18CSC302J- Computer Networks

Unit-3

DNS(Domain Name System)

- TCP/IP protocols uses IP address.
- Identifies connection of a host to the internet.
- System maps a name to an address
- Host file – only two columns (name, address)
- Single host file – maps the names to address
- Host file would be large to store in every host.
- Impossible to update the changes happens every time to the host file.

Solution 1

- Store the host file in a single system and allow the centralized information access to every sytem that needs mapping.

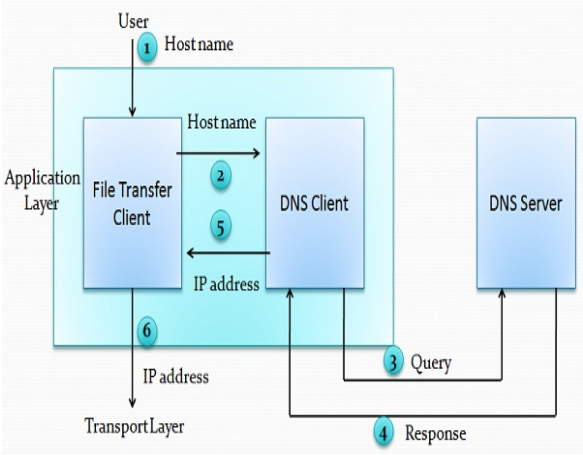
Disadvantage

- Huge amount of traffic to the internet.

Solution 2

- Divide the huge amount of information into smaller parts and store on different systems.
- Host which needs mapping can communicate to the closest system that holds the information.
- This solution is called Domain Name System.

Purpose of DNS



Six steps to map host name to an IP address

1. User passes the host name to the file transfer client (FTC).
2. FTC passes the host name to DNS client.
3. DNS client sends a message to the DNS Server. The query gives the file transfer server name using the known IP address of the DNS server.
4. DNS server responses back with the IP address of the desired file transfer server.
5. DNS client passes the IP address to file transfer server.
6. FTC uses the IP address it received to access the file transfer server.

Two Connections must be made

- Mapping the name to an IP address
- Transferring files

Namespace

- Maps the address to the unique names.
- Organized in two ways flat or hierarchical.

Flat Name Space

- Name is assigned to an address, name is the sequence of characters without structures.

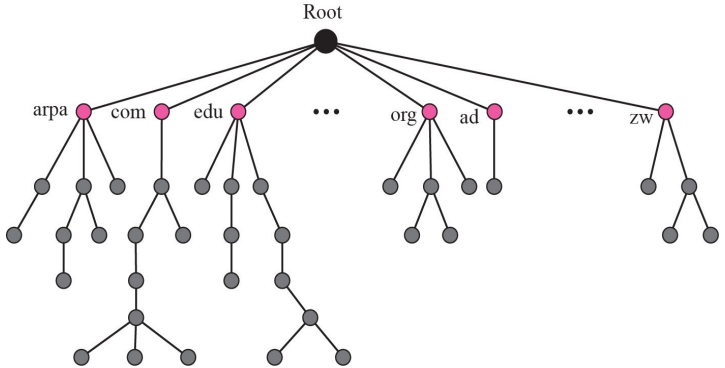
Disadvantage

- Cannot used in large system.
- Centrally controlled to avoid ambiguity and duplications.

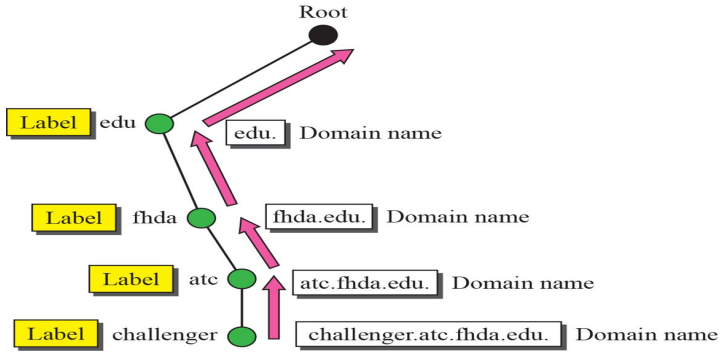
Hierarchical Name Space

- Each name is made up of several parts.
- First part – nature of organization
- Second part – name of an organization
- Third part – departments in the organization
- Namespace can be decentralized.
- Suffixes (or prefixes) are added to the name that defines the host or system.

Domain Name Space



Domain Name System



Domain names and labels

- ✔ Hierarchical name space – DNS was designed.
- ✔ Names are defined in inverted tree structure with root at top.
- ✔ Tree have 128 levels – 0 (root) to 127.

Label

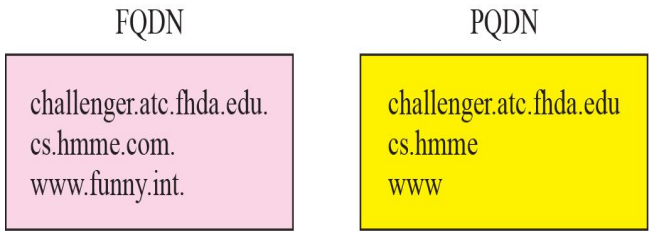
- ✔ Each node in a tree has a label – max of 63 characters.
- ✔ Root label is a null string.
- ✔ Children node should have different labels that will ensure uniqueness in domain names.

Domain Name

- ✔ Full domain name is the sequence of labels separated by dots.
- ✔ Domain names read from nodes up to the root.
- ✔ Full domain name always ends in a null label.

Source:BehrouzA.Forouzan,"TCPIPProtocolSuite"4thedition,2010,McGraw Hill,ISBN:0073376043

Fully Qualified Domain Names (FQDN)
Partially Qualified Domain Names (PQDN)



FQDN and PQDN

Fully Qualified Domain Names (FQDN)

- If the label is terminated by null string it is called fully qualified domain names.
- Contains the full name of the host, contains all labels from most specific to most general.
- DNS server can match an FQDN to an address.

  Eg: challenger.atc.fhda.edu.

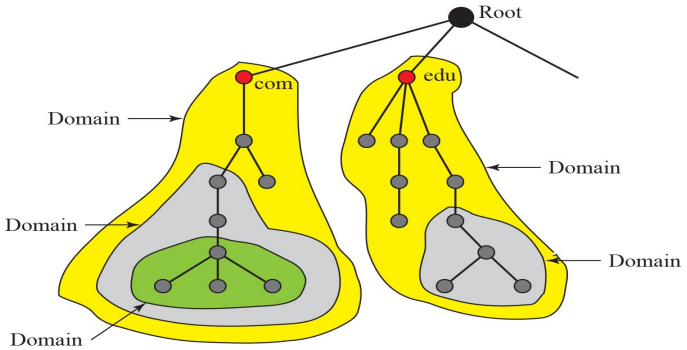
Partially Qualified Domain Names (PQDN)

- If the label is not terminated by null string it is called partially qualified domain name.
- PQDN starts from the node but does not reach the root.
- The resolver will supply the missing part called the suffix to create a PQDN.
- User at fhda.edu site wants to get the IP address of the challenger computer, has to mention the partial name.

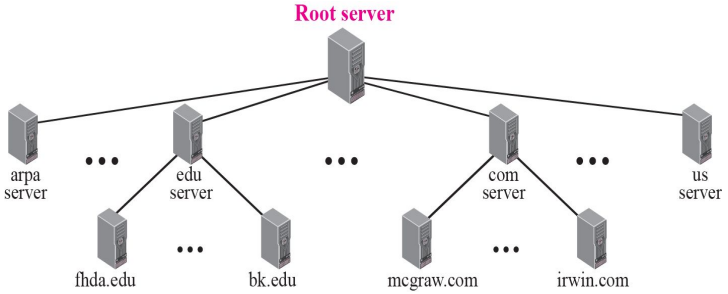
  Eg: challenger

Source:BehrouzA.Forouzan,"TCPIPProtocolSuite"4thedition,2010,McGraw Hill ISBN:0073376043

Domain Name Space



Domains



Hierarchy of name servers

Domain

- It is the subtree of domain name space.
- The of the domain is the name of the node at the top of the subtree.
- Domains may itself divided into sub domains.

Distribution of name space

- Information in the name space must be stored.
- It is inefficient and not reliable to store the information in a single system.

Solution

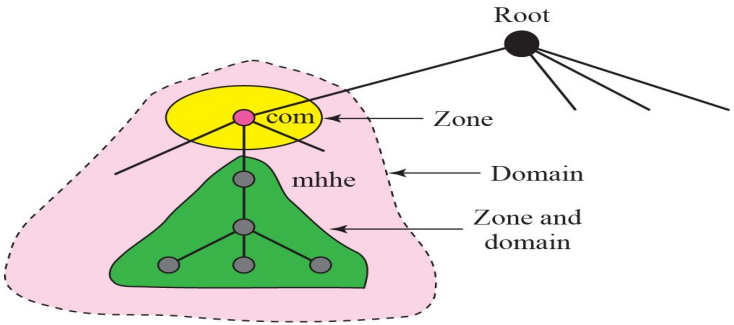
- Distribute the information among many computers called DNS servers.

Hierarchy of name space

- Divide the whole space into many domains based on the first level.

Source:BehrouzA.Forouzan,"TCPIPProtocolSuite"4thedition,2010,McGraw Hill ISBN:0073376043

Domain Name Space



Zones and Domains

Zone

- What a server is responsible for or has authority over is called zones.
- Zone is the contiguous part of the entire tree.
- If server accepts the responsibility for a domain and does not divide the domain into smaller domains then “domain” and “zone” refers the same thing.

Root server

- It is the server whose zone consists of the whole tree.
- It does not store any information about the domains but delegates the authority to other servers, keeping references to those servers.

Source:BehrouzA.Forouzan,“TCPIPProtocolSuite”4thedition,2010,McGraw Hill ISBN:0073376043

Domain Name Space

Primary and Secondary Servers

Primary Server

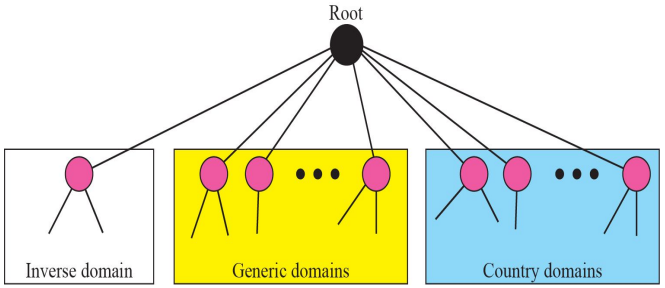
- Server that stores the file about the zone for which it is in authority.
- It is responsible for creating, maintaining and updating the zone files.
- It stores zone file on a local disk.

Secondary Servers

- Server that transfers the complete information about zone from another server and stores the file on its local disk.
- Secondary server neither creates nor updates the zone files.

A primary server loads all information from the disk file; the secondary server loads all information from the primary server. When the secondary downloads information from the primary, it is called zone transfer.

DNS in the Internet



DNS used in internet

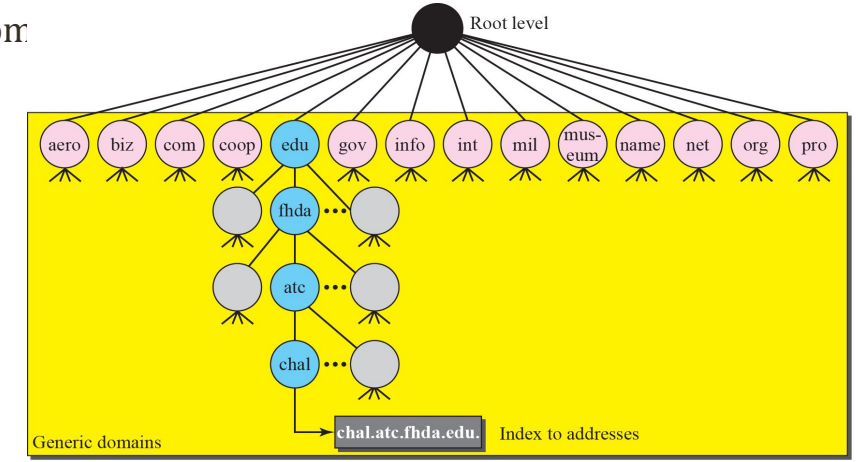
Label	*Description*
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other non-profit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

Generic Domain Labels

- In internet the domain name space is divided into three different sections.
- Generic domains, country domains and the inverse domains.

Generic Domains

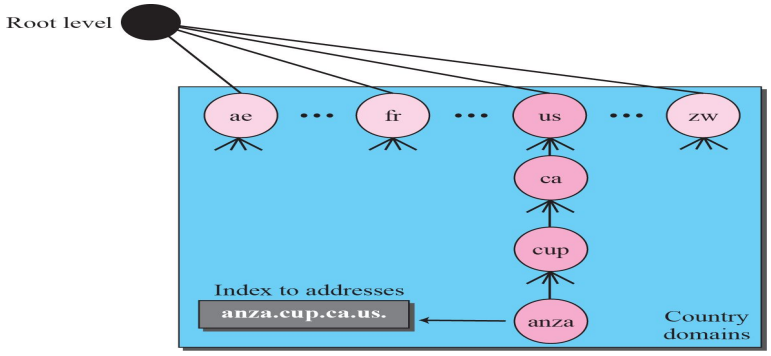
- Define registered hosts according to their generic behaviour.
- Each node in a tree defines a domain which s an index to the dom



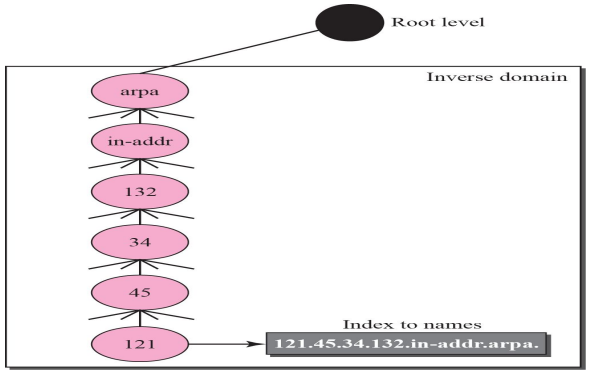
Generic Domains

Source:BehrouzA.Forouzan,"TCPIPProtocolSuite"4thedition,2010,McGraw Hill ISBN:0073376043

DNS in the Internet



Country Domains



Inverse Domain

Country Domains

- Uses two character country abbreviations.

  Eg: US for United Sates

- Second label can be organizational or they can be more specific national designations.

  Eg: ca.us

Inverse Domain

- It is used to map an address to a name.
- This happens when the server has received a request from the client.
- Type of query called an inverse or pointer (PTR) query.
- To handle the pointer query the inverse domain is added to the domain name space with the first level node.

Source:BehrouzA.Forouzan,"TCPIPProtocolSuite"4thedition,2010,McGraw Hill ISBN:0073376043

DNS in Internet

Registrar

- How are the new domains added to DNS?
- Registrar is a commercial entity accredited by ICANN
- A registrar first verifies that the requested domain name is unique and then enters it into the DNS database.
- A fee is charged.

Resolution

Mapping a name to an address or an address to a name is called name address resolution.

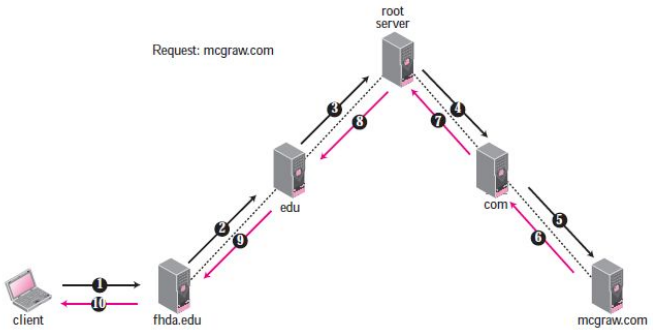
Resolver

- DNS is designed as a client – server application.
- Host that needs to map an address to a name or a name to an address calls a DNS client called a resolver.
- After the resolver receives the mapping, it interprets the response to see if it is a real resolution or an error and finally delivers the results to the process that requested it.

Mapping Names to Addresses

- The resolver gives a domain name to the server and asks for the corresponding address.
- If the domain name is from the generic domain the resolver receives a domain name such as "chal.atc.fhda.edu.
- if the domain name is from the country domain the resolver receives a domain name such as "ch.fhda.cu.ca.us.

Resolution



Recursive resolution

Mapping Addresses to Names

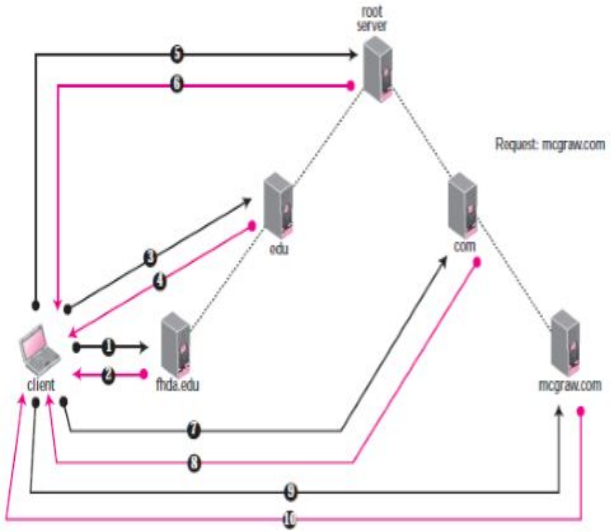
- A client can send an IP address to a server to be mapped to a domain name.
- To answer the PTR query DNS uses the inverse domain.
- in the request the IP address is reversed and two labels in-addr and arpa are appended to create a domain acceptable by the inverse domain.

Recursive Resolution

- The client can ask for a recursive answer from a name server.
- If the server is the authority for the domain name, it checks its database and responds.
- If the server is not the authority it sends the request to another server and waits for the response.
- If the parent is the authority it responds otherwise it sends the query to another server.

Source:BehrouzA.Forouzan,"TCPIPProtocolSuite"4thedition,2010,McGraw Hill ISBN:0073376043

Resolution



Iterative Resolution

Iterative Resolution

- If server is an authority for the name it sends the answer.
- If not it returns the IP address of the server that thinks it can resolve the query.
- The client is responsible for repeating the request to the second server.
- The client repeats the same procedure to next server and so on
- This process is called iterative because the client repeats the same query to multiple servers.

Caching

- Each time the server receives the query for a name that is not in domain it needs to search its database for a server IP address.
- Reduction in searching time would increase the efficiency.
- DNS handles this with the mechanism called catching

Source:BehrouzA.Forouzan,"TCPIPProtocolSuite"4thedition,2010,McGraw Hill ISBN:0073376043

Resolution

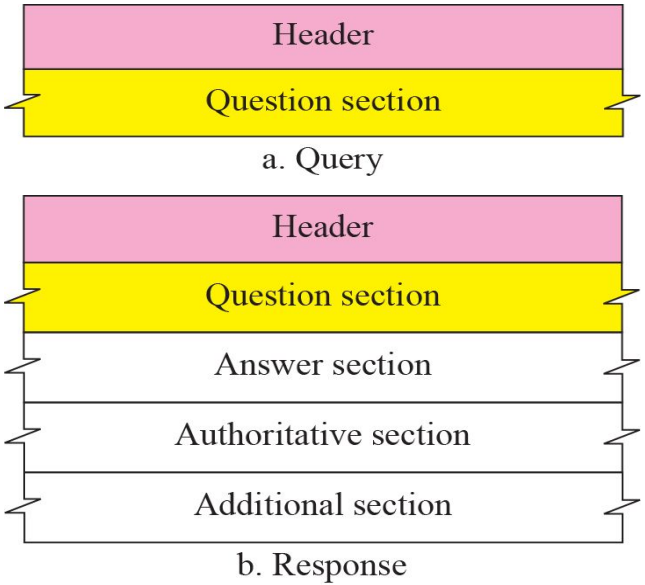
- Reduction of search time would increase the efficiency.
- DNS handles this with the mechanism called catching.
- Catching speeds up resolution but it can also be problematic.
- If the server catches the mapping for a long time it may send an outdated mapping to the client.

Two counter techniques are used

- The authoritative server always adds information to the mapping called time to live.

- DNS requires each server keep a TTL counter for each mapping it caches.

DNS Messages



Query and Response Messages

- DNS messages are of two types
  - Query
  - Response
- The query message consists of header and question records.
- The response message consists of header, question records, answer records, authoritative records and additional records.

Source:BehrouzA.Forouzan,"TCPIPProtocolSuite"4thedition,2010,McGraw Hill ISBN:0073376043

DNS Messages

Identification	Flags
Number of question records	Number of answer records (All 0s in query message)
Number of authoritative records (All 0s in query message)	Number of additional records (All 0s in query message)

Header Format

Flags Field

Header

- Both query and response message have the same header format with some fields set to zero for query messages.
- The header is of 12 bytes.
- Identification - 16 bit field used by client to match the response with the query.
- Flags – 16 bit field consisting of the subfields.
- QR (Query/Response) – 1 bit sub field defines type of message.
  0 – message is query
  1 – message is response

- OpCode - 4 bits, defines the type of query or response
  0 – standard
  1 – inverse
  2 – server status request

Source:BehrouzA.Forouzan,"TCPIPProtocolSuite"4thedition,2010,McGraw Hill ISBN:0073376043

DNS Messages

Flags Field

- AA (Authoritative Answer) – 1 bit subfield
  Set to 1 - name server is the authoritative server
  Used only in response message.
- TC (Truncate) – 1 bit subfield
  Set to 1 – response was mor than 512 bytes and truncated
  It is used when DNS uses the services of UDP
- RD (Recursion Desired) – 1 bit subfield
  Set to 1 – client desires a recursive answer
  It is set in query message and repeated in the response message
- RA (Recursion Available) – 1 bit subfield
  Set in response, means that a recursive response is available
  Set only in response message

Source:BehrouzA.Forouzan,"TCPIPProtocolSuite"4thedition,2010,McGraw Hill ISBN:0073376043

DNS Messages

Flags Field

Value	Meaning	Value	Meaning
0	No error	4	Query type not supported
1	Format error	5	Administratively prohibited
2	Problem at name server	6–15	Reserved
3	Domain reference problem		

Values of rcode

- Reserved – 3 bit sub field set to 000.

  rcode – 4 bit field shows status of error in response

  Only authoritative server can make the judgement
- Number of question records – 16 bit field

  Contains the number of queries in question section of the message
- Number of answer records – 16 bit field

  Contains the number of answer records in answer section of the response message
- Number of authoritative records – 16 bit field

  Contains number of authoritative records in authoritative section of the response message

  It's value is zero in query message
- Number of additional records – 16 bit field

  Contains number of additional records in additional section of a response message

Source:BehrouzA.Forouzan,"TCPIPProtocolSuite"4thedition,2010,McGraw Hill ISBN:0073376043

DNS Messages

- Question Section
  Consists of one or more question records
  It is present in both query and response messages
- Answer Section
  Consists of two or more resource records
  It is present only on response messages
- Authoritative Section
  Consists of two or more resource records
  It is present only on response messages
  Gives information (domain name) about one or more authoritative servers for the query
- Additional Information Section
  Consists of two or more resource records
  It is present only on response messages
  Gives additional information that helps the resolver

TELNET & SSH

TELNET

- **TE**rminaL **NET**work –remote login
- standard TCP/IP protocol for virtual terminal service as proposed by ISO.
- TELNET enables the establishment of a connection to a remote system in such a way that the **local terminal appears to be a terminal at the remote system.**
- TELNET is a general-purpose client-server application program

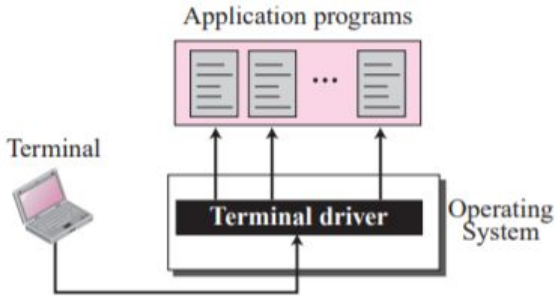
Concepts

a) Timesharing Environment

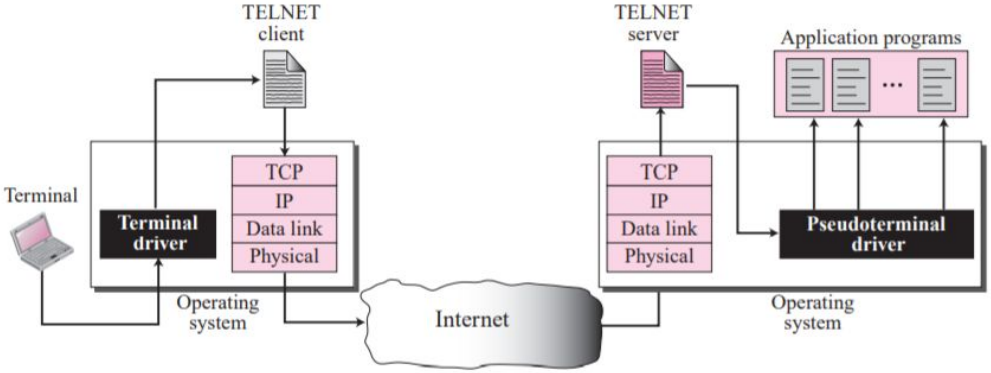
- All of the processing must be done by the central computer. When a user types a character on the keyboard, the character is usually sent to the computer and echoed to the monitor. It creates an environment in which each user has the illusion of a dedicated computer.

Login

- Local login

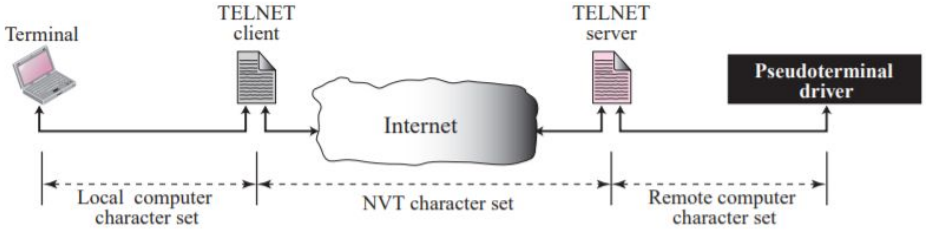


- Remote Login



b) Network Virtual Terminal (NVT)

Character set



- Heterogeneous networks
- remote computer- type of the computer to be known
- The client TELNET translates characters (data or commands) that come from the local terminal into NVT form and delivers them to the network.
- The server TELNET, on the other hand, translates data and commands from NVT form into the form acceptable by the remote computer.

NVT Character Set

- **Data Characters** called **NVT ASCII.**
- This is an 8-bit character set in which the seven lowest order bits are the same as US ASCII and the highest order bit is 0
- Although it is possible to send an 8-bit ASCII (with the highest order bit set to be 0 or 1)-must first be agreed upon between the client and the server using option negotiation.
- To send **control characters** between computers (from client to server or vice versa), NVT uses an 8-bit character set in

a. Data Character b. Control Character

Character	*Decimal*	*Binary*	*Meaning*
EOF	236	11101100	End of file
EOR	239	11101111	End of record
SE	240	11110000	Suboption end
NOP	241	11110001	No operation
DM	242	11110010	Data mark
BRK	243	11110011	Break
IP	244	11110100	Interrupt process
AO	245	11110101	Abort output
AYT	246	11110110	Are you there?
EC	247	11110111	Erase character
EL	248	11111000	Erase line
GA	249	11111001	Go ahead
SB	250	11111010	Suboption begin
WILL	251	11111011	Agreement to enable option
WONT	252	11111100	Refusal to enable option
DO	253	11111101	Approval to option request
DONT	254	11111110	Denial of option request
IAC	255	11111111	Interpret (the next character) as control

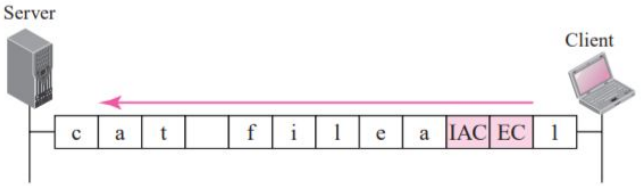
c) Embedding

- TELNET uses only one TCP connection.
- The server uses the well-known port 23 and the client uses an ephemeral port. Same connection is used for sending both data and control characters.
- TELNET accomplishes this by embedding the control characters in the data stream.
- To distinguish data from control characters, each sequence of control characters is preceded by a special control character called interpret as control (IAC).

For example, ima) on a remote serve

cat file1

cat filea1

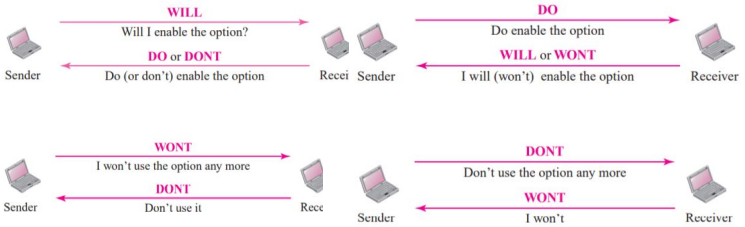


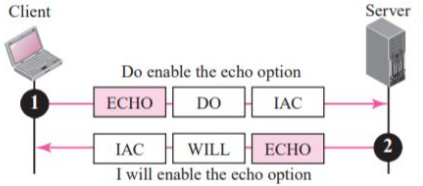
Options

Code	Option	Meaning
0	Binary	Interpret as 8-bit binary transmission
1	Echo	Echo the data received on one side to the other
3	Suppress go-ahead	Suppress go-ahead signals after data
5	Status	Request the status of TELNET
6	Timing mark	Define the timing marks
24	Terminal type	Set the terminal type
32	Terminal speed	Set the terminal speed
34	Line mode	Change to line mode

NVT character set for option negotiation

Character	Code	Meaning 1	Meaning 2	Meaning 3
WILL	251	Offering to enable	Accepting to enable	
WONT	252	Rejecting to enable	Offering to disable	Accepting to disable
DO	253	Approving to enable	Requesting to enable	
DONT	254	Disapproving to enable	Approving to disable	Requesting to disable





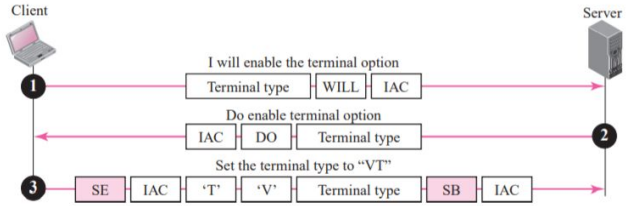
d)Symmetry

- the client and server are given equal opportunity
- both are using a default TELNET implementation with no options enabled.
- If one party wants an option enabled, it can offer or request. The other party has the right to approve the offer or reject the request if the party is not capable of using the option or does not want to use the option.
- This allows for the expansion of TELNET. A client or server can install a more sophisticated version of TELNET with more options.
- When it is connected to a party, it can offer or request these new options.
- If the other party also supports these options, the options can be enabled; otherwise, they are rejected.

NVT character set for sub option negotiation

Character	*Decimal*	*Binary*	*Meaning*
SE	240	11110000	Suboption end
SB	250	11111010	Suboption begin

- To define the type or speed of a terminal, the negotiation includes a string or a number to define the type or speed

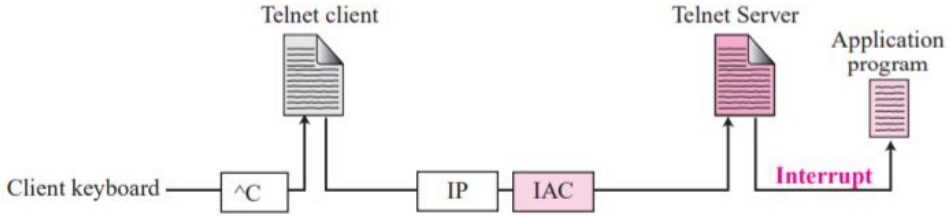


e) Controlling Server

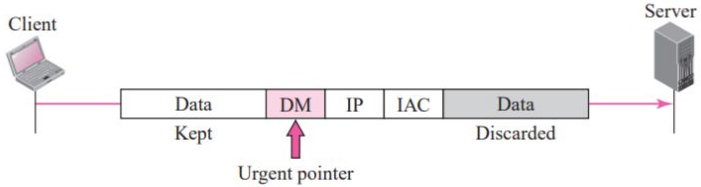
Characters used to control a program running on remote server

Character	*Decimal*	*Binary*	*Meaning*
IP	244	11110100	Interrupt process
AO	245	11110101	Abort output
AYT	246	11110110	Are you there?
EC	247	11110111	Erase the last character
EL	248	11111000	Erase line

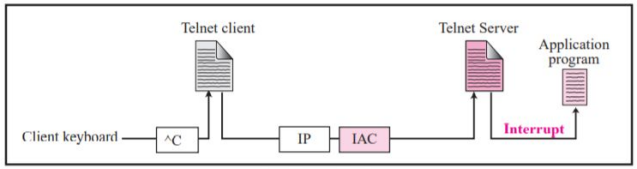
Interrupting an application program



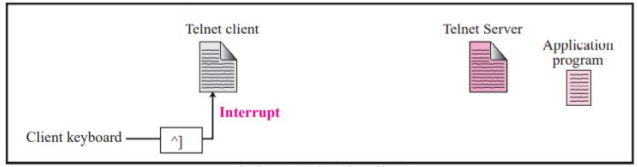
f) Out of Band Signalling



Two different interruptions



a. Interrupting the application program



b. Interrupting the client

- **Mode of Operation**

(i) Character Mode- overhead created

- The user enters a character that is sent to the server
- The server acknowledges the received character and echoes the character back (in one segment).
- The client acknowledges the receipt of the echoed character.

(ii) Linear Mode

- Echoing, character erasing, line erasing, and so on) is done by the client.
- The client then sends TELNET AND SSH 623 the whole line to the server. Although the line mode looks like the default mode, it is not.
- The default mode operates in the half-duplex mode; the line mode is full-duplex with the client sending one line after another, without the need for an intervening GA (go ahead) character from the server.

C) Default mode

- Used if no other modes are invoked through option negotiation.
- In this mode, the echoing is done by the client.
- The user types a character and the client echoes the character on the screen (or printer) but does not send it until a whole line is completed.
- After sending the whole line to the server, the client waits for the GA (go ahead) command from the server before accepting a new line from the user.
- The operation is **half-duplex**.
- Half-duplex operation is not efficient when the TCP connection itself is full-duplex, and so this mode is becoming obsolete.

Interface Commands

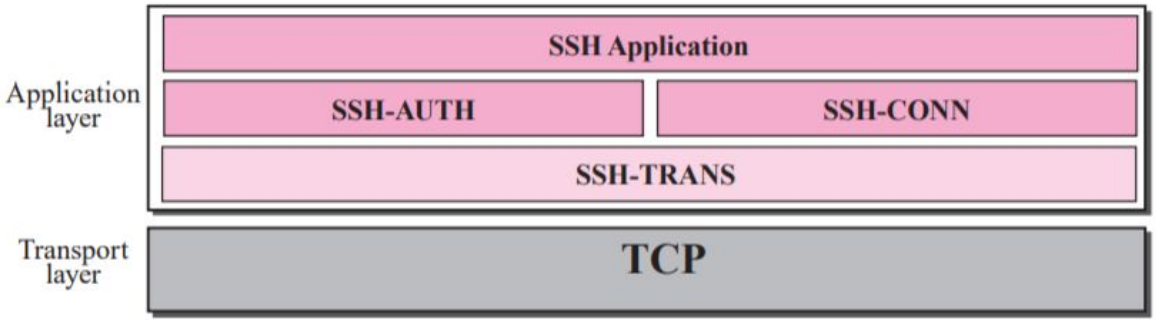
Command	*Meaning*	*Command*	*Meaning*
open	Connect to a remote computer	set	Set the operating parameters
close	Close the connection	status	Display the status information
display	Show the operating parameters	send	Send special characters
mode	Change to line or character mode	quit	Exit TELNET

- TELNET **suffers from security problems**.
- Although TELNET requires only a login name and password (when exchanging text)

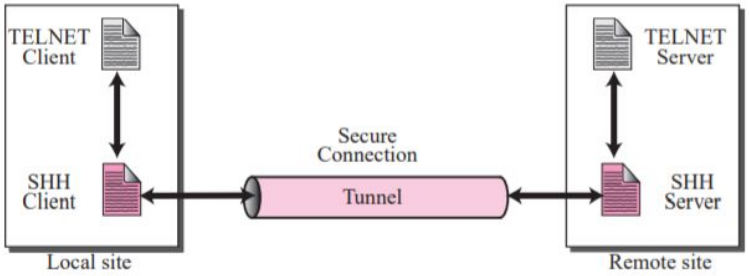
For instance: A microcomputer connected to a broadcast LAN can easily eavesdrop using snooper software and capture a login name and the corresponding password (even if it is encrypted)

Secure Shell (SSH)

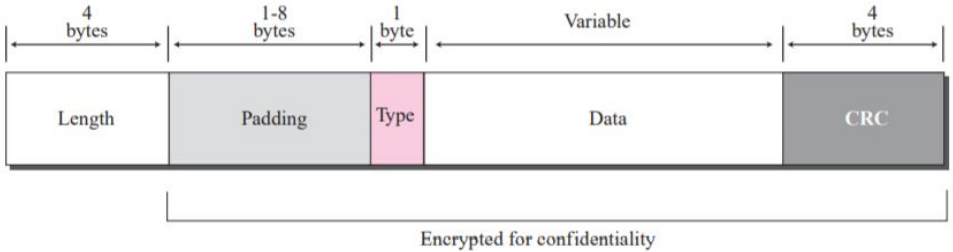
- remote login application program
- Like TELNET, uses TCP as the underlying transport protocol
- SSH is more secure and provides more services than TELNET
- Versions - two versions of SSH: SSH-1 and SSH-2, which are totally incompatible. SSH-1 is now deprecated because of security flaws in it. Now SSH-2 only used



Path Forwarding



SSH Packet Format



- Length. This 4-byte field defines the length of the packet including the type, the data, and the CRC field, but not the padding and the length field.
- Padding. One to eight bytes of padding is added to the packet to make the attack on the security provision more difficult.
- Type. This one-byte field defines the type of the packet used by SSH protocols.
- Data. This field is of variable length. The length of the data can be found by deducting the five bytes from the value of the length field.
- CRC. The cyclic redundancy check filed is used for error detection

File Transfer Protocol

File Transfer Protocol

- FTP (File Transfer Protocol) is the simplest and most secure way to exchange files over the Internet.
- Transferring files from a client computer to a server computer is called **"uploading"** and transferring from a server to a client is **"downloading".**
- To access an FTP server, users must be able to connect to the Internet or an intranet (via a modem or local area network) with an FTP client program.

File Transfer Protocol

- FTP doesn’t really move, it copies files from one computer to another
- FTP is the file transfer protocol in the
- Internet's TCP/IP protocol suite’s Application Layer.

File Transfer Protocol

- An FTP Client is software that is designed to move files back-and-forth between two computers over the Internet.
- It needs to be installed on your computer and can only be used with a live connection to the Internet.

FTP Clients

- Some commonly used FTP clients include the following:
- **FileZilla**- a popular FTP client that is freely available for Windows, Macintosh, and Linux users Available as a free download from the Internet.
- **Fire FTP**- a plug-in for the popular Firefox web browser that can be used just like a standalone FTP program
- Installed through the FireFox browser.

- **Dreamweaver**- page layout/design program, which include FTP access as one of its many features
- Available for purchase from Adobe

FTP Clients

- There are many FTP client programs, some of which are run from a command-line (such as the command ***ftp***, a standard installed in many operating systems), but a large majority allow the user to manipulate files via a graphical interface (such as CuteFTP), which makes file transfers more user-friendly.

FTP Download & Upload

Differences between FTP and HTTP

- The major difference between FTP and HTTP is that FTP is a two-way system - FTP can be used to copy or move files from a server to a client computer as well as upload or transfer files from a client to a server.
- HTTP, on the other hand, is strictly one-way: "transferring" text, pictures and other data(Multimedia files) from the "server" to a client computer which uses a web browser to view the data.

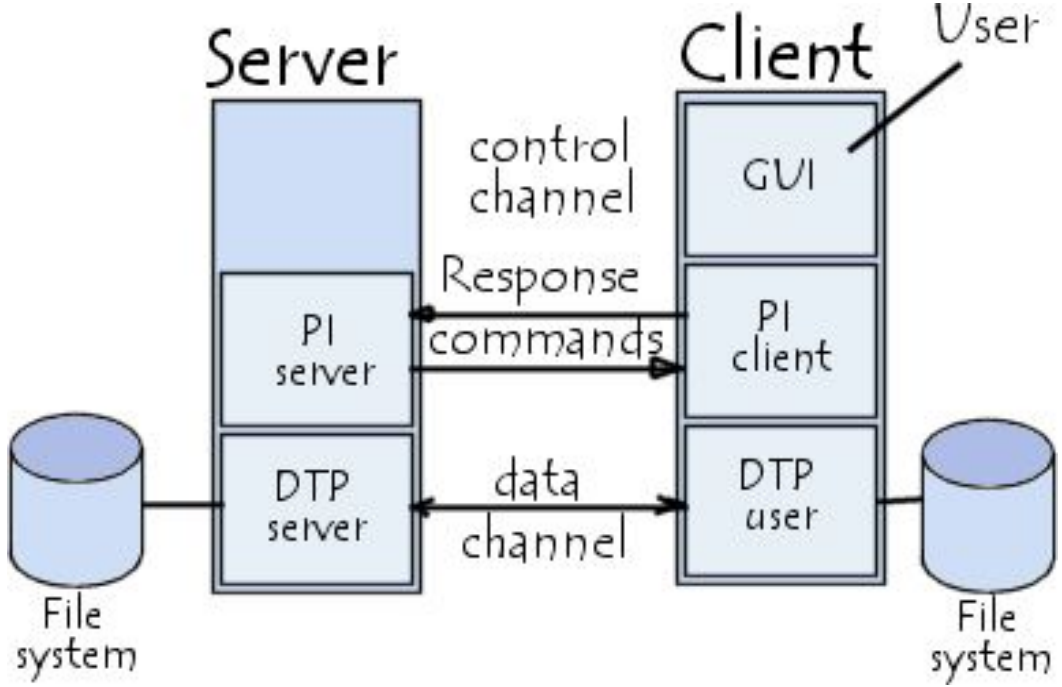
Differences between FTP and HTTP

- FTP systems generally encode and transmit their data in binary sets which allow for faster data transfer; HTTP systems encode their data in MIME format which is larger and more complex.
- Files are automatically copied or moved from a file server to a client computer's hard drive, and vice versa. On the other hand, files in an HTTP transfer are viewed and can 'disappear' when the browser is turned off unless the user executes commands to move the data to the computer's memory.

Differences between FTP and HTTP

- FTP protocol falls within a client-server
- Model, i.e. one machine sends orders (the client) and the other awaits requests to carry out actions (the server).
- During an FTP connection, two transmission channels are open:
- A channel for commands (control channel) , a control channel that stays open for the entire session
- A channel for data , data channel that opens and closes to transfer data such as folder listings and files to or from the server as requested by the client.

The FTP model



The FTP model

- So, both the client and server have two processes allowing these two types of information to be managed:
- **DTP** (*Data Transfer Process*) It establishes the connection and managing the data channel. The server side DTP is called *SERVER-DTP*, the client side DTP is called *USER-DTP*
- **PI** (*Protocol Interpreter*) Controls DTP using commands received over the control channel. It is different on the client and the server:

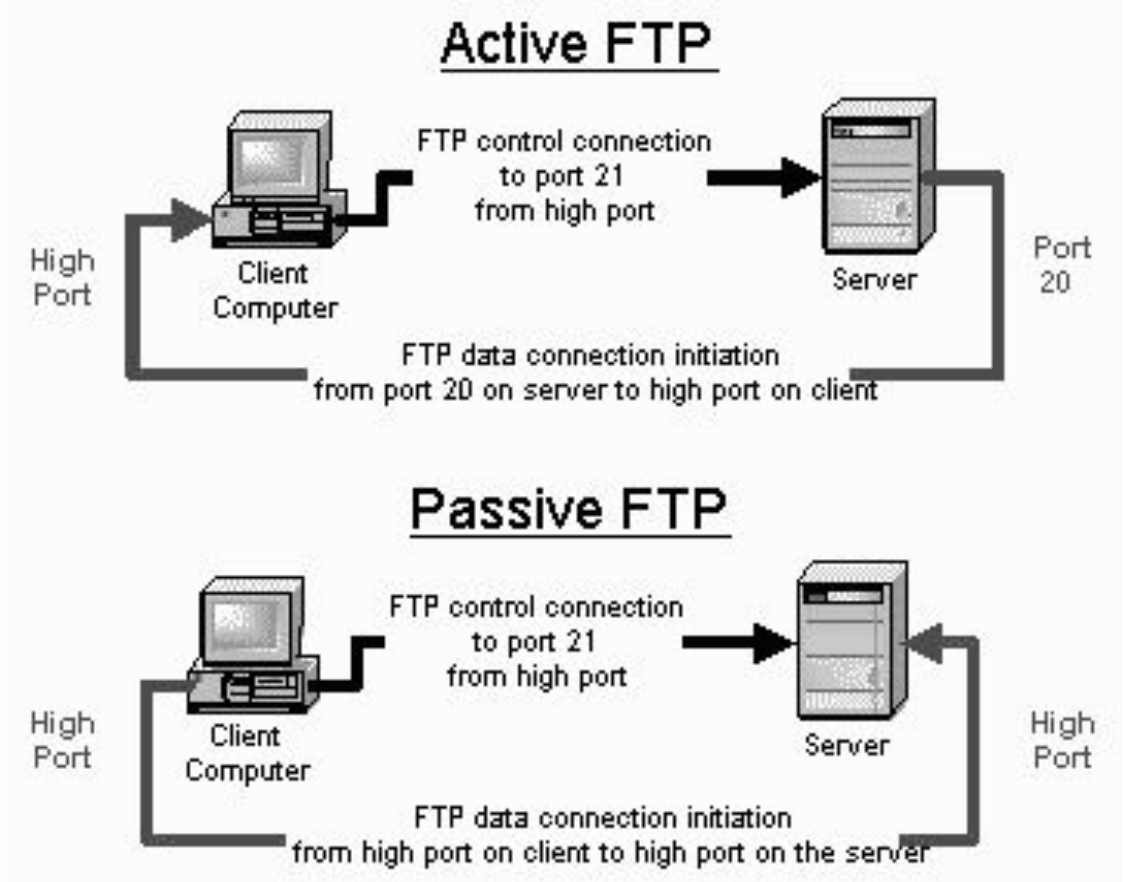
The FTP model

- The **SERVER-PI** is responsible for listening to the commands coming from a USER-PI over the control, establishing the connection for the control channel, receiving FTP commands from the USER-PI over this, responding to them and running the SERVER-DTP.
- The **USER-PI** is responsible for establishing the connection with the FTP server, sending FTP commands, receiving responses from the SERVER-PI and controlling the USER-DTP if needed.

The FTP model

- When an FTP client is connected to a FTP server, the USER-PI initiates the connection to the server according to the Telnet protocol.
- The client sends FTP commands to the server, the server interprets them, runs its DTP, then sends a standard response.
- Once the connection is established, the server-PI gives the port on which data will be sent to the Client DTP.
- The client DTP then listens on the specified port for data coming from the server.

Types of connections

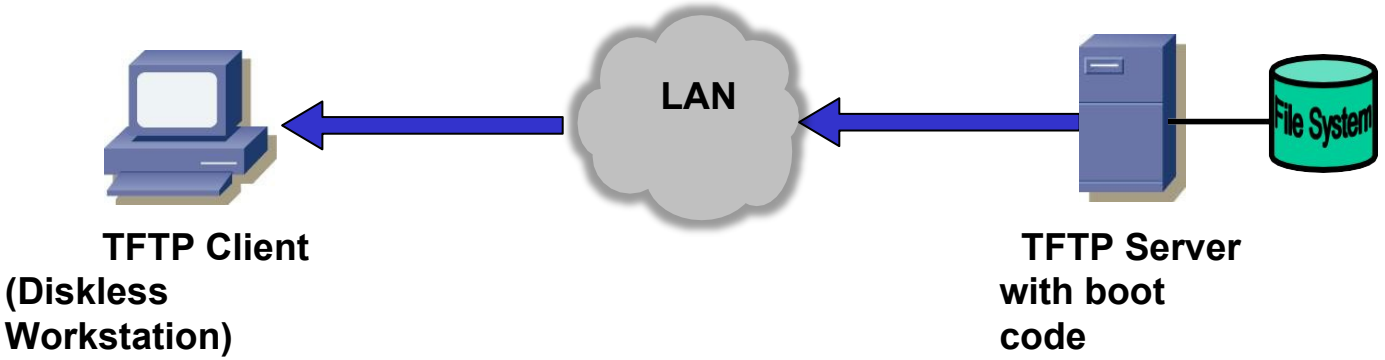


Trivial File Transfer Protocol (TFTP)

TFTP - Trivial File Transfer Protocol

Why TFTP?

- In the old days, TFTP was typically used for downloading boot code to diskless workstations.
- TFTP was simple enough to fit into EEPROMs of diskless workstations (only a few KBytes of code).



TFTP versus FTP

FTP and TFTP both are protocols for transferring files between a client and a server.
However, TFTP and FTP are 2 totally different protocols and do not have anything in common.

Value	FTP	TFTP
Authentication	Authentication based on login with username and password.	TFTP does not provide authentication (login).
Connection	FTP uses TCP (reliable transmission). Errors are handled by the underlying TCP layer.	TFTP uses UDP and thus no connections. Errors in the transmission (lost packets, checksum errors) must be handled by the TFTP server.
Protocol algorithm	Transmission of data and control information is handled by the underlying TCP layer. TCP guarantees maximum throughput (flow control, congestion control) and error control.	TFTP uses a simple lock-step protocol (each data packet needs to be acknowledged). Thus the throughput is limited.
Footprint	FTP is more complex than TFTP, thus requires a larger memory footprint. Often FTP is not suited for small device bootloaders which must fit into constrained EEPROM storage.	TFTP is very simple. Because it uses the equally simple UDP transport protocol, TFTP clients or servers have a very small footprint and are thus suited for use in bootloaders.
Control and data channel	FTP separates user data and control information by using 2 separate TCP connections.	TFTP uses only "1 channel", i.e. control packets (commands) flow in one direction while data packets carrying user data flow in the reverse direction over the same UDP sockets.

TFTP Protocol

- Request – response protocol:

TFTP is a simple request / acknowledge protocol.
The mode of operation is lock-step because each data packet needs to be acknowledged before the next data packet may be sent.
This makes the implementation very simple (no flow control needed), but limits the throughput because each data packet requires 1 round-trip-time (RTT) for transmission.

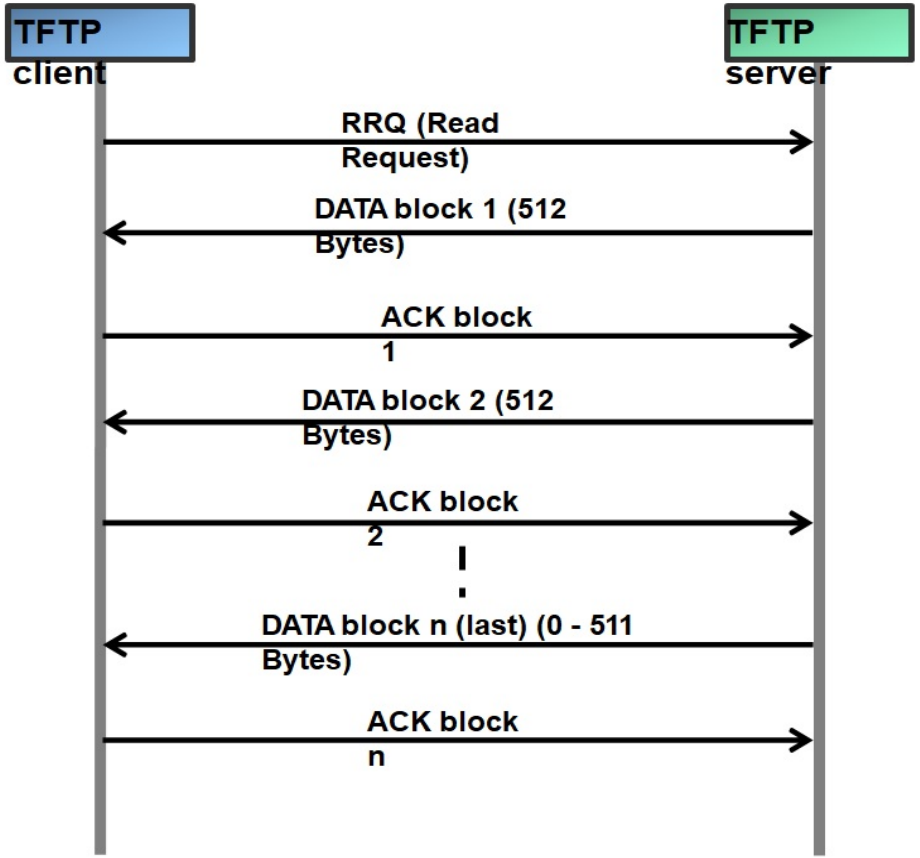
- Acknowledge of data:

TFTP only uses positive acknowledgements (correctly received packets are acknowledged with an ACK packet).
When the sender does not receive an ACK packet in due time, it re-sends the last DATA packet.

- UDP Ports:

The server "listens" on port 69 (TFTP default port), but switches to another port for all replies (DATA, ACK) in order to free the port 69 for other requests (server ‚spawns' a new UDP socket for handling the TFTP request).

TFTP read request (RRQ):



The transfer is initiated by a read request packet (RRQ).

The server responds with the first data block of 512 bytes.

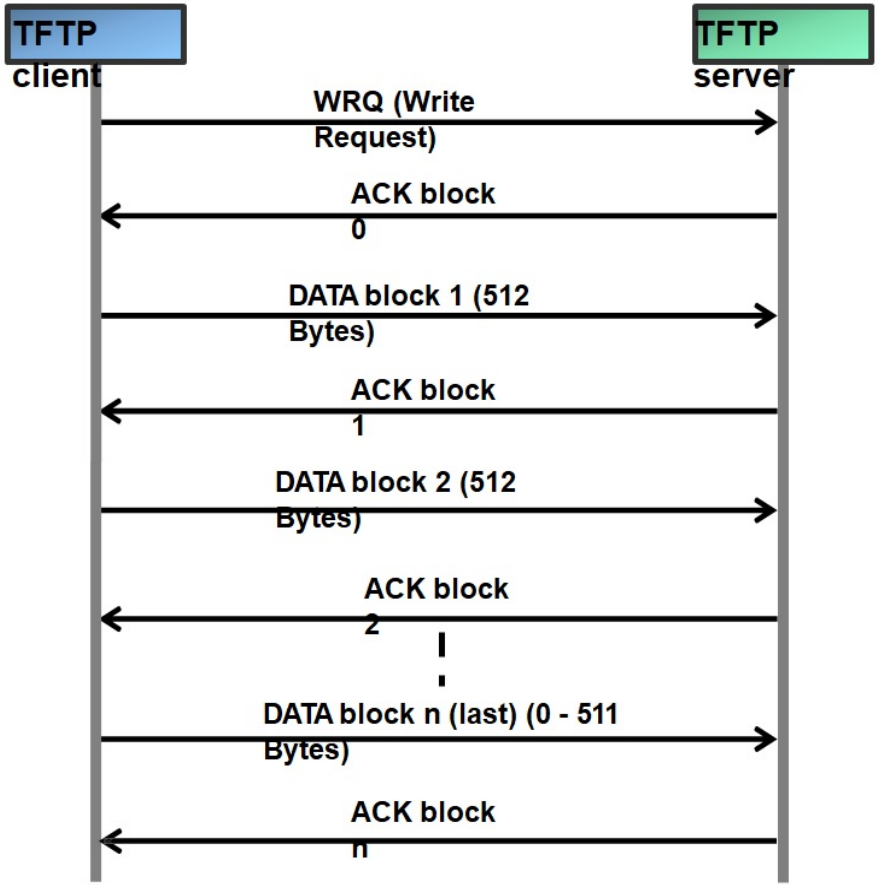
The client acknowledges the reception of the first data block.

The transfer continues with the next data block which is acknowledged by the client.

The last data packet contains 0 – 511 bytes. This signals the end of transfer to the client.
If the entire data file to be transferred is dividable by 512, the last packet contains 0 data bytes (an empty packet).

The transfer is completed by the last acknowledge.

TFTP write request (RRQ):



The transfer is initiated by a write request packet (WRQ).

To keep the scheme with acknowledging every packet as is the case in RRQ, the server acknowledges the "virtual" data block 0 which acknowledges the WRQ packet.

The client sends the first data block of 512 bytes.

The server acknowledges the first data block.

The transfer continues with the next data block which is acknowledged by the server.

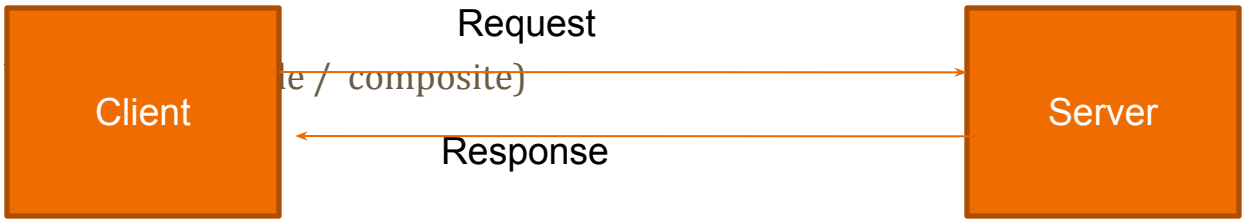
Again, the last data packet contains 0 – 511 bytes signaling
the end of the transfer to the client.

The transfer is completed by the last acknowledge.

WWW Architecture

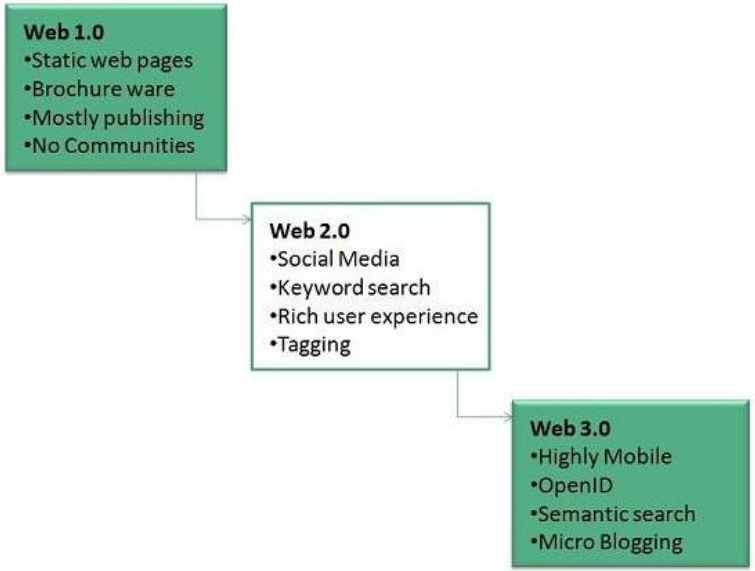
WWW Architecture

- WWW stands for World Wide Web
- WWW is a networked information system (repository of information) and it provides distributed client-server service, in which a client using a browser can access a service using a server.
  - Sites
  - le / composite)



Evolution

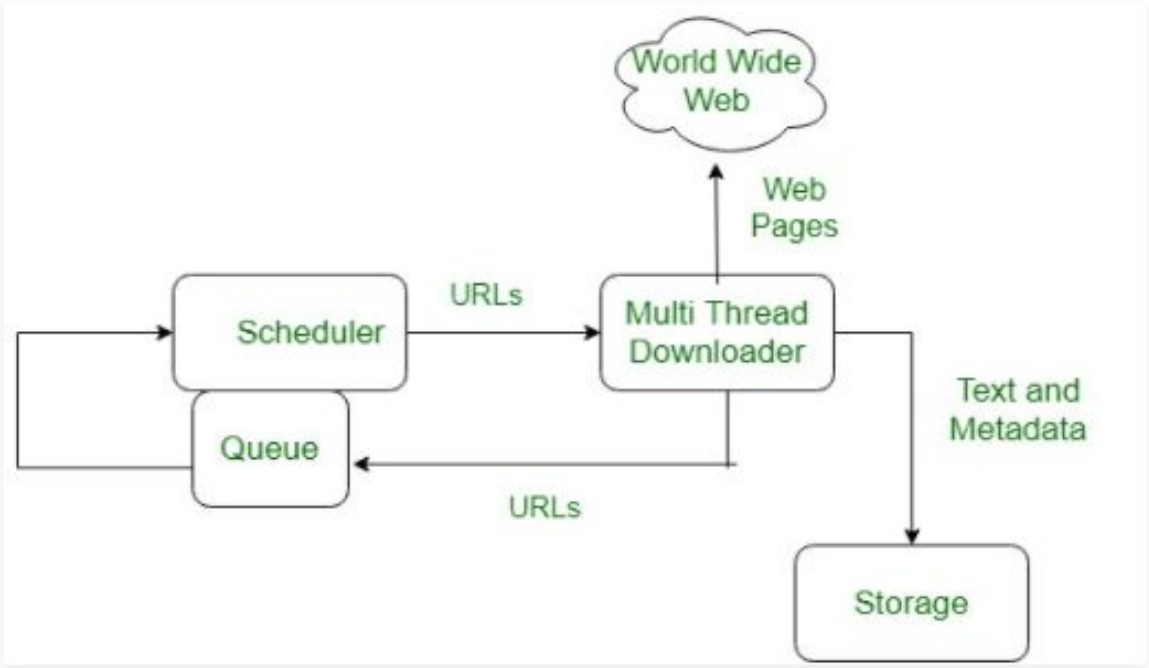
- **World Wide Web** was created by **Timothy Berners Lee**
- allow researchers to work together effectively and efficiently at **CERN.** Eventually it became **World Wide Web**



System Architecture

- **World Wide Web** consist of vast, worldwide connection of documents or web pages.
- Web pages have Hyperlinks which navigate to other web pages.
- The pages can be retrieved and viewed by using browsers of which internet explorer, Netscape Navigator, Google, Chrome etc.
- The browser fetches the page requested interprets the text and formatting commands on it, and displays the page, properly formatted, on the screen.

System Architecture



Features of WWW

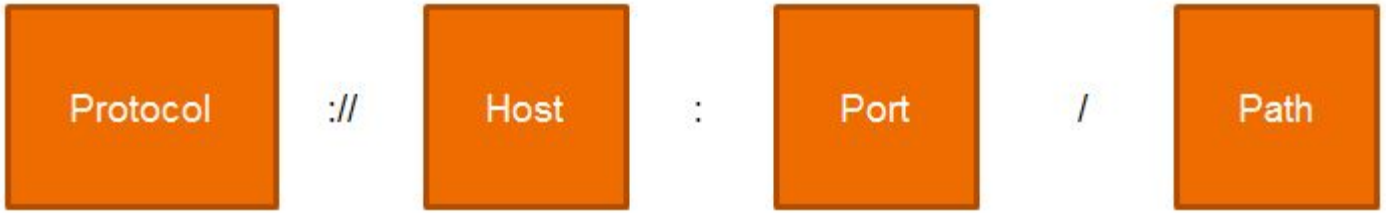
- HyperText Information System
- Cross-Platform
- Distributed
- Open Standards and Open Source
- Uses Web Browsers to provide a single interface for many services
- Dynamic, Interactive and Evolving.
- “Web 2.0”

COMPONENTS OF WEB

- **Uniform Resource Locator (URL):** serves as system for resources on web.
- **HyperText Transfer Protocol (HTTP):** specifies communication of browser and server.
- **Hyper Text Markup Language (HTML):** defines structure, organisation and content of webpage.

Uniform Resource Locator (URL)

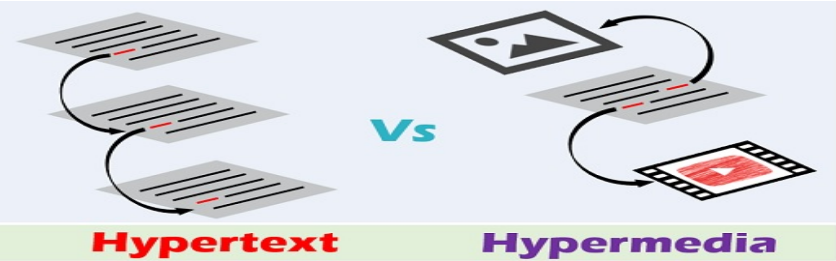
- A URL (Uniform Resource Locator) is a unique identifier used to locate a resource on the internet.



- Protocol - client-server application program used to retrieve the document (http)
- Host - domain name of the computer on which the information is located (www)
- Port – (optional) If the port is included, it is inserted between the host and the path, and it is separated from the host by a colon.
- Path - pathname of the file where the information is located.

Hypertext and Hypermedia

- Hypertext –creating a document that in turn refer to other document. In a hypertext document, a part of text can be defined as a link to another document.
- Hypermedia is a term applied to document that contains links to other textual document or documents containing graphics, video, or audio.



Web Client (Browser)

- It is an application software that allows us to view and explore information on the web. User can request for any web page by just entering a URL into address bar.
- Web browser can show text, audio, video, animation and more. It is the responsibility of a web browser to interpret text and commands contained in the web page.
- A variety of vendors offer commercial browsers that interpret and display a Web document, and all of them use nearly the same architecture. Each browser usually consists of three parts:
  - a controller – receives input from keyboard
  - client protocol – access the document
  - Interpreters – display document on screen

Web Server

- Web site is collection of web pages while web server is a software that respond to the request for web resources.
- When client sends request for a web page, the web server search for the requested page if requested page is found then it will send it to client with an HTTP response.
- If the requested web page is not found, web server will the send an HTTP response : Error 404 Not found.
- A server can also become more efficient through multithreading or multiprocessing. In this case, a server can answer more than one request at a time.
- Some popular Web servers include Apache and Microsoft Internet Information Server.

INTERNET vs WEB

INTERNET	WEB
Network of networks and the network allows to exchange of the data between two or more computers	The Web is a way to access Information through the Internet
It is also known as Network of Networks.	The Web is a model for sharing information using Internet.
The Internet is a way of transporting information between devices.	The protocol used by the web is Http

Web Documents

Web Documents

- **Web page** is a document available on world wide web. Web Pages are stored on web server and can be viewed using a web browser

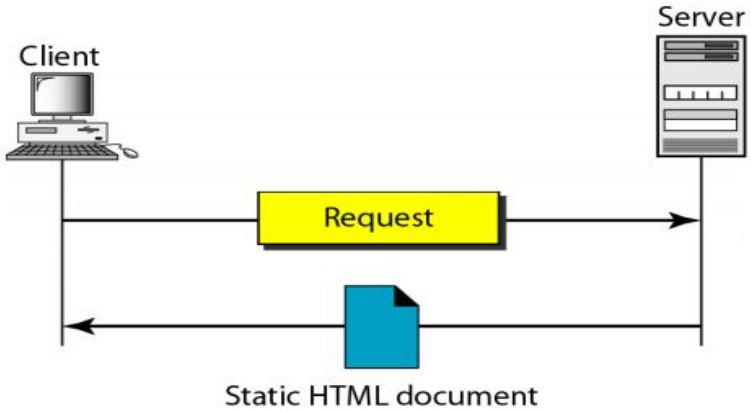
- Web page can contain huge information including text, graphics, audio, video and hyper links. These hyper links are the link to other web pages.

- Types are

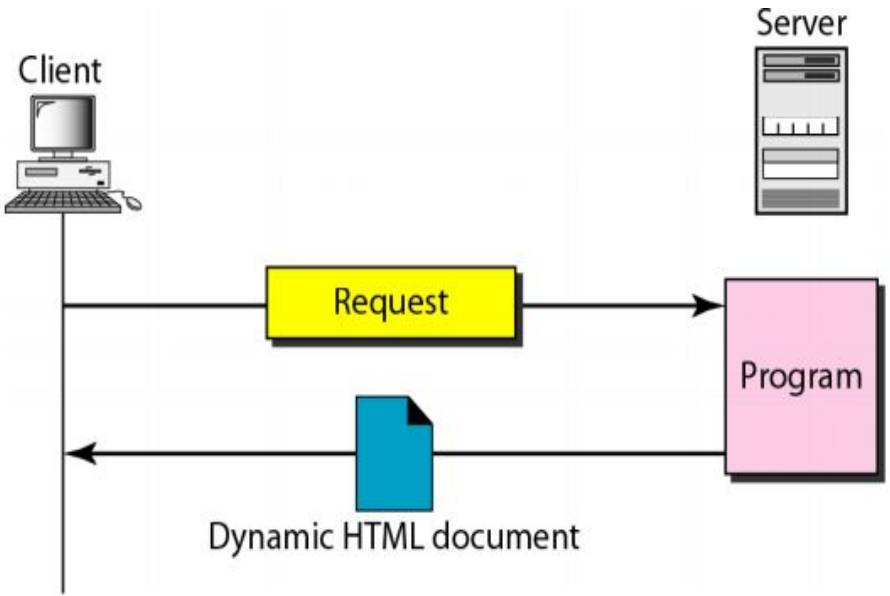
    - Static Web Documents
    - Dynamic Web Documents

Static Documents

- **Static web pages** are also known as flat or stationary web page
- Contains only Static information where the user can only read the information but can't do any modification or interact with the information.
- They are loaded on the client's browser as exactly they are stored on the web server
- Static documents are prepared using – HTML, XML, XSL, XHTML.

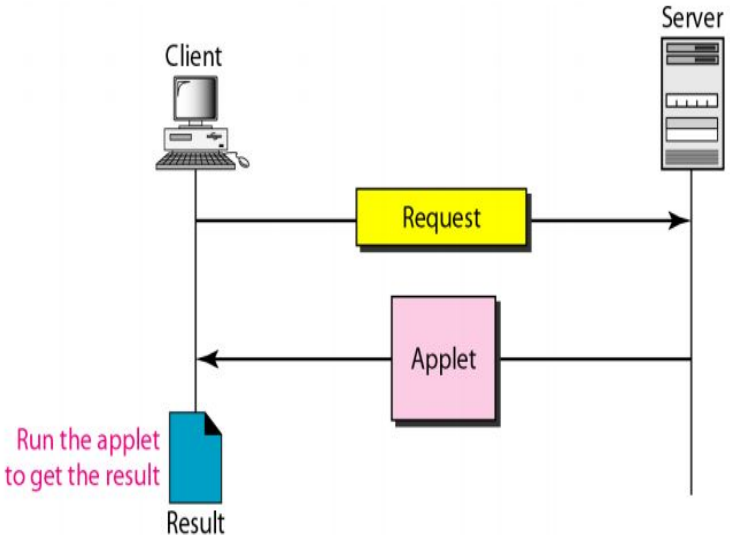


Dynamic Documents



- A dynamic web document does not exist in a predefined form.
- When a request arrives the web server runs an application program that creates the document.
- The server returns the output of the program as a response to the browser that requested the document.
- Since a fresh document is created for each request, the contents of a dynamic document can vary from one request to another.
- Technologies involved – PHP, JSP, ASP etc.
- Dynamic documents are sometimes referred

Active Documents



- An active web document consists of a computer program that the server sends to the browser and that the browser must run locally.
- When it runs, the active document program can interact with the user and change the display continuously.
- Active documents are sometimes referred to as client-site dynamic documents.

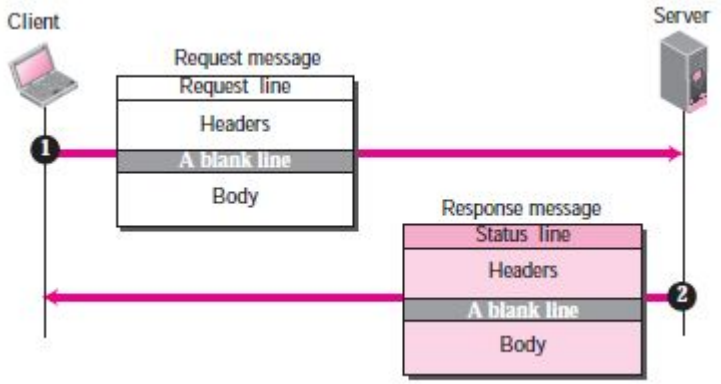
HTTP

HTTP

- The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web.
- HTTP retrieves webpages from the web.
- HTTP functions as a combination of FTP and SMTP.
- HTTP uses the services of TCP on well-known port 80.
- Since HTTP uses the services of TCP, HTTP is a connection oriented and reliable protocol.

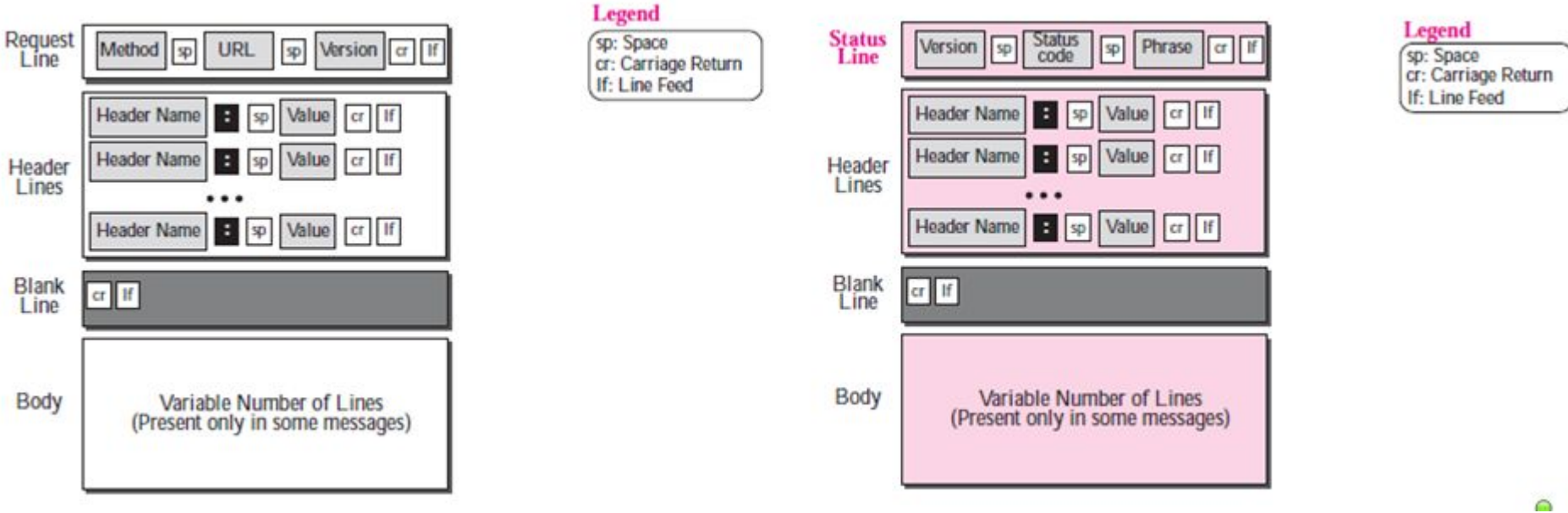
HTTP Transaction

- The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web.
- HTTP functions as a combination of FTP and SMTP.
- HTTP uses the services of TCP on well-known port 80.
    - Request message
    - Request Line



HTTP Transaction (Cont . . .)

- Format of request message and response message



Conditional Request

- Request based on condition is possible.
- If condition is met, server sends it; else client is informed about it.
- Example conditions - time and date the Web page is modified.

    - Request

    GET http://www.commonServer.com/information/file1 HTTP/1.1

    If-Modified-Since: Thu, Sept 04 00:00:00 GMT

    - Response

    HTTP/1.1 304 Not Modified

    Date: Sat, Sept 06 08 16:22:46 GMT

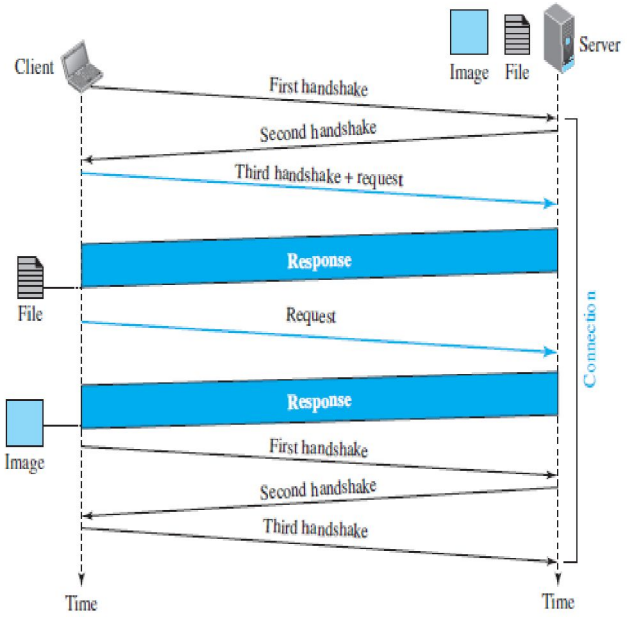
    Server: commonServer.com

    (Empty Body)

Persistent vs Non Persistent connections

- Hypertext content embedded in the webpage may need multiple request and response
- If the webpages where the objects need to be retrieved are located in different server, a new TCP connection should be established for each server
- But in the case, if all the webpages are located in same server, then two choices are there:
  - Nonpersistent connection: New TCP connection for each object access
  - Persistent connection: One TCP connection for all objects
- HTTP prior to version 1.1 uses Nonpersistent connection, from version 1.1 persistent connection is used as default
- From HTTP 1.1, connection is left open for more requests.
- Connection will be closed only after a request or if a time-out is reached.
- Length of data is sent by the sender on each response, but if it is unknown (Dynamic documents) then the server informs client and closes the connection.

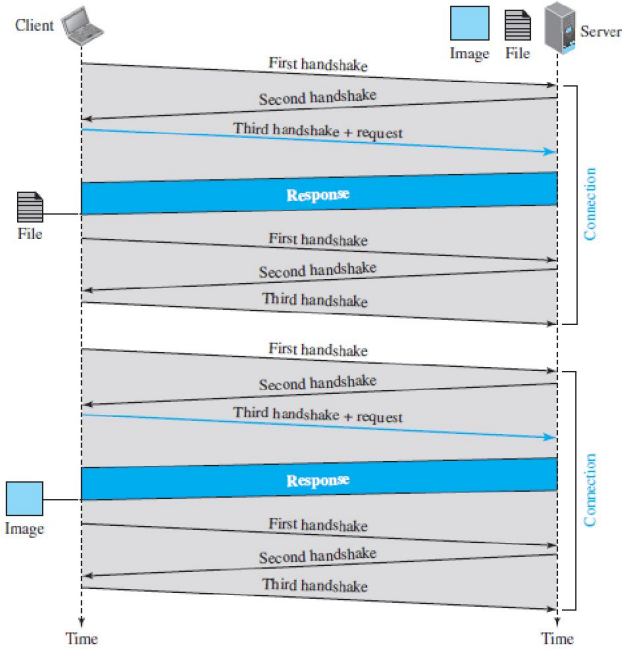
Persistent Connection



Nonpersistent connection

- One TCP connection is established for one request/response
- Following steps are as follows,
    - The client opens a TCP connection and sends a request
    - The server sends the response and closes the connection
    - The client reads the data until it encounters an end of the file marker, it then closes the connection
- Note: if a webpage contains N different pictures in different files, then it needs N+1 connection establishment and it is an overhead at server end

Nonpersistent Connection (Contd)



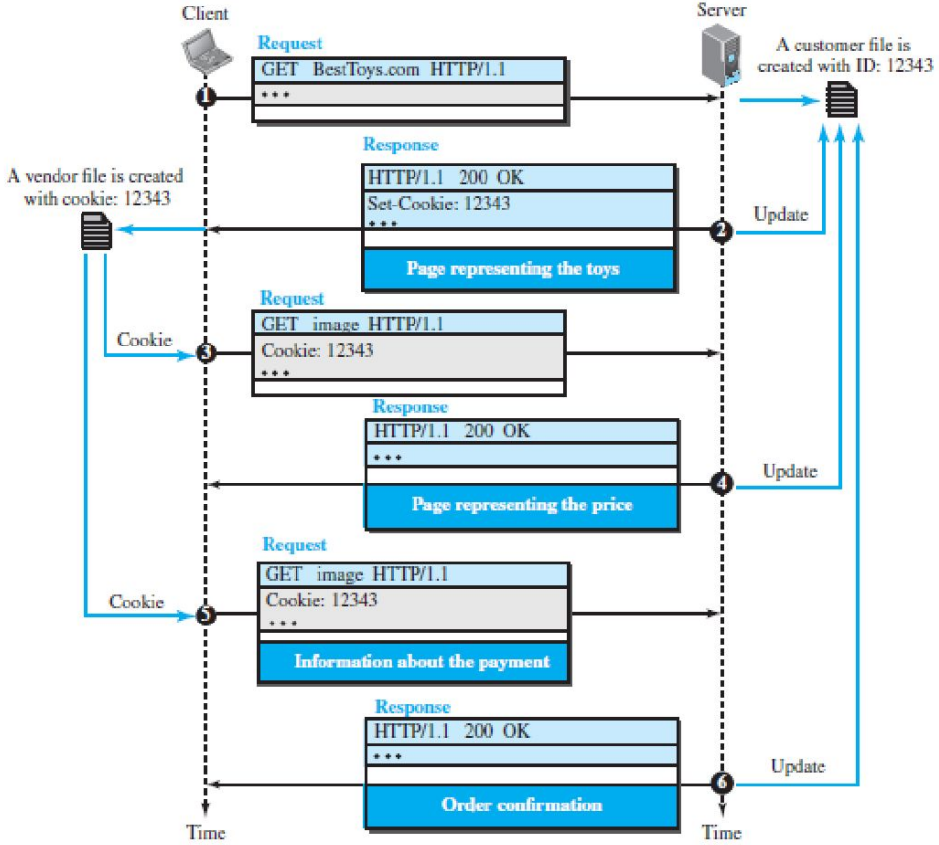
Cookies

- Originally, web was designed as a stateless entity (i.e.) Any information or details about a client will be stored at server side. Simply for each request, a response will come
- But today web has evolved to a different dimension:
  - Websites as electronic stores
  - Allow only registered clients
  - Websites as portal, the user selects the webpage he wants to see
  - Some websites are only advertising agencies

Using Cookies

- It is a small piece of data stored in users system by the browser while browsing a website.
- When the client receives the response from server on request, the browser stores the cookie in the cookie directory.
- Next time, when a client sends a request to a server, the browser looks in the cookie directory to
- see if it can find a cookie sent by that server. If found, the cookie is included in the request.
- Example – e-commerce

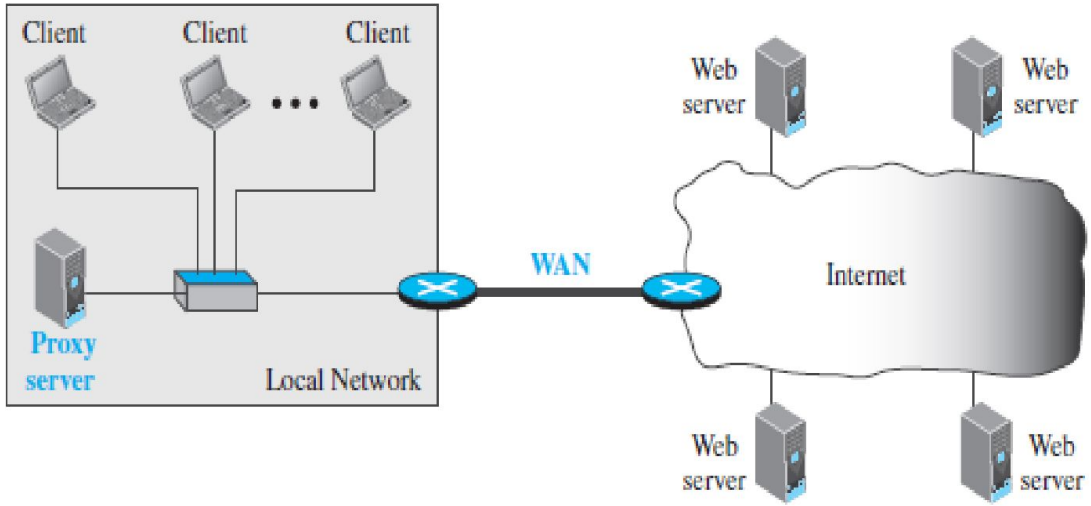
Cookie Scenario



Web caching: Proxy server

- Proxy server acts as a gateway between client and server.
- It keeps copies of responses to recent requests.
- On receiving the request from client, proxy server checks its cache and if it is not found then the request is sent to corresponding server.
- This reduces the load on the original server, decreases traffic, and improves latency.
- However, to use the proxy server, the client must be configured to access the proxy instead of the target server.

Sample Proxy server scenario



HTTP security

- HTTP does not provides security
- But HTTP running over Secure Socket layer (SSL) which is referred as HTTPS provides,
  - confidentiality
  - client and server authentication
  - data integrity

DHCP

Introducing DHCP

- DHCP is a service that permits network administrators to set up servers to allocate and manage collections of IP addresses for workstations, desktop computers, and other client machines that do not require fixed IP addresses

- DHCP can also supply important IP configuration data for clients, including the subnet mask, the local IP gateway (router) address, and even DNS and WINS data, where needed or appropriate.

- DHCP servers can manage one or more ranges of IP addresses, each of which may be called an address pool (if considered as a range of available addresses from which unused addresses may be allocated), or an address scope (if considered as a range of numeric IP addresses that fall under DHCPs control)

- Here is a brief rundown of how DHCP works, from a client perspective.

- When TCP/IP is configured on the client computer, the Obtain an IP address automatically option button is the only necessary set-up element. Everything is automatic.

- The next time the workstation attempts to access the network (older versions of Windows must be rebooted first), it broadcasts a DHCP address request to the network because it has no IP address, but is now configured as a DHCP client.

- All DHCP servers present on the same cable segment or broadcast domain receive this request, and send back a message that indicates a willingness to grant an address lease, if an address is available

- Every computer that utilizes TCP/IP protocol should know its IP address.
- In addition to this, Subnet mask is also needed, if the computer is under a subnet.
- The other two information needed for most of the recent machines are
    - The default router's address – to interface with other networks
    - The name server's address – to use names rather than addresses.

DHCP (Definition)

It is a Client/server protocol to provide the four required parameters to a diskless machine to enable the machine communicate with other networks.

DHCPs Origins

- The DHCP protocol is an extension of an earlier IP protocol called BOOTP.

- BOOTP was originally developed to permit diskless workstations to bootstrap from a Programmable Read-Only Memory (PROM) or Erasable PROM (EPROM) on their network interface cards

DHCP Software Elements

- Three pieces of software that work together define a complete DHCP networking environment
- DHCP client
- DHCP server
- DHCP relay agent
- Please note that most other DHCP requests such as lease renewals or surrenders occur as unicast messages because as soon as a machine obtains an IP address and a default IP gateway address, it is able to communicate directly with the DHCP server and no longer needs an intermediary

DHCP Lease Types

- A DHCP server recognizes three types of address leases
- Manual With a manual lease, the administrator explicitly assigns all IP addresses manually
- Automatic The DHCP server permanently assigns certain IP addresses
- Dynamic The DHCP server assigns addresses for specific periods of time

IP Address Management with DHCP

- When a DHCP client has no IP address (booting for the first time, or after a lease expires), it must broadcast a request for an IP address to obtain one this process is called DHCP Discovery

- DHCP servers that can hear this discovery broadcast offer an IP address to a client for a specific amount of time (the lease time)

- The default DHCP lease time varies according to which server is used

- In the middle of the lease time, the client starts a renewal process to determine if it can keep the address past the lease time
- If the client cannot renew the address from that DHCP server within the stipulated lease period, that client must begin the more desperate process of renewing the address from another DHCP server
- This is called the rebinding process
- If rebinding fails, a client must completely release its address

- The DHCP Discovery process relies on the initial DHCP broadcast
- Naturally, routers do not forward these discovery broadcasts so the entire discovery process is a local process
- There must be a DHCP server on the local network segment
- Because it is impractical to place a DHCP server on every network segment, the DHCP specification includes the relay agent process to help route the DHCP discovery broadcasts to another network segment

The Standard Address Discovery Process

- The DHCP Discovery process actually uses four packets
- DHCP Discover packet
- DHCP Offer packet
- DHCP Request packet
- DHCP Acknowledge packet

The Discover Packet

- During the DHCP Discovery process, the client broadcasts a Discover packet that identifies the clients hardware address
- If the DHCP client was on the network before, the client also defines a preferred address typically the client prefers the last address it used
- The Message Type value is one this indicates that this packet is a DHCP Discover packet
- The Client Identifier field value is based on the clients hardware address
- DHCP Discover Packet Is Always Sent as a Hardware and IP Broadcast

The Offer Packet

- The DHCP server sends the Offer packet to offer an IP address to the DHCP client
- The Offer packet includes the IP address that is offered to the client, and sometimes answers to the requested options in the DHCP Discover packet
- Note in the IP address field that the DHCP server offers 10.1.0.2 to the client
- DHCP Offer Packet Includes the Suggested IP Address for the DHCP Client

The Request Packet

- Once the Offer packet is received, the client can either accept the offer by issuing a DHCP Request packet, or reject the offer by sending a DHCP Decline packet
- Typically, a client only sends a Decline if it received more than one Offer
- DHCP Client May List Additional Configuration Parameters in the DHCP Request Packet

The Acknowledgement Packet

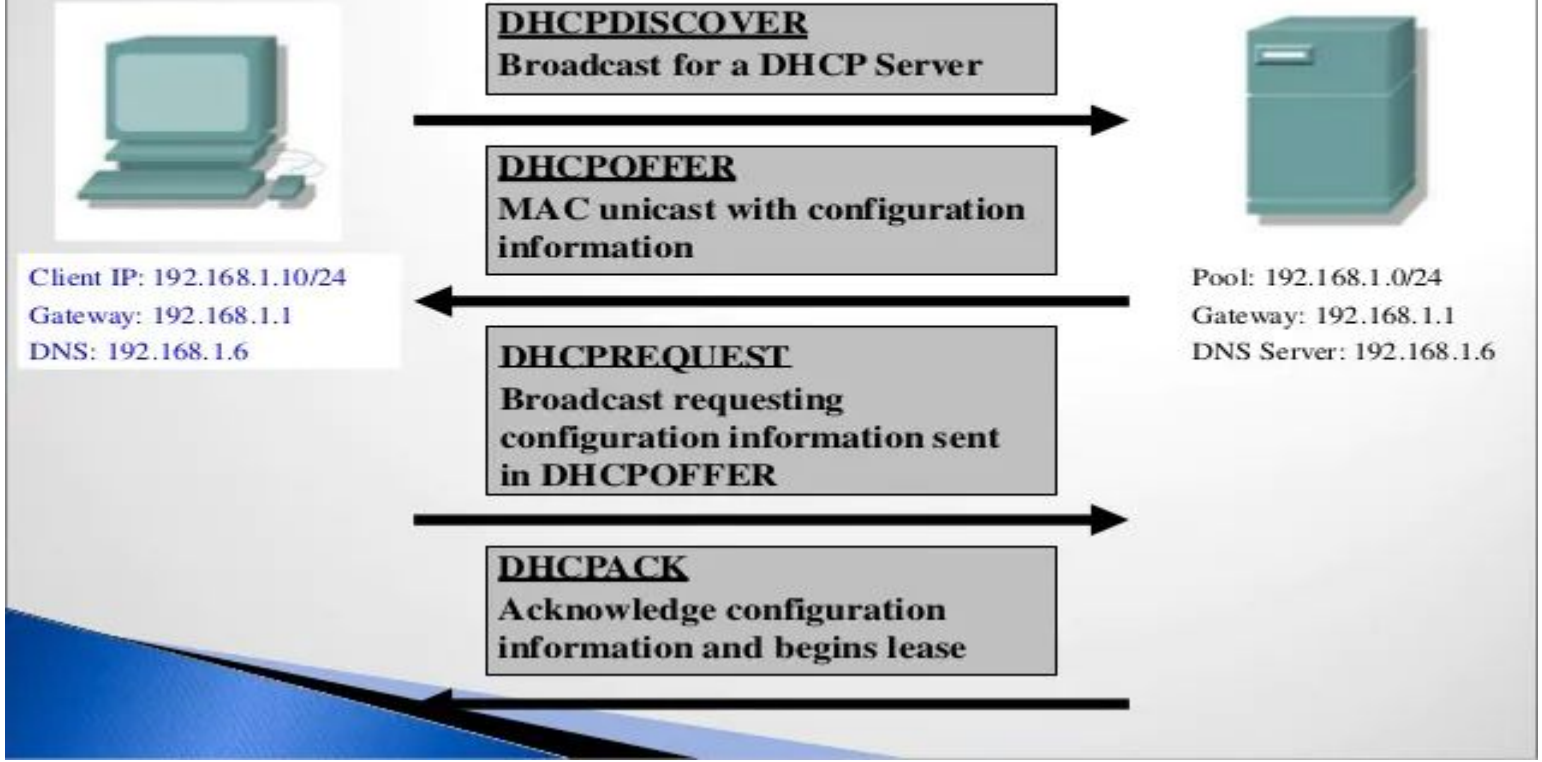
- Acknowledgement packet is sent from the server to the client to indicate the completion of the four-packet DHCP Discovery process

- This response contains answers to any options to which the DHCP server replies

DHCP Operation

- The operation is initiated with a broadcasting request by the client depending upon the client and server's location, which could be any one of the following
- Same network - Client and server are present on the same network
- Different network - Client and server are present on different network

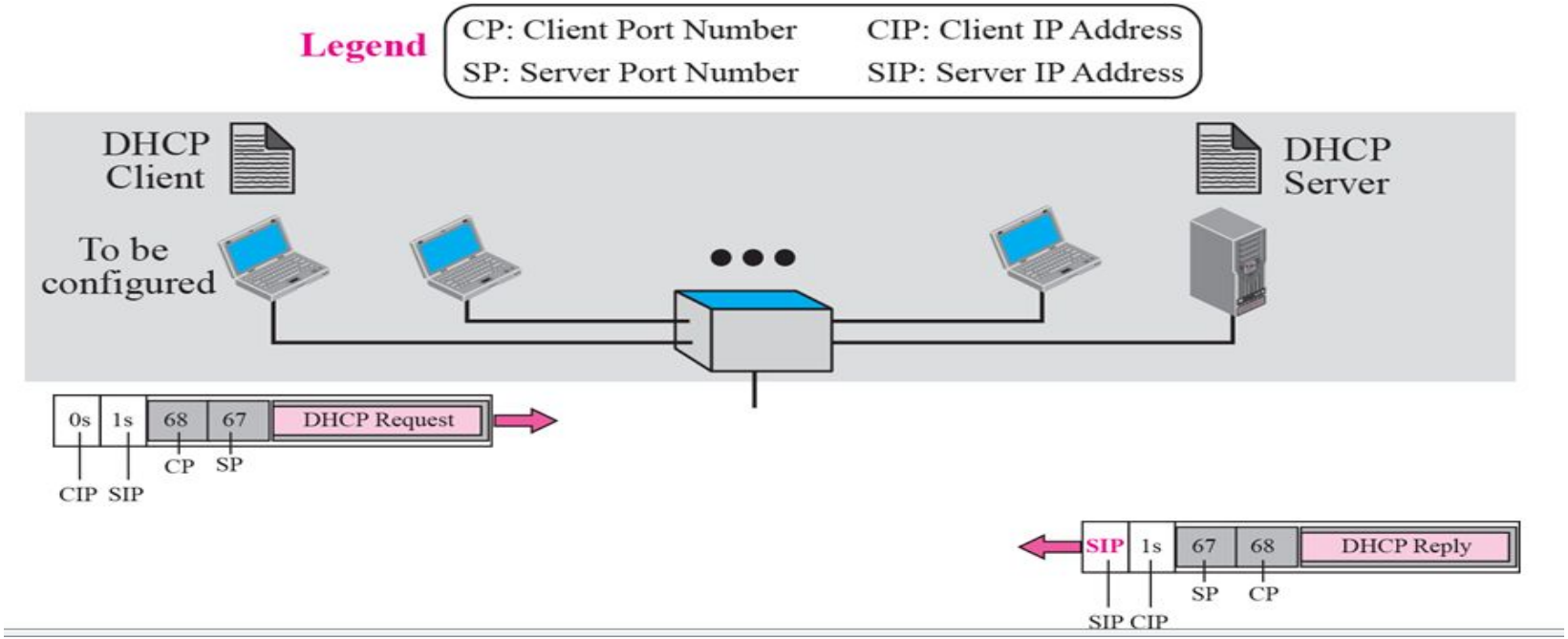
Normal DHCP Operation



DHCP – a client-server protocol

- **DHCP operates in a Client/Server environment and uses the following messages**
  - DHCPDISCOVER : Client request for server
  - DHCPOFFER: DHCP server replies to client with configuration information
  - DHCPREQUEST: Client requests the use of configuration information from one of the DHCP servers that sent an offer
    - DHCPNAK
      - DHCP server declines Client request to use configuration information
  - DHCPACK:
    - from DHCP server acknowledges that Client can now begin to use configuration information
  - DHCPRELEASE
    - Client requests a release of its DHCP configuration

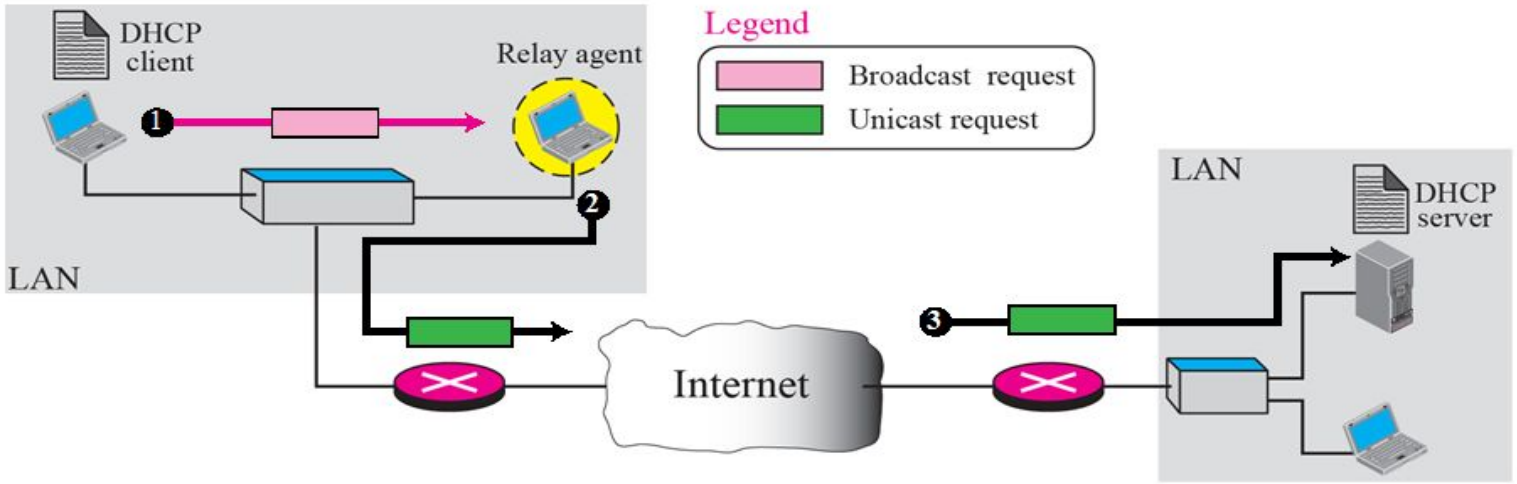
Same Network



Same network Operation

- A open command is provided by the server on UDP port number 67.
- Server waits for the client to respond
- The server gets the response from the booted client on port number 68
- A connection is now established between the source port 67 and destination port 68 by the server acknowledging with either a broadcast or unicast message.

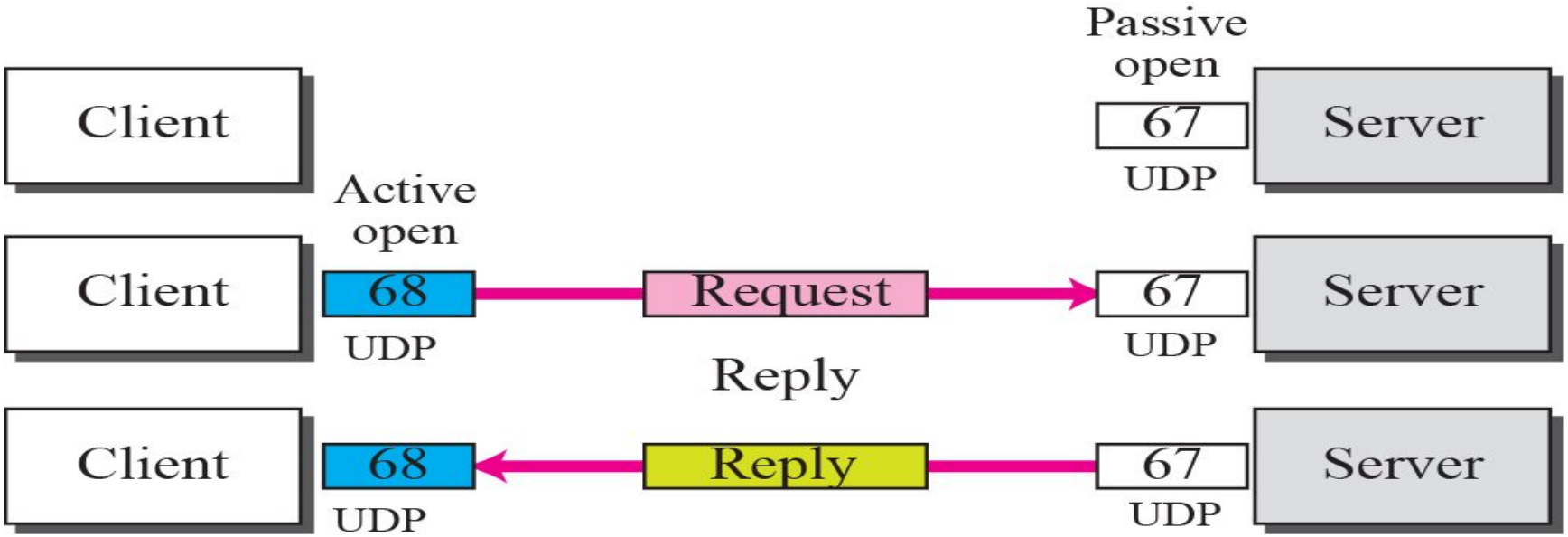
Different network



Different network Operation

- As the client is unaware of the server, a DHCP request is broadcasted.
- A relay agent (host) is used, as the router discards the broadcasted IP datagram.
- This relay agent is aware of the server's address and hence listens on UDP port 67 for the messages
- The received message is enfold in a unicast datagram (with the destination address) and sent to the server by the relay.
- It reaches the server through any router

UDP ports


Passive
open
Client
67
Server
UDP
Active
open
Client
68
Request
67
Server
UDP
UDP
Reply
Client
68
Reply
67
Server
UDP
UDP

UDP Ports

- Port 67 - used by server (Common)
- Port 68 - used by client (to overcome the demultiplexing issue)
- Consider the below scenario
    - Host A uses DHCP client
    - Host B uses DAYTIME client
    - (both are in the same network and uses ephermal port 2017)
    - A broadcast message is sent from the server as an acknowledgement

UDP ports (Contd..)

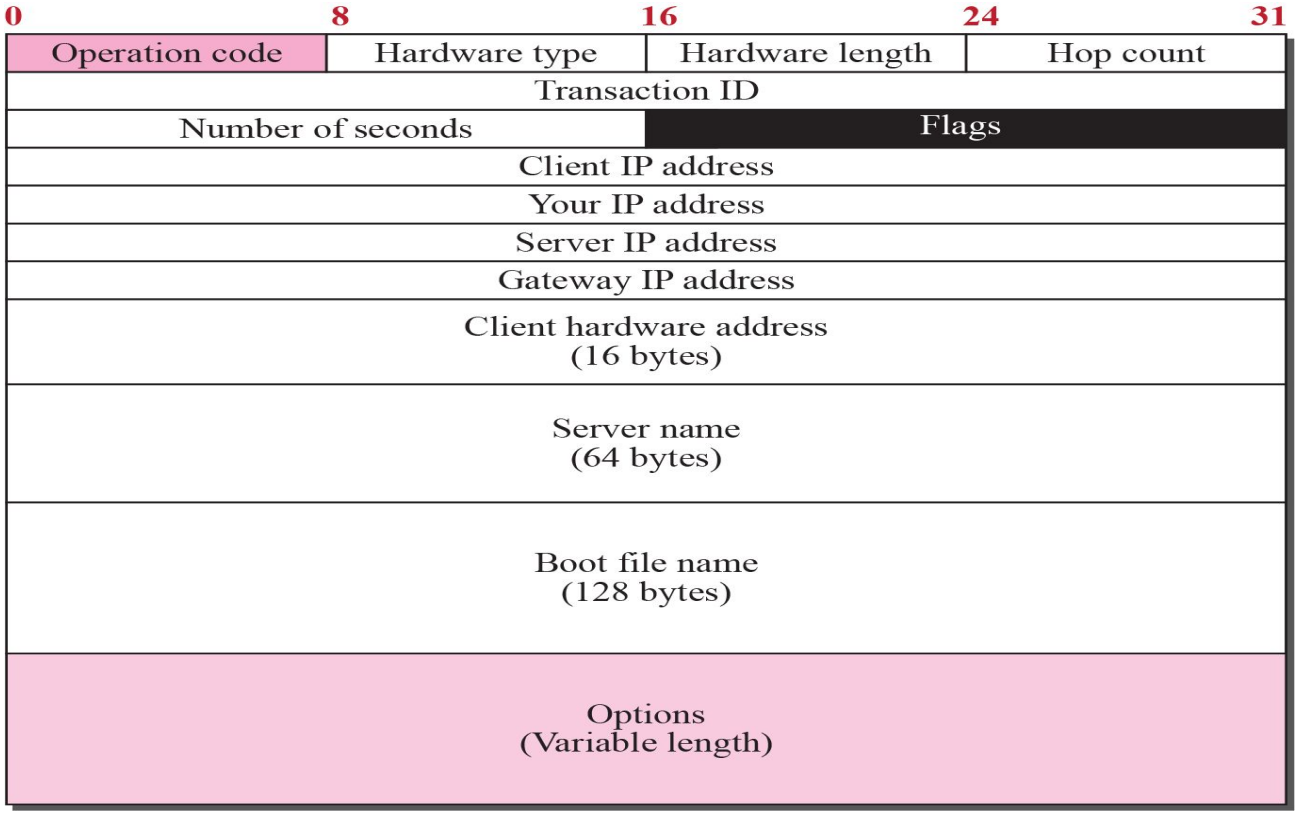
- This message contains the destination port 2017 and broadcast IP address FFFFFFFF16
- Host A finds a message from application program on 2017
- A correct message and incorrect message is delivered to DHCP and DAYTIME clients respectively
- Transaction ID is also used to identify the clients which avoids the confusion created.

Error control

- To take a control over the lost or damaged response, DHCP requires
    - Checksum
    - Retransmission

- To prevent traffic jam (Created by retransmission)
    - Random numbers for timers are used

Packet Format



Packet Format (Contd..)

- Operation code (8 bit) – Variant of DHCP
- Hardware type (8 bit) - variant of physical network
- Hardware length (8 bit) - length of physical address in bytes
- Hop count (8 bit) - Maximum number of hops
- Transaction ID (4 byte) - To match a reply with the request
- Number of seconds (16 bit) – Time elapsed to boot the client
- Flag (16 bit) – left-most bit is used leaving the remaining bits to be zero.
- Client IP address (4 byte) – holds client's IP address
- Server IP address (4 byte) - holds server's IP address

Packet Format (Contd..)

- Gateway IP address (4 byte) – holds router's IP address
- Client Hardware address – Client's physical address
- Server name (64 byte) – holds server's domain name
- Boot file name (128 byte) – Holds path name
- Options (64 byte) – carries either vendor information or other additional information.

CONFIGURATION

Static address allocation

- A database is used to match physical address to IP address.
- DHCP is backward compatible in this case

Dynamic address allocation

- An additional database containing the unused IP addresses.
- On request from a client, an IP address (temporary) from this database is allocated to the requesting client on lease.
- This is based on the entry in the static database.
- This allocation is essential when there is a transfer of host from one network to another.

Transition states

- To enable dynamic address allocation, the machine passes through several transitions
- The type of the transition is indicated tag 53.

States

INIT state – Client initiates by sending DHCPDISCOVER message

SELECTING STATE – SERVERS offers DHCPOFFER message. Client has to select one among the offers. Client sends DHCPREQUEST message to the selected server.

REQUESTING STATE – Until the client receives DHCPACK message, it stays in the same state

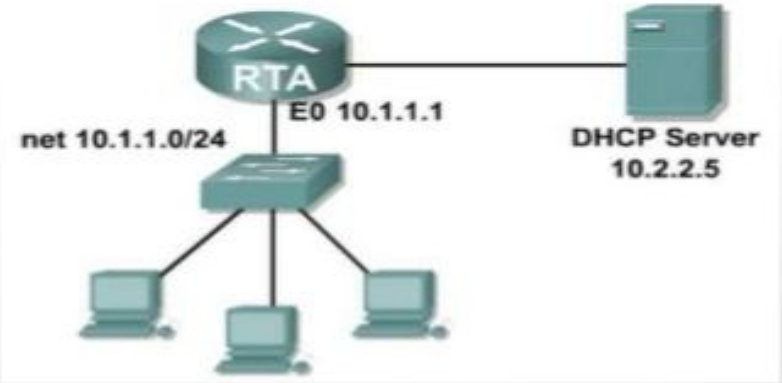
States (Contd..)

- BOUND STATE – Client uses the IP address until the lease expires. DHCPREQUEST is again initiated by the client to renew the lease when 50% of the lease period is expired.
- RENEWING STATE – If DHCPACK is received, client gets back to BOUND state otherwise enters into the REBINDING state after 87.5% of time expires
- REBINDING STATE – The client does the following
    - DHCPNACK / lease expired – Client goes to the initializing state and gets new IP address.
    - DHCPACK – It goes to the bound state – resets timer.

DCHP Configuration Example

```
RTA(config)#ip helper-address 10.2.2.5
```

- The `ip helper-address` command configures the router to forward eight UDP services:
  - Time
  - TACACS
  - DNS
  - BOOTP/DHCP Server
  - BOOTP/DHCP Client
  - TFTP
  - NetBIOS Name Service
  - NetBIOS datagram Service



Verify DHCP Configuration

- Use the following commands to verify and troubleshoot your DHCP configuration:
  - **`show running-config`**
    - view the DHCP configuration
  - **`show ip dhcp binding`**
    - displays IP to MAC address bindings and lease expiration date and time
  - **`show ip dhcp server statistics`**
    - displays a count of the number and type of DHCP messages sent and received
  - **`debug ip dhcp server events`**
    - watch interactions between the DHCP server and clients

E - Mail: SMTP, POP, IMAP, and MIME

SMTP

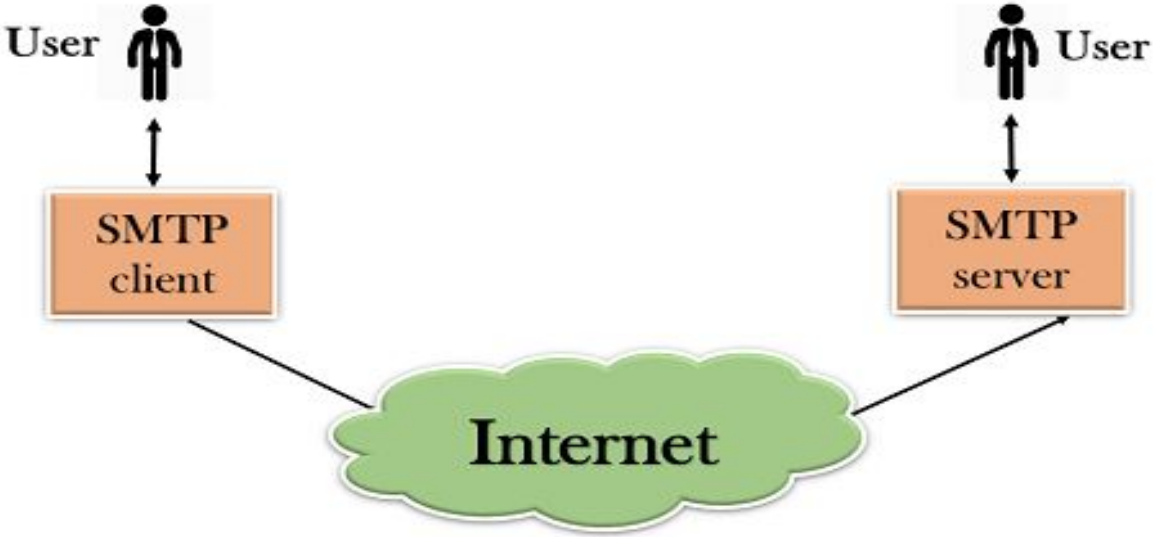
- SMTP stands for Simple Mail Transfer Protocol.
- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called Simple Mail Transfer Protocol.
- It is a program used for sending messages to other computer users based on e-mail addresses.
- It provides a mail exchange between users on the same or different computers, and it also supports:

  It can send a single message to one or more recipients.

  Sending message can include text, voice, video or graphics.

  It can also send the messages on networks outside the internet.
- The main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.

Components of SMTP

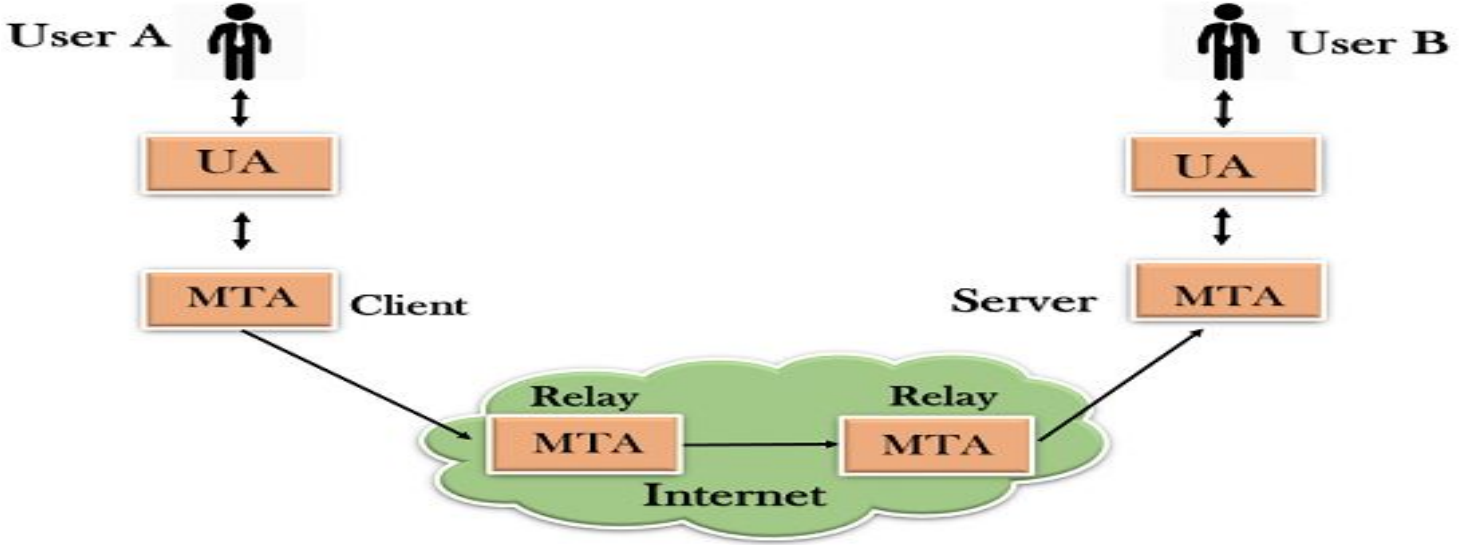


- First, we will break the SMTP client and SMTP server into two components such as user agent (UA) and mail transfer agent (MTA). The user agent (UA) prepares the message, creates the envelope and then puts the message in the envelope. The mail transfer agent (MTA) transfers this mail across the internet.

Components of SMTP(Contd..)

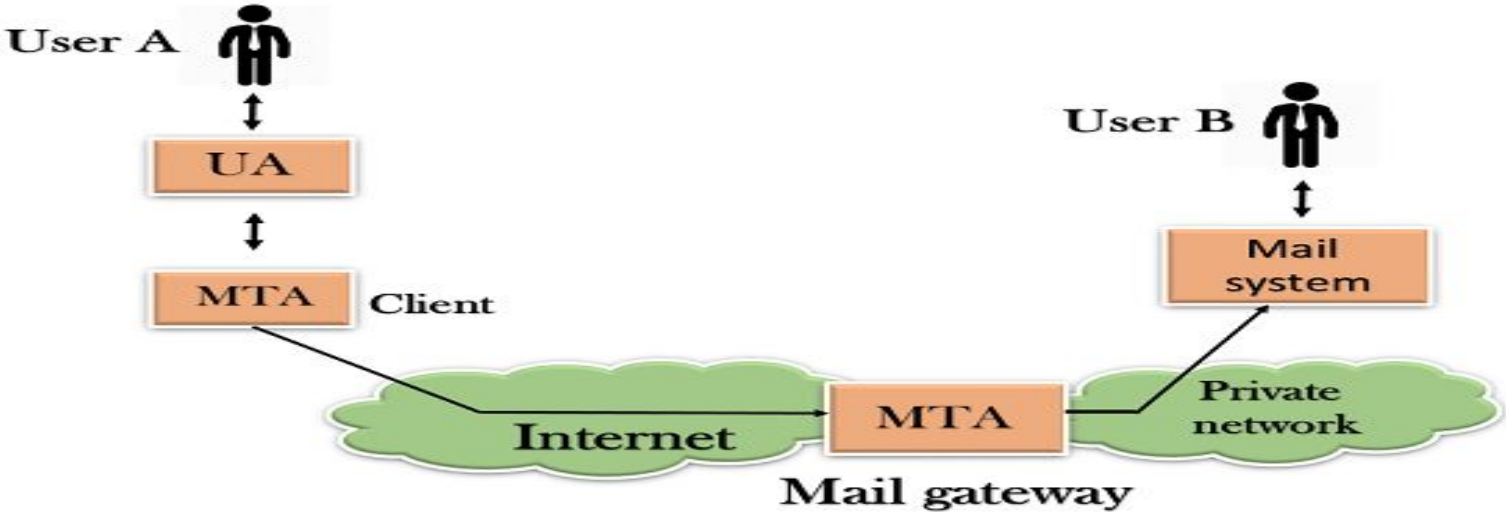
- SMTP allows a more complex system by adding a relaying system. Instead of just having one MTA at sending side and one at receiving side, more MTAs can be added, acting either as a client or server to relay the email.

Components of SMTP(Contd..)



- The relaying system without TCP/IP protocol can also be used to send the emails to users, and this is achieved by the use of the mail gateway. The mail gateway is a relay MTA that can be used to receive an email.

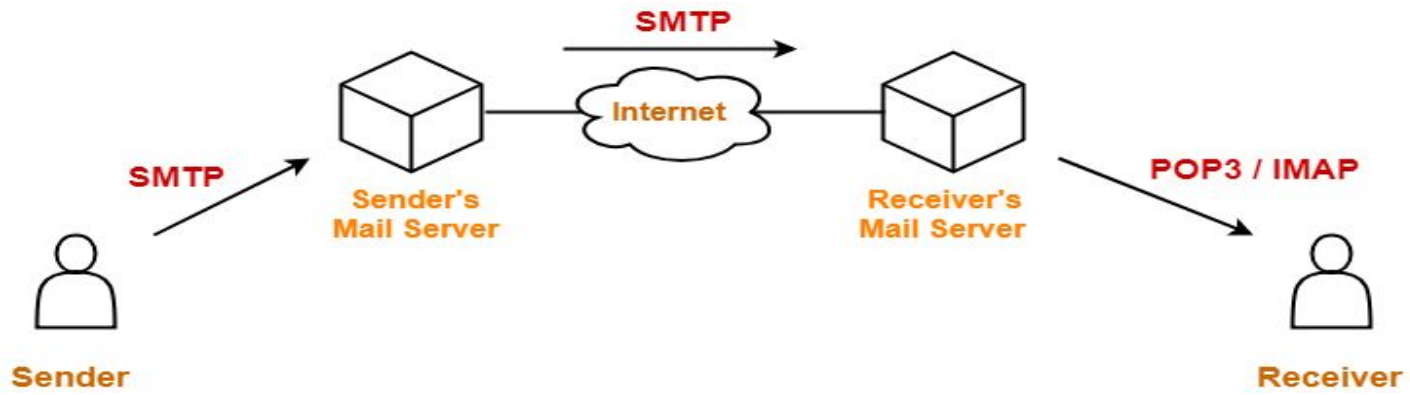
Components of SMTP(Contd..)



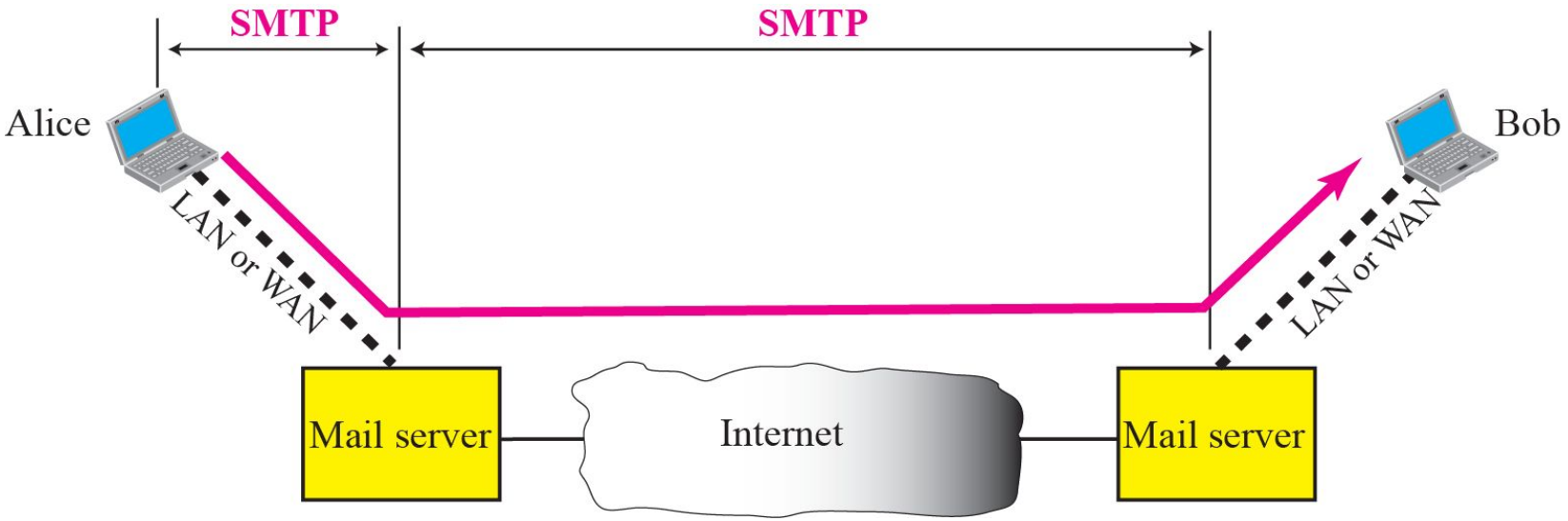
- The relaying system without TCP/IP protocol can also be used to send the emails to users, and this is achieved by the use of the mail gateway. The mail gateway is a relay MTA that can be used to receive an email.

Working of SMTP

- SMTP server is always on a listening mode.
- Client initiates a TCP connection with the SMTP server.
- SMTP server listens for a connection and initiates a connection on that port.
- The connection is established.
- Client informs the SMTP server that it would like to send a mail.
- Assuming the server is OK, client sends the mail to its mail server.
- Client's mail server use DNS to get the IP Address of receiver's mail server.
- Then, SMTP transfers the mail from sender's mail server to the receiver's mail server.



SMTP range


SMTP
SMTP
Alice
Bob
LAN or WAN
LAN or WAN
Mail server
Internet
Mail server

SMTP range (Contd..)

- SMTP is used two times, between the sender and the sender's mail server and between the two mail servers. SMTP defines how commands and responses must be sent back and forth

Commands and responses

- SMTP uses commands and responses to transfer messages between an MTA client and an MTA server.

Commands

- Commands are sent from the client to the server.

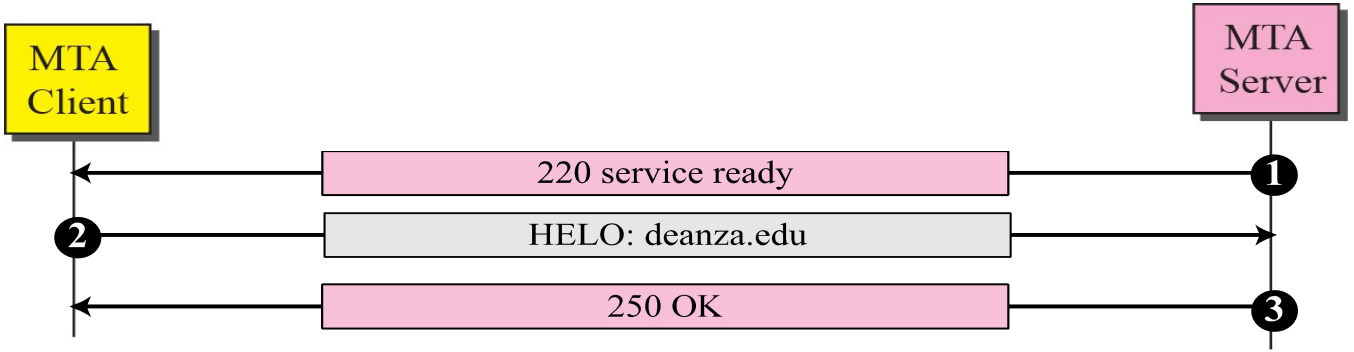
Keyword	*Argument(s)*	*Keyword*	*Argument(s)*
HELO	Sender's host name	NOOP	
MAIL FROM	Sender of the message	TURN	
RCPT TO	Intended recipient	EXPN	Mailing list
DATA	Body of the mail	HELP	Command name
QUIT		SEND FROM	Intended recipient
RSET		SMOL FROM	Intended recipient
VRFY	Name of recipient	SMAL FROM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

Responses

Code	*Description*
	Positive Completion Reply
211	System status or help reply
214	Help message
220	Service ready
221	Service closing transmission channel
250	Request command completed
251	User not local; the message will be forwarded
	Positive Intermediate Reply
354	Start mail input
	Transient Negative Completion Reply
421	Service not available
450	Mailbox not available
451	Command aborted: local error
452	Command aborted; insufficient storage
	Permanent Negative Completion Reply
500	Syntax error; unrecognized command
501	Syntax error in parameters or arguments
502	Command not implemented
503	Bad sequence of commands
504	Command temporarily not implemented
550	Command is not executed; mailbox unavailable
551	User not local
552	Requested action aborted; exceeded storage location
553	Requested action not taken; mailbox name not allowed
554	Transaction failed

- Responses are sent from the server to the client. A response is a three-digit code that may be followed by additional textual information.

Connection establishment

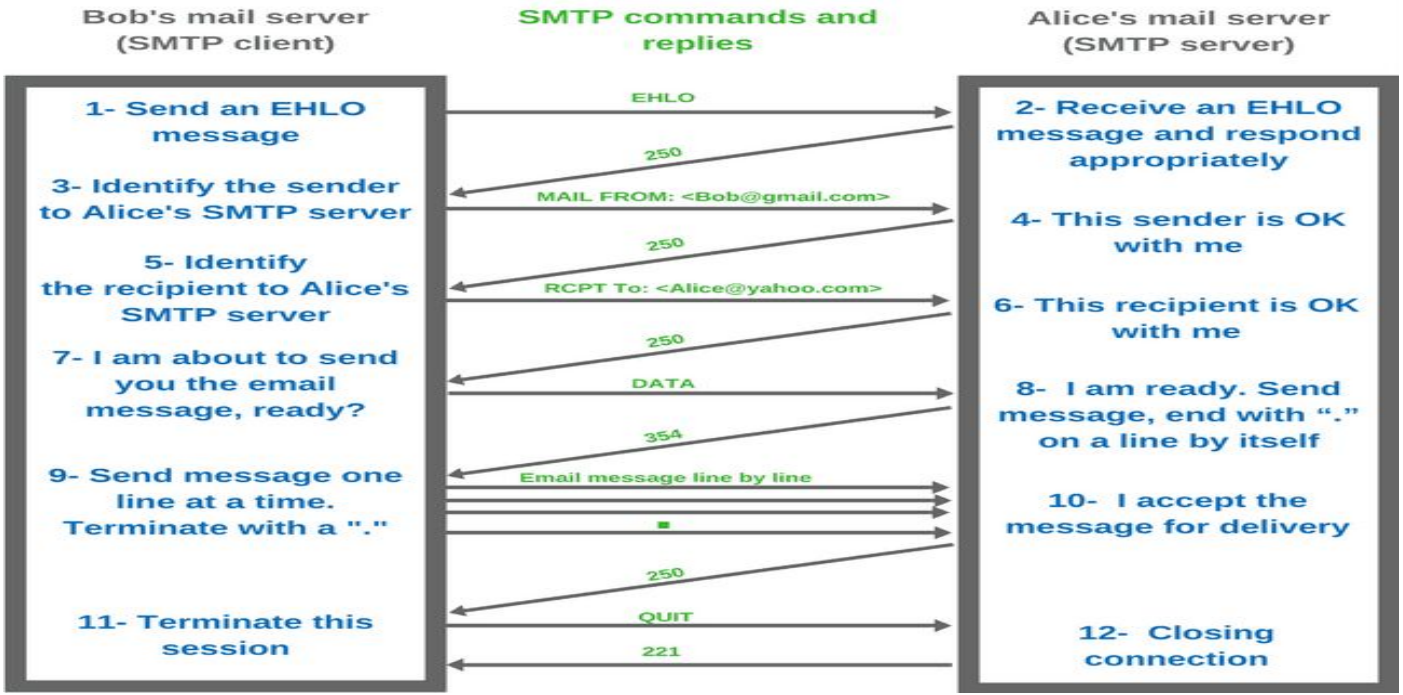


- The server sends code 220 to tell the client that it is ready to receive mail.
- The client sends the HELO message to identify itself using its domain name address. This step is necessary to inform the server of the domain name of the client.
- The server responds with code 250

Mail Transfer

- The client sends the message to introduce the sender of the message. It includes the mail address of the sender. This step is needed to give the server the return mail address for reporting messages.
- The server responds with code.
- The client sends the message, which includes the mail, that address of the recipient.
- The server responds with code.
- The client sends the DATA message to initialize the message transfer.
- The server responds with code to start mail input.
- The client sends the contents of the message in consecutive lines. Each line is terminated by a two-character end-of-line token.
- The server responds with code.

Mail transfer



POP3

POP3(Post Office Protocol, version 3):

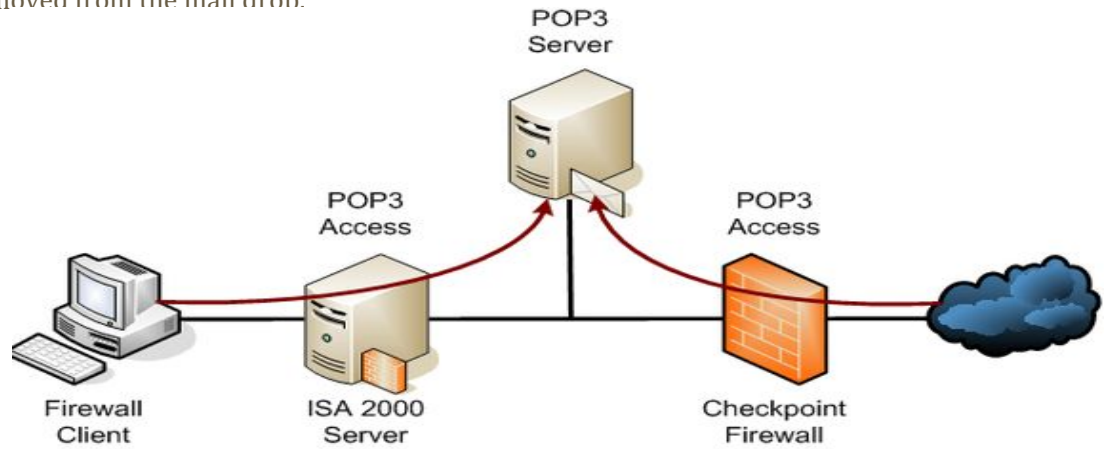
- The client POP3 software is installed on the recipient computer; the server POP3 software is installed on the mail server. Mail access starts with the client when the user needs to download its e-mail from the mailbox.
- The client opens a connection to the server on TCP port. It then sends its user name and password to access the mailbox. The user can then list and retrieve the mail messages, one by one.
- POP3 is the most recent version of a standard protocol for receiving e-mail. It is a client/server protocol in which e-mail is received and held for you by your Internet server. POP3 is designed to delete mail on the server as soon as the user has downloaded it.
- The Post Office Protocol provides access via an Internet Protocol (IP) network for a user client application to a mailbox (mail drop) maintained on a mail server. The protocol supports download and delete operations for messages. POP3 clients connect, retrieve all messages, store them on the client computer, and finally delete them from the server. This design of POP and its procedures was driven by the need of users having only temporary Internet connections, such as dial-up access, allowing these users to retrieve e-mail when connected, and subsequently to view and manipulate the retrieved messages when offline.

POP3 (Contd..)

- POP3 clients also have an option to leave mail on the server after download. By contrast, the Internet Message Access Protocol (IMAP) was designed to normally leave all messages on the server to permit management with multiple client applications, and to support both connected (online) and disconnected (offline) modes of operation.
- A POP3 server listens on well-known port number 110 for service requests. Encrypted communication for POP3 is either requested after protocol initiation, using the STLS command, if supported, or by POP3S, which connects to the server using Transport Layer Security (TLS) or Secure Sockets Layer (SSL) on well-known TCP port number 995.

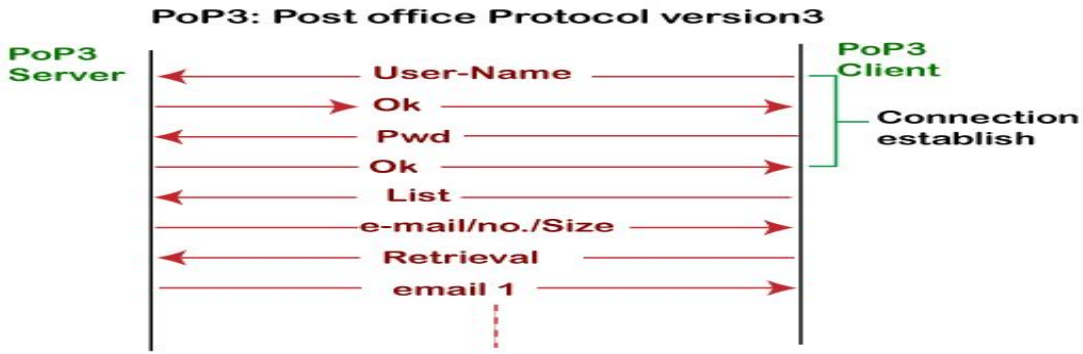
POP3 (Contd..)

- Messages available to the client are determined when a POP3 session opens the mail drop, and are identified by message-number local to that session or, optionally, by a unique identifier assigned to the message by the POP server. This unique identifier is permanent and unique to the mail drop and allows a client to access the same message in different POP sessions. Mail is retrieved and marked for deletion by the message-number. When the client exits the session, mail marked for deletion is removed from the mail drop.



Working of Pop3 Protocol

- To establish the connection between the POP3 server and the POP3 client, the POP3 server asks for the user name to the POP3 client. If the username is found in the POP3 server, then it sends the ok message. It then asks for the password from the POP3 client; then the POP3 client sends the password to the POP3 server. If the password is matched, then the POP3 server sends the OK message, and the connection gets established. After the establishment of a connection, the client can see the list of mails on the POP3 mail server. In the list of mails, the user will get the email numbers and sizes from the server. Out of this list, the user can start the retrieval of mail.
- Once the client retrieves all the emails from the server, all the emails from the server are deleted. Therefore, we can say that the emails are restricted to a particular machine, so it would not be possible to access the same mails on another machine. This situation can be overcome by configu



Advantages of a POP3 protocol

- It allows the users to read the email offline. It requires an internet connection only at the time of downloading emails from the server. Once the mails are downloaded from the server, then all the downloaded mails reside on our PC or hard disk of our computer, which can be accessed without the internet. Therefore, we can say that the POP3 protocol does not require permanent internet connectivity.
- It provides easy and fast access to the emails as they are already stored on our PC.
- There is no limit on the size of the email which we receive or send.
- It requires less server storage space as all the mails are stored on the local machine.
- There is maximum size on the mailbox, but it is limited by the size of the hard disk.
- It is a simple protocol so it is one of the most popular protocols used today.
- It is easy to configure and use.

Disadvantages of POP3 protocol

- If the emails are downloaded from the server, then all the mails are deleted from the server by default. So, mails cannot be accessed from other machines unless they are configured to leave a copy of the mail on the server.
- Transferring the mail folder from the local machine to another machine can be difficult.
- Since all the attachments are stored on your local machine, there is a high risk of a virus attack if the virus scanner does not scan them. The virus attack can harm the computer.
- The email folder which is downloaded from the mail server can also become corrupted.
- The mails are stored on the local machine, so anyone who sits on your machine can access the email folder.

IMAP4

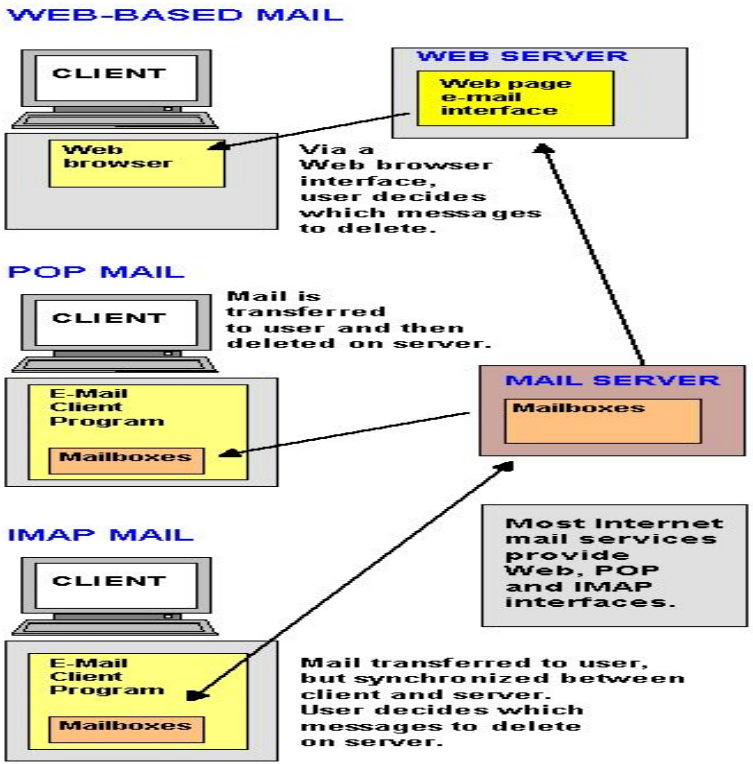
- IMAP stands for **Internet Message Access Protocol**, and it's the open standard that describes how to access messages in an email mailbox.
- **IMAP** is short for Internet Message Access Protocol. With **IMAP**, the message does not remain on the local device, such as a computer, it remains on the server. **POP3** is short for Post Office Protocol. With **POP3** mail, it will connect and attempt to keep the mail located on the local device (computer or mobile).
- IMAP4 clients **can create, rename, and/or delete mailboxes** (usually presented to the user as folders) on the server, and copy messages between mailboxes. Multiple mailbox support also allows servers to provide access to shared and public folders.
- IMAP4 **provides mechanisms for storing messages received by SMTP in a receptacle called a mailbox**. An IMAP4 server stores messages received by each user until the user connects to download and read them using an IMAP4 client such as Microsoft Outlook 2000 or Microsoft Outlook Express.

IMAP4(contd…)

- IMAP4 includes a number of features that are not supported by POP3. Specifically, IMAP4 allows users to
- Access multiple folders, including public folders
- Create hierarchies of folders for storing messages
- Leave messages on the server after reading them so that they can access the messages again from another location
- Search a mailbox for a specific message to download
- Flag messages as read
- Selectively download portions of messages or attachments only
- Review the headers of messages before downloading them
- To retrieve a message from an IMAP4 server, an IMAP4 client first establishes a Transmission Control Protocol (TCP) session using TCP port 143. The client then identifies itself to the server and issues a series of IMAP4 commands:

  LIST: Retrieves a list of folders in the client's mailbox
  SELECT: Selects a particular folder to access its messages
  FETCH: Retrieves individual messages

IMAP4(contd...)


WEB-BASED MAIL
CLIENT
Web browser
WEB SERVER
Web page e-mail interface
Via a Web browser interface, user decides which messages to delete.
POP MAIL
CLIENT
E-Mail Client Program
Mailboxes
Mail is transferred to user and then deleted on server.
MAIL SERVER
Mailboxes
IMAP MAIL
CLIENT
E-Mail Client Program
Mailboxes
Most Internet mail services provide Web, POP and IMAP interfaces.
Mail transferred to user, but synchronized between client and server. User decides which messages to delete on server.

IMAP4(Contd…)

- Internet Message Access Protocol (IMAP) allows remote manipulation of messages on the server. IMAP was implemented in response to the shortcomings of POP; including an inability for sophisticated mail manipulation on the server, and restricted access to mail from more than one computer.
- Similarly to POP and other protocols, the IMAP server responds to commands issued by the client. Every command is preceded by a unique, client-defined identifier (for example, A0001), which increments with each successive command. These commands allow a client to create and manipulate folders called "mailboxes" on the server in a way that is functionally equivalent to manipulating local folders. As commands are issued, an IMAP4 session progresses through four states: non-authenticated, authenticated, selected and logout.

IMAP4 Non-Authenticated State

- When a client makes a TCP connection with the server (typically on port 143), the session enters the non-authenticated state. In this state, the client has access to four commands: CAPABILITY (displays special capabilities of the server), NOOP (causes the server to give a positive response), LOGIN (authenticates the client), and LOGOUT (ends the session). In order for the session to continue, the client must supply authentication credentials with the LOGIN command. Once proper credentials have been supplied, the session moves into the authenticated state.

IMAP4(Contd…)

IMAP4 Authenticated State

- In the authenticated state, the client has access to all commands from the non-authenticated state (except for LOGIN). The client can also CREATE a mailbox, get the STATUS of a mailbox, RENAME a mailbox, and perform other commands involving the manipulation of mailboxes. The client may also select a valid mailbox using either the SELECT or the EXAMINE command, followed by a valid mailbox name. SELECT opens the mailbox with read/write privileges, whereas EXAMINE opens the mailbox with read-only privileges. Once one of these commands is executed successfully, the session moves into the selected state.

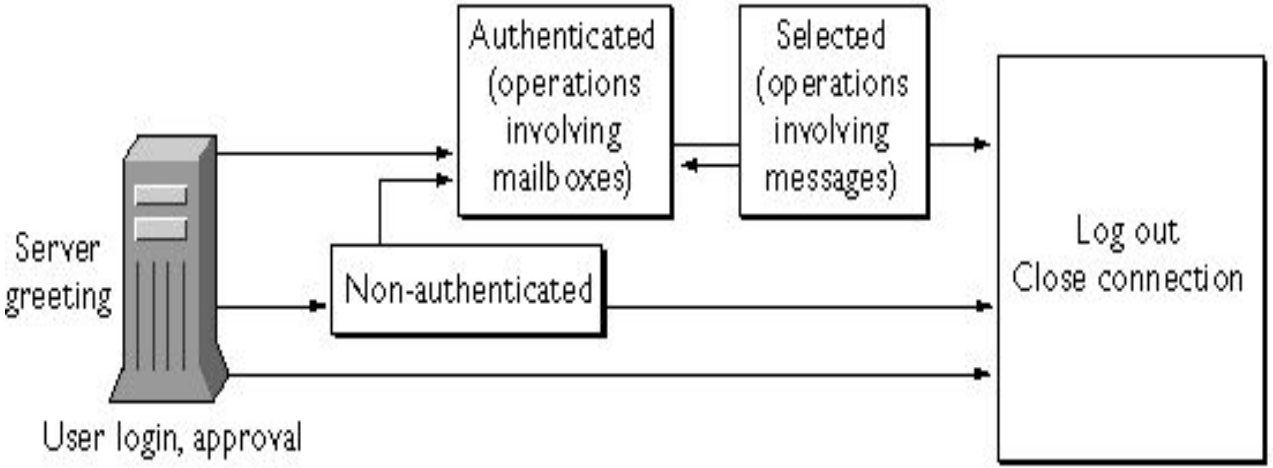
IMAP4 Selected State

- Messages are accessed in the selected state. The client can issue any of the commands from the authenticated state, as well as CLOSE (closes the mailbox and returns to authenticated state), EXPUNGE (removes all messages flagged for deletion), SEARCH (allows the client to find messages using certain criteria), FETCH (returns all or a part of a message), STORE (allows updating of flags stored with each message), and COPY (allows a message set to be copied to a mailbox). From the selected state, the client may use CLOSE to return to the authenticated state, or LOGOUT to go to the logout state.

IMAP4 Logout State

- In the logout state, the server simply terminates the connection.
- The graphic below illustrates this progression through the four states.

IMAP4(Contd…)



Note: All states can result in logging out and closing the connection in response to the logout command, server shutdown, or a closed connection.

IMAP4(Contd...)

ADVANTAGES

- Access emails from any computer
- Emails aren't lost if device breaks
- Ideal for those who travel a lot.

DISADVANTAGES

- Mails won't work without an active internet connection.
- In case email usage is more, you would need a larger mailbox storage which might cost more.
- Accessing mails little slower as compared to POP3, as all folders get synchronized every time there is a Send / Receive

IMAP4(Contd...)

Feature	POP3	IMAP
Protocol defined in	RFC 1939	RFC 2060
TCP port used	110	143
E-mail stored on	user's PC	Server
e-mail is read	offline	on-line
Connection time required	little	much
Use of sever resources	minimal	extensive
Multiple mailboxes	No	Yes
Mailboxes backup by	user	ISP
Good for mobile users	No	Yes
User control over downloading	little	great
Partial message download facility	No	Yes
Simple to implement	Yes	No
Widespread support	Yes	Growing

MIME

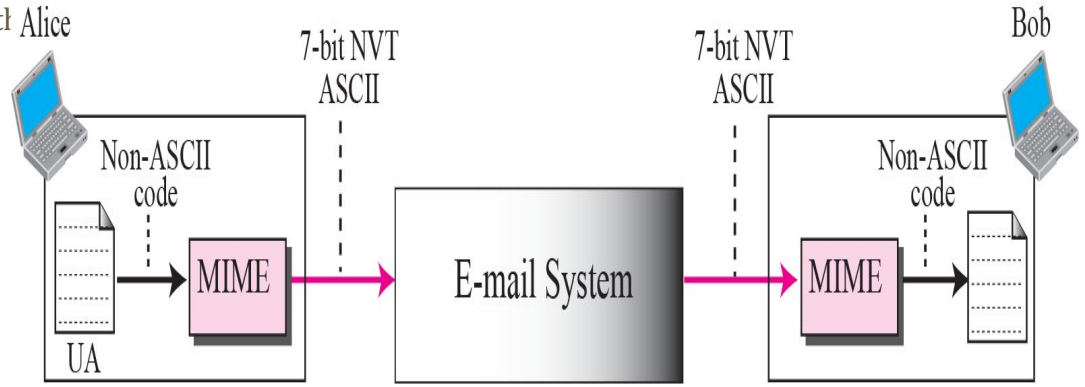
- **MIME** stands for ***(Multipurpose Internet Mail Extensions)***.
- It is widely used internet standard for coding binary files to send them as e-mail attachments over the internet.
- MIME allows an E-mail message to contain a non-ASCII file such as a video image or a sound and it provides a mechanism to transfer a non text characters to text characters.

MIME was invented to overcome the following limitations of SMTP:

- SMTP cannot transfer executable files and binary objects.
- SMTP cannot transmit text data of other language, e.g. French, Japanese, Chinese etc, as these are represented in 8-bit codes.
- SMTP services may reject mails having size greater than a certain size.
- SMTP cannot handle non-textual data such as pictures, images, and video/audio content.

MIME

- E - mail has a simple structure. It can send messages only in NVT 7-bit ASCII format.
- Multipurpose Internet Mail Extensions (MIME) is a supplementary protocol that allows non-ASCII data to be sent through e-mail.
- MIME transforms non-ASCII data at the sender site to NVT ASCII data and delivers it to the client MTA to be sent through the Internet.
- The message at tl

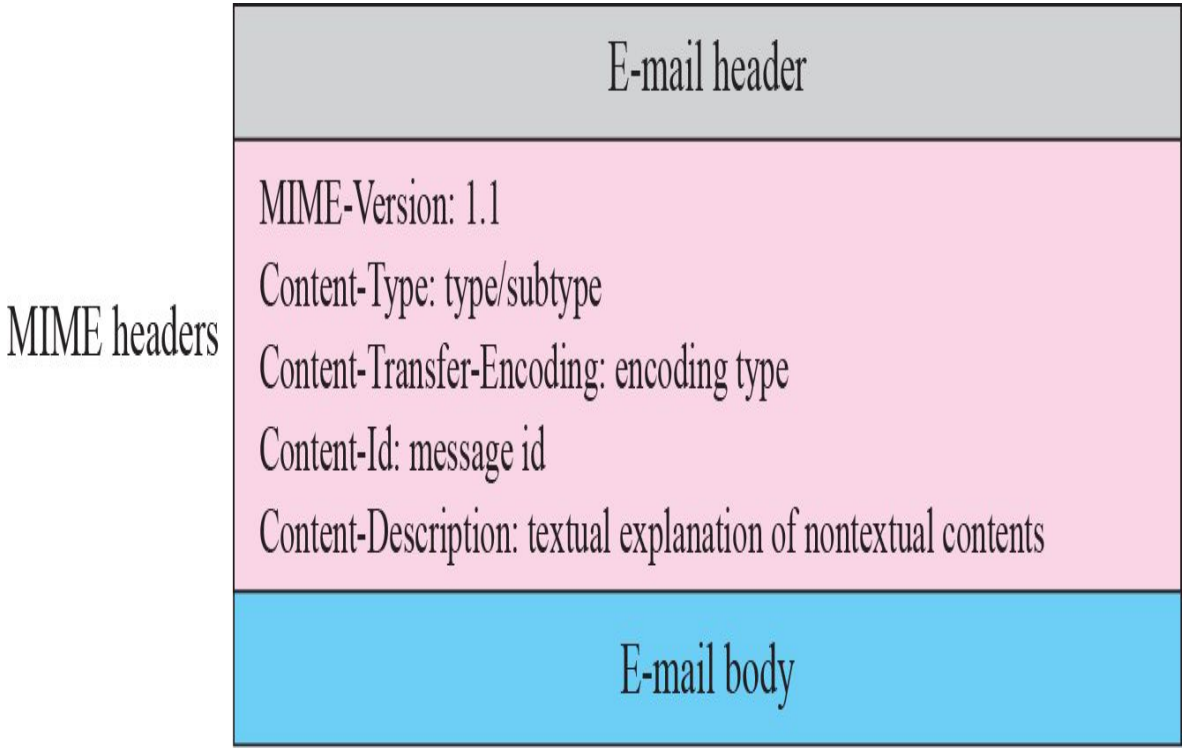


Multipurpose Internet Mail Extensions (MIME)

- MIME has five additional extensions to SMTP message.
- It supports multipart messages with more two parts, and allows the encoding of 8-bit binary data such as image files so that they can be using SMTP.
- The encoding method for translation binary information used by MIME, Base64 Encoding, essentially provides a mechanism for translating non text information into text characters.
- The MIME extensions are implemented as fields in the e-mail message header.

❑ The MIME fields are of the following: Content type, Content transfer encoding method, MME version number Content ID (optional), Content description (optional).

MIME header


E-mail header
MIME headers
MIME-Version: 1.1
Content-Type: type/subtype
Content-Transfer-Encoding: encoding type
Content-Id: message id
Content-Description: textual explanation of nontextual contents
E-mail body

MIME header (Contd..)

❑ **MIME Header**

The five header fields defined in MIME are as follows:

1. **MIME-version**. It indicates the MIME version being used. The current version is 1.1. It is represented as : MIME-version: 1.1.
2. **Content-type**.

✔ It describes the type and subtype of the data in the body of the message.

✔ The content type and content subtype are separated by slash.

✔ This field describes how the object in the body is to be interpreted.

✔ The default value is plaintext in US ASCII.

Content type field is represented as:

Context-type: <type/subtype; parameters>

Data Type and Subtype in MIME

- There are seven different types and fourteen sub-types of content.

The various content type are listed in the table below:

Type	*Subtype*	*Description*
Text	Plain	Unformatted
	HTML	HTML format (see Appendix E)
Multipart	Mixed	Body contains ordered parts of different data types
	Parallel	Same as above, but no order
	Digest	Similar to Mixed, but the default is message/RFC822
	Alternative	Parts are different versions of the same message
Message	RFC822	Body is an encapsulated message
	Partial	Body is a fragment of a bigger message
	External-Body	Body is a reference to another message
Image	JPEG	Image is in JPEG format
	GIF	Image is in GIF format
Video	MPEG	Video is in MPEG format
Audio	Basic	Single channel encoding of voice at 8 KHz
Application	PostScript	Adobe PostScript
	Octet-stream	General binary data (eight-bit bytes)

Content Transfer Encoding

3. **Content-transfer encoding:**

It describes how the object within the body has been encoded to US ASCII to make it acceptable for mail transfer.

The content transfer encoding field is represented as :

Content-transfer-encoding : <type>

- Content-Transfer-Encoding: This header defines the method used to encode the messages into 0s and 1s for transport:
- The five types of encoding methods are listed

Type	*Description*
7bit	NVT ASCII characters and short lines
8bit	Non-ASCII characters and short lines
Binary	Non-ASCII characters with unlimited-length lines
Base64	6-bit blocks of data are encoded into 8-bit ASCII characters
Quoted-printable	Non-ASCII characters are encoded as an equal sign plus an ASCII code

Content Id and Content Description

4. Content-Id:

- It is used to uniquely identify the MIME entities in multiple contexts i.e.
- It uniquely identifies the whole message in a multiple message environment.

This field is represented as:

Content-id : id = <content-id>

5. Content-description:

- It is a plaintext description of the object within the body;
- It specifies whether the body is image, audio or video.

This field is represented as:

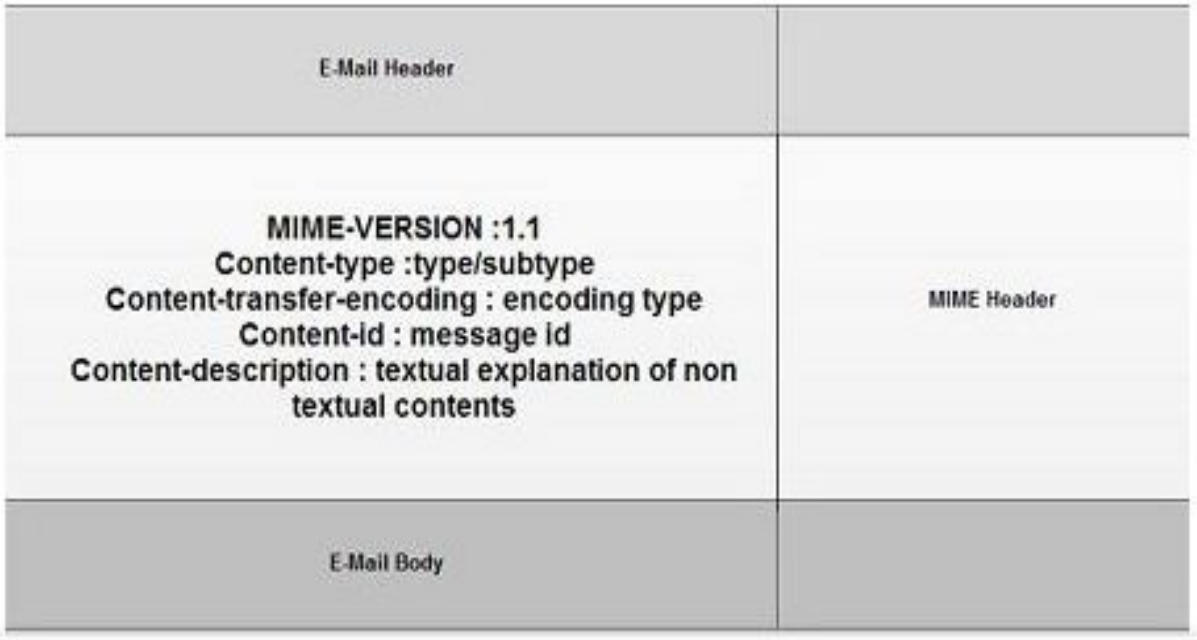
Content-description: <description>

Content-Id :This header uniquely identifies the whole message in a multiple message environment.

Content-Description : This header defines whether the body is image, audio, or video

Content Id and Content Description

- 6. The various fields in the MIME header are



References (finishing slides covering references for all the topics)

1. Douglas E. Comer, Internetworking with TCP/IP, Principles, protocols, and architecture,Vol 1 5th Edition,2006 ISBN: 0131876716, ISBN: 978-0131876712 **(Ref 2 in syllabus)**
2. https://slideplayer.com/slide/13911208/
3. http://www.csun.edu/~jeffw/Semesters/2006Fall/COMP429/Presentations/Ch25-FTP.pdf
4. https://study.com/academy/lesson/testing-an-ftp-connection.html
5. www.afternerd.com/blog/smtp