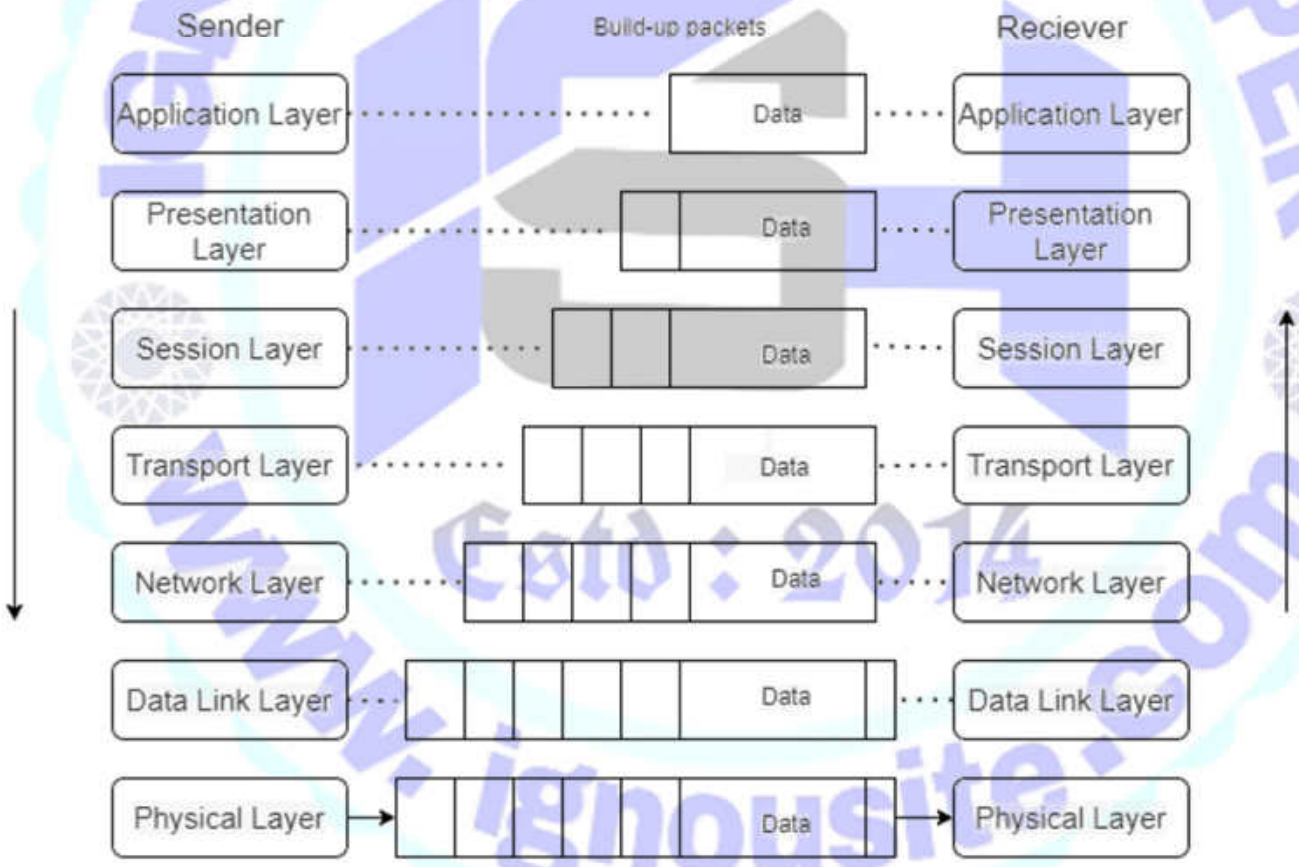
**Course Code : MCS-218**
**Course Title : Data Communication and Computer Networks**
**Assignment Number : MCA_NEW(II)/218/Assign/2023-24**
**Maximum Marks : 100**
**Weightage : 30%** www.ignousite.com
**Last Dates for Submission : 31st October, 2023 (For July, 2023 Session)**
**: 15th April, 2024 (For January, 2024 Session)**



**Q1: What is OSI model? What is TCP/IP model? Compare them.**

**Ans. OSI Model:** The OSI (Open Systems Interconnection) model and the TCP/IP (Transmission Control Protocol/Internet Protocol) model are two conceptual frameworks used to understand and describe how network protocols and communication occur in computer networks. Both models provide a layered approach to network communication, but they have some differences in their design and functionality.




**OSI Model**

**Layers of OSI Model**

1. Physical Layer
2. Data Link Layer
3. Network Layer

4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

**Layer 1- Physical Layer:**

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

The Functions of the Physical Layer

- Bit synchronization: The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.
- Bit rate control: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
- Physical topologies: Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
- Transmission mode: Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

**Layer 2- Data Link Layer (DLL):**

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address.

The Functions of the Data Link Layer

- Framing: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
- Physical addressing: After creating frames, the Data link layer adds physical addresses (MAC addresses) of the sender and/or receiver in the header of each frame.
- Error control: The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
- Flow Control: The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.
- Access control: When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

**Layer 3- Network Layer:**

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP addresses are placed in the header by the network layer.

The Functions of the Network Layer

- Routing: The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
- Logical Addressing: To identify each device on Internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

**Layer 4- Transport Layer:**

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as Segments. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

The Functions of the Transport Layer

- Segmentation and Reassembly: This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
- Service Point Addressing: To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

**Layer 5- Session Layer:**

This layer is responsible for the establishment of connection, maintenance of sessions, and authentication, and also ensures security.

The Functions of the Session Layer

- Session establishment, maintenance, and termination: The layer allows the two processes to establish, use and terminate a connection.
- Synchronization: This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
- Dialog Controller: The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

**Layer 6- Presentation Layer:**

The presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

The Functions of the Presentation Layer are

- Translation: For example, ASCII to EBCDIC.
- Encryption/ Decryption: Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
- Compression: Reduces the number of bits that need to be transmitted on the network.

**Layer 7- Application Layer:**

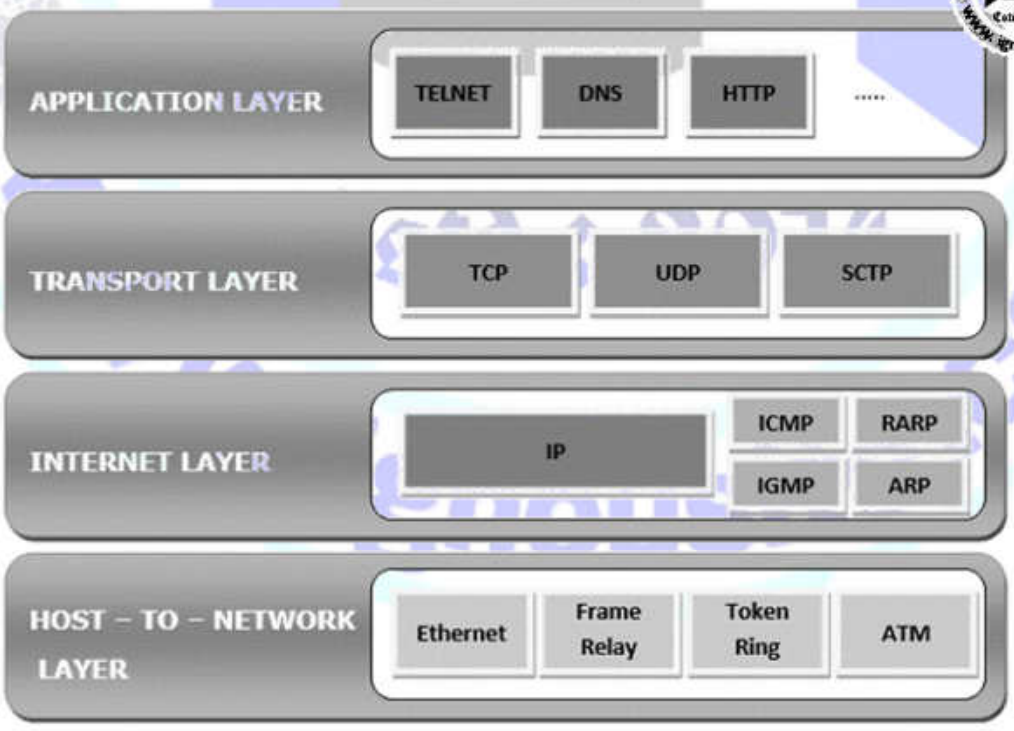
At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

The Functions of the Application Layer are

- Network Virtual Terminal: It allows a user to log on to a remote host.
- FTAM- File transfer access and management : This application allows a user to access file in a remote host, retrieve files in remote host and manage or control files from a remote computer.
- Mail Services : Provide email service.
- Directory Services : This application provides distributed database sources and access for global information about various objects and services.

**TCP/IP Model (Transmission Control Protocol/Internet Protocol Model):** The TCP/IP model is a practical implementation of the networking protocols used in the Internet. It was developed by the U.S. Department of Defense in the 1970s and became the foundation of the modern internet. The TCP/IP model consists of four layers, which are sometimes grouped together:

1. Application Layer
2. Transport Layer
3. Internet Layer
4. Network Interface/Host-to- Network Layer



**1.Application Layer**: This is the topmost layer and defines the interface of host programs with the transport layer services. This layer includes all high-level protocols like Telnet, DNS, HTTP, FTP, SMTP, etc.

**2.Transport Layer**: It is responsible for error-free end-to-end delivery of data. The protocols defined here are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

**3.Internet Layer**: It defines the protocols for logical transmission of data over the network. The main protocol in this layer is Internet Protocol (IP) and it is supported by the protocols ICMP, IGMP, RARP, and ARP.

**4.Host-to- Network Layer (Network Interface)**: It is the lowest layer that is concerned with the physical transmission of data. TCP/IP does not specifically define any protocol here but supports all the standard protocols.

**Compare TCP/IP and OSI model:**

| TCP/IP | OSI |
|---|---|
| TCP refers to Transmission Control Protocol. | OSI refers to Open Systems Interconnection. |
| TCP/IP uses both the session and presentation layer in the application layer itself. | OSI uses different session and presentation layers. |
| TCP/IP follows connectionless a horizontal approach. | OSI follows a vertical approach. |
| The Transport layer in TCP/IP does not provide assurance delivery of packets. | In the OSI model, the transport layer provides assurance delivery of packets. |
| Protocols cannot be replaced easily in TCP/IP model. | While in the OSI model, Protocols are better covered and are easy to replace with the technology change. |
| TCP/IP model network layer only provides connectionless (IP) services. The transport layer (TCP) provides connections. | Connectionless and connection-oriented services are provided by the network layer in the OSI model. |

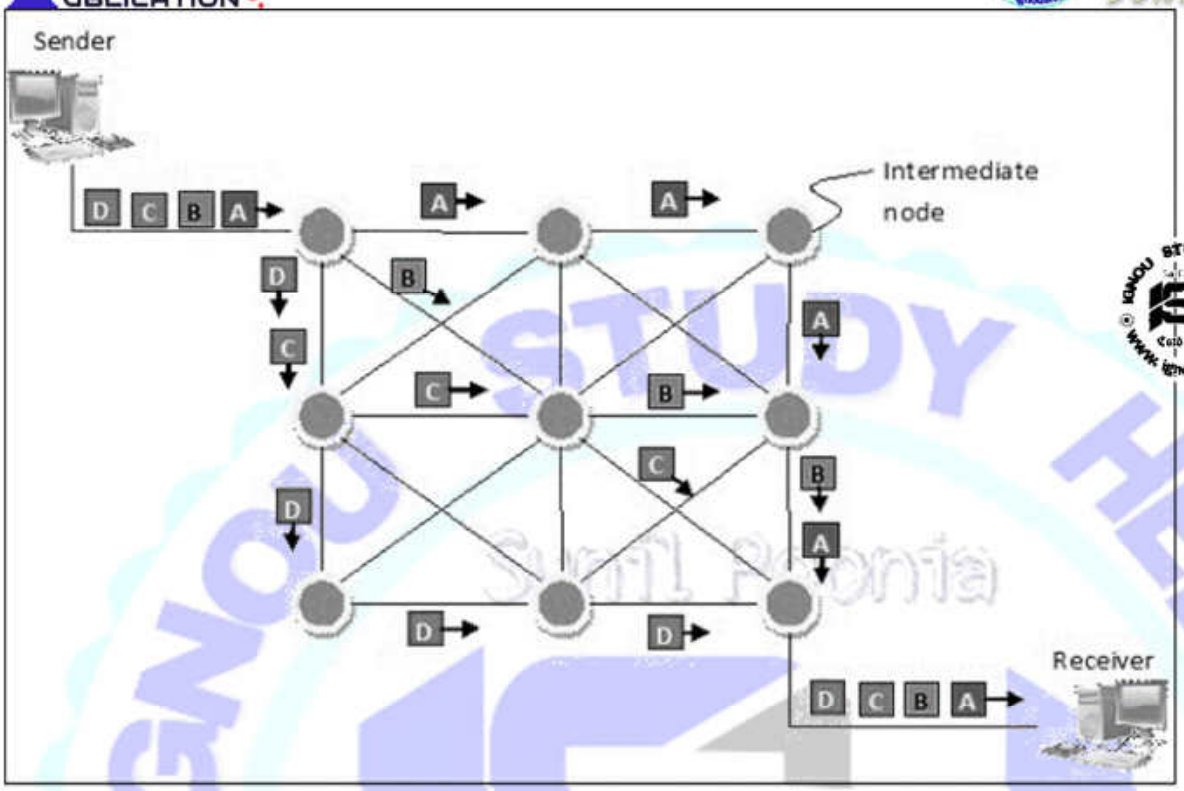
**Q2: What is Packet Switching? What is Circuit Switching? Compare them.**

**Ans. Packet switching:** Packet switching is a connectionless network switching technique. Here, the message is divided and grouped into a number of units called packets that are individually routed from the source to the destination. There is no need to establish a dedicated circuit for communication.

**Process**: Each packet in a packet switching technique has two parts: a header and a payload. The header contains the addressing information of the packet and is used by the intermediate routers to direct it towards its destination. The payload carries the actual data.

A packet is transmitted as soon as it is available in a node, based upon its header information. The packets of a message are not routed via the same path. So, the packets in the message arrives in the destination out of order. It is the responsibility of the destination to reorder the packets in order to retrieve the original message.

The process is diagrammatically represented in the following figure. Here the message comprises of four packets, A, B, C and D, which may follow different routes from the sender to the receiver.




**Key features of packet switching:**

- Packetization: Data is divided into packets before transmission.
- Store-and-Forward: Each packet is stored at intermediate network nodes before being forwarded to the next hop.
- Dynamic Routing: Each packet can take a different route to reach its destination, based on network conditions and availability.
- Shared Resources: The network resources (links and nodes) are shared among multiple users, enabling better resource utilization.
- Bursty Traffic: Suitable for bursty data transmission, where data is sent intermittently.

**Advantages and Disadvantages of Packet Switching**

**Advantages**

- Delay in delivery of packets is less, since packets are sent as soon as they are available.
- Switching devices don't require massive storage, since they don't have to store the entire messages before forwarding them to the next node.
- Data delivery can continue even if some parts of the network faces link failure. Packets can be routed via other paths.
- It allows simultaneous usage of the same channel by multiple users.
- It ensures better bandwidth usage as a number of packets from multiple sources can be transferred via the same link.

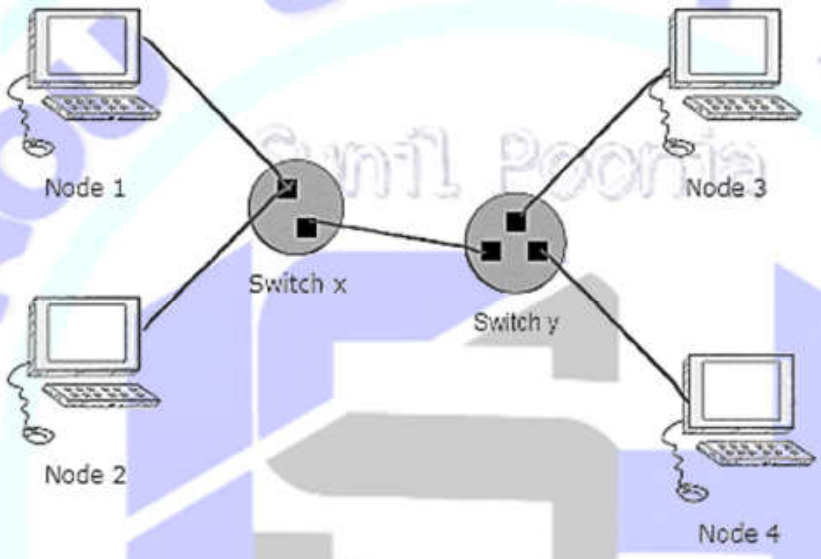
**Disadvantages**

- They are unsuitable for applications that cannot afford delays in communication like high quality voice calls.
- Packet switching high installation costs.
- They require complex protocols for delivery.

- Network problems may introduce errors in packets, delay in delivery of packets or loss of packets. If not properly handled, this may lead to loss of critical information.

**Circuit Switching**: Circuit Switching is a connection-oriented service that uses a dedicated path from the sender to the receiver. Before sending any data from the source to the destination, it needs to set up an end-to-end path.

Circuit switching has the minimum chance of data loss due to the dedicated circuit path, but a lot of bandwidth is wasted as a path cannot be used by other senders during a congestion.




**Circuit Switching**

**Three Phases of Circuit Switching**

Following are the three phases of circuit switching –

- **Circuit Establishment** – A dedicated circuit is established between the two end-devices or from the source to the destination using the number of intermediate switching center offices. The sender from the source side and the receiver from the destination side transmit communication signals to request and ACK of circuit's establishment. The intermediate switches are connected by the physical links.
- **Data Transfer** – After a dedicated connection is established from the source to the destination. Data and voice are traveled from the source to the destination. This connection remains till the communication is the end.
- **Disconnect the circuit** – when the data transfer is completed, the circuit disconnects the connection.

**Advantages and Disadvantages of Circuit Switching**

Following are the advantages of using circuit switching –

- Circuit switching uses a dedicated path exists for the data to travel from source to destination.
- It has no header overhead.
- It has no waiting time at any switch and the data is transmitted without any delay.
- Data always reaches the other end in order.
- Reordering is not required.

Following are the disadvantages of using circuit switching –

- The channel is blocked after the communication is ended.
- Circuit switching is inefficient in terms of the utilization of system resources.
- It needs a long time to establish the connection from the source to the destination. More
- Bandwidth is required for the dedicated channels.
- It is more expensive than other switching techniques.
- Routing decisions cannot be changed once the circuit is established.

**Q3: Explain STOP & WAIT ARQ.**

**Ans. STOP & WAIT ARQ:** STOP & WAIT Automatic Repeat Request (ARQ) is a flow control protocol used in data communication to ensure reliable transmission of data between a sender and a receiver over an unreliable channel. It is a simple and straightforward mechanism where the sender sends a single packet (frame) to the receiver and waits for an acknowledgment (ACK) from the receiver before sending the next packet. If the sender does not receive an ACK within a certain time, it assumes that the packet was lost or corrupted and retransmits it.

Here's how the STOP & WAIT ARQ protocol works:

**1.Data Transmission:**

- The sender divides the data into fixed-size packets (frames) and sends the first frame to the receiver.
- After sending a frame, the sender starts a timer to wait for the ACK from the receiver.

**2.Receiver's Processing:**

- The receiver receives the frame and checks for errors or corruption.
- If the frame is error-free, the receiver sends an ACK to the sender indicating successful receipt of the frame.
- If the frame is corrupted, the receiver discards the frame and does not send an ACK.

**3.ACK Reception at Sender:**

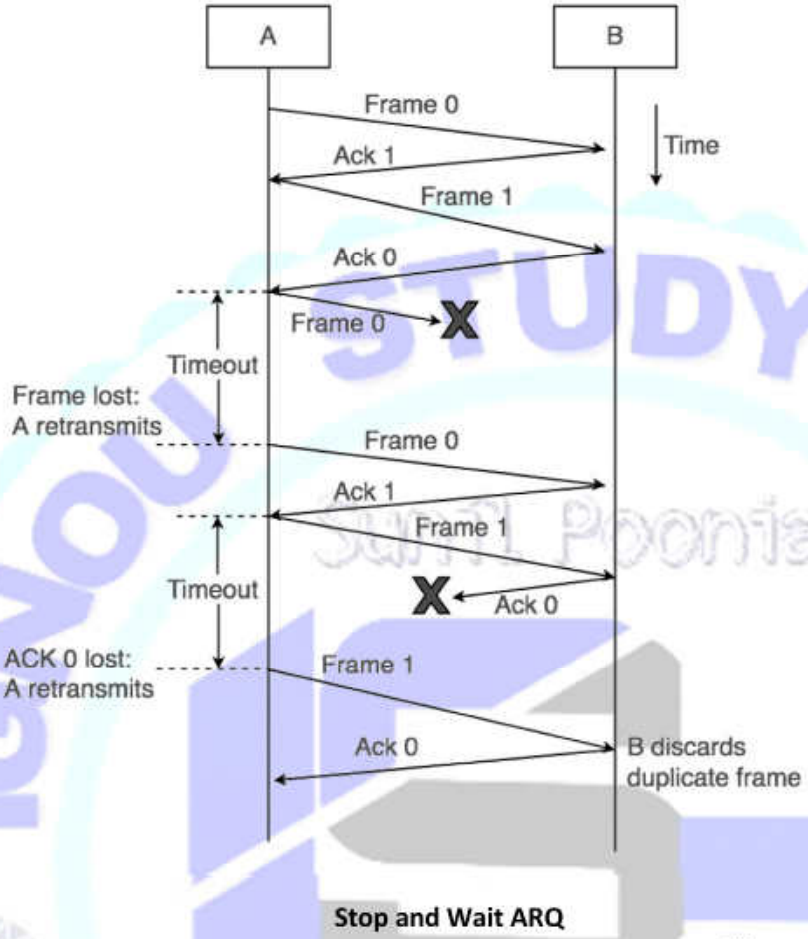
- The sender waits for the ACK to arrive within a specific time window (timeout period).
- If the ACK is received before the timeout expires, the sender knows that the frame was successfully received, and it proceeds to send the next frame.
- If the ACK is not received within the timeout period, the sender assumes that the frame was lost or corrupted during transmission.

**4.Retransmission:**

- If the sender does not receive an ACK within the timeout period, it assumes that the frame was lost or corrupted and retransmits the same frame.
- The receiver detects the duplicate frame and discards it since it has already processed the original frame and sent an ACK.

**5.Repeat Process:**

- The process continues with the sender sending the next frame after receiving the ACK for the previous frame, or retransmitting the same frame in case of a timeout.




**Stop and Wait ARQ**

**Characteristics of Stop and Wait ARQ:**

- 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 acknowledgements 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 2 sequence numbers 0 and 1

**Constraints:**

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.