Selective Repeat Algorithm

Introduction:

Selective Repeat is part of the automatic repeat request (ARQ) in the data-link layer in the computer network . With selective repeat, the sender sends a number of frames specified by a window size even without the need to wait for individual ACK from the receiver as in Go-Back-N (ARQ). The receiver may selectively reject a single frame, which may be retransmitted alone; this contrasts with other forms of ARQ, which must send every frame from that point again. The receiver accepts out-of-order frames and buffers them. The sender individually retransmits frames that have timed out.

Before we understand what is the selective repeat algorithm, we better come a little backward to see what is a frame? What do we mean by data-link layer? What is a computer network?

Computer network:

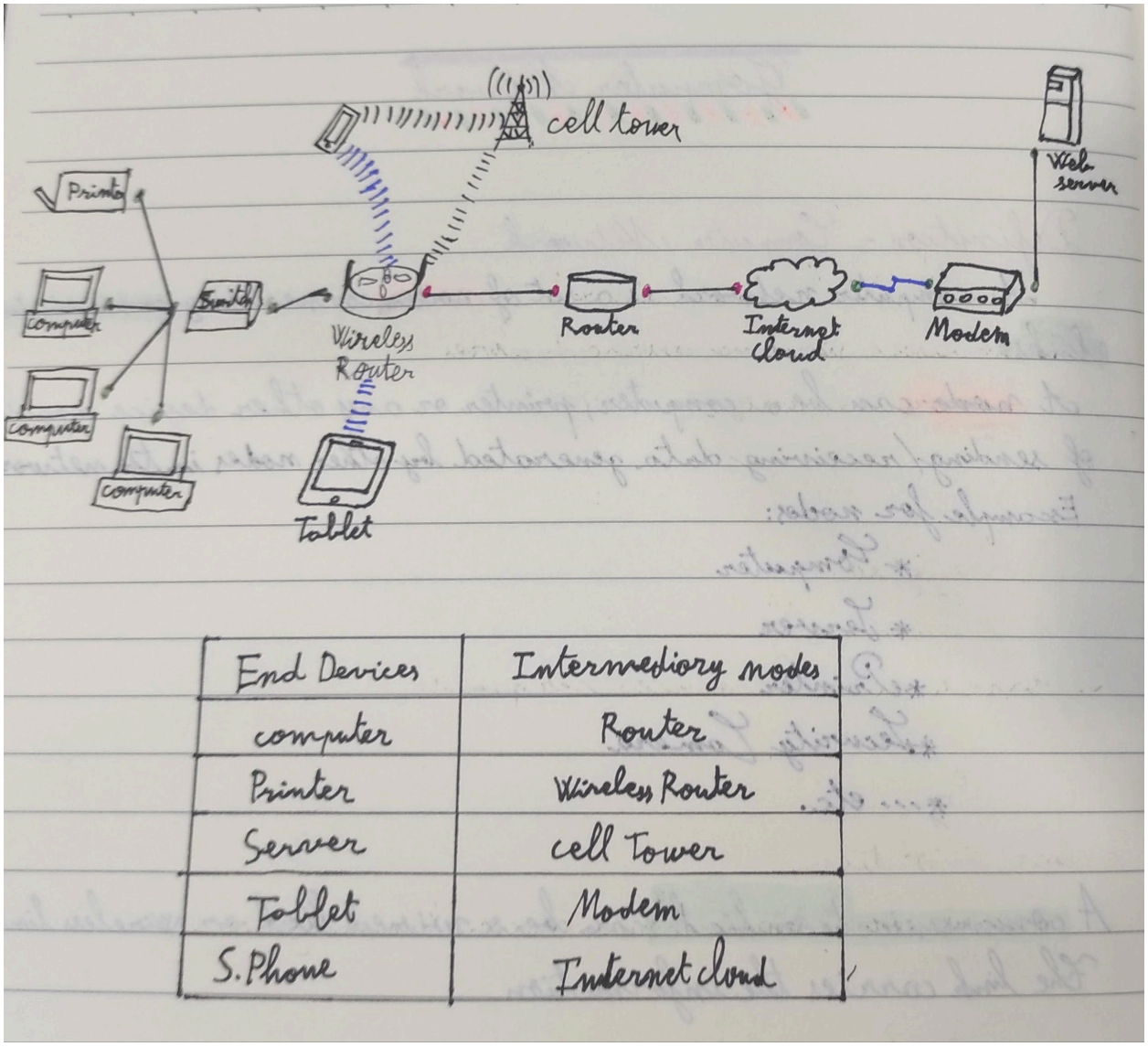
A computer network is a set of nodes connected via a communication link. A node can be a computer, printer or any other device capable of sending/receiving data generated by other nodes in the network.

Example of nodes:

- Computer
- Server
- Printer
- Security camera
- …etc

A communication layer can be wired or wireless link. The link carries the information.

This is an example of a computer network:



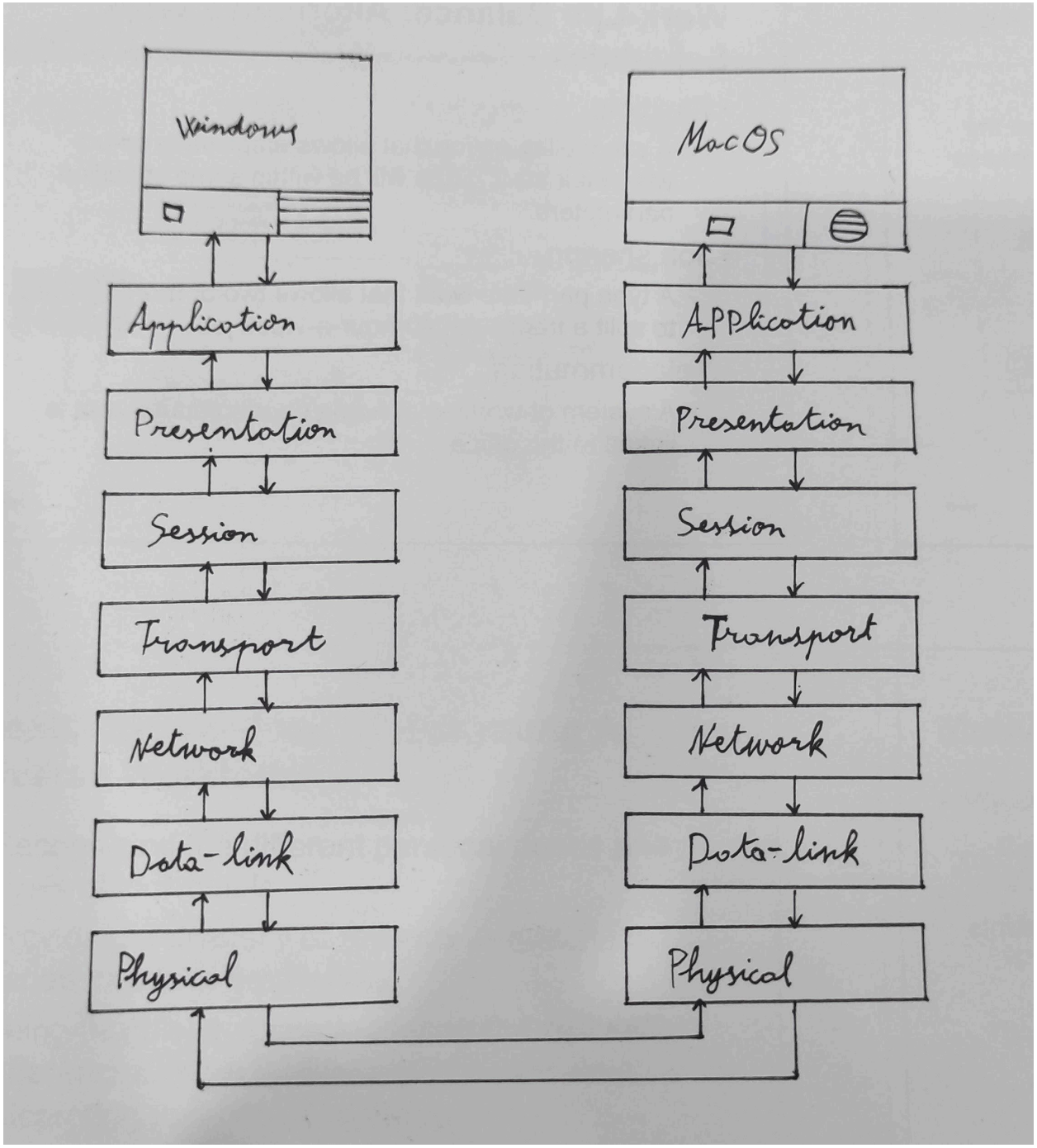
End Devices	Intermediary nodes
computer	Router
Printer	Wireless Router
Server	cell Tower
Tablet	Modem
S.Phone	Internet cloud

OSI MODEL:

In the 70s to 80s, ISO (international organization for standardization) decided to make a NETWORKING STANDARDS, so that two computers with different operating systems can communicate with each other without any problem, and a standard system all the companies follow. Therefore, ISO collaborated with IEEE (**Institute of Electrical and Electronics Engineers**) to make the reference model that will be followed by all the companies.

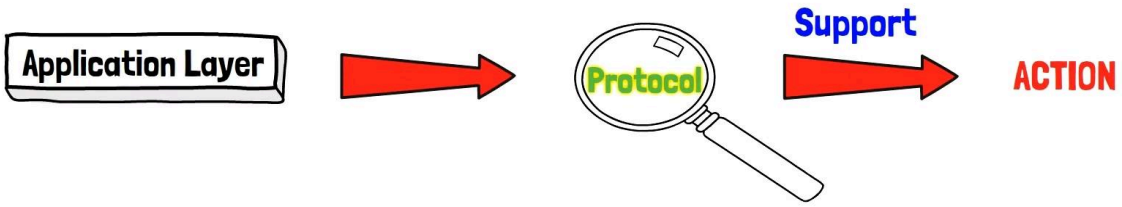
IEEE split the connection into seven layers, so that if a device is sending anything to another device, it should pass through those 7 layers, and it will

be received through them but in reverse order, and they called this model **OSI MODEL** (open systems interconnection model).



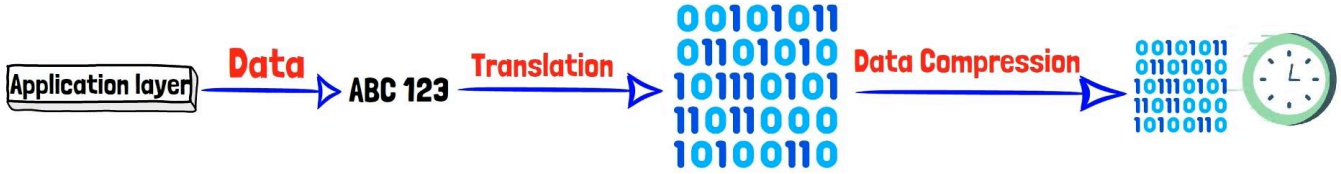
Application layer:

Application layer indicates which protocol supports the action you requested, and afford it. For example, if you search for baidu (“www.baidu.com”) you find that it adds https protocol (Hypertext Transfer Protocol Secure) this is the protocol for browsing (“https://www.baidu.com”), if you start download a file, it starts a FTP protocol (File Transfer Protocol), if you want to send an email, SMTP protocol starts (Simple Mail Transfer Protocol). And there are many other protocols that work in the application layer.



Presentation layer:

This layer took the data coming from application layer which is human-readable, and transfer it to machine code, this operation called translation, then it compresses the number of bite to smaller one so the size decrease and transferring become easier and timeless, this operation called Date Compression, and that is why when we send a picture in facebook or whatsapp, always it size become less.



Also, Presentation layer is responsible of encryption/decryption, and it happened under the SSL protocol.

Presentation layer does three operations:

- Translation
- Data Compression
- Encryption

Session layer:

Session layer is responsible for four operations:

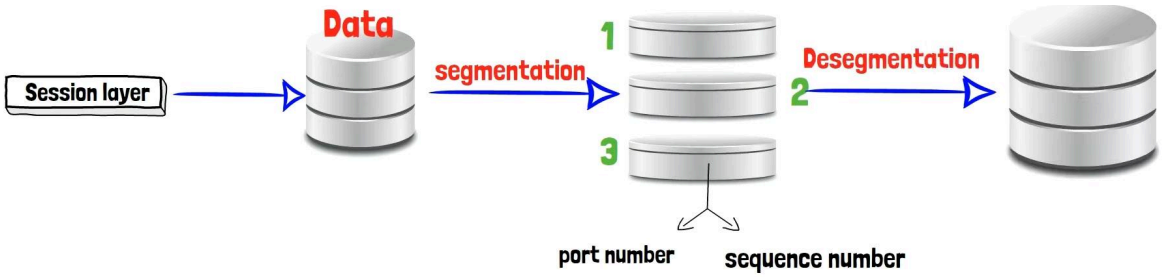
1. Transmission mode
    - Simplex mode
    - Half-duplex mode
    - Full-duplex mode
2. Authentication
   For example, when you want to login in a server, the server always asks for authentication which is username and password.
3. Authorization
   After you login in the server, server decides if you have the authorization to access certain files or not.
4. Session management
   For example, if you are offline and you open facebook, you will find some posts, videos and pictures that were in the last session you opened, that happened because it took data from your last session and temporary stored, and when you open facebook again, it starts to restored, so you can see it even if you are offline.

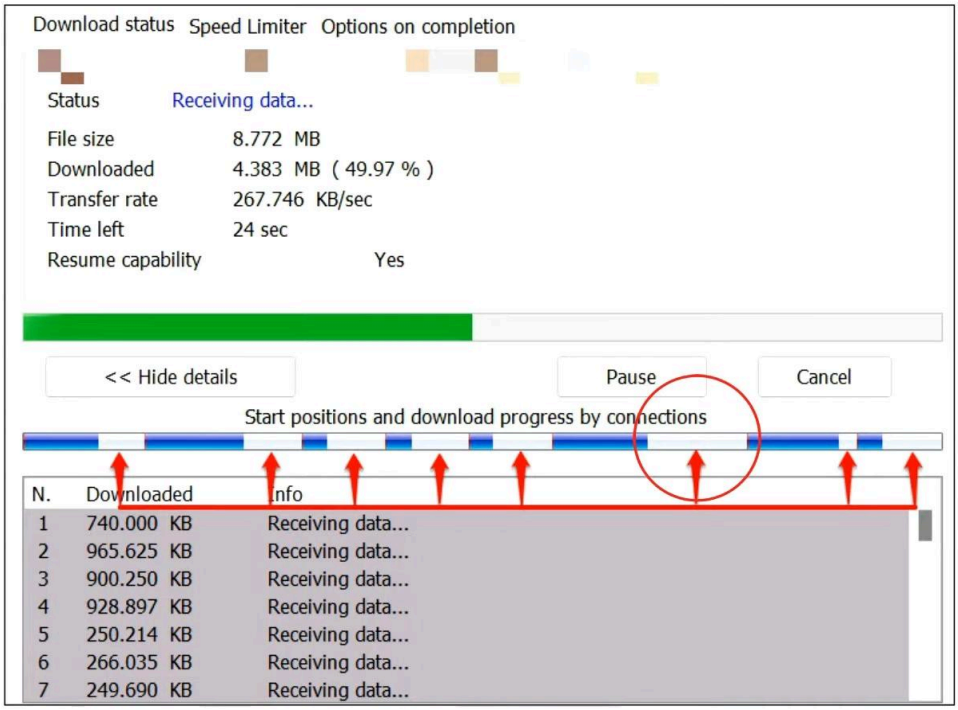
Here we discovered the first three layers and they are called software layers. And now let's discover the most important layer in the osi model which is the transport layer.

Transport layer:

1. segmentation/desegmentation:
   This layer does a very important operation called segmentation. That is, it took data coming from the software layer and starts to split it into segments (to make transferring easier), and we can see that when a problem happens while downloading a file, we see that is not need to start downloading overhead, it just starts redownloading the segment where the collision happened.

Every segment has a port number and sequence number to make the distribution flexible.





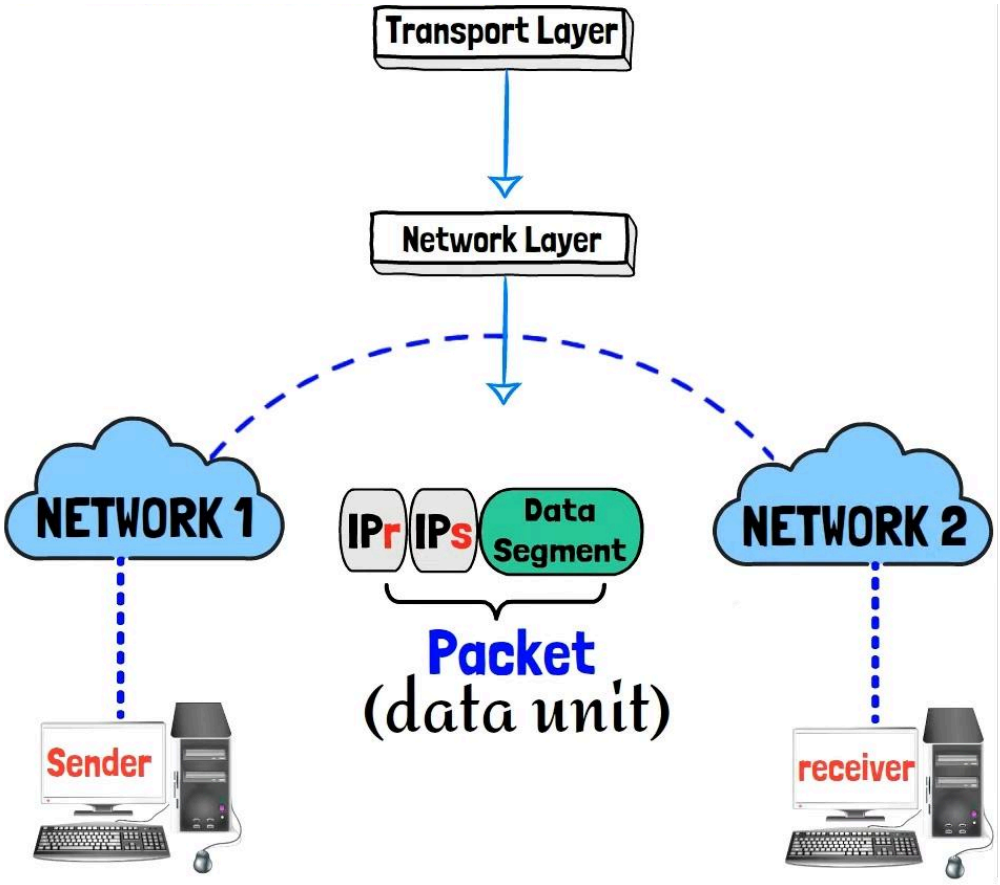
2. Flow control:
   Flow control means that the transport layer controls the quantity of data transferred. For example, if a computer is transferring data to a mobile phone, the computer transferring speed is 100Mbps and the mobile phone one is 10Mbps, so normally a collision will happen. Therefore the transport layer controls the flow of data by increasing or decreasing the transferring speed rate.

3. Determine Protobol:
   The last thing Transport layer does is determining the type of protocol depending on action that user do, and there is two types of protocols:

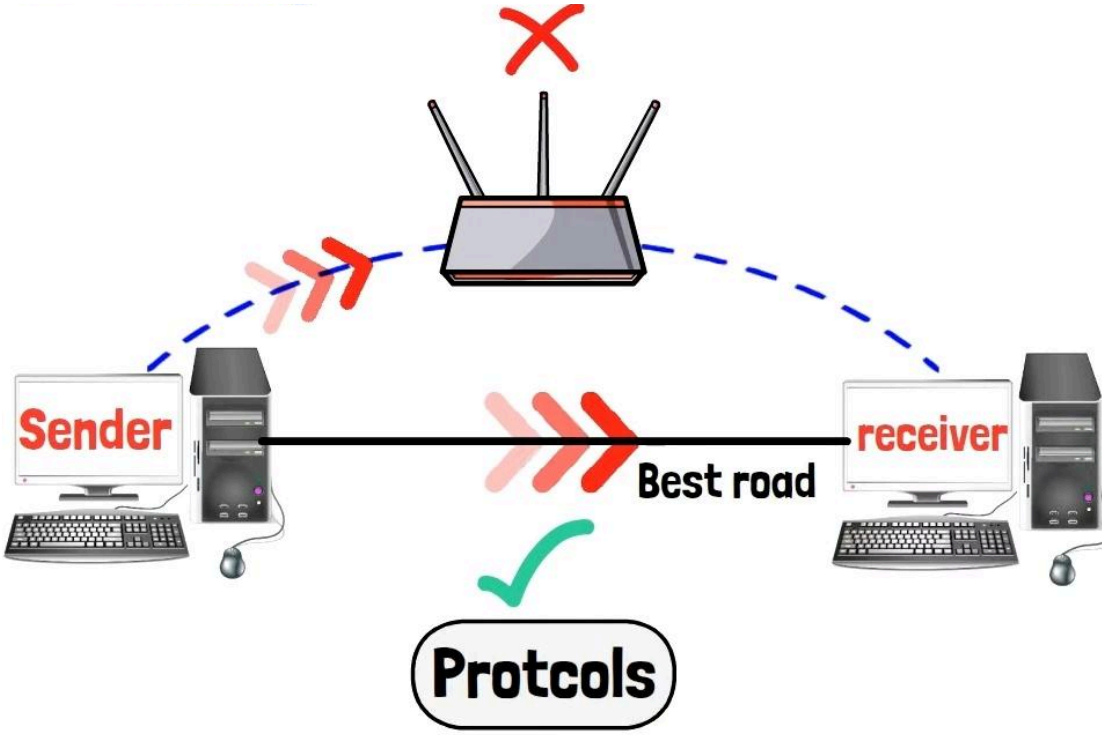
- TCP (Transmission Control Protocol) is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network. Major internet applications such as the World Wide Web, email, remote administration, and file transfer rely on TCP, which is part of the Transport Layer of the TCP/IP suite. SSL/TLS often runs on top of TCP.
- UDP (User Datagram Protocol) is one of the core communication protocols of the Internet protocol suite used to send messages (transported as datagrams in packets) to other hosts on an Internet Protocol (IP) network. Within an IP network, UDP does not require prior communication to set up communication channels or data paths.

Network layer:

1. Logical addressing:
   Every device in the network you can communicate with via a unique IP address (Internet Protocol),-- like if you want to send a mail you should know the address of the receiver–.
   The Network layer receives the data segment from the Transport layer and add to it the IP address of the receiver and the sender, this new data called Packet which is the data unit of the Network layer.

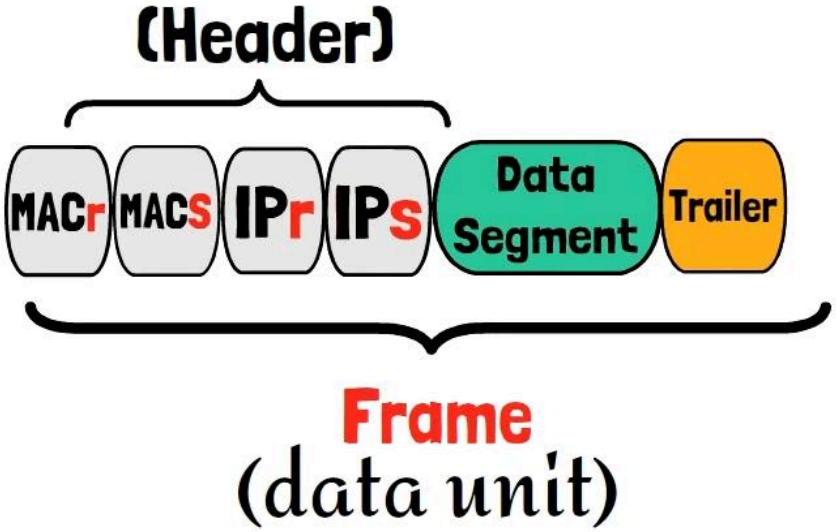


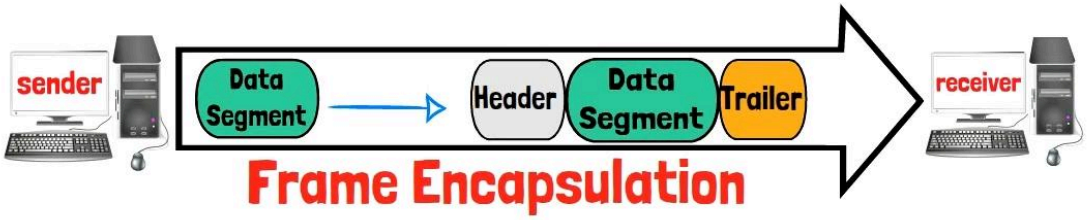
2. Routing:
   Routing in general is choosing the best path to transfer data between source and destination, and this happen via protocols like RIP(Routing Information Protocol) and OSPF(Open Shortest Path First).



Data-link layer:

1. Physical Addressing:
   The data-link layer like the previous layer, receives the data which data packet and adds the physical address which MAC address(Media Access Control), adds mac address of the source and the receiver, and that makes a new data unit called frame.





2. Error detection and correction:
   The data link layer handles such tasks as gathering up sets of bits for transmission as packets and making sure the packets get from one end to the other. In addition, recognizing that physical layer transmission sometimes introduces errors, the data link layer handles error detection (and sometimes correction).
   Data-link layer detects the error using several algorithms such as:
   - Checksum
   - Parity checking
   - CRC (Cyclic Redundancy Check)

   So Data-link layer to control the error uses several protocol:
   - Stop-and-Wait ARQ
   - Sliding window Protocol
     - Go-Back-N ARQ
     - Selective Repeat ARQ

   And here we are going to explain Selective Repeat ARQ

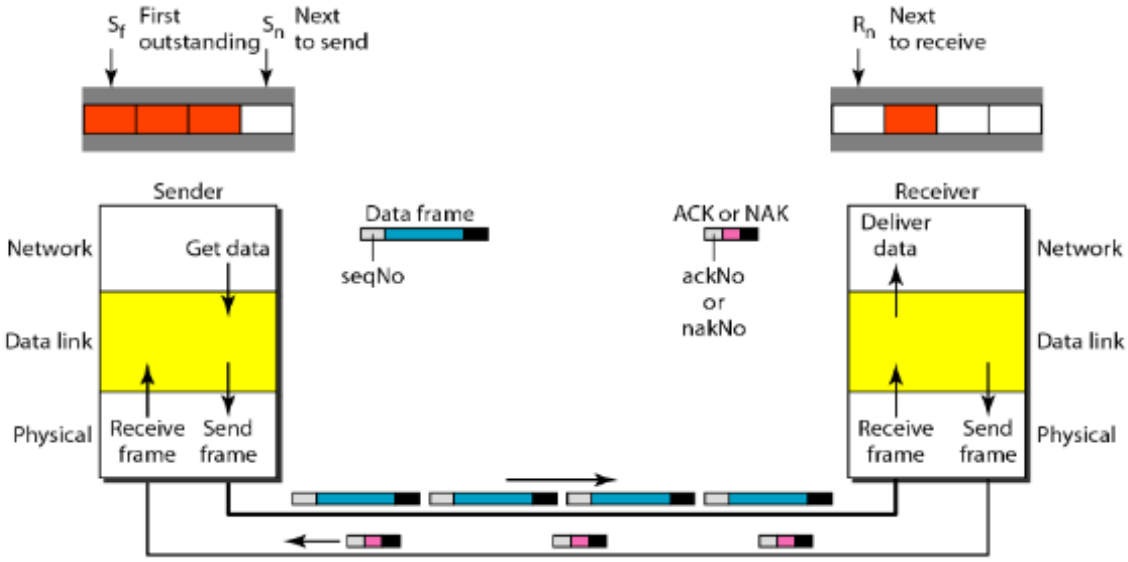
Selective Repeat ARQ:

It is also known as Sliding Window Protocol and used for error detection and control in the data link layer.

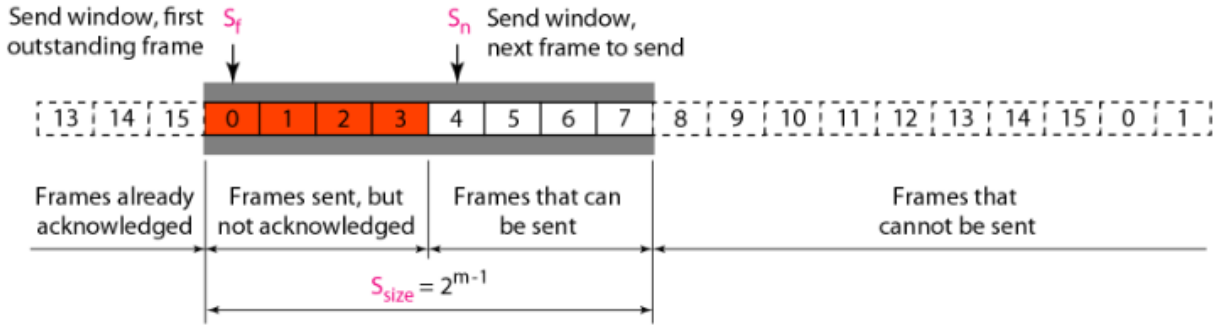
In the selective repeat, the sender sends several frames specified by a window size even without the need to wait for individual acknowledgement from the receiver as in Go-Back-N ARQ. In selective repeat protocol, the retransmitted frame is received out of sequence.

In Selective Repeat ARQ only the lost or error frames are retransmitted, whereas correct frames are received and buffered.

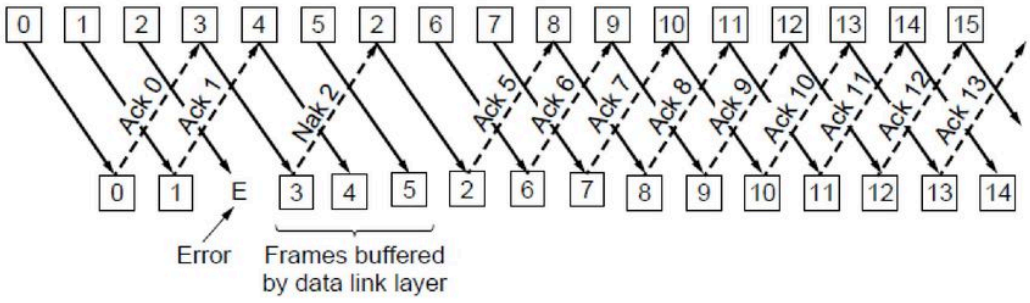
The receiver while keeping track of sequence numbers buffers the frames in memory and sends NACK for only frames which are missing or damaged. The sender will send/retransmit a packet for which NACK is received.



In the Selective repeat ARQ there are three types of frames, frames already sent and acknowledged, frames sent but not acknowledged and frames not sent and not acknowledged.



Example:



Given upward is an example of the Selective Repeat ARQ −

Explanation:

Step 1 − Frame 0 sends from sender to receiver and set timer.

Step 2 − Without waiting for acknowledgement from the receiver another frame, Frame1 is sent by sender by setting the timer for it.

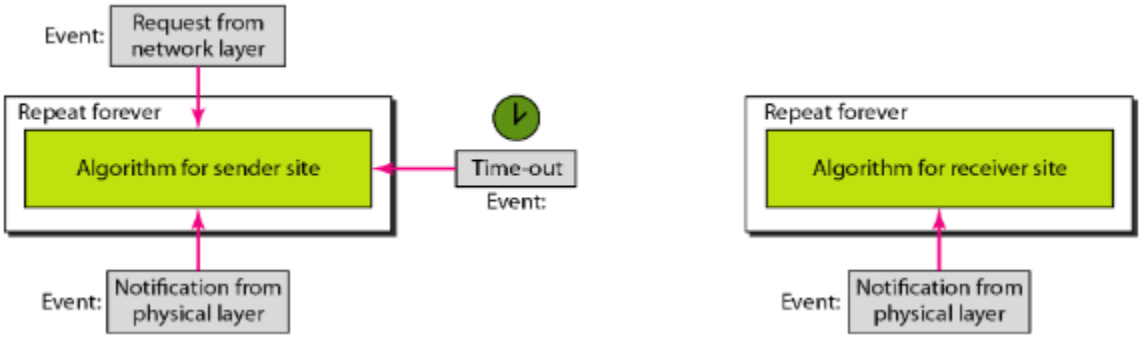
Step 3 − In the same way frame2 is also sent to the receiver by setting the timer without waiting for previous acknowledgement.

Step 4 − Whenever sender receives the ACK0 from receiver, within the frame 0 timer then it is closed and sent to the next frame, frame 3.

Step 5 − Whenever the sender receives the ACK1 from the receiver, within the frame 1 timer then it is closed and sent to the next frame, frame 4.

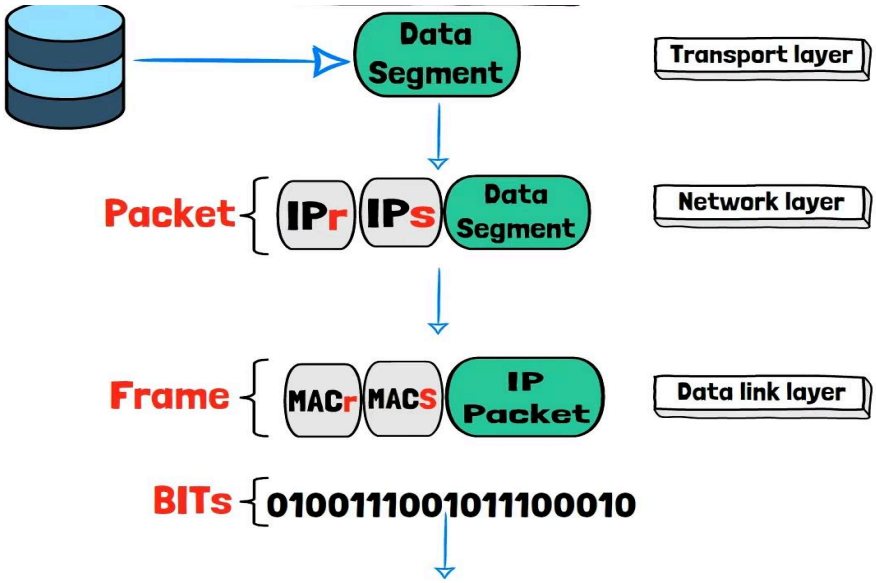
Step 6 − If the sender doesn’t receive the ACK2 from the receiver within the time slot or receives an NACK2, it declares timeout for frame 2 and resends the frame 2 again, because it thought the frame2 may be lost or damaged. The receiver buffers the frames after frame 2 till it receives the frame then the receiver add the frames buffered to the database, and empty the buffer.

Conclusion, Selective Repeat ARQ is more complex than Go-Back-N due to buffering at receiver but it is more efficient use of link bandwidth as only lost frames are resent.

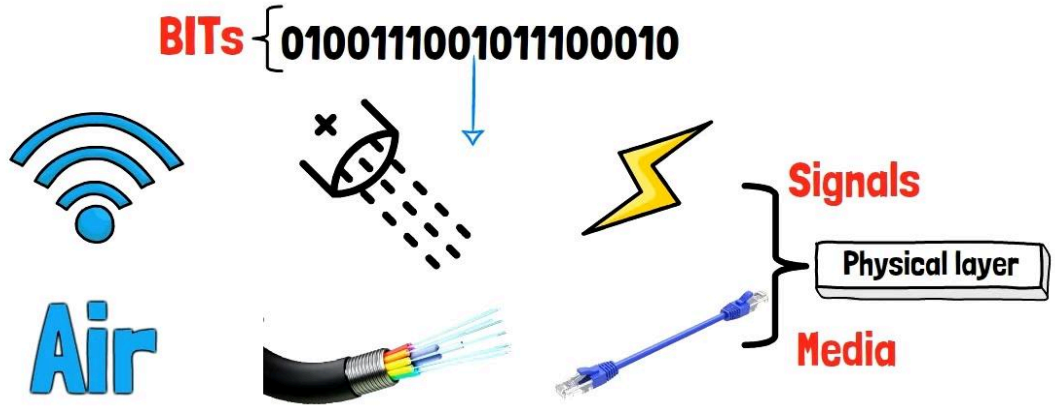


Physical layer:

As we discovered previously, data pass into the transport layer and get segmented forming a data segment, then this data segment passes into the network layer and forms a Packet, finally the Packet passes into the data link layer and forms a frame. This frame is basically made in bits (0's and 1's).



The role of the Physical layer is to transform those bits into signals so they can be accepted by the media. Those signals could be electric signals in the case of ethernet cable, optical signals in case of fiber optic or radio signals in case that media is wireless.



Conclusion:

The OSI model remains a valuable framework for understanding network communication principles. It provides a foundation for network technologies and protocols, facilitating communication across diverse systems. While its limitations should be acknowledged, its strengths continue to make it a relevant and influential model in the field of networking. Additionally, the OSI model continues to evolve as new technologies and protocols emerge. Its layered structure offers adaptability and can be extended or modified to accommodate advancements in network communication.