidth or Throughput
 = Efficiency * Bandwidth
 = (N/(1+2a)) * B
```

2. Receiver Window Size (W_R)

In the GB-N the receiver window size is one always. i.e. W_R is always 1 in GBN.

3. Acknowledgements

In flow control, acknowledgments (ACKs) are signals sent by the receiver to the sender to confirm that data packets have been successfully received. When the sender transmits data, it waits for an acknowledgment before sending more. This process helps ensure that data is received correctly. If an acknowledgment isn't received within a certain time, the sender assumes the packet was lost and retransmits it.

There are 2 kinds of acknowledgements namely:

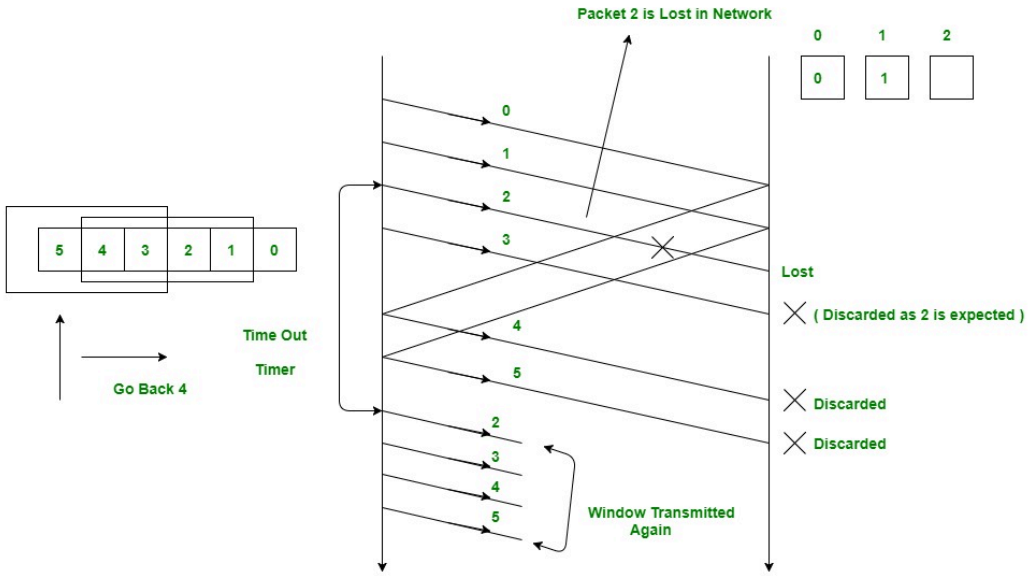
- **Cumulative Ack**: One acknowledgement is used for many packets. The main advantage is traffic is less. A disadvantage is less reliability as if one ack is the loss that would mean that all the packets sent are lost.
- **Independent Ack**: If every packet is going to get acknowledgement independently then the reliability is high here but a disadvantage is that traffic is also high since for every packet we are receiving independent ack.

Working of GB-N Protocol

Now what exactly happens in GBN, we will explain with a help of example. Consider the diagram given below. We have sender window size of 4. Assume that we have lots of sequence numbers just for the sake of explanation. Now the sender has sent the packets 0, 1, 2 and 3. After acknowledging the packets 0 and 1, receiver is now expecting packet 2 and sender window has also slided to further transmit the packets 4 and 5. Now suppose the packet 2 is lost in the network, Receiver will discard all the packets which sender has transmitted after packet 2 as it is expecting sequence number of 2.

On the sender side for every packet send there is a time out timer which will expire for packet number 2 and hence the last transmitted packet 5

sender will go back to the packet number 2 in the current window and transmit all the packets till packet number 5. That's why it is called Go Back N. Go back means sender has to go back N places from the last transmitted packet in the unacknowledged window and not from the point where the packet is lost.



Relationship Between Window Size and Sequence Numbers

The **window size** and **sequence numbers** in a sliding window protocol, like Go-Back-N or Selective Repeat, are closely related.

- The **window size** determines how many packets the sender can transmit without needing an acknowledgment. It's like a limit on how much data can be sent before the sender has to stop and wait for confirmation.
- **Sequence numbers** are used to label packets so the receiver knows their order and can detect any missing packets.

The **window size** should be smaller than or equal to the range of available **sequence numbers**. If the window size is too large compared to the sequence number range, the receiver might get confused because the same sequence number could be reused before the first one is acknowledged. This would make it hard to know if a packet is new or a duplicate.

Relation between window size and sequence number is given by the formula:
$W_S+W_R<=ASN$
where W_S is sender window size and W_R is receiver window size, and ASN is available sequence number.
$W_S+1<=ASN$ because $W_R=1$ in GB-N protocol
So minimum sequence numbers required in GBN = N + 1

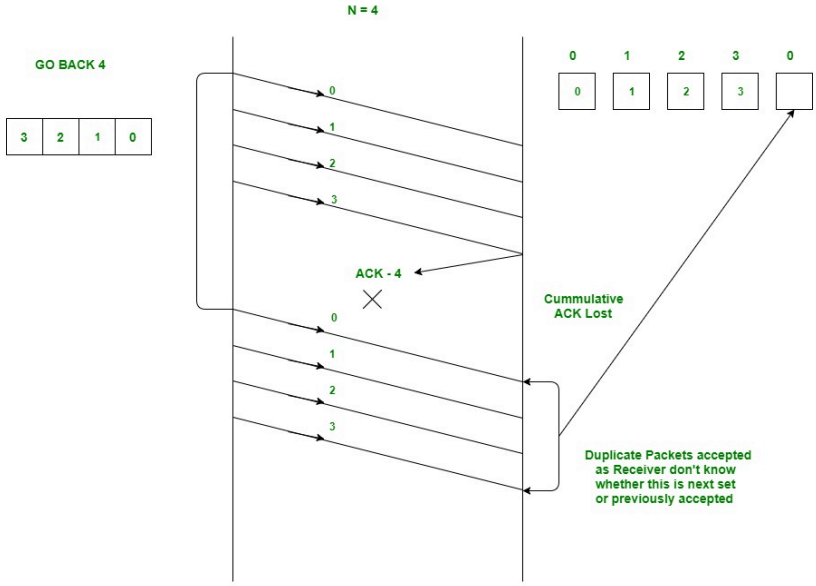
Bits Required in GBN = ceil(log2 (N + 1))

The extra 1 is required in order to
avoid the problem of duplicate packets
as described below.

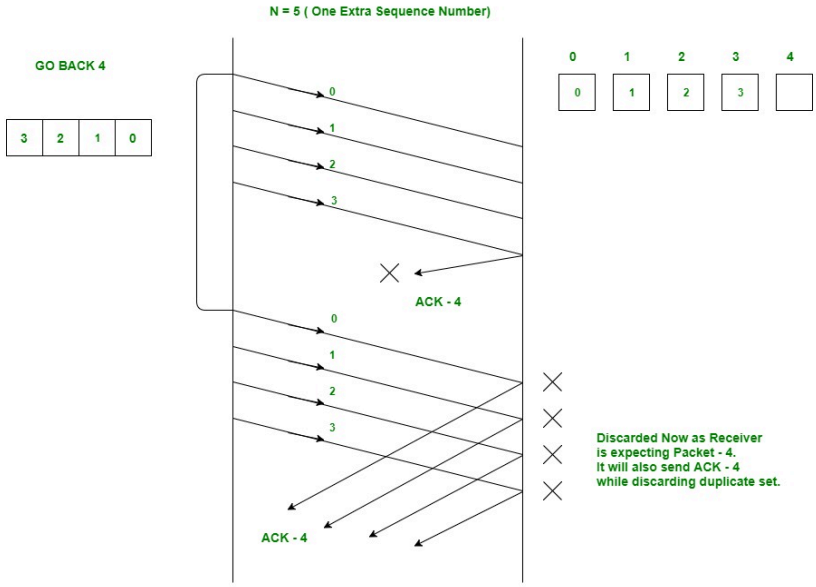
Example: Consider an Example of GB4.

- Sender window size is 4 therefore we require a minimum of 4 sequence numbers to label each packet in the window.
- Now suppose receiver has received all the packets(0, 1, 2 and 3 sent by sender) and hence is now waiting for packet number 0 again (We can not use 4 here as we have only 4 sequence numbers available since N = 4).
- Now suppose the cumulative ack for the above 4 packets is lost in the network.
- On sender side, there will be timeout for packet 0 and hence all the 4 packets will be transmitted again.
- Problem now is receiver is waiting for new set of packets which should have started from 0 but now it will receive the duplicate copies of the previously accepted packets.
- In order to avoid this, we need one extra sequence number.
- Now the receiver could easily reject all the duplicate packets which were starting from 0 because now it will be waiting for packet number 4 (We have added an extra sequence number now).

This is explained with the help of the illustrations below. **Trying with Sequence numbers 4.**



Now Trying with one extra Sequence Number.



Now it is clear as to why we need an extra 1 bit in the GBN protocol.

Advantages of GBN Protocol

- Simple to implement and effective for reliable communication.
- Better performance than stop-and-wait protocols for error-free or low-error networks.

Disadvantages of GBN Protocol

- Inefficient if errors are frequent, as multiple frames might need to be retransmitted unnecessarily.
- Bandwidth can be wasted due to redundant retransmissions.

Stop and Wait ARQ

Last Updated : 11 Feb, 2025

Stop and Wait ARQ is a Sliding Window Protocol method used for the reliable delivery of data frames. The stop-and-wait ARQ is used for noisy channels or links to handle flow and error control between sender and receiver. The Stop and Wait ARQ protocol sends a data frame and then waits for an acknowledgment (ACK) from the receiver.

What is Stop and Wait ARQ?

The Stop and Wait ARQ protocol sends a data frame and then waits for an acknowledgment (ACK) from the receiver. The ACK indicates that the receiver successfully received the data frame. After receiving the ACK from the receiver, the sender delivers the next data frame. So there is a stop before the next data frame is transferred, hence it is known as the Stop and Wait ARQ protocol.

Characteristics of Stop and Wait ARQ

- Used in Connection-oriented communication.
- It offers error and flow control.
- It is used in Data Link and Transport Layers
- Stop and Wait for ARQ mainly implements the Sliding Window Protocol concept with Window Size 1
- It uses a link between sender and receiver as a half-duplex link
- Throughput = 1 Data packet/frame per RTT
- If the bandwidth*Delay product is very high, then they stop and wait for protocol if it is not so useful. The sender has to keep waiting for acknowledgments before sending the processed next packet.
- It is an example of "**Closed Loop OR connection-oriented** " protocols
- It is a special category of SWP where its window size is 1
- Irrespective of the number of packets sender is having stop and wait for protocol requires only two sequence numbers 0 and 1

Useful Terms in Stop and Wait Protocol

- **Propagation Delay:** Amount of time taken by a packet to make a physical journey from one router to another **router.**

Propagation Delay = (Distance between routers) / (Velocity of propagation)

- RoundTripTime (RTT) = Amount of time taken by a packet to reach the receiver + Time taken by the Acknowledgement to reach the sender
- TimeOut (**TO**) = 2* RTT
- Time To Live (TTL) = 2* TimeOut. (Maximum TTL is 255 seconds)

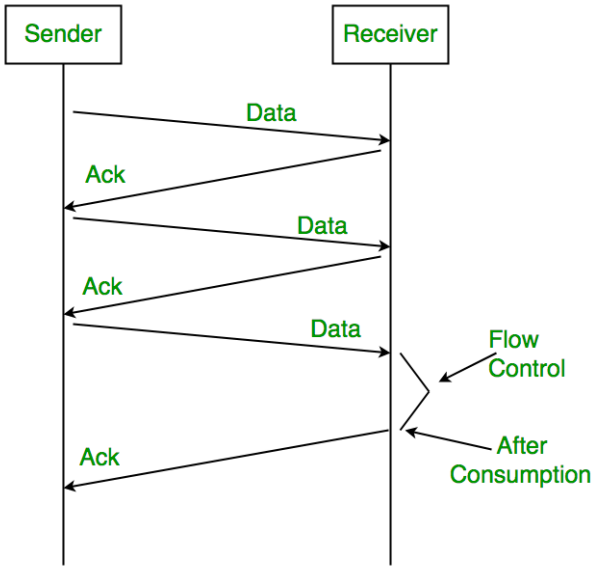
Simple Stop and Wait

At Sender

- Rule 1: Send one data packet at a time.
- Rule 2: Send the next packet only after receiving acknowledgment for the previous.

At Receiver

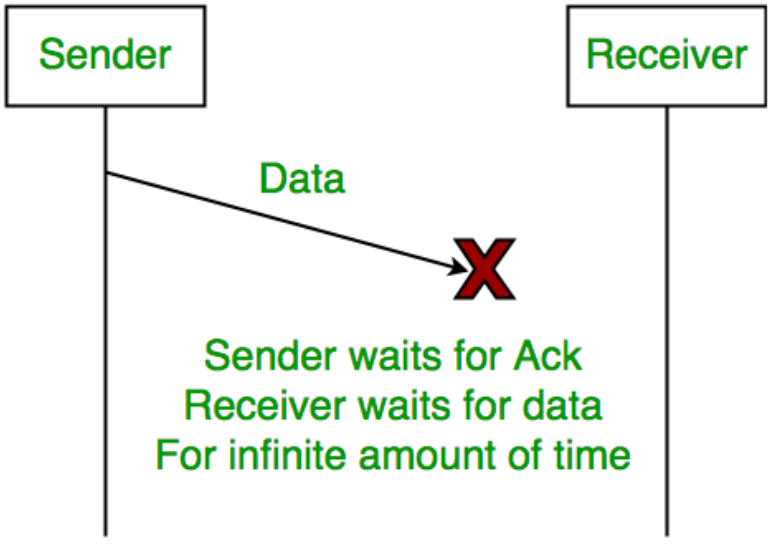
- Rule 1: Send acknowledgement after receiving and consuming a data packet.
- Rule 2: After consuming packet acknowledgement need to be sent (Flow Control)



Problems Associated with Stop and Wait

1. Lost Data

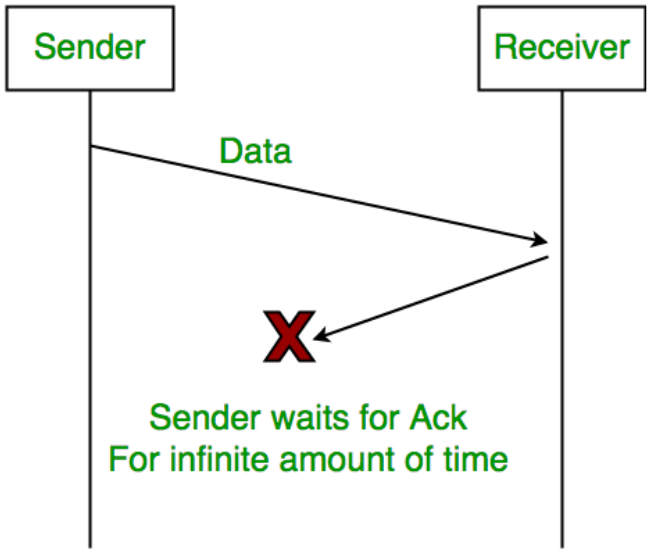
Assume the sender transmits the data packet and it is lost. The receiver has been waiting for the data for a long time. Because the data is not received by the receiver, it does not transmit an acknowledgment. The sender does not receive an acknowledgment, it will not send the next packet. This problem is caused by a loss of data.



2. Lost Acknowledgement

Assume the sender sends the data, which is also received by the receiver. The receiver sends an acknowledgment after receiving the

packet. In this situation, the acknowledgment is lost in the network. The sender does not send the next data packet because it does not receive acknowledgement, under the stop and wait protocol, the next packet cannot be transmitted until the preceding packet's acknowledgment is received.

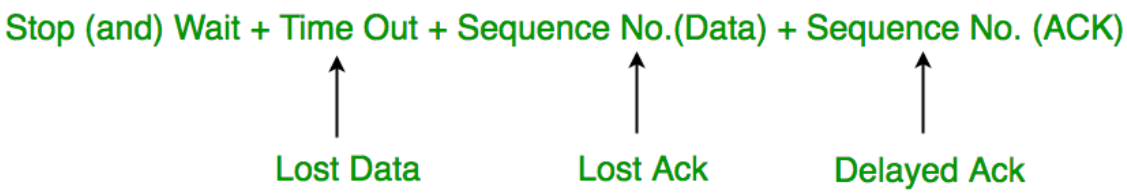


3. Delayed Acknowledgement/Data

Assume the sender sends the data, which is also received by the receiver. The receiver then transmits the acknowledgment, which is received after the sender's timeout period. After a timeout on the sender side, a long-delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet.

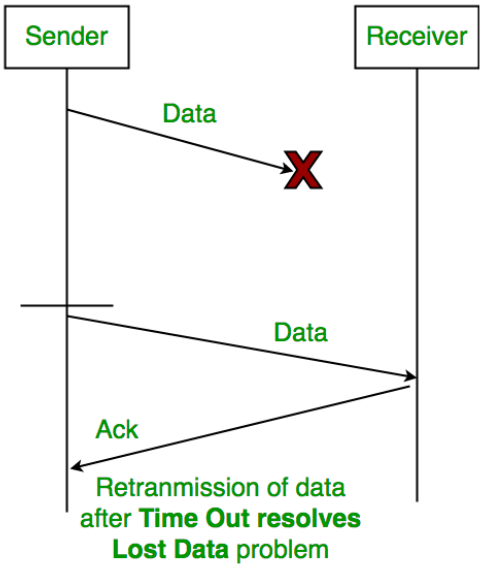
Stop and Wait for ARQ (Automatic Repeat Request)

The above 3 problems are resolved by Stop and Wait for ARQ (Automatic Repeat Request) that does both error control and flow control.



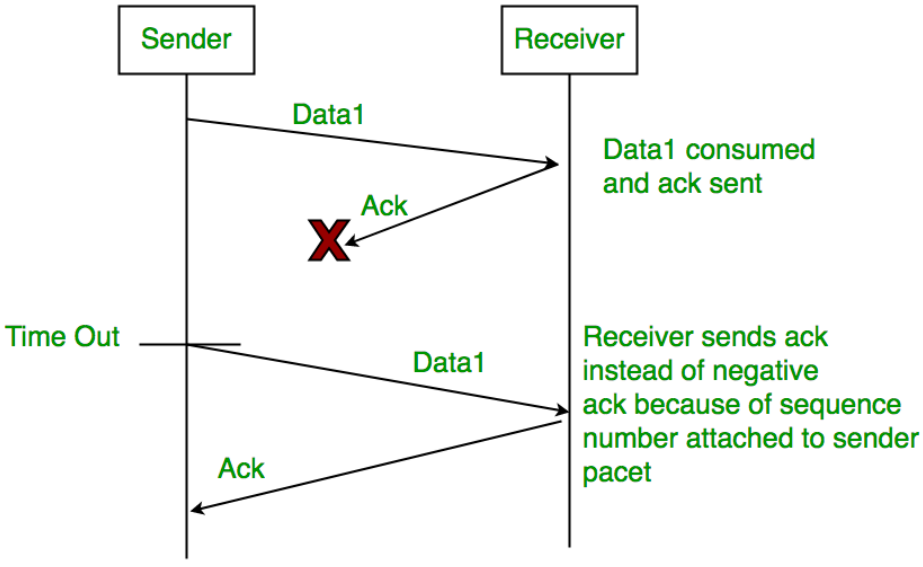
1. Time Out

Timeout refers to the duration for which the sender waits for an acknowledgment (ACK) from the receiver after transmitting a data packet. If the sender does not receive an ACK within this timeout period, it assumes that the frame was lost or corrupted and retransmits the frame.



2. Sequence Number (Data)

In Stop-and-Wait ARQ, the sender assigns sequence numbers to each data frame it sends. This allows the receiver to identify and acknowledge each frame individually, ensuring reliable delivery of data packets. After sending a frame, the sender waits for an acknowledgment before sending the next frame.

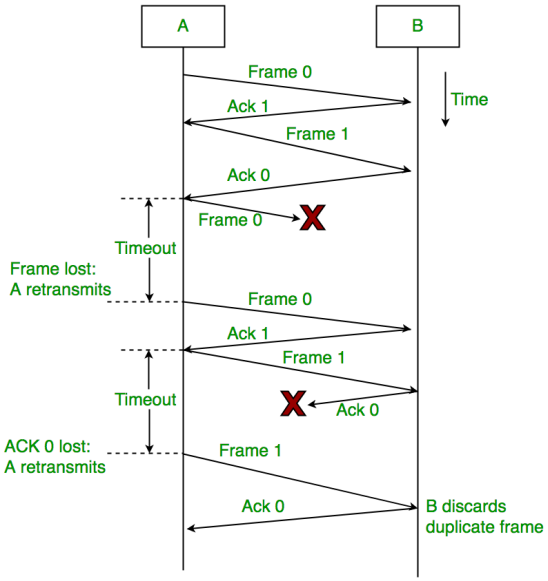


3. Sequence Number(Acknowledgement)

Similarly, sequence numbers are also used in acknowledgments (ACKs) sent by the receiver to acknowledge received data frames. When the receiver successfully receives a data frame, it sends an ACK back to the sender, indicating the sequence number of the next expected frame. The sender uses this ACK to determine whether the transmission was successful and whether it can proceed to send the next frame.

Working of Stop and Wait for ARQ

- Sender A sends a data frame or packet with sequence number 0.
- Receiver B, after receiving the data frame, sends an acknowledgement with sequence number 1 (the sequence number of the next expected data frame or packet)
  There is only a one-bit sequence number that implies that both sender and receiver have a buffer for one frame or packet only.



Constraints in Stop and Wait ARQ

Stop and Wait ARQ has very less efficiency , it can be improved by increasing the window size. Also , for better efficiency , Go back N and Selective Repeat Protocols are used. The Stop and Wait ARQ solves the main three problems but may cause big performance issues as the sender always waits for acknowledgement even if it has the next packet ready to send. Consider a situation where you have a high bandwidth connection and propagation delay is also high (you are

connected to some server in some other country through a high-speed connection). To solve this problem, we can send more than one packet at a time with a larger sequence number. We will be discussing these protocols in the next articles. So Stop and Wait ARQ may work fine where propagation delay is very less for example LAN connections but performs badly for distant connections like satellite connections.

Advantages of Stop and Wait ARQ

- **Simple Implementation:** Stop and Wait ARQ is a simple protocol that is easy to implement in both hardware and software. It does not require complex algorithms or hardware components, making it an inexpensive and efficient option.
- **Error Detection:** Stop and Wait ARQ detects errors in the transmitted data by using checksums or cyclic redundancy checks (CRC). If an error is detected, the receiver sends a negative acknowledgment (NAK) to the sender, indicating that the data needs to be retransmitted.
- **Reliable:** Stop and Wait ARQ ensures that the data is transmitted reliably and in order. The receiver cannot move on to the next data packet until it receives the current one. This ensures that the data is received in the correct order and eliminates the possibility of data corruption.
- **Flow Control:** Stop and Wait ARQ can be used for flow control, where the receiver can control the rate at which the sender transmits data. This is useful in situations where the receiver has limited buffer space or processing power.
- **Backward Compatibility:** Stop and Wait ARQ is compatible with many existing systems and protocols, making it a popular choice for communication over unreliable channels.

Disadvantages of Stop and Wait ARQ

- **Low Efficiency:** Stop and Wait ARQ has low efficiency as it requires the sender to wait for an acknowledgment from the receiver before sending the next data packet. This results in a low data transmission rate, especially for large data sets.

- **High Latency:** Stop and Wait ARQ introduces additional latency in the transmission of data, as the sender must wait for an acknowledgment before sending the next packet. This can be a problem for real-time applications such as video streaming or online gaming.
- **Limited Bandwidth Utilization:** Stop and Wait ARQ does not utilize the available bandwidth efficiently, as the sender can transmit only one data packet at a time. This results in underutilization of the channel, which can be a problem in situations where the available bandwidth is limited.
- **Limited Error Recovery:** Stop and Wait ARQ has limited error recovery capabilities. If a data packet is lost or corrupted, the sender must retransmit the entire packet, which can be time-consuming and can result in further delays.
- **Vulnerable to Channel Noise:** Stop and Wait ARQ is vulnerable to channel noise, which can cause errors in the transmitted data. This can result in frequent retransmissions and can impact the overall efficiency of the protocol.

Question For Practice

Question: Suppose two hosts are connected by a point-to-point link and they are configured to use Stop and Wait protocol for reliable data transfer. Identify in which one of the following scenarios, the utilization of the link is the lowest. **[GATE CS/IT 2023]**

(A) Longer link length and lower transmission rate

(B) Longer link length and higher transmission rate

(C) Shorter link length and lower transmission rate

(D) Shorter link length and higher transmission rate

Solution: *Correct option is (A)*

Explanation- *Link utilization depends on* ***propagation delay*** *and* ***transmission rate.***