Unit-4

E-mail and other Internet Services: Structure of an Email – Email Address, Email Header, Body and Attachments, Email Clients: Netscape mail Clients, Outlook Express, Web based E-mail. Email encryption Address Book, Signature File. Email Networks and Servers, Email protocols –SMTP, POP3, IMAp4, MIME6, Telnet, FTP, IRC and Search Engine. ISDN, Protocol options – Shell, SLIP, PPP, Service options.

1. **Electronic Mail (e-mail)** is one of the most widely used services of the Internet. This service allows an Internet user to send a **message in a formatted manner (mail)** to other Internet users in any part of the world. Message in the mail not only contain text, but it also contains images, audio and videos data. The person who is sending mail is called **sender** and person who receives mail is called the **recipient**. It is just like postal mail service.

Format of E-mail :
An e-mail consists of three parts that are as follows :

(i). Envelope

(ii). Header

(iii). Body

These are explained as following below.

(i) Envelope :
The envelope part encapsulates the message. It contains all information that is required for sending any e-mail such as destination address, priority and security level. The envelope is used by MTAs for routing message.

(ii) Header :
The header consists of a series of lines. Each header field consists of a single line of ASCII text specifying field name, colon and value. The main header fields related to message transport are :

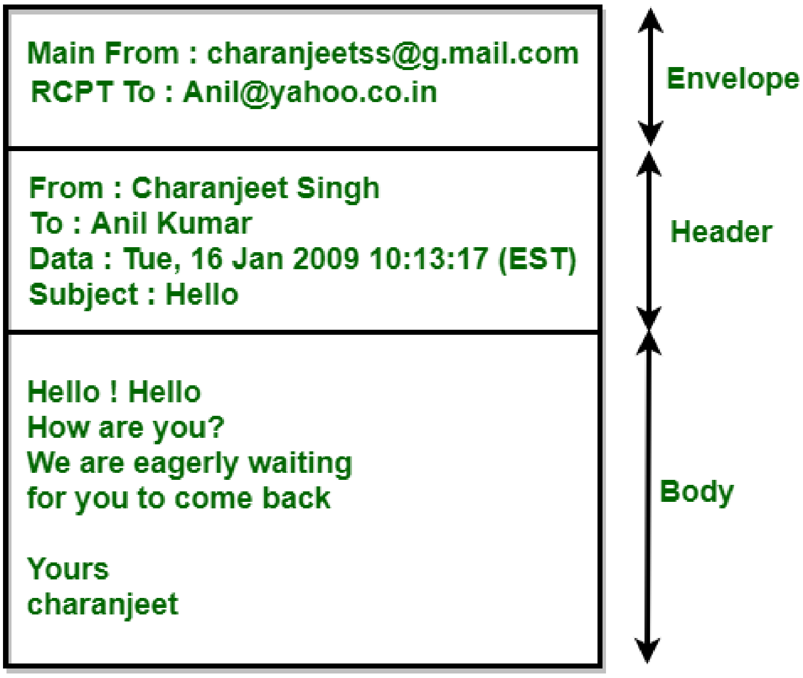
1. **To:** It specifies the DNS address of the primary recipient(s).
2. **Cc :** It refers to carbon copy. It specifies address of secondary recipient(s).
3. **BCC:** It refers to blind carbon copy. It is very similar to Cc. The only difference between Cc and Bcc is that it allow user to send copy to the third party without primary and secondary recipient knowing about this.
4. **From :** It specifies name of person who wrote message.
5. **Sender :** It specifies e-mail address of person who has sent message.

6. **Received :** It refers to identity of sender's, data and also time message was received. It also contains the information which is used to find bugs in routing system.

7. **Return-Path:** It is added by the message transfer agent. This part is used to specify how to get back to the sender.

(iii) Body:- The body of a message contains text that is the actual content/message that needs to be sent, such as "Employees who are eligible for the new health care program should contact their supervisors by next Friday if they want to switch." The message body also may include signatures or automatically generated text that is inserted by the sender's email system.

The above-discussed field is represented in tabular form as follows :



Main From : charanjeetss@g.mail.com
RCPT To : Anil@yahoo.co.in

From : Charanjeet Singh
To : Anil Kumar
Data : Tue, 16 Jan 2009 10:13:17 (EST)
Subject : Hello

Hello ! Hello
How are you?
We are eagerly waiting
for you to come back

Yours
charanjeet

Header	**Meaning**
To:	E-mail address of primary receipt(s).
Cc:	E-mail address of secondary receipt(s).
Bcc:	E-mail address for blind carbon copies.

Header	Meaning
From:	Person or people who have created a message.
Sender:	E-mail address of the actual sender.
Received:	It is used to specify how to get back to the sender.
Return-Path	It can be used to identify a path back to the sender.

In addition to above-discussed fields, the header may also contain a variety of other fields which are as follows:

Header	Meaning
Date:	Date and time when the message was sent.
Reply-To:	It contains e-mail address to which replies should be sent.
Message-Id:	It refers to the unique number for referencing this message later.
In-Reply-To:	Message-Id of a message to which this is as a reply.
References:	It contains other relevant message-ids.
Keywords:	User-chosen keywords.

Header	**Meaning**
Subject:	It contains short summary of message for one-line display.

What is an Email Attachment?

Email attachments are files you send along with the email to support its content or add value or information to the email. A file can be anything like a video, audio, image, chart, document or link that redirects to another webpage or requires a separate download. The purpose of an attachment is to add value to that email and provide more data to the reader to support the content, which the sender cannot include in the email body. The attachment can be of any format and the size varies depending on the email service provider.

2. Email Client

An **email client**, **email reader** or, more formally, **message user agent** (MUA) or **mail user agent** is a computer program used to access and manage a user's email. A web application which provides message management, composition, and reception functions may act as a web email client, and a piece of computer hardware or software whose primary or most visible role is to work as an email client may also use the term.

Netscape Mail Client

Netscape Mail Client was an email client developed by Netscape Communications Corporation. It was a part of the **Netscape Communicator** suite, which included a web browser, an email client, and other internet-related applications. Netscape Mail was popular in the 1990s and early 2000s as one of the first widely-used internet email clients before the rise of modern web-based email services like Gmail.

Key Features of Netscape Mail Client:

(i) **Email Management**: Netscape Mail allowed users to send, receive, and organize emails using protocols like POP3 and IMAP.
(ii) **Address Book**: It had an integrated address book for storing contacts.
(iii) **HTML Email Support**: Users could send and receive HTML emails, which supported rich text formatting, images, and links.
(iv) **Newsgroup Reader**: The client also had a Usenet newsgroup reader, allowing users to participate in internet discussion forums.
(v) **Security Features**: Netscape Mail included support for SSL (Secure Sockets Layer) to enable secure email transmission.
(vi) **Multiple Accounts**: Users could manage multiple email accounts from different service providers in one place.

Netscape's email client was eventually phased out as Mozilla Thunderbird, a standalone email client from the Mozilla project (which originated from Netscape), gained popularity. Today, Netscape Mail is no longer in use, and its development has been discontinued.

What is outlook express

Outlook Express is a discontinued email and news client that was included with Internet Explorer versions 4.0 through 6.0 on Microsoft Windows. It was used primarily to manage email and newsgroups and was designed as a simple email solution for personal use.

Key features of Outlook Express included:

1. **Email Management**: Sending, receiving, and organizing emails.
2. **Newsgroups**: Reading and posting on Usenet newsgroups.
3. **Contacts**: Managing a contact list for easier emailing.
4. **Simple Interface**: A straightforward, easy-to-use interface for basic email tasks.

Unlike Microsoft Outlook, which is a more robust and feature-rich email client included with Microsoft Office, Outlook Express had fewer business-focused tools (such as calendar integration and advanced task management).

Outlook Express was eventually replaced by **Windows Mail** in Windows Vista and later by **Windows Live Mail** in the Windows Live Essentials suite.

What is web-based Email

Web-based email is an email service that is accessed via a web browser, allowing users to send, receive, and manage their emails directly on the web, without needing to install or configure an email client (software on a computer or mobile device). The main advantage of web-based email is that it can be accessed from any device with an internet connection, offering flexibility and convenience.

Popular examples of web-based email services include:

1. **Gmail** (Google)
2. **Outlook.com** (Microsoft)
3. **Yahoo Mail** (Yahoo)
4. **ProtonMail** (secure, privacy-focused email)
5. **Zoho Mail**

Key Features of Web-Based Email:

- **Accessibility**: Can be accessed from any device with a web browser (computer, tablet, smartphone).
- **Storage**: Usually offers a significant amount of online storage for emails and attachments.
- **Spam Filtering**: Automatically filters spam and phishing emails.
- **Attachment Management**: Allows the sending and receiving of files via email.

- **Integration**: Many services integrate with other tools like calendars, cloud storage, and task managers.

Web-based email services are typically hosted by companies (e.g., Google or Microsoft) and offer both free and paid options with varying features.

3. Email encryption Address Book

An **email encryption address book** refers to a feature in some email clients or services that allows users to securely store and manage contacts along with their associated encryption keys (such as PGP keys or S/MIME certificates). This address book ensures that when sending encrypted emails, the correct public encryption key of the recipient is automatically used, helping to maintain the confidentiality of the email content.

Key Aspects of an Email Encryption Address Book:

1. **Storage of Encryption Keys**:
   - Each contact in the address book can have their associated public key stored. This key is used to encrypt emails sent to them.
   - In the case of digital signatures, the sender’s private key is used to sign emails, and the recipient can verify the signature using the sender’s public key.
2. **Automatic Encryption**:
   - When sending an email, the encryption system will check the address book to find the public key of the recipient, ensuring the email is encrypted before sending.
3. **Integration with Email Clients**:
   - Email encryption address books are often part of email clients that support encryption protocols such as **PGP** (Pretty Good Privacy) or **S/MIME** (Secure/Multipurpose Internet Mail Extensions). Examples of such clients include Mozilla Thunderbird and Microsoft Outlook.
4. **Security and Privacy**:
   - Helps users maintain privacy by encrypting the content of emails so that only the intended recipient, who possesses the correct private key, can decrypt the message.
   - Prevents unauthorized access during email transmission over the internet.

4. What is an email signature?

An email signature or signature block or signature file is the block of text that appears at the end of an email message that provides more information about the sender. This can include details such as the sender's full name, occupation or job title, business name, phone number, email address and their website and social media links. In addition to contact information, many people also include a favorite quote, company motto or short personal statement. Users can create email signatures manually or through email generator programs that use Hypertext

Markup Language (HTML). These signatures incorporate colors and shapes instead of just text.

Most email applications let users maintain more than one signature and assign a name to each. One of the signatures is configured as the default signature, which is automatically appended to the end of all email messages. Users can also manually add a signature at the end of a message by selecting from one or more preconfigured signatures.

Many organizations have policies mandating employees' business email signatures follow a certain style. In some cases, they must include the company logo, social media links and icons, or a disclaimer regarding how the recipient of the email can use the data contained in the sender's email.

5. What is a Mail Server?

A **mail server** is a computer system or application that manages and stores emails sent and received over a network, such as the internet. It acts as a digital post office, handling email traffic and ensuring messages are routed to the correct recipients. Mail servers enable users to send, receive, and store emails using their email accounts.

Key Components of a Mail Server

SMTP Server (Simple Mail Transfer Protocol): This server handles the **sending** of emails. When you send an email, the SMTP server transfers the email from your email client to the recipient’s mail server. It’s also responsible for routing the message through multiple servers if the email has to cross different domains.

POP3 Server (Post Office Protocol 3) or **IMAP Server (Internet Message Access Protocol)**: These servers manage the **receiving** of emails.

- **POP3** downloads the email from the server to the user’s device and then deletes it from the server, so it's only accessible locally.
- **IMAP** allows users to view and manage emails directly on the server without downloading, making emails accessible from multiple devices.

Mail Storage: This component stores emails on the server. For IMAP, the emails are retained on the server, while for POP3, they are downloaded and typically removed from the server.

Webmail Access: Some mail servers offer a web-based interface (like Gmail or Outlook Web Access) that allows users to access their email through a web browser without needing a separate email client.

6. Email Protocols

Email is an essential part of business and personal communication online. The email protocols define the mechanism of the email exchange between servers and clients. This way, they allow us to send and receive messages over the network correctly.

Email protocols list

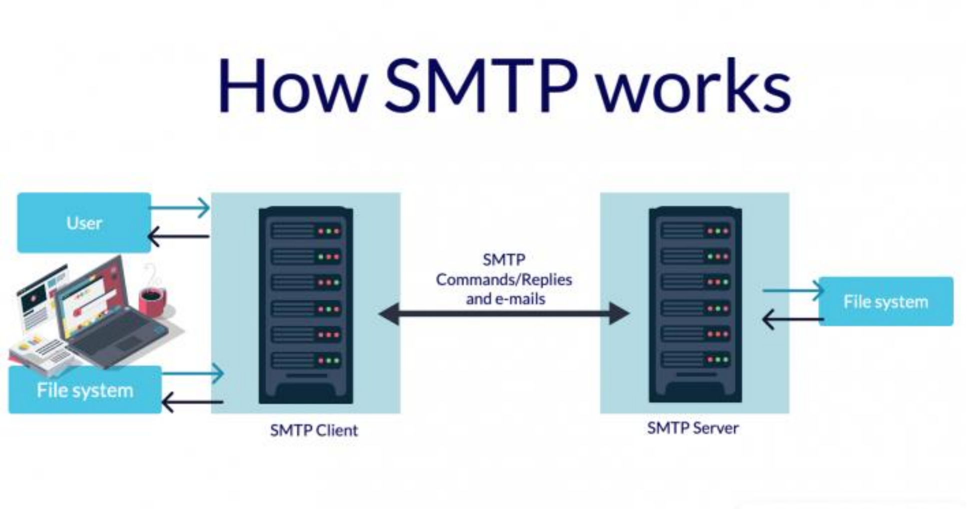
The standard email protocol list includes:

- SMTP
- POP3
- IMAP
- Telnet
- FTP
- MIME

Each of them operates differently and provides a different service for managing your email account.

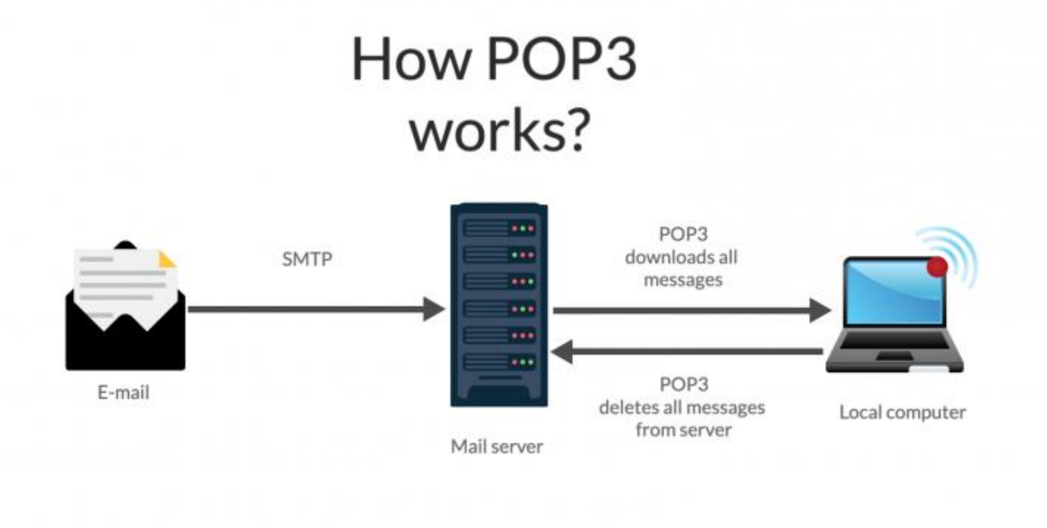
What is SMTP?

SMTP stands for Simple Mail Transfer Protocol, and it is responsible for sending email messages. This protocol is used by email clients and mail servers to exchange emails between computers.



A mail client and the SMTP server communicate with each other over a connection established through a particular email port. Both entities are using SMTP commands and replies to process your outgoing emails. Thanks to the Simple Mail Transfer Protocol, messages can be sent from the same account on different email applications.

What is POP3?

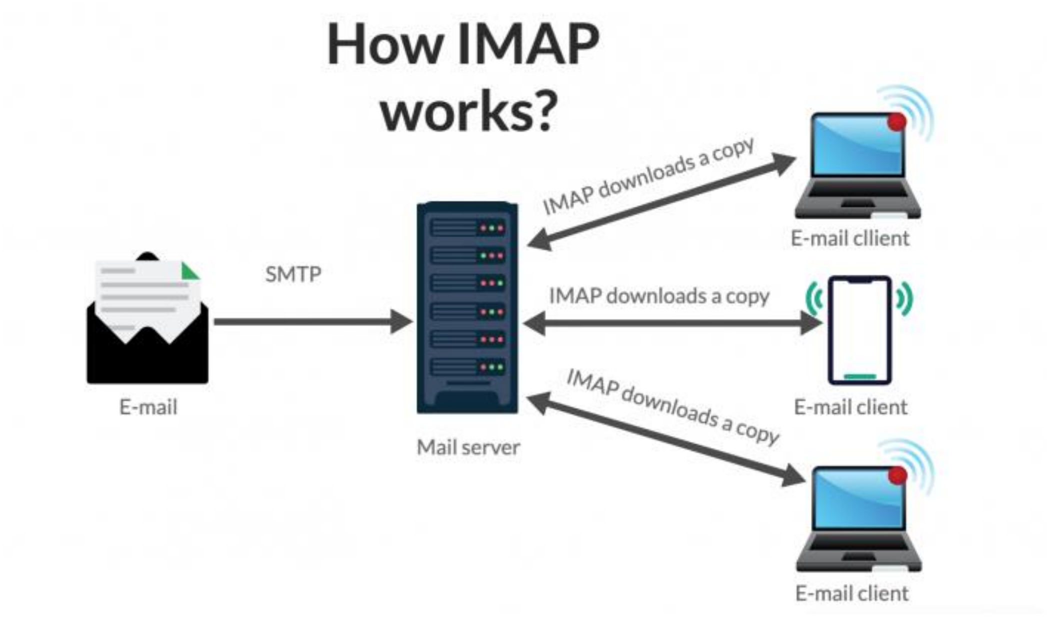

How POP3 works?
SMTP
E-mail
Mail server
POP3 downloads all messages
POP3 deletes all messages from server
Local computer

The POP3 abbreviation stands for Post Office Protocol version 3, which provides access to an inbox stored in an email server. It executes the download and deletes operations for messages. Thus, when a POP3 client connects to the mail server, it retrieves all messages from the mailbox. Then it stores them on your local computer and deletes them from the remote server.

Thanks to this protocol, you are able to access the messages locally in offline mode as well.

Modern POP3 clients allow you to keep a copy of your messages on the server if you explicitly select this option.

What is IMAP?



The Internet Message Access Protocol (IMAP) allows you to access and manage your email messages on the email server. This protocol permits you to manipulate folders, permanently delete and efficiently search through messages. It also gives you the option to set or remove email flags, or fetch email attributes selectively. By default, all messages remain on the server until the user specifically deletes them.

IMAP supports the connection of multiple users to a single mail server.

MIME

Multipurpose Internet Mail Extension (MIME) is a standard that was proposed by Bell Communications in 1991 in order to expand the limited capabilities of email.

MIME is a kind of add-on or a supplementary protocol that allows non-ASCII data to be sent through SMTP. It allows the users to exchange different kinds of data files on the Internet: audio, video, images, application programs as well.

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

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

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

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

What is TELNET?

TELNET is a type of protocol that enables one computer to connect to the local computer. It is used as a standard TCP/IP protocol for virtual terminal service which is provided by ISO. The computer which starts the connection is known as the local computer. The computer which is being connected to i.e. which accepts the connection known as the remote computer. During telnet operation, whatever is being performed on the remote computer will be displayed by the local computer. Telnet operates on a client/server principle.

The **Telnet protocol** originated in the late 1960s, it was created to provide remote terminal access and control over mainframes and minicomputers. Initially, it was designed to be a simple and secure method of connecting to a remote system. This protocol allowed users to access remote computers using a terminal or command-line interface. Over time, Telnet’s use has diminished due to security concerns, and alternatives like **SSH** are now preferred for secure remote management.

How TELNET Works?

Client-Server Interaction

- The Telnet client initiates the connection by sending requests to the Telnet server.
- Once the connection is established, the client can send commands to the server.
- The server processes these commands and responds accordingly.

Character Flow

- When the user types on the local computer, the local operating system accepts the characters.
- The Telnet client transforms these characters into a universal character set called Network Virtual Terminal (NVT) characters.
- These NVT characters travel through the Internet to the remote computer via the local TCP/IP protocol stack.
- The remote Telnet server converts these characters into a format understandable by the remote computer.
- The remote operating system receives the characters from a pseudo-terminal driver and passes them to the appropriate application program

What is FTP?

FTP or File Transfer Protocol is said to be one of the earliest and also the most common forms of transferring files on the internet. Located in the application layer of the OSI model, FTP is a basic system that helps in transferring files between a client and a server. It is what makes the FTP unique that the system provides a reliable and efficient means of transferring files from one system to another even if they have different file structures and operating systems. Contrary to other protocols such as http that cover hypertexts and web resources in general, ftp is dedicated to the management and the transfer of text, binary, or image files.

What is File Transfer Protocol?

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

7. IRC (Internet Relay Chat)

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.

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.

Search Engine

Search engines are the software program that provides information according to the user query. It finds various websites or web pages that are available on the internet and gives related results according to the search. To rank well on a Search Engine, it’s important to know What are Search engines and how they work.

What are Search engines?

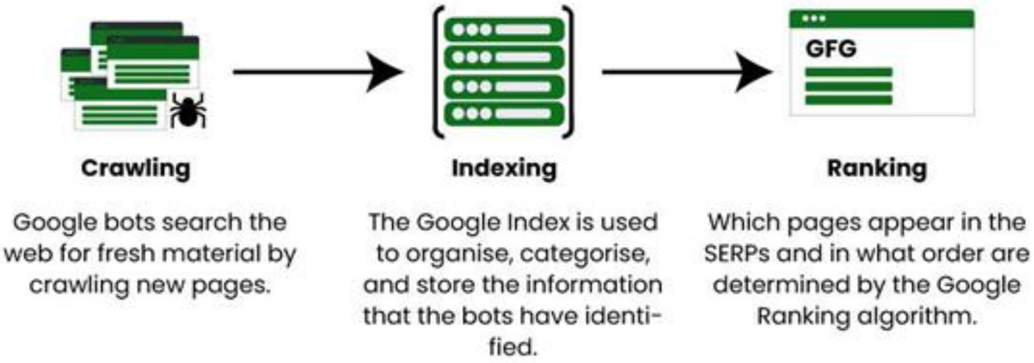
Search engines are programs that allow users to search and retrieve information from the vast amount of content available on the internet. They use algorithms to index and rank web pages based on relevance to a user’s query, providing a list of results for users to explore. Popular search engines include Google, Bing, and Yahoo.

Search engines are generally work on three parts that are **Crawling, Indexing, and Ranking**

1. Crawling: Search engines have a number of computer programs that are responsible for finding information that is publicly available on the internet. The crawler scans the web and creates a list of all available websites. Then they visit each website and by reading HTML code they try to understand the structure of the page, the type of the content, the meaning of the content, and when it was created or updated. Why crawling is important? Your first concern when optimizing your website for search engines is to make sure that they can access it correctly. If crawler cannot find your content you won’t get any ranking or search engine traffic.

2. Indexing: Information identified by the crawler needs to be organized, Sorted, and Stored so that it can be processed later by the ranking algorithm. Search engines don’t store all the information in your index, but they keep things like the Title and description of the page, The type of content, Associated keywords Number of incoming and outgoing links, and a lot of other parameters that are needed by the ranking algorithm. Why indexing is important? Because if your website is not in their index it will not appear for any searches this also means that if you have any pages indexed you have more chances of appearing in the search results for a related query.

3. Ranking: Ranking is the position by which your website is listed in any Search Engine. There is following three steps in which how ranking works .


GFG
Crawling
Google bots search the web for fresh material by crawling new pages.
Indexing
The Google Index is used to organise, categorise, and store the information that the bots have identified.
Ranking
Which pages appear in the SERPs and in what order are determined by the Google Ranking algorithm.

8. What is ISDN?

ISDN is a circuit-switched telephone network system, but it also provides access to packet-switched networks that allow digital transmission of voice and data. This results in potentially better voice or data quality than an analog phone can provide. It provides a packet-switched connection for data in increments of 64 kilobit/s. It provided a maximum of 128 kbit/s bandwidth in both upstream and downstream directions. A greater data rate was achieved through channel bonding. Generally, ISDN B-channels of three or four BRIs (six to eight 64 kbit/s channels) are bonded.

History of ISDN

Before the *Integrated Services Digital Network (ISDN)*, the telephone system was seen as a way to transmit voice, with some special services available for data. The main feature of ISDN is that it can integrate speech and data on the same lines, which were not available in the classic telephone system. In the context of the OSI model, ISDN is employed as the network in data-link and physical layers but commonly ISDN is often limited to usage to Q.931 and related protocols. These protocols introduced in 1986 are a set of signalling protocols establishing and breaking circuit-switched connections and for advanced calling features for the user. ISDN provides simultaneous voice, video, and text transmission between individual desktop videoconferencing systems and group video conferencing systems.

ISDN Services

ISDN provides a fully integrated digital service to users. These services fall into 3 categories- bearer services, teleservices, and supplementary services.

- **Bearer Services:** Transfer of information (voice, data, and video) between users without the network manipulating the content of that information is provided by the bearer network. There is no need for the network to process the information and therefore does not change the content. Bearer services belong to the first three layers of the OSI model. They are well defined in the ISDN standard. They can be provided using circuit-switched, packet-switched, frame-switched, or cell-switched networks.

- **Teleservices:** In this, the network may change or process the contents of the data. These services correspond to layers 4-7 of the OSI model. Teleservices rely on the facilities of the bearer services and are designed to accommodate complex user needs. The user need not be aware of the details of the process. Teleservices include telephony, teletex, telefax, videotex, telex, and teleconferencing. Though the ISDN defines these services by name yet they have not yet become standards.

- **Supplementary Service:** Additional functionality to the bearer services and teleservices are provided by supplementary services. Reverse charging, call waiting, and message handling are examples of supplementary services which are all familiar with today's telephone company services.

9. Protocol Options

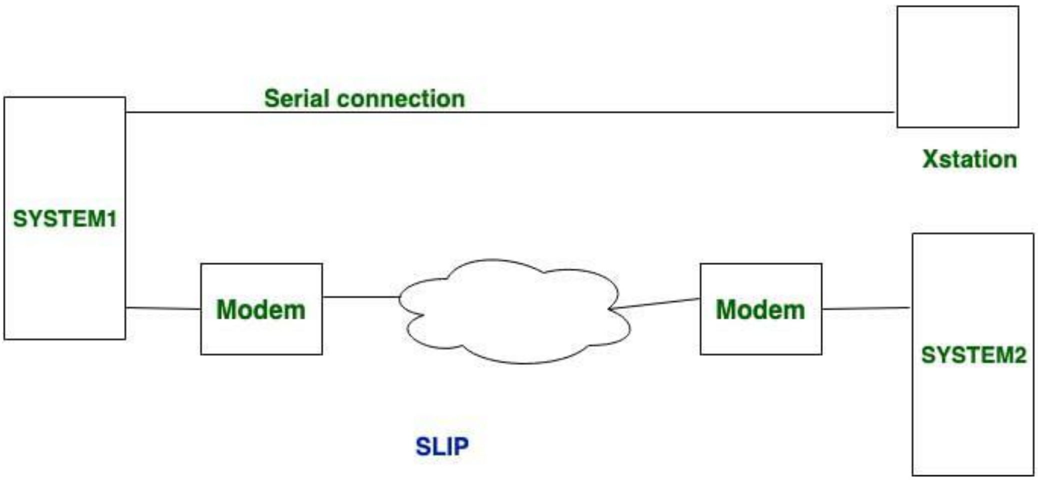
Shell : The term "shell protocol" can refer to various protocols and interfaces for interacting with a computer's operating system shell, but it commonly means protocols or systems enabling remote or local command-line access and control over systems. Here's an overview of what "shell protocol" may entail in different contexts:

1. Secure Shell (SSH) Protocol

- Definition: SSH is a cryptographic network protocol for securely accessing remote computers over a network. It enables command-line access, file transfer, and tunneling of other protocols in a secure manner.
- Uses: SSH is widely used for securely logging into a remote system and executing commands, transferring files, and managing networked systems.
- How It Works: SSH operates over TCP and uses public-key cryptography for authentication, encrypting both the login process and subsequent data transmission.
- Key Features:
  - Secure login and session encryption.
  - Public-key authentication for identity verification.
  - Data integrity and confidentiality during remote sessions.

What is SLIP?

The SLIP is short for the Serial Line Internet Protocol and is actually a very rudimentary one that enables any IP packets to be sent over a serial port. It was conceived as a natural sequence to how the IP datagrams should be forwarded across a point-to-point serial link. As much as it is known and documented, SLIP is relatively simple and compact and therefore is well suited for use.



Features of SLIP

- **Simple:** SLIP is a simple protocol that does not include any error detection or correction mechanisms.
- **Efficient:** SLIP is an efficient protocol that does not include any unnecessary overhead, which makes it ideal for low-bandwidth connections.
- **Supported by many operating systems:** SLIP is supported by many operating systems, including Windows and Linux.
- **Used for point-to-point connections:** SLIP is used to establish a point-to-point connection between two network devices.

Advantages of SLIP

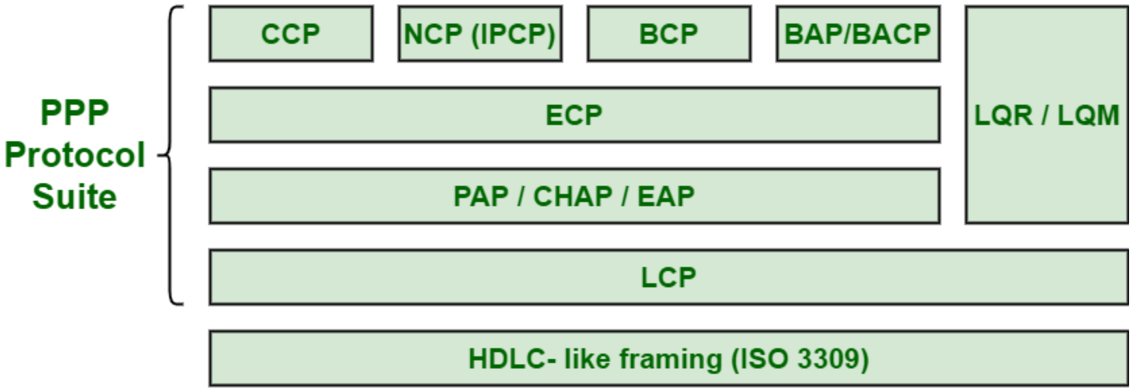
- Small coverage in which high volumes of information can be transmitted with a measure of economy over low-speed networks.
- Ease of implementation; this is one of the major strengths of SLIP considering the fact that it is relatively easy to implement and use in a simple network.

Disadvantages of SLIP

- It also provides no evidence of authentication, error detection, or correction and is very slow.
- This device supports only the fixed type of the IP addressing and can be applied only to the TCP/IP protocol.

What is PPP?

Point-to-Point Protocol (PPP) is a more advanced and generalized protocol than that of SLIP, having some additional features such as authentication, error control, and the protocol of network layer independence. It is most sought-after for setting up end-to-end channels over the serial link joined in a range of networking settings.



Features of PPP

- Authentication: PPP includes authentication mechanisms such as Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) to ensure secure communication.
- Error detection and correction: PPP uses error detection and correction mechanisms such as CRCs and acknowledgments to ensure the integrity of the transmitted data.
- Network layer protocol independence: PPP is independent of the network layer protocol being used, making it compatible with various network protocols.
- Multilink support: PPP supports multilink connections, which allow multiple physical connections to be combined to increase the data transmission rate.

What is an email protocol?

Email protocol is a set of rules defined to ensure that emails can be exchanged between various servers and email clients in a standard manner. This ensures that the email is universal and works for all users.

Example:

A sender using an Apple email client with a Gmail server can send an email to another user using a Zoho mail server on an Outlook email client. This is possible because the servers and the email clients follow the rules and standards defined by the email protocols.

Why do we need email protocols?

Consider the difference between sending a message via a messaging platform like WhatsApp and sending an email. When you send a message using WhatsApp, the recipient will also use WhatsApp to read the messages. The server which processes the message is also the WhatsApp server. The same platform is used in the server and the client, and hence the entire flow of data is handled by the serving platform in a custom manner.

In the case of email, the sender, recipients, and servers involved can all be different but then they need to receive the data, decipher the content and render it in the same way the sender has sent it. Email protocols define how the email message has to be encoded, how it needs to be sent, received, rendered, and so on, and hence they are essential. While email protocols make the process behind emails a bit complex, the protocols ensure that email is a standard, reliable, and universal mode of communication.

What are the different email protocols?

The common protocols for email delivery are Post Office Protocol (POP), Internet Message Access Protocol (IMAP), and Simple Mail Transfer Protocol (SMTP). Each of these protocols has a standard methodology to deal with the emails and also has defined functions.

POP Protocol

POP stands for Post Office Protocol. Email clients use the POP protocol support in the server to download the emails. This is primarily a one-way protocol and does not sync back the emails to the server.

IMAP Protocol

IMAP stands for Internet Message Access Protocol. IMAP Protocol is used to sync the emails in the server with the email clients. It allows two-way sync of emails between the server and the email client, while the emails are stored on the server.

SMTP Protocol

SMTP stands for Simple Mail Transfer Protocol. SMTP is the principal email protocol that is responsible for the transfer of emails between email clients and email servers.

Email clients and email protocols

Email clients use Mail Access protocols like the POP/ IMAP protocols to retrieve/ sync emails from the server. Basically, mail access protocols are used to download or sync emails from the server.

Email clients use transfer protocol - the SMTP protocol to transfer/ send emails through the server. These protocols are quintessential to ensure that users have the independence to use the email application of their choice, on their own devices. Email clients depend on these protocols to send/ receive emails using a user account that is created in an email server.

Chapter: 3.5 Internet Accounts by ISP

Topic: 3.5.2 Protocol Options

Protocol Options

Secure Shell (SSH)

- Secure Shell or SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices.
- It is used primarily on Linux and Unix based system to access shell accounts, SSH was designed as a replacement for Telnet and other in secure remote shells, which send information, notably passwords, in plain text, leaving them open for interception.
- The encryption used by SSH provides confidentially and integrity of data over an insecure network, such as the Internet.
- SSH is typically used to log into a remote machine and execute commands

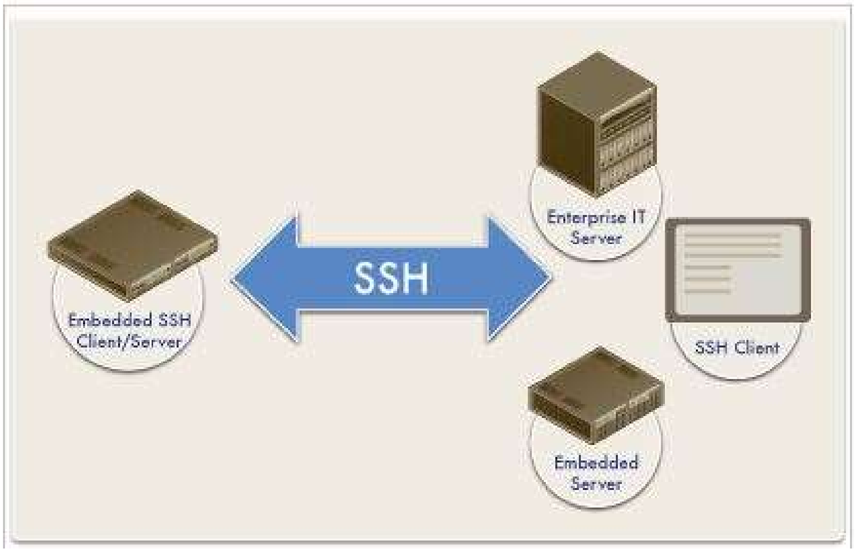


FIG 3.8: Secure Shell (SSH)

SLIP

- The Serial Line Internet Protocol (SLIP) is a mostly obsolete encapsulation of the Internet Protocol designed to work over serial ports and modem connections.
- SLIP (on PCs) has been largely replaced by the Point-to-Point Protocol (PPP), which is better engineered, has more features and does not require its IP address configuration to be set before it is established.
- SLIP does not provide error detection, therefore SLIP on its own is not satisfactory over an error-prone dial-up connection.
- SLIP is a protocol for connection to the Internet via a dial-up connection.

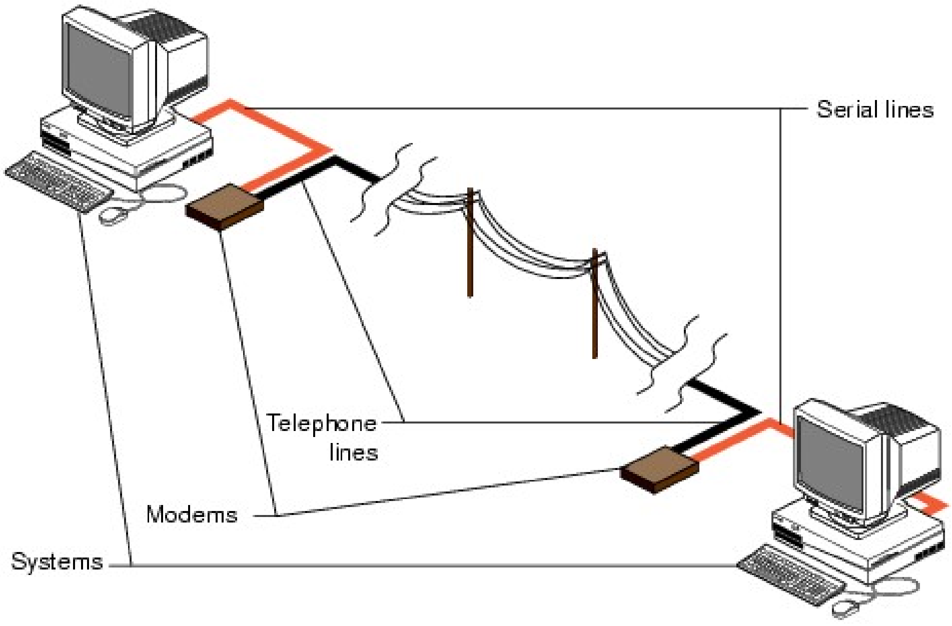


FIG 3.9: SLIP

PPP

- Point-to-Point Protocol or PPP is a data link protocol commonly used to establish a direct connection between two networking nodes.
- PPP originally emerged as are encapsulation protocol for transporting IP traffic over Point-to-Point links.
- It is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server.

- PPP is a full duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission.
- PPP is usually preferred over the earlier de facto standard SLIP because it can handle synchronous as well as asynchronous communication.
- PPP can share a line with other users and it has error detection that SLIP lacks.

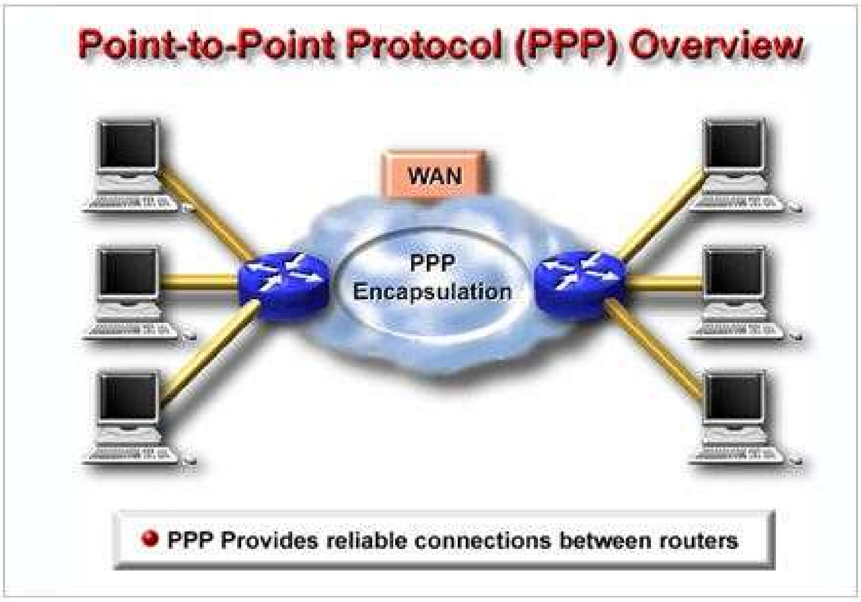

Point-to-Point Protocol (PPP) Overview
WAN
PPP
Encapsulation
● PPP Provides reliable connections between routers

FIG 3.10: Point-to-Point Protocol

Bandwidth

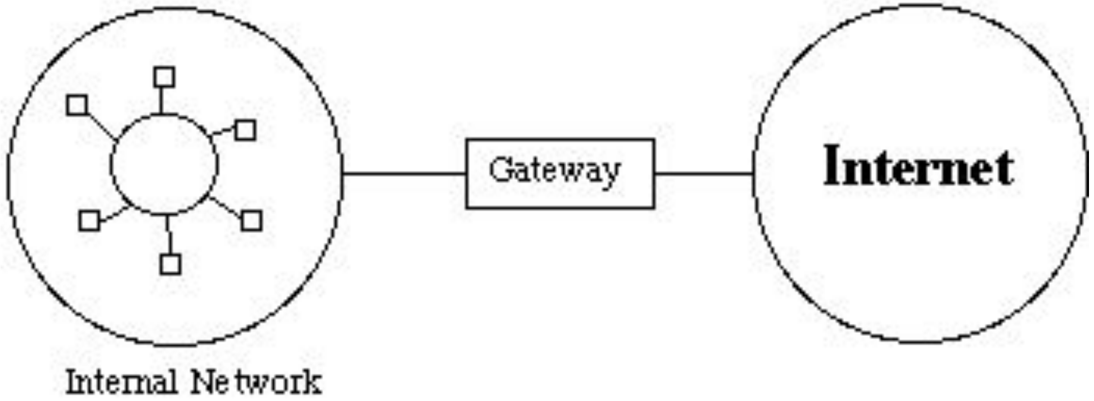
- The amount of data that can be transmitted in a fixed amount of time.
    - For digital devices, the bandwidth is usually expressed in bits per second(bps) or bytes per second(Bps). For analog devices, the bandwidth is expressed in cycles per second or Hertz(Hz).
- OR
- A range of frequencies within a given band, in particular that used for transmitting a signal.
- OR
- Bandwidth describes the maximum data transfer rate of a network or Internet connection. It measures how much data can

Levels of Internet Connectivity

- Level 1 - Access through a gateway
- Level 2 - Access via modem to host connected to network
- Level 3 - Direct Internet Access

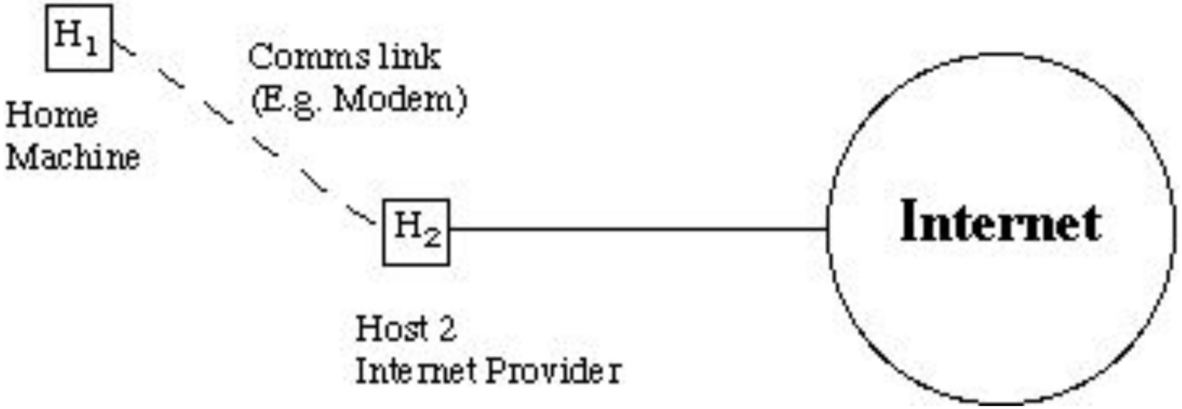
Level 1 Connectivity

- Services are limited to what gateway supports
- Examples
  - Department's / University's Computer Network.
  - America On-Line, Compuserve, Prodigy, etc.
  - Sub-network is not really on the Internet but has access to it in accordance with traffic allowed through gateway



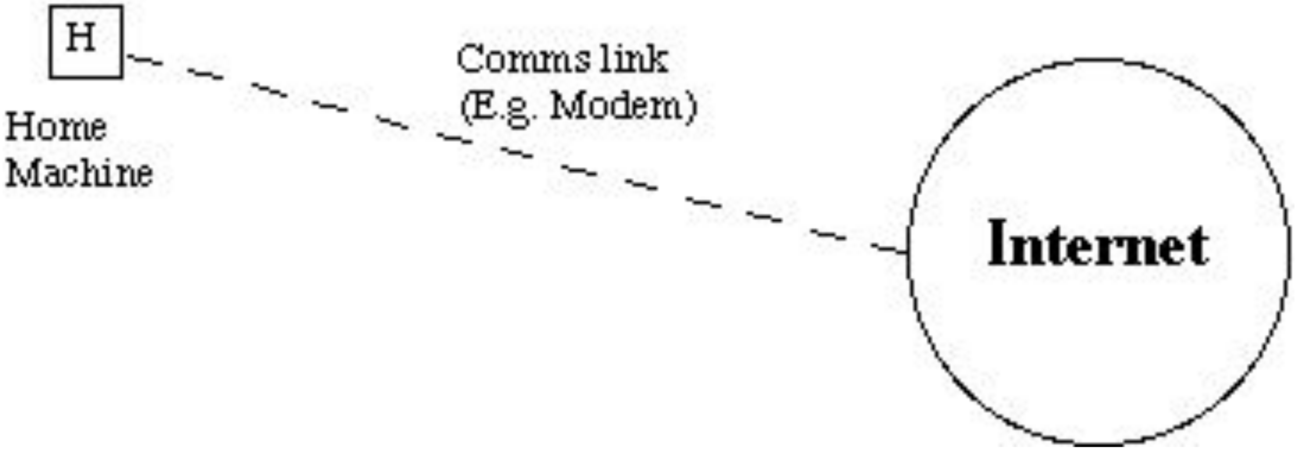
Level 2 Connectivity

- Services are limited to what the connected-to host (H_2) provides
- Everything is accomplished through the H_2
- File transfers from Internet to H_1 require two downloads: Internet to H_2 and H_2 to H_1
- Level 2 connectivity is the most prevalent of Internet access



Level 3 Connectivity for Consumer

- Some local companies provide ***Serial Line Interface Protocol (SLIP)*** or ***Point-to-Point Protocol (PPP)*** Internet access
-



Hardware and Software Requirements for Internet connection:

- The following are the methods of connecting a computer to the Internet using software and hardware peripherals.
    - Connecting a computer using Wireless Broadband
    - Connecting a computer using an Ethernet Cable
    - Connecting a Computer Using Dial-Up Community

Hardware Requirement :

- To connect the Internet, any one of the following is mandatory.
- Modem is used to connect Internet thorugh Telephoneconnection.
- NIC- Network Interface Card(wired/ wireless) facility is the most important hardware required to connect Internet. For example, the Laptop can be connected Internet through the wired/wireless.
- Dongle is used to connect the Internet using cellular network
- Wi-Fi router or Hotspot is used to connect the Internet using wireless network
- Electronic device which supports cellular network
- Internet Connectivity such as Dial-up connection, ISDN, DSL, Cable TV, wired and wireless (Cellular) Network.

Software Requirement

- The operating system should support TCP (Transfer Control Protocol) / IP (Internet Protocol), SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), HTTP (Hyper Text Transfer Protocol) and HTTPS (Hyper Text Transfer Protocol Secured) protocols.
- Browsers and other Internet clients access to the web applications such as Outlook, Gmail, Whatsapp, Facebook, Twitter and etc.

Unit IV

What is meant by email client?

An email client is a software application that is used to access, manage, and send emails. It provides users with a user interface that allows them to view and organize their email messages. Email clients can be standalone applications, web-based applications, or mobile applications.

Netscape Mail Client

The Netscape Navigator is a free open source mail and news client developed by Netscape on 11 June 2007. It is also known as Netscape Messenger, a standalone cross platform desktop email client available for Windows, MAC and Linux users. Initially the Netscape mail program was released as Netscape Mercury was based on Mozilla's Thunderbird. Later it replaced the former Netscape Mail & Newsgroups client for versions 4 to 7.2.

Netscape Messenger contains all the features of Mozilla Thunderbird 2.0.0.9, beside greater AIM integration. It is also similar to the Mozilla SeaMonkey application. Keeps reading to know why Netscape is used for and what file extensions are used by this software.

What is Netscape Used For?

Netscape is a complete internet suit and cab used for multiple purposes as shown below:

- **Netscape Mail & Newsgroups**: The application is mostly used for messaging purposes. By using Netscape as a desktop email client you can configure and manage multiple email accounts. You can also subscribe newsgroups.
- **Netscape Browser**: It was the first browser of the Netscape series, which is totally based on **Mozilla Firefox**. By using Netscape as a web browser you can simply surf internet.

Protocols Used by Netscape Mail Client!

Netscape Mail & Newsgroups supports all email relevant protocols such as IMAP, POP3 & SMTP.

Valuable Features of Netscape Mail & Newsgroups

1. **Supports Multiple Email Accounts**: This is the best feature of Netscape mail client by using which you can add/configure multiple email accounts from the same profile.

2. **Advance Message Search**: By using this advance message search function you may able to find out any particular email or message you are looking for.
3. **Message Filter**: By using message filter function you can easily create new filter rules or manage previous filter rules.
4. **Import Tool**: By using this import tool, you can simply import address books, mail or settings from **Microsoft Outlook**, **Outlook Express** and **Eudora** mail clients.
5. **Download Manager**: The download manager show downloading status including: file name, progress, time remaining, transferred and speed etc.
6. **Password Manager:** By using password manager feature you can simply manage old stored passwords and also can log out from the account.
7. **One Click Address Book**: Netscape provide one click Address book feature under the Tools from menu bar. By using this option you can add new contacts or import existing contacts. It also allows importing **.vcf** and **.csv file extensions**.
8. **Instant Messenger:** Netscape also provide instant messages with name AOL Instant messenger by using it you can directly contact to a person though chat.
9. **Web Browser:** This internet suite also has web browser function by using it you can surf internet without any ads or popups.
10. **Helpful Navigator:** With the help of Netscape Navigator you may able to navigate the application and also can read current news.

What is Outlook Express?

Microsoft Outlook Express is a discontinued email client. It was included with older versions of the Windows operating system, such as Windows XP, but it is no longer available or supported by Microsoft. Here is a comprehensive review of Outlook Express and its features –

Email Management

- Outlook Express is essentially an email management application, allowing users to send, receive, and organize emails.
- It supports POP3, IMAP, and HTTP-based email providers, as well as multiple email accounts.
- Users may organize their emails by creating folders, and they have basic options for sorting and searching messages.

What is Webmail?

Webmail is a cloud-based service or Web-based email system that allows you to access and use your email from almost anywhere through an internet connection. Unlike Thunderbird or Microsoft Outlook, it does not need software installation. It is a kind of service, which is provided by certain companies and ISPs (Internet service providers).

Especially, these kinds of server-based email systems are more popular for younger users. As with Microsoft Outlook, where emails are stored on-site in the hardware storage drive and logging into a connection with the server is needed to get email; so, in this situation, these services provide an appropriate option to email services.

For people who frequently away from their computers and use multiple devices, Webmail is a great solution for those people. Gmail, Hotmail, and other mainstream providers are the common examples of webmail from Yahoo!, which offer huge amounts of storage, and almost all are free.

They are very calm to set up and use. Although experts have pointed out, these models have advantages and limitations. With client-side email, users do not need an internet connection to review old emails as they can be archived directly on the computer. However, with webmail, you always need an internet connection to review mails as they are available via the dedicated servers over a network connection. Like some resident systems, webmail systems do not need communications protocols; that is one of another benefit of webmail. Some of the less tech-savvy users are frustrated by mail delivery failures while using continue resident or non-webmail systems, but a webmail product helps to prevent that issue.

Why is webmail so popular?

Webmail accounts allow users to send, reply, read, organize their email into saving attachments and folders without the need of installing or using an email application software like Microsoft Outlook. The webmail service provides you a web page for accessing your email account and holds all of your emails on their computer systems and storage systems.

Some popular webmail services

In modern times, many webmail services are available for users, which are not software-based. Below, a list contains some the free webmail services.

- **Gmail:** Gmail is a type of Webmail, a free Web-based e-mail service that allows users a gigabyte of storage for messages or other data. It is a very popular email service developed by Google. There are 1.5 billion active users of Gmail by October 2019.
- **Yahoo! Mail:** It is a web and cloud-based messaging solution that is launched by the American company Yahoo! on 8 October 1997. You can connect with your email with one-tap access to your inbox with the help of Yahoo! Mail, and it had 225 million users by January 2020. You can use to create Yahoo account by using this link - https://overview.mail.yahoo.com/

- **com:** It is a free web-based e-mail service that allows you to send and receive e-mail on your computer. Somewhat, it is like Google's Gmail service but something different in terms of linking desktop Outlook data. Outlook has two types of versions: Microsoft Outlook and Microsoft Outlook Express. To create an Outlook account, you can use this link https://signup.live.com/?lic=1
- **ProtonMail:** Unlike Gmail and Outlook.com., it uses client-side encryption to protect user data and email content, which is founded in 2013. To create a ProtonMail account, use this link - https://protonmail.com/
- **Zoho:** It holds a lot of potential for businesses, which is the first of the lesser-known free email accounts for making a list. It is an email service that very user-friendliness. It provides an easier way to accomplish all of your daily tasks by integrating with Google Drive, cloud-based file managers, Box.
- **GMX Mail:** GMX Mail is a free advertising-supported email service that may be accessed via POP3 and IMAP4 protocols as well as through webmail. It is provided by GMX (Global Mail eXchange) in Germany in 1997 that offers 65GB of storage.

Email Encryption Definition

Email encryption is an authentication process that prevents messages from being read by an unintended or unauthorized individual. It scrambles the original sent message and converts it into an unreadable or undecipherable format . Email encryption is necessary when sharing sensitive information via email.

Hackers use email to target victims and steal data, such as personal information like names, addresses, and login credentials, then commit crimes like identity theft or identity fraud. Furthermore, most sent emails are encrypted while the data is transmitted, but the information is stored in clear text, making the content readable by email providers. Popular free-to-use email services typically do not provide end-to-end encryption, which means hackers can easily intercept sent messages.

An address book is a way to manage your email contacts. With an address book, you can store contact information, such as names, phone numbers, and email addresses, of people you know.

Email encryption is a crucial aspect of securing your communications. Here's how it relates to your address book and signature file:

Email Encryption

1. **What It Is**: Email encryption secures the content of your emails, ensuring that only the intended recipient can read them. This can be done using various protocols like PGP (Pretty Good Privacy) or S/MIME (Secure/Multipurpose Internet Mail Extensions).
2. **Importance**: Protects sensitive information from unauthorized access, helps maintain privacy, and is essential for compliance with data protection regulations.

Address Book Considerations

- **Secure Storage**: When using encrypted email, make sure your address book is also secure. Use strong passwords and consider encrypting the storage of your contacts if possible.
- **Trusted Contacts**: Ensure that the contacts in your address book are aware of and capable of using encryption, as this is necessary for secure communication.

Signature File

1. **What It Is**: A signature file is a block of text automatically appended to the end of your email messages. It often includes your name, title, contact information, and can include a legal disclaimer.
2. **Using with Encryption**:
   - **Plain Text vs. HTML**: Ensure your signature is simple, especially when using encryption, as complex HTML signatures may not render correctly for all recipients.
   - **Security Note**: While your signature does not need to be encrypted, be cautious about including sensitive information.

Best Practices

- **Use Trusted Tools**: Choose reliable email clients and encryption tools that support secure communications.
- **Educate Contacts**: Inform your contacts about encryption and encourage them to use it for sensitive exchanges.
- **Regularly Update**: Keep your address book updated and periodically review your signature file to ensure it reflects your current contact information.

What is an email protocol?

Email protocol is a set of rules defined to ensure that emails can be exchanged between various servers and email clients in a standard manner. This ensures that the email is universal and works for all users.

Example:

A sender using an Apple email client with a Gmail server can send an email to another user using a Zoho mail server on an Outlook email client. This is possible because the servers and the email clients follow the rules and standards defined by the email protocols.

Why do we need email protocols?

Consider the difference between sending a message via a messaging platform like WhatsApp and sending an email. When you send a message using WhatsApp, the recipient will also use WhatsApp to read the messages. The server which processes the message is also the WhatsApp server. The same platform is used in the server and the client, and hence the entire flow of data is handled by the serving platform in a custom manner.

In the case of email, the sender, recipients, and servers involved can all be different but then they need to receive the data, decipher the content and render it in the same way the sender has sent it. Email protocols define how the email message has to be encoded, how it needs to be sent, received, rendered, and so on, and hence they are essential. While email protocols make the process behind emails a bit complex, the protocols ensure that email is a standard, reliable, and universal mode of communication.

What are the different email protocols?

The common protocols for email delivery are Post Office Protocol (POP), Internet Message Access Protocol (IMAP), and Simple Mail Transfer Protocol (SMTP). Each of these protocols has a standard methodology to deal with the emails and also has defined functions.

POP Protocol

POP stands for Post Office Protocol. Email clients use the POP protocol support in the server to download the emails. This is primarily a one-way protocol and does not sync back the emails to the server.

IMAP Protocol

IMAP stands for Internet Message Access Protocol. IMAP Protocol is used to sync the emails in the server with the email clients. It allows two-way sync of emails between the server and the email client, while the emails are stored on the server.

SMTP Protocol

SMTP stands for Simple Mail Transfer Protocol. SMTP is the principal email protocol that is responsible for the transfer of emails between email clients and email servers.

Email clients and email protocols

Email clients use Mail Access protocols like the POP/ IMAP protocols to retrieve/ sync emails from the server. Basically, mail access protocols are used to download or sync emails from the server.

Email clients use transfer protocol - the SMTP protocol to transfer/ send emails through the server. These protocols are quintessential to ensure that users have the independence to use the email application of their choice, on their own devices. Email clients depend on these protocols to send/ receive emails using a user account that is created in an email server.

What is an email protocol?

Email protocol is a set of rules defined to ensure that emails can be exchanged between various servers and email clients in a standard manner. This ensures that the email is universal and works for all users.

Example:

A sender using an Apple email client with a Gmail server can send an email to another user using a Zoho mail server on an Outlook email client. This is possible because the servers and the email clients follow the rules and standards defined by the email protocols.

Why do we need email protocols?

Consider the difference between sending a message via a messaging platform like WhatsApp and sending an email. When you send a message using WhatsApp, the recipient will also use WhatsApp to read the messages. The server which processes the message is also the WhatsApp server. The same platform is used in the server and the client, and hence the entire flow of data is handled by the serving platform in a custom manner.

In the case of email, the sender, recipients, and servers involved can all be different but then they need to receive the data, decipher the content and render it in the same way the sender has sent it. Email protocols define how the email message has to be encoded, how it needs to be sent, received, rendered, and so on, and hence they are essential. While email protocols make the process behind emails a bit complex, the protocols ensure that email is a standard, reliable, and universal mode of communication.

What are the different email protocols?

The common protocols for email delivery are Post Office Protocol (POP), Internet Message Access Protocol (IMAP), and Simple Mail Transfer Protocol (SMTP). Each of these protocols has a standard methodology to deal with the emails and also has defined functions.

POP Protocol

POP stands for Post Office Protocol. Email clients use the POP protocol support in the server to download the emails. This is primarily a one-way protocol and does not sync back the emails to the server.

IMAP Protocol

IMAP stands for Internet Message Access Protocol. IMAP Protocol is used to sync the emails in the server with the email clients. It allows two-way sync of emails between the server and the email client, while the emails are stored on the server.

SMTP Protocol

SMTP stands for Simple Mail Transfer Protocol. SMTP is the principal email protocol that is responsible for the transfer of emails between email clients and email servers.

Email clients and email protocols

Email clients use Mail Access protocols like the POP/ IMAP protocols to retrieve/ sync emails from the server. Basically, mail access protocols are used to download or sync emails from the server.

Email clients use transfer protocol - the SMTP protocol to transfer/ send emails through the server. These protocols are quintessential to ensure that users have the independence to use the email application of their choice, on their own devices. Email clients depend on these protocols to send/ receive emails using a user account that is created in an email server.

Unit IV

Email Structure?

Every computer user is familiar with email. It is one of the modern communication mediums that has influenced society. Knowledge pertaining to the structure of the email will help us to use it effectively. We are going to discuss what email is and how it is structured.

What is Email?

“Email” stands for electronic mail. It is the message distributed by electronic means among computer users in a network. An email will be sent from one user and can be distributed to many. The email was initially first used in the 1960s. It took its current form in the 1970s. In fact, some earlier systems required both the sender and receiver to be online which is similar to how instant messaging works today.

Let us see the parts of email and their sub divisions in detail. The popular email services are listed below and are available at free of cost.

1) Outlook.com
2) Gmail
3) Yahoo Mail
4) Inbox.com
5) Mail.com
6) AOL Mail
7) Zoho Mail

The common protocols used for email services are IMAP, POP and SMTP.

Structure of an email

There is a standard structure for emails. Email contents are primarily classified as two, the header and the body. We are going to see the contents come under the two subparts.

The Header

The email header gives us common details about the message such as the unique identity of the message. The details of the users of the ‘from’ and ‘to’ ends are also stored here. The email header consists of the following parts. However, the exact contents of the header can vary according to the email systems that generate the email message.

1) Subject
2) Sender (From:)
3) Date and time received (On)
4) Reply-to
5) Recipient (To:)
6) Recipient email address
7) Attachments

Subject

The subject part is the topic of the message. In most email systems, if the content view of the folders is set to view each messages separately, the subject part also will be visible with the user’s name. These subject fields are scanned by the spam scanners to evaluate the messages.

Sender (From:)

This field describes the ‘from’ address of the email. This will specify the sender’s email address. Usually, it will be the “reply-to” address.

Date and time received (On)

This is the date and time the message received.

Reply-to

This field describes the email address that will become the recipient of the reply to the particular email. When you reply, it will go to this email address despite the sender email address.

Recipient (To:)

This is the first/last name of the email recipient as configured by the sender.

Recipient email address

The email address of the recipient is specified here.

Attachments

Some emails could be attached with files such as text, image, audio, video etc. These files are specified here.

Body

The actual content is stored in this part. This will be in the format of text. This field could also include signatures or text generated automatically by the sender's email system. As we mentioned earlier, the contents of the emails can be varied according to the different email systems used by each user.

OR

Electronic Mail (e-mail) is one of the most widely used services of the Internet. This service allows an Internet user to send a **message in a formatted manner (mail)** to other Internet users in any part of the world. Message in the mail not only contain text, but it also contains images, audio and videos data. The person who is sending mail is called **sender** and person who receives mail is called the **recipient**. It is just like postal mail service.

Format of E-mail :

An e-mail consists of three parts that are as follows :

```
1. Envelope
2. Header
3. Body
```

These are explained as following below.

1. **Envelope :**

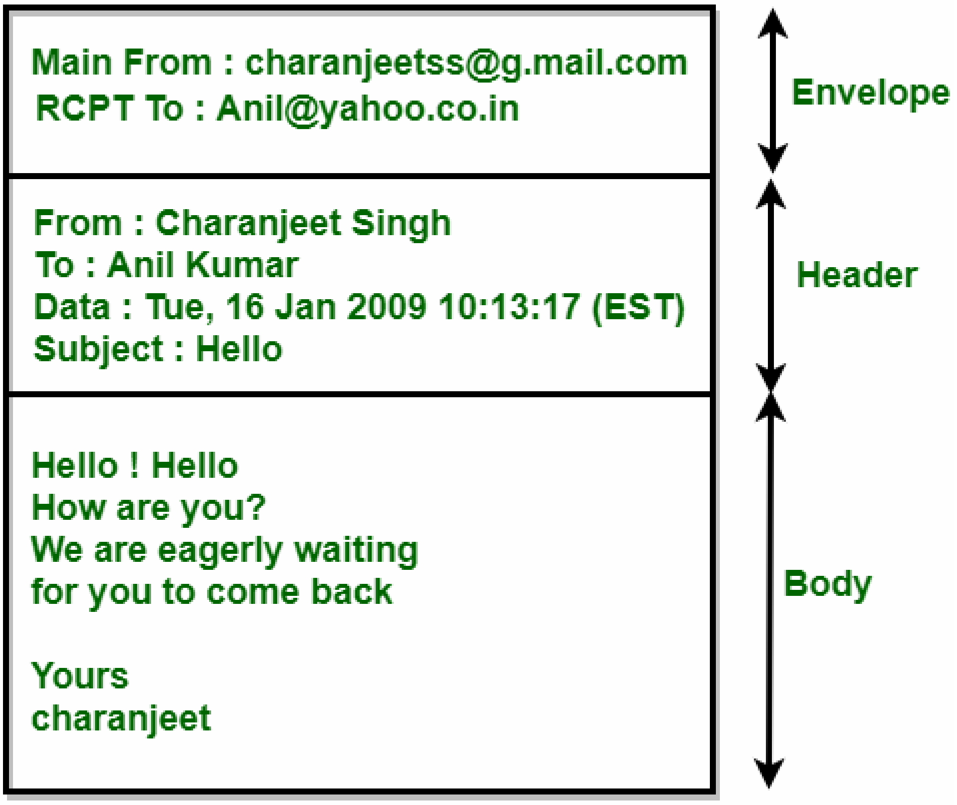
   The envelope part encapsulates the message. It contains all information that is required for sending any e-mail such as destination address, priority and security level. The envelope is used by MTAs for routing message.
2. **Header :**

   The header consists of a series of lines. Each header field consists of a single line of ASCII text specifying field name, colon and value. The main header fields related to message transport are :

1. **To:** It specifies the DNS address of the primary recipient(s).
2. **Cc :** It refers to carbon copy. It specifies address of secondary recipient(s).
3. **BCC:** It refers to blind carbon copy. It is very similar to Cc. The only difference between Cc and Bcc is that it allow user to send copy to the third party without primary and secondary recipient knowing about this.
4. **From :** It specifies name of person who wrote message.
5. **Sender :** It specifies e-mail address of person who has sent message.
6. **Received :** It refers to identity of sender's, data and also time message was received. It also contains the information which is used to find bugs in routing system.
7. **Return-Path:** It is added by the message transfer agent. This part is used to specify how to get back to the sender.

3. Body:- The body of a message contains text that is the actual content/message that needs to be sent, such as "Employees who are eligible for the new health care program should contact their supervisors by next Friday if they want to switch." The message body also may include signatures or automatically generated text that is inserted by the sender's email system.

The above-discussed field is represented in tabular form as follows :



Main From : charanjeetss@g.mail.com
RCPT To : Anil@yahoo.co.in

From : Charanjeet Singh
To : Anil Kumar
Data : Tue, 16 Jan 2009 10:13:17 (EST)
Subject : Hello

Hello ! Hello
How are you?
We are eagerly waiting
for you to come back

Yours
charanjeet

Header	Meaning
To:	E-mail address of primary receipt(s).
Cc:	E-mail address of secondary receipt(s).
Bcc:	E-mail address for blind carbon copies.
From:	Person or people who have created a message.
Sender:	E-mail address of the actual sender.
Received:	It is used to specify how to get back to the sender.
Return-Path	It can be used to identify a path back to the sender.

In addition to above-discussed fields, the header may also contain a variety of other fields which are as follows :

Header	Meaning
Date:	Date and time when the message was sent.
Reply-To:	It contains e-mail address to which replies should be sent.
Message-Id:	It refers to the unique number for referencing this message later.
In-Reply-To:	Message-Id of a message to which this is as a reply.
References:	It contains other relevant message-ids.
Keywords:	User-chosen keywords.
Subject:	It contains short summary of message for one-line display.

What is the Secure Shell Key?

Secure Shell or SSH, is a protocol that allows you to connect securely to another computer over an unsecured network. It developed in 1995. SSH was designed to replace older methods like Telnet, which transmitted data in plain text.

Imagine a system administrator working from home who needs to manage a remote server at a company data center. Without SSH, they would have to worry about their login credentials being intercepted, leaving the server vulnerable to hackers. Instead of it after using SSH, the administrator establishes a secure connection that encrypts all data sent over the internet. They can now log in with their username and a private key, allowing them to safely execute commands on the server, transfer files, and make necessary updates, all of these without the risk of spying eyes watching their actions. This secure access is essential for maintaining the integrity of sensitive information of the company. **SSH (Secure Shell)** is an access credential that is used in the SSH Protocol. In other words, it is a cryptographic network protocol that is used for transferring encrypted data over the network.

What is SLIP?

Serial Line Internet Protocol (SLIP) is a basic protocol for encapsulating Internet Protocol (IP) packets over serial communication lines. SLIP was created to allow computers to connect to the Internet over dial-up or leased-line connections. It is a protocol that runs at the OSI model's data link layer and was widely used in the early days of the Internet.

When a computer connects to the Internet using SLIP, it makes a serial connection to a modem or other serial device. The SLIP protocol is then used to encapsulate IP packets and transport them to the other end of the connection through the serial line.

However, the SLIP protocol has limitations. One of the most significant disadvantages is the absence of error-checking methods. This means that SLIP does not identify or retransmit packets that are lost or corrupted during transmission. As a result, SLIP is regarded as an unreliable protocol.

Another limitation of SLIP is that it does not have encryption or authentication techniques. This means that data sent through a SLIP connection is insecure and can be intercepted and accessed by unauthorised users.

Despite these drawbacks, SLIP continues to be used in some specialised applications where simplicity and low overhead favour reliability and security. Other protocols, such as PPP (Point-to-Point Protocol), are chosen for most current applications due to their more robust features and increased security.

What is PPP?

PPP (Point-to-Point Protocol) is a data link layer protocol that is used to connect two network devices, such as a computer and a modem or a router and a network. PPP is frequently used for connecting to the Internet through dial-up, DSL, cable, or other types of connection.

PPP has various advantages over SLIP that make it a more robust and secure protocol. To begin, PPP includes error detection and correction techniques to ensure that data is reliably transferred over the connection. PPP will detect and retransmit a packet if it is lost or corrupted during transmission.

Second, PPP has procedures for verifying the identification of the connecting devices. This prevents unauthorised access and potential security breaches by ensuring that only authorised users can access the network.

Third, PPP has encryption techniques to prevent unauthorised users from eavesdropping and interception of data transmitted over the connection.

Fourth, PPP can handle a variety of network layer protocols, including IP, Internetwork Packet Exchange (IPX), and AppleTalk. PPP can therefore be used in a variety of network environments.

The Link Control Protocol (LCP) is a three-stage mechanism used by PPP. Link establishment, authentication, and network layer protocol configuration are the three stages. During the Link Establishment stage, the two devices negotiate and come to terms on connection settings such as MTU size, compression options, and error correction methods.

The two devices authenticate each other's identities during the authentication stage using protocols such as the Password Authentication Protocol (PAP) or the Challenge Handshake Authentication Protocol (CHAP).

The two devices negotiate the network layer protocol to be used, such as IP or IPX, and specify the required settings for that protocol during the Network Layer Protocol Configuration stage.

PPP is a more robust and secure protocol than SLIP in general, supporting error detection and correction, authentication, encryption, and several network layer protocols. As a result, PPP is the preferred protocol for connecting to the Internet and other network settings where dependability and security are important.

Difference between SLIP and PPP

The following table highlights the major differences between SLIP and PPP −

Characteristics	**SLIP**	**PPP**
Protocol	It is a simple protocol	It is a robust protocol
Error-checking	No Error-checking	Error detection and correction
Authentication	No Authentication	It has authentication mechanisms.
Encryption	No Encryption	It has encryption mechanisms.

Reliability	Unreliable	Reliable
Security	Insecure	Secure
Overhead	Low Overhead	Higher Overhead
Stands for	Serial Line Internet Protocol (SLIP)	Point-to-Point Protocol (PPP)