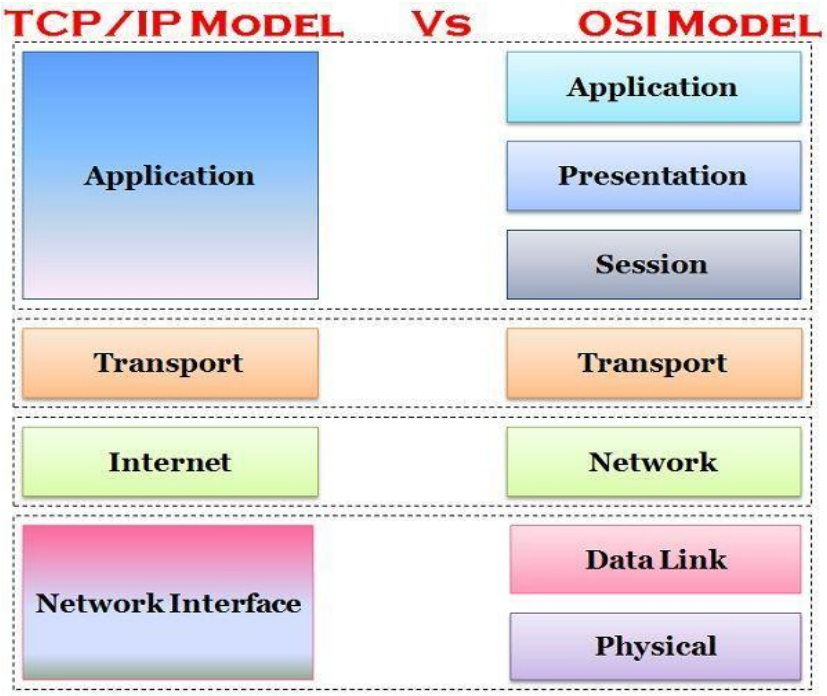
Module 5: Application Layer

- Introduction, providing services, Client server model, Standard client-server application-HTTP, DNS, SSH.

- Malware Detection System, Types of Malware, Viruses & Countermeasures, Worms, Bots. E-mail Security: PGP, S/MIME.


TCP/IP MODEL
Vs
OSI MODEL
Application
Application
Presentation
Session
Transport
Transport
Internet
Network
Network Interface
Data Link
Physical

Introduction

- Application layer is the top most layer in OSI (Layer 7) and TCP/IP (Layer 5).
- This layer is for applications which are involved in communication systems.
- Communication is provided using logical connection.
- The application layer and the end user can communicate with software applications and protocols.

Application layer

The application layer in the OSI model is the closest layer to the end user which means that the application layer and end user can interact directly with the software application.

The application layer programs are based on client and servers.

This layer also serves as a window for the application services to access the network and for displaying the received information to the user. Ex: Application – Browsers, Skype Messenger etc.

Example: Web Browsers

Functions of Application layer

The Application layer includes the following functions:

- **Identifying communication partners:** The application layer identifies the availability of communication partners for an application with data to transmit.
- **Determining resource availability:** The application layer determines whether sufficient network resources are available for the requested communication.
- **Synchronizing communication:** All the communications occur between the applications requires cooperation which is managed by an application layer.

Services of Application Layers

- **Network Virtual terminal:** An application layer allows a user to log on to a remote host.
- **File Transfer, Access, and Management (FTAM):** An application allows a user to access files in a remote computer, to retrieve files from a computer and to manage files in a remote computer.
- **Addressing:** When a client made a request to the server, the request contains the server address and its own address.
- **Mail Services:** An application layer provides Email forwarding and storage.

Services of Application Layers contd..

- **Directory Services:** An application contains a distributed database that provides access for global information about various objects and services.
- **Authentication**: It authenticates the sender or receiver's message or both.

Standard & Non-Standard Protocols

- To provide smooth operation of the Internet, protocols used in four layers need to be standardized and documented.

- They normally become part of the package that is included in the operating systems.

- Application-layer protocols can be standard or non standard.

Standard Application-Layer Protocols

- Several Protocols are standardized and documented by Internet Authorities.
- Each protocol is a software that interacts with user and the transport layer to provide the service.
- Ex: HTTP, HTTPS, DNS

Non-Standard Application Layer Protocols

- A Non-Standard protocol, does not need approval of Internet authorities.
- Used privately for communication.
- A private company can create a new customized application protocol for communication.

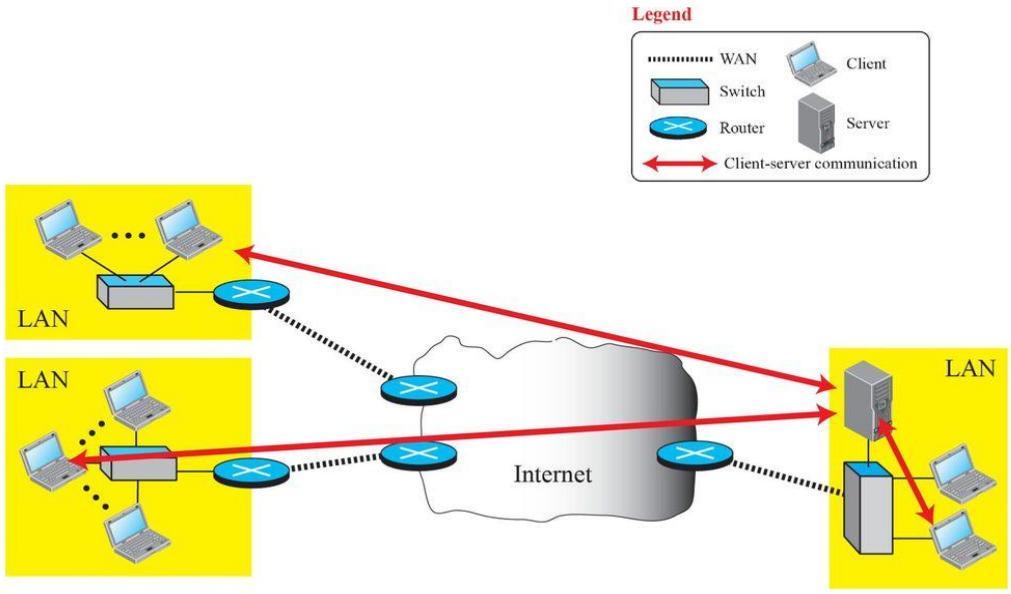
Application Layer Paradigms

- To use the internet, there is a need for two application programs located in two different places.
  - One running on a computer somewhere in the world
  - Another running on a computer somewhere else
- The relationship between these two programs can be of the following:
  - Client-Server Paradigm
  - Peer-to-Peer Paradigm
  - Mixed Paradigm

Traditional Paradigm: Client - Server

- Most popular paradigm.
- The service provider is an application program called Server.
- Server continuously wait for another application program called Client.
- Client makes a connection through the internet and ask for the service.
- Server process must be running all the time.
- Client process runs only when it needs to receive the service.

Figure 25.2: Example of a client-server paradigm



Characteristics Of Client-server architecture

- In Client-server architecture, clients do not directly communicate with each other. For example, in a web application, two browsers do not directly communicate with each other.
- A server is fixed, well-known address known as IP address because the server is always on while the client can always contact the server by sending a packet to the sender's IP address.

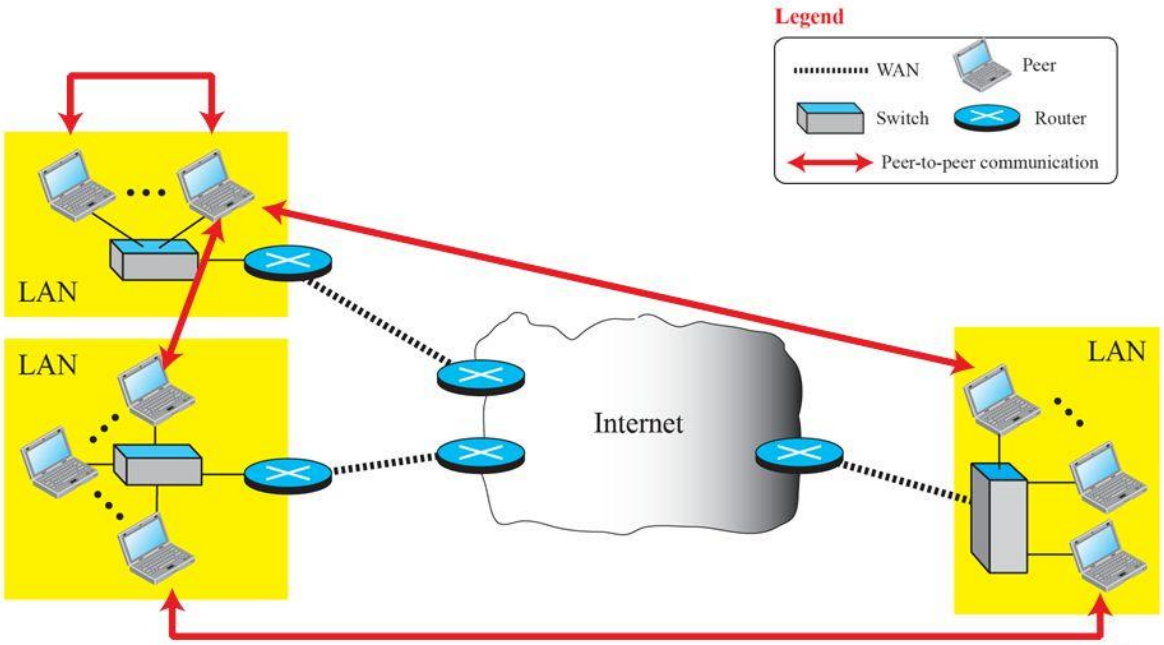
Disadvantages

- The whole communication depends on the server.
- If the server fails, none of the requests can be processed.
- There must be a service provider willing to accept the cost to create a powerful server for a specific service.
- If all the clients request simultaneously, server may get overloaded.

New Paradigm: Peer-to-Peer

- No need of server processes waiting for clients.
- Responsibility is shared between the peers.
- Ex 1 : Telephone System, sharing a file.
- Ex 2 : Skype, BitTorrent.
- Disadvantages:
  - Difficult to create secure communication.
  - Not all applications can use this paradigm.

Figure 25.3: Example of a peer-to-peer paradigm



P2P (peer-to-peer) architecture

It has no dedicated server in a data center.

The peers are the computers which are not owned by the service provider.

Most of the peers reside in the homes, offices, schools, and universities.

The peers communicate with each other without passing the information through a dedicated server, this architecture is known as peer-to-peer architecture.

The applications based on P2P architecture includes file sharing and internet telephony.

Features of P2P architecture

Self scalability: In a file sharing system, although each peer generates a workload by requesting the files, each peer also adds a service capacity by distributing the files to the peer.

Cost-effective: It is cost-effective as it does not require significant server infrastructure and server bandwidth.

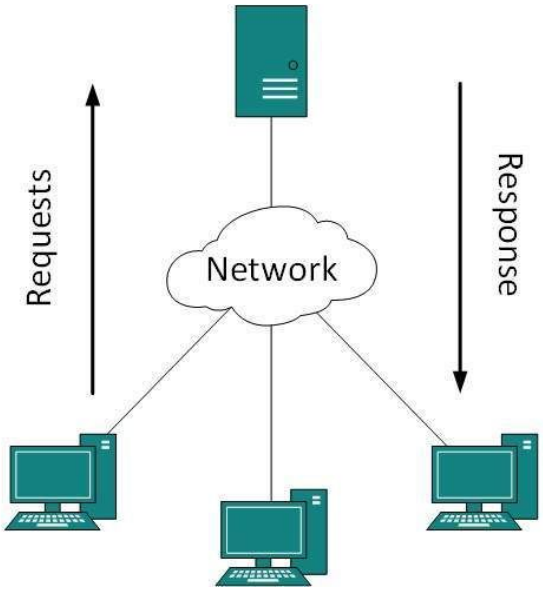
Mixed Paradigm

- An application may choose to use a mixture of any of the two paradigms.

Client Server Model

- Client-Server model is a network architecture that describes how servers interact with network devices.
- In this mode of interaction a program sends a request to another program and awaits for a response.
- Requesting program is called client.
- Answering program is called server.

Client Server Model



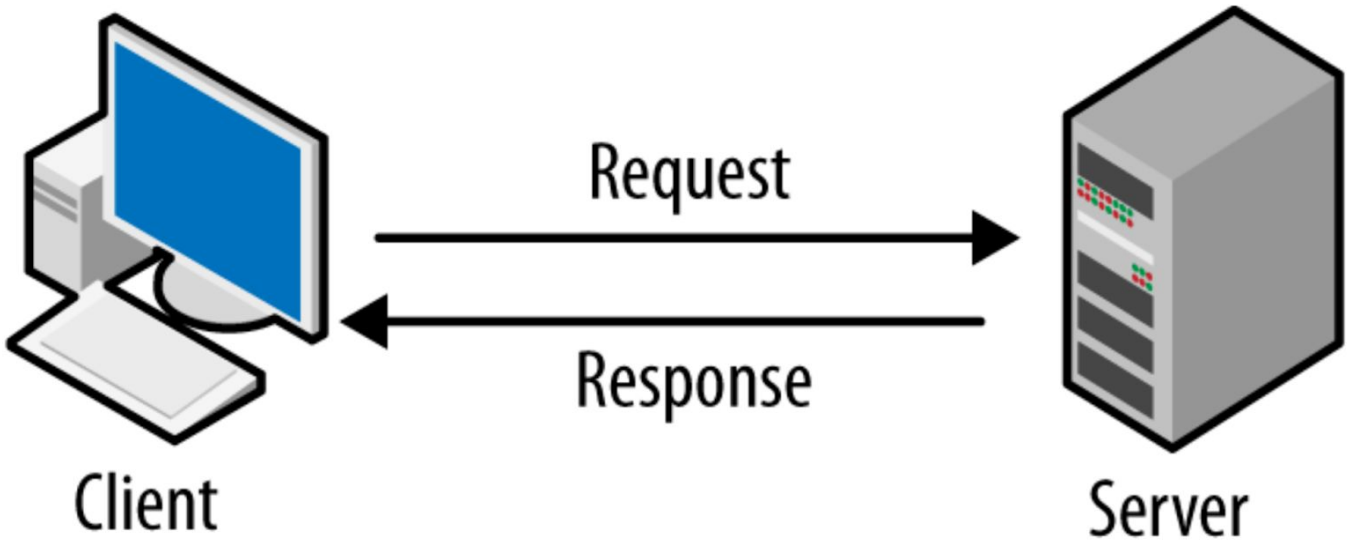
Components of Client Server Model

- The main three components of Client-Server Model are:
  - Client
  - Server
  - Networking devices.

Components of Client Server Model

- Client
  - Computer that connects to and uses the resources of a remote computer or server. Resources can be files, information, internet, processing power etc.
- Server
  - Computer that provides services to the network.
- Networking devices
  - Physical and wireless networking devices like hubs, switches, routers etc.

Working of Client-Server Model



Examples

- Mail Servers:
  - Used for sending and receiving emails.
- File Servers
  - Centralized location for the files (cloud)
- Web Servers
  - Servers hosting different websites.

Advantages

- Centralized
- Security
- Performance
- scalability

Disadvantages

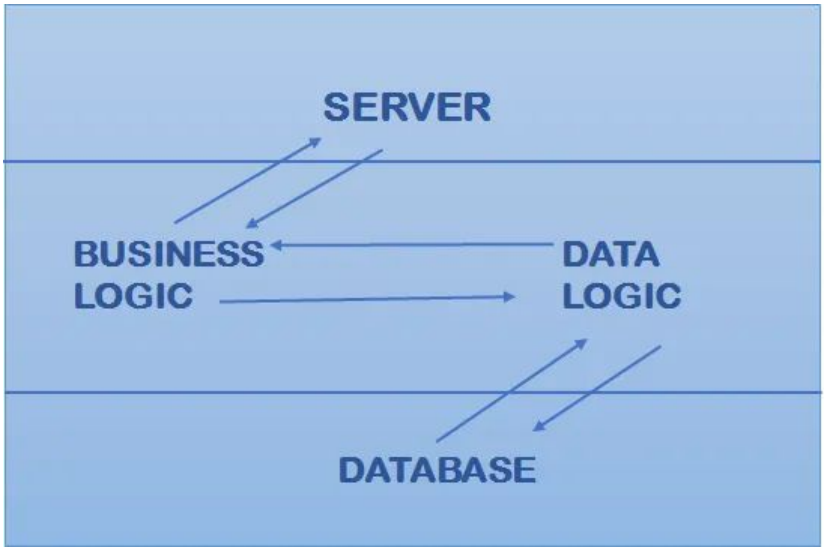
- Clients are prone to virus, can be uploaded into the server.
- Servers are prone to DoS attack.

Types of Client-Server Architecture

- There are different types of architecture in client-server model:
  - 1-tier Architecture
  - 2-tier Architecture
  - 3-tier Architecture
  - N-tier Architecture

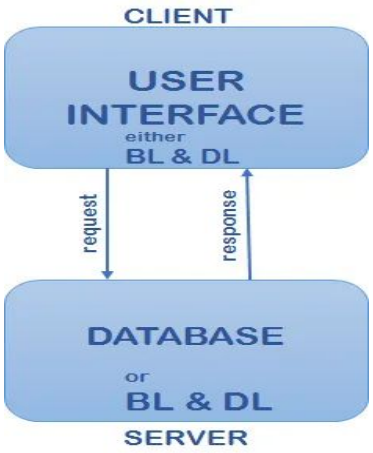
1-tier Architecture

- All client or server configuration settings, UI environment, data logic is on the same system.
- Ex: MS office, MP3 player



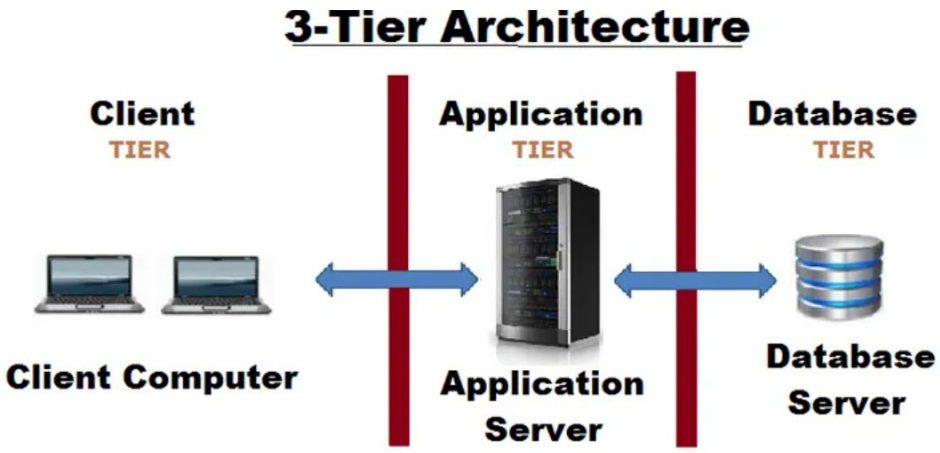
2-tier Architecture

- UI is stored in client machine and database is in server.
- Ex: Online ticket reservation system



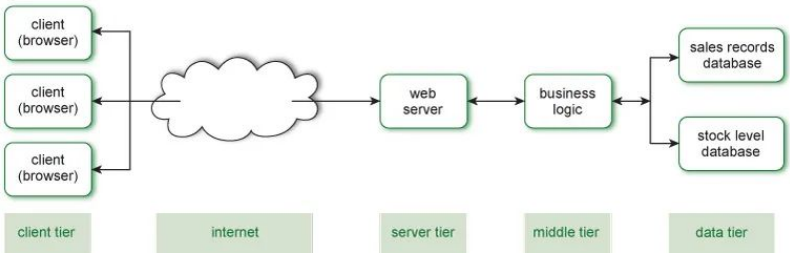
3-tier Architecture

- Contains middleware, and request sent by client is processed by middle layer and request is given to server.



N-Tier Architecture

- Also known as Multi Tier Architecture.



HTTP

- HTTP stands for **Hyper Text Transfer Protocol**.
- It is a protocol used to access the data on the World Wide Web (WWW).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- HTTP transfers the files from one host to another host.

HTTP

- HTTP is an application Layer protocol, used to retrieve web pages from the web.
- A HTTP client sends a request and a HTTP server returns a response.
- HTTP uses TCP which is connection-oriented and reliable protocol.
- A connection is established before communication and the connection is terminated after communication.

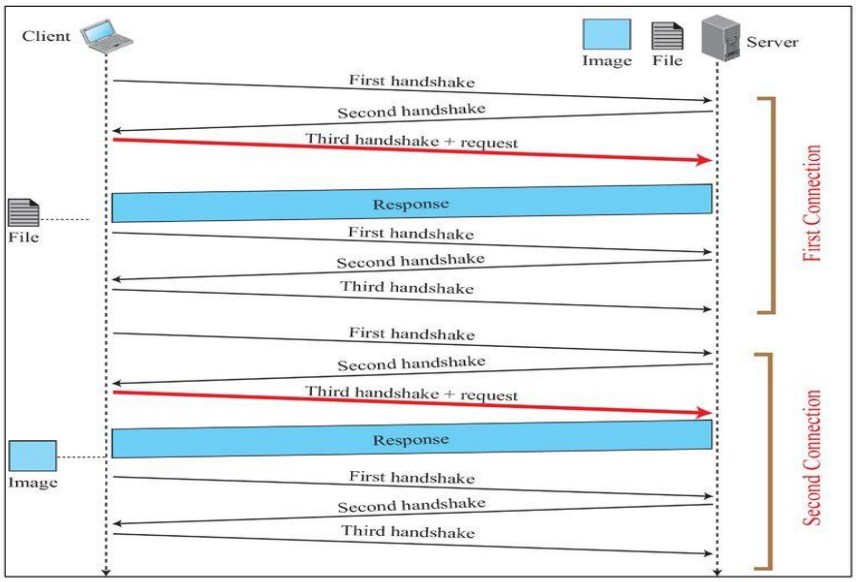
Persistent and Non-persistent Connections

- To retrieve a web object, a TCP connection is made.
- If the objects are located on different servers, then different connections are established.
- However, if the objects are located on same server, then any of these two following can happen:
  - Retrieve each object using new TCP connection (Non-persistent).
  - Make a single TCP connection and retrieve all the objects (Persistent).

Non-persistent Connection

- In a non-persistent connection, one TCP connection is made for each request/response.
- Earlier to HTTP 1.1, specified non-persistent connections.
- The following steps happen:
  - Client opens a TCP connection and sends a request.
  - Server sends the response and closes the connection.
  - Client reads the data with EOF marker and closes the connection.

Non-persistent Connection



Persistent Connections

- HTTP version 1.1, specifies persistent connection by default. It can be changed by the user.
- In this mode of connection, server leaves the connection open for more requests after sending a response.
- Server closes the connection at the request of a client or because of time out.
- Time and resources are saved using these connections.

Persistent Connections

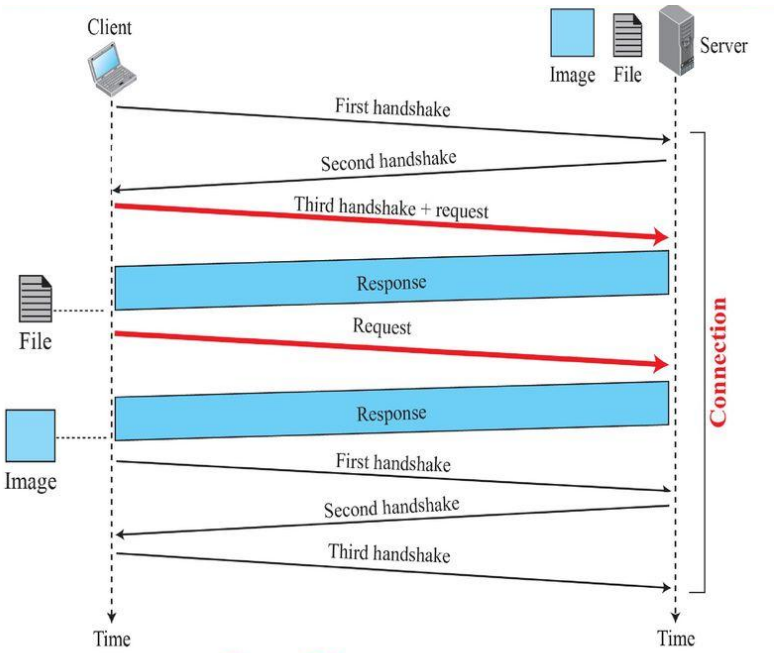
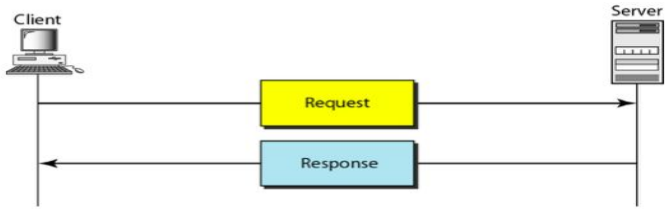


Figure 26.4: ***Example 26.4***

HTTP Transactions

- The client initiates a transaction by sending a request message to the server.
- The server replies to the request message by sending a response message.

Figure 27.12 *HTTP transaction*



Messages

HTTP messages are of two types: request and response. Both the message types follow the same message format.

Request Message: The request message is sent by the client that consists of a request line, headers, and sometimes a body.

Response Message: The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.

Domain Name System

- DNS Overview:-
- Uses:-
- Domain Name:-
- Name Server:-
- Types of DNS:-
  1)Generic Domain:
  2)Country Domain:
  3)Inverse Domain:

DNS Overview

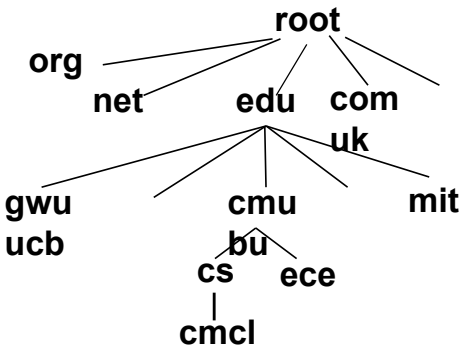
- On the Internet, the **Domain Name System** (DNS) associates various sorts of information with domain names
  - Serves as the "phone book" for the Internet
  - Translates human-readable computer hostnames into IP addresses
    - Required by networking equipment to delivering information
  - Also stores other information
    - Such as the list of mail exchange servers that accept email for a given domain.
    - By providing a worldwide keyword-based redirection service, the Domain Name System is an essential component of the modern Internet

DNS:-

- It stands for domain name system.
- The naming scheme used in the internet is called DNS.
- To identify an entity the internet uses the IP address.
- Which identifies connection of computer to internet.
- But user to use names of numeric address because to remember numeric address are difficult compare to names.

- We need a system that can map a name to an address or an address to name.
- So, the naming scheme used in the internet is called the DNS.
- In DNS name must be unique because the address are unique.
- In DNS names are defined in an inverted tree structure with the root at the top.

- Fig:- DNS



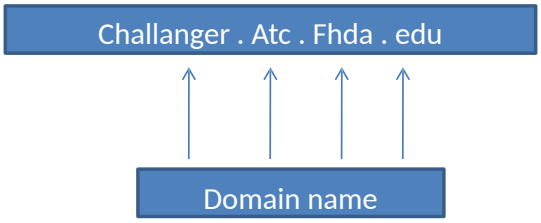
- Each node has maximum 63 character.

Uses:

- The most basic use of DNS is to translate hostnames to IP addresses.
  - Very much like a phone book
  - For example, what is the internet address of en.wikipedia.org?
    - The Domain Name System can be used to tell you it is 66.230.200.100

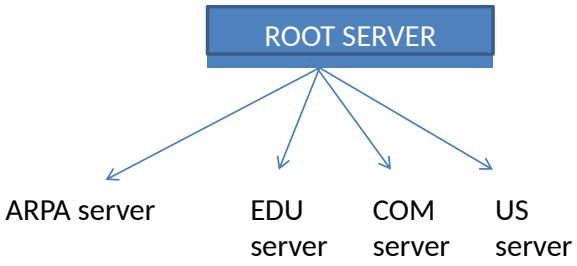
Domain Name:

- Each node in the tree has a domain name.
- It is separated by dots.
- Ex:-



Name Server:

- Distribute the information among computer called DNS server.
- DNS allows domain to be divided future into smaller domains.
- Each server can responsible for domain.

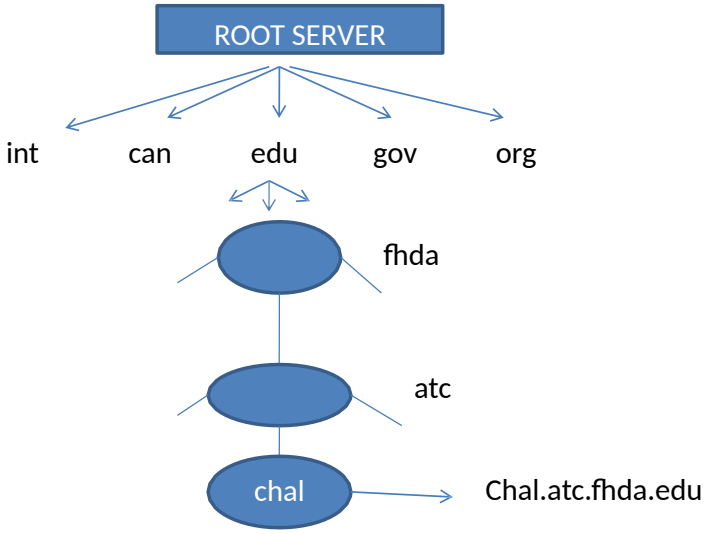


TYPES:

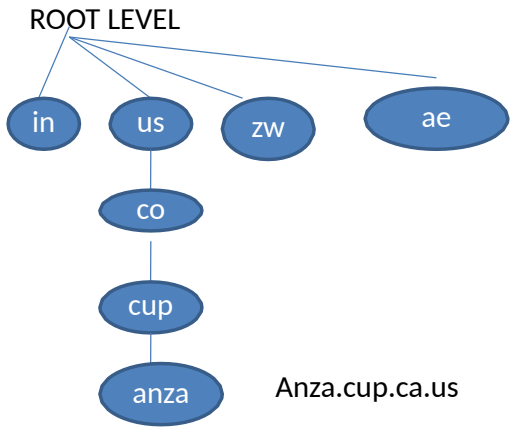
Generic Domain:-

- It defines registered hosts according to their behavior.
- Each node in the tree defines a domain.
- It has node 3 character name.

- Fig:-


ROOT SERVER
int
can
edu
gov
org
fhda
atc
chal
Chal.atc.fhda.edu

- Country Domain:- It uses two character country abbreviation in place of three character abbreviation at first level.



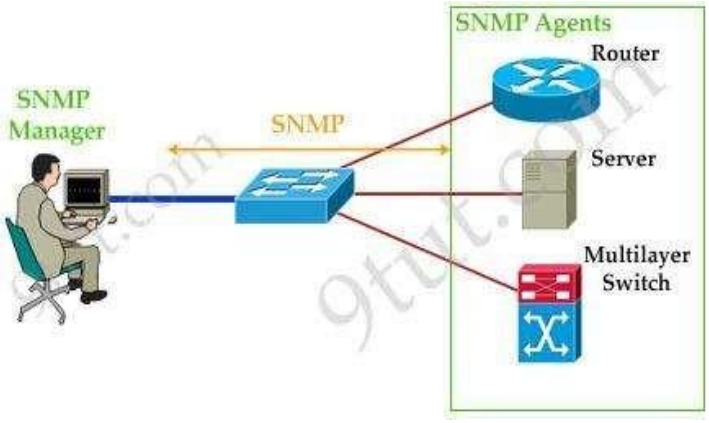
Inverse Domain:-

- It used to map an address to a name.
- The inverse domain is to the domain name space with the first level node called ARPA(advanced research project agency).
- The second level is also one single node named in-addr(for inverse address).
- The rest of the domain defines IP address.
- For EX: 121.45.34.132.in-addr.arpa

What is SNMP?

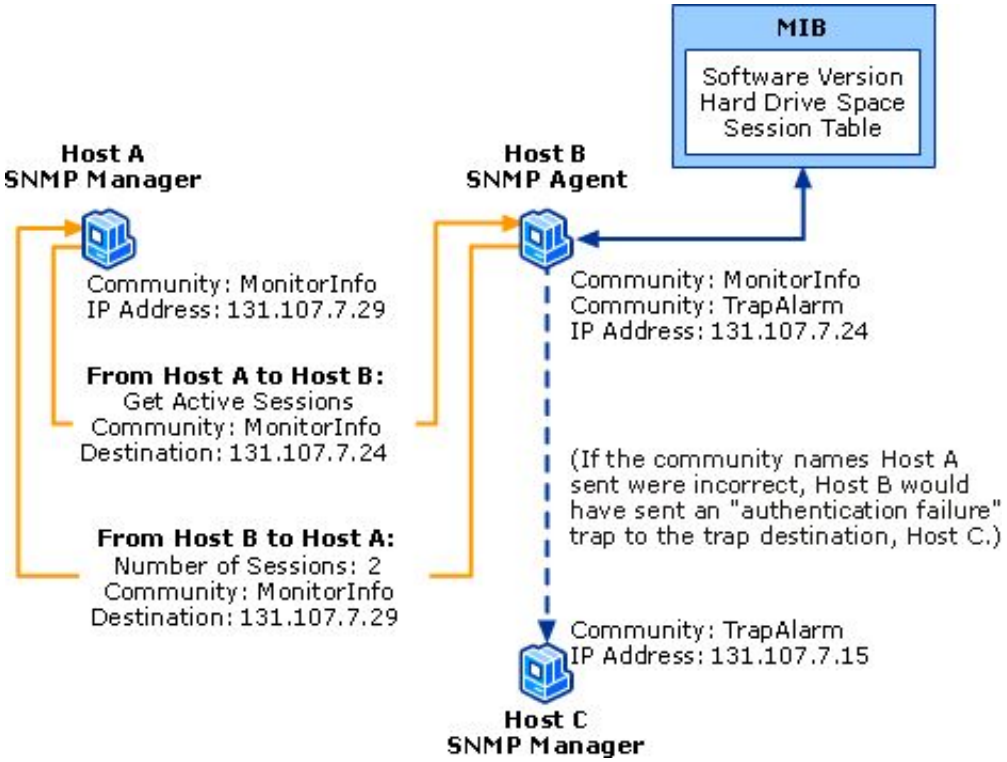
- The Simple Network Management Protocol (SNMP) is a framework for managing devices in an internet using the TCP/IP protocol suite. It provides a set of fundamental operations for monitoring and maintaining an internet

- Comprised of agents and managers
  - Agent - process running on each managed node collecting information about the device it is running on.
  - Manager - process running on a management workstation that requests information about devices on the network.



- SNMP is Simple Network Management Protocol. This network protocol is used to monitor the health status, disk utilisation, temprature, no of cpu’s and other parameters of a network device. These network device can be a router, switch, load-balancer, server, etc. For SNMP there has to be a server which listens on UDP port 514.

- SNMP is based on three basic ideas.
  - A manager checks an agent by requesting information that reflects the behavior of the agent.
  - A manager forces an agent to perform a task by resetting values in the agent database.
  - An agent contributes to the management process by warning the manager of an unusual situation.


MIB
Software Version
Hard Drive Space
Session Table
Host A
SNMP Manager
Host B
SNMP Agent
Community: MonitorInfo
IP Address: 131.107.7.29
From Host A to Host B:
Get Active Sessions
Community: MonitorInfo
Destination: 131.107.7.24
From Host B to Host A:
Number of Sessions: 2
Community: MonitorInfo
Destination: 131.107.7.29
Community: MonitorInfo
Community: TrapAlarm
IP Address: 131.107.7.24
(If the community names Host A sent were incorrect, Host B would have sent an "authentication failure" trap to the trap destination, Host C.)
Community: TrapAlarm
IP Address: 131.107.7.15
Host C
SNMP Manager

Advantages of using SNMP

- Standardized
- Universally supported
- Extendible
- Portable
- Allows distributed management access
- Lightweight protocol

Client Pull & Server Push

- SNMP is a “client pull” model
  - The management system (client) “pulls” data from the agent (server).

- SNMP is a “server push” model
  - The agent (server) “pushes” out a trap message to a (client) management system

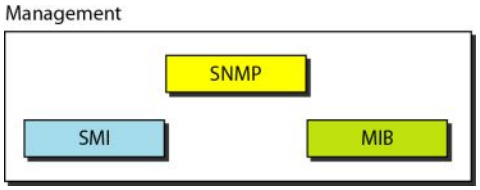
Ports & UDP

- SNMP uses User Datagram Protocol (UDP) as the transport mechanism for SNMP messages

- Like FTP, SNMP uses two well-known ports to operate:
  - **UDP Port 161** - SNMP Messages
  - **UDP Port 162** - SNMP Trap Messages

The Three Parts of SNMP

- SNMP network management is based on three parts:



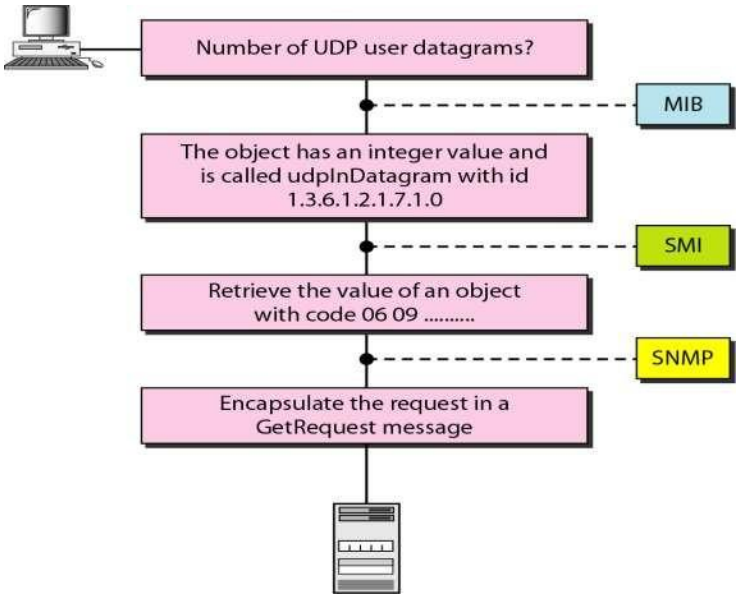
  - **SNMP Protocol**
    - Defines format of messages exchanged by management systems and agents.
    - Specifies the Get, GetNext, Set, and Trap operations
  - **Structure of Management Information (SMI)**
    - Rules specifying the format used to define objects managed on the network that the SNMP protocol accesses
  - **Management Information Base (MIB)**
    - A map of the hierarchical order of all managed objects and how they are accessed

Role of SMI

- SMI defines the general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values. SMI does not define the number of objects an entity should manage or name the objects to be managed or define the association between the objects and their values.

Role of MIB

MIB creates a collection of named objects, their types, and their relationships to each other in an entity to be managed.



SMTP

Simple Mail Transfer Protocol

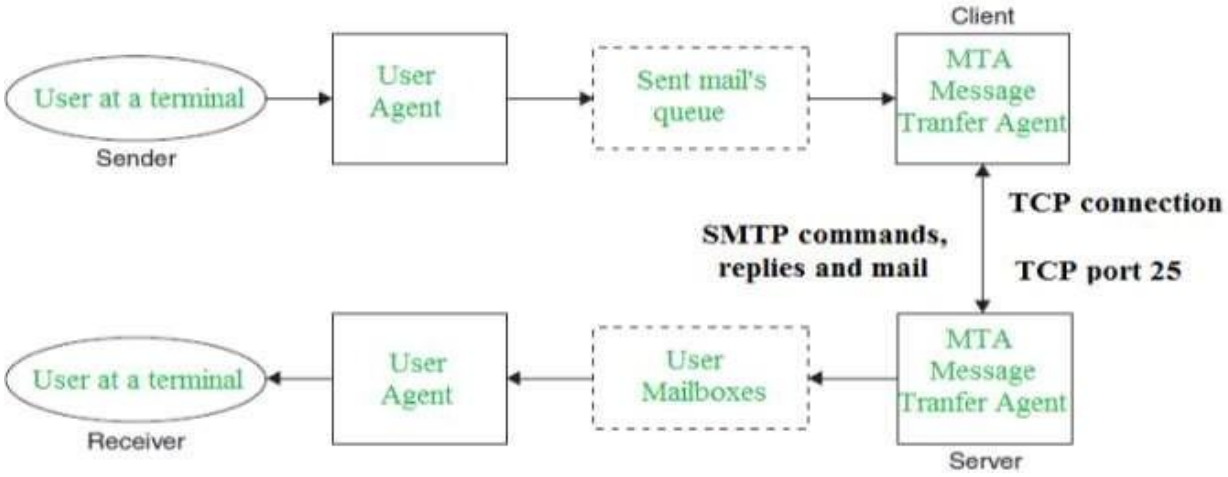
What is SMTP ?

- Simple Mail Transfer Protocol (SMTP) is an Internet Standard for electronic mail (email) transmission.
- SMTP is a TCP/IP protocol used in sending and receiving e-mail.
- Users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail.
- SMTP communication between mail servers uses TCP port 25. Mail clients on the other hand, often submit the outgoing emails to a mail server on port 587. A few Web email services, such as Gmail, use the unofficial TCP port 465 for SMTP.
- SMTP is an application layer protocol.

Protocol Overview

- SMTP is a connection-oriented, text-based protocol in which a mail sender communicates with a mail receiver by issuing command strings and supplying necessary data over a reliable ordered data stream channel, typically a Transmission Control Protocol (TCP) connection.
- An SMTP session consists of commands originated by an SMTP client (sender) and corresponding responses from the SMTP server (receiver) so that the session is opened, and session parameters are exchanged.
- The sender's, user agent prepare the message and send it to the MTA(Message Transfer Agent). The MTA functioning is to transfer the mail across the network to the receiver's MTA.

Model of SMTP system



Sending Email

- Mail is send by a series of request and response messages between the client and a server.
- The message which is send across consists of a **header** and the **body**.
- A **null line** is used to terminate the mail header. Everything which is after the null line is considered as body of the message which is a sequence of ASCII characters.
- The message body contains the actual information read by the receipt.

Receiving Email

- The user agent at the server side checks the mailboxes at a particular time of intervals. If any information is received it informs the user about the mail.
- When user tries to read the mail it displays a list of mails with a short description of each mail in the mailbox.
- By selecting any of the mail user can view its contents on the terminal.

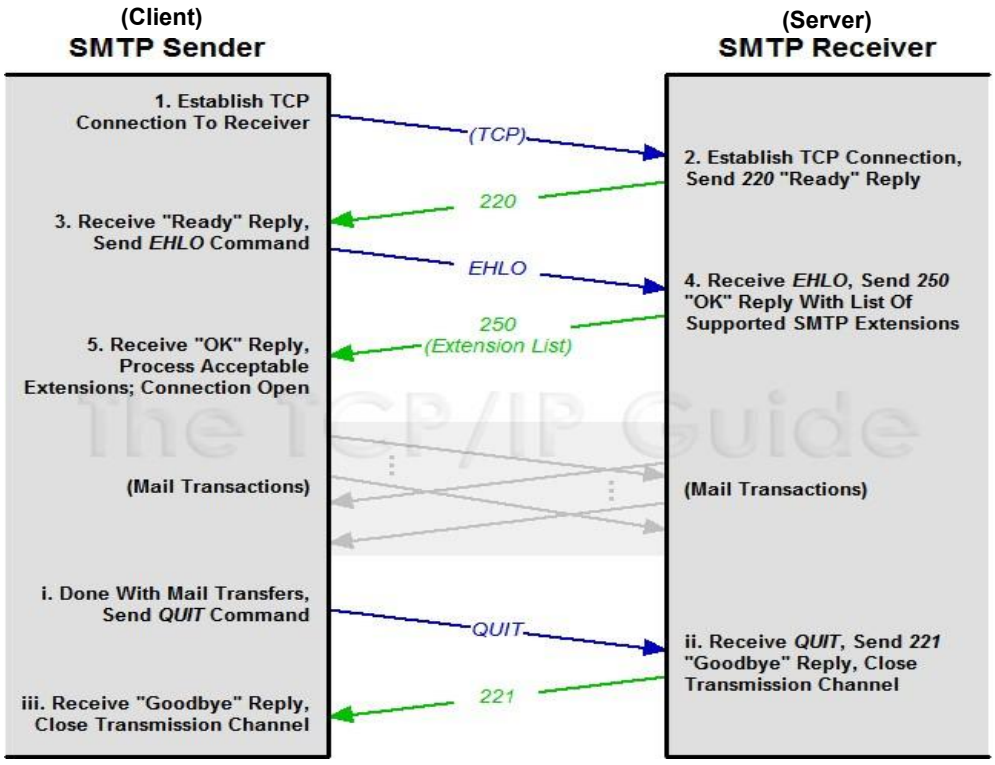
SMTP Transaction Commands

- **HELO** / **EHLO** - It initiate a new transaction between client and server.
- **RSET** - to reset the SMTP connection to the initial state in which the sender and recipient buffers are erased and the connection is ready to begin a new mail transaction.
- **NOOP** - an empty ("no operation") message designed as a kind of ping to check for responsiveness of the other end of the session
- **QUIT** - terminates the protocol session

SMTP Transaction Commands

- **MAIL** command, to establish the return address, also called return-path.
- **RCPT** command, to establish a recipient of the message.This command can be issued multiple times, one for each recipient. These addresses are also part of the envelope.
- **DATA** to signal the beginning of the *message text*; the content of the message, as opposed to its envelope. It consists of a *message header* and a *message body* separated by an empty line. DATA is actually a group of commands, and the server replies twice:
  1. once to the *DATA command* itself, to acknowledge that it is ready to receive the text
  2. second time after the end-of-data sequence, to either accept or reject the entire message.

SMTP Connection



Commands

Keyword	*Argument(s)*
HELO	Sender's host name
MAIL FROM	Sender of the message
RCPT TO	Intended recipient of the message
DATA	Body of the mail
QUIT	
RSET	
VRFY	Name of recipient to be verified
NOOP	
TURN	
EXPN	Mailing list to be expanded
HELP	Command name
SEND FROM	Intended recipient of the message
SMOL FROM	Intended recipient of the message
SMAL FROM	Intended recipient of the message

- 14 different commands. First 5 are required by all institutions.
- Next 3 are often used, but highly recommended

SMTP Transport Example

S: 220 smtp.example.com ESMTP Postfix
C: **HELO** relay.example.com
S: 250 smtp.example.com, I am glad to meet you
C: **MAIL** FROM:<bob@example.com>
S: 250 Ok
C: **RCPT** TO:<alice@example.com>
S: 250 Ok
C: **RCPT** TO:<theboss@example.com>
S: 250 Ok
C: **DATA**
S: 354 End data with <CR><LF>.<CR><LF>

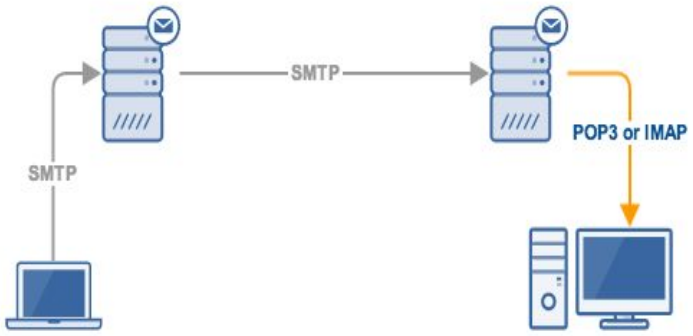
- C: From: "Bob Example" <bob@example.com>
- C: To: Alice Example <alice@example.com> C: Cc: theboss@example.com
- C: Date: Tue, 15 January 2008 16:02:43 -0500
- C: Subject: Test message

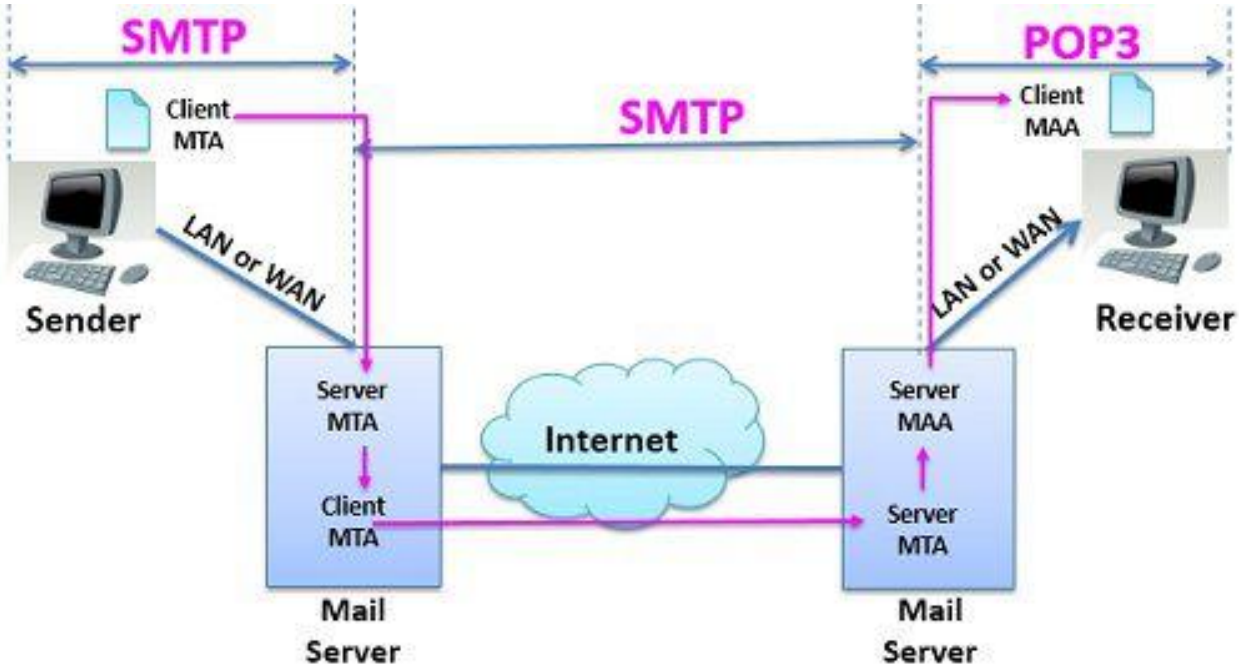
C: Hello Alice. This is a Test
C: .
C: **QUIT**
S: 221 Bye
{The server closes the connection}

Email

LIMITATIONS OF SMTP:

- Security matters for SMTP are worse.
- Its usefulness is limited by its simplicity.
- Transmission of binary files using SMTP is not possible without converting into text files. Use MIME to send mail in other format.
- It is limited to 7-bit ASCII characters only.
- SMTP servers may reject mail messages beyond some specific length.


SMTP
SMTP
POP3 or IMAP


SMTP
POP3
Client
MTA
SMTP
Client
MAA
LAN or WAN
LAN or WAN
Sender
Receiver
Server
MTA
Internet
Server
MAA
Client
MTA
Server
MTA
Mail
Server
Mail
Server

BASIS FOR COMPARISON	SMTP	POP3
Basic	It is message transfer agent.	It is message access agent.
Full form	Simple Mail Transfer Protocol.	Post Office Protocol version 3.
Implied	Between sender and sender mail server and between sender mail server and receiver mail server.	Between receiver and receiver mail server.
work	It transfers the mail from senders computer to the mail box present on receiver's mail server.	It allows to retrieve and organize mails from mailbox on receiver mail server to receiver's computer.

POP3 AND I MAPV4

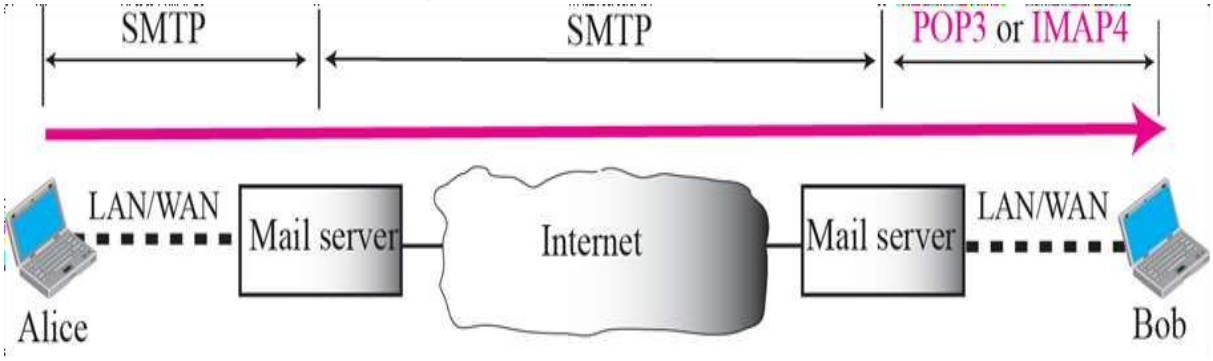
- The first and the second stages of mail delivery use SMTP. However, SMTP is not involved in the third stage because SMTP is a push protocol; it pushes the message from the client to the server.

- In other words, the direction of the bulk data (messages) is from the client to the server.

- On the other hand, the third stage needs a pull protocol; the client must pull messages from the server. The direction of the bulk data are from the server to the client. The third stage uses a message access agent.

STAGES OF MAIL DELIVERY

Stages of

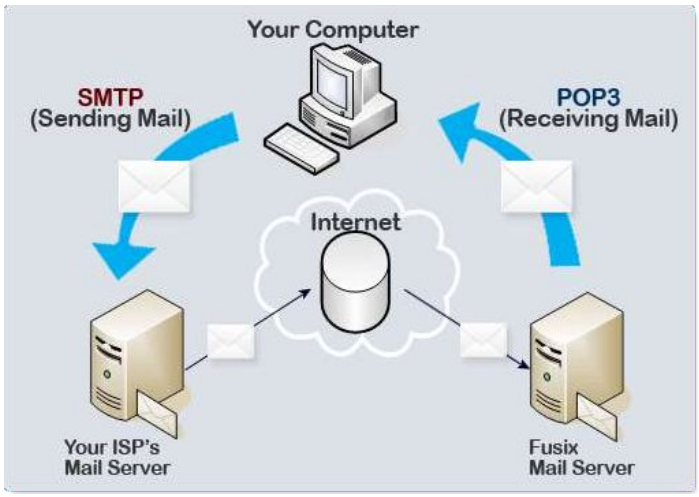


There are 3 stages in Mail Delivery:

- The first and the second stages of mail delivery use SMTP(push messages)
- The third stage of mail delivery use POP3 or IMAP4(pull messages)

What is POP?

- **The Post Office Protocol (POP3) is an Internet standard protocol working on Application Layer used by local email software to retrieve emails from a remote mail server over a TCP/IP connection.**



History Of Pop

- The Post Office Protocol has been updated 2 times since it was first published. A rough history of POP is
- POP : Post Office Protocol: published 1984
- POP2: Post Office Protocol: published 1985
- POP3: Post Office Protocol: published 1988.
- So, POP3 means "Post Office Protocol – Version 3". Since 1988, POP3 has been the active version.

Pop 3

- POP3 is simple and limited in functionality.
- Need POP3 client on user machine and POP3 server on the mail server machine.
- It is a pull protocol; the client must pull messages from the server.
- The direction of the bulk data are from the server to the client.
- It is a message access agent.

a. Client pushes messages

b. Client pulls messages

POP 3

- Pop3 has two modes: keep mode and delete mode
- In delete mode mail is deleted from mailbox after each retrieval.
- In keep mode, mail remains in mailbox after each retrieval.

Advantages:

- Simple protocol
- Easier to implement
- Copies all messages when connection is made.

Disadvantages:

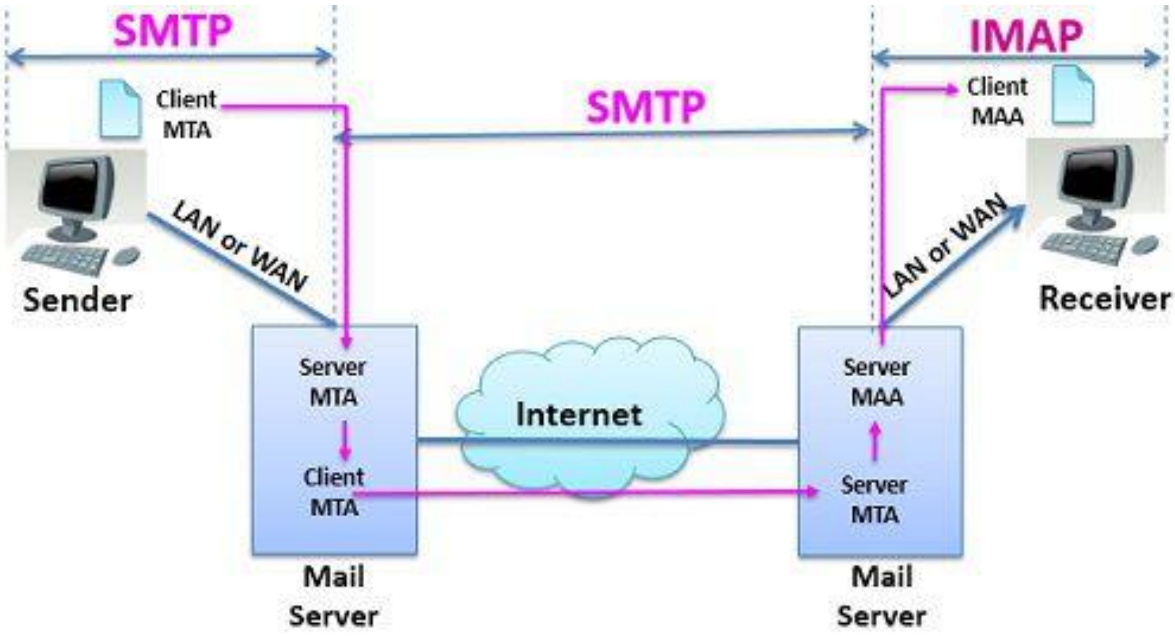
- Don’t allow user to organize mails on server.
- Don’t allow user to partially check the contents of mail before downloading.

How Does POP Work?

- **Incoming messages are stored at a POP server until the user logs in using an email client and downloads the messages to their computer. After user downloads the message, it is deleted from the server.**
- **While SMTP is used to transfer email messages from server to server, POP is used to collect mail with an email client from a server and does not include means to send**

Common Clients Using POP3

- **Eudora**
- **Gmail**
- **Outlook Express**
- **Mozilla Thunderbird**
- **Netscape**
- **Internet Explorer**


SMTP
IMAP
Client
MTA
SMTP
Client
MAA
LAN or WAN
LAN or WAN
Sender
Receiver
Server
MTA
Internet
Server
MAA
Client
MTA
Server
MTA
Mail
Server
Mail
Server

IMAP4

- As its name implies, IMAP allows us to access email messages wherever we are .
- Basically, email messages are stored on servers. Whenever we heck inbox, our email client contacts the server to connect with
- messages.
- When we read an email message using IMAP, we aren't actually downloading or storing it on computer; instead, we are reading it off of the server.
- As a result, it's possible to email from

- It as an intermediary between email client and email server.
- When you sign into an email client like Microsoft Outlook, it contacts the email server using IMAP.
- The headers of all of your email messages are then displayed.
- If you choose to read a message, it is quickly downloaded so that you can see it - emails are not downloaded unless you need to open them.

Advantages of imapv4

- A user can check the email header prior to downloading
- A user can search the contents of the email for a specific string of characters prior to downloading
- A user can partially download email (helpful if email contains huge attachments and connection is slow)
- A user can create, delete, or rename mailboxes on the mail server

- It allows us to access email messages from anywhere, and from many different devices as we want.

- It only downloads a message when we click on it. As a result, you do not have to wait for all of your new messages to download from the server before you can read them.

- Attachments are not automatically downloaded with IMAP. As a result, you're able to check your messages a lot more quickly and have greater control over which attachments are opened.

- Finally, IMAP can be used offline just like POP - you can basically enjoy the benefits of both protocols in

BASIS FOR COMPARISON	POP3	IMAP
Basic	To read the mail ithas to be downloaded first.	The mail content can be checked partially before downloading.
Organize	The user can not organize mails in the mailbox of the mail server.	The user can organize the mails on the server.
Folder	The user can not create, delete or rename mailboxes on a mail server.	The user can create, delete or rename mailboxes on the mail server.
Content	A user can not search the content of mail for prior downloading.	A user can search the content of mail for specific string of character before downloading.
Partial Download	The user has to download the mail for accessing it.	The user can partially download the mail if bandwidth is limited.
Functions	POP3 is simple and has limited functions.	IMAP is more powerful, more complex and has more features over POP3.