BCAAIML403 COMPUTER NETWORKS
UNIT-2

Course- BCAAIML **Semester-IV**

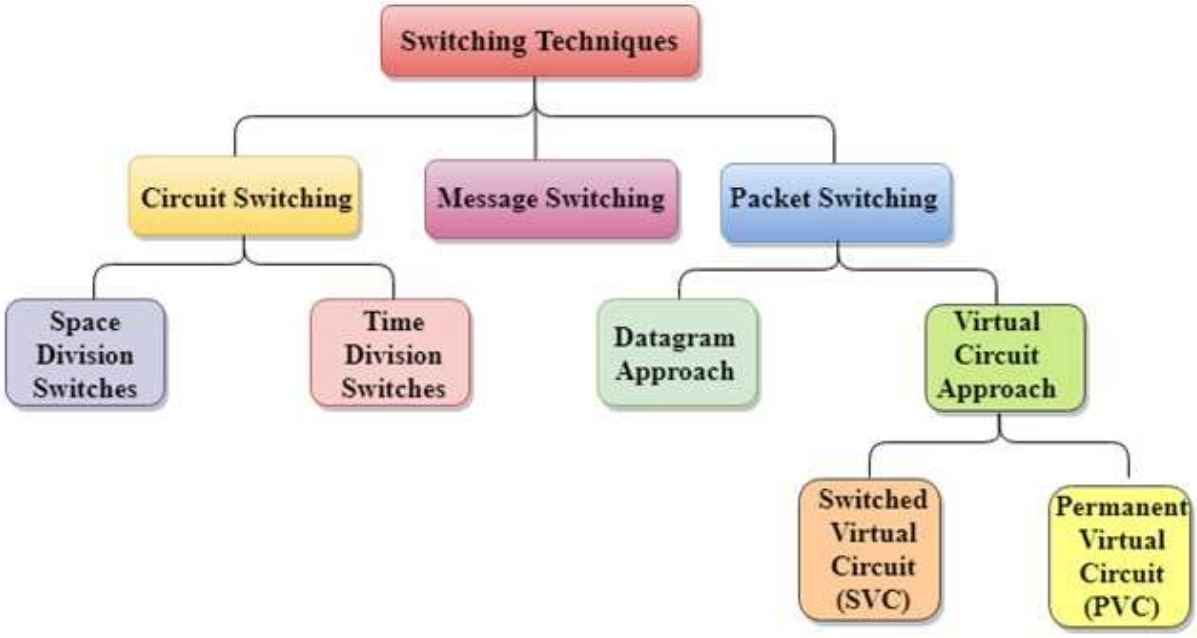
Subject- COMPUTER NETWORKS

Subject Code- BCAAIML403

Switching techniques

Definition: In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission. Switching technique is used to connect the systems for making one-to-one communication.

Classification of Switching Techniques:



Circuit Switching:

Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.

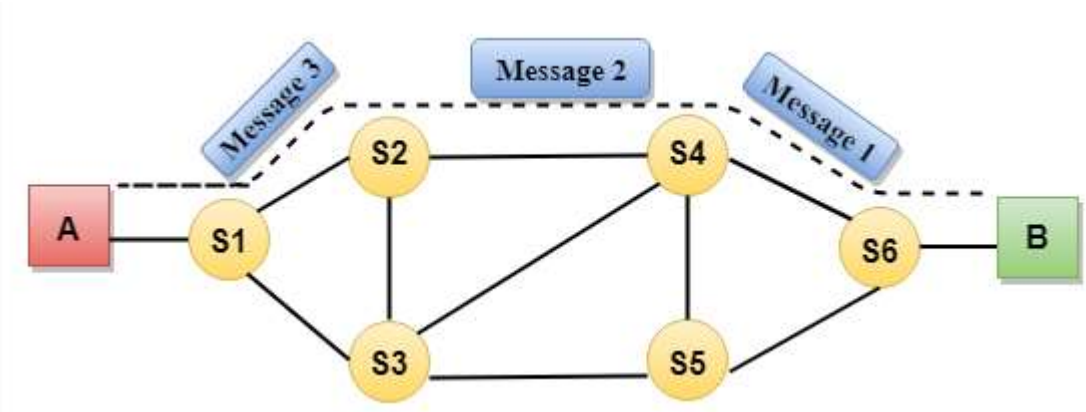
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the

acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.

- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

Communication through circuit switching has 3 phases:

- Circuit establishment
- Data transfer
- Circuit Disconnect



Circuit Switching can use either of the two technologies:

Space Division Switches:

- Space Division Switching is a circuit switching technology in which a single transmission path is accomplished in a switch by using a physically separate set of crosspoints.
- Space Division Switching can be achieved by using crossbar switch. A crossbar switch is a metallic crosspoint or semiconductor gate that can be enabled or disabled by a control unit.
- The Crossbar switch is made by using the semiconductor. For example, Xilinx crossbar switch using FPGAs.
- Space Division Switching has high speed, high capacity, and nonblocking switches.

Space Division Switches can be categorized in two ways:

- Crossbar Switch
- Multistage Switch

Crossbar Switch

- The Crossbar switch is a switch that has n input lines and n output lines. The crossbar switch has n2 intersection points known as **crosspoints.**

Disadvantage of Crossbar switch:

The number of crosspoints increases as the number of stations is increased. Therefore, it becomes very expensive for a large switch. The solution to this is to use a multistage switch.

Multistage Switch

- Multistage Switch is made by splitting the crossbar switch into the smaller units and then interconnecting them.
- It reduces the number of crosspoints.
- If one path fails, then there will be an availability of another path.

Advantages of Circuit Switching:

- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

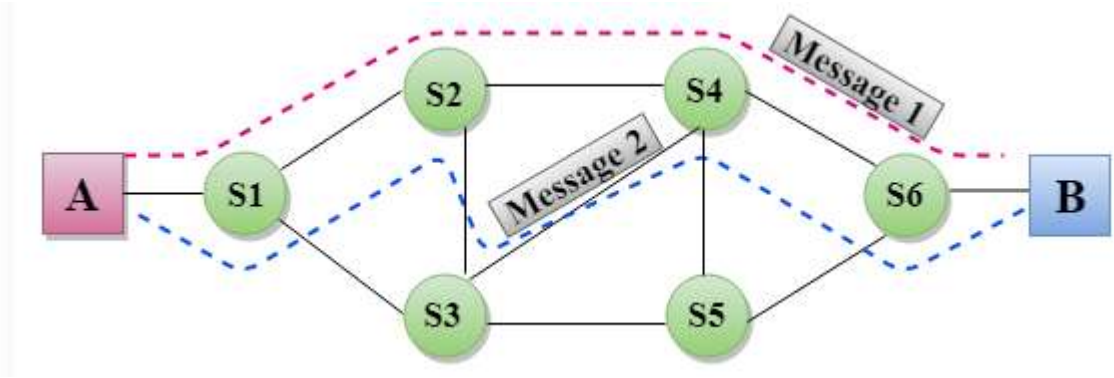
Disadvantages of Circuit Switching:

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**

- Message switching treats each message as an independent entity.



Advantages of Message Switching

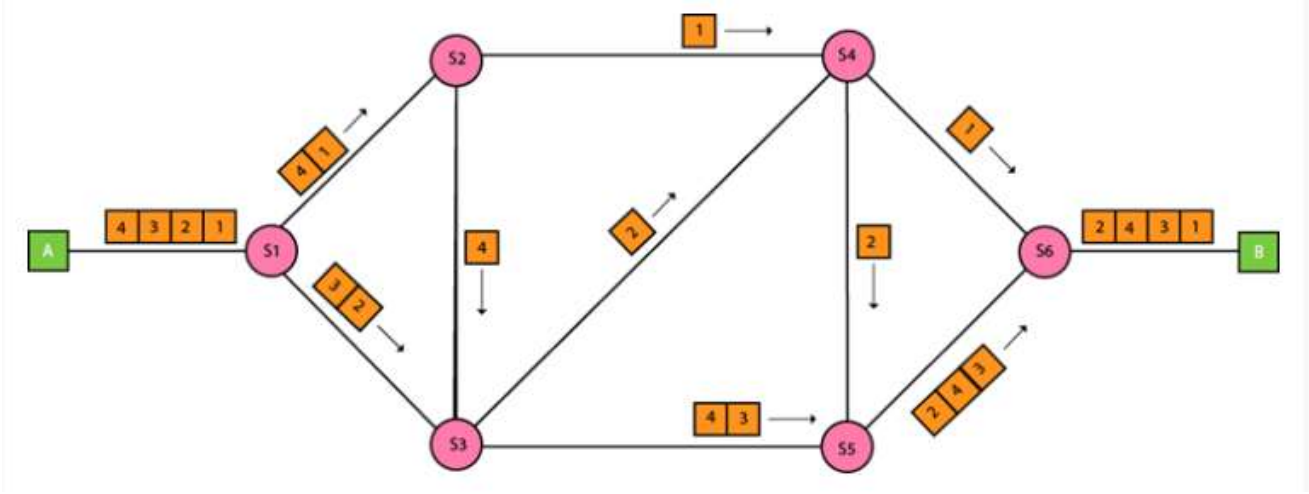
- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.
- The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

Disadvantages of Message Switching

- The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
- The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.



Approaches Of Packet Switching:
There are two approaches to Packet Switching:

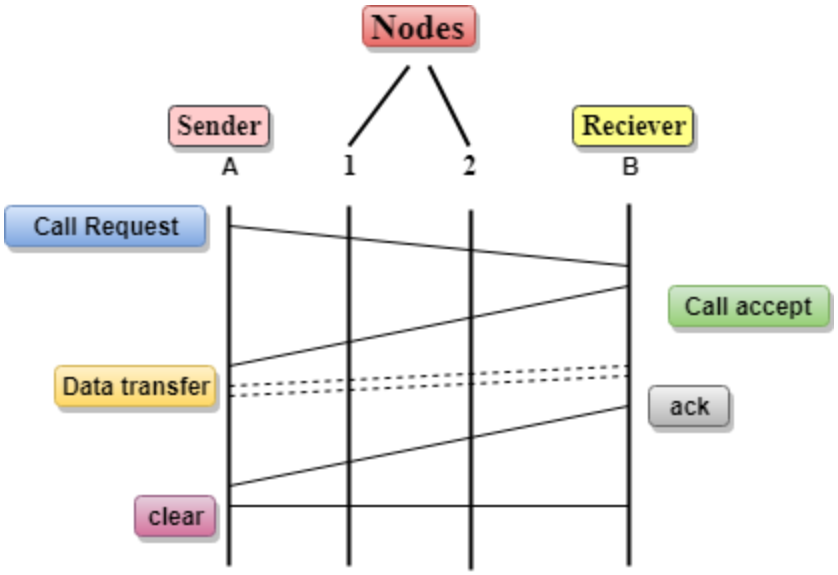
Datagram Packet switching:

- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.

Virtual Circuit Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.

Let's understand the concept of virtual circuit switching through a diagram:



- In the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.
- Call request and call accept packets are used to establish a connection between the sender and receiver.
- When a route is established, data will be transferred.
- After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.
- If the user wants to terminate the connection, a clear signal is sent for the termination.

Differences b/w Datagram approach and Virtual Circuit approach

Datagram approach	Virtual Circuit approach
Node takes routing decisions to forward the packets.	Node does not take any routing decision.
Congestion cannot occur as all the packets travel in different directions.	Congestion can occur when the node is busy, and it does not allow other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible.

Advantages Of Packet Switching:

- **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.

- **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages Of Packet Switching:

- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

Dial-up modems

Dial-up Internet access is a form of Internet access that uses the facilities of the public switched telephone network (PSTN) to establish a connection to an Internet service provider (ISP) by dialing a telephone number on a conventional telephone line which could be connected using an RJ-11 connector.[1] Dial-up connections use modems to decode audio signals into data to send to a router or computer, and to encode signals from the latter two devices to send to another modem at the ISP.

Dial-up Internet reached its peak popularity during the dot-com bubble with the likes of ISPs such as Sprint, EarthLink, MSN Dial-up, NetZero, Prodigy, and America Online (more commonly known as AOL). This was in large part because broadband Internet did not become widely used until well into the 2000s. Since then, most dial-up access has been replaced by broadband.

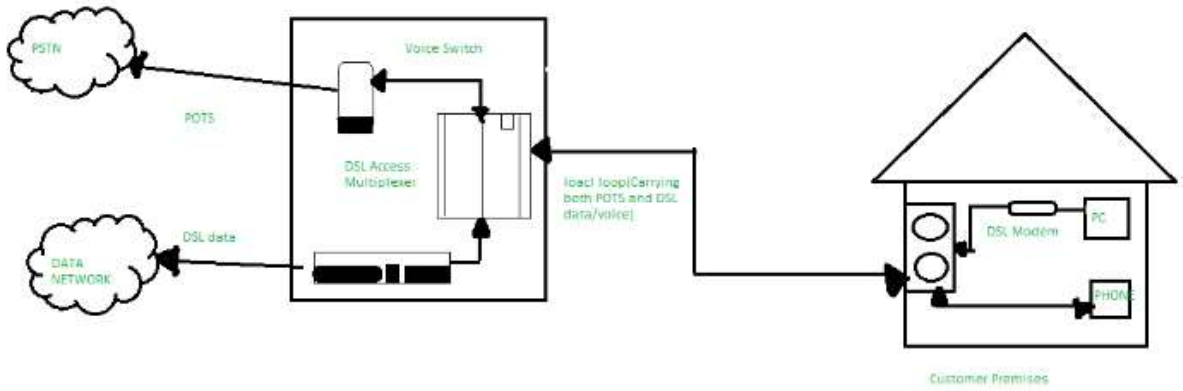
56K dial-up modem used at a customer site

Digital Subscriber Line (DSL)

The Digital Subscriber Line (DSL), *originally*, a **digital subscriber loop** is a communication medium, which is used to transfer the internet through copper wire telecommunication lines. Along with cable internet, DSL is one of the most popular ways *ISPs* provide broadband internet access.

Properties of DSL

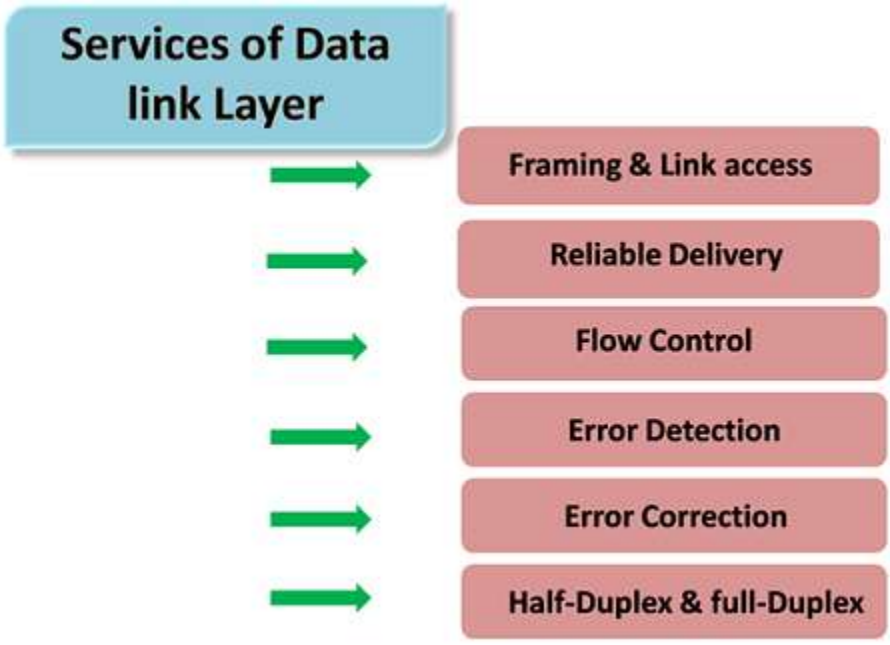
- Its aim is to maintain the high speed of the data being transferred.
- If we ask how we going to achieve such a thing i.e., both telephone and internet facilities, then the answer is by using splitters or DSL *filters*(shown in the below diagram). Basically, the *splitter* is used to split the frequency and make sure that it can't get interrupted.



Data Link Layer

- In the OSI model, the data link layer is a 4th layer from the top and 2nd layer from the bottom.
- The communication channel that connects the adjacent nodes is known as links, and in order to move the datagram from source to the destination, the datagram must be moved across an individual link.
- The main responsibility of the Data Link Layer is to transfer the datagram across an individual link.
- The Data link layer protocol defines the format of the packet exchanged across the nodes as well as the actions such as Error detection, retransmission, flow control, and random access.
- The Data Link Layer protocols are Ethernet, token ring, FDDI and PPP.
- An important characteristic of a Data Link Layer is that datagram can be handled by different link layer protocols on different links in a path. For example, the datagram is handled by Ethernet on the first link, PPP on the second link.

Following services are provided by the Data Link Layer:

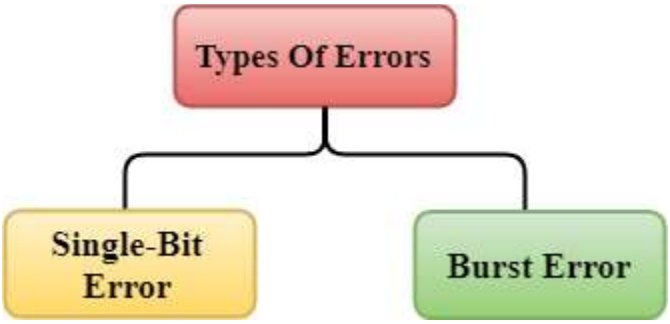


- **Framing & Link access:** Data Link Layer protocols encapsulate each network frame within a Link layer frame before the transmission across the link. A frame consists of a data field in which network layer datagram is inserted and a number of data fields. It specifies the structure of the frame as well as a channel access protocol by which frame is to be transmitted over the link.
- **Reliable delivery:** Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A reliable delivery service is accomplished with transmissions and acknowledgements. A data link layer mainly provides the reliable delivery service over the links as they have higher error rates and they can be corrected locally, link at which an error occurs rather than forcing to retransmit the data.
- **Flow control:** A receiving node can receive the frames at a faster rate than it can process the frame. Without flow control, the receiver's buffer can overflow, and frames can get lost. To overcome this problem, the data link layer uses the flow control to prevent the sending node on one side of the link from overwhelming the receiving node on another side of the link.
- **Error detection:** Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors. This is achieved by adding error detection bits in the frame and then receiving node can perform an error check.
- **Error correction:** Error correction is similar to the Error detection, except that receiving node not only detect the errors but also determine where the errors have occurred in the frame.
- **Half-Duplex & Full-Duplex:** In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.

Error Detection

When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device. An Error is a situation when the message received at the receiver end is not identical to the message transmitted.

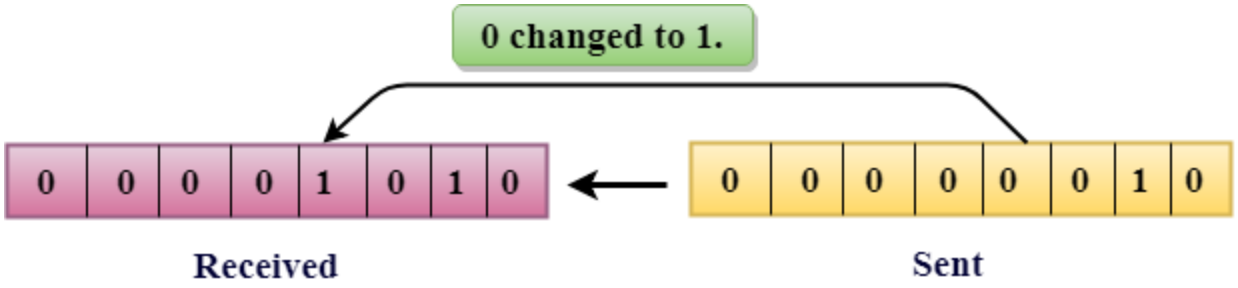
Types Of Errors



Errors can be classified into two categories:

- Single-Bit Error
- Burst Error

Single-Bit Error:
The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



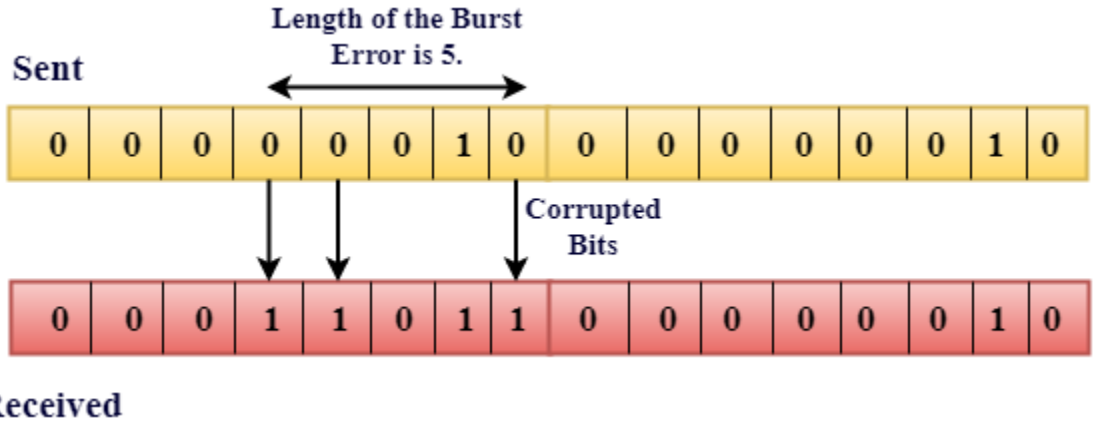
In the above figure, the message which is sent is corrupted as single-bit, i.e., 0 bit is changed to 1.

Single-Bit Error does not appear more likely in Serial Data Transmission. For example, Sender sends the data at 10 Mbps, this means that the bit lasts only for 1 ?s and for a single-bit error to occurred, a noise must be more than 1 ?s.

Single-Bit Error mainly occurs in Parallel Data Transmission. For example, if eight wires are used to send the eight bits of a byte, if one of the wire is noisy, then single-bit is corrupted per byte.

Burst Error:
The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.

The Burst Error is determined from the first corrupted bit to the last corrupted bit.



The duration of noise in Burst Error is more than the duration of noise in Single-Bit.

Burst Errors are most likely to occurr in Serial Data Transmission.

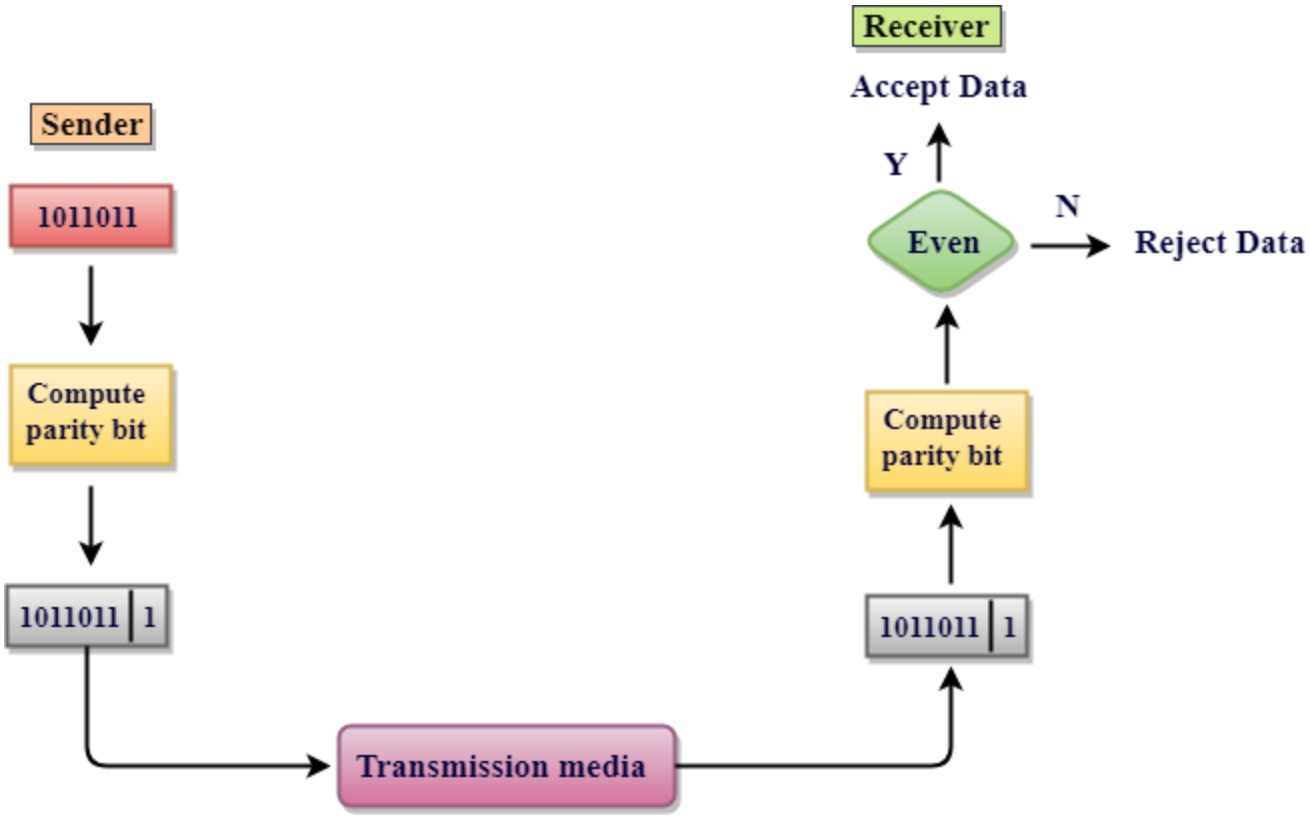
The number of affected bits depends on the duration of the noise and data rate.

Error Detecting Techniques:
The most popular Error Detecting Techniques are:

- Single parity check
- Two-dimensional parity check
- Checksum
- Cyclic redundancy check

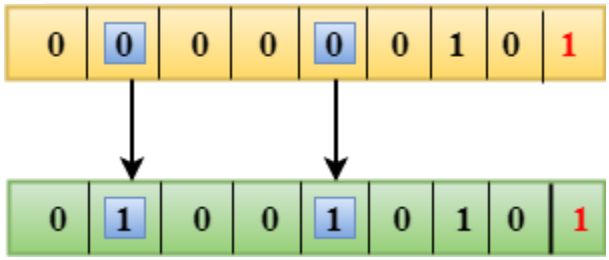
Single Parity Check

- Single Parity checking is the simple mechanism and inexpensive to detect the errors.
- In this technique, a redundant bit is also known as a parity bit which is appended at the end of the data unit so that the number of 1s becomes even. Therefore, the total number of transmitted bits would be 9 bits.
- If the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.
- At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.
- This technique generates the total number of 1s even, so it is known as even-parity checking.



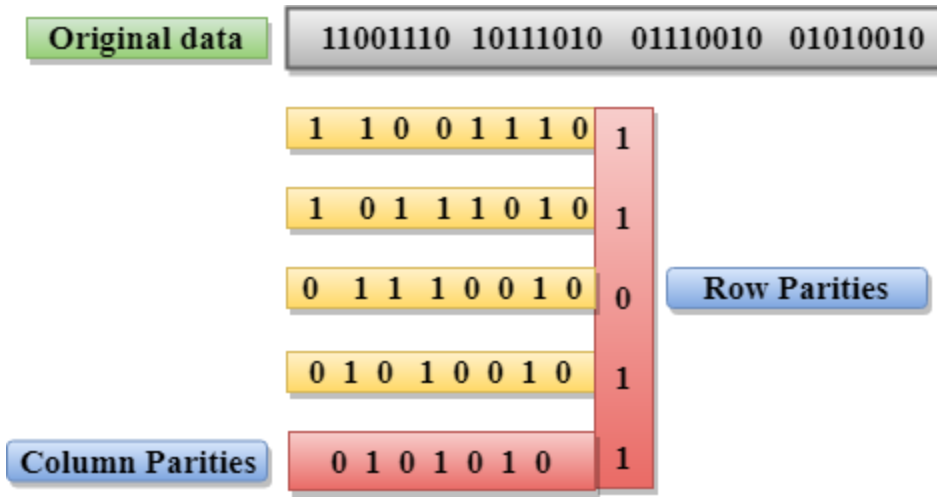
Drawbacks Of Single Parity Checking

- It can only detect single-bit errors which are very rare.
- If two bits are interchanged, then it cannot detect the errors.



Two-Dimensional Parity Check

- Performance can be improved by using **Two-Dimensional Parity Check** which organizes the data in the form of a table.
- Parity check bits are computed for each row, which is equivalent to the single-parity check.
- In Two-Dimensional Parity check, a block of bits is divided into rows, and the redundant row of bits is added to the whole block.
- At the receiving end, the parity bits are compared with the parity bits computed from the received data.



Drawbacks Of 2D Parity Check

- If two bits in one data unit are corrupted and two bits exactly the same position in another data unit are also corrupted, then 2D Parity checker will not be able to detect the error.
- This technique cannot be used to detect the 4-bit errors or more in some cases.

Checksum

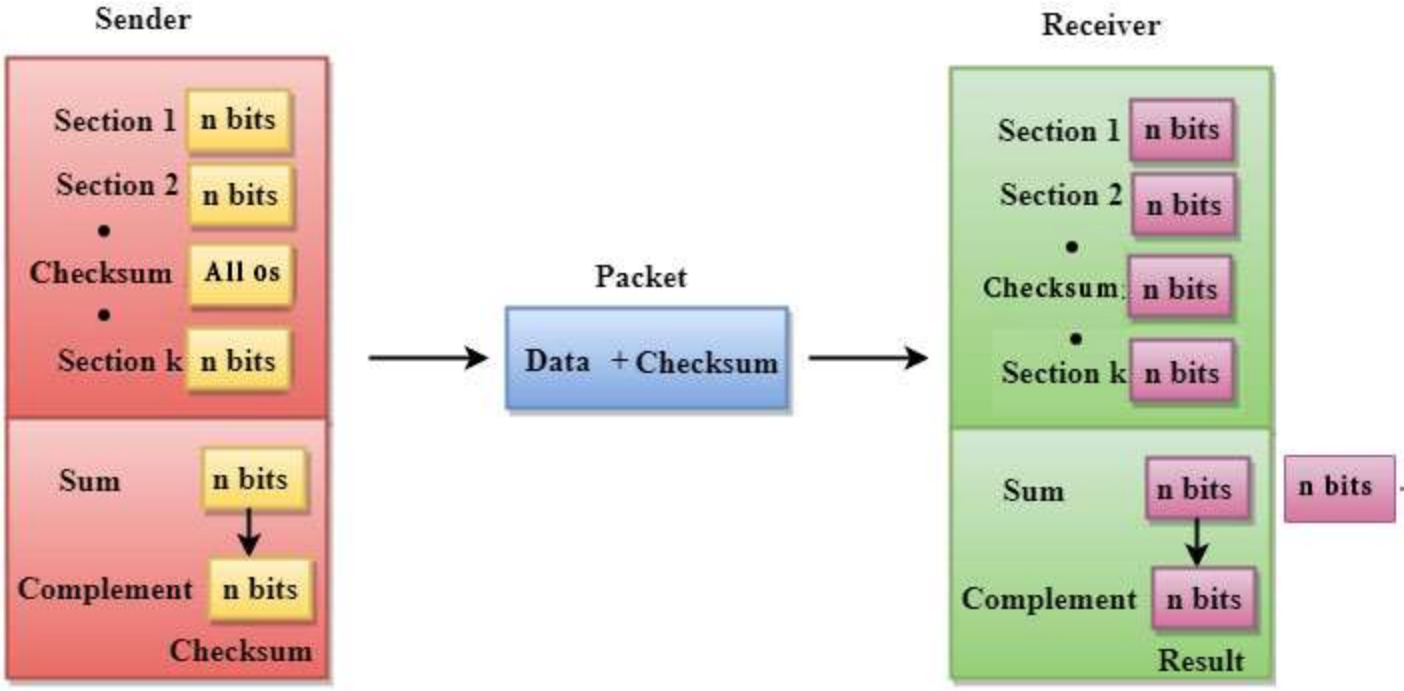
A Checksum is an error detection technique based on the concept of redundancy.

It is divided into two parts:

Checksum Generator

A Checksum is generated at the sending side. Checksum generator subdivides the data into equal segments of n bits each, and all these segments are added together by using one's complement arithmetic. The sum is complemented and appended to the original data, known as checksum field. The extended data is transmitted across the network.

Suppose L is the total sum of the data segments, then the checksum would be ?L



1. The Sender follows the given steps:
2. The block unit is divided into k sections, and each of n bits.
3. All the k sections are added together by using one's complement to get the sum.
4. The sum is complemented and it becomes the checksum field.
5. The original data and checksum field are sent across the network.

Checksum Checker

A Checksum is verified at the receiving side. The receiver subdivides the incoming data into equal segments of n bits each, and all these segments are added together, and then this sum is complemented. If the complement of the sum is zero, then the data is accepted otherwise data is rejected.

1. The Receiver follows the given steps:
2. The block unit is divided into k sections and each of n bits.
3. All the k sections are added together by using one's complement algorithm to get the sum.
4. The sum is complemented.
5. If the result of the sum is zero, then the data is accepted otherwise the data is discarded.

Cyclic Redundancy Check (CRC)

CRC is a redundancy error technique used to determine the error.

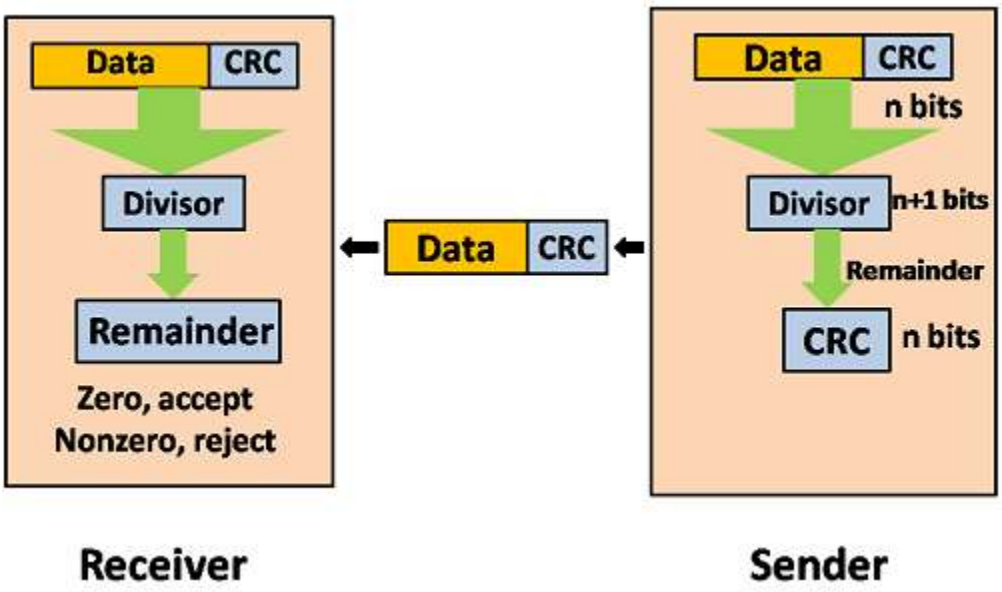
Following are the steps used in CRC for error detection:

- In CRC technique, a string of n 0s is appended to the data unit, and this n number is less than the number of bits in a predetermined number, known as division which is n+1 bits.

- Secondly, the newly extended data is divided by a divisor using a process is known as binary division. The remainder generated from this division is known as CRC remainder.
- Thirdly, the CRC remainder replaces the appended 0s at the end of the original data. This newly generated unit is sent to the receiver.
- The receiver receives the data followed by the CRC remainder. The receiver will treat this whole unit as a single unit, and it is divided by the same divisor that was used to find the CRC remainder.

If the resultant of this division is zero which means that it has no error, and the data is accepted.

If the resultant of this division is not zero which means that the data consists of an error. Therefore, the data is discarded.

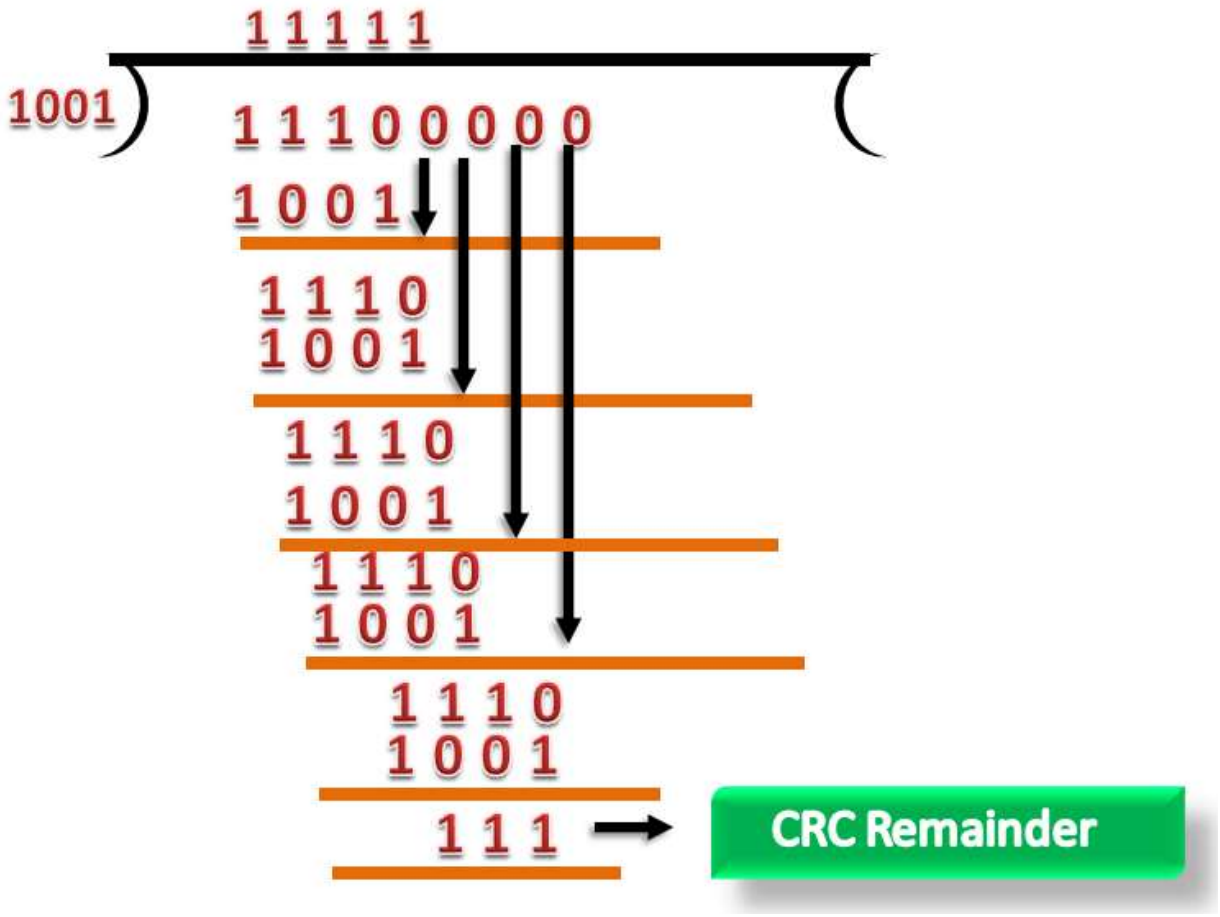


Let's understand this concept through an example:

Suppose the original data is 11100 and divisor is 1001.

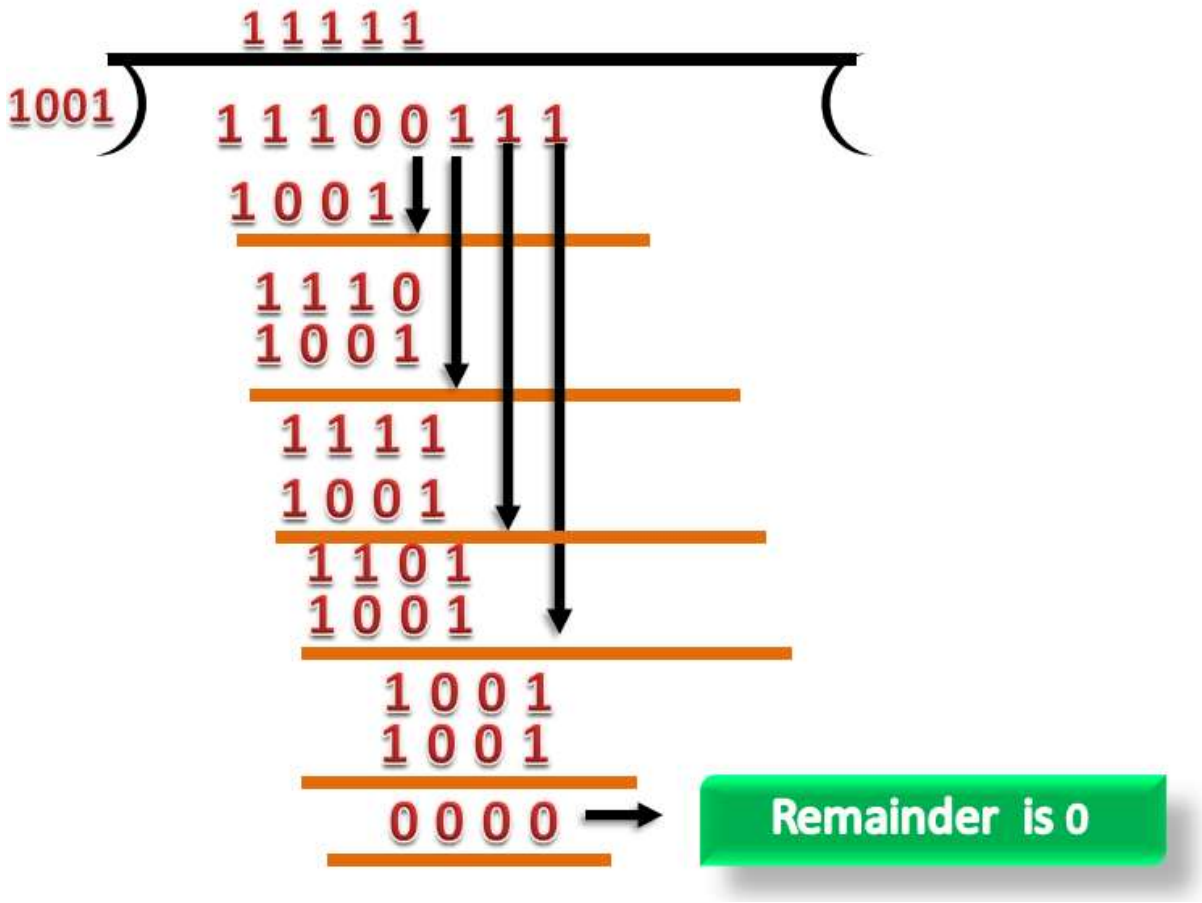
CRC Generator

- A CRC generator uses a modulo-2 division. Firstly, three zeroes are appended at the end of the data as the length of the divisor is 4 and we know that the length of the string 0s to be appended is always one less than the length of the divisor.
- Now, the string becomes 11100000, and the resultant string is divided by the divisor 1001.
- The remainder generated from the binary division is known as CRC remainder. The generated value of the CRC remainder is 111.
- CRC remainder replaces the appended string of 0s at the end of the data unit, and the final string would be 11100111 which is sent across the network.



CRC Checker

- The functionality of the CRC checker is similar to the CRC generator.
- When the string 11100111 is received at the receiving end, then CRC checker performs the modulo-2 division.
- A string is divided by the same divisor, i.e., 1001.
- In this case, CRC checker generates the remainder of zero. Therefore, the data is accepted.



Stop and Wait Protocol

Before understanding the stop and Wait protocol, we first know about the error control mechanism. The error control mechanism is used so that the received data should be exactly same whatever sender has sent the data. The error control mechanism is divided into two categories, i.e., Stop and Wait ARQ and sliding window. The sliding window is further divided into two categories, i.e., Go Back N, and Selective Repeat. Based on the usage, the people select the error control mechanism whether it is **stop and wait** or **sliding window**.

What is Stop and Wait protocol?

Here stop and wait means, whatever the data that sender wants to send, he sends the data to the receiver. After sending the data, he stops and waits until he receives the acknowledgment from the receiver. The stop and wait protocol is a flow control protocol where flow control is one of the services of the data link layer.

It is a data-link layer protocol which is used for transmitting the data over the noiseless channels. It provides unidirectional data transmission which means that either sending or receiving of data will take place at a time. It provides flow-control mechanism but does not provide any error control mechanism.

The idea behind the usage of this frame is that when the sender sends the frame then he waits for the acknowledgment before sending the next frame.

Primitives of Stop and Wait Protocol

The primitives of stop and wait protocol are:

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.

Therefore, the idea of stop and wait protocol in the sender's side is very simple, i.e., send one packet at a time, and do not send another packet before receiving the acknowledgment.

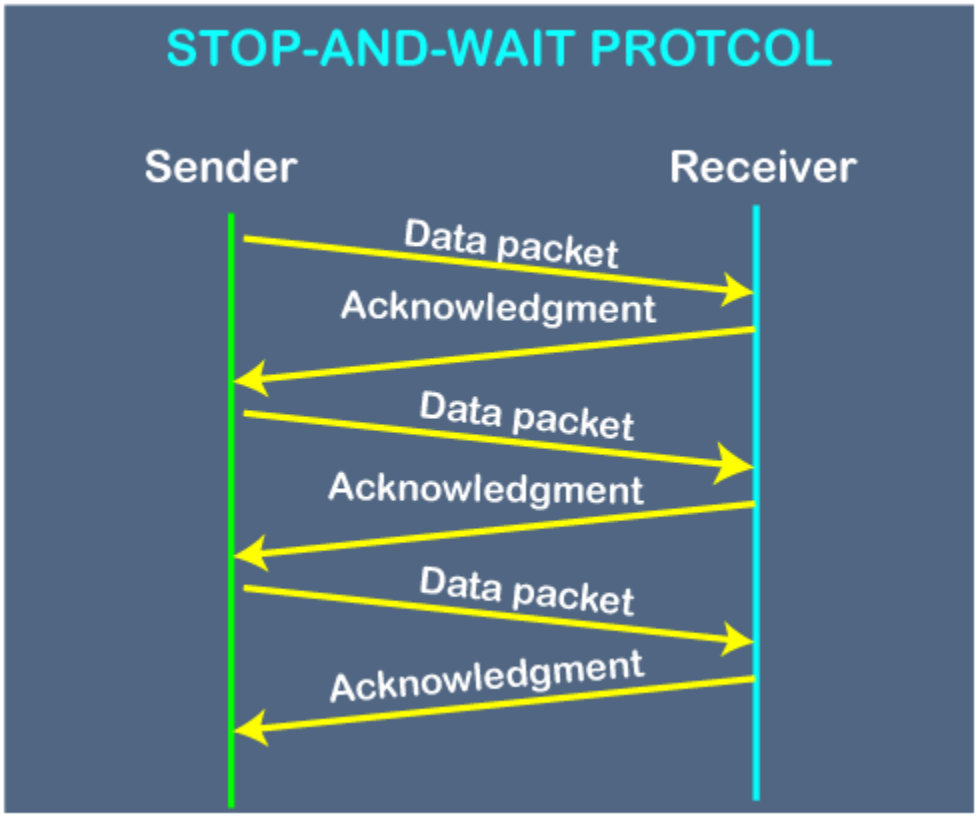
Receiver side

Rule 1: Receive and then consume the data packet.

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

Therefore, the idea of stop and wait protocol in the receiver's side is also very simple, i.e., consume the packet, and once the packet is consumed, the acknowledgment is sent. This is known as a flow control mechanism.

Working of Stop and Wait protocol

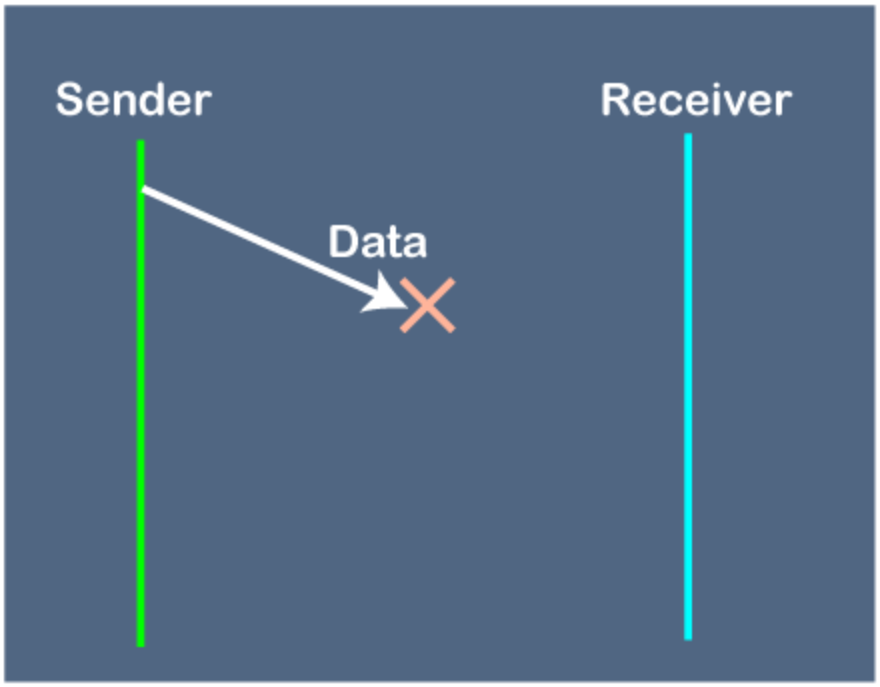


The above figure shows the working of the stop and wait protocol. If there is a sender and receiver, then sender sends the packet and that packet is known as a data packet. The sender will not send the second packet without receiving the acknowledgment of the first packet. The receiver sends the acknowledgment for the data packet that it has received. Once the acknowledgment is received, the sender sends the next packet. This process continues until all the packet are not sent. The main advantage of this protocol is its simplicity but it has some disadvantages also. For example, if there are 1000 data packets to be sent, then all the 1000 packets cannot be sent at a time as in Stop and Wait protocol, one packet is sent at a time.

Disadvantages of Stop and Wait protocol

The following are the problems associated with a stop and wait protocol:

1. Problems occur due to lost data

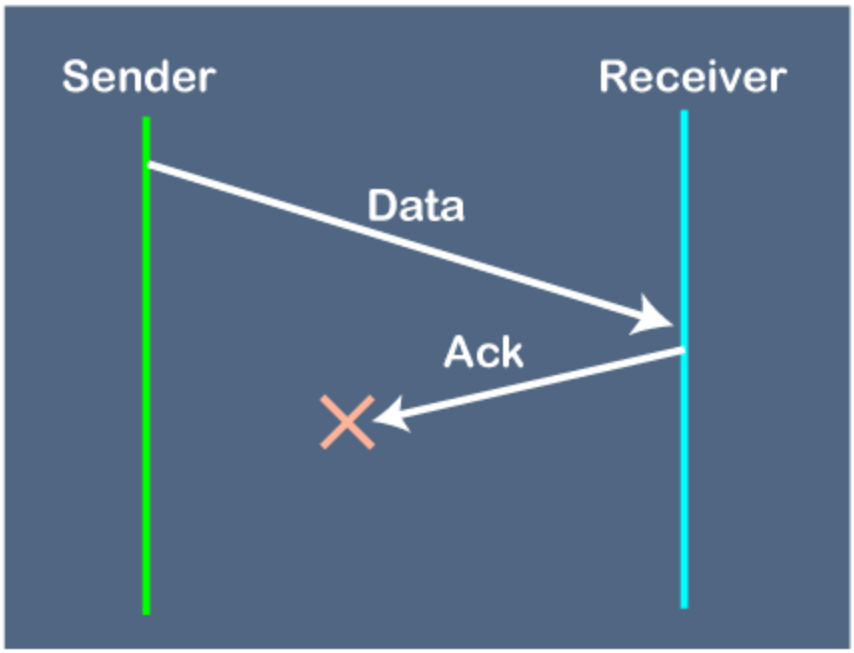


Suppose the sender sends the data and the data is lost. The receiver is waiting for the data for a long time. Since the data is not received by the receiver, so it does not send any acknowledgment. Since the sender does not receive any acknowledgment so it will not send the next packet. This problem occurs due to the lost data.

In this case, two problems occur:

- Sender waits for an infinite amount of time for an acknowledgment.
- Receiver waits for an infinite amount of time for a data.

2. Problems occur due to lost acknowledgment

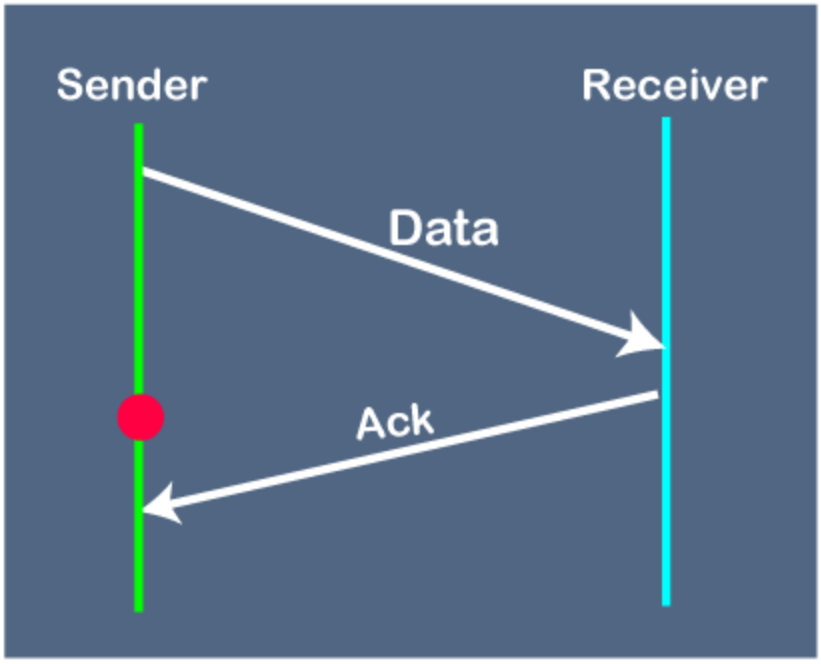


Suppose the sender sends the data and it has also been received by the receiver. On receiving the packet, the receiver sends the acknowledgment. In this case, the acknowledgment is lost in a network, so there is no chance for the sender to receive the acknowledgment. There is also no chance for the sender to send the next packet as in stop and wait protocol, the next packet cannot be sent until the acknowledgment of the previous packet is received.

In this case, one problem occurs:

- Sender waits for an infinite amount of time for an acknowledgment.

3. Problem due to the delayed data or acknowledgment



Suppose the sender sends the data and it has also been received by the receiver. The receiver then sends the acknowledgment but the acknowledgment is received after the timeout period on the sender's side. As the acknowledgment is received late, so acknowledgment can be wrongly considered as the acknowledgment of some other data packet.

Go-Back-N ARQ

Before understanding the working of Go-Back-N ARQ, we first look at the sliding window protocol. As we know that the sliding window protocol is different from the stop-and-wait protocol. In the stop-and-wait protocol, the sender can send only one frame at a time and cannot send the next frame without receiving the acknowledgment of the previously sent frame, whereas, in the case of sliding window protocol, the multiple frames can be sent at a time. The variations of sliding window protocol are Go-Back-N ARQ and Selective Repeat ARQ. Let's understand 'what is Go-Back-N ARQ'.

What is Go-Back-N ARQ?

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 we have five frames and the concept is Go-Back-3, which means that the three frames can be sent, i.e., frame no 1, frame no 2, frame no 3 can be sent before expecting the acknowledgment of frame no 1.

In Go-Back-N ARQ, the frames are numbered sequentially as Go-Back-N ARQ sends the multiple frames at a time that requires the numbering approach to distinguish the frame from another frame, and these numbers are known as the sequential numbers.

The number of frames that can be sent at a time totally depends on the size of the sender's window. So, we can say that 'N' is the number of frames that can be sent at a time before receiving the acknowledgment from the receiver.

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. Suppose we have sent the frame no 5, but we didn't receive the acknowledgment of frame no 5, and the current window is holding three frames, then these three frames will be retransmitted.

The sequence number of the outbound frames depends upon the size of the sender's window. Suppose the sender's window size is 2, and we have ten frames to send, then the sequence numbers will not be 1,2,3,4,5,6,7,8,9,10. Let's understand through an example.

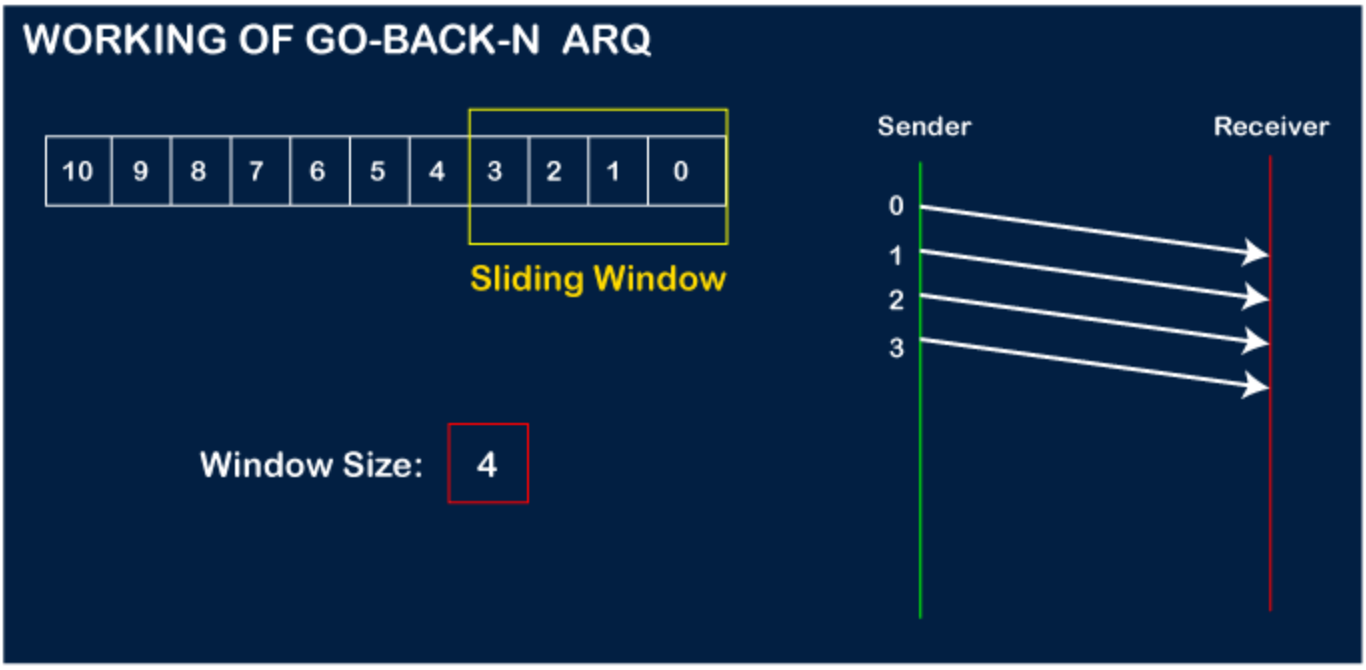
- N is the sender's window size.
- If the size of the sender's window is 4 then the sequence number will be 0,1,2,3,0,1,2,3,0,1,2, and so on.

The number of bits in the sequence number is 2 to generate the binary sequence 00,01,10,11.

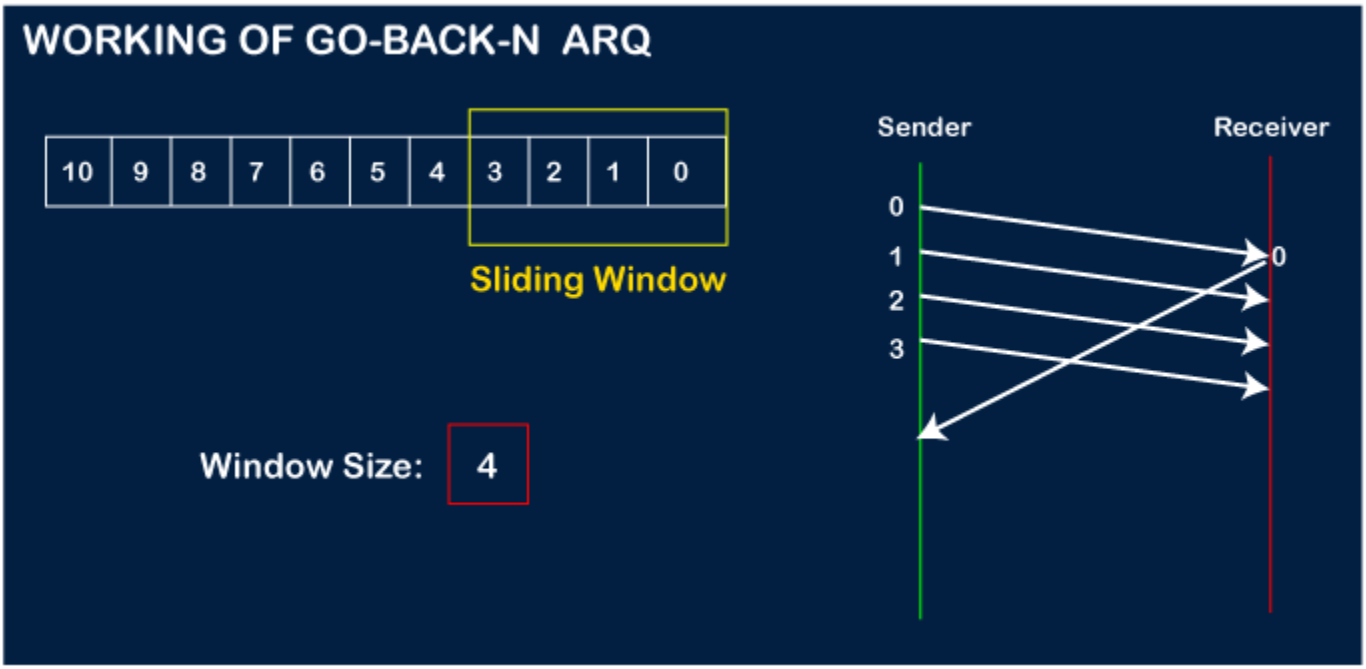
Working of Go-Back-N ARQ

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, and these are the sequence numbers of the frames. Mainly, the sequence number is decided by the sender's window size. But, for the better understanding, we took the running sequence numbers, i.e., 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.

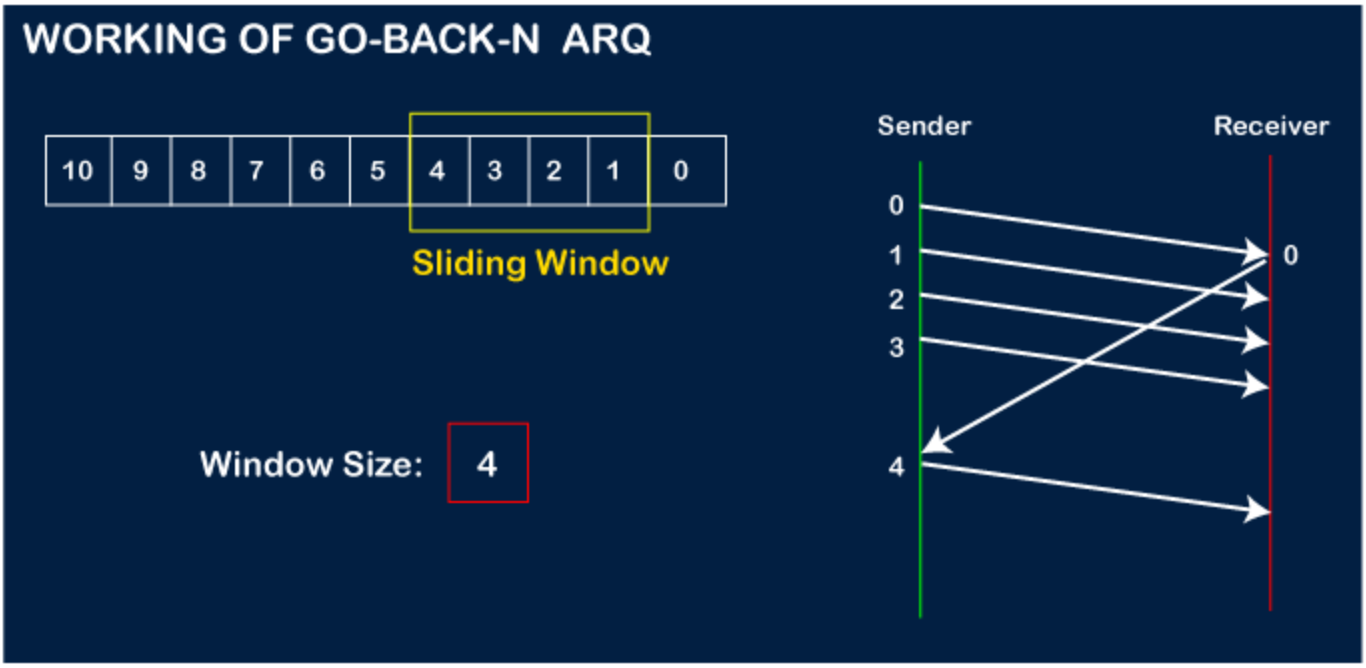
Step 1: Firstly, the sender will send the first four frames to the receiver, i.e., 0,1,2,3, and now the sender is expected to receive the acknowledgment of the 0^{th} frame.



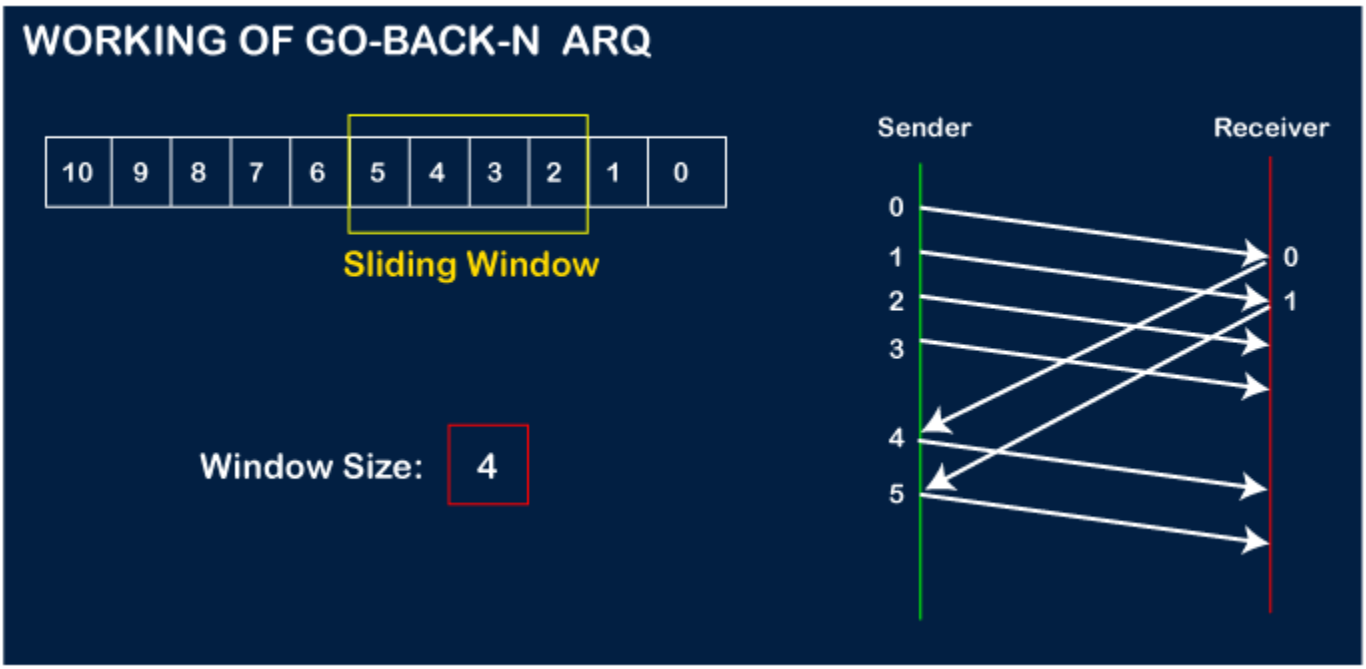
Let's assume that the receiver has sent the acknowledgment for the 0 frame, and the receiver has successfully received it.



The sender will then send the next frame, i.e., 4, and the window slides containing four frames (1,2,3,4).

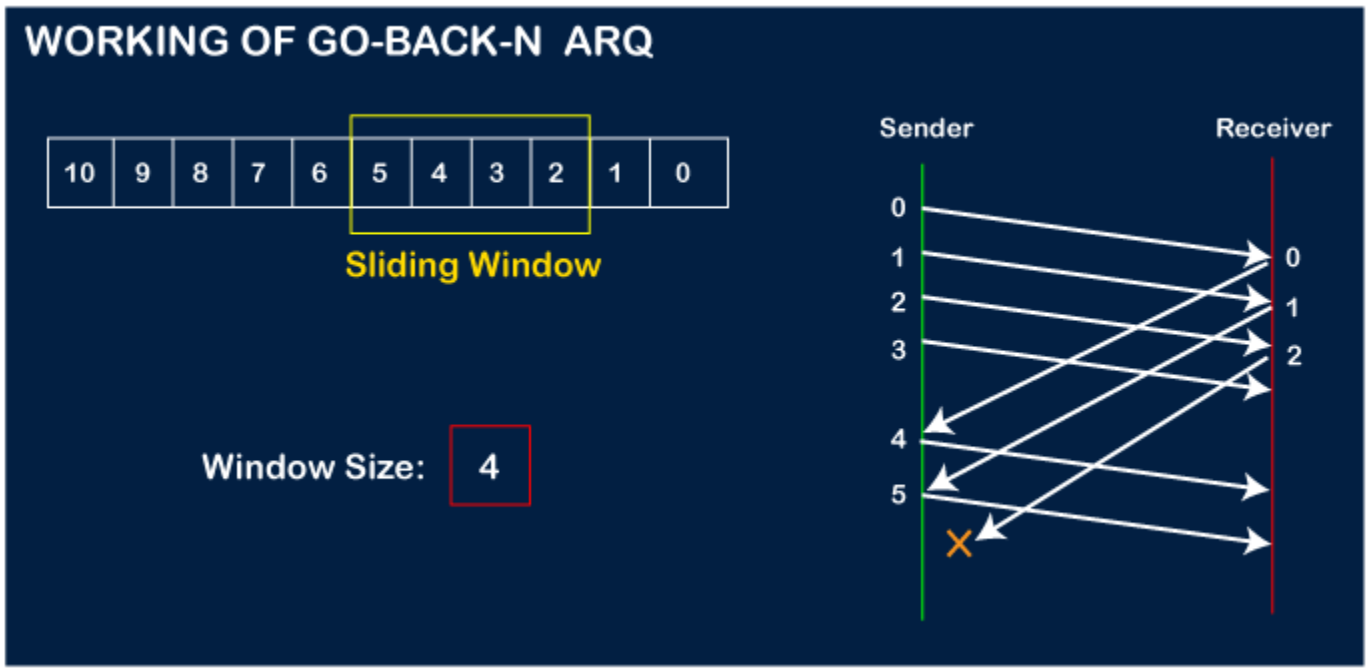


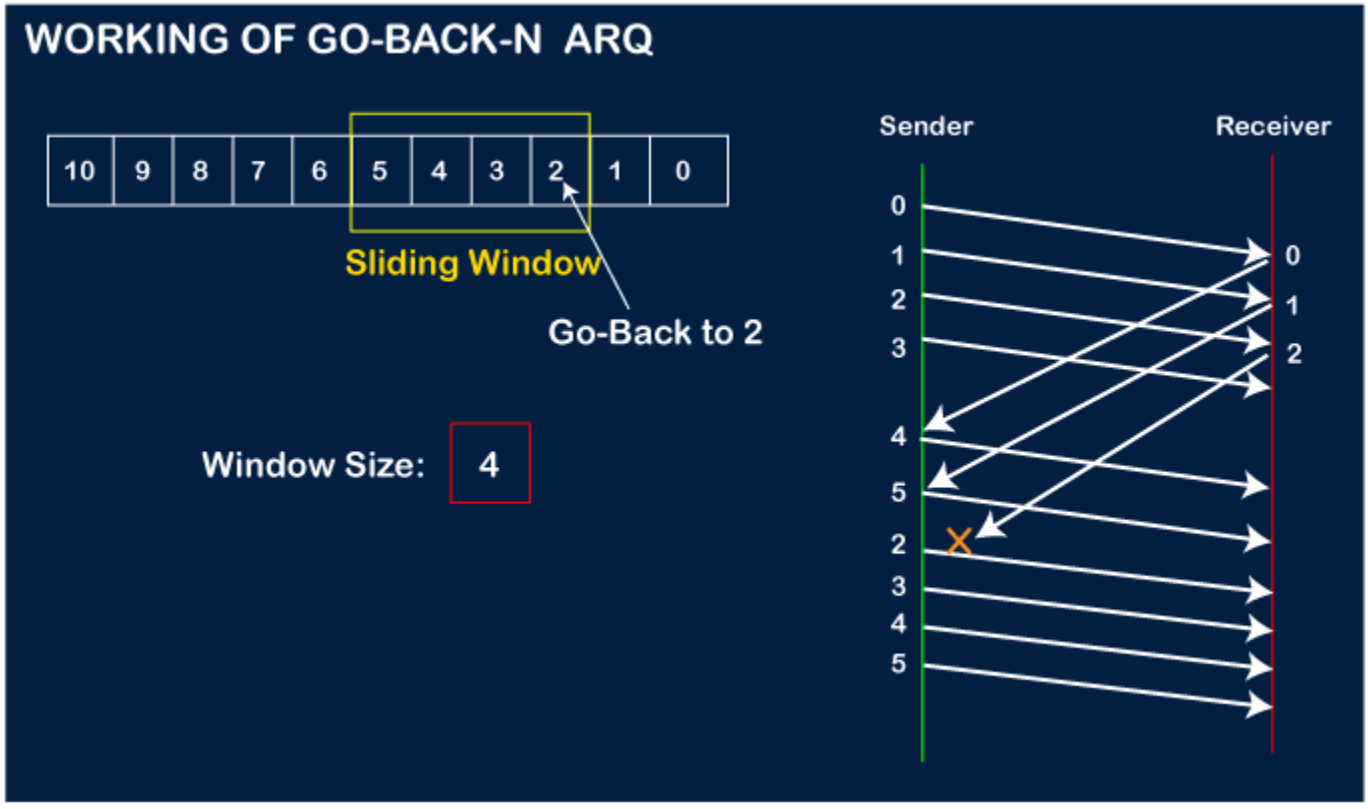
The receiver will then send the acknowledgment for the frame no 1. After receiving the acknowledgment, the sender will send the next frame, i.e., frame no 5, and the window will slide having four frames (2,3,4,5).



Now, let's assume that the receiver is not acknowledging the frame no 2, either the frame is lost, or the acknowledgment is lost. Instead of sending the frame no 6, the sender Go-Back to 2,

which is the first frame of the current window, retransmits all the frames in the current window, i.e., 2,3,4,5.





Important points related to Go-Back-N ARQ:

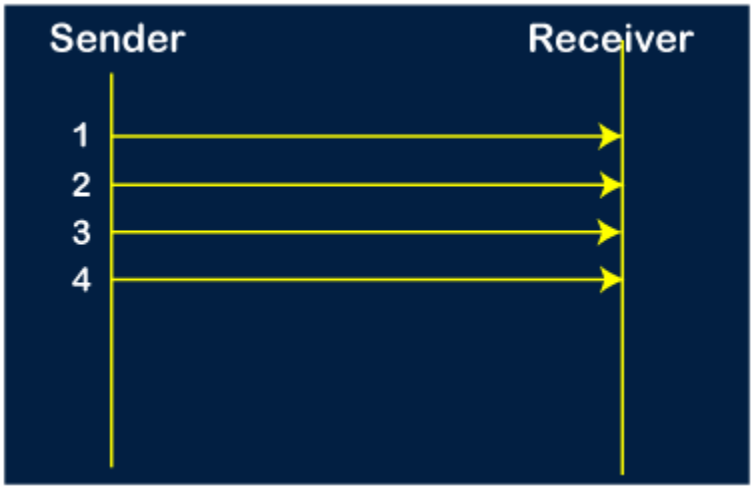
- In Go-Back-N, N determines the sender's window size, and the size of the receiver's window is always 1.
- It does not consider the corrupted frames and simply discards them.
- It does not accept the frames which are out of order and discards them.
- If the sender does not receive the acknowledgment, it leads to the retransmission of all the current window frames.

Let's understand the Go-Back-N ARQ through an example.

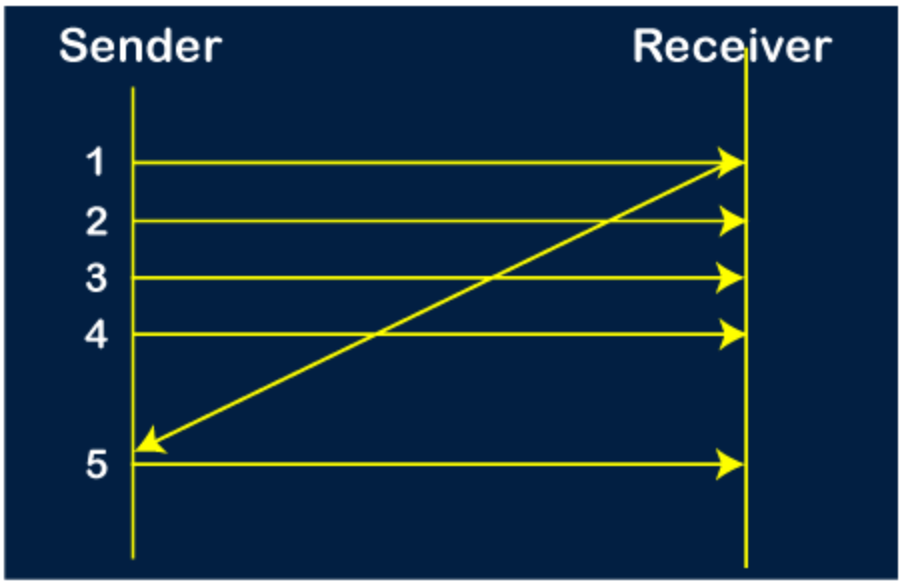
Example 1: In GB4, if every 6th packet being transmitted is lost and if we have to spend 10 packets then how many transmissions are required?

Solution: Here, GB4 means that N is equal to 4. The size of the sender's window is 4.

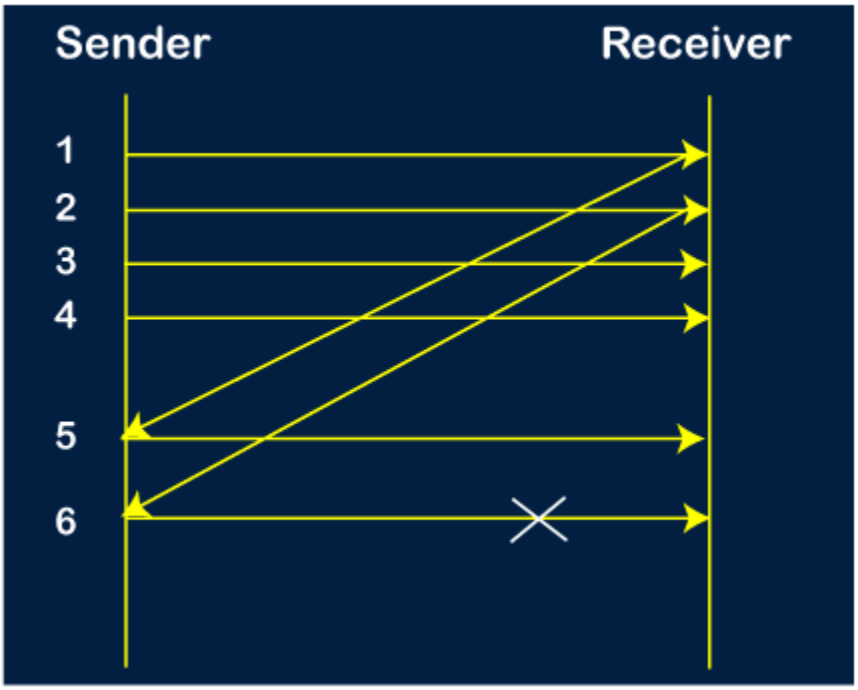
Step 1: As the window size is 4, so four packets are transferred at a time, i.e., packet no 1, packet no 2, packet no 3, and packet no 4.



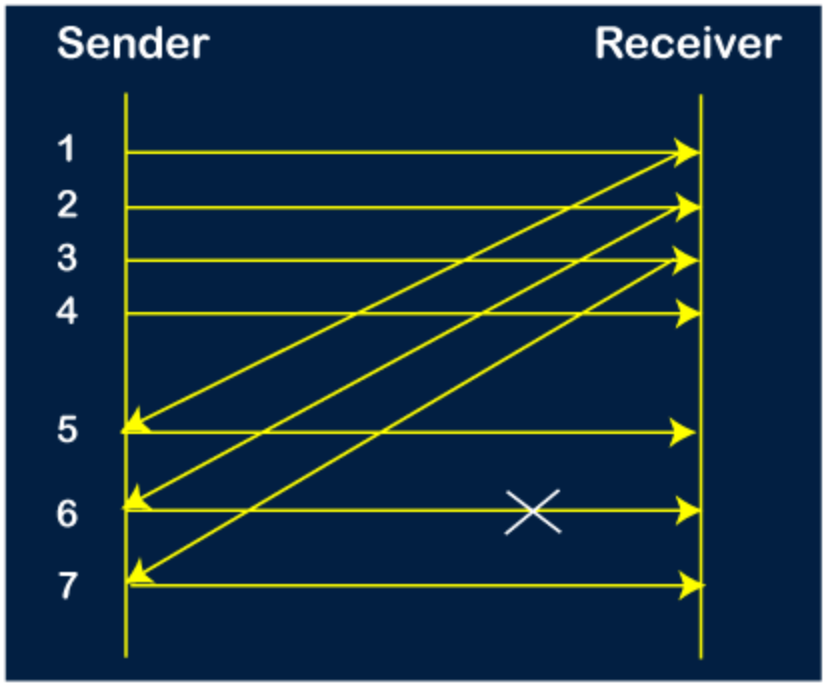
Step 2: Once the transfer of window size is completed, the sender receives the acknowledgment of the first frame, i.e., packet no1. As the acknowledgment receives, the sender sends the next packet, i.e., packet no 5. In this case, the window slides having four packets, i.e., 2,3,4,5 and excluded the packet 1 as the acknowledgment of the packet 1 has been received successfully.



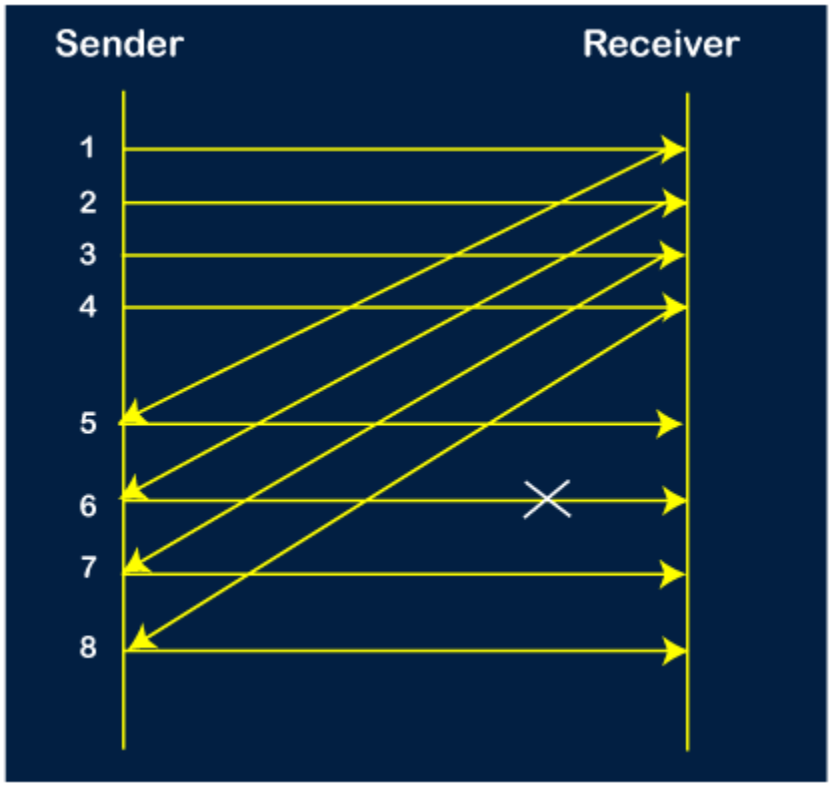
Step 3: Now, the sender receives the acknowledgment of packet 2. After receiving the acknowledgment for packet 2, the sender sends the next packet, i.e., packet no 6. As mentioned in the question that every 6th is being lost, so this 6th packet is lost, but the sender does not know that the 6th packet has been lost.



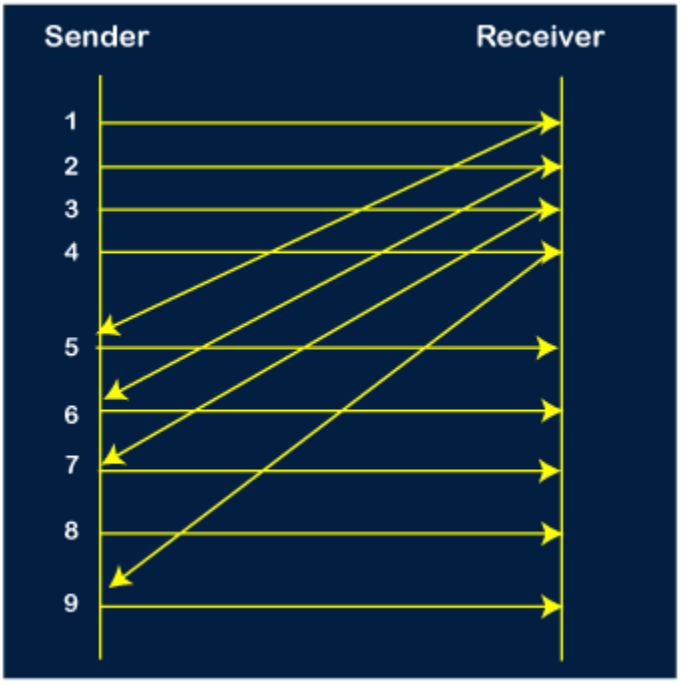
Step 4: The sender receives the acknowledgment for the packet no 3. After receiving the acknowledgment of 3rd packet, the sender sends the next packet, i.e., 7th packet. The window will slide having four packets, i.e., 4, 5, 6, 7.



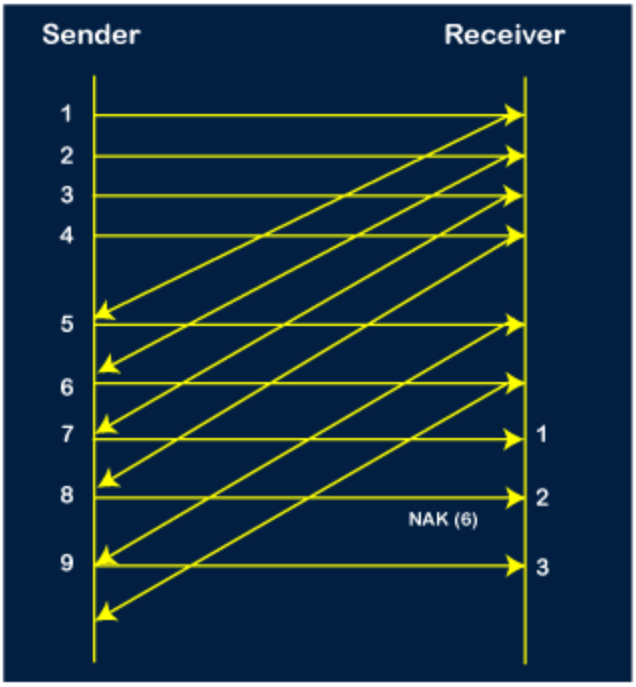
Step 5: When the packet 7 has been sent, then the sender receives the acknowledgment for the packet no 4. When the sender has received the acknowledgment, then the sender sends the next packet, i.e., the 8th packet. The window will slide having four packets, i.e., 5, 6, 7, 8.



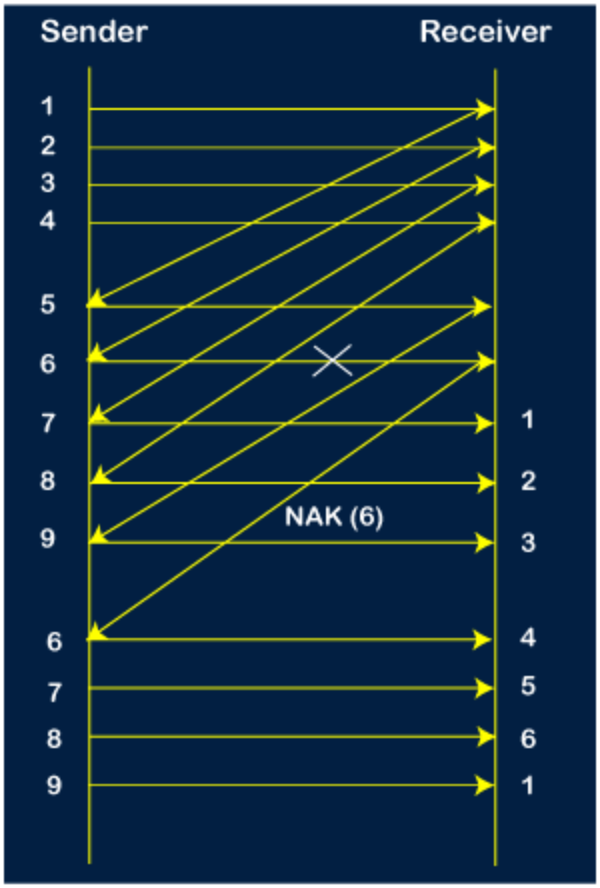
Step 6: When the packet 8 is sent, then the sender receives the acknowledgment of packet 5. On receiving the acknowledgment of packet 5, the sender sends the next packet, i.e., 9th packet. The window will slide having four packets, i.e., 6, 7, 8, 9.



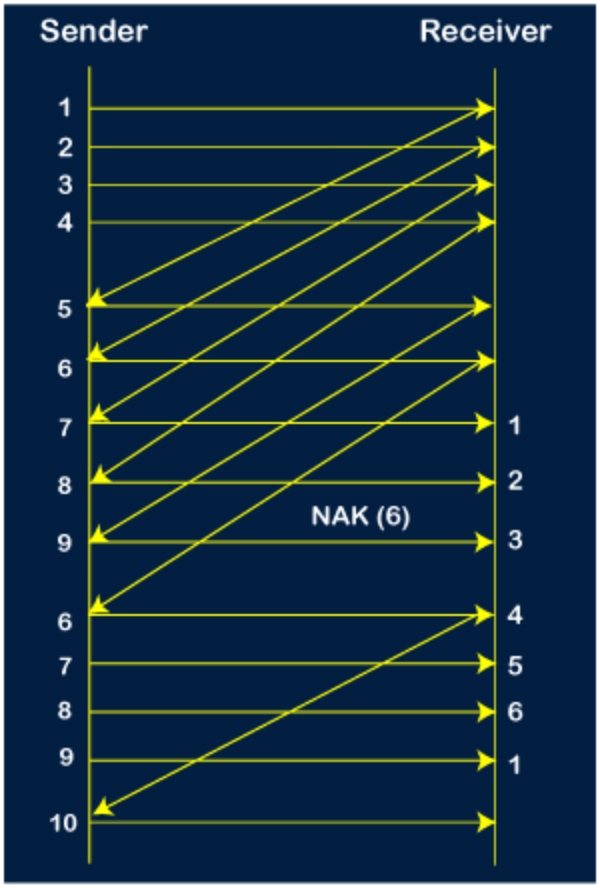
Step 7: The current window is holding four packets, i.e., 6, 7, 8, 9, where the 6th packet is the first packet in the window. As we know, the 6th packet has been lost, so the sender receives the negative acknowledgment NAK(6). As we know that every 6th packet is being lost, so the counter will be restarted from 1. So, the counter values 1, 2, 3 are given to the 7th packet, 8th packet, 9th packet respectively.



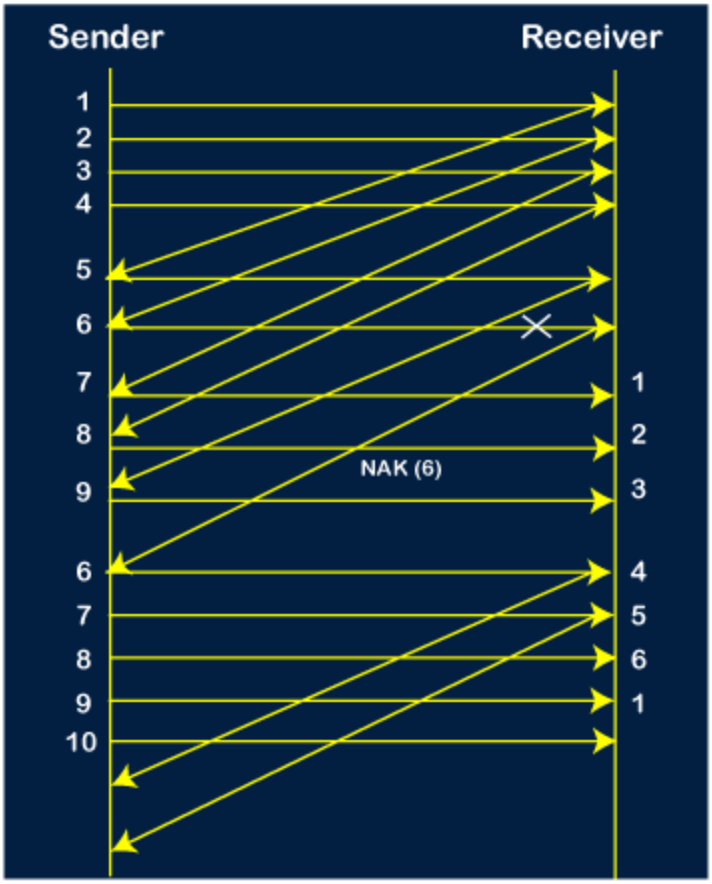
Step 8: As it is Go-BACK, so it retransmits all the packets of the current window. It will resend 6, 7, 8, 9. The counter values of 6, 7, 8, 9 are 4, 5, 6, 1, respectively. In this case, the 8th packet is lost as it has a 6-counter value, so the counter variable will again be restarted from 1.



Step 9: After the retransmission, the sender receives the acknowledgment of packet 6. On receiving the acknowledgment of packet 6, the sender sends the 10^{th} packet. Now, the current window is holding four packets, i.e., 7, 8, 9, 10.

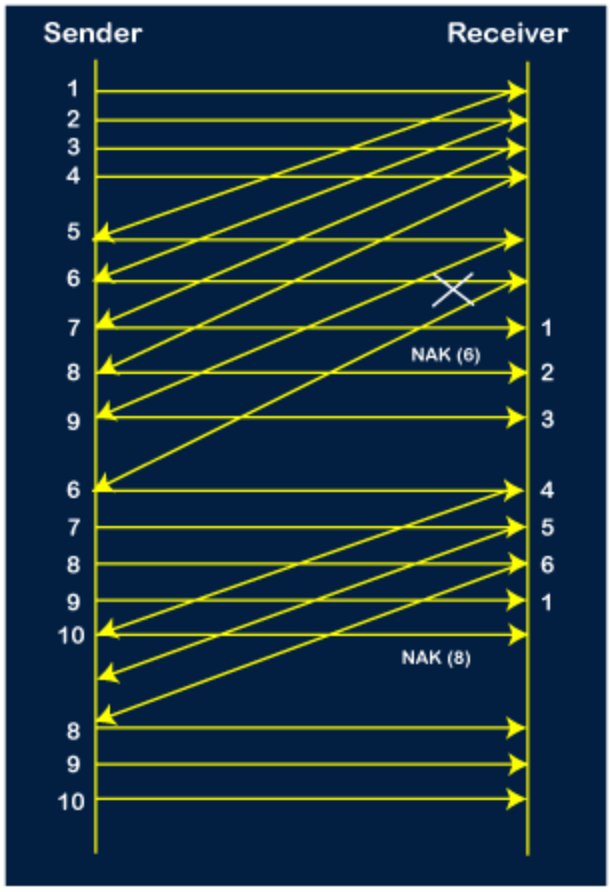


Step 10: When the 10th packet is sent, the sender receives the acknowledgment of packet 7. Now the current window is holding three packets, 8, 9 and 10. The counter values of 8, 9, 10 are 6, 1, 2.



Step 11: As the 8th packet has 6 counter value which means that 8th packet has been lost, and the sender receives NAK (8).

Step 12: Since the sender has received the negative acknowledgment for the 8th packet, it resends all the packets of the current window, i.e., 8, 9, 10.

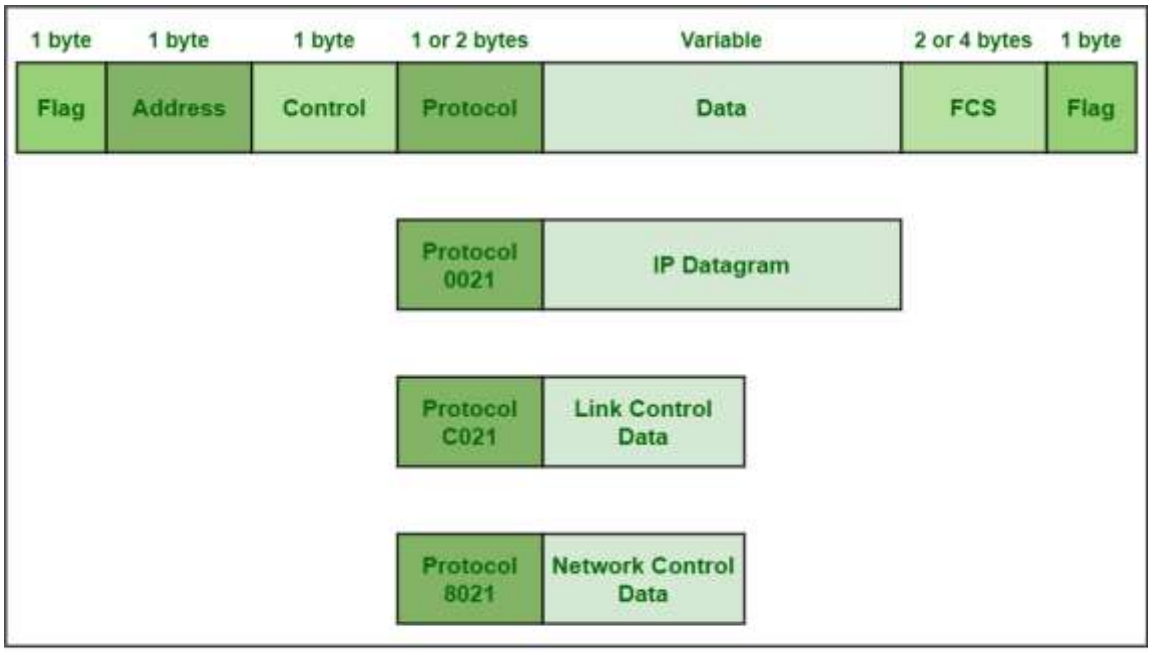


Step 13: The counter values of 8, 9, 10 are 3, 4, 5, respectively, so their acknowledgments have been received successfully.

We conclude from the above figure that total 17 transmissions are required.

Point-to-Point Protocol (PPP) Frame Format

Point-to-Point Protocol (PPP) is generally the default RAS protocol in Windows and is most commonly used protocol of data link layer that is required to encapsulate higher network-layer protocols simply to pass over synchronous and asynchronous communication lines. In PPP, link establishment is controlled and handled mainly by Link Control Protocol (LCP). It is also required to connect the Home PC to server of ISP through a modem. It was also adopted by ISPs to simply provide dial-up Internet Access. **PPP Frame Format :** PPP frame is generally required to encapsulate packets of information or data that simply includes either configuration information or data. PPP basically uses the same basic format as that of HDLC. PPP usually contains one additional field i.e. protocol field. This protocol field is present just after control field and before information or data field.



PPP Frame Format

Various fields of Frame are given below :

1. **Flag field –** PPP frame similar to HDLC frame, always begins and ends with standard HDLC flag. It always has a value of 1 byte i.e., 01111110 binary value.
2. **Address field –** Address field is basically broadcast address. In this, all 1's simply indicates that all of the stations are ready to accept frame. It has the value of 1 byte i.e., 11111111 binary value. PPP on the other hand, does not provide or assign individual station addresses.
3. **Control field –** This field basically uses format of U-frame i.e., Unnumbered frame in HDLC. In HDLC, control field is required for various purposes but in PPP, this field is set to 1 byte i.e., 00000011 binary value. This 1 byte is used for a connection-less data link.
4. **Protocol field –** This field basically identifies network protocol of the datagram. It usually identifies the kind of packet in the data field i.e., what exactly is being carried in data field. This field is of 1 or 2 bytes and helps in identifies the PDU (Protocol Data Unit) that is being encapsulated by PPP frame.
5. **Data field –** It usually contains the upper layer datagram. Network layer datagram is particularly encapsulated in this field for regular PPP data frames. Length of this field is not constant rather it varies.
6. **FCS field –** This field usually contains checksum simply for identification of errors. It can be either 16 bits or 32 bits in size. It is also calculated over address, control, protocol, and even information fields. Characters are added to frame for control and handling of errors.

Notes :

- It has the ability to negotiate IP Addresses dynamically.
- It contains Link Control Protocol (LCP) simply to develop link options.
- It contains error checking for each PPP frame.
- It also has the ability to transport several protocols on a single serial connection.