**Unit 5**

Presentation Layer is the 6th layer in the Open System Interconnection (OSI) model. This layer is also known as Translation layer, as this layer serves as a data translator for the network. The data which this layer receives from the Application Layer is extracted and manipulated here as per the required format to transmit over the network. The main responsibility of this layer is to provide or define the data format and encryption. The presentation layer is also called as Syntax layer since it is responsible for maintaining the proper syntax of the data which it either receives or transmits to other layer(s).

**Functions of Presentation Layer :**

Presentation layer format and encrypts data to be sent across the network.

This layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data efficiently and effectively.

This layer manages the abstract data structures and allows high-level data structures (example- banking records), which are to be defined or exchanged.

This layer carries out the encryption at the transmitter and decryption at the receiver.

This layer carries out data compression to reduce the bandwidth of the data to be transmitted (the primary goal of data compression is to reduce the number of bits which is to be transmitted).

This layer is responsible for interoperability (ability of computers to exchange and make use of information) between encoding methods as different computers use different encoding methods.

This layer basically deals with the presentation part of the data.

Presentation layer, carries out the data compression (number of bits reduction while transmission), which in return improves the data throughput.

This layer also deals with the issues of string representation.

The presentation layer is also responsible for integrating all the formats into a standardized format for efficient and effective communication.

This layer encodes the message from the user-dependent format to the common format and vice-versa for communication between dissimilar systems.

This layer deals with the syntax and semantics of the messages.

This layer also ensures that the messages which are to be presented to the upper as well as the lower layer should be standardized as well as in an accurate format too.

Presentation layer is also responsible for translation, formatting, and delivery of information for processing or display.

This layer also performs serialization (process of translating a data structure or an object into a format that can be stored or transmitted easily).

Features of Presentation Layer in the OSI model: Presentation layer, being the 6th layer in the OSI model, plays a vital role while communication is taking place between two devices in a network.

**List of features which are provided by the presentation layer are:**

Presentation layer could apply certain sophisticated compression techniques, so fewer bytes of data are required to represent the information when it is sent over the network.

If two or more devices are communicating over an encrypted connection, then this presentation layer is responsible for adding encryption on the sender’s end as well as the decoding the encryption on the receiver’s end so that it can represent the application layer with unencrypted, readable data.

This layer formats and encrypts data to be sent over a network, providing freedom from compatibility problems.

This presentation layer also negotiates the Transfer Syntax.

This presentation layer is also responsible for compressing data it receives from the application layer before delivering it to the session layer (which is the 5th layer in the OSI model) and thus improves the speed as well as the efficiency of communication by minimizing the amount of the data to be transferred.

**Working of Presentation Layer in the OSI model :**

Presentation layer in the OSI model, as a translator, converts the data sent by the application layer of the transmitting node into an acceptable and compatible data format based on the applicable network protocol and architecture. Upon arrival at the receiving computer, the presentation layer translates data into an acceptable format usable by the application layer. Basically, in other words, this layer takes care of any issues occurring when transmitted data must be viewed in a format different from the original format. Being the functional part of the OSI mode, the presentation layer performs a multitude (large number of) data conversion algorithms and character translation functions. Mainly, this layer is responsible for managing two network characteristics: protocol (set of rules) and architecture.

**AFP** stands for Apple Filing Protocol. It is a Mac OS network protocol that is used for sharing files among servers and clients. It permits users to access files that belong to external systems. It is an application and session layer protocol.

**Features** :

It supports Unicode file names.

It provides a Portable Operating System Interface (POSIX).

It also provides Access Control List (ACL) permissions that specify which system processes and users are allowed to access the objects and perform the necessary operations.

It offers a storage facility for structured data using Resource Fork and unstructured data using Data Fork.

It supports both TCP/IP and AppleTalk for communication and to provide various services.

Commands like create directory, close directory, copy file, delete file and close volume can be executed in AFP protocol.

**Advantages** :

It offers security features to the system that limits the users to access hazardous files using advanced file locking mechanisms.

It also includes named extended attributes that can be used by the users to map un-interpreted computer files with metadata.

Along with local file access, it also supports Server file access by building a remote file server connection.

It provides 100% compatibility with the Mac file system (HFS+) and is also the native file-sharing protocol.

It provides built-in features such as Spotlight Search, Time Machine, Mac Aliases, and Bonjour Services.

**Disadvantages** :

It is not compatible with storage devices formatted using the Apple File System (APFS).

Its sequential read and write speed is less than the Server Message Block (SMB) protocol.

**Lightweight Presentation Protocol (LPP)** is a protocol used to provide ISO presentation services on top of TCP/IP based protocol stacks. It is defined in RFC 1085. The Lightweight Presentation Protocol describes an approach for providing "stream-lined" support of OSI application services on top of TCP/IP-based network for some constrained environments. It was initially derived from a requirement to run the ISO Common Management Information Protocol (CMIP) in TCP/IP-based networks.

**Network Control Protocol (NCP):**

ARPANET began its development in the year 1966. Several standards were upgraded. Network Control Program (NCP) was responsible for communication between hosts and could support the first commands, on the other hand, Telnet and File Transfer Protocol (FTP) used packet-switching technology to communicate moreover Interface Message Processor was developed to pass messages between hosts. Network Control Protocol (NCP) was an early protocol that later evolved into the Internet. NCP got replaced by TCP/IP in the 1980s.

**Layers in NCP:**

NCP rendered a Transport Layer which included the ARPANET Host-to-Host Protocol (AHHP) and the Initial Connection Protocol (ICP).

ARPANET Host-to-Host Protocol(AHHP) was a simple connection between two host computers.

**Protocols in NCP:**

Encryption Control Protocol (ECP): It is needed to configure, enable, disable, negotiate and control or maintain data encryption algorithms on both ends of the PP connection.

Compression Control Protocol (CCP): CCP is basically responsible for configuring, enabling, disabling, negotiating, and controlling or maintaining data compression algorithms on both ends of the PP connection.

Bridging Control Protocol (BCP): BCP is responsible for configuring, enabling, disabling, negotiating, and controlling or maintaining bridge control modules on both ends of the PP connection. It is similar to IPCP but rather than routing, it initializes bridging.

**Some examples NCPs are:**

Internet Protocol Control Protocol (IPCP): IPCP’s main task is the configuration of the IP addresses over a point-to-point link. LCP or Link control protocol and IPCP of them use exact packet exchange mechanisms.

OSI Network Layer Control Protocol (OSINLCP): OSI protocol modules are configured, enabled and disabled by OSINLCP on either end of the PPP link.

Internetwork Packet Exchange Control Protocol (IPXCP): Internet Packet Exchange (IPX) modules on either end of the PPP link are configured, enabled, and disabled with the help of IPXCP.

IPv6 Control Protocol (IPV6CP): It helps in the configuration of the IPv6 addresses it also enables and disables IP protocol modules over PPP.

NetBIOS Frames Control Protocol (NBFCP): NBF protocol modules on either end of the PPP link are configured, enabled and disabled by NBFCP.

**TELNET** stands for Teletype Network. It is a type of protocol that enables one computer to connect to local computer. It is a used as a standard TCP/IP protocol for virtual terminal service which is given by ISO. Computer which starts connection known as the local computer. Computer which is being connected to i.e. which accepts the connection known as remote computer. When the connection is established between local and remote computer. During telnet operation whatever that is being performed on the remote computer will be displayed by local computer. Telnet operates on client/server principle. Local computer uses telnet client program and the remote computers uses telnet server program.

**Session Layer protocols**

The Session Layer is the 5th layer in the Open System Interconnection (OSI) model. This layer allows users on different machines to establish active communications sessions between them. It is responsible for establishing, maintaining, synchronizing, terminating sessions between end-user applications. In Session Layer, streams of data are received and further marked, which is then resynchronized properly, so that the ends of the messages are not cut initially and further data loss is avoided. This layer basically establishes a connection between the session entities. This layer handles and manipulates data which it receives from the Session Layer as well as from the Presentation Layer.

**Working of Session Layer :**

Session Layer, which is the 5th layer in the OSI model, uses the services provided by The transport layer, enables applications to establish and maintain sessions and to synchronize the sessions.

Now, in order to establish a session connection, several things should be followed.

First thing is we should map the session address to the shipping address. The second thing is that we need to select the required transport quality of service (also referred as QoS) parameters. Next thing is we need to take care of the negotiations which should happen between session parameters. Then we further need to transmit limited transparent user data. Then at last, we need to monitor Data Transfer phase properly. The ability to send larger amount of data files is extremely important and a necessary thing too.

**Functions of Session Layer :**

The session layer being the fifth layer in the OSI model performs several different as well as important functions which are need for establishing as well as maintaining a safe and secure connection.

Following are some of the functions which are performed by Session Layer –

Session Layer works as a dialog controller through which it allows systems to communicate in either half-duplex mode or full duplex mode of communication.

This layer is also responsible for token management, through which it prevents two users to simultaneously access or attempting the same critical operation.

This layer allows synchronization by allowing the process of adding checkpoints, which are considered as synchronization points to the streams of data.

This layer is also responsible for session checkpointing and recovery.

This layer basically provides a mechanism of opening, closing and managing a session between the end-user application processes.

The services offered by Session Layer are generally implemented in application environments using remote procedure calls (RPCs).

The Session Layer is also responsible for synchronizing information from different sources.

This layer also controls single or multiple connections for each-end user application and directly communicates with both Presentation and transport layers.

Session Layer creates procedures for checkpointing followed by adjournment, restart and termination.

Session Layer uses checkpoints to enable communication sessions which are to be resumed from that particular checkpoint at which communication failure has occurred.

The session Layer is responsible for fetching or receiving data information from its previous layer (transport layer) and further sends data to the layer after it (presentation layer).

**Password Authentication Protocol (PAP)**

There are simply two methods to authenticate PPP links namely Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

From these two authentication protocols, PAP is less secured as the password is sent in clear text and is performed only at the initial link establishment.

PAP is a password Authentication Protocol used by PPP links to validate users. PAP authentication requires the calling device to enter the username and password. If the credentials match with the local database of the called device or in the remote AAA database then it is allowed to access otherwise denied.

**Application layer services**

The application layer in the OSI model is the closest layer to the end user which means that the application layer and end user can interact directly with the software application. The application layer programs are based on client and servers.

The application layer enables the user, whether human or software, to access the network.

It provides user interfaces and support for services such as electronic mail, file

access and transfer, access to system resources, surfing the world wide web, and network

management.

The application layer is responsible for providing services to the user.

In this part, we briefly discuss some applications that are designed as a client/server

pair in the Internet. The client sends a request for a service to the server; the server

responds to the client.

**Network Application Architectures**

In a client-server architecture, there is an always-on host, called the server, which services requests from many other hosts, called clients. A data center, housing a large number of hosts, is often used to create a powerful virtual server. In a P2P architecture, there is minimal (or no) reliance on dedicated servers in data centers.

We mention that some applications have hybrid architectures, combining both client-server and P2P elements. For example, for many instant messaging applications, servers are used to track the IP addresses of users, but user-touser messages are sent directly between user hosts (without passing through intermediate servers).

**P2P architectures is self-scalability.**

**Processes Communicating** Processes on two different end systems communicate with each other by exchanging messages across the computer network. With 2P file sharing, the peer that is downloading the file is labeled as the client, and the peer that is uploading the file is labeled as the server.

In the context of a communication session between a pair of processes, the process that initiates the communication (that is, initially contacts the other process at the beginning of the session) is labeled as the client. The process that waits to be contacted to begin the session is the server.

**The Interface Between the Process and the Computer Network**

A process sends messages into, and receives messages from, the network through a software interface called a socket. Asocket is the interface between the application layer and the transport layer within a host. It is also referred to as the Application Programming Interface (API) between the application and the network.

On the transport-layer side, the application developer can only control: (1) the choice of transport protocol and (2) a few transport-layer parameters such as maximum buffer and maximum segment sizes.

**Addressing Processes**

In the Internet, the host is identified by its IP address. A destination port number identify the receiving process (more specifically, the receiving socket) running in the host.

**Transport Services Available to Applications**

We can broadly classify the possible services along four dimensions: reliable data transfer, throughput, timing, and security.

**Reliable Data Transfer**

If a protocol provides such a guaranteed data delivery service, it is said to provide reliable data transfer.

This may be acceptable for loss-tolerant applications, most notably multimedia applications such as conversational audio/video that can tolerate some amount of data loss.

**Transport Services Provided by the Internet**

The Internet (and, more generally, TCP/IP networks) makes two transport protocols available to applications, UDP and TCP.

**TCP Services**

The TCP service model includes a connection-oriented service and a reliable data transfer service.

* Connection-oriented service

After the handshaking phase, a TCP connection is said to exist between the sockets of the two processes. The connection is a full-duplex connection in that the two processes can send messages to each other over the connection at the same time. When the application finishes sending messages, it must tear down the connection.

Reliable data transfer service.

Without error and in the proper order.

TCP also includes a congestion-control mechanism. The TCP congestion-control mechanism throttles a sending process (client or server) when the network is congested between sender and receiver.

* SSL

Enhancement for TCP, called Secure Sockets Layer (SSL). TCP-enhanced-with-SSL not only does everything that traditional TCP does but also provides critical process-to-process security services, including encryption, data integrity, and end-point authentication.

If an application wants to use the services of SSL, it needs to include SSL code in both the client and server sides of the application.

When an application uses SSL, the sending process passes cleartext data to the SSL socket; SSL in the sending host then encrypts the data and passes the encrypted data to the TCP socket.

**UDP Services**

UDP is connectionless, so there is no handshaking before the two processes start to communicate.

UDP provides an unreliable data transfer service—that is, when a process sends a message into a UDP socket, UDP provides no guarantee that the message will ever reach the receiving process. Furthermore, messages that do arrive at the receiving process may arrive out of order.

UDP does not include a congestion-control mechanism.

Services Not Provided by Internet Transport Protocols

Throughput or timing guarantees are services that are not provided by today’s Internet transport protocols.

In summary, today’s Internet can often provide satisfactory service to time-sensitive applications, but it cannot provide any timing or throughput guarantees.

**Application-Layer Protocols**

An application-layer protocol defines how an application’s processes, running on different end systems, pass messages to each other. It defines:

The types of messages exchanged, for example, request messages and response messages

The syntax of the various message types, such as the fields in the message and how the fields are delineated.

The semantics of the fields, that is, the meaning of the information in the fields

Rules for determining when and how a process sends messages and responds to messages

The Web’s application-layer protocol, HTTP (the HyperText Transfer Protocol [RFC 2616]), is available as an RFC.

An application-layer protocol is only one piece of a network application.

**Network Applications**

The Web, electronic mail, directory service video streaming, and P2P applications.

For example, DNS provides a directory service for the Internet.

**The Web** is the common name for the World Wide Web, a subset of the Internet consisting of the pages that can be accessed by a Web browser. Many people assume that the Web is the same as the Internet, and use these terms interchangeably. However, the term Internet actually refers to the global network of servers that makes the information sharing that happens over the Web possible. So, although the Web does make up a large portion of the Internet, but they are not one and same.

Web pages are formatted in a language called Hypertext Markup Language (HTML). It this language that allows users to click through pages on the Web via links. The Web uses HTTP protocol to transmit data and share information. Browsers such as Internet Explorer, Google Chrome or Mozilla Firefox are used to access Web documents, or Web pages, which are connected via links.

The Web is just one of the ways that information is shared over the Internet; others include email, instant messaging and File Transfer Protocol (FTP).

**HTTP** stands for HyperText 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 HyperText 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.

**HTTP Transactions**



The above figure shows the HTTP transaction between client and server. The client initiates a transaction by sending a request message to the server. The server replies to the request message by sending a response message.

**HTTPS**

HTTPS is an abbreviation of Hypertext Transfer Protocol Secure. It is a secure extension or version of HTTP. This protocol is mainly used for providing security to the data sent between a website and the web browser. It is widely used on the internet and used for secure communications. This protocol uses the 443 port number for communicating the data.

This protocol is also called HTTP over SSL because the HTTPS communication protocols are encrypted using the SSL (Secure Socket Layer).By default, it is supported by various web browsers.

Those websites which need login credentials should use the HTTPS protocol for sending the data.

protect their information from being stolen.

Difference between HTTP and HTTPS

HTTP HTTPS

1. It is an abbreviation of Hypertext Transfer Protocol 1. It is an abbreviation of Hypertext Transfer Protocol Secure.

2. This protocol operates at the application layer. 2. This protocol operates at the transport layer.

3. The data which is transferred in HTTP is plain text. 3. The data which is transferred in HTTPS is encrypted, i.e., ciphertext.

4. By default, this protocol operates on port number 80. 4. By default, this protocol operates on port number 443.

5. The URL (Uniform Resource Locator) of HTTP start with [http://](http:///) 5. The URL (Uniform Resource Locator) of HTTPS start with [https://](https:///)

6. This protocol does not need any certificate. 6. But, this protocol requires an SSL (Secure Socket Layer) certificate.

7. Encryption technique is absent in HTTP. 7. Encryption technique is available or present in HTTPS.

8. The speed of HTTP is fast as compared to HTTPS. 8. The speed of HTTPS is slow as compared to HTTP.

9. It is un-secure. 9. It is highly secure.

10. Examples of HTTP websites are Educational Sites, Internet Forums, etc. 10. Examples of HTTPS websites are shopping websites, banking websites, etc.

**Advantages of HTTPS**

Following are the advantages or benefits of a Hypertext Transfer Protocol Secure (HTTPS):

The main advantage of HTTPS is that it provides high security to users.

Data and information are protected. So, it ensures data protection.

SSL technology in HTTPS protects the data from third-party or hackers. And this technology builds trust for the users who are using it.

It helps users by performing banking transactions.

**Disadvantages of HTTPS**

Following are the disadvantages or limitations of a Hypertext Transfer Protocol Secure (HTTPS):

The big disadvantage of HTTPS is that users need to purchase the SSL certificate.

The speed of accessing the website is slow because there are various complexities in communication.

Users need to update all their internal links.

**File Transfer Protocol (FTP)**

File Transfer Protocol (FTP) is the standard mechanism provided by *TCP/IP* for

copying a file from one host to another. Although transferring files from one system to

another seems simple and straightforward, some problems must be dealt with first. For

example, two systems may use different file name conventions. Two systems may have

different ways to represent text and data. Two systems may have different directory

structures. All these problems have been solved by FTP in a very simple and elegant

approach.

FTP differs from other client/server applications in that it establishes two connections

between the hosts. One connection is used for data transfer, the other for control

information (commands and responses). Separation of commands and data transfer

makes FTP more efficient. The control connection uses very simple rules of communication.

Wc need to transfer only a line of command or a line of response at a time. The

data connection, on the other hand, needs more complex rules due to the variety of data

types transferred. However, the difference in complexity is at the FTP level, not TCP.

For TCP, both connections are treated the same.

FTP uses two well-known TCP ports: Port 21 is used for the control connection,

and port 20 is used for the data connection. The client has three components: user

interface, client control process, and the client data transfer process. The server has two

components: the server control process and the server data transfer process. The control

connection is made between the control processes. The data connection is made between

the data transfer processes.



The control connection remains connected during the entire interactive FTP session.

The data connection is opened and then closed for each file transferred. It opens

each time commands that involve transferring files are used, and it closes when the file

is transferred. In other words, when a user starts an FTP session, the control connection

opens. While the control connection is open, the data connection can be opened and

closed multiple times if several files are transferred.

**ELECTRONIC MAIL**

One of the most popular Internet services is electronic mail (e-mail). The designers of

the Internet probably never imagined the popularity of this application program. Its

architecture consists of several components that we discuss in this chapter.

At the beginning of the Internet era, the messages sent by electronic mail were short

and consisted of text only; they let people exchange quick memos. Today, electronic

mail is much more complex. It allows a message to include text, audio, and video. It also

allows one message to be sent to one or more recipients.

In this chapter, we first study the general architecture of an e-mail system including

the three main components: user agent, message transfer agent, and message access

agent. We then describe the protocols that implement these components.

Components of E-Mail System : The basic components of an email system are : User Agent (UA), Message Transfer Agent (MTA), Mail Box, and Spool file. These are explained as following below.

User Agent (UA) : The UA is normally a program which is used to send and receive mail. Sometimes, it is called as mail reader. It accepts variety of commands for composing, receiving and replying to messages as well as for manipulation of the mailboxes.

Message Transfer Agent (MTA) : MTA is actually responsible for transfer of mail from one system to another. To send a mail, a system must have client MTA and system MTA. It transfer mail to mailboxes of recipients if they are connected in the same machine. It delivers mail to peer MTA if destination mailbox is in another machine. The delivery from one MTA to another MTA is done by Simple Mail Transfer Protocol.



Mailbox : It is a file on local hard drive to collect mails. Delivered mails are present in this file. The user can read it delete it according to his/her requirement. To use e-mail system each user must have a mailbox . Access to mailbox is only to owner of mailbox.

Spool file : This file contains mails that are to be sent. User agent appends outgoing mails in this file using SMTP. MTA extracts pending mail from spool file for their delivery. E-mail allows one name, an alias, to represent several different e-mail addresses. It is known as mailing list, Whenever user have to sent a message, system checks recipient’s name against alias database. If mailing list is present for defined alias, separate messages, one for each entry in the list, must be prepared and handed to MTA. If for defined alias, there is no such mailing list is present, name itself becomes naming address and a single message is delivered to mail transfer entity.

Services provided by E-mail system :

Composition – The composition refer to process that creates messages and answers. For composition any kind of text editor can be used.

Transfer – Transfer means sending procedure of mail i.e. from the sender to recipient.

Reporting – Reporting refers to confirmation for delivery of mail. It help user to check whether their mail is delivered, lost or rejected.

Displaying – It refers to present mail in form that is understand by the user.

Disposition – This step concern with recipient that what will recipient do after receiving mail i.e save mail, delete before reading or delete after reading.

*MIME*

Electronic mail has a simple structure. Its simplicity, however, comes at a price. It can

send messages only in NVT 7-bit ASCII format. In other words, it has some limitations.

For example, it cannot be used for languages that are not supported by 7-bit

ASCII characters (such as French, German, Hebrew, Russian, Chinese, and Japanese).

Also, it cannot be used to send binary files or video or audio data.

Multipurpose Internet Mail Extensions (MIME) is a supplementary protocol that

allows non-ASCII data to be sent through e-mail. MIME transforms non-ASCII data at

the sender site to NVT ASCII data and delivers them to the client MTA to be sent through

the Internet. The message at the receiving side is transformed back to the original data.

We can think of MIME as a set of software functions that transforms non-ASCII

data (stream of bits) to ASCII data and vice versa, as shown in Figure 26.14.



Message Transfer Agent: SMTP

The actual mail transfer is done through message transfer agents. To send mail, a system

must have the client MTA, and to receive mail, a system must have a server MTA. The

formal protocol that defines the MTA client and server in the Internet is called the Simple

Mail Transfer Protocol (SMTP). As we said before, two pairs of MTA client/server

programs are used in the most common situation (fourth scenario). Figure 26.16 shows

the range of the SMTP protocol in this scenario.



SMTP is used two times, between the sender and the sender's mail server and

between the two mail servers. As we will see shortly, another protocol is needed

between the mail server and the receiver.

SMTP simply defines how commands and responses must be sent back and forth.

Each network is free to choose a software package for implementation. We discuss the

mechanism of mail transfer by SMTP in the remainder of the section.

Message Access Agent: **POP** and IMAP

The first and the second stages of mail delivery use SMTP. However, SMTP is not

involved in the third stage because SMTP is a *push* protocol; it pushes the message from the client to the server. In other words, the direction of the bulk: data (messages) is from

the client to the server. On the other hand, the third stage needs a *pull* protocol; the client

must pull messages from the server. The direction of the bulk data is from the server to

the client. The third stage uses a message access agent.

Currently two message access protocols are available: Post Office Protocol, version 3

(POP3) and Internet Mail Access Protocol, version 4 (IMAP4). Figure 26.19 shows the

position of these two protocols in the most common situation (fourth scenario).



*POP3*

Post Office Protocol, version 3 (POP3) is simple and limited in functionality. The

client POP3 software is installed on the recipient computer; the server POP3 software

is installed on the mail server.

Mail access starts with the client when the user needs to download e-mail from the

mailbox on the mail server. The client opens a connection to the server on TCP port 110.

It then sends its user name and password to access the mailbox. The user can then list

and retrieve the mail messages, one by one. Figure 26.20 shows an example of downloading

using POP3.

POP3 has two modes: the delete mode and the keep mode. In the delete mode, the

mail is deleted from the mailbox after each retrieval. In the keep mode, the mail

remains in the mailbox after retrieval. The delete mode is normally used when the user

is working at her permanent computer and can save and organize the received mail after

reading or replying. The keep mode is normally used when the user accesses her mail

away from her primary computer (e.g., a laptop). The mail is read but kept in the system

for later retrieval and organizing.

*IMAP4*

Another mail access protocol is Internet Mail Access Protocol, version 4 (IMAP4).

IMAP4 is similar to POP3, but it has more features; IMAP4 is more powerful and more

complex. POP3 is deficient in several ways. It does not allow the user to organize her mail on

the server; the user cannot have different folders on the server. (Of course, the user can

create folders on her own computer.) In addition, POP3 does not allow the user to

partially check the contents of the mail before downloading.

IMAP4 provides the following extra functions:

o A user can check the e-mail header prior to downloading.

o A user can search the contents of the e-mail for a specific string of characters prior

to downloading.

o A user can partially download e-mail. This is especially useful if bandwidth is limited

and the e-mail contains multimedia with high bandwidth requirements.

o A user can create, delete, or rename mailboxes on the mail server.

o A user can create a hierarchy of mailboxes in a folder for e-mail storage.

Internet Relay Chat (IRC) is an Internet application that was developed by Jakko Oikarinen in Finland. Chat is the most convenient immediate way to communicate with others via Internet. There are a number of topics called “channels” through which you can chat with many people all over the world. After joining channel, you can see what other people on this channel type on their keyboards. In that situation, everyone on this channel can see whatever you type on your keyboard. You can also hold individual conversations with someone. Channels get live on different servers around the world. Some servers have only a few channels, while others have many of them.

Model used for IRC :

IRC follows client-server model. It means that both client and server software are required in order to use it. Many IT (Information Technology) clients are available for different kinds of computers, so whether you have a PC, Macintosh, or UNIX work-section, you will be able to use IRC.

**Chatting on IRC :**

IRC client connects/communicates with IRC server on Internet. First, you have to log on to the server using a client and then pick the channel on which you want to chat. They are sent to your server when you type words on your keyboard. Now your server is part of global IRC server network. Your server sends your messages to other servers, which in turn, sends your messages to people who are part of your channel.

They can then read and respond to your messages. Many websites use proprietary chat software that does not use IRC protocol but enables you to chat when you are on site. There is another kind of chat, called Instant Messaging. In this kind of chatting, you communicate privately, one-to-one, with another person. You can create special lists so that you are informed when your “buddies” come online, ready to chat, and they are informed when you come online.

**Working on IRC :**

When you want to chat, first you have to make a connection to Internet and then start your client software. After that, you need to log on to IRC server which is located on Internet. There are many IRC servers are located all over the world. Those IRC servers are connected together in network so that they can communicate with each other.

Servers are connected in spanning tree architecture. In this case, each server is connected to several others, but these servers are not directly connected to one another. When you connect to server, first you have to choose a specific channel to join and then choose a user name to identify yourself when you at chat. Many channels are available that cover different topics. Your message is sent from client software on your PC to IRC server to which you are connected. Then message is sent from one server to other servers where all users on this channel are logged on.

In this network, messages are transferred from one server to another server. Under a spanning-tree server architecture, a message always takes the shortest route through network to reach its final destination. Each server sends messages to client software of their respected users who are connected to channel/network. Then people/users can read and respond to your message on their computers.

*Domain Name System*

There are several applications in the application layer of the Internet model that follow

the client/server paradigm. The client/server programs can be divided into two categories:

those that can be directly used by the user, such as e-mail, and those that support other

application programs. The Domain Name System (DNS) is a supporting program that

is used by other programs such as e-mail.

Figure 25.1 shows an example of how a DNS client/server program can support an

e-mail program to find the IP address of an e-mail recipient. A user of an e-mail program

may know the e-mail address of the recipient; however, the IP protocol needs the

IP address. The DNS client program sends a request to a DNS server to map the e-mail

address to the corresponding IP address.

Requirement: Every host is identified by the IP address but remembering numbers is very difficult for the people also the IP addresses are not static therefore a mapping is required to change the domain name to the IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

Domain: There are various kinds of DOMAIN:

Generic domain: .com(commercial) .edu(educational) .mil(military) .org(non profit organization) .net(similar to commercial) all these are generic domain.

Country domain .in (india) .us .uk

Inverse domain if we want to know what is the domain name of the website. Ip to domain name mapping. So DNS can provide both the mapping for example to find the ip addresses of geeksforgeeks.org then we have to type nslookup [www.geeksforgeeks.org](http://www.geeksforgeeks.org/).

Organization of Domain:

**What Is Video Conferencing?**

Video conferencing is an online technology that allows users in different locations to hold face-to-face meetings without having to move to a single location together. This technology is particularly convenient for business users in different cities or even different countries because it saves time, expenses, and hassles associated with business travel. Uses for video conferencing include holding routine meetings, negotiating business deals, and interviewing job candidates.

When a video conference is held for informal purposes, it is called a video call or video chat.

**How Video Conferencing Works**

Video conferencing's main advantage over telephone conference calls is that users can see each other, which allows them to develop stronger relationships.

There are a variety of ways video conferencing can be conducted. Individuals may use web cameras connected to or built into laptops, tablets, or desktop computers. Smartphones and other connected mobile devices equipped with cameras may also be used to connect for video conferences. In such instances, a software-based platform typically is used to transmit the communication over internet protocols.

Some businesses use dedicated video conferencing rooms that have been equipped with high-grade cameras and screens to ensure the conversation is clear and with limited technical faults. Third-party providers often install and assemble the hardware needed to conduct the video conference.

**Cryptography** is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”. In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used For Cryptography: In today’s age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

**Features Of Cryptography are as follows:**

Confidentiality: Information can only be accessed by the person for whom it is intended and no other person except him can access it.

Integrity: Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

Non-repudiation: The creator/sender of information cannot deny his intention to send information at later stage.

Authentication: The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

**Types Of Cryptography:** In general there are three types Of cryptography**:**

**Symmetric Key Cryptography:** It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).

**Hash Functions:** There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

**Asymmetric Key Cryptography:** Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

**Applications Of Cryptography:**

* Computer passwords
* Digital Currencies
* Secure web browsing
* Electronic Signatures
* Authentication
* Cryptocurrencies
* End-to-end encryption

**Firewall – meaning and definition**

A firewall is a computer network security system that restricts internet traffic in to, out of, or within a private network.

This software or dedicated hardware-software unit functions by selectively blocking or allowing data packets. It is typically intended to help prevent malicious activity and to prevent anyone—inside or outside a private network—from engaging in unauthorized web activities.

What is a firewall?

Firewalls can be viewed as gated borders or gateways that manage the travel of permitted and prohibited web activity in a private network. The term comes from the concept of physical walls being barriers to slow the spread of fire until emergency services can extinguish it. By comparison, network security firewalls are for web traffic management — typically intended to slow the spread of web threats.

Firewalls create 'choke points' to funnel web traffic, at which they are then reviewed on a set of programmed parameters and acted upon accordingly. Some firewalls also track the traffic and connections in audit logs to reference what has been allowed or blocked.

Firewalls are typically used to gate the borders of a private network or its host devices. As such, firewalls are one security tool in the broader category of user access control. These barriers are typically set up in two locations — on dedicated computers on the network or the user computers and other endpoints themselves (hosts).

How do firewalls work?

A firewall decides which network traffic is allowed to pass through and which traffic is deemed dangerous. Essentially, it works by filtering out the good from the bad, or the trusted from the untrusted. However, before we go into detail, it helps to understand the structure of web-based networks.

Firewalls are intended to secure private networks and the endpoint devices within them, known as network hosts. Network hosts are devices that ‘talk’ with other hosts on the network. They send and receive between internal networks, as well as outbound and inbound between external networks.

Computers and other endpoint devices use networks to access the internet and each other. However, the internet is segmented into sub-networks or 'subnets' for security and privacy. The basic subnet segments are as follows:

External public networks typically refer to the public/global internet or various extranets.

Internal private network defines a home network, corporate intranets, and other ‘closed’ networks.

Perimeter networks detail border networks made of bastion hosts — computer hosts dedicated with hardened security that are ready to endure an external attack. As a secured buffer between internal and external networks, these can also be used to house any external-facing services provided by the internal network (i.e., servers for web, mail, FTP, VoIP, etc.). These are more secure than external networks but less secure than internal. These are not always present in simpler networks like home networks but may often be used in organizational or national intranets.

A **gateway** is a network node that forms a passage between two networks operating with different transmission protocols. The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model. However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model. It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway. Only the internal traffic between the nodes of a LAN does not pass through the gateway.

**Features of Gateways**

Gateway is located at the boundary of a network and manages all data that inflows or outflows from that network.

It forms a passage between two different networks operating with different transmission protocols.

A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.

The feature that differentiates a gateway from other network devices is that it can operate at any layer of the OSI model.

It also stores information about the routing paths of the communicating networks.

When used in enterprise scenario, a gateway node may be supplemented as proxy server or firewall.

A gateway is generally implemented as a node with multiple NICs (network interface cards) connected to different networks. However, it can also be configured using software.

It uses packet switching technique to transmit data across the networks.