Course Code : BCS-041

Course Title : Fundamentals of Computer Networks

Assignment Number : BCA (IV)/041/Assignment/2024-25

Maximum Marks : 100

Weightage : 25% www.ignousite.com

Last Date of Submission : 31st October, 2024 (for July 2024 session)

: 30th April, 2025 (for January 2025 session)

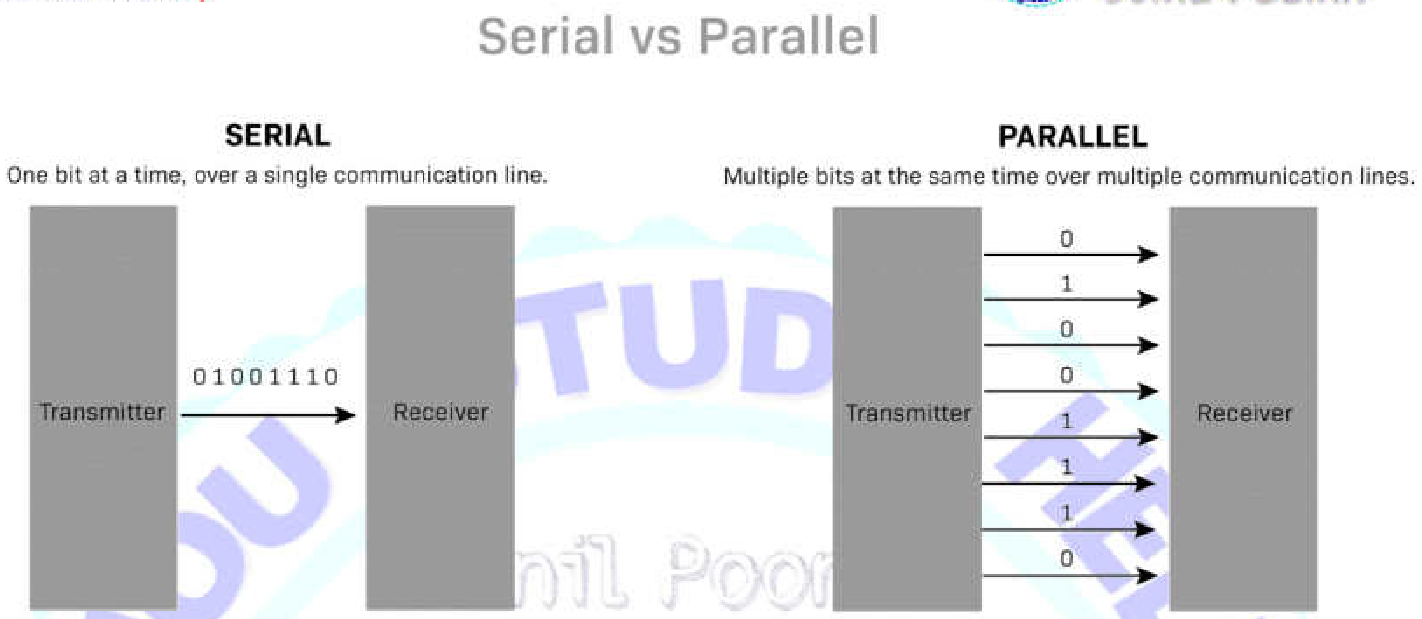
Q1.

(a) Differentiate between parallel and serial communication. Give an example of each.

Ans.

Difference between serial and parallel communication:

Serial Communication	Parallel Communication
In this type, a single communication link is used to transfer data from one end to another	In this type, multiple parallels links used to transmit the data
In serial transmission, data(bit) flows in bi-direction.	In Parallel Transmission, data flows in multiple lines.
Serial Transmission is cost-efficient.	Parallel Transmission is not cost-efficient.
In serial transmission, one bit transferred at one clock pulse.	In Parallel Transmission, eight bits transferred at one clock pulse.
Serial Transmission is slow in comparison of Parallel Transmission.	Parallel Transmission is fast in comparison of Serial Transmission.
Generally, Serial Transmission is used for long-distance.	Generally, Parallel Transmission is used for short distance.
The circuit used in Serial Transmission is simple.	The circuit used in Parallel Transmission is relatively complex.
Serial Transmission is full duplex as sender can send as well as receive the data	Parallel Transmission is half-duplex since the data is either send or receive
Converters are required in a serial transmission to convert the data between internal and parallel form	No converters are required in Parallel Transmission
Serial transmission is reliable and straightforward.	Parallel transmission is unreliable and complicated.


Serial vs Parallel
SERIAL
One bit at a time, over a single communication line.
Transmitter
01001110
Receiver
PARALLEL
Multiple bits at the same time over multiple communication lines.
Transmitter
0
1
0
0
1
1
1
0
Receiver

Example:

Serial communication: Serial communication is a method of sending data one bit at a time, in a sequential order, over a single channel. For example, if you want to send the byte 01011010, you would send each bit one after another, starting from the leftmost or rightmost bit, depending on the protocol. Serial communication is often used for long-distance or wireless communication, as it requires less wires and reduces interference. However, it also has some drawbacks, such as lower speed, higher latency, and more complex synchronization.

Parallel communication: Parallel communication is a method of sending data multiple bits at a time, in parallel, over multiple channels. For example, if you want to send the byte 01011010, you would send each bit simultaneously over eight wires, one for each bit. Parallel communication is often used for short-distance or high-speed communication, as it allows faster data transfer and lower latency. However, it also has some challenges, such as more wires and connectors, higher cost, and more susceptibility to noise and crosstalk.

(b) Compare POP and IMAP.

Ans. Difference between POP and IMAP:

Post Office Protocol (POP3)	Internet Message Access Protocol (IMAP)
POP is a simple protocol that only allows downloading messages from your Inbox to your local computer.	IMAP (Internet Message Access Protocol) is much more advanced and allows the user to see all the folders on the mail server.
The POP server listens on port 110, and the POP with SSL secure(POP3DS) server listens on port 995	The IMAP server listens on port 143, and the IMAP with SSL secure(IMAPDS) server listens on port 993.
In POP3 the mail can only be accessed from a single device at a time.	Messages can be accessed across multiple devices
To read the mail it has to be downloaded on the local system.	The mail content can be read partially before downloading.

The user can not organize mail in the mailbox of the mail server.	On the mail server, the user can directly arrange the email.
The user can not create, delete,e or rename email on the mail server.	The user can create, delete,e or rename an email on the mail server.
It is unidirectional i.e. all the changes made on a device do not affect the content present on the server.	It is Bi-directional i.e. all the changes made on the server or device are made on the other side too.
It does not allow a user to sync emails.	It allows a user to sync their emails.
It is fast.	It is slower as compared to POP3.
A user can not search the content of mail before downloading it to the local system.	A user can search the content of mail for a specific string before downloading.
It has two modes: delete mode and keep mode. • In delete mode, the mail is deleted from the mailbox after retrieval. • In keep mode, the mail remains in the mailbox after retrieval.	Multiple redundant copies of the message are kept at the mail server, in case of loss of message on a local server, the mail can still be retrieved
Changes in the mail can be done using local email software.	Changes made to the web interface or email software stay in sync with the server.
All the messages are downloaded at once.	The Message header can be viewed before downloading.

Q2.

(a) What is Ad hoc Wireless Communication System? Explain.

Ans. Ad hoc wireless communication system: An ad hoc wireless communication system refers to a decentralized and self-configuring network of wireless devices that can communicate with each other without the need for a pre-existing infrastructure or centralized control. In other words, ad hoc wireless communication systems enable devices to establish direct communication links with nearby devices to form a temporary network on the fly. This type of network is often referred to as an "ad hoc network."

Key Characteristics of Ad Hoc Wireless Communication Systems:

1. **Decentralization:** Ad hoc networks do not rely on a central server or base station for communication. Instead, each device can act as both a transmitter and a receiver, contributing to the network's operation.
2. **Dynamic Formation**: Devices in an ad hoc network can dynamically join or leave the network as needed. This allows for flexibility and adaptability in changing environments.
3. **Self-Organization**: Ad hoc networks use self-organization and distributed algorithms to determine network topology, routing paths, and communication channels without external configuration.
4. **Peer-to-Peer Communication**: Devices communicate directly with each other, establishing peer-to-peer connections rather than relying on intermediaries.

5. **Infrastructureless**: Unlike traditional wireless networks, ad hoc networks do not require any pre-existing infrastructure, such as access points or base stations. They can be set up anywhere, making them suitable for scenarios where infrastructure is lacking or impractical.
6. **Short to Medium Range**: Ad hoc networks typically operate over relatively short to medium communication ranges, depending on the technology used and environmental conditions.

Applications of Ad Hoc Wireless Communication Systems:

1. **Emergency Response**: Ad hoc networks are valuable in emergency situations where communication infrastructure may be damaged or nonexistent. First responders' devices can create an ad hoc network to share critical information quickly.
2. **Military Operations**: Military personnel can use ad hoc networks to establish communication links in remote or hostile environments, allowing for secure and flexible communication.
3. **Collaborative Computing**: Ad hoc networks are used for collaborative computing scenarios, such as sharing files or presentations during meetings or conferences.
4. **Vehicular Networks**: Vehicles equipped with wireless communication capabilities can form ad hoc networks to share information about traffic conditions, accidents, or other road-related data.
5. **Disaster Recovery**: In disaster-stricken areas, where communication infrastructure might be compromised, ad hoc networks can help survivors and aid organizations communicate and coordinate relief efforts.
6. **IoT and Sensor Networks**: Ad hoc networks can be used to connect and coordinate IoT devices and sensor nodes for data collection, environmental monitoring, and other applications.

(b) What is better for computer communication — analog or digital? Justify your answer.

Ans. For computer communication, digital communication is far superior to analog communication. This is due to several key advantages that digital communication offers over analog in terms of efficiency, accuracy, scalability, and reliability.

1. Precision and Noise Resistance

Digital Signals: Digital communication uses discrete values (0s and 1s) to represent data, which makes it highly resistant to noise and signal degradation. Even if noise affects the signal during transmission, the distinct binary nature of digital signals makes it easier for systems to detect and correct errors using techniques like parity checks and error-correcting codes.

Analog Signals: Analog communication involves continuous signals, making it more susceptible to interference and signal degradation. Noise can distort an analog signal in such a way that the original message becomes irretrievable, especially over long distances.

2. Data Integrity and Accuracy

Digital Communication: Digital systems allow for lossless data transmission, ensuring the message received is identical to the message sent. This is crucial for accurate communication, especially in fields like computing, where even small data errors can have significant consequences.

Analog Communication: In contrast, analog signals are vulnerable to data loss and distortion, which can degrade the quality of communication. For instance, in analog telephony, noise on the line can make a conversation difficult to hear clearly.

3. Efficiency and Speed

Digital Communication: Digital systems can transmit data at much higher speeds and handle greater bandwidths compared to analog systems. Compression techniques can also be applied to digital signals, allowing for efficient use of communication channels. This is particularly beneficial for transmitting large volumes of data, such as in modern internet communications.

Analog Communication: Analog transmission typically requires more bandwidth and is less efficient, especially when transmitting complex data like multimedia files.

4. Scalability and Flexibility

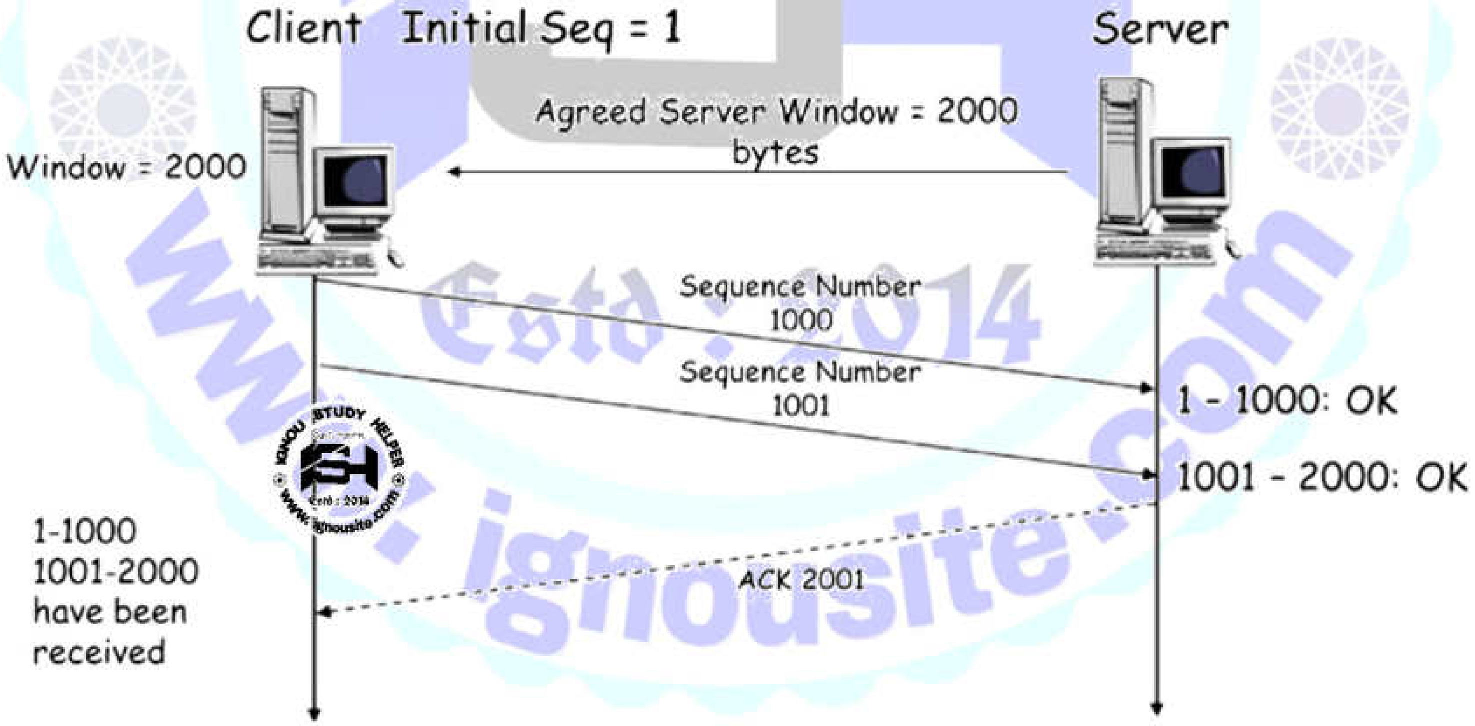
Digital Communication: Digital systems are highly scalable and can be integrated easily into modern network infrastructures. Technologies like fiber optics, Ethernet, and Wi-Fi are optimized for digital communication, enabling faster and more efficient data transfer.

Analog Communication: Analog systems lack the flexibility of digital systems and are increasingly outdated in modern computing environments.

Digital communication is better for computer communication due to its superior noise resistance, higher accuracy, efficiency, and scalability. It has become the standard for modern computing and communication systems, while analog communication is largely obsolete in this context.

Q3. What is Windowing? How is flow control and reliability achieved through windowing at transport layer?

Ans. Windowing is a technique used in computer networks, particularly at the transport layer (e.g., in protocols like TCP), to control the flow of data between two devices. It manages the amount of data that can be sent before requiring an acknowledgment from the receiving device. This approach allows for efficient data transmission while preventing the sender from overwhelming the receiver or the network with too much data at once.



How Windowing Works: In windowing, a window size is established, representing the number of bytes (or packets) that the sender can transmit before it must wait for an acknowledgment (ACK) from the receiver. As data is sent, the sender tracks which data has been acknowledged and which data still needs to be acknowledged. This sliding window mechanism moves forward as acknowledgments are received, allowing new data to be transmitted.

There are two key types of windowing:

1. **Fixed Windowing**: The window size remains constant throughout the communication.
2. **Sliding Windowing**: The window size can dynamically change based on network conditions and the receiver's capacity.

Achieving Flow Control Through Windowing: Flow control ensures that the sender does not overwhelm the receiver with more data than it can handle. In windowing, flow control is implemented by adjusting the window size based on the receiver's capacity to process data.

1. **Window Size Adjustments**: The receiver advertises its buffer space (i.e., the window size) to the sender, indicating how much data it can receive at one time without getting overwhelmed. If the receiver's buffer fills up, it reduces the advertised window size, signaling the sender to slow down.
2. **Avoiding Congestion**: If the receiver has a small buffer or is processing data slowly, the window size is kept small, limiting the sender to transmit only a small amount of data. Once the receiver processes some of the data and its buffer is freed up, it increases the window size, allowing the sender to transmit more data.

This dynamic adjustment ensures that the sender sends only what the receiver can handle, thus preventing data loss or the need for retransmission due to buffer overflow.

Achieving Reliability Through Windowing:
Reliability in windowing is achieved through mechanisms that ensure all data is delivered correctly and in order. Windowing supports reliability using the following features:

1. **Acknowledgments (ACKs):** For each segment of data sent, the sender expects an acknowledgment from the receiver. If an ACK is not received within a certain time (due to data loss or delay), the sender retransmits the unacknowledged data, ensuring that no data is lost in transit.
2. **Sliding Window Mechanism**: As the sender receives ACKs for data segments, the window slides forward, allowing the sender to transmit more data. If data segments are lost, the sliding window stops advancing, ensuring that the sender retransmits only the missing segments.
3. **Sequence Numbers**: Each data segment is assigned a sequence number. The receiver uses these numbers to keep track of the order of the segments and detect any missing or out-of-order segments. This helps maintain the correct data order, even if segments are received out of sequence.
4. **Retransmission and Timeouts**: If the sender doesn't receive an ACK within a specific time period (timeout), it assumes the segment was lost and retransmits it. This mechanism guarantees that any lost data is re-sent until successfully acknowledged by the receiver.

Example: TCP Windowing:
In the Transmission Control Protocol (TCP), windowing is crucial for managing the flow of data and ensuring reliability.

Flow Control in TCP: TCP uses a sliding window mechanism where the receiver advertises its available buffer space to the sender, indicating how much data can be transmitted before needing an acknowledgment. If the receiver's buffer is full, the window size is reduced, preventing data loss.

Reliability in TCP: TCP ensures reliable communication by using sequence numbers, ACKs, and retransmission mechanisms. If segments are lost, the receiver requests their retransmission using the sequence numbers to reorder the segments correctly.

Q4.

(a) Compare between CSMA/CD and Ethernet protocol. How does CSMA/CD resolve the problem of line connection? Explain.

Ans. Comparison Between CSMA/CD and Ethernet Protocol: Ethernet is a widely used communication protocol that defines how devices on a local area network (LAN) communicate with each other. Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a media access control (MAC) protocol that is part of Ethernet and is used to manage how devices share the communication medium, particularly in early Ethernet networks with shared mediums like coaxial cables or hubs.

Although CSMA/CD is a fundamental aspect of early Ethernet implementations, modern Ethernet primarily uses full-duplex communication and switches, making collision detection less relevant today.

Feature	CSMA/CD Protocol	Ethernet Protocol
Purpose	CSMA/CD is a mechanism to detect and resolve collisions on a shared medium.	Ethernet is a broader protocol that defines how devices communicate in a LAN. CSMA/CD is just one part of Ethernet.
Network Type	CSMA/CD is used in half-duplex Ethernet networks where devices share the same communication medium.	Ethernet includes both half-duplex (where CSMA/CD is relevant) and full-duplex modes (collision detection is unnecessary).
Collision Management	CSMA/CD detects and resolves collisions when two devices attempt to transmit data simultaneously.	Modern Ethernet primarily uses switches and full-duplex communication, which eliminates the need for collision detection.
Media Access Control (MAC)	CSMA/CD ensures fair access to the shared medium, handling the situation when multiple devices want to send data.	Ethernet defines both physical (cabling) and MAC layer rules for communication, which can include CSMA/CD in shared networks.
Scalability	Not scalable for high-speed networks due to performance degradation as collisions increase.	Ethernet is highly scalable, especially with the introduction of switches and full-duplex modes.
Speed	Slower performance due to collisions and retransmissions in shared networks.	Modern Ethernet can achieve high speeds (10 Gbps and beyond) without collision issues in switched, full-duplex networks.
Current Relevance	Largely obsolete in modern networks with switched Ethernet.	Ethernet is widely used in modern networks, but CSMA/CD is no longer needed due to advancements in technology.

How CSMA/CD Resolves Line Connection Problems

In a network using CSMA/CD, multiple devices share the same physical communication channel. The main challenge in this setup is ensuring that only one device transmits data at a time to avoid collisions. Here's how CSMA/CD resolves the problem of simultaneous transmissions:

1. Carrier Sense (CS): Before a device attempts to send data, it listens to the communication channel to determine if it is free or busy. This process is called Carrier Sense. If the channel is idle, the device can proceed with transmission. If the channel is busy (another device is transmitting), the device waits for the channel to become free.

2. Multiple Access (MA): Multiple devices have equal access to the shared communication channel. They all use the same medium and must take turns transmitting data. The protocol allows any device to access the medium once it becomes free.

3. Collision Detection (CD): Even though devices try to avoid sending data at the same time by using the carrier sense mechanism, collisions can still occur. This happens if two devices listen, find the channel idle, and then start transmitting simultaneously (since there is a delay in propagation).

To handle this, each device monitors the communication channel during its transmission. If a device detects that a collision has occurred (because the voltage levels on the medium will deviate from expected values), it stops transmitting immediately.

4. Collision Resolution: When a collision is detected, both devices stop transmitting data and send a special signal called a jamming signal to notify all other devices that a collision has occurred. After that, the involved devices use an algorithm known as binary exponential backoff to decide when to retry transmission.

> **Binary Exponential Backoff**: Each device waits for a random period before attempting to retransmit. If another collision occurs, the waiting period is doubled, and the process repeats. This exponentially increasing backoff time reduces the likelihood of collisions happening again, helping manage network traffic more efficiently.

Steps in CSMA/CD Process

1. **Listen to the Channel (Carrier Sense)**: Devices check if the medium is idle before transmitting data.
2. **Transmit Data**: If the channel is idle, the device sends its data.
3. **Monitor for Collisions**: While transmitting, the device monitors the channel for any signs of collision.
4. **Collision Detection**: If a collision is detected, the device immediately stops transmitting.
5. **Send Jamming Signal**: The device broadcasts a jamming signal to alert other devices of the collision.
6. **Backoff and Retransmit**: The device waits for a random time interval before attempting to retransmit the data.

Impact on Network Efficiency: While CSMA/CD worked well for early Ethernet networks with fewer devices and lower speeds, it became less efficient as network speed and the number of connected devices increased. The frequent collisions, especially in heavily utilized networks, degraded performance. This led to the transition to switched Ethernet and full-duplex communication, which eliminated the need for CSMA/CD by allowing simultaneous transmission and reception without collisions.

(b) Differentiate between circuit switching and virtual circuit. Also explain the effect of router failure in virtual circuits.

Ans. A comparison between circuit switching and virtual circuits, followed by an explanation of the effect of router failure in virtual circuits:

Comparison Table: Circuit Switching vs. Virtual Circuits

Aspect	Circuit Switching	Virtual Circuit
Definition	A dedicated communication path is established between the sender and receiver for the duration of the session.	A logical path is established between sender and receiver, using the underlying network's shared resources.
Connection Type	Physical and dedicated circuit throughout the communication.	Logical path; not dedicated. Uses packet-switching techniques.
Resource Reservation	Resources (bandwidth, channels) are reserved for the entire session.	No exclusive reservation of resources; packets are routed dynamically along a predefined logical path.
Setup Delay	Requires significant time to establish the circuit before communication can start.	Less setup time, as it relies on packet switching; logical connection is established first.
Data Transmission	Continuous data transmission with guaranteed bandwidth.	Data is transmitted in packets, with each packet containing a header to identify the virtual circuit.
Reliability	Highly reliable since the dedicated path is established end-to-end.	Generally reliable, but less than circuit switching because it depends on routers and the underlying packet-switched network.

Connection Duration	Connection remains active until terminated by the users.	The logical path exists only as long as the session is active; the path may change if necessary.
Example	Traditional telephone networks (e.g., landline calls).	Frame Relay, MPLS (Multiprotocol Label Switching), and ATM (Asynchronous Transfer Mode).
Failure Impact	The entire communication session is disrupted if a physical link fails.	More flexible; failure of one router or path can be mitigated by rerouting packets via alternative paths.
Network Efficiency	Less efficient; resources are locked for the duration of the connection, even if no data is being transmitted.	More efficient as resources are used dynamically and shared among multiple virtual circuits.
Scalability	Less scalable due to the need for dedicated physical resources.	More scalable since multiple virtual circuits can share the same physical infrastructure.
Use Case	Ideal for voice communication where real-time, consistent transmission is critical.	Used in data transmission where flexibility, efficiency, and dynamic routing are needed.
Connection Maintenance	Once a circuit is established, the same path is used throughout the communication.	The logical path can change during the session, especially in case of failure or congestion.

Effect of Router Failure in Virtual Circuits: In a virtual circuit, packets follow a pre-established logical path through the network. However, the underlying physical infrastructure (routers, switches, etc.) is shared with other circuits, and if a router fails, the system must respond to maintain communication.

1. **Router Failure Impact**:
   a) **Packet Loss**: Initially, packets that are being routed through the failed router might be lost because the router can't forward them.

   b) **Rerouting**: Most modern networks employing virtual circuits use dynamic routing protocols (like OSPF or MPLS) to detect failures. When a router fails, these protocols quickly reroute the data packets through alternative paths.

   c) **Temporary Disruption**: There may be a temporary disruption in communication while the network recalculates the new path and re-establishes the virtual circuit.

   d) **Resilience**: Virtual circuit networks are more resilient to failures than circuit-switched networks. Instead of the entire communication session being terminated, the network can recover by rerouting around the failure point.

2. **Handling Router Failure**:
   a) **Fast Recovery**: In systems like MPLS, fast reroute mechanisms can redirect packets to alternative routes, ensuring minimal downtime.

   b) **Network Overhead**: Though rerouting provides flexibility and reliability, it can lead to a slight increase in network overhead, as packets may take longer routes temporarily, potentially increasing latency.

Q5. Given data frame is 1101011011 and generator polynomial G(x) = x^4+ x + 1. Derive the transmitted frame using CRC method. Write all the steps involved in the process.

Ans. To derive the transmitted frame using the CRC (Cyclic Redundancy Check) method with the given data frame and generator polynomial, follow these steps:

Step-by-Step CRC Calculation

1. **Data Frame and Generator Polynomial Given:**

   Data Frame: D(x)=1101011011

   Generator Polynomial: G(x)=x^4+x+1

2. **Append Zeros (Padding):**
   Append zeros to the data frame to match the degree of the generator polynomial minus one (4 zeros for G(x)=x^4+x+1:

Original Data Frame: 1101011011 Appended with zeros: 11010110110000

3. **Initial Division:**
   Perform the division of the data frame by the generator polynomial using modulo-2 arithmetic (XOR operation):

Divide: 11010110110000 by G(x)=x^4+x+1

Start with the leftmost bits that align with the generator polynomial.

```
 1101011011 0000  (Data Frame)
 10011          (Generator Polynomial, x^4 + x + 1)
__________
0101011011 0000   (Result of first XOR operation)
 10011
 __________
   11001011 0000    (Result of second XOR operation)
   10011
   __________
     1001011 0000   (Result of third XOR operation)
     10011
     __________
      1011000   (Result of fourth XOR operation)
      10011
      __________
       111011   (Result of fifth XOR operation)
       10011
      ___________
        10110  (Result of sixth XOR operation)
        10011
        ___________
         1101 (Result of seventh XOR operation)
         10011
         __________
          111 (Result of eighth XOR operation)
          10011
          __________
           110 (Result of ninth XOR operation)
           10011
           ___________
            10 (Result of tenth XOR operation)
```

10011

0 (Final remainder after all divisions)

4. **Obtain CRC (Remainder):**
   After performing all the XOR operations, the remainder is 101010.

5. **Transmitted Frame (Data + CRC):**
   Append the remainder (CRC) to the original data frame to get the transmitted frame:

Original Data Frame: 1101011011 CRC (remainder): 10

Transmitted Frame: 110101101110

This transmitted frame 110101101110 includes the original data frame followed by the calculated CRC (remainder) bits. This ensures that during transmission, the receiver can perform the same CRC calculation and verify if the data frame is received correctly by checking if the remainder is zero. If not, an error in transmission may have occurred.

Q6. Differentiate between public key cryptography and private-key cryptography. Assume two prime numbers p and q are 13 and 17 respectively. Calculate private key and public key using RSA algorithm.

Ans. A comparison between public key cryptography (asymmetric cryptography) and private-key cryptography (symmetric cryptography), along with the calculation of private and public keys using the RSA algorithm with given prime numbers p=13 and q=17:

Comparison Table: Public Key Cryptography vs. Private-Key Cryptography

Aspect	Public Key Cryptography (Asymmetric)	Private-Key Cryptography (Symmetric)
Key Type	Uses two keys: Public Key for encryption and Private Key for decryption.	Uses a single key for both encryption and decryption.
Security	More secure due to the separation of keys; private key remains secret.	Less secure because the same key is used for encryption and decryption.
Key Distribution	Public keys can be distributed widely; private keys are kept secret.	Key distribution is challenging as both parties need the same key.
Computational Complexity	Generally slower due to complex mathematical operations with large keys.	Faster because operations involve simpler algorithms and smaller keys.
Application	Used for secure communication, digital signatures, and key exchange protocols.	Ideal for fast data encryption/decryption in secure environments.
Examples	RSA, ECC (Elliptic Curve Cryptography), DSA (Digital Signature Algorithm).	AES (Advanced Encryption Standard), DES (Data Encryption Standard).

RSA Algorithm Example: Calculation of Private and Public Keys

Given:

p=13

q=17

1. **Calculate nnn (Modulus):**

$n = p \times q = 13 \times 17 = 221$

2. **Calculate φ(n) (Euler's Totient Function):**
   $\varphi(n) = (p-1) \times (q-1) = (13-1) \times (17-1) = 12 \times 16 = 192$

3. **Choose Public Key e:**
   Select e such that $1 < e < \varphi(n)$ and $\gcd(e,\varphi(n)) = 1$. Common choices are primes or numbers coprime to φ(n).

   Let's choose e = 5.

4. **Calculate Private Key ddd (Modular Multiplicative Inverse of e mod φ(n)):**
   Find d such that $d \cdot e \equiv 1 \pmod{\varphi(n)}$.

Use the Extended Euclidean Algorithm to find d:

e = 5

φ(n) = 192

Extended Euclidean Algorithm:
192 = 5 \times 38 + 2
5 = 2 \times 2 + 1
2 = 1 \times 2 + 0

Back substitution gives us:
1 = 5 - 2 \times 2
 = 5 - 2 \times (192 - 5 \times 38)
 = 77 \times 5 - 2 \times 192

Therefore, d = 77 mod 192 = 77
So, d=77 is the private key.

5. **Public and Private Keys:**
   Public Key: (e,n)=(5, 221)

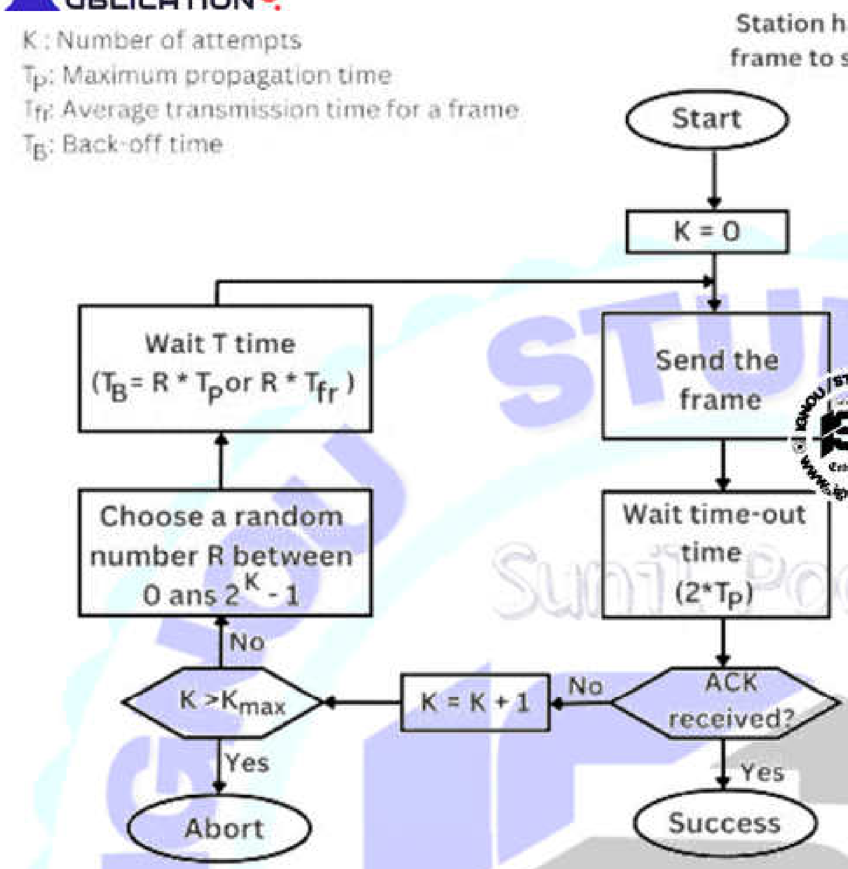
   Private Key: (d,n)=(77, 221)

Q7.

(a) Differentiate between pure ALOHA and slotted ALOHA. Give formulas for their throughput.

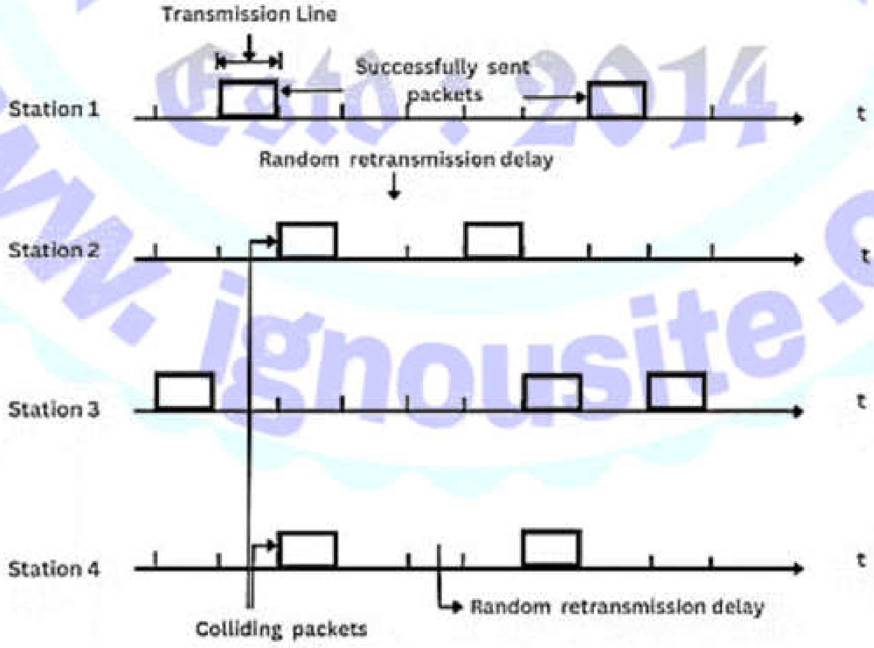
Ans. Pure Aloha: Pure Aloha can be termed as the main Aloha or the original Aloha. Whenever any frame is available, each station sends it, and due to the presence of only one channel for communication, it can lead to the chance of collision.

In the case of the pure aloha, the user transmits the frame and waits till the receiver acknowledges it, if the receiver does not send the acknowledgment, the sender will assume that it has not been received and sender resends the acknowledgment.


K : Number of attempts
T_P: Maximum propagation time
T_{fr}: Average transmission time for a frame
T_B: Back-off time
Station has a frame to send
Start
K = 0
Send the frame
Wait time-out time ($2*T_P$)
ACK received?
No
Yes
Success
K = K + 1
K >K_{max}
Yes
Abort
No
Choose a random number R between 0 ans 2^K - 1
Wait T time (T_B= R * $T_P$or R * T_{fr})

Slotted Aloha: Slotted Aloha is simply an advanced version of pure Aloha that helps in improving the communication network. A station is required to wait for the beginning of the next slot to transmit. The vulnerable period is halved as opposed to Pure Aloha.

Slotted Aloha helps in reducing the number of collisions by properly utilizing the channel and this basically results in the somehow delay of the users. In Slotted Aloha, the channel time is separated into particular time slots.


Transmission Line
Successfully sent packets
Station 1
t
Random retransmission delay
Station 2
t
Station 3
t
Station 4
t
Colliding packets
Random retransmission delay

Differences Between Pure Aloha and Slotted Aloha

Pure Aloha	Slotted Aloha
In this Aloha, any station can transmit the data at any time.	In this, any station can transmit the data at the beginning of any time slot.
In this, The time is continuous and not globally synchronized.	In this, The time is discrete and globally synchronized.
Vulnerable time for Pure Aloha = 2 x Tt	Vulnerable time for Slotted Aloha = Tt
In Pure Aloha, the Probability of successful transmission of the data packet = G x e-2G	In Slotted Aloha, the Probability of successful transmission of the data packet = G x e-G
In Pure Aloha, Maximum efficiency = 18.4%	In Slotted Aloha, Maximum efficiency = 36.8%
Pure Aloha doesn't reduce the number of collisions to half.	Slotted Aloha reduces the number of collisions to half and doubles the efficiency of Pure Aloha.

Throughput Formulas

1. Pure ALOHA:

Throughput (S): Represents the fraction of time that the channel is used successfully for transmitting data.

$S = G \cdot e^{-2G}$

GGG is the average number of frames generated by the system in one frame time.

e^{-2G} accounts for the probability that no other frames are transmitted during the time a frame is being sent (considering collisions).

The maximum throughput for Pure ALOHA occurs when G=0.5, which results in $S_{max}=1/2e \approx 0.184$ or 18.4%.

2. Slotted ALOHA:

Throughput (S): Represents the fraction of time the channel is used successfully for transmitting data, but only during the time slots.

$S=G \cdot e^{-G}$

G is the average number of frames generated by the system in one time slot.

e^{-G} accounts for the probability that no other frames are transmitted during the time slot a frame is being sent (considering collisions).

The maximum throughput for Slotted ALOHA occurs when G = 1, which results in $S_{max} = e^{-1} \approx 0.368$ or 36.8%.

(b) Explain the importance of Sliding Window Protocol. Also, list the types of sliding window techniques.

Ans. Sliding Window Protocol: The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol).

In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

Types of Sliding Window Techniques

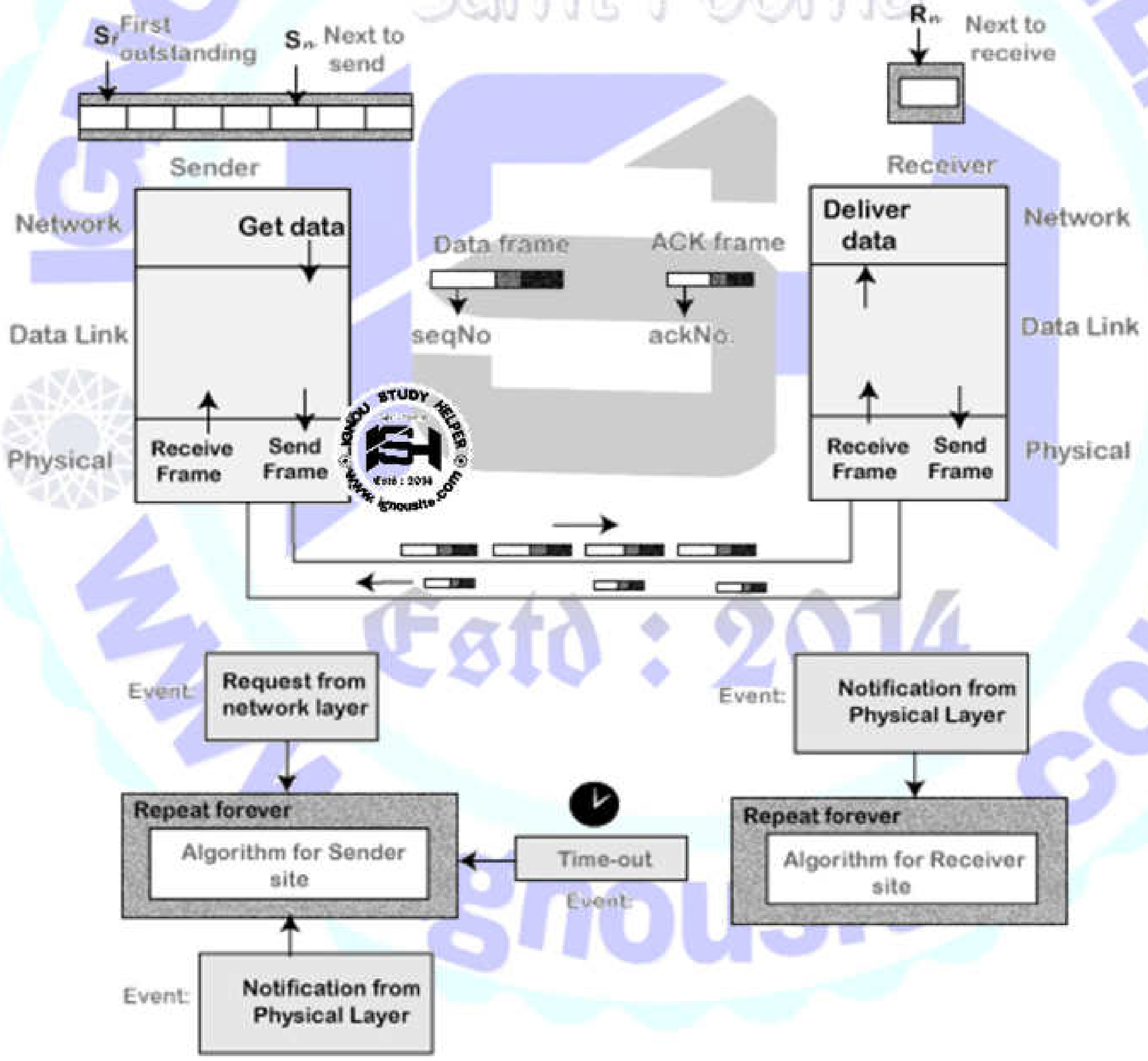
Sliding window technique has two types:

1. Go-Back-N ARQ
2. Selective Repeat ARQ

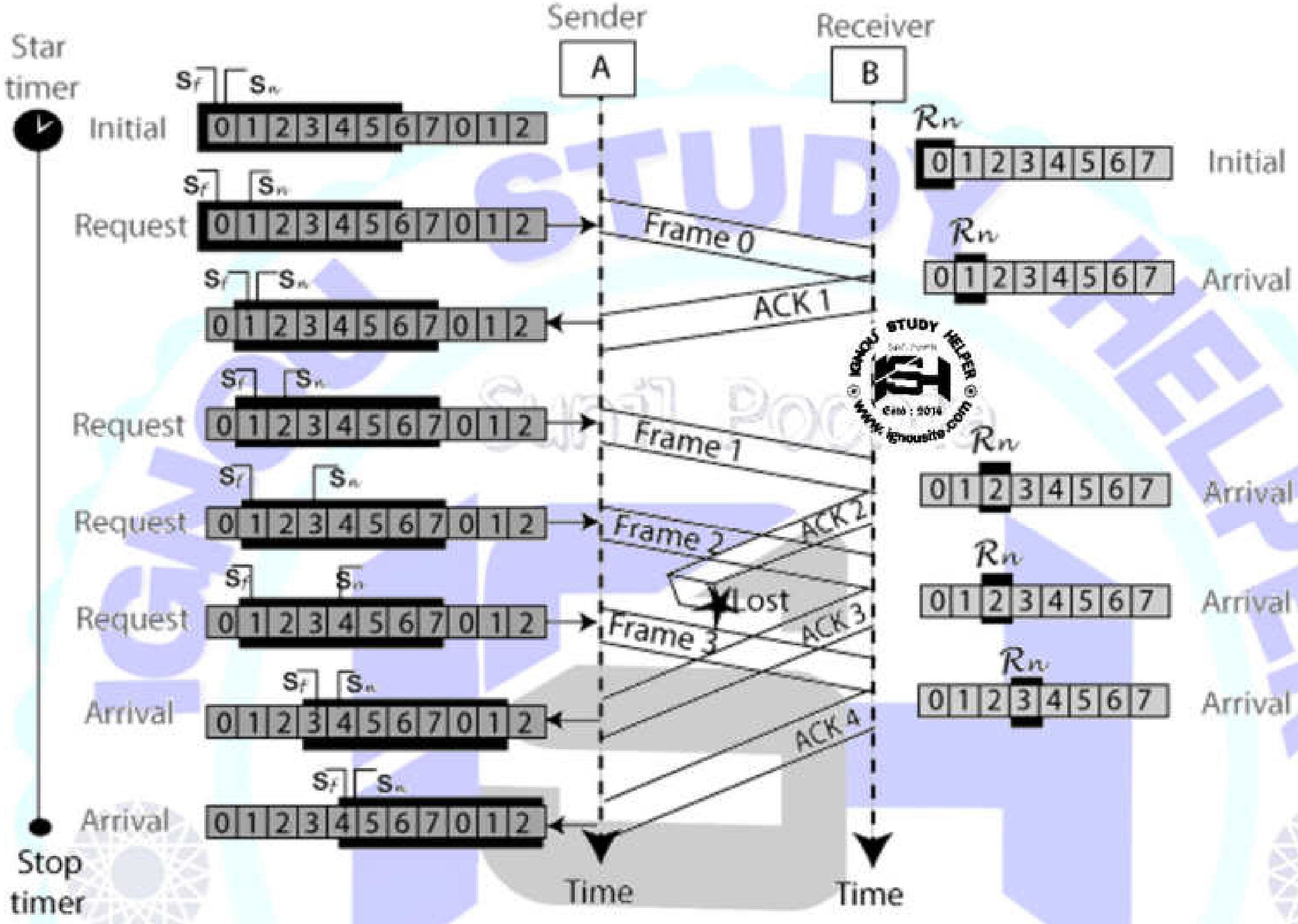
1. Go-Back-N ARQ: Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.

The size of the sender window is N in this protocol. For example, Go-Back-8, the size of the sender window, will be 8. The receiver window size is always 1.

If the receiver receives a corrupted frame, it cancels it. The receiver does not accept a corrupted frame. When the timer expires, the sender sends the correct frame again. The design of the Go-Back-N ARQ protocol is shown below.

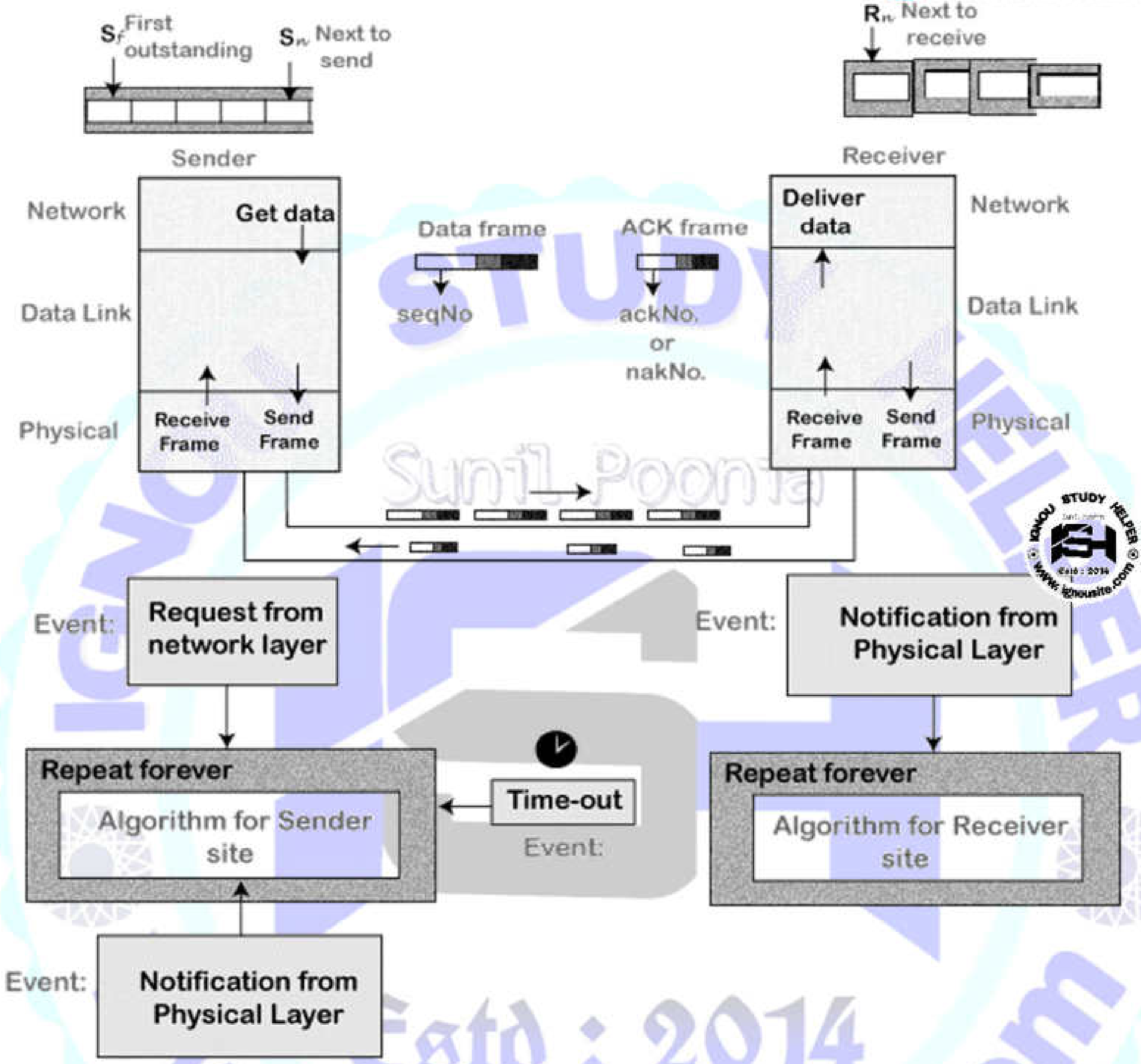


The example of Go-Back-N ARQ is shown below in the figure.

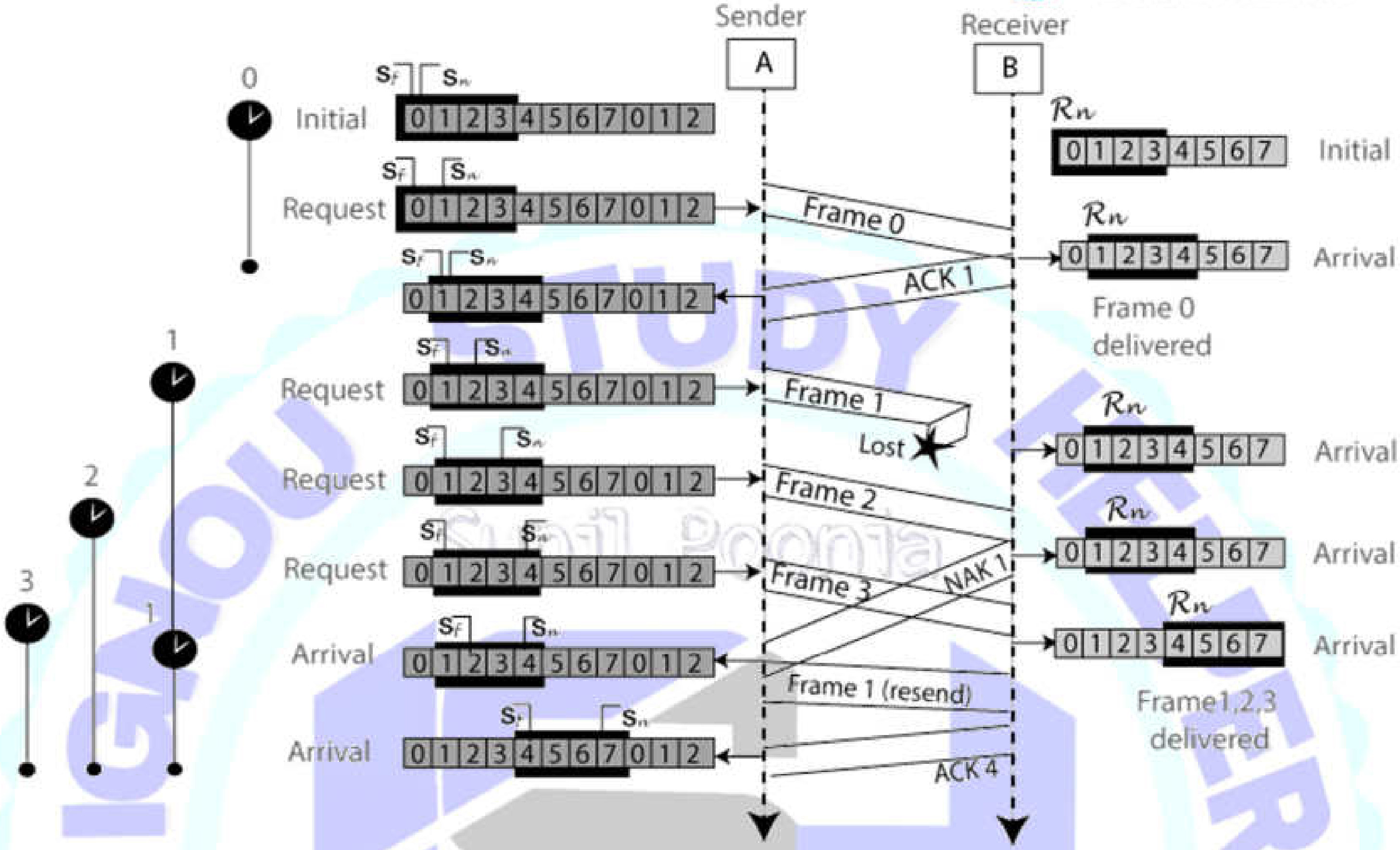


2. Selective Repeat ARQ: Selective Repeat ARQ is also known as the Selective Repeat Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. The Go-back-N ARQ protocol works well if it has fewer errors. But if there is a lot of error in the frame, lots of bandwidth loss in sending the frames again. So, we use the Selective Repeat ARQ protocol. In this protocol, the size of the sender window is always equal to the size of the receiver window. The size of the sliding window is always greater than 1.

If the receiver receives a corrupt frame, it does not directly discard it. It sends a negative acknowledgment to the sender. The sender sends that frame again as soon as on the receiving negative acknowledgment. There is no waiting for any time-out to send that frame. The design of the Selective Repeat ARQ protocol is shown below.



The example of the Selective Repeat ARQ protocol is shown below in the figure.



Q8.

(a) Write the step-by-step working of Link State Routing. Also, compare it with Distance Vector Routing.

Ans. Link State Routing: Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork.

The three keys to understand the Link State Routing algorithm:

1. **Knowledge about the neighborhood:** Instead of sending its routing table, a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.

2. **Flooding:** Each router sends the information to every other router on the internetwork except its neighbors. This process is known as Flooding. Every router that receives the packet sends the copies to all its neighbors. Finally, each and every router receives a copy of the same information.

3. **Information sharing:** A router sends the information to every other router only when the change occurs in the information.

Link State Routing has two phases:

Reliable Flooding

a) **Initial state:** Each node knows the cost of its neighbors.

b) **Final state:** Each node knows the entire graph.

Route Calculation

Each node uses Dijkstra's algorithm on the graph to calculate the optimal routes to all nodes.

a) The Link state routing algorithm is also known as Dijkstra's algorithm which is used to find the shortest path from one node to every other node in the network.

b) The Dijkstra's algorithm is an iterative, and it has the property that after k^{th} iteration of the algorithm, the least cost paths are well known for k destination nodes.

Let's describe some notations:

- **c(i , j):** Link cost from node i to node j. If i and j nodes are not directly linked, then c(i , j) = ∞.
- **D(v):** It defines the cost of the path from source code to destination v that has the least cost currently.
- **P(v):** It defines the previous node (neighbor of v) along with current least cost path from source to v.
- **N:** It is the total number of nodes available in the network.

Algorithm:

```
Initialization
N = {A} // A is a root node.
for all nodes v
if v adjacent to A
then D(v) = c(A,v)
else D(v) = infinity
loop
find w not in N such that D(w) is a minimum.
Add w to N
Update D(v) for all v adjacent to w and not in N:
D(v) = min(D(v) , D(w) + c(w,v))
Until all nodes in N
```

Comparison between Distance Vector Routing and Link State Routing

Distance Vector Routing	Link State Routing
Bandwidth required is less due to local sharing, small packets and no flooding.	Bandwidth required is more due to flooding and sending of large link state packets.
Based on local knowledge, since it updates table based on information from neighbours.	Based on global knowledge, it have knowledge about entire network.
Make use of Bellman Ford Algorithm.	Make use of Dijakstra's algorithm.
Traffic is less.	Traffic is more.
Converges slowly i.e, good news spread fast and bad news spread slowly.	Converges faster.

Count of infinity problem.	No count of infinity problem.
Persistent looping problem i.e, loop will be there forever.	No persistent loops, only transient loops.
Practical implementation is RIP and IGRP.	Practical implementation is OSPF and ISIS.

(b) Explain leaky bucket algorithm for congestion control. Also list its advantages and disadvantages.

Ans. leaky bucket algorithm for congestion control: Congestion control is a crucial concept in computer networks. It refers to the methods used to prevent network overload and ensure smooth data flow. When too much data is sent through the network at once, it can cause delays and data loss. Congestion control techniques help manage the traffic, so all users can enjoy a stable and efficient network connection. These techniques are essential for maintaining the performance and reliability of modern networks.

Congestion in a computer network happens when there is too much data being sent at the same time, causing the network to slow down. Just like traffic congestion on a busy road, network congestion leads to delays and sometimes data loss. When the network can't handle all the incoming data, it gets "clogged," making it difficult for information to travel smoothly from one place to another.

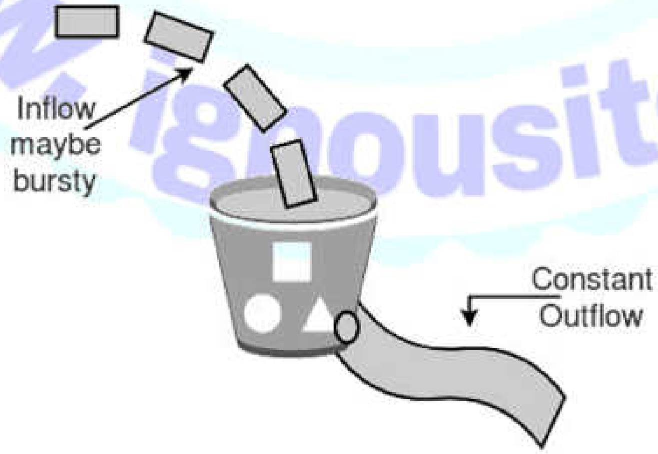
Congestion Control Algorithm

- Congestion Control is a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse.
- **Congestive-avoidance algorithms** (CAA) are implemented at the TCP layer as the mechanism to avoid congestive collapse in a network.
- There are two congestion control algorithms which are as follows:

Leaky Bucket Algorithm

- The leaky bucket algorithm discovers its use in the context of network traffic shaping or rate-limiting.
- A leaky bucket execution and a token bucket execution are predominantly used for traffic shaping algorithms.
- This algorithm is used to control the rate at which traffic is sent to the network and shape the burst traffic to a steady traffic stream.
- The disadvantages compared with the leaky-bucket algorithm are the inefficient use of available network resources.
- The large area of network resources such as bandwidth is not being used effectively.

Let us consider an example to understand Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate. When the bucket is full with water additional water entering spills over the sides and is lost.



Similarly, each network interface contains a leaky bucket and the following steps are involved in leaky bucket algorithm:

- When host wants to send packet, packet is thrown into the bucket.
- The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
- Bursty traffic is converted to a uniform traffic by the leaky bucket.
- In practice the bucket is a finite queue that outputs at a finite rate.

Advantages

a) **Stable Network Operation**: Congestion control ensures that networks remain stable and operational by preventing them from becoming overloaded with too much data traffic.

b) **Reduced Delays**: It minimizes delays in data transmission by managing traffic flow effectively, ensuring that data packets reach their destinations promptly.

c) **Less Data Loss**: By regulating the amount of data in the network at any given time, congestion control reduces the likelihood of data packets being lost or discarded.

d) **Optimal Resource Utilization**: It helps networks use their resources efficiently, allowing for better throughput and ensuring that users can access data and services without interruptions.

e) **Scalability**: Congestion control mechanisms are scalable, allowing networks to handle increasing volumes of data traffic as they grow without compromising performance.

f) **Adaptability**: Modern congestion control algorithms can adapt to changing network conditions, ensuring optimal performance even in dynamic and unpredictable environments.

Disadvantages

a) **Complexity**: Implementing congestion control algorithms can add complexity to network management, requiring sophisticated systems and configurations.

b) **Overhead**: Some congestion control techniques introduce additional overhead, which can consume network resources and affect overall performance.

c) **Algorithm Sensitivity**: The effectiveness of congestion control algorithms can be sensitive to network conditions and configurations, requiring fine-tuning for optimal performance.

d) **Resource Allocation Issues**: Fairness in resource allocation, while a benefit, can also pose challenges when trying to prioritize critical applications over less essential ones.

e) **Dependency on Network Infrastructure**: Congestion control relies on the underlying network infrastructure and may be less effective in environments with outdated or unreliable equipment.