APPLICATION LAYER

Application Layer in OSI Layers and TCP/IP

- The Application Layer of OSI (Open System Interconnection) model, is the top layer in this model and takes care of network communication. The application layer provides the functionality to send and receive data from users. It acts a"s the interface between the user and the application. The application provides services like file transmission, mail service, and many more.

Working of Application Layer

- At first, client sends a command to server and when server receives that command, it allocates port number to client.
- Thereafter, the client sends an initiation connection request to server and when server receives request, it gives acknowledgement (ACK) to client through client has successfully established a connection with the server.
- Therefore, now client has access to server through which it may either ask server to send any types of files or other documents or it may upload some files or documents on server itself.

HTTP

HTTP stands for Hypertext Transfer Protocol, and it's the system that allows communication between web browsers (like Google Chrome or Firefox) and websites.

Open Web Browser: First, you open your web browser and type a website URL (e.g., www.example.com).

DNS Lookup: Your browser asks a Domain Name System (DNS) server to find out the IP address associated with that URL. Think of this as looking up the phone number of the website.

Send HTTP Request: Once the browser has the website's IP address, it sends an HTTP request to the server. The request asks the server for the resources needed to display the page (like text, images, and videos).

Server Response: The server processes your request and sends back an HTTP response. This response contains the requested resources (like HTML, CSS, JavaScript) needed to load the page.

Rendering the Web Page: Your browser receives the data from the server and displays the webpage on your screen.

Understanding HTTP Request and Response

- HTTP Version: The version of HTTP (like HTTP/1.1 or HTTP/2) being used.
- URL: The specific address of the resource (e.g., https://www.example.com/about).
- HTTP Method: The type of action being requested (e.g., GET to retrieve information or POST to send data).
- HTTP Request Headers: Extra information about the request, like what kind of browser you're using or what kind of content you’re expecting.
- HTTP Request Body: In some cases, the request will include a body that contains data (e.g., when you submit a form).

HTTP/3: The Latest Version

HTTP/3, released in 2022, builds on HTTP/2 but with a key improvement: it uses the QUIC protocol instead of TCP. QUIC is faster and more reliable because it:

Reduces connection setup time.

Handles data loss better, especially in poor network conditions.

Offers better security by integrating encryption directly into the protocol.

TELNET

- TELNET stands for Teletype Network. It is a client/server application protocol that provides access to virtual terminals of remote systems on local area networks or the Internet. The local computer uses a telnet client program and the remote computers use a telnet server program. In this article, we will discuss every point about TELNET. It is used as a standard TCP/IP protocol for virtual terminal service which is provided by ISO. The computer which starts the connection is known as the local computer. The computer which is being connected to i.e. which accepts the connection known as the remote computer. During telnet operation, whatever is being performed on the remote computer will be displayed by the local computer. Telnet operates on a client/server principle.

Dynamic Host Configuration Protocol (DHCP)

- Dynamic Host Configuration Protocol is a network protocol used to automate the process of assigning IP addresses and other network configuration parameters to devices (such as computers, smartphones and printers) on a network.

- Instead of manually configuring each device with an IP address, DHCP allows devices to connect to a network and receive all necessary network information, like IP address, subnet mask, default gateway and DNS server addresses, automatically from a DHCP server.

- DHCP Server: DHCP Server is a server that holds IP Addresses and other information related to configuration.
- DHCP Client: It is a device that receives configuration information from the server. It can be a mobile, laptop, computer or any other electronic device that requires a connection.
- DHCP Relay: DHCP relays basically work as a communication channel between DHCP Client and Server.
- IP Address Pool: It is the pool or container of IP Addresses possessed by the DHCP Server. It has a range of addresses that can be allocated to devices.
- Subnets: Subnets are smaller portions of the IP network partitioned to keep networks under control.
- Lease: It is simply the time that how long the information received from the server is valid, in case of expiration of the lease, the tenant must have to re-assign the lease.

- DNS Servers: DHCP servers can also provide DNS (Domain Name System) server information to DHCP clients, allowing them to resolve domain names to IP addresses.
- Default Gateway: DHCP servers can also provide information about the default gateway, which is the device that packets are sent to when the destination is outside the local network.
- Options: DHCP servers can provide additional configuration options to clients, such as the subnet mask, domain name and time server information.
- Renewal: DHCP clients can request to renew their lease before it expires to ensure that they continue to have a valid IP address and configuration information.
- Failover: DHCP servers can be configured for failover, where two servers work together to provide redundancy and ensure that clients can always obtain an IP address and configuration information, even if one server goes down.
- Dynamic Updates: DHCP servers can also be configured to dynamically update DNS records with the IP address of DHCP clients, allowing for easier management of network resources.
- Audit Logging: DHCP servers can keep audit logs of all DHCP transactions, providing administrators with visibility into which devices are using which IP addresses and when leases are being assigned or renewed.

File Transfer Protocol (FTP)

- FTP is a basic system that helps in transferring files between a client and a server. It is what makes the FTP unique that the system provides a reliable and efficient means of transferring files from one system to another even if they have different file structures and operating systems.

Types of FTP

- Anonymous FTP: Anonymous FTP is enabled on some sites whose files are available for public access. A user can access these files without having any username or password. Instead, the username is set to anonymous, and the password is to the guest by default. Here, user access is very limited. For example, the user can be allowed to copy the files but not to navigate through directories.
- Password Protected FTP: This type of FTP is similar to the previous one, but the change in it is the use of username and password.
- FTP Secure (FTPS): It is also called as FTP Secure Sockets Layer (FTP SSL). It is a more secure version of FTP data transfer. Whenever FTP connection is established, Transport Layer Security (TLS) is enabled.
- FTP over Explicit SSL/TLS (FTPES): FTPES helps by upgrading FTP Connection from port 21 to an encrypted connection.
- Secure FTP (SFTP): SFTP is not a FTP Protocol, but it is a subset of Secure Shell Protocol, as it works on port 22.

How Does FTP Work?

Here are steps mentioned in which FTP works:

- A user has to log in to FTP Server first, there may be some servers where you can access to content without login, known as anonymous FTP.
- Client can start a conversation with server, upon requesting to download a file.
- The user can start different functions like upload, delete, rename, copy files, etc. on server.

DNS(Domain Name System)

- DNS is a hierarchical and distributed naming system that translates domain names into IP addresses.
- User Input: You enter a website address (for example, www.geeksforgeeks.org) into your web browser.
- Local Cache Check: Your browser first checks its local cache to see if it has recently looked up the domain. If it finds the corresponding IP address, it uses that directly without querying external servers.
- DNS Resolver Query: If the IP address isn’t in the local cache, your computer sends a request to a DNS resolver. The resolver is typically provided by your Internet Service Provider (ISP) or your network settings.
- Root DNS Server: The resolver sends the request to a root DNS server. The root server doesn’t know the exact IP address for www.geeksforgeeks.org but knows which Top-Level Domain (TLD) server to query based on the domain’s extension (e.g., .org).

- TLD Server: The TLD server for .org directs the resolver to the authoritative DNS server for geeksforgeeks.org.
- Authoritative DNS Server: This server holds the actual DNS records for geeksforgeeks.org, including the IP address of the website's server. It sends this IP address back to the resolver.
- Final Response: The DNS resolver sends the IP address to your computer, allowing it to connect to the website's server and load the page.

Structure of DNS

- Root DNS Servers: These are the highest-level DNS servers and know where to find the TLD servers. They are crucial for directing DNS queries to the correct locations.
- TLD Servers: These servers manage domain extensions like .com, .org, .net, .edu, .gov and others. They help route queries to the authoritative DNS servers for specific domains.
- Authoritative DNS Servers: These are the servers that store the actual DNS records for domain names. They are responsible for providing the correct IP addresses that allow users to reach websites.

Types of DNS Queries

- Recursive Query: In this query, if the resolver is unable to find the record, in that case, DNS client wants the DNS Server will respond to the client in any way like with the requested source record or an error message.
- Iterative Query: Iterative Query is the query in which DNS Client wants the best answer possible from the DNS Server.
- Non-Recursive Query: Non-Recursive Query is the query that occurs when a DNS Resolver queries a DNS Server for some record that has access to it because of the record that exists in its cache.

DNS Lookup

- DNS Lookup, also called DNS Resolution, is the process of translating a human-readable domain name (like www.example.com) into its corresponding IP address (like 192.0.2.1), which computers use to locate and communicate with each other on the internet. It allows users to access websites easily using names instead of remembering numeric IP addresses.

- DNS Lookup starts when a user types a domain name into their browser.
- The query goes through a series of servers: the DNS resolver, Root server, TLD server and authoritative server.
- Each server plays a role in finding the correct IP address for the domain.
- Once the IP address is found, the browser connects to the website’s server and loads the page.

Simple Mail Transfer Protocol (SMTP)

- Simple Mail Transfer Protocol (SMTP) is an application layer protocol used for exchanging email messages between servers. It is essential in the email communication process and operates at the application layer of the TCP/IP stack.
- To send an email, the client opens a TCP connection to the SMTP server. The server, which is always listening on port 25, initiates the connection as soon as it detects a client. Once the TCP connection is established, the client sends the email across the connection.

Types of SMTP Protocol

- End-to-end delivery is used between organizations. In this method, the email is sent directly from the sender's SMTP client to the recipient's SMTP server without passing through intermediate servers.
- Store-and-forward is used within organizations that have TCP/IP and SMTP-based networks. In this method, the email may pass through several intermediate servers (Message Transfer Agents, or MTAs) before reaching the recipient.

Components of SMTP

- Mail User Agent (MUA): It is a computer application that helps you in sending and retrieving mail. It is responsible for creating email messages for transfer to the mail transfer agent(MTA).
- Mail Submission Agent (MSA): It is a computer program that receives mail from a Mail User Agent(MUA) and interacts with the Mail Transfer Agent(MTA) for the transfer of the mail.
- Mail Transfer Agent (MTA): It is software that has the work to transfer mail from one system to another with the help of SMTP.
- Mail Delivery Agent (MDA): A mail Delivery agent or Local Delivery Agent is basically a system that helps in the delivery of mail to the local system.

How does SMTP Work?

1. Sending Email:

- When a user wants to send an email, they use a User Agent (UA), like Outlook or Gmail.
- The email is handed over to the MTA, which is responsible for transferring the email to the recipient's mail server.

2. SMTP Client and Server:

Sender-SMTP (Client): The email sender's MTA initiates the connection to the recipient's MTA (Receiver-SMTP).

- Receiver-SMTP (Server): The receiving MTA listens for incoming connections and receives the email from the sender-SMTP.
- This communication happens over TCP port 25.

3. Relays and Gateways:

Relays: In some cases, the email may pass through several intermediate MTAs before reaching the destination server. These MTAs act as relays.

Gateways: If the sending and receiving systems use different email protocols (e.g., SMTP and non-SMTP), an email gateway can convert the email to the appropriate format for delivery.

4. Email Delivery:

The sender’s MTA sends the email to the receiver’s MTA, either directly or through relays.

The MTA uses the SMTP protocol to transfer the message. Once it’s delivered to the destination MTA, the email is placed in the recipient’s mailbox.

The recipient’s User Agent (UA) can then download the email.

POP3

- POP 3 stands for Post Office Protocol Version 3. POP3 protocol is used to provide access to the mail inbox that is stored in the email server. POP3 protocol can download and delete messages. Once the POP3 client has established a connection with the mail server it can easily retrieve all the messages from the server. The user can access the messages locally even if the user is offline.

Working of POP3

- Initially POP3 needs to establish a connection between the POP client and the POP server.
- Once a secure connection is established several commands are exchanged between them to perform the task.
- Once a connection is established client requests available email messages.
- The Server sends the available messages along with their size and unique identifier number.
- Once the client receives the message, it makes a request to the server for downloading the messages. The user marks such messages and sends them to the server.
- Upon receiving from the client-server sends the messages selected by the client and accordingly marks them as read or unread.
- The client if want sends a request for deleting the messages.
- Once the tasks are completed the client sends a close connection request to the server
- The server then sends an acknowledgment to the client and closes the connection.

Internet Message Access Protocol (IMAP)

- Internet Message Access Protocol (IMAP) is an application layer protocol that operates as a contract for receiving emails from the mail server. It was designed by Mark Crispin in 1986 as a remote access mailbox protocol, the current version of IMAP is IMAP4.

- It is used as the most commonly used protocol for retrieving emails. This term is also known as Internet mail access protocol, Interactive mail access protocol, and Interim mail access protocol.

Working of IMAP

The following steps are taken for the working of the IMAP :

- Email client Gmail establishes a connection with Gmail's SMTP server.
- By approving the sender's and recipient's email addresses, the SMTP server verifies (authenticates) that the email can be sent.
- The email is sent to the Outlook SMTP server by Gmail's SMTP server.
- The recipient's email address is authenticated by the Outlook SMTP server.
- IMAP or POP3 is used by the Outlook SMTP server to deliver the email to the Outlook email client.