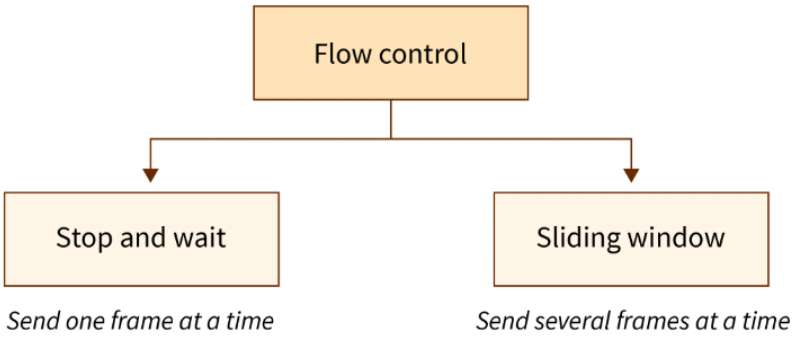
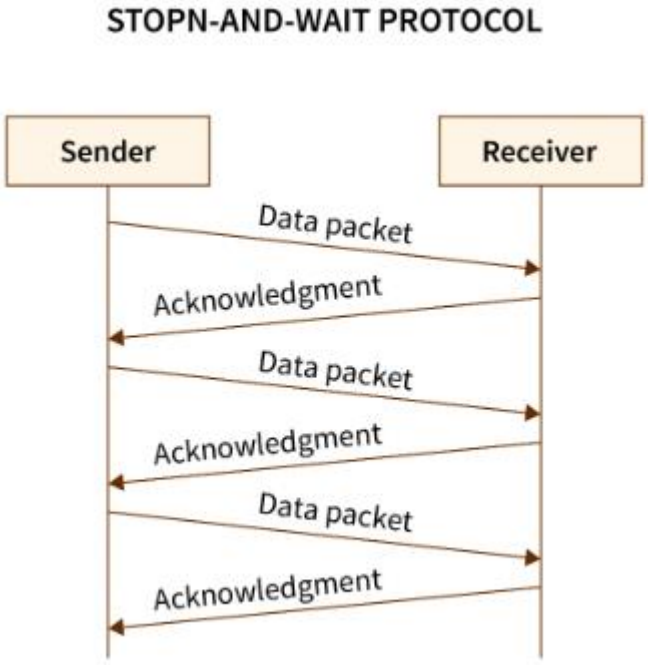
Explain how flow control and error control are ensured in data link layer.



Stop-and-wait Protocol

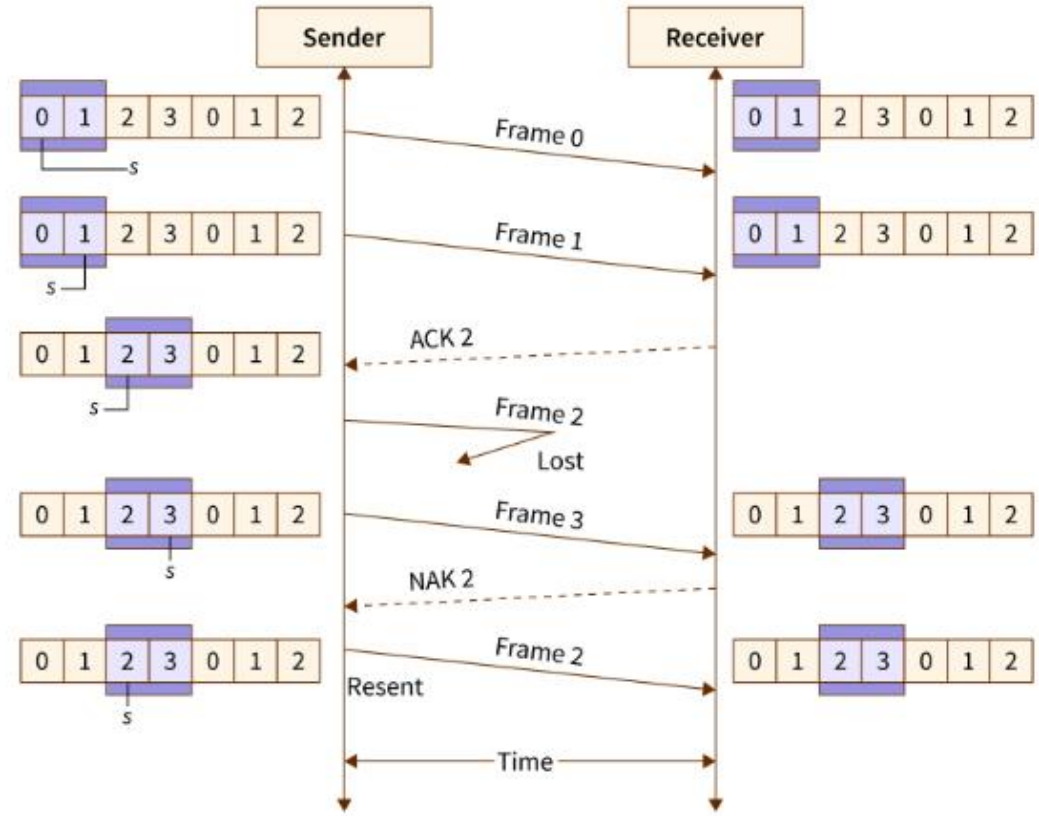
- The sender sends data to the receiver.
- The sender stops and waits for the acknowledgment.
- The receiver receives the data and processes it.
- The receiver sends an acknowledgment for the above data to the sender.
- The sender sends data to the receiver after receiving the acknowledgment of previously sent data.
- The process is unidirectional and continues until the sender sends the End of Transmission (EoT) frame.

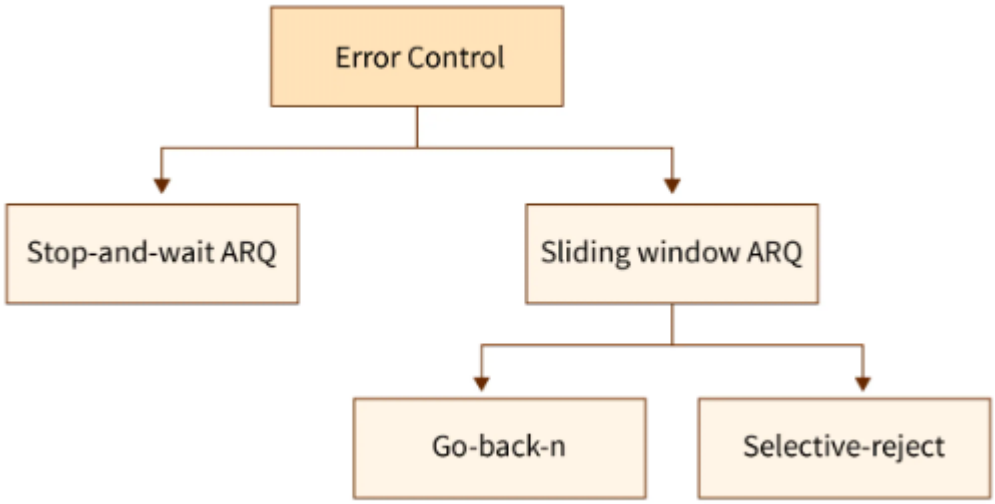


Sliding Window Protocol

- The sender and receiver have a “window” of frames. A window is a space that consists of multiple bytes. The size of the window on the receiver side is always 1.
- Each frame is sequentially numbered from 0 to n - 1, where n is the window size at the sender side.
- The sender sends as many frames as would fit in a window.

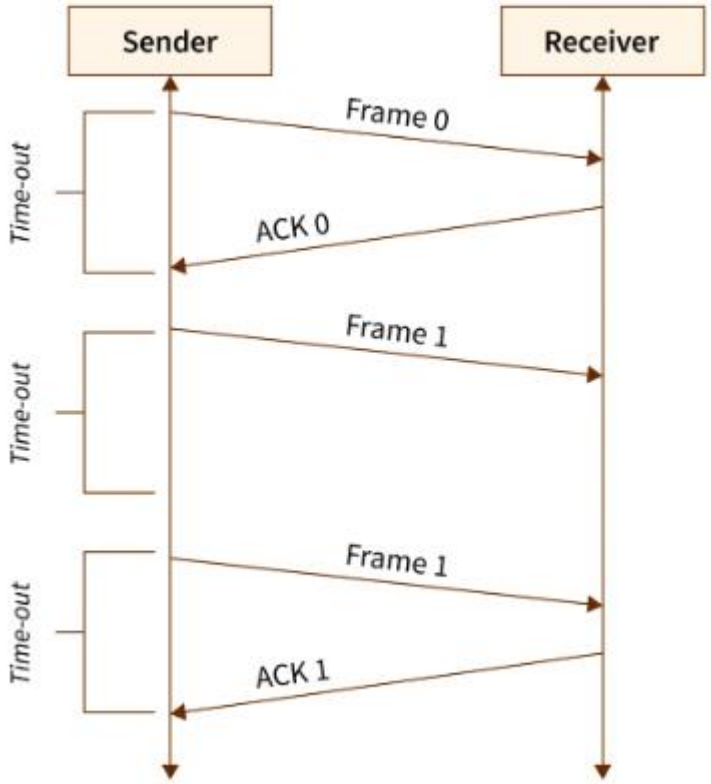
- After receiving the desired number of frames, the receiver sends an acknowledgment. The acknowledgment (ACK) includes the number of the next expected frame.





Stop-and-wait ARQ

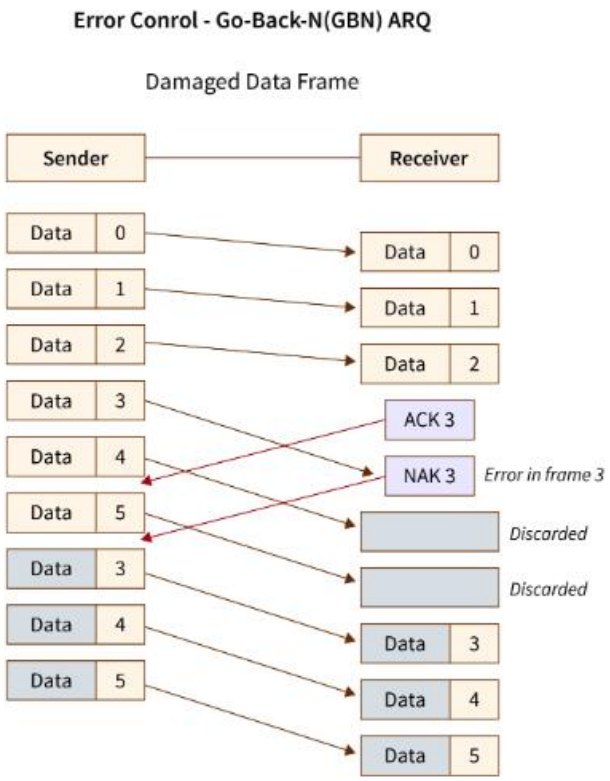
- In the case of stop-and-wait ARQ after the frame is sent, the sender maintains a timeout counter.
- If acknowledgment of the frame comes in time, the sender transmits the next frame in the queue.
- Else, the sender retransmits the frame and starts the timeout counter.
- In case the receiver receives a negative acknowledgment, the sender retransmits the frame.



Sliding Window ARQ

Go-Back-N ARQ :

In Go-Back-N ARQ, if the sent frames are suspected or damaged, all the frames are re-transmitted from the lost packet to the last packet transmitted.

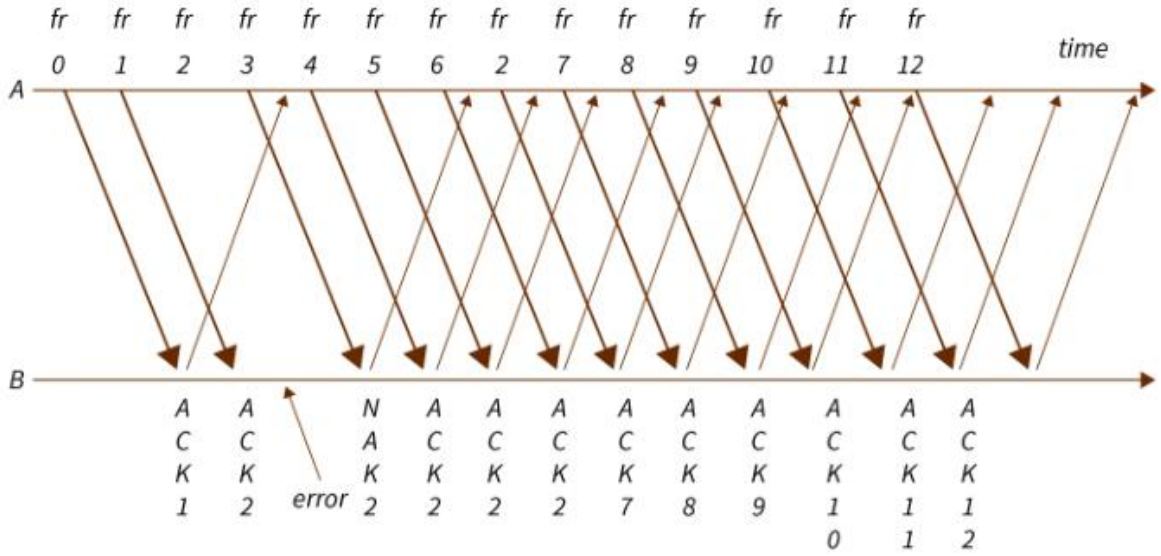


Selective Repeat ARQ:

In Selective Repeat ARQ only the suspected or damaged frames are re-transmitted.

Error Control - Selective Repeat ARQ

Error recovery in selective Repeat ARQ



Mention various parameters considered in hierarchical routing.

1. Network Size and Structure
2. Traffic Patterns
3. Administrative Boundaries
4. Scalability
5. Performance
6. Reliability

Explain the role of choke packets in congestion control.

A choke packet is a packet sent by a node to the source to inform it of congestion. Whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic. The intermediate nodes through which the packets have travelled are not warned about congestion.

Compare private network and virtual private network. Give their applications.

Private Network	**Virtual Private Network**
Uses dedicated physical connections.	Uses virtual connections over the Internet.
Limited to authorized users within the organization.	Allows remote access for users
Inherently secure due to its closed nature.	Relies on encryption and tunnelling protocols
More costly	Less costly
Applications: Corporate office, hospital	Applications: Remote work, Accessing content restricted to certain regions.

Explain the role of ports in transport layer.

1. **Multiplexing:** Ports enable multiplexing, allowing multiple applications to run concurrently on a device.
2. **Demultiplexing:** At the receiving end, the Transport Layer uses port numbers to demultiplex incoming data.

Explain the role of security considered in internet protocol and email.

IP works alongside other protocols like TCP and UDP, which offer higher-level security features like encryption and authentication. Secure protocols like IPSec can be implemented at the network level to provide encryption.

Security consideration in email include: authentication, encryption, anti-spam and malware and data deletion and privacy

Compare the features of static web pages and dynamic web pages used in WWW.

Static Web Pages	**Dynamic Web Pages**
Used for making static website	Used for making dynamic website
Simple code	Complex code
Information change rarely.	Information change frequently.
Takes less time to load	Takes more time to load
Database is not used.	Database is used.
Low cost	High cost

Explain the working mechanism of symmetric key algorithms in network security.

Symmetric key algorithm uses a shared secret key for both encryption and decryption. The sender uses the secret key to encrypt the plaintext message to unreadable ciphertext. The encrypted ciphertext is sent over the network. The receiver, having the same secret key, applies it to the ciphertext to decrypt it back into the original plaintext message.

Compare ARP and RARP. Give an illustration for each.

ARP	**RARP**
Used to obtain the MAC address of a device when only its IP address is known	Used to obtain the IP address of a device when only its MAC address is known
Maps IP address to MAC address	Maps MAC address to IP address
Translates 32-bit logical address to 48-bit physical address.	Translates 48-bit physical address to its 32-bit logical address.
Used by router or host	Used by client
Used on sender's side	Used on receiver's side
Local host maintains the ARP table.	RARP server maintains the RARP table.

Compare guided media and unguided media with reference to speed and security.

Feature	Guided Media	Unguided Media
Speed	Generally faster than unguided media	Generally slower than guided media
Security	More secure due to physical confinement.	Less secure due to open transmission.

Give an example to illustrate data link layer protocol.

Point to Point Protocol(PPP): It is the most robust data link protocol that is used to transport other types of packets also along with IP Packets. It can also be required for dial-up and leased router-router lines. It basically provides framing method to describe frames. It is a character-oriented protocol that is also used for error detection.

Compare static channel and dynamic channel allocation.

Static Channel Allocation	Dynamic Channel Allocation
Fixed number of channels are allocated to cells.	Fixed number of channels are not allocated to cells.
Frequency reuse is maximum	Frequency reuse is not maximum
Low cost	High cost
Performs better under heavy traffic	Performs better under light traffic
Low computational efforts	High computational efforts
Centralized control	Centralized or distributed control

Explain TDMA and FDMA used in MAC layer.

FDMA	TDMA
FDMA stands for Frequency Division Multiple Access.	TDMA stands for Time Division Multiple Access.
Guard bands between adjacent channels is necessary.	Guard time between adjacent slots is necessary.
Synchronization is not required.	Synchronization is necessary.
Power efficiency is less.	Power efficiency is high.
Bandwidth is divided into various frequency bands	Bandwidth is divided into various stations on time basis.
Each station is given a band to send data and that band is reserved for particular station	Each station is given a time slot, station can transmit data during that time slot only

Explain distance vector routing and link state routing. Give an example for each.

Distance Vector Routing	Link State Routing
Make use of Bellman Ford Algorithm.	Make use of Dijakstra's algorithm.
Based on local knowledge	Based on global knowledge

Bandwidth required is less	Bandwidth required is more
Converges slowly	Converges quickly
Count of infinity problem	No count of infinity problem.
Persistent looping problem	No persistent looping problem
Example: RIP	Example: OSPF

Compare multicast and anycast routing. Give their applications.

Multicast	Anycast
Single source sends a message to a group of devices	Single source sends a message to the nearest destination
Uses multicast group addresses to identify and address a group of hosts	Uses the same destination address for multiple hosts
Data is sent to all members of the multicast group simultaneously.	Data is sent to the nearest host
Reduced congestion	Improved performance
Application: Streaming, gaming, video conferencing	Application: CDNs, load balancing, distributed DNS

Explain the following congestion control algorithms:

Load shedding

It is a technique of congestion control. Router contains a buffer to store packets and route it to destination. When the buffer is full, it simply discards some packets. It chooses the packet to be discarded based on the strategy implemented in the data link layer.

Advantages:

- It can be used to detect congestion.
- It can be used to recover from congestion.
- It reduces the network traffic flow.

Disadvantages:

- It cannot avoid congestion
- Loss of packets

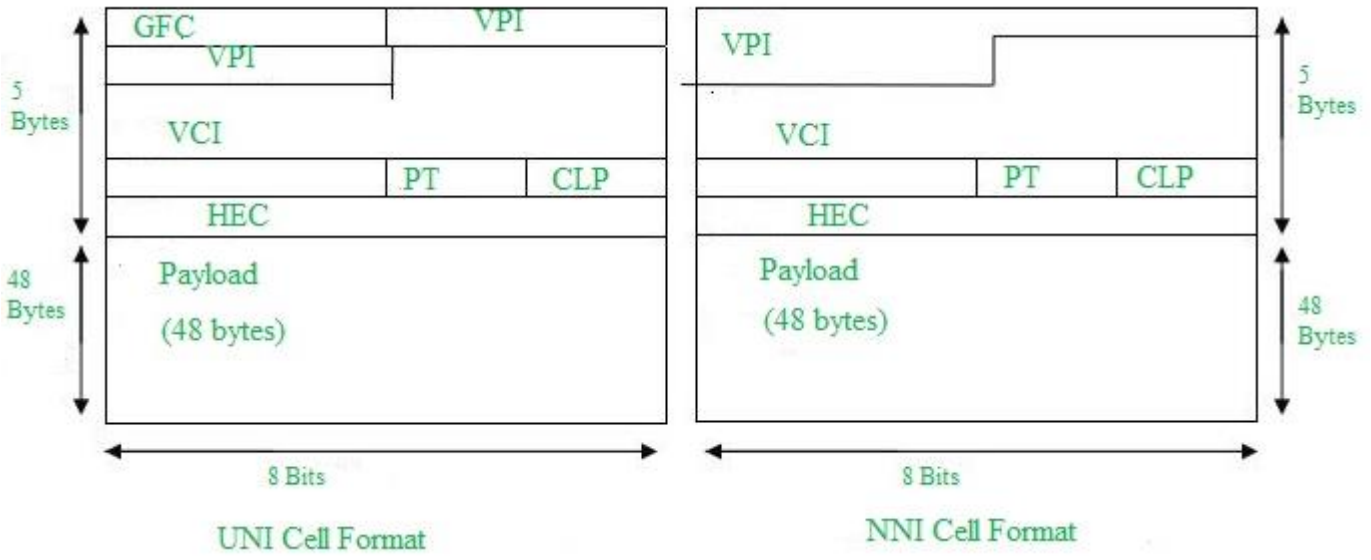
Admission control

The idea is do not set up a new virtual circuit unless the network can carry the added traffic without becoming congested.

Advantages: Congestion control, Improved network stability

Disadvantages: Increased delay, Increased cost

Give the ATM header format for: UNI (User-Network Interface) and NNI (Network-Network Interface)



Explain any four parameters considered in router configuration.

1. **Interface:** Act as virtual ports that connect the router to different network or device.
2. **Routing Protocols:** Exchange routing information with other routers to dynamically build routing tables.
3. **IP Addressing:** Assigns unique IP addresses to devices on the network for proper identification and communication.
4. **Security:** Protects the router and network from unauthorized access, attacks, and data breaches.

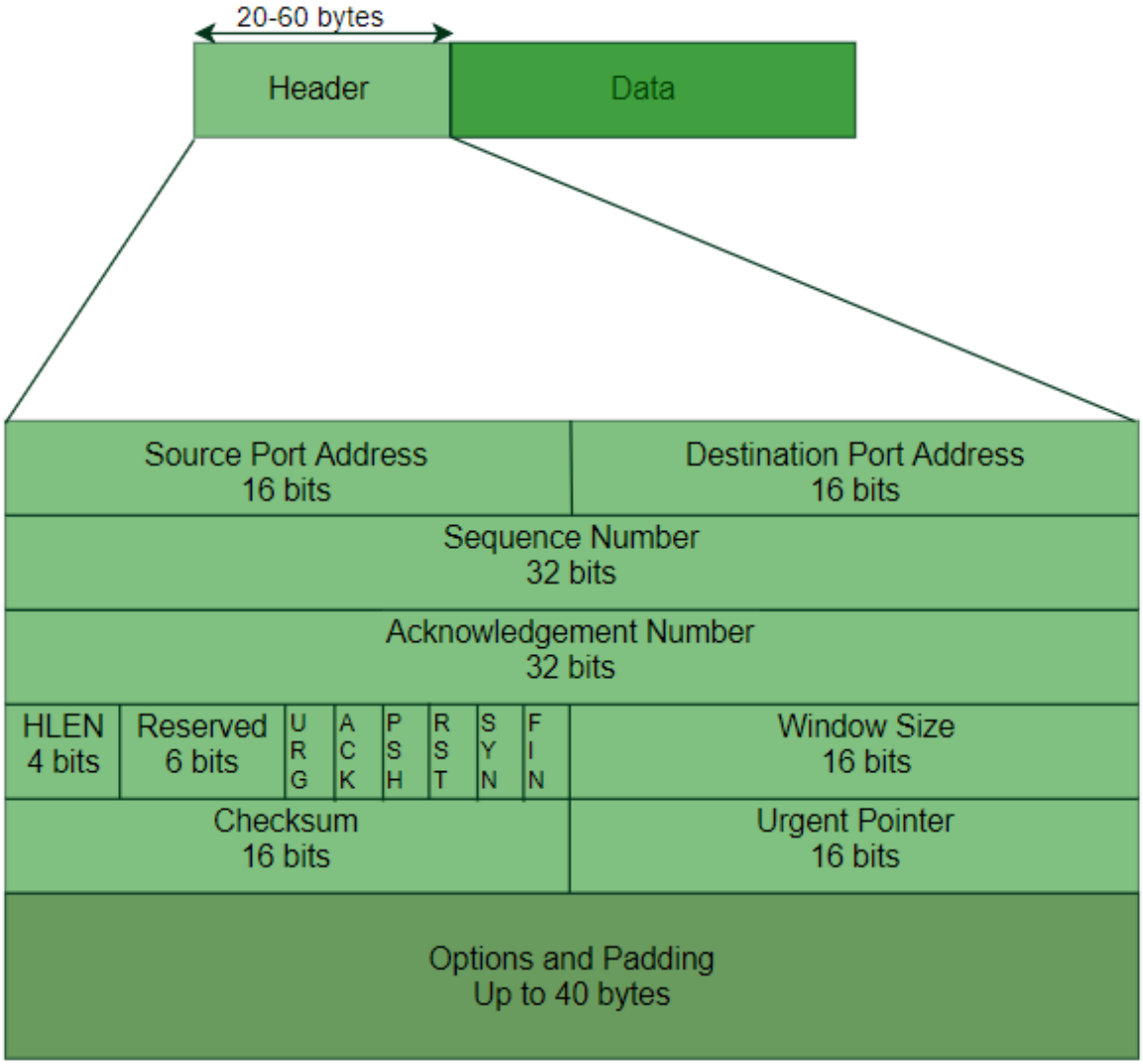
Explain various features of RMON.

RMON stands for Remote Network Monitoring. It is an extension of the Simple Network Management Protocol (SNMP) that allows detailed monitoring of network statistics for Ethernet networks.

Benefits of RMON:

1. Improved network performance
2. Enhanced troubleshooting
3. Centralized monitoring

Draw the format of TCP header and explain various fields.



Source Port Address: A 16-bit field that holds the port address of the application that is sending the data segment.

Destination Port Address: A 16-bit field that holds the port address of the application that is receiving the data segment.

Sequence Number: A 32-bit field that holds the sequence number

Acknowledgement Number: A 32-bit field that holds the acknowledgement number

Header Length (HLEN): A 4-bit field that indicates the length of the TCP header

Control flags:

- URG: Urgent pointer is valid
- ACK: Acknowledgement number is valid
- PSH: Request for push
- RST: Reset the connection
- SYN: Synchronize sequence numbers
- FIN: Finish the connection

Window size: Window size of the sending TCP in bytes.

Checksum: Holds the checksum for error control.

Urgent pointer: Points to data that is urgently required

Explain SNMP. Describe briefly the role of SMI and MIB in SNMP.

SNMP: Exchanges data between network management systems (NMS) and managed devices like routers, switches, and servers.

Components:

- **SNMP manager:** The software application that polls devices for information and sends configuration changes.
- **SNMP agent:** Software running on managed devices that collects and reports data to the manager.
- **MIB (Management Information Base):** A database defining standardized objects that agents can report and managers can manage.
- **SMI (Structure of Management Information):** A set of rules for defining and describing these objects in the MIB.

Explain the role of message transfer agent and user agent in electronic mail.

Role of Message Transfer Agent:

1. Receives emails from user agents or other MTAs.
2. Analyses the recipient address and determines the next server in the delivery route.
3. Forwards the email to the next server until it reaches the recipient's server.
4. If delivery fails, it handles bounces and error messages.

Role of User Agent:

1. Allows you to compose email messages with text, attachments, and formatting.
2. Provides contact management features for storing recipient addresses.
3. Downloads incoming emails from the server and displays them in your inbox.
4. Offers features like filtering, searching, and spam protection.

Explain the features of ATM AAL1 and ATM AAL2.

ATM AAL1: Provides a simple and efficient service for constant bit rate (CBR) traffic, often used for voice and circuit emulation.

Features:

- **Payload size:** Fixed 47 bytes per cell
- **Error detection:** Uses checksum for basic error detection.
- **No segmentation or reassembly:** Suitable for real-time applications.
- **Low overhead:** Simple structure minimizes processing overhead

ATM AAL2: Handles variable bit rate (VBR) traffic with time dependence, making it suitable for video conferencing

Features:

- **Payload size:** Variable, ranging from 0 to 47 bytes per cell
- **Error Detection:** Uses Forward Error Correction mechanisms
- **Segmentation and reassembly:** Breaks down large VBR data into smaller ATM cells and reassembles them at the destination.
- **4-bit time stamp:** Helps preserve data arrival order

Explain the process of authentication in network security.

Authentication is the process of verifying the identity of a user or information. There are different types of authentication systems which are: –

1. **Single-Factor authentication:** In this authentication system, the user has to enter the username and the password
2. **Two-factor Authentication:** In this authentication system, the user has to give a username, password, and other information like OTP
3. **Multi-Factor authentication system:** In this type of authentication, more than one factor of authentication is needed. This gives better security to the user.

Explain the features of secure sockets layer.

1. **Encryption**: The SSL certificate uses encryption algorithms to secure the communication between the website and its users.
2. **Authentication**: The SSL certificate verifies the identity of the website, protecting from impostor.
3. **Integrity**: The SSL certificate uses message authentication codes (MACs) to detect any tampering with the data during transmission.
4. **Non-denial**: The recipient of the data cannot deny having received it.
5. **Public-key cryptography:** SSL certificates use public-key cryptography for secure key exchange between the client and server.

Explain various types of attacks.

Active attacks: An attacker attempts to alter, destroy, or disrupt the normal operation of a system or network. Active attacks involve the attacker taking direct action against the target system or network, and can be more dangerous than passive attacks. e.g. Denial of Service, Modification of messages, etc.

Passive attacks: An attacker attempts to learn or make use of information from the system but does not affect system resources. The goal of the attacker is to obtain information that is being transmitted. An attacker passively collects data without altering or destroying it. e.g. Traffic analysis, release of messages, etc.

Explain briefly packet filter firewall and proxy firewall.

Packet Filter Firewall: It works in the network layer of the OSI Model. It applies a set of rules on each packet and based on the outcome, decides to either forward or discard the packet. It controls access to packets on the basis of packet source and destination address. It considers only the most basic attributes of each packet. It can decide packet flow very quickly.

Proxy Firewall: It provides security by controlling the information going in and out of the network. It's servers filter cache, log, and control requests coming from a client to keep the network secure and free of intruders and viruses. Proxy firewall has its own IP address so that internal network never makes a direct connection with outside internet. Since it monitors information at the application level, it is also known as application firewall.

Explain the features of virtual private network.

1. It ensures security by providing an encrypted tunnel between client and server.
2. It is used to bypass many blocked sites.
3. It facilitates anonymous browsing by hiding your IP address.
5. It helps in Search engine optimization(SEO) by analysing the data
6. It encrypts internet traffic, safeguarding online activities

Explain various components of cryptography.

1. **Algorithms:** Mathematical formulas and procedures that transform data
2. **Keys:** Long strings of bits used to lock and unlock encrypted data
3. **Ciphers:** Practical implementations of cryptographic algorithms
4. **Protocols:** Define how cryptographic algorithms and keys are used in communication systems
5. **Hash Functions:** Create unique fixed-length "fingerprints" of data