18CSC302J- Computer Networks

Unit-3

Syllabus

1. DNS- DNS in the Internet, DNS Resolution, DNS Messages
2. TELNET – SSH
3. FTP- TFTP
4. WWW Architecture, Documents
5. HTTP, HTTP Request and Reply,
6. DHCP Operation, DHCP Configuration
7. SMTP, POP3, IMAP, MIME

Learning Resources

1. Douglas E. Comer, Internetworking with TCP/IP, Principles, protocols, and architecture,Vol 1 5th Edition,2006 ISBN: 0131876716, ISBN: 978-0131876712

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 system that needs mapping.

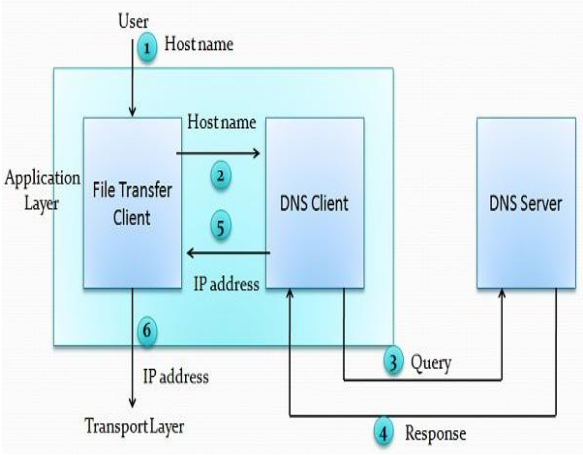
Disadvantage

- 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.

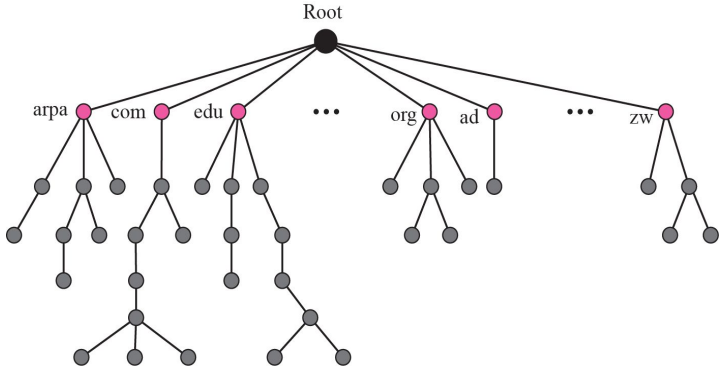
Disadvantage

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

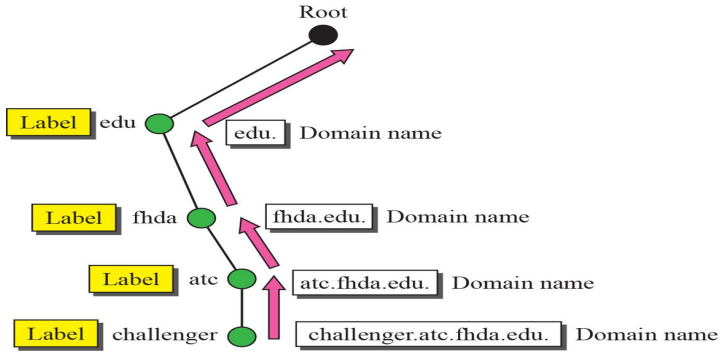
Hierarchical Name Space

- 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.

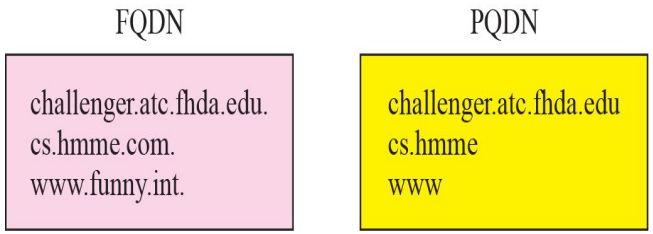
Label

- ✔ 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.

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.

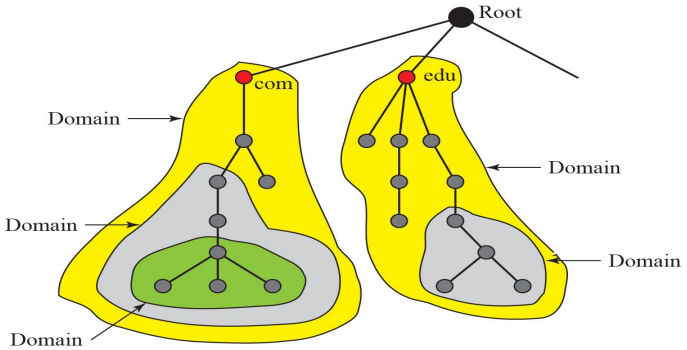
  Eg: challenger.atc.srmuniv.edu.

Partially Qualified Domain Names (PQDN)

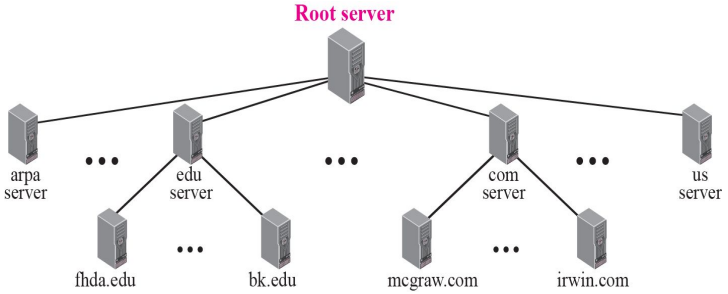
- If the label is not terminated by null string it is called partially qualified domain name.
- PQDN starts from the node but does not reach the root.
- The resolver will supply the missing part called the suffix to create a PQDN.
- User at fhda.edu site wants to get the IP address of the challenger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

  Eg: challenger

Domain Name Space



Domains



Hierarchy of name servers

Domain

- It is the subtree of domain name space.
- 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.

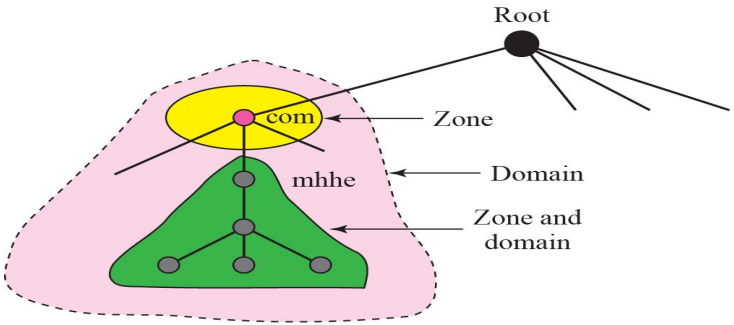
Solution

- 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.

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.

Domain Name Space

Primary and Secondary Servers

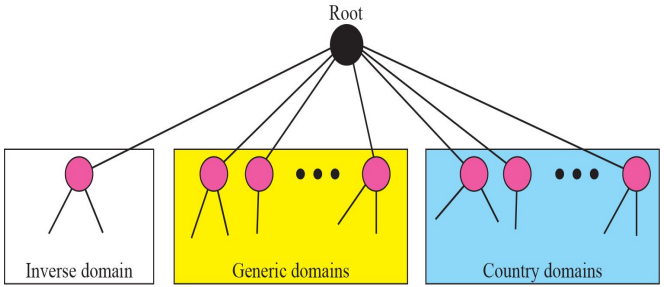
Primary Server

- 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.

DNS in the Internet



DNS used in internet

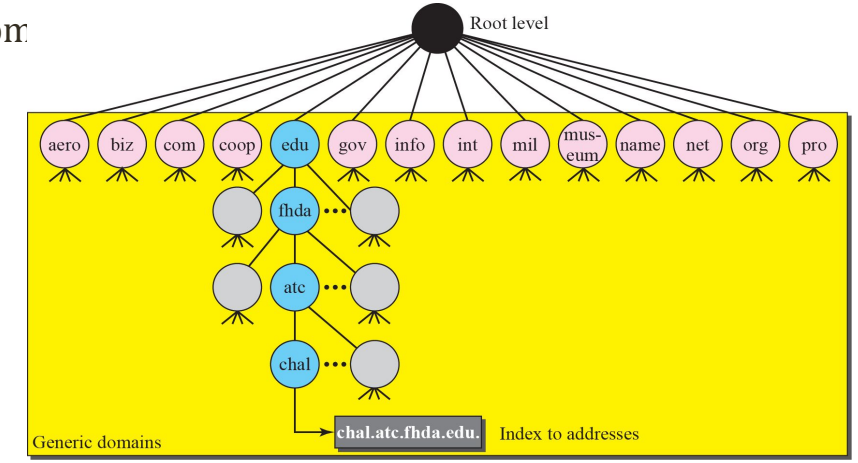
Label	*Description*
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military 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.

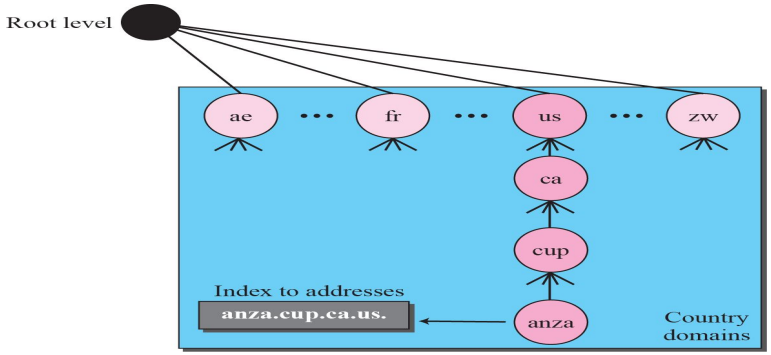
Generic Domains

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

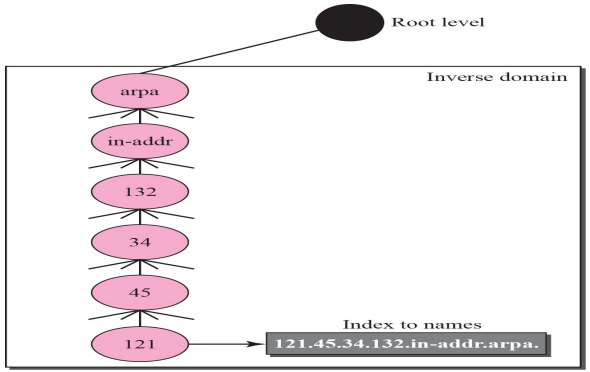


Generic Domains

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.
- Second level is also one single node named in addr (for

Resolution

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

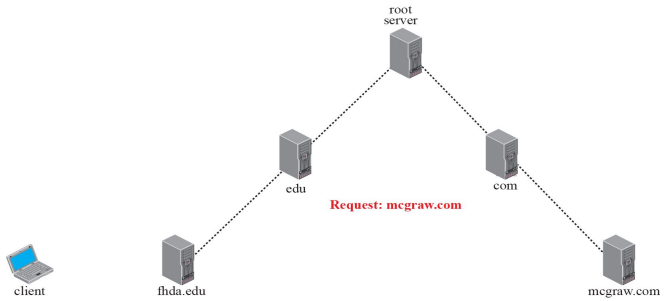
Resolver

- 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

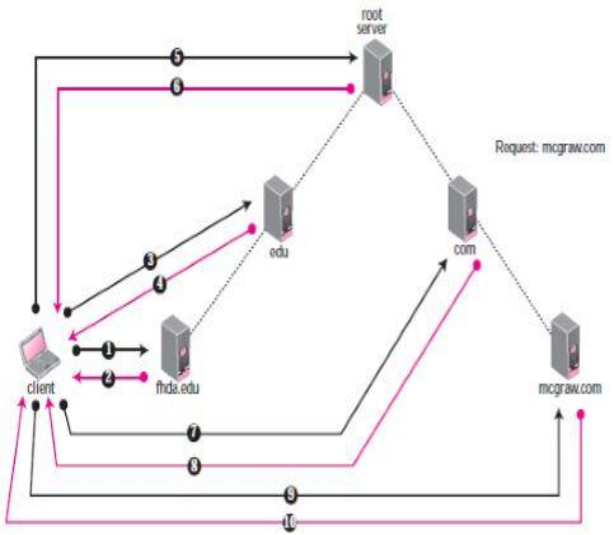
Mapping Addresses to Names

- 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.

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.

Catching

- 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 search time would increase the efficiency.
- DNS handles this with the mechanism called **catching**.

Resolution

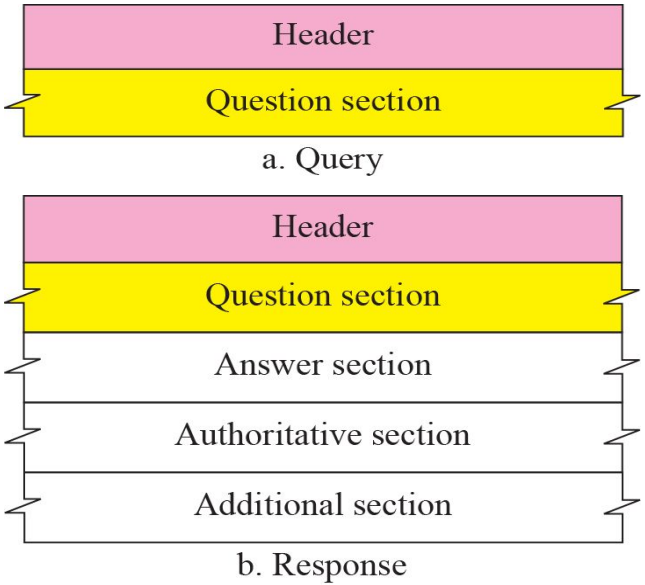
- **Reduction of search** time would increase the **efficiency**.
- DNS handles this with the mechanism called **catching.**
- **Catching speeds up** resolution but it can also **be problematic**.
- If the server **catches the mapping** for a long time it may send an **outdated mapping to the client**.

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.

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

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 more 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

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

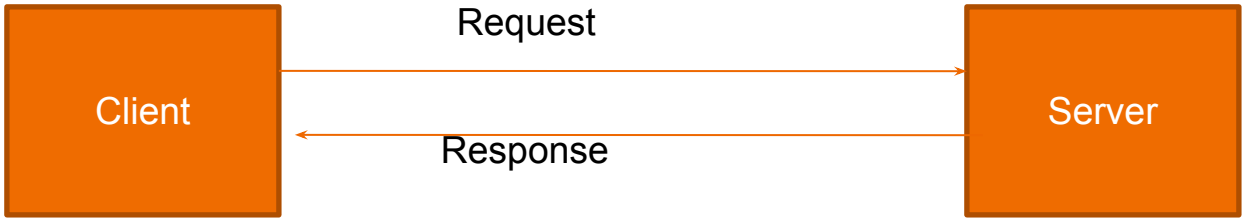
DNS Messages

- 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

WWW Architecture

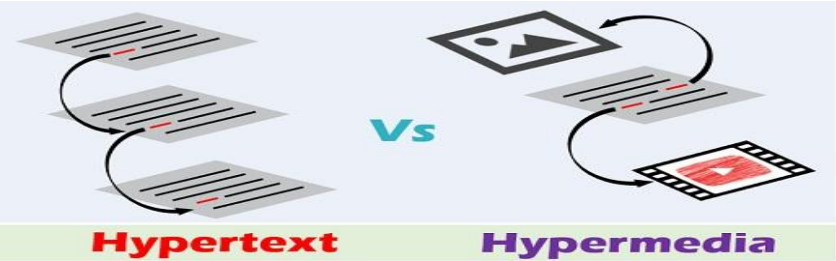
WWW Architecture

- 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
    - Web pages (simple / composite)



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)

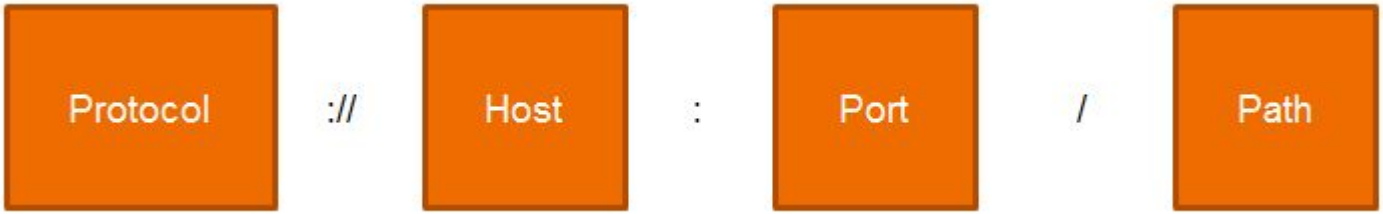
- It is an application software that allows us to view and explore information on the web. User can request for any web page by just entering a URL into address bar.
- Web browser can show text, audio, video, animation and more. It is the responsibility of a web browser to interpret text and commands 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.

Uniform Resource Locator (URL)

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

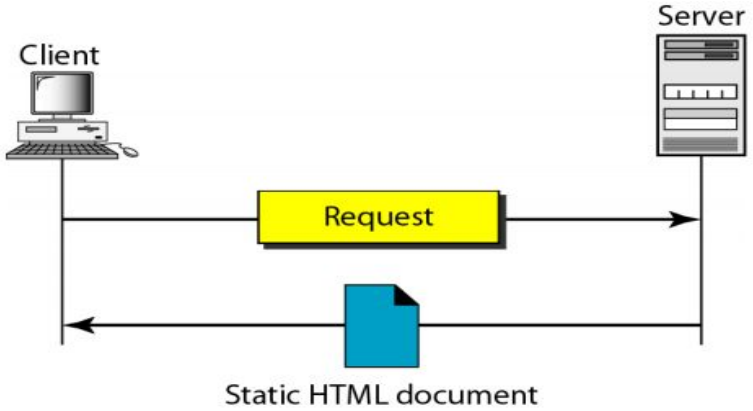


- Protocol - client-server application program used to retrieve the document (http)
- Host - domain name of the computer on which the information is located (www)
- Port – (optional) If the port is included, it is inserted between the host and the path, and it is separated from the host by a colon.
-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

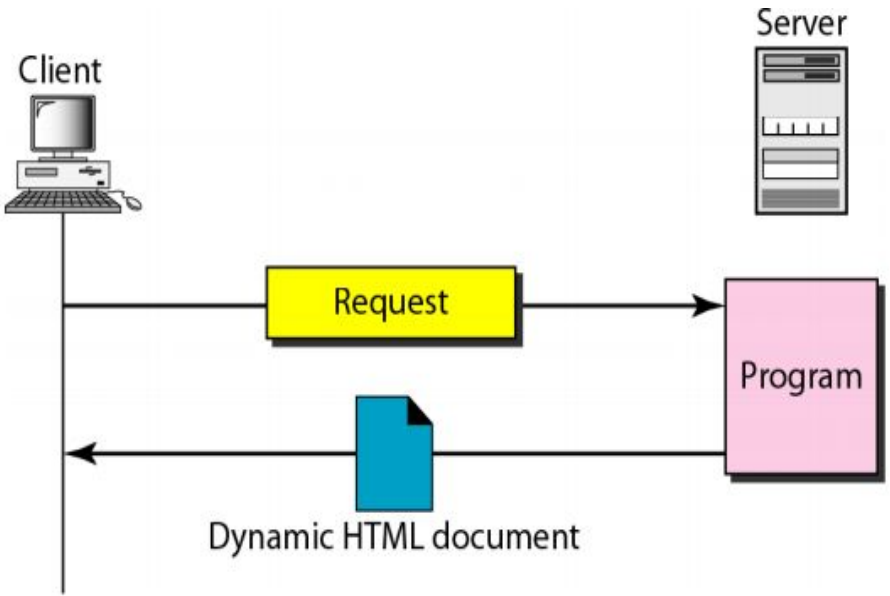
Web Documents

Static Documents

- The author of a static document determines the contents at the time the document is written.
- Since the contents do not change, each request for a static document results in exactly the same response.
- Static documents are prepared using – HTML, XML, XSL, XHTML.

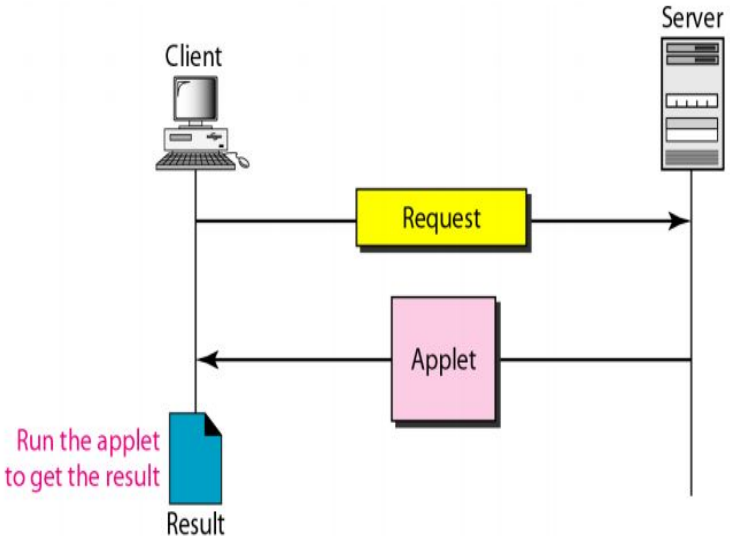


Dynamic Documents



- 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 to as server-site dynamic documents.

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.

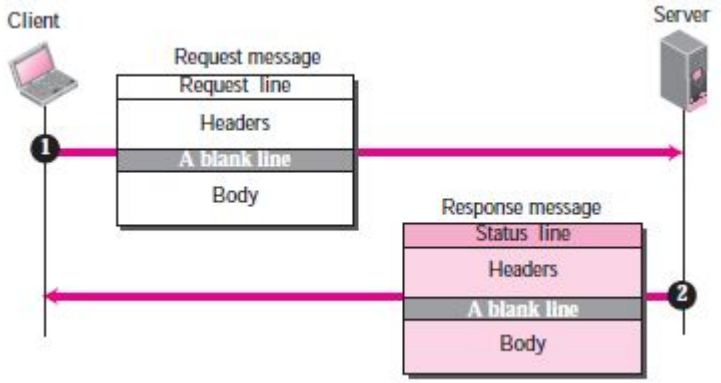
HTTP

HTTP

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

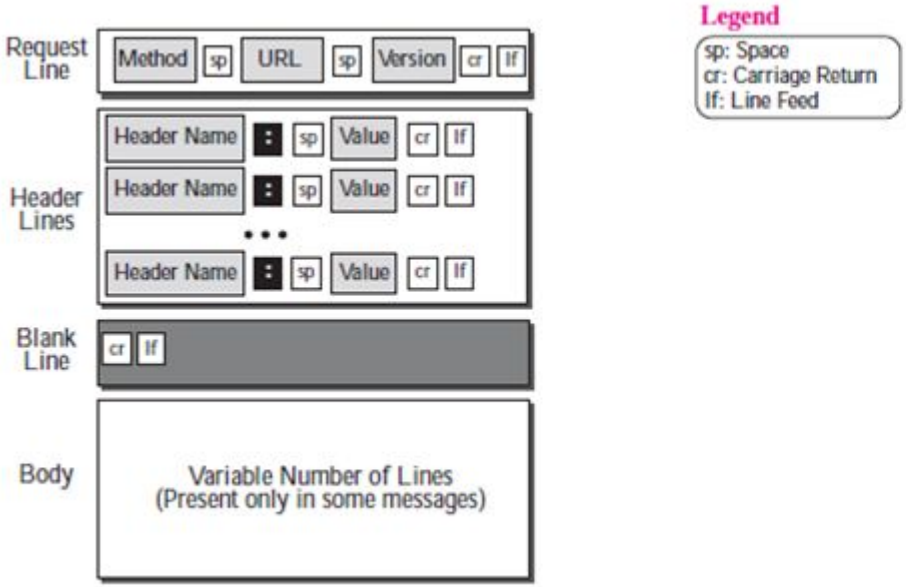
HTTP Transaction

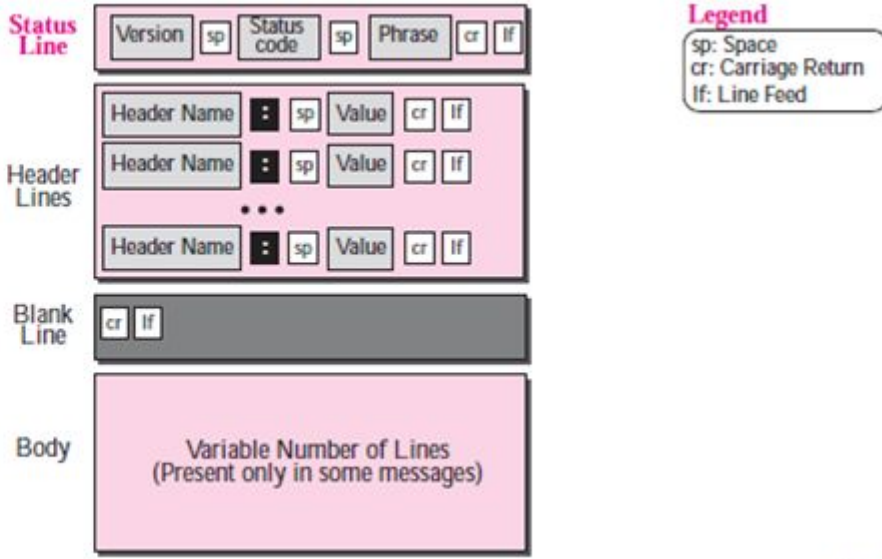
- The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web.
- HTTP functions as a combination of FTP and SMTP.
- HTTP uses the services of TCP on well-known port 80.
    - Request message
    - Request Line



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)

Persistence

- HTTP version 1.1 specifies a persistent connection by default.
- 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.

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

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.

HTTP security

- HTTPS provides confidentiality, client and server authentication, and data integrity.

DHCP

Introduction

- 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.

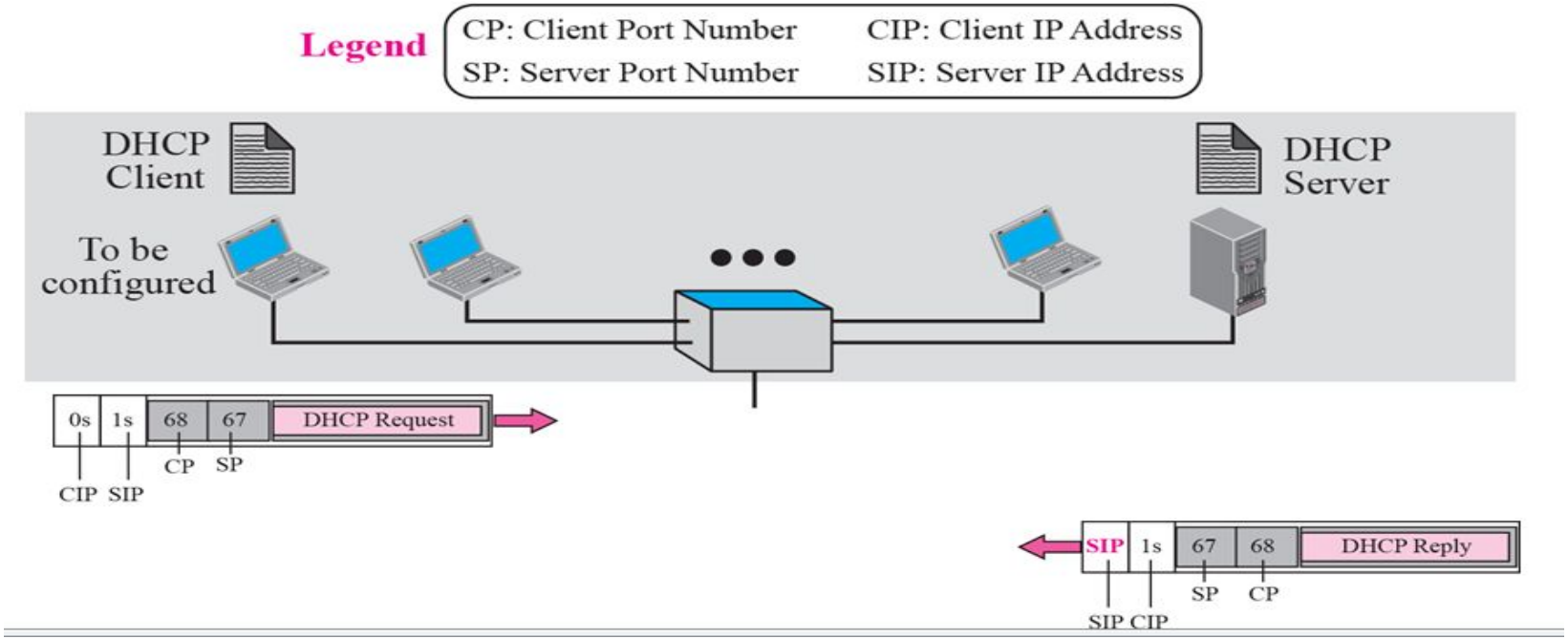
DHCP (Definition)

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

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

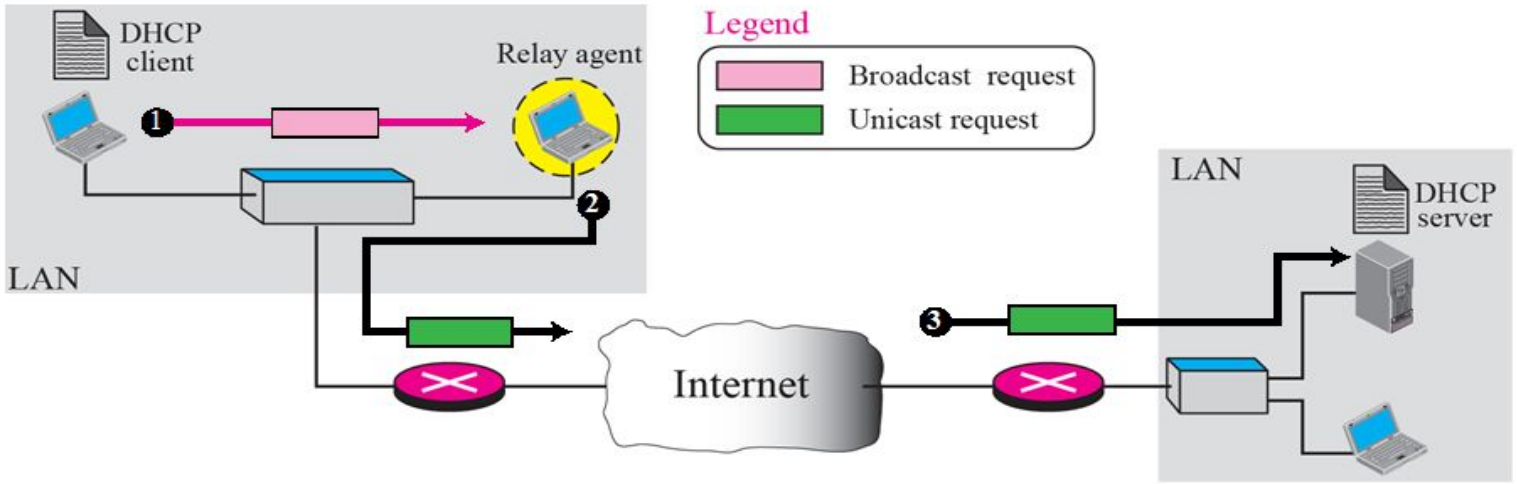
Same Network



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.

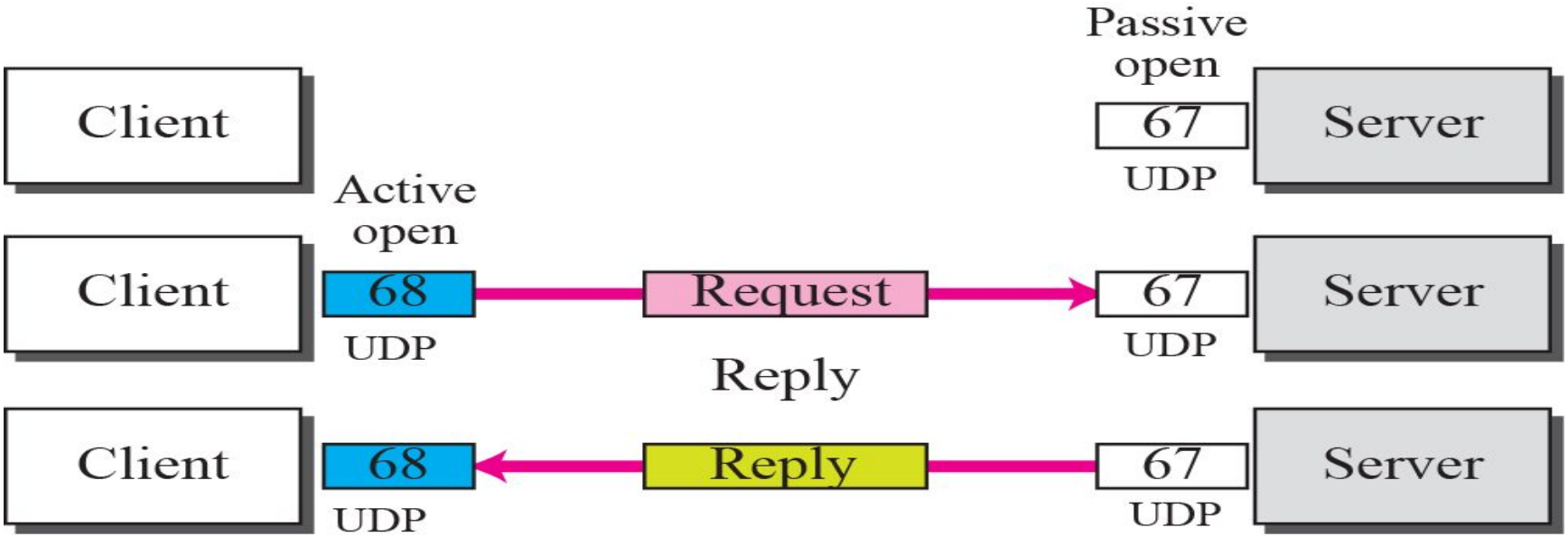
Different network



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.

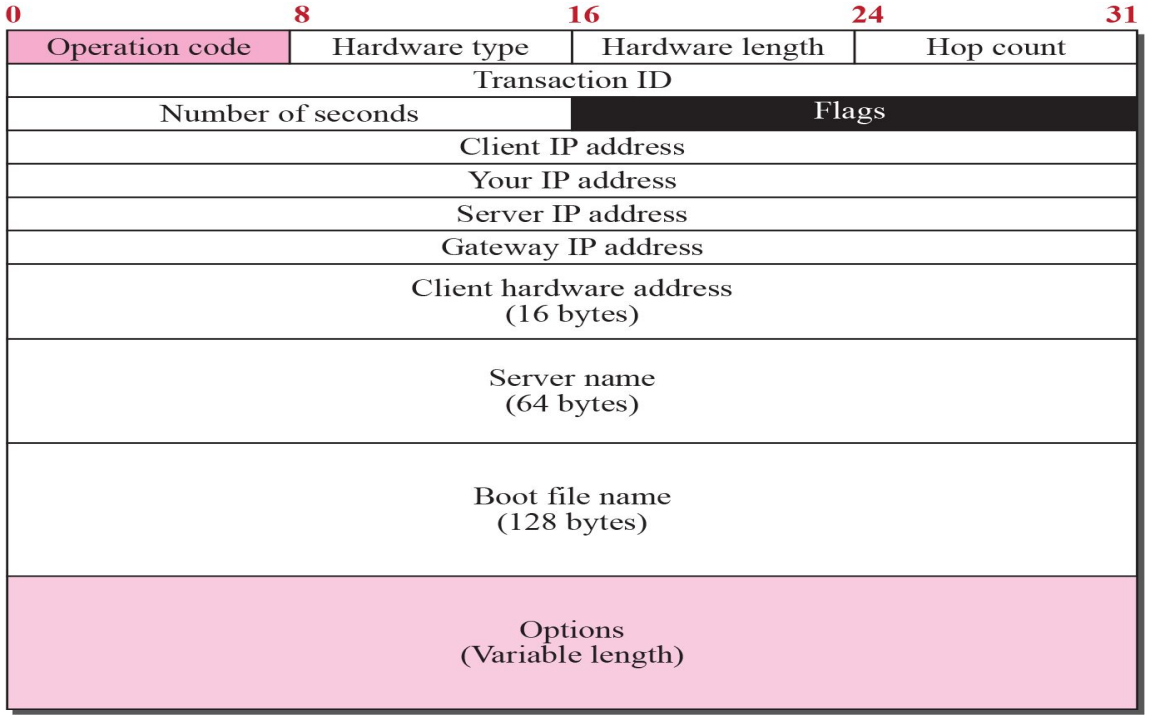
TFTP

- It is an acknowledgement from the server, containing the pathname of a file which has the complete booting information.

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

Packet Format (Contd..)

- 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

States (Contd..)

- 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.

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

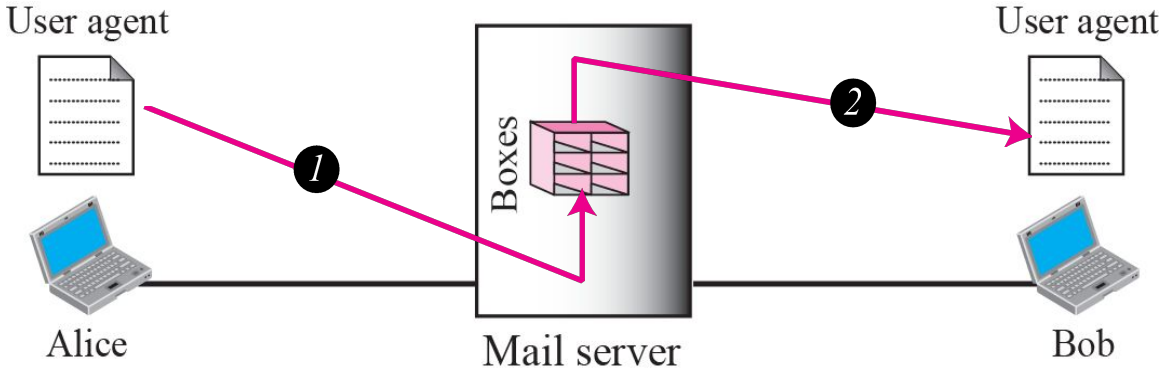
Discussion On

- Architecture
- User agent
- Message transfer agent
- Message access agent
- MIME

Architecture

- We have 4 scenarios in explain the architecture of e-mail.
    - First Scenario
    - Second Scenario
    - Third Scenario
    - Fourth Scenario

First scenario



- The sender and the receiver of the e-mail are users on the same mail server; they are directly connected to a shared mail server.

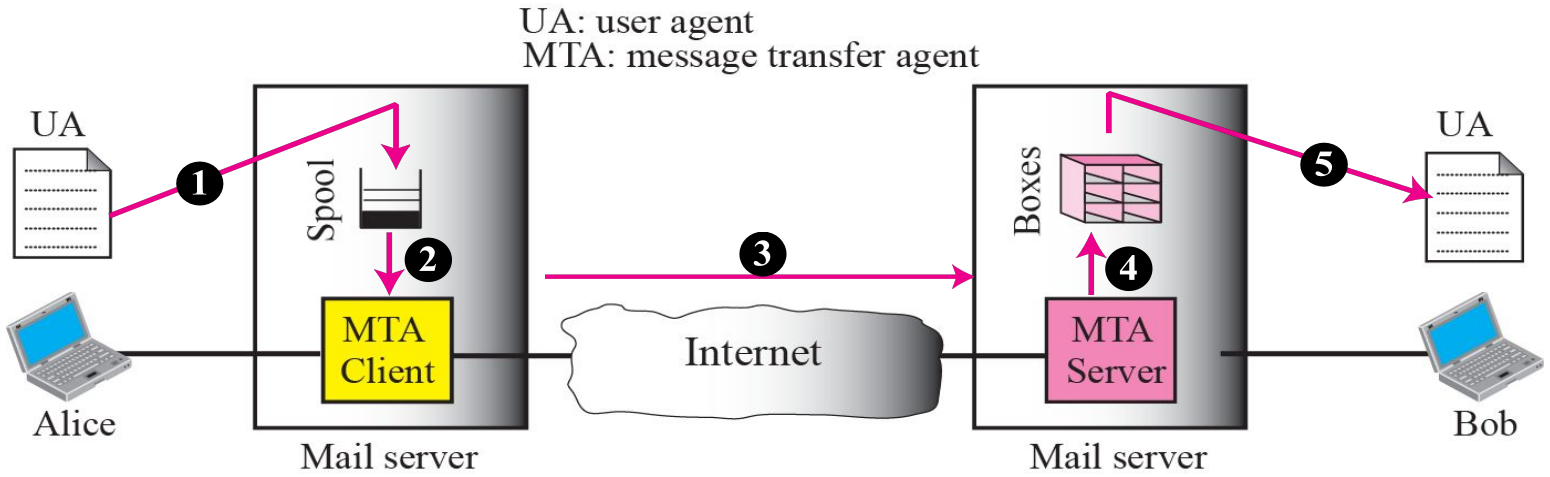
- The admin has created one mailbox to store the received messages. Only the sender or the receiver of the mailbox has access to it.

First scenario(Contd..)

- When Alice needs to send a message to Bob, she runs a user agent(is a program) to prepare the message and store it in Bob's mailbox.

- The message has the sender and recipient mailbox addresses. Bob can retrieve and read the contents of his mailbox at his convenience using a user agent.

Second scenario



Second scenario (Contd..)

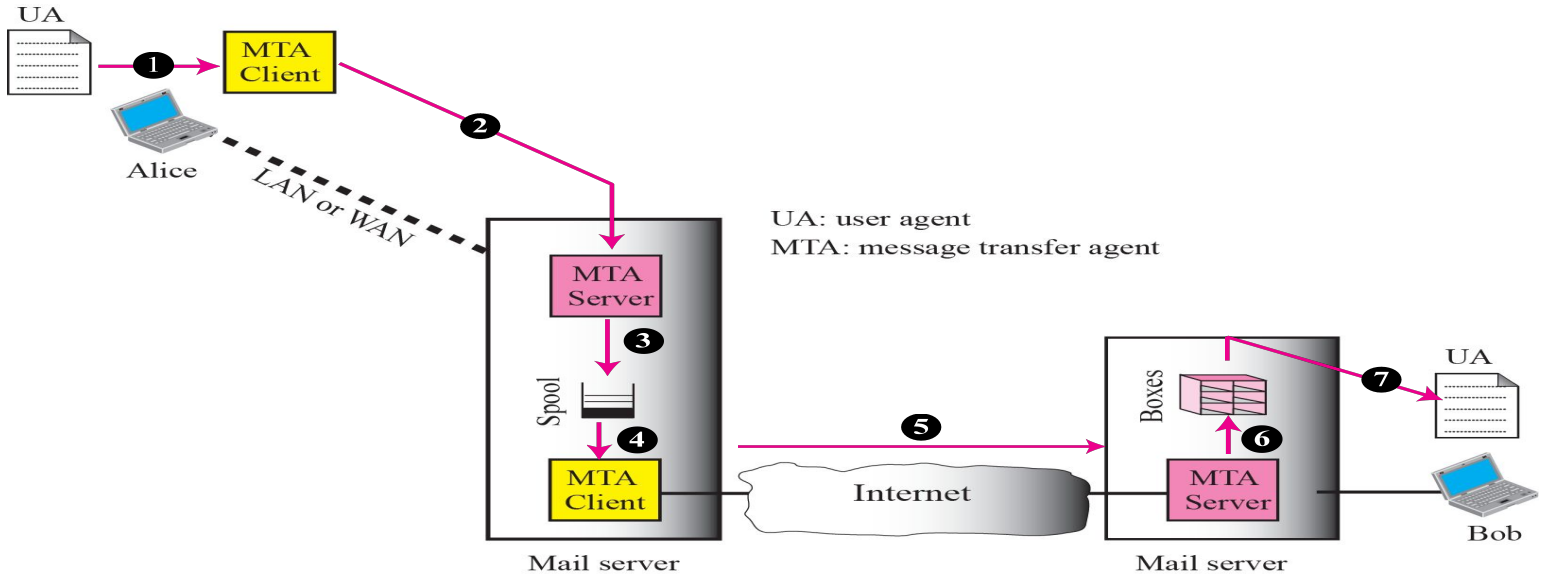
- Here, the sender and the receiver of the e-mail are users on two different mail servers. The message needs to be sent over the Internet. Here we need user agents (UAs) and message transfer agents (MTAs)

- Alice needs to use a user agent to send her message to the mail server at her own site. The mail server at her site uses a buffer (queue) to store messages waiting to be sent.

- Bob also needs a user agent to retrieve messages stored in the mailbox of the system at his site. Here two message transfer agents are needed: one client and one server.

- The server needs to run all of the time because it does not know when a client will ask for a connection. The client, on the other hand, can be triggered by the system when there is a message in the queue to be sent.

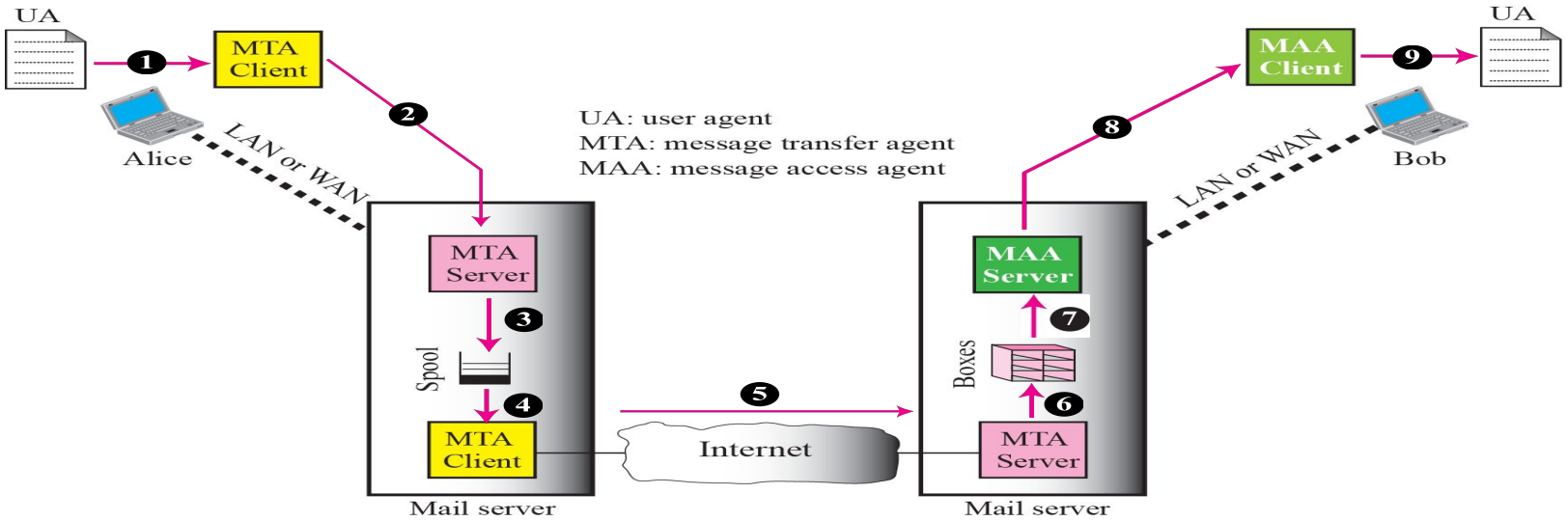
Third scenario



Third scenario (Contd..)

- Alice needs a user agent to prepare her message. She then needs to send the message through the LAN or WAN.
- This can be done through a pair of message transfer agents (client and server). Whenever Alice has a message to send, she calls the user agent which, in turn, calls the MTA client.
- The MTA client establishes a connection with the MTA server on the system, which is running continuously. The system at Alice's site queues all messages received.
- It then uses an MTA client to share the messages to the system at Bob's site; the system receives the message and stores it in Bob's mailbox.

Fourth scenario



Fourth scenario (Contd..)

- Here, Bob is also connected to his mail server by a WAN or a LAN. After the message has arrived at Bob's mail server, Bob needs to retrieve it.

- Here, we need another set of client-server agents, which we call message access agents (MAAs).

- Bob uses an MAA client to retrieve his messages. The client sends a request to the MAA server, which is running all the time, and requests the transfer of the messages.

- Bob cannot bias the mail server to use the MTA server directly. To use the MTA server directly, Bob would need to run the MTA server all the time because he does not know when a message will arrive.

Push vs Pull

- Here, Bob needs another pair of client-server programs: message access programs. This is because an MTA client-server program is a push program:

- The client pushes the message to the server. Bob needs a pull program. The client needs to pull the message from the server.

a. Client pushes messages

b. Client pulls messages

User Agent

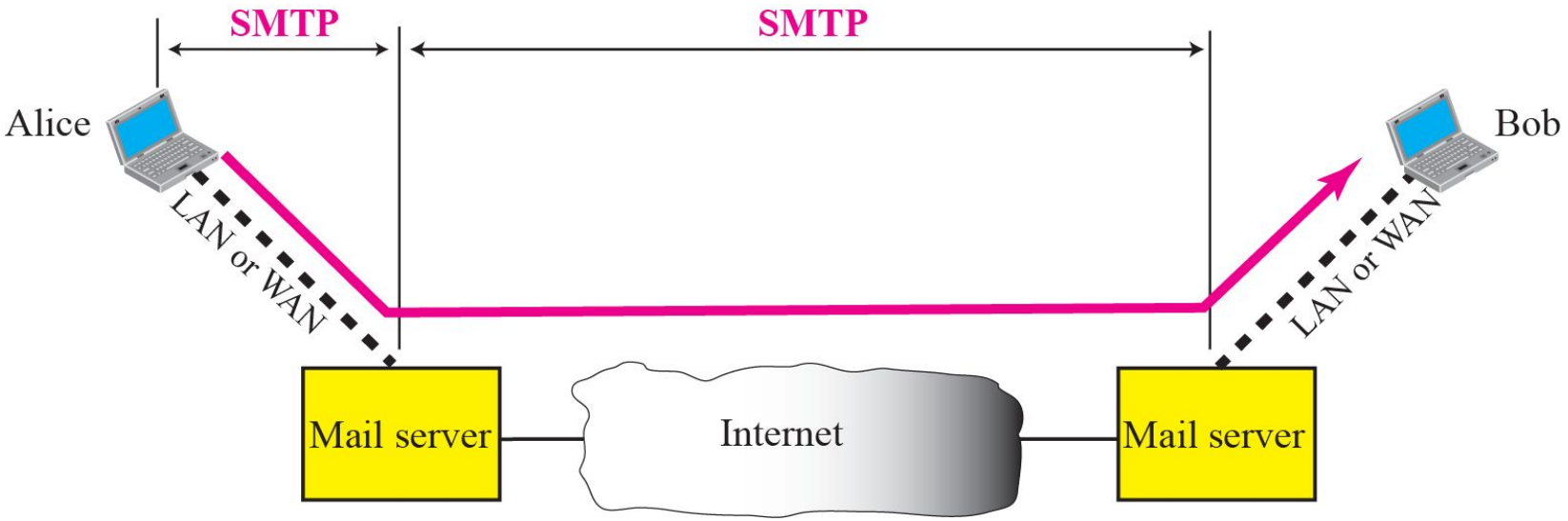
- The first component of an electronic mail system is the user agent (UA). It provides service to the user to make the process of sending and receiving a message easier.

  - Services Provided by a User Agent
  - User Agent Types
  - Sending Mail
  - Receiving Mail
  - Addresses
  - Mailing List or Group List

Message transfer agent

- The actual mail transfer is done through message transfer agents (MTAs). To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA.
- The formal protocol that defines the MTA client and server in the Internet is called Simple Mail Transfer Protocol (SMTP).

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.

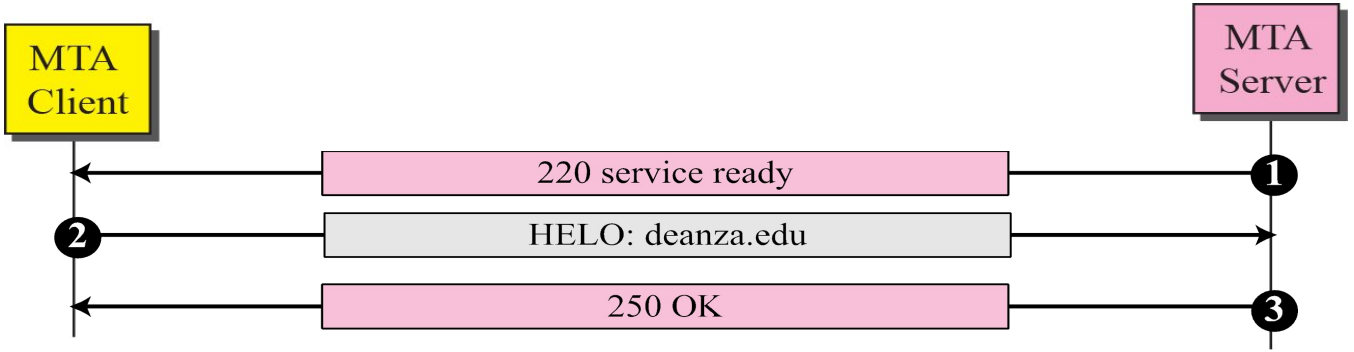
Keyword	*Argument(s)*	*Keyword*	*Argument(s)*
HELO	Sender's host name	NOOP	
MAIL FROM	Sender of the message	TURN	
RCPT TO	Intended recipient	EXPN	Mailing list
DATA	Body of the mail	HELP	Command name
QUIT		SEND FROM	Intended recipient
RSET		SMOL FROM	Intended recipient
VRFY	Name of recipient	SMAL FROM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

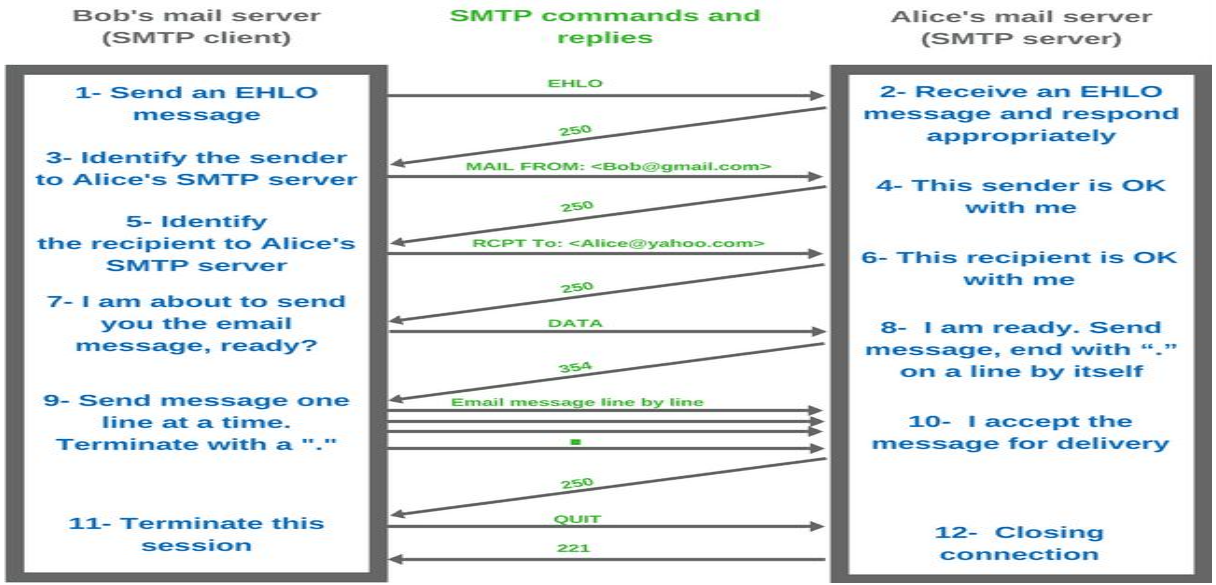


- The server sends code 220 to tell the client that it is ready to receive mail.
- The client sends the HELO message to identify itself using its domain name address. This step is necessary to inform the server of the domain name of the client.
- The server responds with code 250

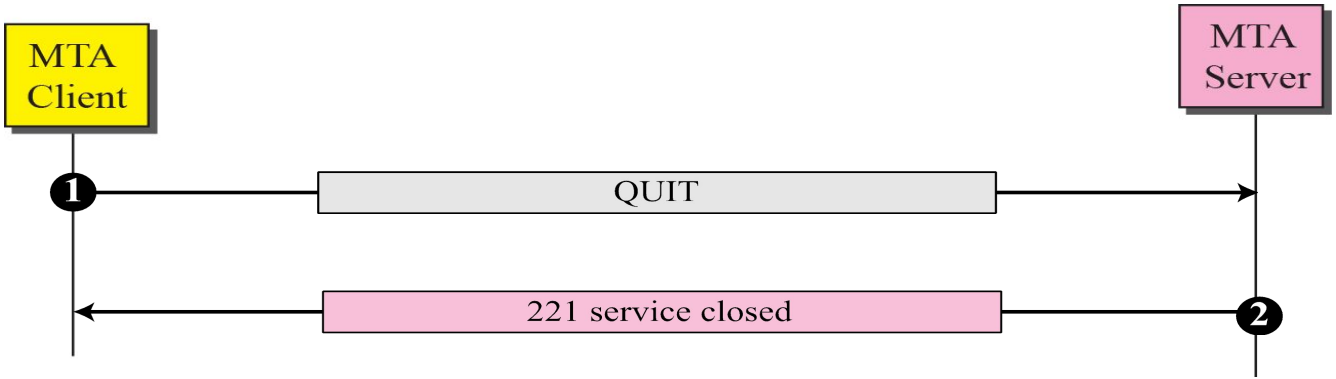
Mail Transfer

- 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



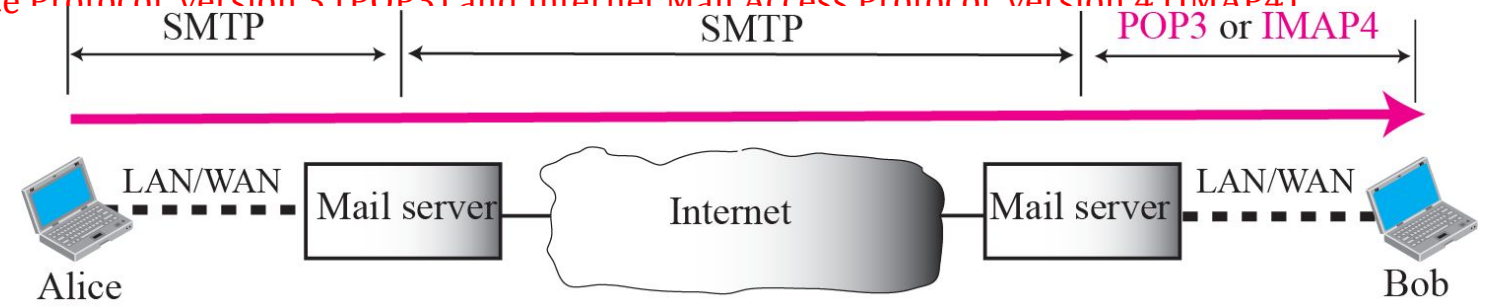
Connection termination



- When the message is transferred successfully, the client terminates the connection.

Message access agent

- The first and the second stages of mail delivery use SMTP. Here, SMTP is not involved in the third stage because SMTP is a push protocol; it pushes the message from the client to the server.
- The third stage needs a pull protocol; the client must pull messages from the server. The direction of the bulk data are from the server to the client.
- The third stage uses a message access agent. Currently two message access protocols are available: Post Office Protocol, version 3 (POP3) and Internet Mail Access Protocol, version 4 (IMAP4)



POP3 & IMAP4

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.

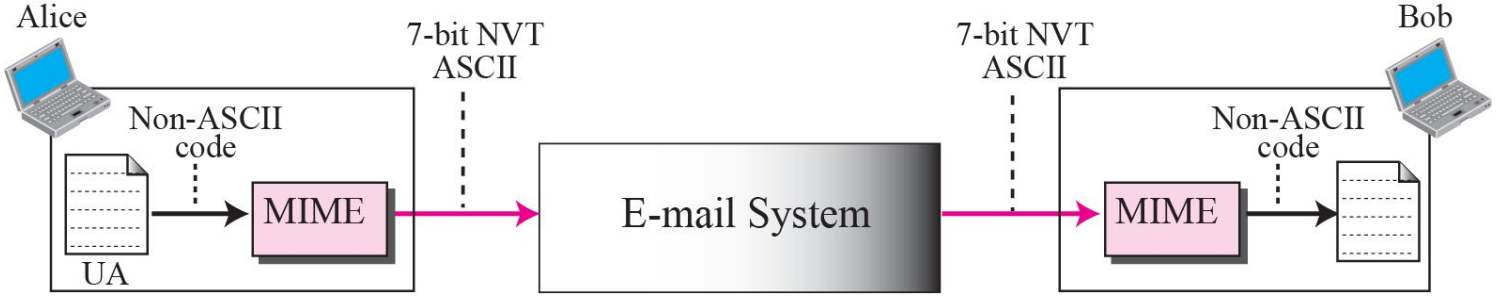
POP3 & IMAP4 (Contd..)

IMAP4(Internet Mail Access Protocol, version 4): It is more powerful and more complex.
IMAP4 provides the following extra functions:

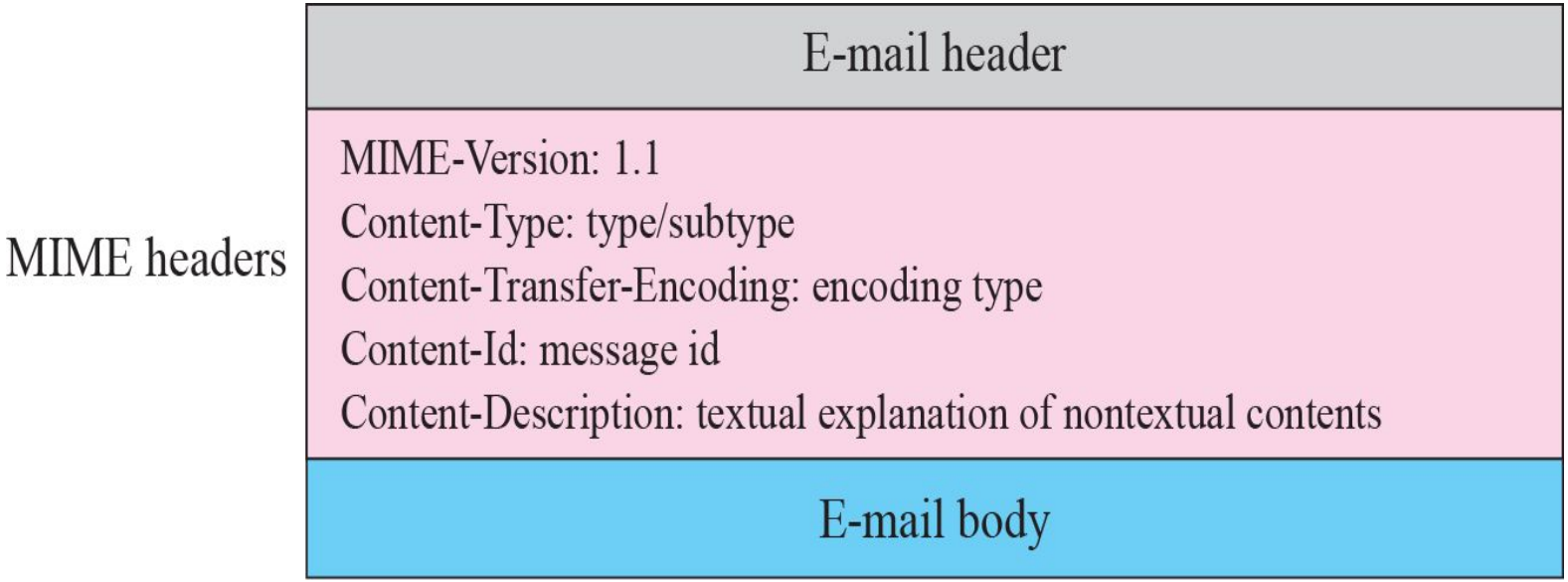
- A user can check the e-mail header prior to downloading.
- A user can search the contents of the e-mail for a specific string of characters prior to downloading.
- A user can partially download e-mail. This is especially useful if bandwidth is limited and the e-mail contains multimedia with high bandwidth requirements.
- A user can create, delete, or rename mailboxes on the mail server.
- A user can create a hierarchy of mailboxes in a folder for e-mail storage.

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 the receiving site is transformed back to the original data.



MIME header


E-mail header
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 headers

MIME header (Contd..)

- MIME-Version: This header defines the version of MIME used. The current version is 1.1.
- Content-Type :
  - This header defines the type of data used in the body of the message. The content type and the content subtype are separated by a slash.
  - Depending on the subtype, the header may contain other parameters.

Data Type and Subtype in MIME

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

- 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 :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

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