Application Layer

HTTP

HTTP stands for HyperText Transfer Protocol. Tim Berner invents it. HyperText is the type of text that is specially coded with the help of some standard coding language called HyperText Markup Language (HTML). HTTP/2 is the new version of HTTP. HTTP/3 is the latest version of HTTP, which is published in 2022.

The protocol used to transfer hypertext between two computers is known as HyperText Transfer Protocol.

HTTP provides a standard between a web browser and a web server to establish communication. It is a set of rules for transferring data from one computer to another. Data such as text, images, and other multimedia files are shared on the World Wide Web. Whenever a web user opens their web browser, the user indirectly uses HTTP. It is an application protocol that is used for distributed, collaborative, hypermedia information systems.

Working of HTTP

First of all, whenever we want to open any website then first open a web browser after that we will type the URL of that website (e.g., www.facebook.com). This URL is now sent to the Domain Name Server (DNS). Then DNS first check records for this URL in their database, then DNS will return the IP address to the web browser corresponding to this URL. Now the browser is able to send requests to the actual server.

After the server sends data to the client, the connection will be closed. If we want something else from the server we should have to re-establish the connection between the client and the server.

Characteristics of HTTP

HTTP is IP based communication protocol that is used to deliver data from server to client or vice-versa.

- The server processes a request, which is raised by the client, and also server and client know each other only during the current bid and response period.
- Any type of content can be exchanged as long as the server and client are compatible with it.

- *Once data is exchanged, servers and clients are no longer connected.*
- *It is a request and response protocol based on client and server requirements.*
- *It is a connection-less protocol because after the connection is closed, the server does not remember anything about the client and the client does not remember anything about the server.*
- *It is a stateless protocol because both client and server do not expect anything from each other but they are still able to communicate.*

Advantages of HTTP

- *Memory usage and CPU usage are low because of fewer simultaneous connections.*
- *Since there are few TCP connections hence network congestion is less.*
- *Since handshaking is done at the initial connection stage, then latency is reduced because there is no further need for handshaking for subsequent requests.*
- *The error can be reported without closing the connection.*
- *HTTP allows HTTP pipe-lining of requests or responses.*

Disadvantages of HTTP

- *HTTP requires high power to establish communication and transfer data.*
- *HTTP is less secure because it does not use any encryption method like HTTPS and use TLS to encrypt regular HTTP requests and response.*
- *HTTP is not optimized for cellular phones and it is too gabby.*
- *HTTP does not offer a genuine exchange of data because it is less secure.*
- *The client does not close the connection until it receives complete data from the server; hence, the server needs to wait for data completion and cannot be available for other clients during this time.*

FTP

File transfer protocol (FTP) is an Internet tool provided by TCP/IP. The first feature of FTP is developed by Abhay Bhushan in 1971. It helps to transfer files from one computer to another by providing access to directories or folders on remote computers and allows software, data, text file to be transferred between different kinds of computers. The end-user in the connection is known as localhost and the server which provides data is known as the remote host.

The goals of FTP are:

- It encourages the direct use of remote computers.
- It shields users from system variations (operating system, directory structures, file structures, etc.)
- It promotes sharing of files and other types of data.

Why FTP?

FTP is a standard communication protocol. There are various other protocols like HTTP which are used to transfer files between computers, but they lack clarity and focus as compared to FTP. Moreover, the systems involved in connection are heterogeneous systems, i.e. they differ in operating systems, directory, structures, character sets, etc the FTP shields the user from these differences and transfer data efficiently and reliably. FTP can transfer ASCII, EBCDIC, or image files. The ASCII is the default file share format, in this, each character is encoded by NVT ASCII. In ASCII or EBCDIC the destination must be ready to accept files in this mode. The image file format is the default format for transforming binary files.

Applications of FTP

The following are the applications of FTP:

- FTP connection is used by different big business organizations for transferring files in between them, like sharing files to other employees working at different locations or different branches of the organization.
- FTP connection is used by IT companies to provide backup files at disaster recovery sites.
- Financial services use FTP connections to securely transfer financial documents to the respective company, organization, or government.

- *Employees use FTP connections to share any data with their co-workers.*

Advantages

1. ***Multiple transfers:*** *FTP helps to transfer multiple large files in between the systems.*
2. ***Efficiency:*** *FTP helps to organize files in an efficient manner and transfer them efficiently over the network.*
3. ***Security:*** *FTP provides access to any user only through user ID and password. Moreover, the server can create multiple levels of access.*
4. ***Continuous transfer:*** *If the transfer of the file is interrupted by any means, then the user can resume the file transfer whenever the connection is established.*
5. ***Simple:*** *FTP is very simple to implement and use, thus it is a widely used connection.*
6. ***Speed:*** *It is the fastest way to transfer files from one computer to another.*

Disadvantages

1. ***Less security:*** *FTP does not provide an encryption facility when transferring files. Moreover, the username and passwords are in plain text and not a combination of symbols, digits, and alphabets, which makes it easier to be attacked by hackers.*
2. ***Old technology:*** *FTP is one of the oldest protocols and thus it uses multiple TCP/IP connections to transfer files. These connections are hindered by firewalls.*
3. ***Virus:*** *The FTP connection is difficult to be scanned for viruses, which again increases the risk of vulnerability.*
4. ***Limited:*** *The FTP provides very limited user permission and mobile device access.*
5. ***Memory and programming:*** *FTP requires more memory and programming efforts, as it is very difficult to find errors without the commands.*

SMTP

Email is emerging as one of the most valuable services on the internet today. Most internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) is used to retrieve those emails at the receiver's side.

Components of SMTP

Mail User Agent (MUA)

Mail Submission Agent (MSA)

Mail Transfer Agent (MTA)

Mail Delivery Agent (MDA)

1. **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).
2. **Mail Submission Agent (MSA):** It is a computer program that basically receives mail from a Mail User Agent(MUA) and interacts with the Mail Transfer Agent(MTA) for the transfer of the mail.
3. **Mail Transfer Agent(MTA):** It is basically software that has the work to transfer mail from one system to another with the help of SMTP.
4. **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.

Advantages of SMTP

- If necessary, the users can have a dedicated server.
- It allows for bulk mailing.
- Low cost and wide coverage area.
- Offer choices for email tracking.
- Reliable and prompt email delivery.

Disadvantages of SMTP

- SMTP's common port can be blocked by several firewalls.
- SMTP security is a bigger problem.
- Its simplicity restricts how useful it can be.
- Just 7-bit ASCII characters can be used.

- *If a message is longer than a certain length, SMTP servers may reject the entire message.*
- *Delivering your message will typically involve additional back-and-forth processing between servers, which will delay sending and raise the likelihood that it won't be sent.*

MIME

Why do we need MIME?

Limitations of Simple Mail Transfer Protocol (SMTP):

SMTP has a very simple structure

Its simplicity however comes with a price as it only sends messages in NVT 7-bit ASCII format.

It cannot be used for languages that do not support 7-bit ASCII format such as French, German, Russian, Chinese and Japanese, etc. so it cannot be transmitted using SMTP. So, in order to make SMTP more broad, we use MIME.

It cannot be used to send binary files or video or audio data.

Purpose and Functionality of MIME –

Growing demand for Email Messages as people also want to express themselves in terms of Multimedia. So, MIME another email application is introduced as it is not restricted to textual data.

MIME transforms non-ASCII data at the sender side to NVT 7-bit data and delivers it to the client SMTP. The message on the receiver side is transferred back to the original data. As well as we can send video and audio data using MIME as it transfers them also in 7-bit ASCII data.

Features of MIME –

- It is able to send multiple attachments with a single message.
- Unlimited message length.
- Binary attachments (executables, images, audio, or video files) may be divided if needed.
- MIME provided support for varying content types and multi-part messages.

Working of MIME –

Suppose a user wants to send an email through a user agent and it is in a non-ASCII format so there is a MIME protocol that converts it into 7-bit NVT ASCII format. The message is transferred through the e-mail system to the other side in the 7-bit format now MIME protocol again converts it back into non-ASCII code and now the user agent of the receiver side reads it and then information is finally read by the receiver. MIME header is basically inserted at the beginning of any e-mail transfer.

Advantages of MIME:

- It has the ability to transfer text, audio, and video files, among other sorts of data, in a message.
- Additionally, it allows for the sending and receiving of emails in a variety of languages, including Hindi, French, Japanese, Chinese, and others.
- Additionally, it gives users the option to connect HTML and CSS to email, enabling them to customise and beautify email according to their preferences.
- Regardless of how long an email is, it can convey the information inside.
- It gives each email a special ID.

Disadvantages:

- The receiving system's interpretation of MIME media types may not always be accurate, which might cause issues with how the content is handled or displayed.
- Because they call for additional headers to be provided along with the information, MIME media types can increase the overhead associated with content transmission. This might lead to larger transferred data files and slower transfer rates.
- Consumers frequently lack a solid understanding of MIME media types, and the use of several media types can make it even more challenging for consumers to comprehend the content being transferred.
- Some systems might not always support MIME media types, which might cause issues with the transmission of specific kinds of content.

TCP

TCP (Transmission Control Protocol) is one of the main protocols of the Internet protocol suite. It lies between the Application and Network Layers which are used in providing reliable delivery services. It is a connection-oriented protocol for communications that helps in the exchange of messages between different devices over a network. The Internet Protocol (IP), which establishes the technique for sending data packets between computers, works with TCP.

Features of TCP/IP

Some of the most prominent features of Transmission control protocol are

1. Segment Numbering System
   - TCP keeps track of the segments being transmitted or received by assigning numbers to each and every single one of them.
   - A specific *Byte Number* is assigned to data bytes that are to be transferred while segments are assigned *sequence numbers*.
   - *Acknowledgment Numbers* are assigned to received segments.
2. Connection Oriented
   - It means sender and receiver are connected to each other till the completion of the process.
   - The order of the data is maintained i.e. order remains same before and after transmission.
3. Full Duplex
   - In TCP data can be transmitted from receiver to the sender or vice – versa at the same time.
   - It increases efficiency of data flow between sender and receiver.
4. Flow Control
   - Flow control limits the rate at which a sender transfers data. This is done to ensure reliable delivery.
   - The receiver continually hints to the sender on how much data can be received (using a sliding window)
5. Error Control
   - TCP implements an error control mechanism for reliable data transfer
   - Error control is byte-oriented

    - Segments are checked for error detection
    - Error Control includes – *Corrupted Segment & Lost Segment Management, Out-of-order segments, Duplicate segments, etc.*

6. Congestion Control
    - TCP takes into account the level of congestion in the network
    - Congestion level is determined by the amount of data sent by a sender

Advantages

- It is a reliable protocol.
- It provides an error-checking mechanism as well as one for recovery.
- It gives flow control.
- It makes sure that the data reaches the proper destination in the exact order that it was sent.
- Open Protocol, not owned by any organization or individual.
- It assigns an IP address to each computer on the network and a domain name to each site thus making each device site to be distinguishable over the network.

Disadvantages

- TCP is made for Wide Area Networks, thus its size can become an issue for small networks with low resources.
- TCP runs several layers so it can slow down the speed of the network.
- It is not generic in nature. Meaning, it cannot represent any protocol stack other than the TCP/IP suite. E.g., it cannot work with a Bluetooth connection.
- No modifications since their development around 30 years ago.

UDP

User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as UDP/IP suite. Unlike TCP, it is an **unreliable and connectionless protocol.** So, there is no need to establish a connection prior to data transfer. The UDP helps to establish low-latency and loss-tolerating connections establish over the network.The UDP enables process to process communication.

Though Transmission Control Protocol (TCP) is the dominant transport layer protocol used with most of the Internet services; provides assured delivery, reliability, and much more but all these services cost us additional overhead and latency. Here, UDP comes into the picture. For real-time services like computer gaming, voice or video communication, live conferences; we need UDP. Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets. There is no error checking in UDP, so it also saves bandwidth.

User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

Applications of UDP:

- Used for simple request-response communication when the size of data is less and hence there is lesser concern about flow and error control.
- It is a suitable protocol for multicasting as UDP supports packet switching.
- UDP is used for some routing update protocols like RIP(Routing Information Protocol).
- Normally used for real-time applications which can not tolerate uneven delays between sections of a received message.
- UDP is widely used in online gaming, where low latency and high-speed communication is essential for a good gaming experience. Game servers often send small, frequent packets of data to clients, and UDP is well suited for this type of communication as it is fast and lightweight.
- Streaming media applications, such as IPTV, online radio, and video conferencing, use UDP to transmit real-time audio and video data. The loss of some packets can be tolerated in these applications, as the data is continuously flowing and does not require retransmission.

- VoIP (Voice over Internet Protocol) services, such as Skype and WhatsApp, use UDP for real-time voice communication. The delay in voice communication can be noticeable if packets are delayed due to congestion control, so UDP is used to ensure fast and efficient data transmission.
- DNS (Domain Name System) also uses UDP for its query/response messages. DNS queries are typically small and require a quick response time, making UDP a suitable protocol for this application.
- DHCP (Dynamic Host Configuration Protocol) uses UDP to dynamically assign IP addresses to devices on a network. DHCP messages are typically small, and the delay caused by packet loss or retransmission is generally not critical for this application.

Following implementations uses UDP as a transport layer protocol:

- NTP (Network Time Protocol)
- DNS (Domain Name Service)
- BOOTP, DHCP.
- NNP (Network News Protocol)
- Quote of the day protocol
- TFTP, RTSP, RIP.

The application layer can do some of the tasks through UDP-

- Trace Route
- Record Route
- Timestamp

UDP takes a datagram from Network Layer, attaches its header, and sends it to the user. So, it works fast.

Advantages of UDP:

1. Speed: UDP is faster than TCP because it does not have the overhead of establishing a connection and ensuring reliable data delivery.
2. Lower latency: Since there is no connection establishment, there is lower latency and faster response time.
3. Simplicity: UDP has a simpler protocol design than TCP, making it easier to implement and manage.
4. Broadcast support: UDP supports broadcasting to multiple recipients, making it useful for applications such as video streaming and online gaming.

5. Smaller packet size: UDP uses smaller packet sizes than TCP, which can reduce network congestion and improve overall network performance.

Disadvantages of UDP:

1. No reliability: UDP does not guarantee delivery of packets or order of delivery, which can lead to missing or duplicate data.
2. No congestion control: UDP does not have congestion control, which means that it can send packets at a rate that can cause network congestion.
3. No flow control: UDP does not have flow control, which means that it can overwhelm the receiver with packets that it cannot handle.
4. Vulnerable to attacks: UDP is vulnerable to denial-of-service attacks, where an attacker can flood a network with UDP packets, overwhelming the network and causing it to crash.
5. Limited use cases: UDP is not suitable for applications that require reliable data delivery, such as email or file transfers, and is better suited for applications that can tolerate some data loss, such as video streaming or online gaming.

ICMP

The ICMP stands for Internet Control Message Protocol. It is a network layer protocol. It is used for error handling in the network layer, and it is primarily used on network devices such as routers. As different types of errors can exist in the network layer, so ICMP can be used to report these errors and to debug those errors.

For example, some sender wants to send the message to some destination, but the router couldn't send the message to the destination. In this case, the router sends the message to the sender that I could not send the message to that destination.

The IP protocol does not have any error-reporting or error-correcting mechanism, so it uses a message to convey the information. For example, if someone sends the message to the destination, the message is somehow stolen between the sender and the destination. If no one reports the error, then the sender might think that the message has reached the destination. If someone in-between reports the error, then the sender will resend the message very quickly.

IGMP

IGMP is acronym for **Internet Group Management Protocol**. IGMP is a communication protocol used by hosts and adjacent routers for multicasting communication with IP networks and uses the resources efficiently to transmit the message/data packets. Multicast communication can have single or multiple senders and receivers and thus, IGMP can be used in streaming videos, gaming or web conferencing tools. This protocol is used on IPv4 networks and for using this on IPv6, multicasting is managed by Multicast Listener Discovery (MLD). Like other network protocols, IGMP is used on network layer. MLDv1 is almost same in functioning as IGMPv2 and MLDv2 is almost similar to IGMPv3. The communication protocol, IGMPv1 was developed in 1989 at Stanford University. IGMPv1 was updated to IGMPv2 in year 1997 and again updated to IGMPv3 in year 2002.

The IGMP protocol is used by the hosts and router to identify the hosts in a LAN that are the members of a group. IGMP is a part of the IP layer and IGMP has a fixed- size message. The IGMP message is encapsulated within an IP datagram.

The IP protocol supports two types of communication:

Unicasting- It is a communication between one sender and one receiver. Therefore, we can say that it is one-to-one communication.

Multicasting: Sometimes the sender wants to send the same message to a large of receivers simultaneously. This process is known as multicasting which has one-to-many communication.

Applications:

- **Streaming –** Multicast routing protocol are used for audio and video streaming over the network i.e., either one-to-many or many-to-many.
- **Gaming –** Internet group management protocol is often used in simulation games which has multiple users over the network such as online games.
- **Web Conferencing tools –** Video conferencing is a new method to meet people from your own convenience and IGMP connects to the users for conferencing and transfers the message/data packets efficiently.

Advantages:

- IGMP communication protocol efficiently transmits the multicast data to the receivers and so, no junk packets are transmitted to the host which shows optimized performance.
- Bandwidth is consumed totally as all the shared links are connected.
- Hosts can leave a multicast group and join another.

Disadvantages:

- It does not provide good efficiency in filtering and security.
- Due to lack of TCP, network congestion can occur.
- IGMP is vulnerable to some attacks such as DOS attack (Denial-Of-Service).

WWW

WWW (World Wide Web)

Definition:

The World Wide Web, commonly known as the WWW or the Web, is a global system of interconnected hypertext documents and multimedia content. It operates over the Internet and allows users to access and navigate through a vast array of resources, including text, images, videos, and applications.

Components:

1. **1.Web Pages**: Documents containing information, often written in HTML, which is accessible through web browsers.
2. **Hyperlinks**: Text or elements within a web page that, when clicked, direct users to another web page or resource.
3. **Web Browsers**: Software applications that allow users to access and interact with web pages. Examples include Chrome, Firefox, Safari, and Edge.
4. **Web Servers**: Computers or systems that store and deliver web content in response to user requests.
5. **URL (Uniform Resource Locator):** A web address that specifies the location of a resource on the internet, enabling its retrieval.

Advantages:

1. **Global Accessibility**: The WWW provides universal access to information, connecting people worldwide.
2. **Rich Multimedia Content:** Users can access a wide range of content, including text, images, videos, and interactive applications.
3. **Hyperlink Navigation**: Hyperlinks facilitate seamless navigation between web pages, creating a interconnected web of information.
4. **Communication and Collaboration:** The Web supports communication through email, social media, and collaborative platforms, fostering global connectivity.

Disadvantages:

1. **Information Overload:** The abundance of information can lead to challenges in finding relevant content, resulting in information overload.
2. **Security Concerns:** The openness of the Web can lead to security issues, such as privacy breaches, hacking, and phishing attacks.
3. **Digital Divide:** Disparities in internet access and technological resources create a digital divide, limiting access for certain populations.