UNIT 4

#) Process to Process Delivery :

A transport-layer protocol's first task is to perform process-to-process delivery.
The data link layer is responsible for delivery of frames between two neighbouring nodes over a link. This is called node-to-node delivery. The network layer is responsible for delivery of datagrams between two hosts. This is called host-to-host delivery. Real communication takes place between two processes (application programs). We need process-to-process delivery. The transport layer is responsible for process-to-process delivery-the delivery of a packet, part of a message, from one process to another. Figure 4.1 shows these three types of deliveries and their domains

1. Client/Server Paradigm

Although there are several ways to achieve process-to-process communication, the most common one is through the client/server paradigm. A process on the local host, called a client, needs services from a process usually on the remote host, called a server. Both processes (client and server) have the same name.

2. Addressing

Whenever we need to deliver something to one specific destination among many, we need an address. At the data link layer, we need a MAC address to choose one node among several nodes if the connection is not point-to-point. A frame in the data link layer needs a Destination MAC address for delivery and a source address for the next node's reply.

3. lANA Ranges

The lANA (Internet Assigned Number Authority) has divided the port numbers into three ranges: well known, registered, and dynamic (or private)

4. Socket Addresses

Process-to-process delivery needs two identifiers, IP address and the port number, at each end to make a connection. The combination of an IP address and a port number is called a socket address. The client socket address defines the client process uniquely just as the server socket address defines the server process uniquely

5. Multiplexing: At the sender site, multiple processes can occur, and those processes are required to send packets. It is a technique that combines multiple processes into one process.

Demultiplexing: At the receiver site, it is a technique that separates many processes.

#) UDP (User Data Program)

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.

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.

UDP Header –

UDP header is an **8-bytes** fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. The first 8 Bytes contains all necessary header information and the remaining part consist of data. UDP port number fields are each 16 bits long, therefore the range for port numbers is defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or processes.

a. **Source Port:** Source Port is a 2 Byte long field used to identify the port number of the source.
b. **Destination Port:** It is a 2 Byte long field, used to identify the port of the destined packet.
c. **Length:** Length is the length of UDP including the header and the data. It is a 16-bits field.
d. **Checksum:** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, the pseudo-header of information from the IP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

Applications of UDP:

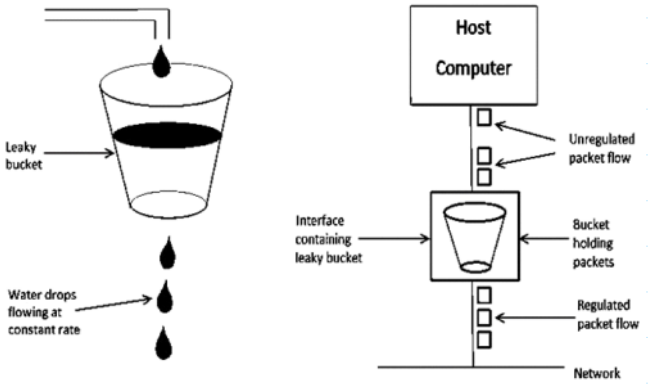
- Used for simple request-response communication when the size of data is less and hence there is lesser concern about flow and error control.
- It is a suitable protocol for multicasting as UDP supports packet switching.
- UDP is used for some routing update protocols like RIP(Routing Information Protocol).
- Normally used for real-time applications which cannot tolerate uneven delays between sections of a received message.

#) UDP v/s TCP

Basis	Transmission control protocol (TCP)	User datagram protocol (UDP)
Type of Service	TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast types of network transmission.
Reliability	TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
Error checking mechanism	TCP provides extensive error-checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Acknowledgment	An acknowledgment segment is present.	No acknowledgment segment.
Sequence	Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in order at the receiver.	There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer.
Speed	TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.
Retransmission	Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in the User Datagram Protocol (UDP).
Header Length	TCP has a (20-60) bytes variable length header.	UDP has an 8 bytes fixed-length header.
Weight	TCP is heavy-weight.	UDP is lightweight.
Handshaking Techniques	Uses handshakes such as SYN, ACK, SYN-ACK	It's a connectionless protocol i.e. No handshake
Broadcasting	TCP doesn't support Broadcasting.	UDP supports Broadcasting.
Protocols	TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet.	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.
Stream Type	The TCP connection is a byte stream.	UDP connection is message stream.
Overhead	Low but higher than UDP.	Very low.

#) **Leaky Bucket Algorithm**

A leaky bucket algorithm is primarily used to control the rate at which traffic enters the network. It provides a mechanism for smoothing bursty input traffic in a flow to present a steady stream into the network. In other words, the leaky bucket enforces a constant transmit rate regardless of the erratic burstiness in the input traffic of a flow.. This basic concept is applied in the case of the Leaky Bucket Algorithm which is nothing but a single server queueing system with constant service time.



1. An interface containing a leaky bucket is connect each host to the network that is a finite internal queue.
2. When space is available in a queue, a packet will send from an application in store.
3. When the queue is full and a new packet will send from an application is discarded.
4. The host operating system builds or simulate this arrangement in the hardware.
5. The packets are queuing and releasing at regular intervals with the regular amount and that reduces the chances of congestion.

The following is an algorithm for variable-length packets:

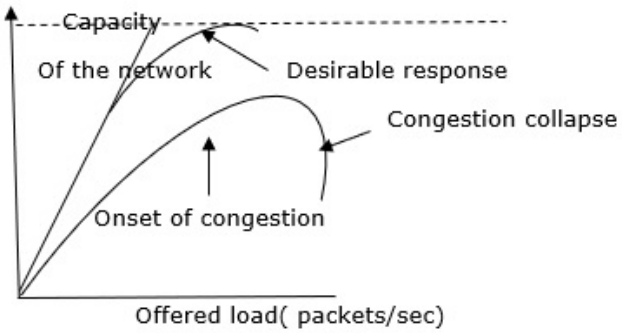
a. Initialize a counter to n at the tick of the clock.
b. If n is greater than the size of the packet, send the packet and decrement the counter by the packet size. Repeat this step until n is smaller than the packet size.
c. Reset the counter and go to step 1.

#) **Token Bucket Algorithm :**

Token bucket algorithm is one of the techniques for congestion control algorithms. When too many packets are present in the network it causes packet delay and loss of packet which degrades the performance of the system. This situation is called congestion.

The network layer and transport layer share the responsibility for handling congestions. One of the most effective ways to control congestion is trying to reduce the load that transport layer is placing on the network. To maintain this network and transport layers have to work together.

The Token Bucket Algorithm is diagrammatically represented as follows –



With too much traffic, performance drops sharply.

Token Bucket Algorithm

The leaky bucket algorithm enforces output patterns at the average rate, no matter how busy the traffic is. So, to deal with the more traffic, we need a flexible algorithm so that the data is not lost. One such approach is the token bucket algorithm.

The token bucket algorithm is an algorithm used in **packet-switched** computer networks to ensure that data transmission in the form of packets does not cross its bandwidth.

To understand the algorithm, we can assume a bucket that is getting filled with tokens. The bucket is of limited size, and the tokens represent packets of predetermined size.

Whenever a packet wants to enter the bucket, the bucket checks its size and compares it with the defined limit of the bucket, if it does not go above the limit, it is allowed or else it is dropped.

Let us understand this algorithm step wise as given below –

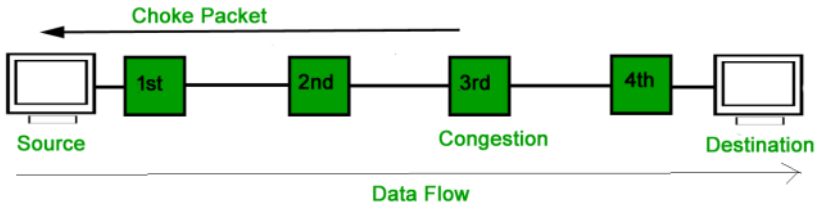
- **Step 1** – In regular intervals tokens are thrown into the bucket f.
- **Step 2** – The bucket has a maximum capacity f.
- **Step 3** – If the packet is ready, then a token is removed from the bucket, and the packet is sent.
- **Step 4** – Suppose, if there is no token in the bucket, the packet cannot be sent.

#) **Choke Packets :**

A choke packet is used in network maintenance and quality management to inform a specific node or transmitter that its transmitted traffic is creating congestion over the network. This forces the node or transmitter to reduce its output rate.

Choke packets are used for congestion and flow control over a network. The source node is addressed directly by the router, forcing it to decrease its sending rate .The source node acknowledges this by reducing the sending rate by some percentage.

Choke packet technique is applicable to both virtual networks as well as datagram subnets. A choke packet is a packet sent by a node to the source to inform it of congestion. Each router monitors its resources and the utilization at each of its output lines. 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 has travelled are not warned about congestion.



#) **Quality-of-Service (QoS) :**

Quality-of-Service (QoS) refers to traffic control mechanisms that seek to either differentiate performance based on application or network-operator requirements or provide predictable or guaranteed performance to applications, sessions, or traffic aggregates. Basic phenomenon for QoS means in terms of packet delay and losses of various kinds.

Quality of Service (QOS) determines a network's capability to support predictable service over various technologies, containing frame relay, Asynchronous Transfer Mode (ATM), Ethernet, SONET IP-routed networks. The networks can use any or all of these frameworks.
The QOS also provides that while supporting priority for one or more flows does not create other flows fail. A flow can be a combination of source and destination addresses, source and destination socket numbers, session identifier, or packet from a specific application or an incoming interface.
The QOS is primarily used to control resources like bandwidth, equipment, wide-area facilities etc. It can get more efficient use of network resources, provide tailored services, provide coexistence of mission-critical applications, etc

Need for QoS –

- Video and audio conferencing require bounded delay and loss rate.
- Video and audio streaming requires bounded packet loss rate, it may not be so sensitive to delay.
- Time-critical applications (real-time control) in which bounded delay is considered to be an important factor.
- Valuable applications should be provided better services than less valuable applications.

#) **QOS Flow Characteristics**

- **Packet loss:** it happens when the network links become congested and the routers and switches start dropping the packets. When these packets are dropped during real-time communication, such as audio or video, these sessions can experience jitter and gaps in speech.
- **Jitter:** occurs as the result of network congestion, timing drift, and route changes. And also, too much jitter can degrade the quality of audio communication.
- **Latency:** is the time delay, which is taken by a packet to travel from its source to its destination. For a great system, latency should be as low as possible, ideally, it should be close to zero.
- **Bandwidth:** is the capacity of a network channel to transmit maximum possible data through the channel in a certain amount of time. QoS optimizes a network by managing its bandwidth and setting the priorities for those applications which require more resources as compared to other applications.
- **Mean opinion score:** it is a metric for rating the audio quality which uses a five-point scale, with a five indicating the highest or best quality.

#) **Techniques for achieving good Quality of Service :**

a. **Overprovisioning –**
The logic of overprovisioning is to provide greater router capacity, buffer space and bandwidth. It is an

expensive technique as the resources are costly. Eg: Telephone System.

b. Buffering –

Flows can be buffered on the receiving side before being delivered. It will not affect reliability or bandwidth, but helps to smooth out jitter. This technique can be used at uniform intervals.

c. Traffic Shaping –

It is defined as about regulating the average rate of data transmission. It smooths the traffic on server side other than client side. When a connection is set up, the user machine and subnet agree on a certain traffic pattern for that circuit called as Service Level Agreement. It reduces congestion and thus helps the carrier to deliver the packets in the agreed pattern.

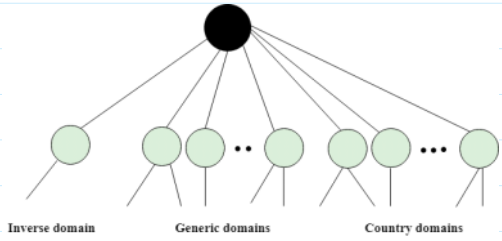
Application Layer

#) **DNS**

An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.

DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.



Generic Domains

- It defines the registered hosts according to their generic behavior.
- Each node in a tree defines the domain name, which is an index to the DNS database.
- It uses three-character labels, and these labels describe the organization type.

Country Domain

The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.

Inverse Domain

The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

Working of DNS

- DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client.
- Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.
- DNS implements a distributed database to store the name of all the hosts available on the internet.
- If a client like a web browser sends a request containing a hostname, then a piece of software such as **DNS resolver** sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

#) SMTP

- SMTP stands for Simple Mail Transfer Protocol.
- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called **Simple Mail Transfer Protocol**.
- It is a program used for sending messages to other computer users based on e-mail addresses.
- It provides a mail exchange between users on the same or different computers, and it also supports:
  - It can send a single message to one or more recipients.
  - Sending message can include text, voice, video or graphics.
  - It can also send the messages on networks outside the internet.
- The main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.

Working of SMTP

1. **Composition of Mail:** A user sends an e-mail by composing an electronic mail message using a Mail User Agent (MUA). Mail User Agent is a program which is used to send and receive mail. The message contains two parts: body and header. The body is the main part of the message while the header includes information such as the sender and recipient address. The header also includes descriptive information such as the subject of the message. In this case, the message body is like a letter and header is like an envelope that contains the recipient's address.
2. **Submission of Mail:** After composing an email, the mail client then submits the completed e-mail to the SMTP server by using SMTP on TCP port 25.
3. **Delivery of Mail:** E-mail addresses contain two parts: username of the recipient and domain name. If the domain name of the recipient's email address is different from the sender's domain name, then MSA will send the mail to the Mail Transfer Agent (MTA). To relay the email, the MTA will find the target domain. It checks the MX record from Domain Name System to obtain the target domain. The MX record contains the domain name and IP address of the recipient's domain. Once the record is located, MTA connects to the exchange server to relay the message.
4. **Receipt and Processing of Mail:** Once the incoming message is received, the exchange server delivers it to the incoming server (Mail Delivery Agent) which stores the e-mail where it waits for the user to retrieve it.
5. **Access and Retrieval of Mail:** The stored email in MDA can be retrieved by using MUA (Mail User Agent). MUA can be accessed by using login and password.

#) **SNMP**

If an organization has 1000 devices then to check all devices, one by one every day, are working properly or not is a hectic task. To ease these up, Simple Network Management Protocol (SNMP) is used.

Simple Network Management Protocol (SNMP) –

SNMP is an application layer protocol that uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults, and sometimes even used to configure remote devices.

SNMP components –

There are 3 components of SNMP:

- **SNMP Manager –**
  It is a centralized system used to monitor network. It is also known as Network Management Station (NMS).
- **SNMP agent –**
  It is a software management software module installed on a managed device. Managed devices can be network devices like PC, routers, switches, servers, etc.
- **Management Information Base –**
  MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables.

SNMP messages –

Different variables are:

a. **GetRequest –**
   SNMP manager sends this message to request data from the SNMP agent. It is simply used to retrieve data from SNMP agents. In response to this, the SNMP agent responds with the requested value through a response message.

b. **GetNextRequest –**
   This message can be sent to discover what data is available on an SNMP agent. The SNMP manager can request data continuously until no more data is left. In this way, the SNMP manager can take knowledge of all the available data on SNMP agents.

c. **GetBulkRequest –**
   This message is used to retrieve large data at once by the SNMP manager from the SNMP agent. It is introduced in SNMPv2c.

d. **SetRequest –**
   It is used by the SNMP manager to set the value of an object instance on the SNMP agent.

e. **Response –**
   It is a message sent from the agent upon a request from the manager. When sent in response to Get messages, it will contain the data requested. When sent in response to the Set message, it will contain the newly set value as confirmation that the value has been set.

f. **Trap –**
   These are the message sent by the agent without being requested by the manager. It is sent when a fault has occurred.

g. **InformRequest –**
   It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to set trap continuously until it receives an Inform message. It is the same as a trap but adds an acknowledgement that the trap doesn't provide.

SNMP security levels –

It defines the type of security algorithm performed on SNMP packets. These are used in only SNMPv3. There are 3 security levels namely:

1. **noAuthNoPriv –**
   This (no authentication, no privacy) security level uses a community string for authentication and no encryption for privacy.
2. **authNopriv** – This security level (authentication, no privacy) uses HMAC with Md5 for authentication and no encryption is used for privacy.
3. **authPriv** – This security level (authentication, privacy) uses HMAC with Md5 or SHA for authentication and encryption uses the DES-56 algorithm.

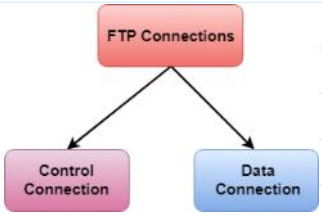
#) FTP

- FTP stands for File transfer protocol.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.

Objectives of FTP

- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

There are two types of connections in FTP:



- **Control Connection:** The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.
- **Data Connection:** The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

Advantages of FTP:

- **Speed:** One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.
- **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.
- **Back & forth movement:** FTP allows us to transfer the files back and forth. Suppose you are a manager of

the company, you send some information to all the employees, and they all send information back on the same server.

Disadvantages of FTP:

- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption.
- FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.
- Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
- It is not compatible with every system.

#) HTTP

- HTTP stands for **Hyper Text Transfer Protocol**.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as Hyper Text Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like format.
- HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

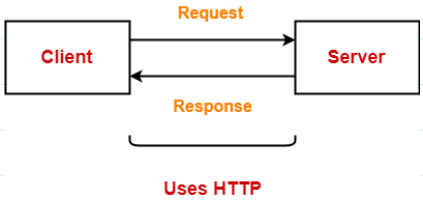
Features of HTTP:

- **Connectionless protocol:** HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.
- **Media independent:** HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.
- **Stateless:** HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

Working-

HTTP uses a client-server model where-

- Web browser is the client.
- Client communicates with the web server hosting the website.



Whenever a client requests some information (say clicks on a hyperlink) to the website server.

The browser sends a request message to the HTTP server for the requested objects.

Then-

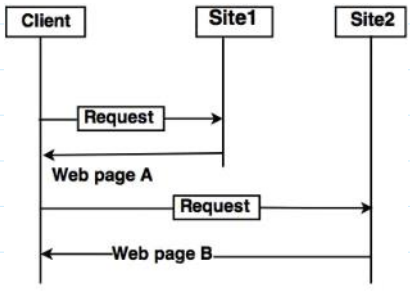
- HTTP opens a connection between the client and server through **TCP**.
- HTTP sends a request to the server which collects the requested data.
- HTTP sends the response with the objects back to the client.
- HTTP closes the connection.

HTTP connections can be of two types-

1) Non-persistent HTTP connection - Non-persistent HTTP connection is one that is used for serving exactly one request and sending one response.
2) Persistent HTTP connection - Persistent HTTP connection is one that can be used for serving multiple requests

#) WWW

- The World Wide Web (WWW) is a collection of documents and other web resources which are identified by URLs, interlinked by hypertext links, and can be accessed and searched by browsers via the Internet.
- World Wide Web is also called the Web and it was invented by Tim Berners-Lee in 1989.
- Website is a collection of web pages belonging to a particular organization.
- The pages can be retrieved and viewed by using browser.



Architecture of WWW

- The client wants to see some information that belongs to site 1.
- It sends a request through its browser to the server at site 2.
- The server at site 1 finds the document and sends it to the client.

Client (Browser):

- Web browser is a program, which is used to communicate with web server on the Internet.
- Each browser consists of three parts: a controller, client protocol and interpreter.
- The controller receives input from input device and use the programs to access the documents.

- After accessing the document, the controller uses one of the interpreters to display the document on the screen.

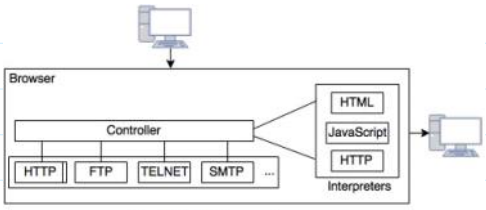


Fig: Client (Browser)

Server:

- A computer which is available for the network resources and provides service to the other computer on request is known as server.
- The web pages are stored at the server.
- Server accepts a TCP connection from a client browser.
- It gets the name of the file required.
- Server gets the stored file. Returns the file to the client and releases the top connection.

Uniform Resource Locater (URL)

- The URL is a standard for specifying any kind of information on the Internet.
- The URL consists of four parts: protocol, host computer, port and path.
- The protocol is the client or server program which is used to retrieve the document or file. The protocol can be ftp or http.
- The host is the name of computer on which the information is located.
- The URL can optionally contain the port number and it is separated from the host name by a colon.
- Path is the pathname of the file where the file is stored.

#) Firewalls

A firewall is a network security tool that monitors incoming and outgoing network traffic and determines whether to allow or block definite traffic based on a defined collection of security rules.
The primary purpose is to enable non-threatening traffic and avoid malicious or unwanted data traffic for protecting the system from viruses and attacks. A firewall is a cybersecurity device that filters network traffic and supports users to block malicious software from creating the Internet in infected computers.

Types of Firewall

Firewalls are generally of two types: *Host-based* and *Network-based.*

1. **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
2. **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

Hardware firewalls

These firewalls are launched either as standalone products for corporate use or, more frequently, as a built-in element of a router or various networking devices. They are considered an essential element of any

traditional security system and network setup.

Software firewalls

These are installed on a device or supported by an operating system or network device manufacturer. They can be customized and support a smaller level of control over functions and protection features. It can protect a system from standard control and access attempts but have trouble with more sophisticated network breaches.

Limitations

There are various limitations of firewalls which are as follows –

- Firewalls cannot stop customers from accessing malicious websites, making them vulnerable to internal threats or attacks.
- Firewalls cannot save against the transfer of virus-infected files or software.
- Firewalls cannot avoid the misuse of passwords.
- Firewalls cannot protect if security rules are misconfigured.
- Firewalls cannot assure against non-technical security risks, including social engineering.

#) Bluetooth

It is a Wireless Personal Area Network (WPAN) technology and is used for exchanging data over smaller distances. This technology was invented by Ericson in 1994. It operates in the unlicensed, industrial, scientific and medical (ISM) band at 2.4 GHz to 2.485 GHz. Maximum devices that can be connected at the same time are 7. Bluetooth ranges upto 10 meters. It provides data rates upto 1 Mbps or 3 Mbps depending upon the version. The spreading technique which it uses is FHSS (Frequency hopping spread spectrum). A Bluetooth network is called a **piconet** and a collection of interconnected piconets is called **scatternet**.

Advantages:

- Low cost.
- Easy to use.
- It can also penetrate through walls.
- It creates an adhoc connection immediately without any wires.
- It is used for voice and data transfer.

Disadvantages:

- It can be hacked and hence, less secure.
- It has slow data transfer rate: 3 Mbps.
- It has small range: 10 meters.

#) Email

E-mail is defined as the transmission of messages on the Internet. It is one of the most commonly used features over communications networks that may contain text, files, images, or other attachments. Generally, it is information that is stored on a computer sent through a network to a specified individual or group of individuals.

Email messages include three components, which are as follows:

- **Message envelope:** It depicts the email's electronic format.
- **Message header:** It contains email subject line and sender/recipient information.
- **Message body:** It comprises images, text, and other file attachments.

Email can be used in different ways: it can be used to communicate either within an organization or personally, including between two people or a large group of people. Most people get benefit from

communicating by email with colleagues or friends or individuals or small groups. It allows you to communicate with others around the world and send and receive images, documents, links, and other attachments. Additionally, it offers benefit users to communicate with the flexibility on their own schedule.

Advantages of Email

There are many advantages of email, which are as follows:

- **Cost-effective:** Email is a very cost-effective service to communicate with others as there are several email services available to individuals and organizations for free of cost. Email offers users the benefit of accessing email from anywhere at any time if they have an Internet connection.
- **Speed and simplicity:** Email can be composed very easily with the correct information and contacts. Also, minimum lag time, it can be exchanged quickly.
- **Mass sending:** You can send a message easily to large numbers of people through email.
- Email provides a simple user interface and enables users to categorize and filter their messages. This can help you recognize unwanted emails like junk and spam mail. Also, users can find specific messages easily when they are needed.
- As compared to traditional posts, emails are delivered extremely fast.
- Email is beneficial for the planet, as it is paperless. It reduces the cost of paper and helps to save the environment by reducing paper usage.

Disadvantages of Email

- **Spam:** Although in recent days, the features of email have been improved, there are still big issues with unsolicited advertising arriving and spam through email. It can easily become overwhelming and takes time and energy to control.
- **Information Overload:** As it is very easy to send email to many people at a time, which can create information overload.
- **Viruses:** Although there are many ways to travel viruses in the devices, email is one of the common ways to enter viruses and infect devices..
- **Time Consuming:** When you get an email and read, write, and respond to emails that can take up vast amounts of time and energy. Many modern workers spend their most time with emails, which may be caused to take more time to complete work.
- **Overlong Messages:** Generally, email is a source of communication with the intention of brief messages. There are some people who write overlong messages that can take much time than required.
- **Insecure:** There are many hackers available that want to gain your important information, so email is a common source to seek sensitive data, such as political, financial, documents, or personal messages.

#) 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 :

IMAP follows Client-server Architecture and is the most commonly used email protocol. It is a combination of client and server process running on other computers that are connected through a network. This protocol resides over the TCP/IP protocol for communication. Once the communication is set up the server listens on port 143 by default which is non-encrypted. For the secure encrypted communication port, 993

is used.

Features of IMAP :

- It is capable of managing multiple mailboxes and organizing them into various categories.
- Provides adding of message flags to keep track of which messages are being seen.
- It is capable of deciding whether to retrieve email from a mail server before downloading.
- It makes it easy to download media when multiple files are attached.

Advantages :

- It offers synchronization across all the maintained sessions by the user.
- It provides security over POP3 protocol as the email only exists on the IMAP server.
- Users have remote access to all the contents.
- It offers easy migration between the devices as it is synchronized by a centralized server.
- There is no need to physically allocate any storage to save contents.

Disadvantages :

- IMAP is complex to maintain.
- Emails of the user are only available when there is an internet connection.
- It is slower to load messages.
- Some emails don't support IMAP which makes it difficult to manage.
- Many browser-based solutions are unavailable due to not support of IMAP.

Network Security

#) Cryptography

Cryptography refers to the science and art of transforming messages to make them secure and immune to attacks. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration but can also be used for user authentication

Types :

There are two types of cryptography which are as follows –

Symmetric Key Cryptography

In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.

Asymmetric-Key Cryptography

In asymmetric or public-key cryptography, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public.

In public-key encryption/decryption, the public key that is used for encryption is different from the private key that is used for decryption. The public key is available to the public, and the private key is available only to an individual.

Cryptography process

Step 1: Encryption

This refers to the process of manipulating a piece of information that usually occurs in the form of plain text using code or encrypting algorithms before transit. This ensures that the information is converted into a

form that the unintentional recipient cannot understand.
The encrypted information is then called cyphertext. The cipher-text is non-readable is the info in transit.

Step 2: Decryption

Decryption converts ciphertext (encrypted text) to plain text. This is done at the receiving end using a code and decryption keys. Special software can also be used for decryption using algorithms to crack decryption.

#) Internet Security Protocols

1. SSL Protocol

SSL Protocol stands for Secure Socket Layer protocol, which is an internet security protocol used for exchanging the information between a web browser and a web server in a secure manner. It provides two basic security services like authentication and confidentiality. SSL protocol has become the world's most popular web security mechanism, all major web browsers support SSL. It is located between the application layer and the transport layer.

2. TLS Protocol

TLS stands for Transport Layer Security, which is an internet security protocol. TLS is an IETF standardization initiative whose goal is to come out with an internet standard version of SSL. To standardized SSL, Netscape handed the protocol to IETF. The idea and implementation are quite similar. Transport layer security protocol uses a pseudo random function to create a master secret. TLS also has three sub protocols same as SSL protocol – Handshake Protocol, Record Protocol, and Alert Protocol.

3. SHTTP

SHTTP stands for Secure HyperText Transfer Protocol, is a set of security mechanism defined for protecting internet traffic. It also includes data entry forms and internet based transaction. Services provided by SHTTP are quite similar to SSL protocol. Secure HyperText Transfer Protocol works at the application layer, and therefore tightly coupled with HTTP. SHTTP supports both authentication and encryption of HTTP traffic between the client and the server. Encryption and digital signature format used in SHTTP have the origins in the PEM (Privacy Enhanced Mail) protocol. SHTTP works at the level of an individual message. It can encrypt and sign an individual message.

4. SET Protocol

SET Protocol stands for Secure Electronic Transaction protocol is an open encryption and security mechanism designed for protecting the eCommerce transaction over the internet. SET is not a payment system, it is a security protocol used over the internet for secure transaction.
The SET protocol provides the following services:

- SET provides authentication by using digital certificates.
- It provides a secure communication channel among all parties involved in an eCommerce transaction.
- It ensures confidentiality because the information is only available for parties involved in a transaction and that too only when and where required.

5. PEM Protocol

PEM Protocol stands for privacy enhanced mail, used for email security over the internet. If we adopted by IAB (Internet Architecture Board) to provide secure electronic mail communication over the internet. PEM working group Privacy Enhanced Mail protocol is described in four specific documents RFC 1421, RFC 1422, RFC 1423, and RFC 1424. It supports cryptographic functions namely encryption, nonrepudiation, and message integrity.

6. PGP Protocol

PGP Protocol stands for Pretty Good Privacy, which we developed by Phil Zimmerman. PGP protocol is easy to use and free including its source code documentation. It also supports the basic requirements of cryptography. PGP protocol becomes extremely popular and more widely used as compared to PEM

protocol. PGP protocol support cryptography like encryption, Non-repudiation, and message integrity.