# Computer Network Security

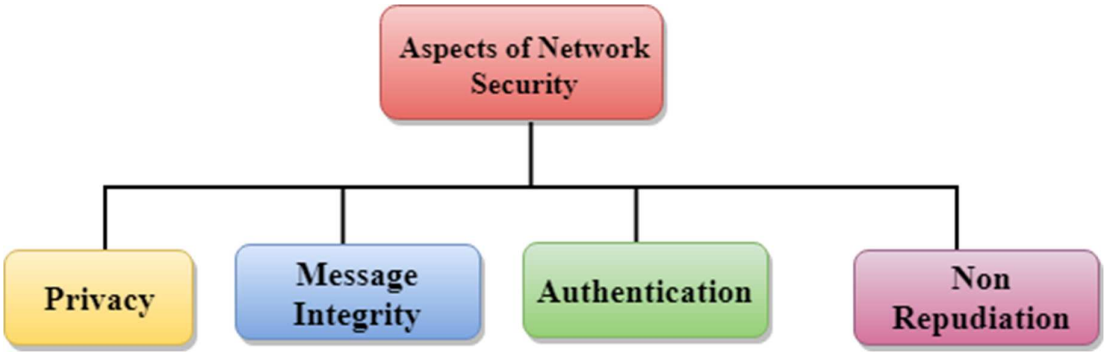
Computer network security consists of measures taken by business or some organizations to monitor and prevent unauthorized access from the outside attackers.

Different approaches to computer network security management have different requirements depending on the size of the computer network. For example, a home office requires basic network security while large businesses require high maintenance to prevent the network from malicious attacks.

Network Administrator controls access to the data and software on the network. A network administrator assigns the user ID and password to the authorized person.

Aspects of Network Security:

Following are the desirable properties to achieve secure communication:




- **Privacy:** Privacy means both the sender and the receiver expects confidentiality. The transmitted message should be sent only to the intended receiver while the message should be opaque for other users. Only the sender and receiver should be able to understand the transmitted message as eavesdroppers can intercept the message. Therefore, there is a requirement to encrypt the message so that the message cannot be intercepted. This aspect of confidentiality is commonly used to achieve secure communication.
- **Message Integrity:** Data integrity means that the data must arrive at the receiver exactly as it was sent. There must be no changes in the data content during transmission, either maliciously or accident, in a transit. As there are more and more monetary exchanges over the internet, data integrity is more crucial. The data integrity must be preserved for secure communication.
- **End-point authentication:** Authentication means that the receiver is sure of the sender's identity, i.e., no imposter has sent the message.
- **Non-Repudiation:** Non-Repudiation means that the receiver must be able to prove that the received message has come from a specific sender. The sender must not deny sending a message that he or she send. The burden of proving the identity comes on the

receiver. For example, if a customer sends a request to transfer the money from one account to another account, then the bank must have a proof that the customer has requested for the transaction.

# Privacy

The concept of how to achieve privacy has not been changed for thousands of years: the message cannot be encrypted. The message must be rendered as opaque to all the unauthorized parties. A good encryption/decryption technique is used to achieve privacy to some extent. This technique ensures that the eavesdropper cannot understand the contents of the message.

## Encryption/Decryption

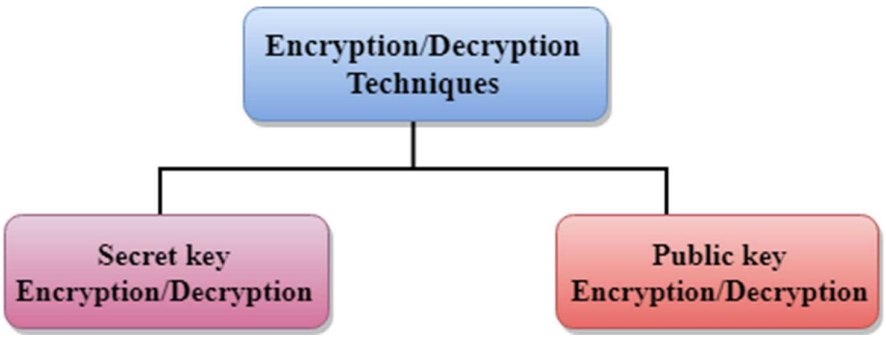
**Encryption:** Encryption means that the sender converts the original information into another form and sends the unintelligible message over the network.

**Decryption:** Decryption reverses the Encryption process in order to transform the message back to the original form.

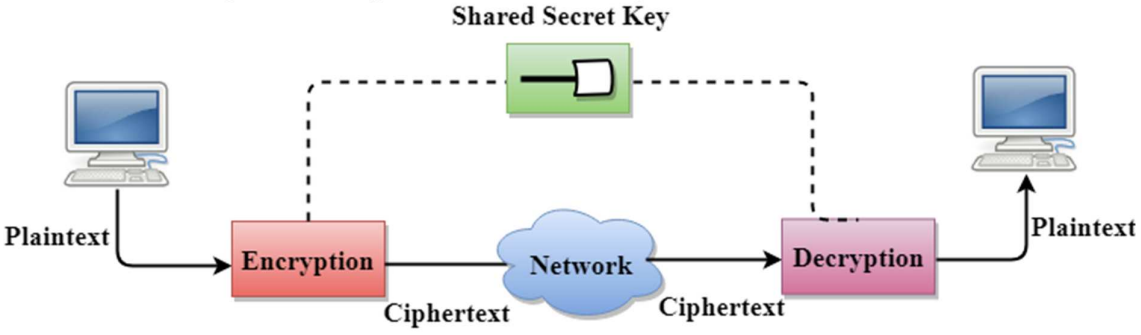
The data which is to be encrypted at the sender site is known as plaintext, and the encrypted data is known as ciphertext. The data is decrypted at the receiver site.

**There are two types of Encryption/Decryption techniques:**

- Privacy with secret key Encryption/Decryption
- Privacy with public key Encryption/Decryption




## Secret Key Encryption/Decryption technique



- In Secret Key Encryption/Decryption technique, the same key is used by both the parties, i.e., the sender and receiver.
- The sender uses the secret key and encryption algorithm to encrypt the data; the receiver uses this key and decryption algorithm to decrypt the data.
- In Secret Key Encryption/Decryption technique, the algorithm used for encryption is the inverse of the algorithm used for decryption. It means that if the encryption algorithm uses a combination of addition and multiplication, then the decryption algorithm uses a combination of subtraction and division.
- The secret key encryption algorithm is also known as symmetric encryption algorithm because the same secret key is used in bidirectional communication.
- In secret key encryption/decryption algorithm, the secret code is used by the computer to encrypt the information before it is sent over the network to another computer.
- The secret key requires that we should know which computers are talking to each other so that we can install the key on each computer.

## Data Encryption Standard (DES)

- The Data Encryption Standard (DES) was designed by IBM and adopted by the U.S. government as the standard encryption method for nonmilitary and nonclassified use.
- The Data Encryption Standard is a standard used for encryption, and it is a form of Secret **Key Cryptography**.

## Advantage

**Efficient:** The secret key algorithms are more efficient as it takes less time to encrypt the message than to encrypt the message by using a public key encryption algorithm. The reason for this is that the size of the key is small. Due to this reason, Secret Key Algorithms are mainly used for encryption and decryption.

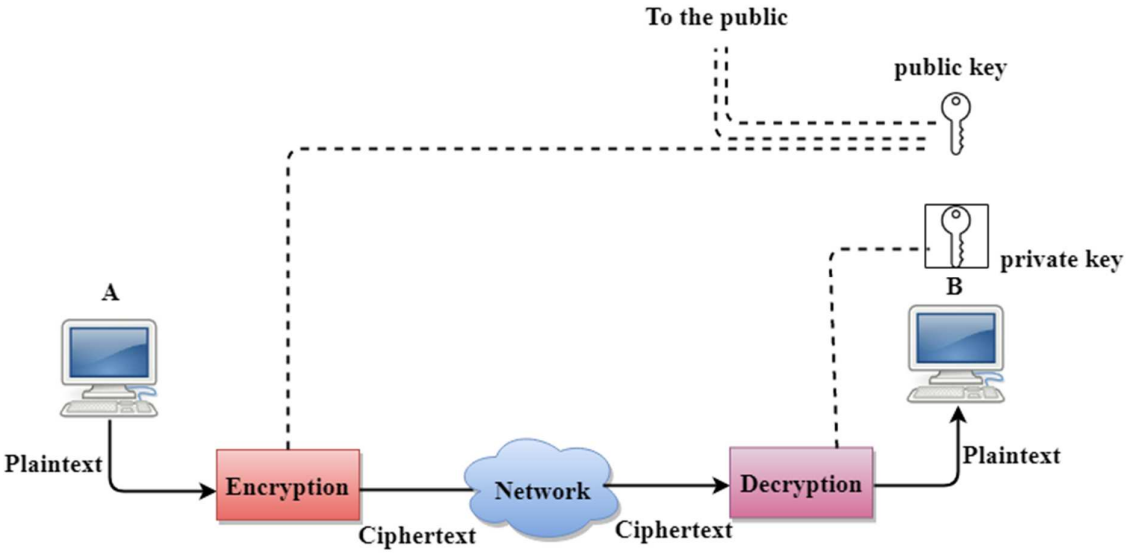
## Disadvantages of Secret Key Encryption

### The Secret Key Encryption/Decryption has the following disadvantages:

- Each pair of users must have a secret key. If the number of people wants to use this method in the world is N, then there are N(N-1)/2 secret keys. For example, for one million people, then there are half billion secret keys.
- The distribution of keys among different parties can be very difficult. This problem can be resolved by combining the Secret Key Encryption/Decryption with the Public Key Encryption/Decryption algorithm.

# Public Key Encryption/Decryption technique

- There are two keys in public key encryption: a private key and a public key.
- The private key is given to the receiver while the public key is provided to the public.




In the above figure, we see that A is sending the message to user B. 'A' uses the public key to encrypt the data while 'B' uses the private key to decrypt the data.

- In public key Encryption/Decryption, the public key used by the sender is different from the private key used by the receiver.
- The public key is available to the public while the private key is kept by each individual.
- The most commonly used public key algorithm is known as RSA.

## Advantages of Public Key Encryption

- The main restriction of private key encryption is the sharing of a secret key. A third party cannot use this key. In public key encryption, each entity creates a pair of keys, and they keep the private one and distribute the public key.
- The number of keys in public key encryption is reduced tremendously. For example, for one million users to communicate, only two million keys are required, not a half-billion keys as in the case of secret key encryption.

## Disadvantages of Public Key Encryption

- **Speed:** One of the major disadvantage of the public-key encryption is that it is slower than secret-key encryption. In secret key encryption, a single shared key is used to encrypt and decrypt the message which speeds up the process while in public key encryption, different two keys are used, both related to each other

by a complex mathematical process. Therefore, we can say that encryption and decryption take more time in public key encryption.

- **Authentication:** A public key encryption does not have a built-in authentication. Without authentication, the message can be interpreted or intercepted without the user's knowledge.
- **Inefficient:** The main disadvantage of the public key is its complexity. If we want the method to be effective, large numbers are needed. But in public key encryption, converting the plaintext into ciphertext using long keys takes a lot of time. Therefore, the public key encryption algorithms are efficient for short messages not for long messages.

## Differences b/w Secret Key Encryption & Public Key Encryption

| Basis for Comparison | Secret Key Encryption | Public Key Encryption |
|---|---|---|
| Define | Secret Key Encryption is defined as the technique that uses a single shared key to encrypt and decrypt the message. | Public Key Encryption is defined as the technique that uses two different keys for encryption and decryption. |
| Efficieny | It is efficient as this technique is recommended for large amounts of text. | It is inefficient as this technique is used only for short messages. |
| Other name | It is also known as Symmetric Key encryption. | It is also known as Asymmetric Key Encryption. |
| Speed | Its speed is high as it uses a single key for encryption and decryption. | Its speed is slow as it uses two different keys, both keys are related to each other through the complicated mathematical process. |
| Algorithms | The Secret key algorithms are DES, 3DES, AES & RCA. | The Public key algorithms are Diffie-Hellman, RSA. |
| Purpose | The main purpose of the secret key algorithm is to transmit the bulk data. | The main purpose of the public key algorithm is to share the keys securely. |

# Cryptography

**Cryptography is the science of writing in secret code so that no other person except the intended recipient could read. Cryptology has two components, kryptos and logos. Cryptographic methods to certify the safety and security of communication and main goal is user authentication, data authentication such as integrity and authentication, non-repudiation of origin, and confidentiality and it has two functions encryption and decryption.**

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. More generally, it is about constructing and analyzing protocols that overcome the influence of attackers or outside people and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Applications of cryptography include ATM cards, computer passwords.

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

## Goals of Cryptography

### The Main Goals of cryptography

- Data Privacy(confidentiality)
- Data Authenticity(it came from from where it claims)
- Data integrity(it has not been modified on the way) in the digital world

### Confidentiality

- Confidentiality is most commonly addressed goal
- The meaning of a message is concealed by encoding it
- The sender encrypts the message using a cryptographic key
- The recipient decrypts the message using a cryptographic key that may or may not be the same as the one used by the sender

### Data Integrity

- Integrity Ensures that the message received is the same as the message that was sent
- Uses hashing to create a unique message digest from the message that is sent along with the message
- Recipient uses the same technique to create a second digest from the message to compare to the original one
- This technique only protects against unintentional alteration of the message
- A variation is used to create digital signatures to protect against malicious alteration

### Authentication

- A user or system can prove their identity to another who does not have personal knowledge of their identity
- Accomplished using digital certificates
- Kerberos is a common cryptographic authentication system

## Type of cryptography

Following three common types of cryptography as below:

**Secret key cryptography** is identified as symmetric key cryptography. Both sender and receiver know same secret code described the key and messages are encrypted by the sender and use key, decrypted by the receiver. It use single key for both encryption and decryption. This method works healthy "if you are communicating with only a limited number of people, but it becomes impractical to exchange secret keys with large numbers of people". Secret key cryptography use is such as data encryption standard, advance encryption standard, Cast-128/256, international data encryption algorithm, and rivest ciphers etc. (Citrix-system, 2010)

**Public key cryptography** is called asymmetric encryption and use couple of keys one for encryption and another for decryption. Key work in pairs of coordination public and private keys. Public key can freely distributed the private key. If senders and receivers don't have to communicate keys openly, they can give private key to communication confidentially. Public key cryptography use for key exchange and digital signatures such as RSA, digital signature algorithm, public-key cryptography standard etc.

**Hash functions** use a mathematical transformation to permanently encrypt information. It also called message digests and one way encryption. Hash function use to provide a digital fingerprint of file contents and it is commonly employed by many operating system to encrypt passwords and it provide measure of the integrity of a file. It is also use message digest, secure hash algorithm, RIPEMD etc. (Kessler, G,2010)

# Network Services

**In computer networking, a network service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture based on application layer network protocols**

# Application Layer - OSI Model

It is the top most layer of OSI Model. Manipulation of data(information) in various ways is done in this layer which enables user or software to get access to the network. Some services provided by this layer includes: E-Mail, transferring files, distributing the results to user, directory services, network resources, etc.

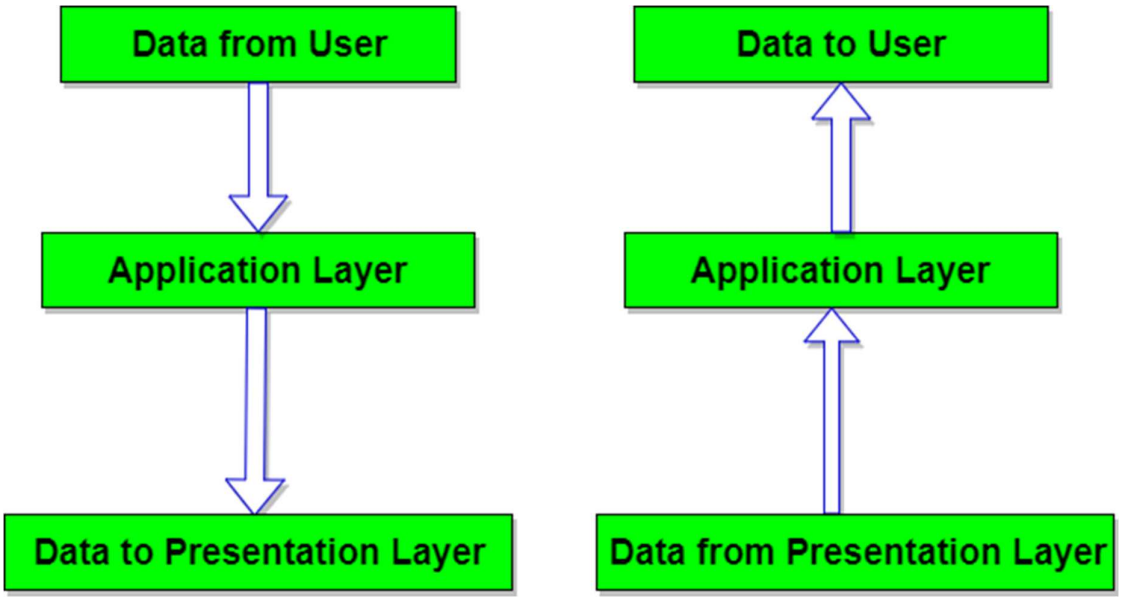
The Application Layer contains a variety of protocols that are commonly needed by users. One widely-used application protocol is **HTTP(HyperText Transfer Protocol)**, which is the basis for the World Wide Web. When a browser wants a web page, it sends the name of the page it wants to the server using HTTP. The server then sends the page back.

Other Application protocols that are used are: **File Transfer Protocol(FTP)**, **Trivial File Transfer Protocol(TFTP)**, **Simple Mail Transfer Protocol(SMTP)**, **TELNET**, **Domain Name System(DNS)** etc.

# Functions of Application Layer

1. **Mail Services:** This layer provides the basis for E-mail forwarding and storage.
2. **Network Virtual Terminal:** It allows a user to log on to a remote host. The application creates software emulation of a terminal at the remote host. User's computer talks to the software terminal which in turn talks to the host and vice versa. Then the remote host believes it is communicating with one of its own terminals and allows user to log on.
3. **Directory Services:** This layer provides access for global information about various services.

4. **File Transfer, Access and Management (FTAM):** It is a standard mechanism to access files and manages it. Users can access files in a remote computer and manage it. They can also retrieve files from a remote computer.




## FTAM (File Transfer Access and Management)

FTAM is an OSI standard that provides file transfer services between client (initiator) and server (responder) systems in an open environment. It also provides access to files and management of files on diverse systems. In these respects, it strives to be a universal file system. FTAM has worked well as a way to bring mainframe information systems into distributed environments, but FTAM has not caught on otherwise.

FTAM is designed to help users access files on diverse systems that use compatible FTAM implementations. It is similar to FTP (File Transfer Protocol) and NFS (Network File System), both of which operate in the TCP/IP environment. Users can manipulate files down to the record level, which is how FTAM stores files. In this respect, FTAM has some relational database features. For example, users can lock files or lock individual records.

FTAM is a system in which connection-oriented information about the user and the session is maintained by a server until the session is taken down. In a stateless system, such as NFS, requests are made independently of one another in a connectionless manner. There are advantages to stateless operation. If the server crashes, the request simply goes away and the client makes another request. This simplifies recovery after the crash. In a stateful system, both systems must be aware that one or the other has crashed so they can restore the states and prevent data corruption.

Files are transferred between systems by first establishing a connection-oriented session. The FTAM client contacts the FTAM server and requests a session. Once the session is established, file transfer can take place. FTAM uses the concept of a virtual file store, which provides a common view of files. The FTAM file system hides the differences between different vendor systems. FTAM specifies document types as files with straight binary information or text files in which each line is terminated with a carriage return. Data is interpreted as records and FTAM provides the virtual filestore capabilities that store record-oriented structured files.

# Electronic mail

Electronic mail, or email, is a very popular application in computer networks such as the Internet. Email appeared in the early 1970s and allows users to exchange text based messages. Initially, it was mainly used to exchange short messages, but over the years its usage has grown. It is now not only used to exchange small, but also long messages that can be composed of several parts.

# Email

Email is a service which allows us to send the message in electronic mode over the internet. It offers an efficient, inexpensive and real time mean of distributing information among people.

# E-Mail Address

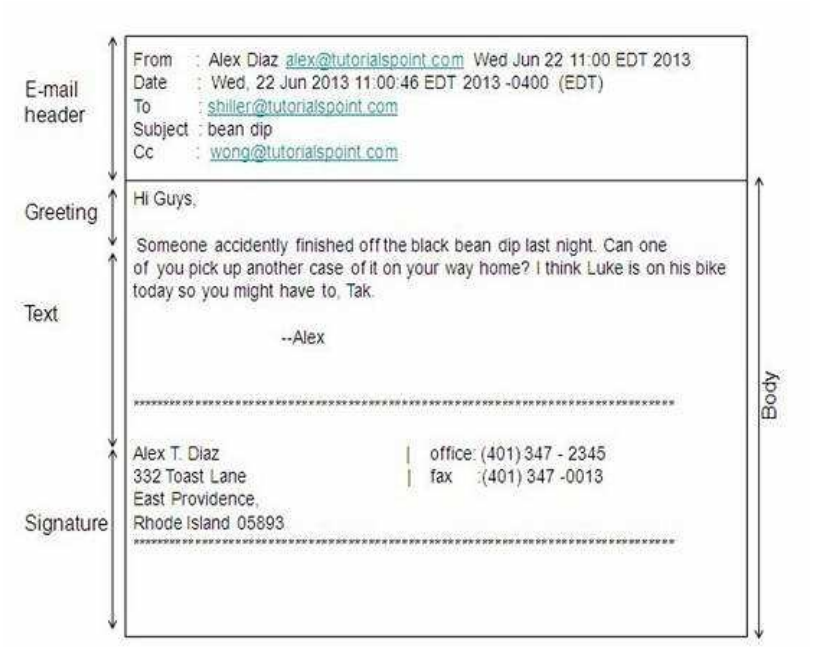
Each user of email is assigned a unique name for his email account. This name is known as E-mail address. Different users can send and receive messages according to the e-mail address.

E-mail is generally of the form username@domainname. For example, webmaster@tutorialspoint.com is an e-mail address where webmaster is username and tutorialspoint.com is domain name.

- The username and the domain name are separated by **@ (at)** symbol.
- E-mail addresses are not case sensitive.
- Spaces are not allowed in e-mail address.

## E-mail Message Components

E-mail message comprises of different components: E-mail Header, Greeting, Text, and Signature. These components are described in the following diagram:



# E-mail Header

The first five lines of an E-mail message is called E-mail header. The header part comprises of following fields:

- From
- Date
- To
- Subject
- CC
- BCC

**From**

The **From** field indicates the sender's address i.e. who sent the e-mail.

**Date**

The **Date** field indicates the date when the e-mail was sent.

**To**

The **To** field indicates the recipient's address i.e. to whom the e-mail is sent.

**Subject**

The **Subject** field indicates the purpose of e-mail. It should be precise and to the point.

**CC**

**CC** stands for Carbon copy. It includes those recipient addresses whom we want to keep informed but not exactly the intended recipient.

**BCC**

**BCC** stands for Black Carbon Copy. It is used when we do not want one or more of the recipients to know that someone else was copied on the message.

**Greeting**

Greeting is the opening of the actual message. Eg. Hi Sir or Hi Guys etc.

**Text**

It represents the actual content of the message.

**Signature**

This is the final part of an e-mail message. It includes Name of Sender, Address, and Contact Number.

## Advantages

E-mail has proved to be powerful and reliable medium of communication. Here are the benefits of **E-mail:**

- Reliable
- Convenience
- Speed
- Inexpensive
- Printable
- Global
- Generality

Reliable : Many of the mail systems notify the sender if e-mail message was undeliverable.

Convenience: There is no requirement of stationary and stamps. One does not have to go to post office. But all these things are not required for sending or receiving an mail.

Speed : E-mail is very fast. However, the speed also depends upon the underlying network.

Inexpensive : The cost of sending e-mail is very low.

Printable : It is easy to obtain a hardcopy of an e-mail. Also an electronic copy of an e-mail can also be saved for records.

Global : E-mail can be sent and received by a person sitting across the globe.

Generality : It is also possible to send graphics, programs and sounds with an e-mail.

## Disadvantages

Apart from several benefits of E-mail, there also exists some disadvantages as discussed below:

- Forgery
- Overload
- Misdirection
- Junk
- No response

# E-mail Protocols

E-mail Protocols are set of rules that help the client to properly transmit the information to or from the mail server. Here in this tutorial, we will discuss various protocols such as **SMTP, POP,** and **IMAP.**

## SMPTP

**SMTP** stands for **Simple Mail Transfer Protocol**. It was first proposed in 1982. It is a standard protocol used for sending e-mail efficiently and reliably over the internet.

**Key Points:**

- SMTP is application level protocol.
- SMTP is connection oriented protocol.
- SMTP is text based protocol.

- It handles exchange of messages between e-mail servers over TCP/IP network.
- Apart from transferring e-mail, SMPT also provides notification regarding incoming mail.
- When you send e-mail, your e-mail client sends it to your e-mail server which further contacts the recipient mail server using SMTP client.
- These SMTP commands specify the sender's and receiver's e-mail address, along with the message to be send.
- The exchange of commands between servers is carried out without intervention of any user.
- In case, message cannot be delivered, an error report is sent to the sender which makes SMTP a reliable protocol.

## SMTP Commands

The following table describes some of the SMTP commands:

| S.N. | Command Description |
|---|---|
| 1 | **HELLO**<br>This command initiates the SMTP conversation. |
| 2 | **EHELLO**<br>This is an alternative command to initiate the conversation. ESMTP indicates that the sender server wants to use extended SMTP protocol. |
| 3 | **MAIL FROM**<br>This indicates the sender's address. |
| 4 | **RCPT TO**<br>It identifies the recipient of the mail. In order to deliver similar message to multiple users this command can be repeated multiple times. |
| 5 | **SIZE**<br>This command let the server know the size of attached message in bytes. |
| 6 | **DATA**<br>The **DATA** command signifies that a stream of data will follow. Here stream of data refers to the body of the message. |
| 7 | **QUIT**<br>This commands is used to terminate the SMTP connection. |
| 8 | **VERFY**<br>This command is used by the receiving server in order to verify whether the given username is valid or not. |
| 9 | **EXPN**<br>It is same as VRFY, except it will list all the users name when it used with a distribution list. |

# IMAP

**IMAP** stands for **Internet Message Access Protocol.** It was first proposed in 1986. There exist five versions of IMAP as follows:

1. Original IMAP

2. IMAP2
3. IMAP3
4. IMAP2bis
5. IMAP4

**Key Points:**

- IMAP allows the client program to manipulate the e-mail message on the server without downloading them on the local computer.
- The e-mail is hold and maintained by the remote server.
- It enables us to take any action such as downloading, delete the mail without reading the mail.It enables us to create, manipulate and delete remote message folders called mail boxes.
- IMAP enables the users to search the e-mails.
- It allows concurrent access to multiple mailboxes on multiple mail servers.

# IMAP Commands

The following table describes some of the IMAP commands:

| S.N. | Command Description |
|---|---|
| 1 | **IMAP_LOGIN**<br>This command opens the connection. |
| 2 | **CAPABILITY**<br>This command requests for listing the capabilities that the server supports. |
| 3 | **NOOP**<br>This command is used as a periodic poll for new messages or message status updates during a period of inactivity. |
| 4 | **SELECT**<br>This command helps to select a mailbox to access the messages. |
| 5 | **EXAMINE**<br>It is same as SELECT command except no change to the mailbox is permitted. |
| 6 | **CREATE**<br>It is used to create mailbox with a specified name. |
| 7 | **DELETE**<br>It is used to permanently delete a mailbox with a given name. |
| 8 | **RENAME**<br>It is used to change the name of a mailbox. |
| 9 | **LOGOUT**<br>This command informs the server that client is done with the session. The server must send BYE untagged response before the OK response and then close the network connection. |

# POP

POP stands for Post Office Protocol. It is generally used to support a single client. There are several versions of POP but the POP 3 is the current standard.

**Key Points**

- POP is an application layer internet standard protocol.
- Since POP supports offline access to the messages, thus requires less internet usage time.
- POP does not allow search facility.
- In order to access the messaged, it is necessary to download them.
- It allows only one mailbox to be created on server.
- It is not suitable for accessing non mail data.
- POP commands are generally abbreviated into codes of three or four letters. Eg. STAT.

## POP Commands

The following table describes some of the POP commands:

| S.N. | Command Description |
|---|---|
| 1 | **LOGIN**<br>This command opens the connection. |
| 2 | **STAT**<br>It is used to display number of messages currently in the mailbox. |
| 3 | **LIST**<br>It is used to get the summary of messages where each message summary is shown. |
| 4 | **RETR**<br>This command helps to select a mailbox to access the messages. |
| 5 | **DELE**<br>It is used to delete a message. |
| 6 | **RSET**<br>It is used to reset the session to its initial state. |
| 7 | **QUIT**<br>It is used to log off the session. |

# Comparison between POP and IMAP

| S.N. | POP | IMAP |
|---|---|---|
| 1 | Generally used to support single client. | Designed to handle multiple clients. |
| 2 | Messages are accessed offline. | Messages are accessed online although it also supports offline mode. |
| 3 | POP does not allow search facility. | It offers ability to search emails. |

| | | |
|---|---|---|
| 4 | All the messages have to be downloaded. | It allows selective transfer of messages to the client. |
| 5 | Only one mailbox can be created on the server. | Multiple mailboxes can be created on the server. |
| 6 | Not suitable for accessing non-mail data. | Suitable for accessing non-mail data i.e. attachment. |
| 7 | POP commands are generally abbreviated into codes of three or four letters. Eg. STAT. | IMAP commands are not abbreviated, they are full. Eg. STATUS. |
| 8 | It requires minimum use of server resources. | Clients are totally dependent on server. |
| 9 | Mails once downloaded cannot be accessed from some other location. | Allows mails to be accessed from multiple locations. |
| 10 | The e-mails are not downloaded automatically. | Users can view the headings and sender of e-mails and then decide to download. |
| 10 | POP requires less internet usage time. | IMAP requires more internet usage time. |

## E-mail System

E-mail system comprises of the following three components:

- Mailer
- Mail Server
- Mailbox

### Mailer

It is also called **mail program, mail application** or **mail client.** It allows us to manage, read and compose e-mail.

## Mail Server

The function of mail server is to receive, store and deliver the email. It is must for mail servers to be Running all the time because if it crashes or is down, email can be lost.

## Mailboxes

Mailbox is generally a folder that contains emails and information about them.

### Working of E-mail

Email working follows the client server approach. In this client is the mailer i.e. the mail application or mail program and server is a device that manages emails.

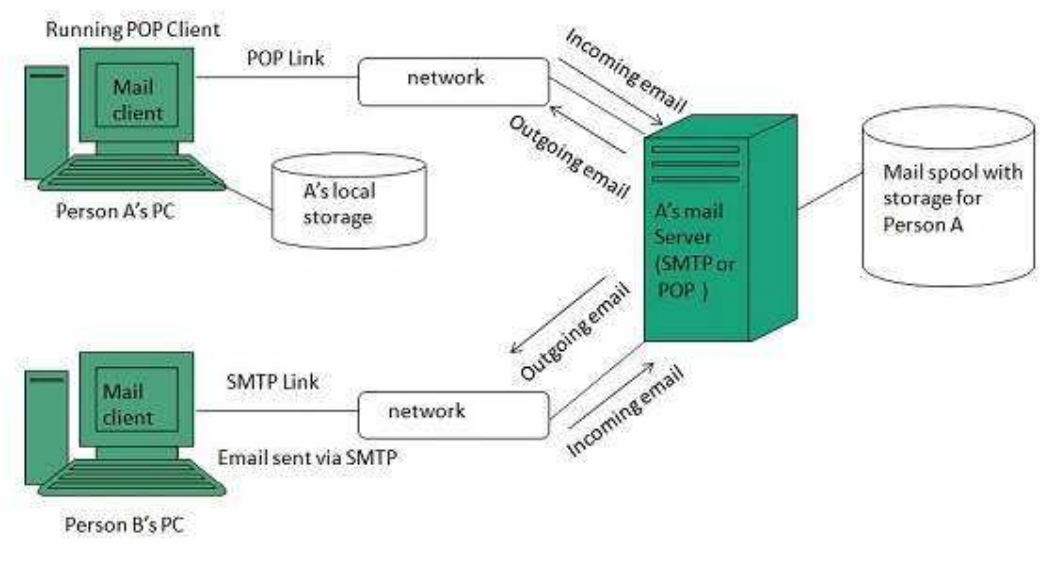
Following example will take you through the basic steps involved in sending and receiving emails and will give you a better understanding of working of email system:

- Suppose person A wants to send an email message to person B.
- Person A composes the messages using a mailer program i.e. mail client and then select Send option.
- The message is routed to **Simple Mail Transfer Protocol** to person B's mail server.
- The mail server stores the email message on disk in an area designated for person B.

The disk space area on mail server is called mail spool.

- Now, suppose person B is running a POP client and knows how to communicate with B's mail server.
- It will periodically poll the POP server to check if any new email has arrived for B.As in this case, person B has sent an email for person B, so email is forwarded over the network to B's PC. This is message is now stored on person B's PC.

The following diagram gives pictorial representation of the steps discussed above:




# E-mail Security

## E-mail Hacking

Email hacking can be done in any of the following ways:

- Spam
- Virus
- Phishing

## Spam

E-mail spamming is an act of sending **Unsolicited Bulk E-mails (UBI)** which one has not asked for. Email spams are the junk mails sent by commercial companies as an advertisement of their products and services.

# Virus

Some emails may incorporate with files containing malicious script which when run on your computer may lead to destroy your important data.

# Phishing

Email phishing is an activity of sending emails to a user claiming to be a legitimate enterprise. Its main purpose is to steal sensitive information such as usernames, passwords, and credit card details.

Such emails contains link to websites that are infected with malware and direct the user to enter details at a fake website whose look and feels are same to legitimate one.

## E-mail Spamming and Junk Mails

Email spamming is an act of sending Unsolicited Bulk E-mails (UBI) which one has not asked for. Email spams are the junk mails sent by commercial companies as an advertisement of their products and services.

Spams may cause the following problems:

- It floods your e-mail account with unwanted e-mails, which may result in loss of important e-mails if inbox is full.
- Time and energy is wasted in reviewing and deleting junk emails or spams.
- It consumes the bandwidth that slows the speed with which mails are delivered.
- Some unsolicited email may contain virus that can cause harm to your computer.

## Blocking Spams

Following ways will help you to reduce spams:

- While posting letters to newsgroups or mailing list, use a separate e-mail address than the one you used for your personal e-mails.
- Don’t give your email address on the websites as it can easily be spammed.
- Avoid replying to emails which you have received from unknown persons.
- Never buy anything in response to a spam that advertises a product.

## E-mail Cleanup and Archiving

In order to have light weighted Inbox, it’s good to archive your inbox from time to time. Here I will discuss the steps to clean up and archive your Outlook inbox.

- Select **File** tab on the mail pane.
- Select **Cleanup Tools** button on account information screen.
- Select **Archive** from cleanup tools drop down menu.
- Select **Archive this folder and all subfolders** option and then click on the folder that you want to archive. Select the date from the **Archive items older than:** list. Click **Browse** to create new **.pst** file name and location. Click **OK.**

# Remote Login

**Remote Login** is a process in which user can login into remote site i.e. computer and use services that are available on the remote computer. With the help of remote login a user is able to understand result of transferring result of processing from the remote computer to the local computer.

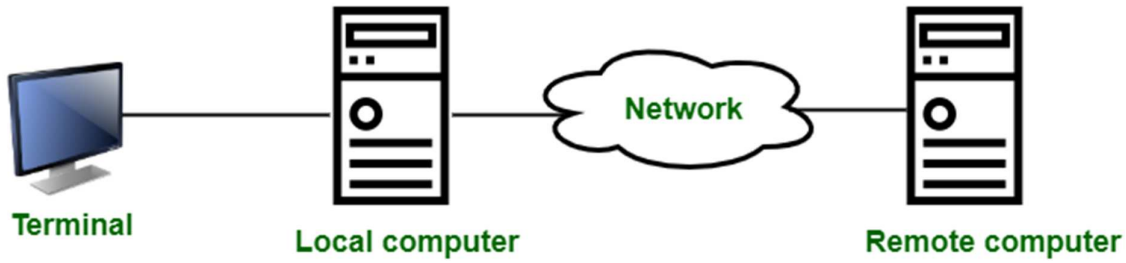



**Figure –** Remote login

It is implemented using Telnet.

**Procedure of Remote Login :**

1. When the user types something on local computer, then local operating system accepts character.
2. Local computer does not interpret the characters, it will send them to TELNET client.
3. TELNET client transforms these characters to a universal character set called **Network Virtual Terminal (NVT) characters** and it will pass them to the local TCP/IP protocol Stack.
4. Commands or text which is in the form of NVT, travel through Internet and it will arrive at the TCP/IP stack at remote computer.
5. Characters are then delivered to operating system and which later on passed to TELNET server.
6. Then TELNET server changes that characters to characters which can be understandable by remote computer.
7. Remote operating system receives character from a **pseudo-terminal driver**, which is a piece of software that pretends that characters are coming from a terminal.
8. Operating system then passes character to the appropriate application program.

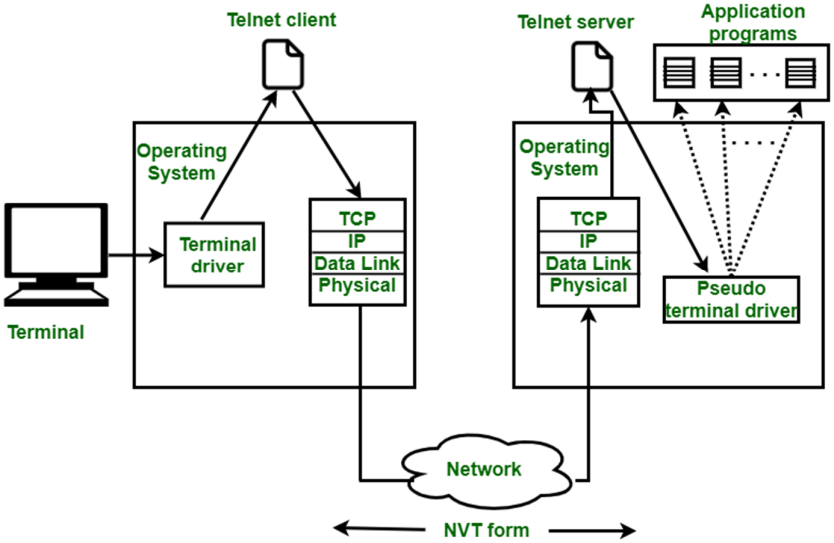



**Figure –** Remote login procedure