- Tcp 6 ta flags details(syn,ack....)
- how dhcp server works with image
- zero trust architecture requirement
- http methods 5ta (get,post,trace,put)
- smtp server use kore yahoo user kivabe gmail user ke kivabe mail pathabe. Explain the steps.
- primary dns, forwarder and secondary dns er functionality
- ip protocol er field gular description
-Http to https convertion with tls protocol: how
-IPsec mode: tunnel mode and transport mode
-Tcp session establishment 3 way handshake with closing mechanism of the session.
-UDP TCP comparison with context with example
-Natting context: destination and source NaT explanation with example
-Eigrp neighbour table discovery, toplogy table, routing table
- DHCP IP renew process, how to extend time, server or client will remind? And how to get the intitial lease of IP as well.

1) Details of TCP 6 Flags:

Source Port(16 bits): It holds the source/transmitting application’s port number and helps in determining the application where the data delivery is planned.

Destination Port (16 bits): This field has the port number of the transmitting application and helps to send the data to the appropriate application.

Sequence Number (32 bits): It ensures that the data is received in proper order by ordered segmenting and reassembling them at the receiving end.

Acknowledgment Number (32 bits): This field contains the upcoming sequence number and it acknowledges the feedback up to that.

Data Offset (4 bits): The data offset field indicates the starting point of the TCP data payload also storing the size of the TCP header.

Control Flags (9 bits): TCP uses a few control flags to regulate communication. Some of the important flags include:

SYN (Synchronize): Responsible for connecting the sender and receiver.

ACK (Acknowledgement): Its purpose is to transfer the acknowledgement of whether the sender has received data.

FIN (Finish): It informs whether the TCP connection is terminated or not.

RST (Reset): Mainly used to reset the connection when an error occurs.

Window Size (16 bits): The size of the sender's receive window is specified by this property.

Checksum (16 bits): It reveals if the header was damaged during transportation.

Urgent Pointer (16 bits): This field points to the packet's first byte of urgent data.

Options (Variable length): This field represents the different TCP options.

Data Payload: This field mainly contains the information which is the actual application data that is being transmitted.

2)Details of IP Protocol headers:

Version (4 bits): This field contains a value in four bits which is 0100 generally. This value is utilized in distinguishing between IPv4 and IPv6, using four bits.

Header Length (4 bits): This value is 4 bits in size and it represents how many 32-bit words are present in the IP header.

Type of Service (TOS) (8 bits): This field mainly deals with the information about how the quality of the service is being delivered. The first 3 bits provides distinction and prioritization of IP packets depending on certain service needs, such as precedence, delay, throughput, dependability, and cost.

Total Length (16 bits): The total length of the IP packet is stored in bytes. This value and the HE-LEN sums up to the value of the Payload.

Identification (16 bits): This field gives a specific IP packet a distinctive identity. This helps to identify the fragments of an IP Datagram Uniquely.

Flags (3 bits): Contains control flags for packet fragmentation and reassembly, such as the "Don't Fragment" and "More Fragments" flags.
Fragment Offset (13 bits): After a packet is fragmented and put back together, this field contains the location of it inside the original packet. It represents the number of Data Bytes ahead of the particular fragment in the specific Datagram.

Time to Live (TTL) (8 bits): This field specifies the total lifetime of the Data packet in the internet system. This field indicates how many hops (routers) an IP packet can make before being terminated. This value goes from 0-255.

Protocol (8 bits): This IPv4 header specifies the type of transport layer protocol, such as TCP, UDP, or ICMP, to which the IP packet will be routed. For example, TCP is indicated by number 6 and UDP protocol is denoted by number 17.

Header Checksum (16 bits): This is an error checking layer which is added to identity errors in the header. By comparing the IP header with its checksum for error detection, it ensures the IP header's integrity.

Source IP Address (32 bits): The IPv4 sender's 32-bit address is represented by this value.

Destination IP Address (32 bits): This value represents the 32-bit IP address of the intended recipient.

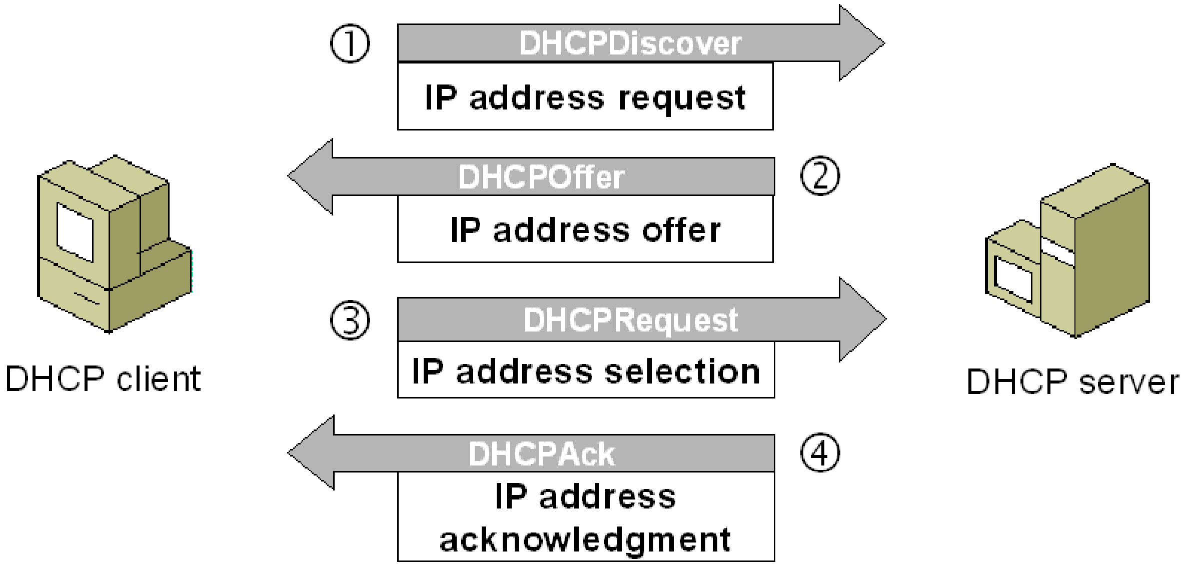
Options (variable length): This field has options and parameters for security, record route, time stamp, etc. You can see that the End of Options, or EOL, usually marks the end of the list of options components.

3) How DHCP works Explained with Examples

When a host (DHCP client) needs an IP configuration, it connects to a DHCP server and requests an IP configuration. A DHCP server contains several pre-configured IP configurations. When it receives a DHCP request from a DHCP client, it provides an IP configuration to the client from all available IP configurations.

This process goes through four steps: Discover, Offer, Request, and Acknowledgment.

The following image shows all four steps of a DHCP communication



DHCP Discovery:

- When a device starts without a valid IP configuration, it sends a DHCP DISCOVER message as a broadcast on the local LAN segment.
- The source address is 0.0.0.0, and the destination address is 255.255.255.255.
- These special addresses allow devices to send broadcast messages.

DHCP Offer:

- DHCP servers on the local network receive the DHCP DISCOVER message and respond with a DHCPOFFER message.

- DHCPOFFER is broadcasted to the local network and includes IP configuration details.
- The client's MAC address in the DHCPDISCOVER helps the host identify if the DHCPOFFER is for it.

- If multiple offers are received, the host accepts only one with a DHCPREQUEST message.

DHCP Request:

- The DHCPREQUEST message indicates the chosen offer to the DHCP server.
- Multiple servers withdraw offers if one is accepted.
- DHCPREQUEST contains a Transaction ID to identify the accepted offer.

DHCP Acknowledgment:

- The DHCP server responds with a DHCPACK message, acknowledging the client's DHCPREQUEST.
- DHCPNACK may be sent if the offer is no longer valid, prompting the client to request again.
- DHCPACK indicates the client can use the offered IP configuration.

4) How TLS convert the HTTP to HTTPS

Handshake Process:

When a client initiates a connection to a server using HTTPS, the TLS handshake process begins.
The client sends a "ClientHello" message, indicating its intention to establish a secure connection.
The server responds with a "ServerHello" message, containing information about the selected cryptographic parameters.

Server Certificate Exchange:

The server sends its digital certificate to the client. This certificate contains the server's public key and information about the certificate issuer.
The client verifies the certificate's authenticity using a chain of trust, ensuring it is signed by a trusted certificate authority (CA).

Key Exchange:

The client generates a pre-master secret and encrypts it with the server's public key (from the received certificate).
The server decrypts the pre-master secret using its private key.

Both the client and server use the pre-master secret to independently generate a shared secret, known as the master secret.

Session Key Derivation:

The master secret is used to derive encryption keys for securing the communication.
These keys are used for symmetric encryption and decryption of data during the session.

Secure Data Transfer:

With the session keys established, the client and server switch to a secure mode of communication.
All data exchanged between the client and server, including HTTP requests and responses, is encrypted using symmetric encryption algorithms.

HTTPS Communication:

At this point, the connection has been secured by TLS, and regular HTTP communication now occurs over this secure connection.
The client and server continue to exchange HTTP requests and responses, but the data is encrypted and secure from eavesdropping or tampering.

Closing the Connection:

When the communication is complete, the TLS connection can be closed gracefully.
The TLS "goodbye" messages are exchanged, ensuring that any remaining data is securely transmitted before the connection is closed.

In summary, TLS adds a layer of security to the HTTP protocol by encrypting the data exchanged between the client and server, creating HTTPS. This encryption helps protect sensitive information, such as login credentials or personal data, from unauthorized access during transmission.

5) Primary DNS, Secondary DNS, and DNS forwarders Functionalities:

Primary DNS, Secondary DNS, and DNS forwarders play crucial roles in the Domain Name System (DNS), which translates human-readable domain names into IP addresses. Here's a brief overview of their functionalities:

Primary DNS Server:

The primary DNS server is the authoritative server for a particular domain.

It stores the original copies of domain records, including information such as IP addresses associated with domain names.
Responsible for handling queries related to the domain for which it is authoritative.
If the primary DNS server is unavailable, secondary DNS servers can take over.

Secondary DNS Server:

The secondary DNS server is a backup to the primary DNS server.
It contains a copy of the zone data (DNS records) of the primary DNS server.
The secondary server serves as a failover mechanism. If the primary server is unavailable, the secondary server can respond to DNS queries.
Helps distribute the DNS query load and improves fault tolerance in case the primary server experiences issues.

DNS Forwarder:

A DNS forwarder is a DNS server that forwards DNS queries to another DNS server, typically an upstream or external DNS server.
Instead of resolving queries directly, a DNS server configured as a forwarder sends the queries to one or more specified DNS servers and returns the results to the original requester.
Forwarders can be used to improve DNS resolution efficiency, reduce latency, and leverage the caching capabilities of larger, external DNS servers.
Commonly used in enterprise networks and internet service providers (ISPs) to optimize DNS resolution.

6)

IPsec (Internet Protocol Security) is a protocol that provides security for IP-based communication. IPsec can operate in two modes: Tunnel Mode and Transport Mode.

Tunnel Mode:

- In Tunnel Mode, the entire original IP packet is encapsulated in a new IP packet. The new packet is then encrypted and sent over the network.
- This mode is used when two entire networks need to be connected over a public network, such as the Internet.
- In Tunnel Mode, the entire IP packet, including the original source and destination addresses, is encrypted, providing end-to-end security.

Transport Mode:

- In Transport Mode, only the payload of the IP packet is encrypted, not the entire packet.
- This mode is used when a single host needs to communicate with another single host over a public network.
- In Transport Mode, only the data being transmitted is encrypted, not the header information such as the source and destination addresses.

When comparing Tunnel Mode and Transport Mode, one key difference is the level of encryption provided. Tunnel Mode provides end-to-end security by encrypting the entire IP packet, while Transport Mode only encrypts the payload of the packet.

Another difference is the use case: Tunnel Mode is used for connecting entire networks, while Transport Mode is used for host-to-host communication.

Ultimately, the choice between Tunnel Mode and Transport Mode depends on the specific requirements of the network and the level of security desired. Both modes have their advantages and disadvantages, and the appropriate mode should be selected based on the specific security and networking needs of the organization.