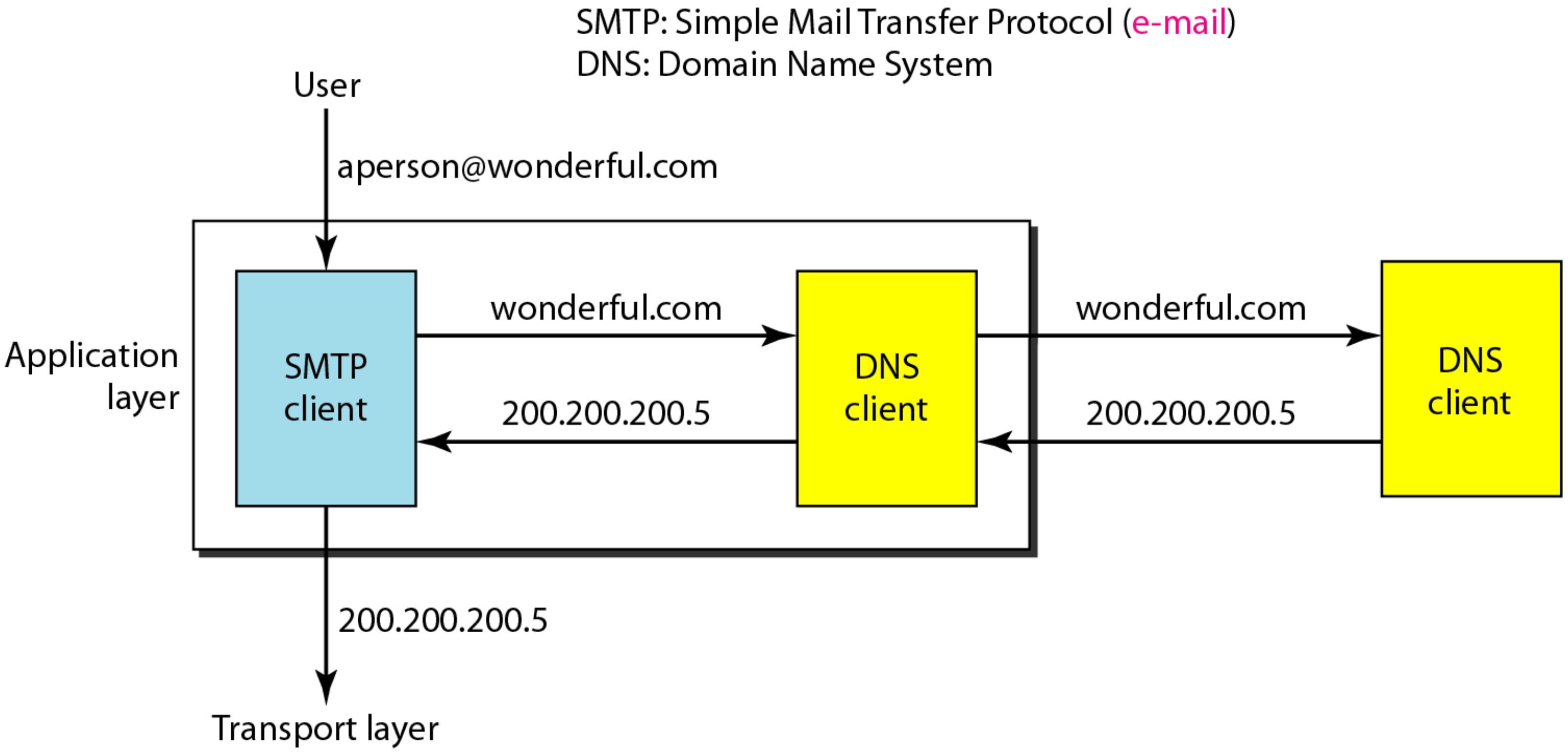
Application Layer

Unit-11

DNS: Domain Name System

- DNS is an client/server application that translates ***domain names*** into IP addresses.
- Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses.
- Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name *www.example.com* might translate to*198.105.232.4*.

Example of using DNS service



SMTP: Simple Mail Transfer Protocol (e-mail)
DNS: Domain Name System

- Figure shows an example of how a DNS client/server program can support an e-mail program to find the IP address of an e-mail recipient.
- A user of an e-mail program may know the e-mail address of recipient; however, the IP protocol needs the IP address.
- The DNS client program sends a request to a DNS server to map the e-mail address to the corresponding IP address.

Name space

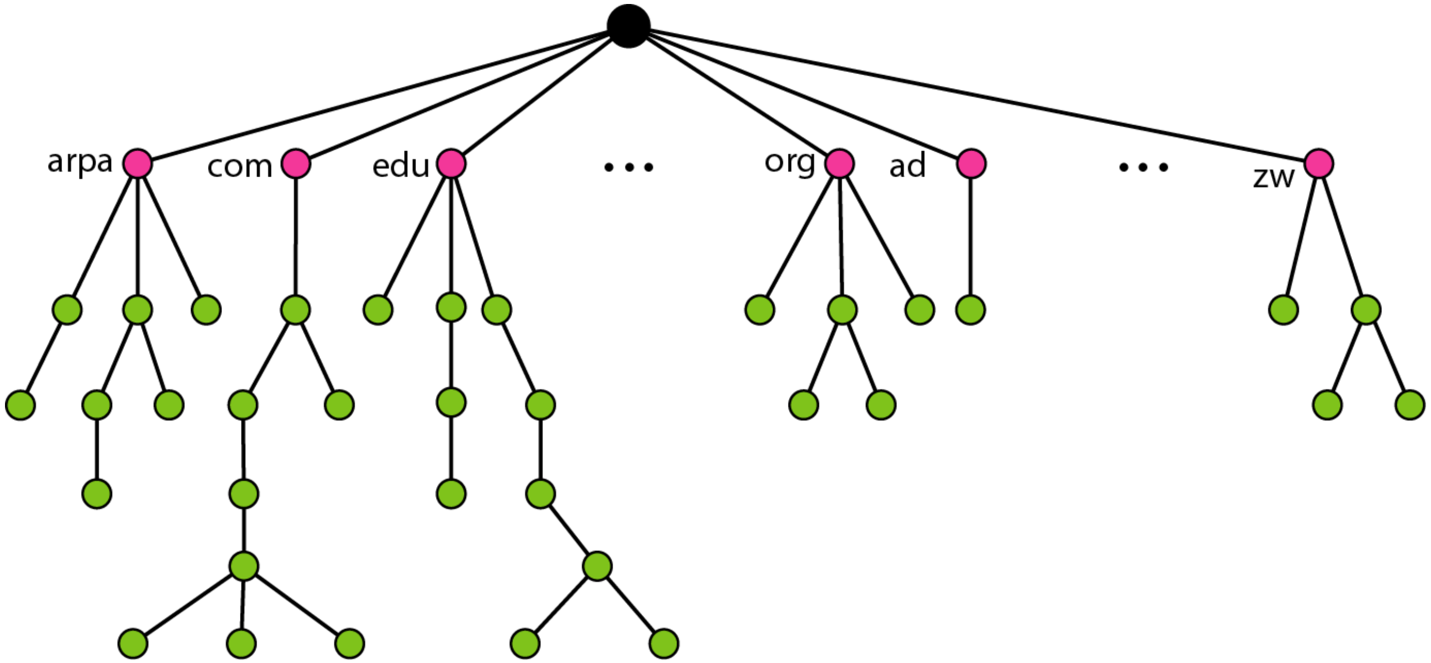
- To be unambiguous, the names assigned to machines must be carefully selected from a name space with complete control over the binding between the names and IP addresses.
- In other words, the name must be unique because the address are unique.
- Organized into two ways:
  - Flat name space
  - Hierarchical name space

Domain Name Space

- To have a hierarchical name space, a domain name space was designed. In this design the names are defined in an inverted-tree structure with the root at the top. The tree can have only 128 levels: level 0 (root) to level 127.

Components:

- ➢ Label
- ➢ Domain Name
- ➢ Domain



Label

- Each node in the tree has a label, which is a string with a maximum of 63 characters.
- The root label is a null string (empty string).

Domain Name

- Each node in the tree has a domain name .
- A full domain name is a sequence of labels separated by dots(.) .
- The domain names are always read from the node up to the root.

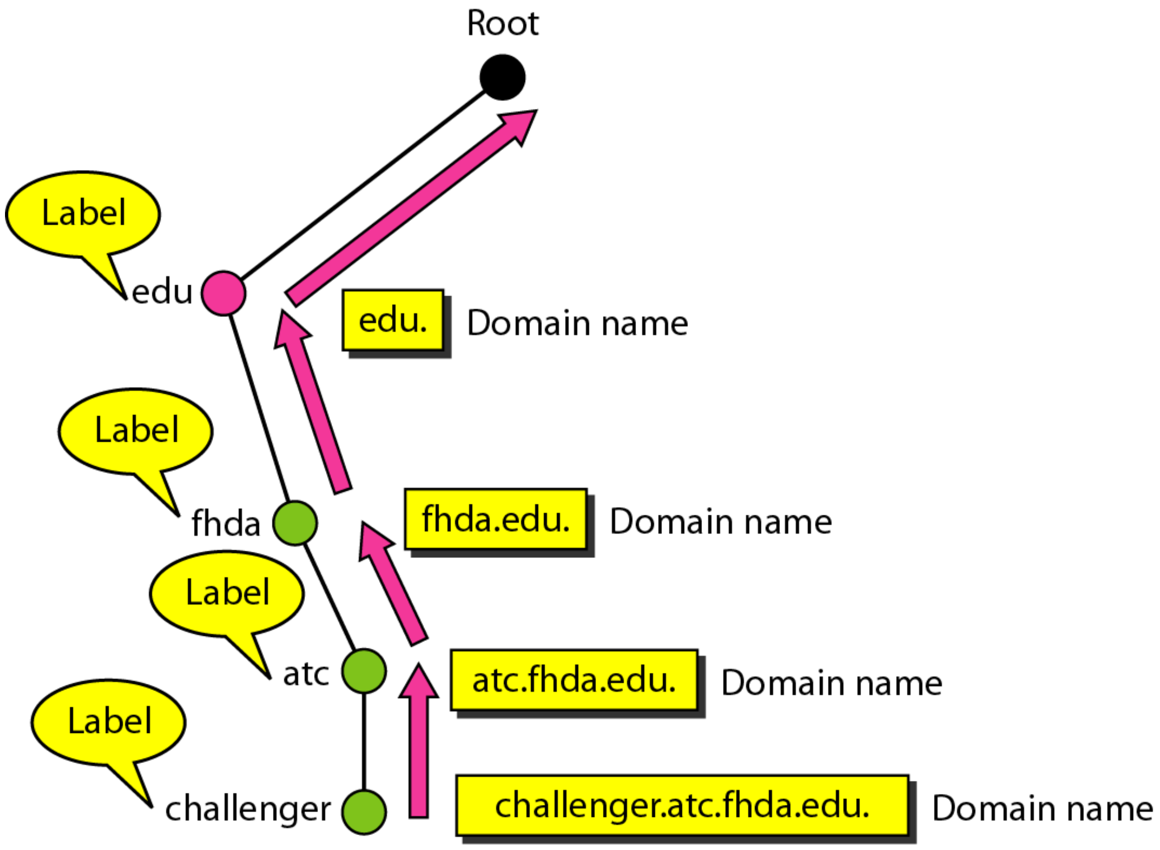


Figure: Domain names and labels

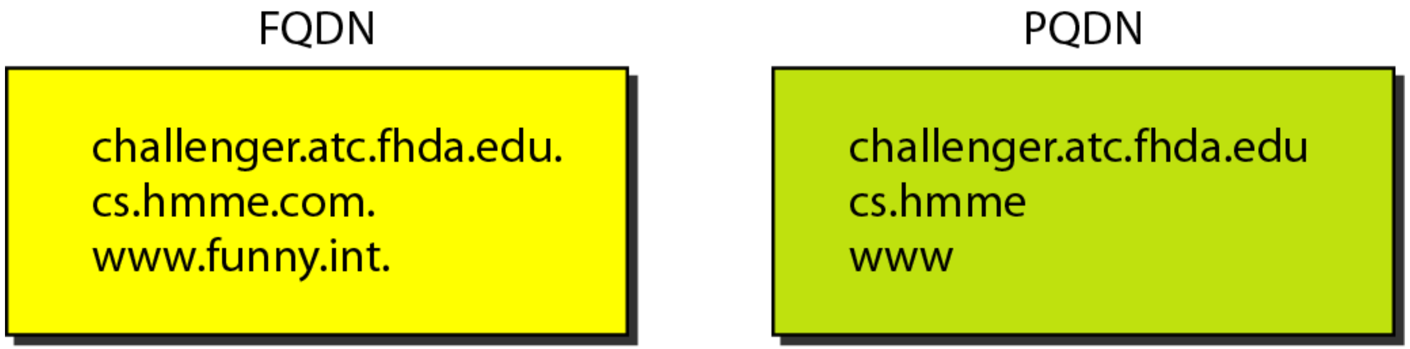
FQDN and PQDN

FQDN : Fully Qualified Domain Name

- If a label is terminated by a null string, it is called FQDN.
- An FQDN is a domain name that contains the full name of a host.
- A DNS server can only match FQDN to an address.

PQDN : Partially Qualified Domain Name

- If a label is not terminated with a null string, it is called a partially domain name. (PQDN) .
- A PQDN starts from a node, but it does not reach the root



FQDN

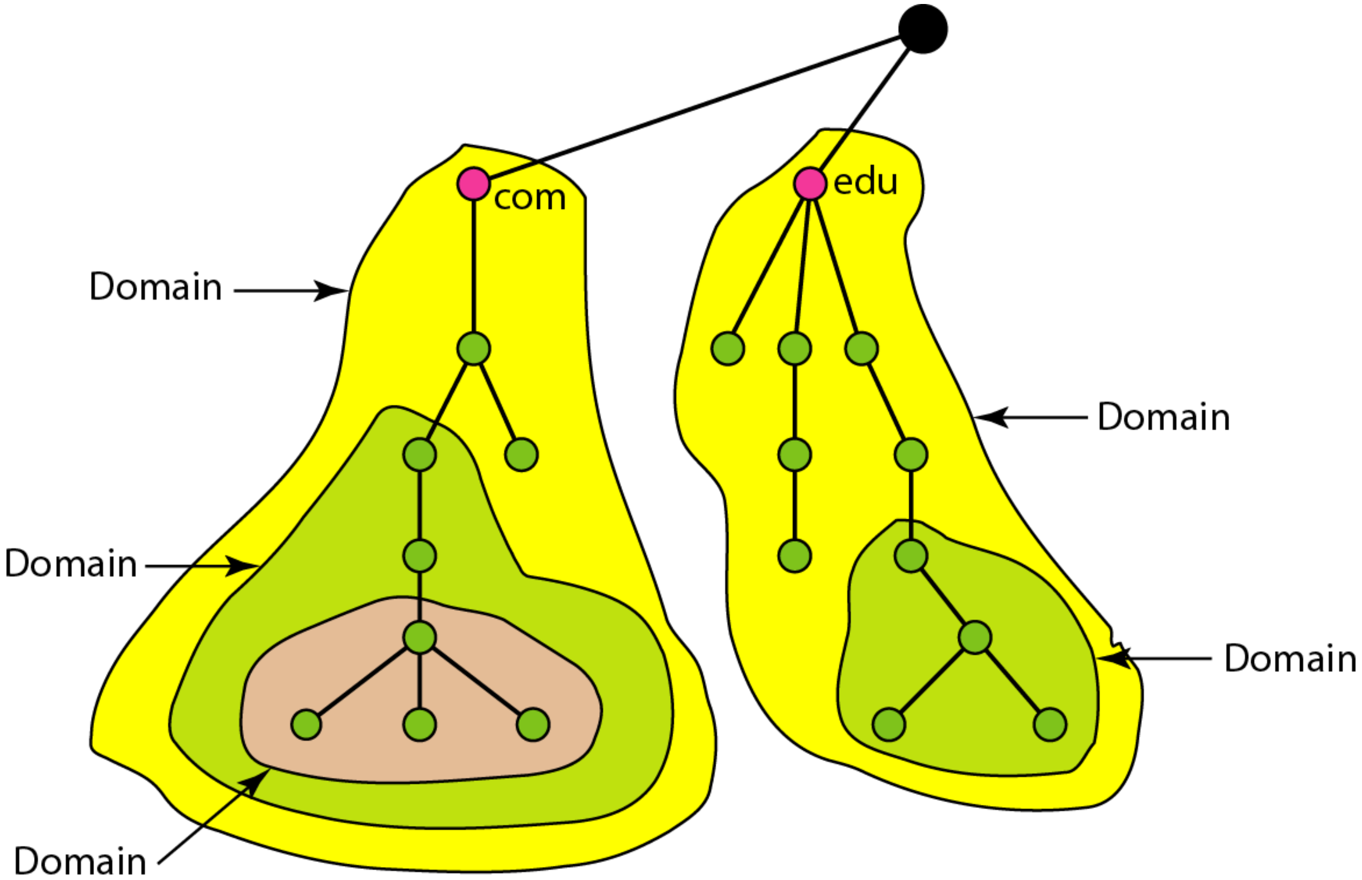
challenger.atc.fhda.edu.
cs.hmme.com.
www.funny.int.

PQDN

challenger.atc.fhda.edu
cs.hmme
www

Domain

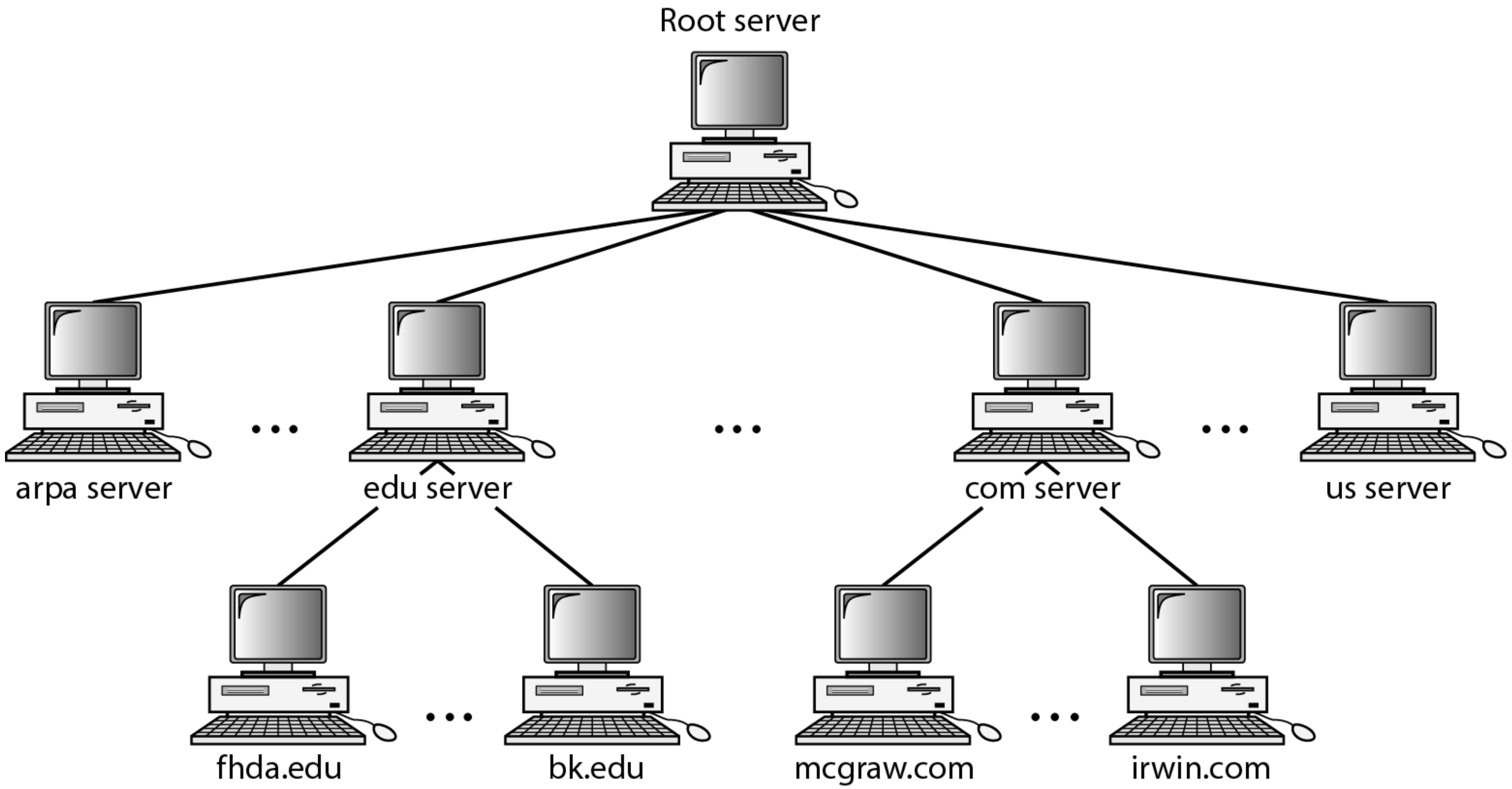
- A domain is a subtree of the domain name space.
- The name of domain is the domain name of the node at the top of the subtree.



Distribution of Name space

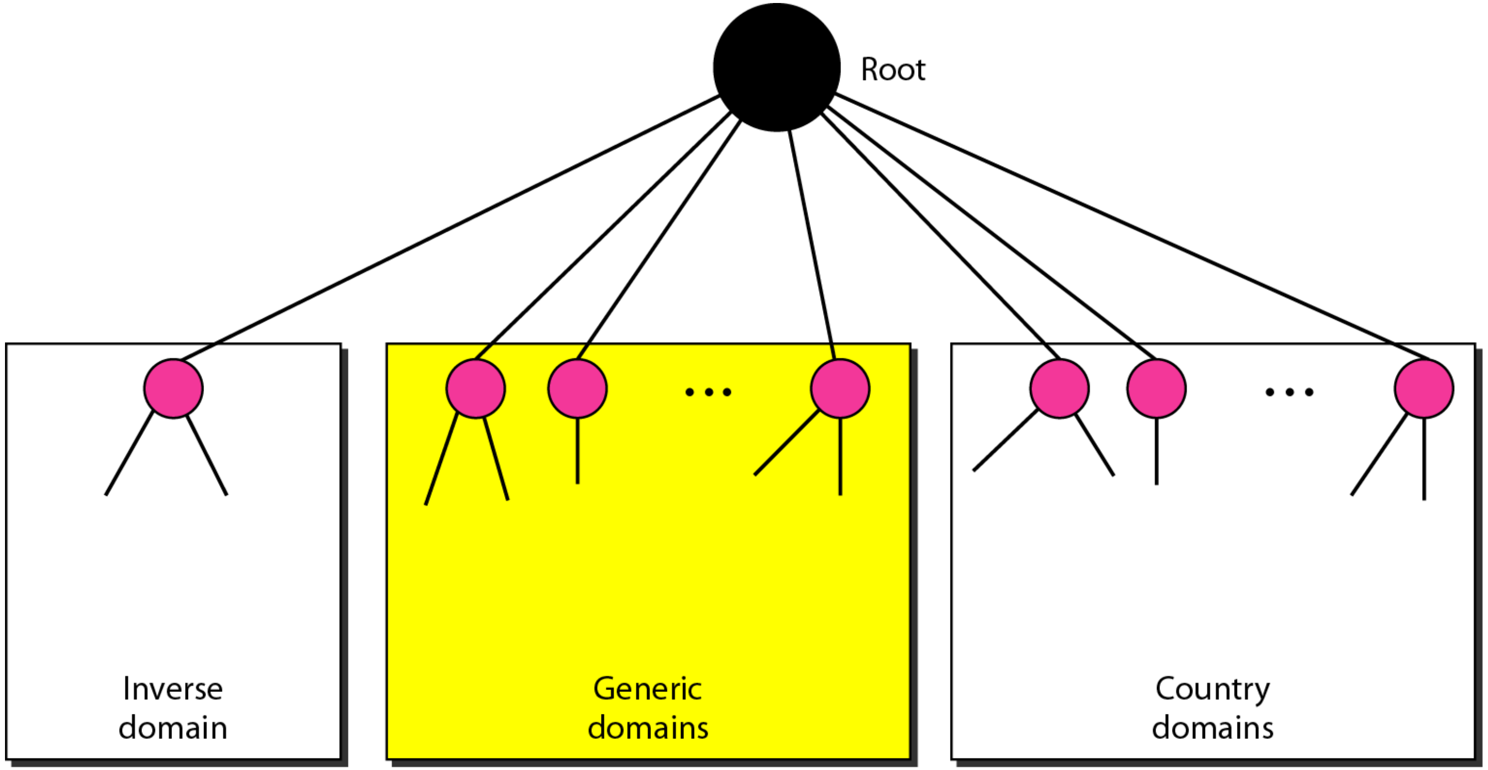
- The information contained in the domain name space must be stored. However, it is very inefficient and also unreliable to have just one computer store such a huge amount of information. In this section, we discuss the distribution of the domain name space.

Hierarchy of Name space



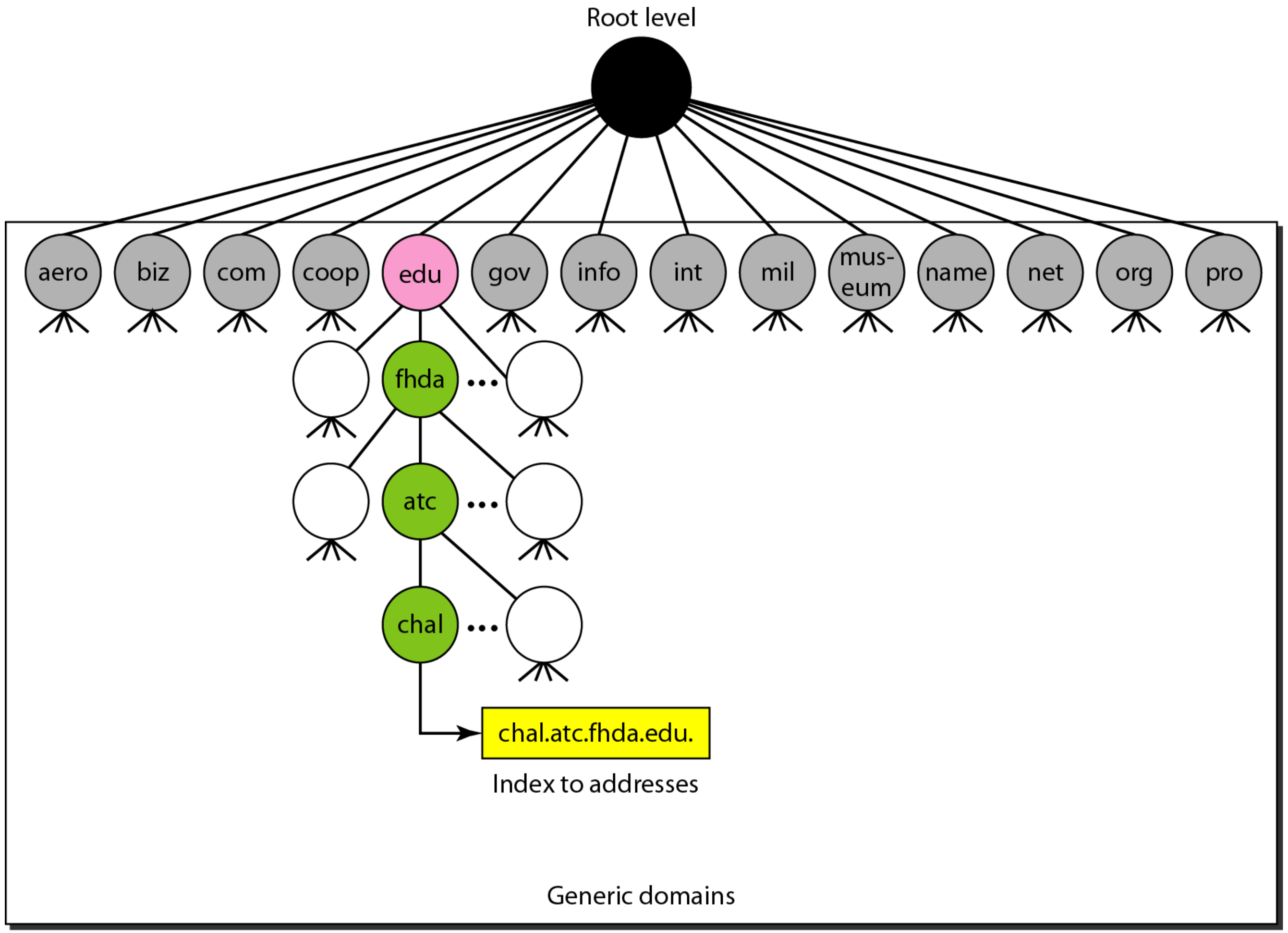
DNS in internet

- DNS is a protocol that can be used in different platforms. In the Internet, the domain name space (tree) is divided into three different sections: generic domains, country domains, and the inverse domain.

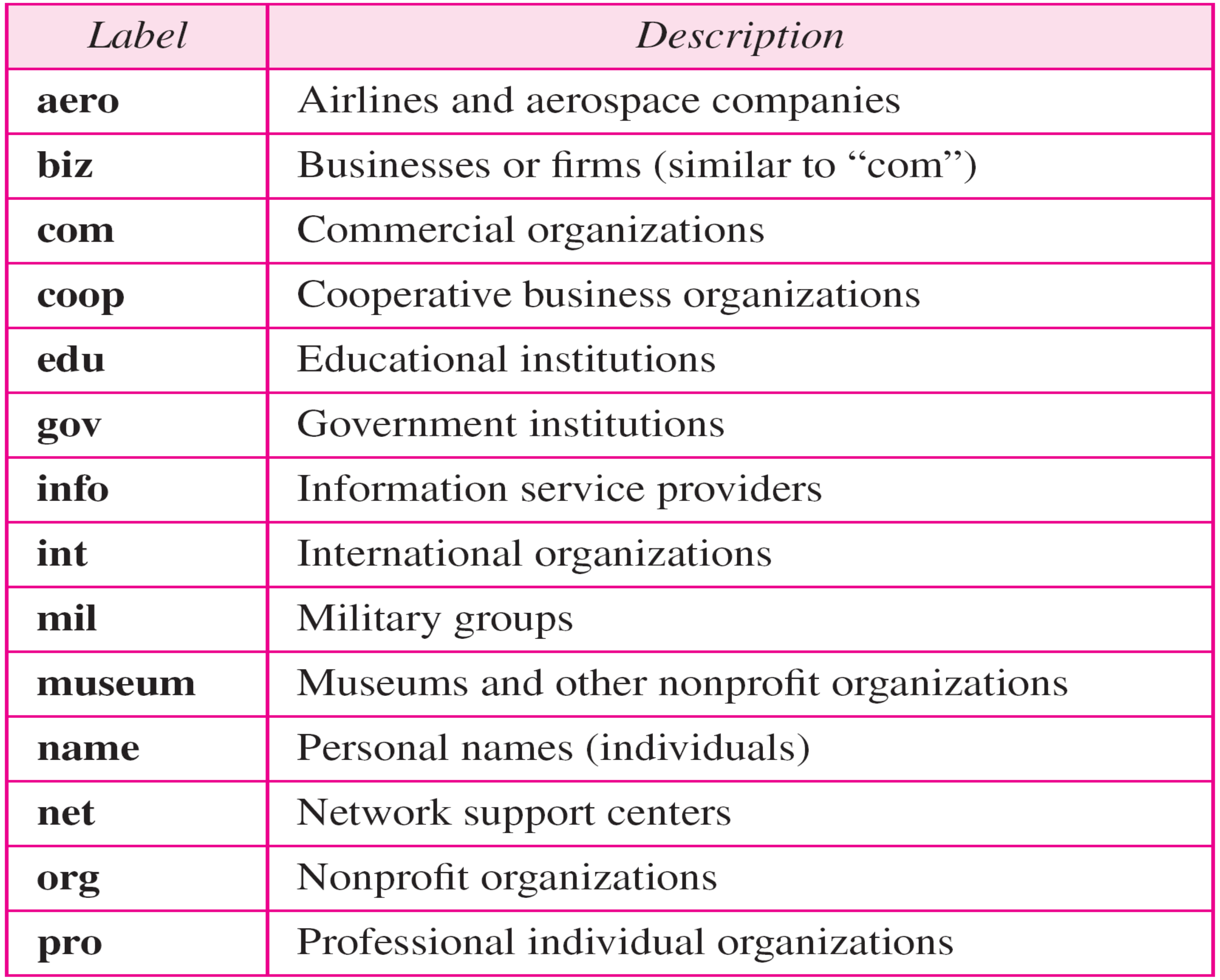


Generic Domain

- The generic domain defines the registered hosts according to their generic domain.



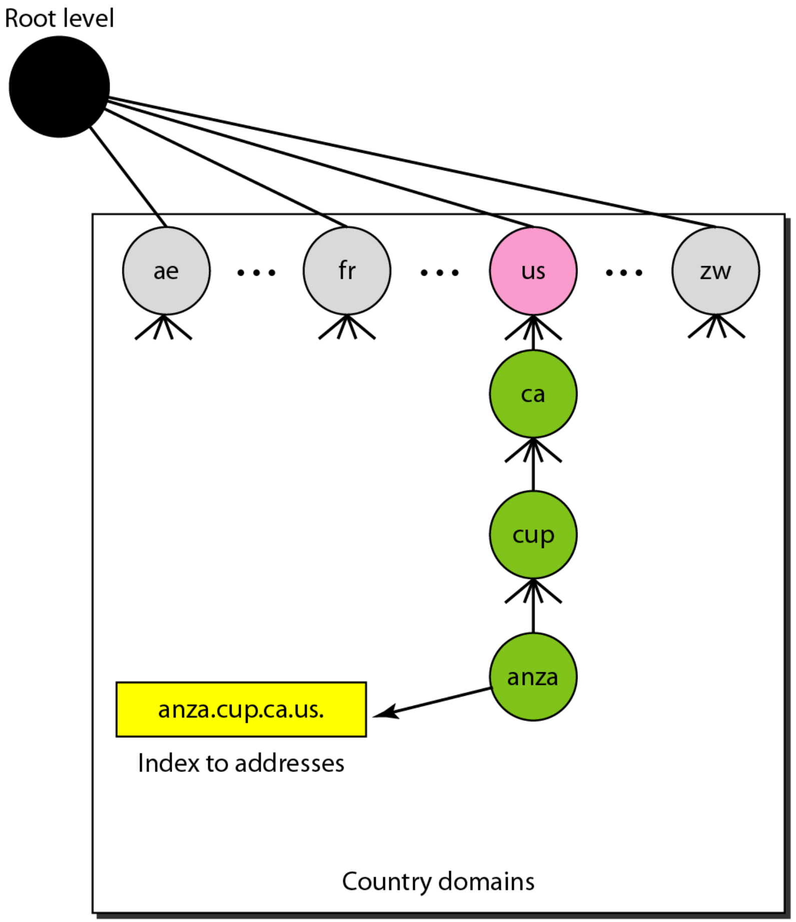
Generic Domain Level



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 nonprofit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

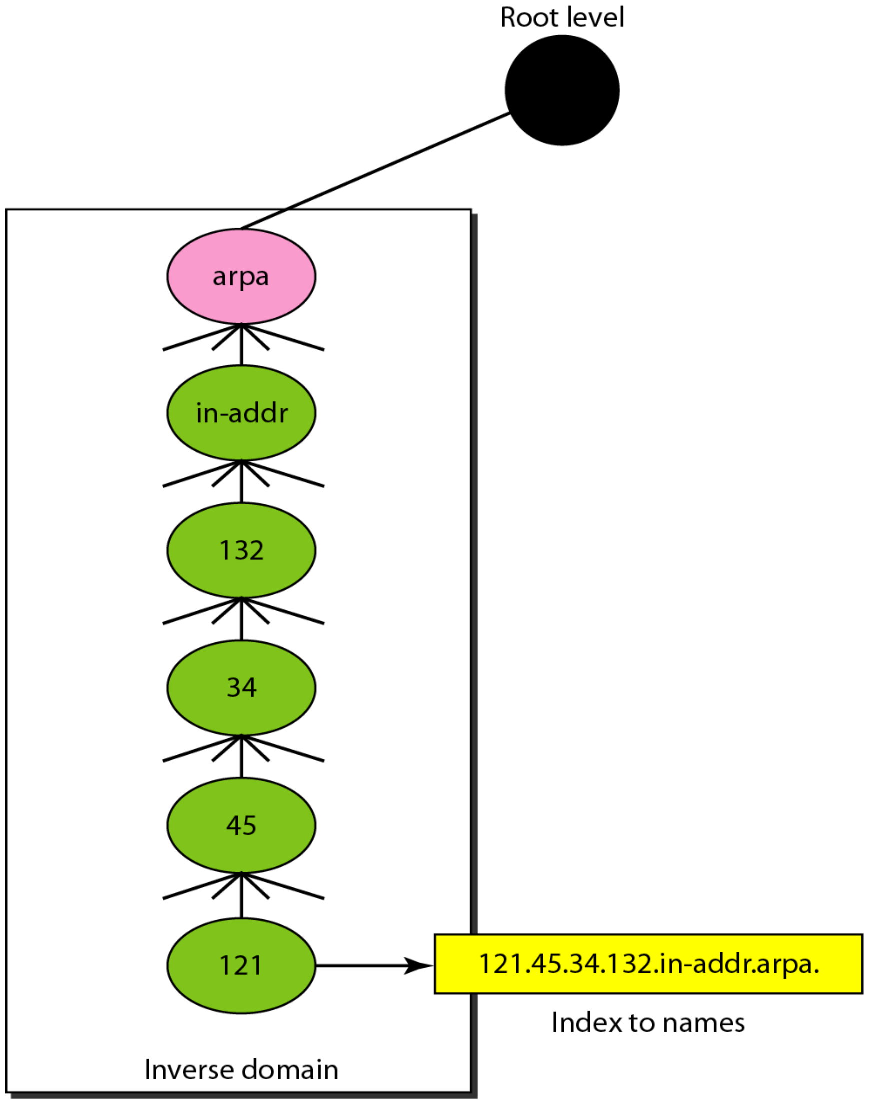
Country Domains

Uses two characters abbreviation



Inverse Domain

- Used to map address to an name. this is called address-to-name resolution.



Resolution

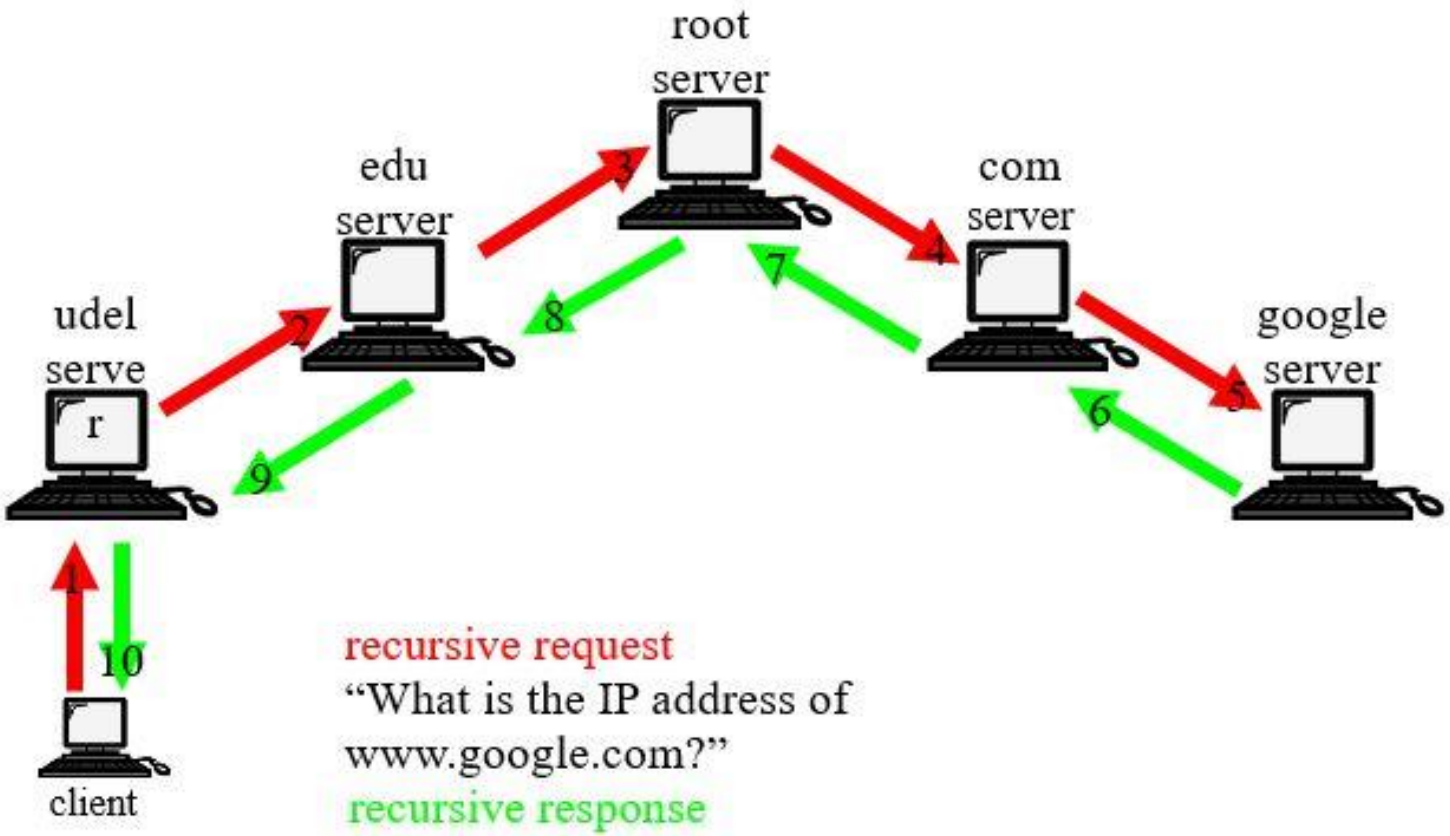
- Mapping a name to an address or an address to a name is called **name-address resolution**.

- A host that needs to map an address to a name or a name to an address calls a **DNS client** called a **resolver**.
- The resolver accesses the closest DNS server with a mapping request.
- If the server has the information, it satisfies the resolver; otherwise, it either refers the resolver to other servers or asks other servers to provide the information.

Resolution Types

- Recursive Resolution
- Iterative Resolution
- Caching

Recursive Resolution



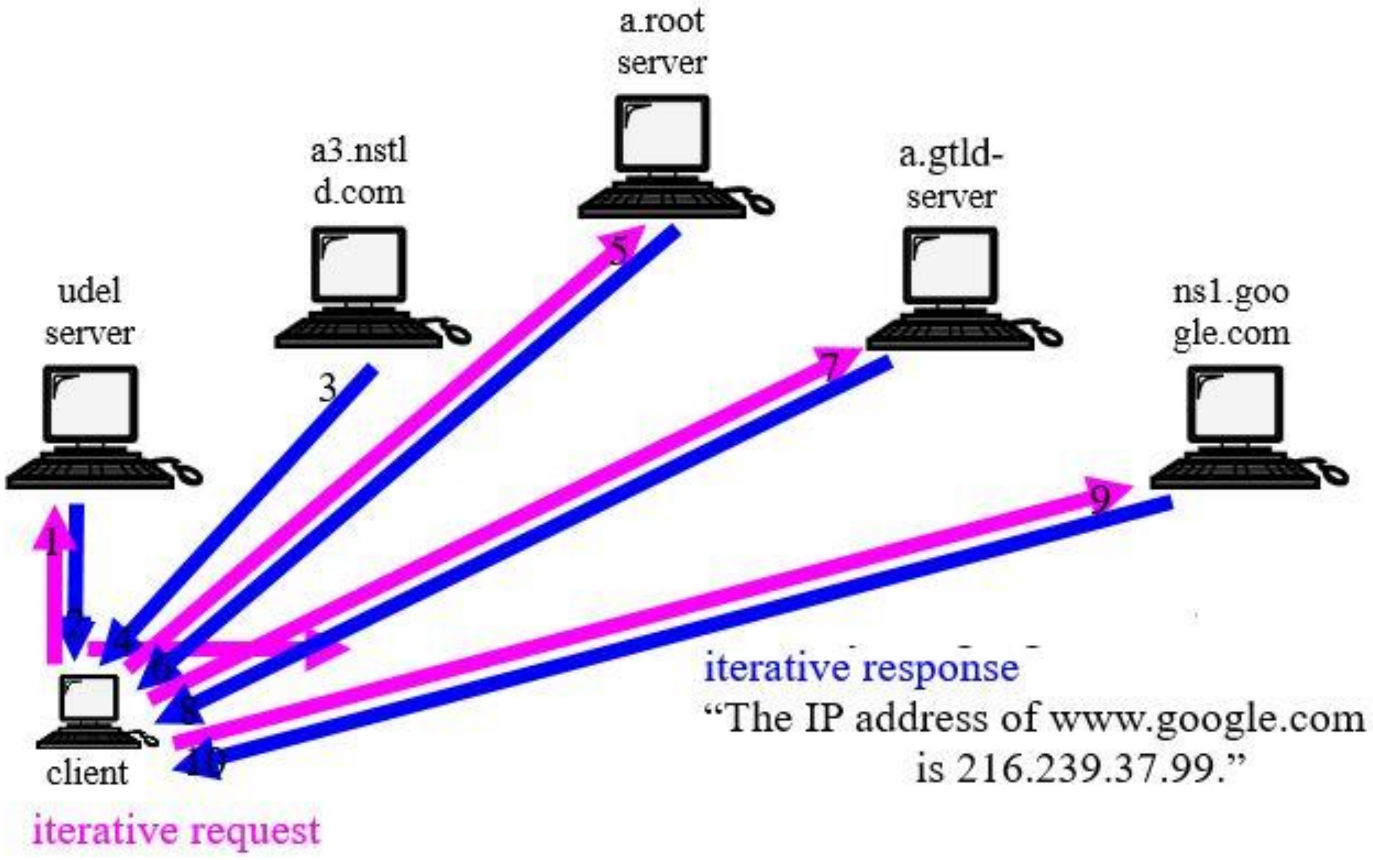
recursive request

"What is the IP address of www.google.com?"

recursive response

"The IP address of www.google.com is 216.239.37.99."

Iterative Resolution

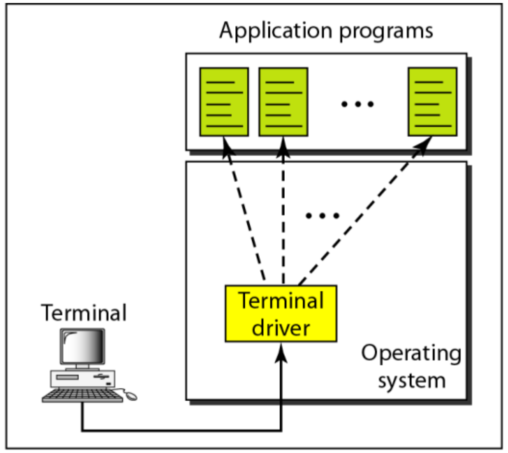


What is the IP address of www.google.com ?

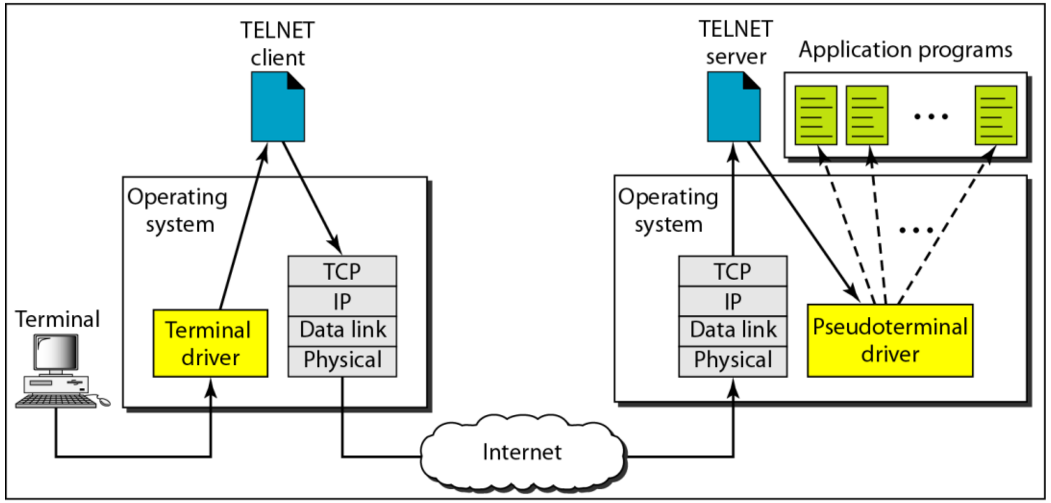
TELNET

- Abbreviation for TELecommunication NETwork.
- It is a client/server application program that allows a user to log on to a remote machine, giving the user access to the remote system.
- TELNET uses the ***network virtual terminal*** *(NVT)* system to encode the characters on the local system. On the server machine, NVT decodes the characters to a form acceptable to the remote machine.
- NVT uses the set of characters for data and a set of characters for control.
- TELNET uses only one TCP connection. The server uses the well known port 23 and client uses the an ephemeral port.
- The same connection is used to send data and control characters. Control characters are embedded in the data stream.

Local and Remote Log-in



a. Local log-in



b. Remote log-in

Local log-in

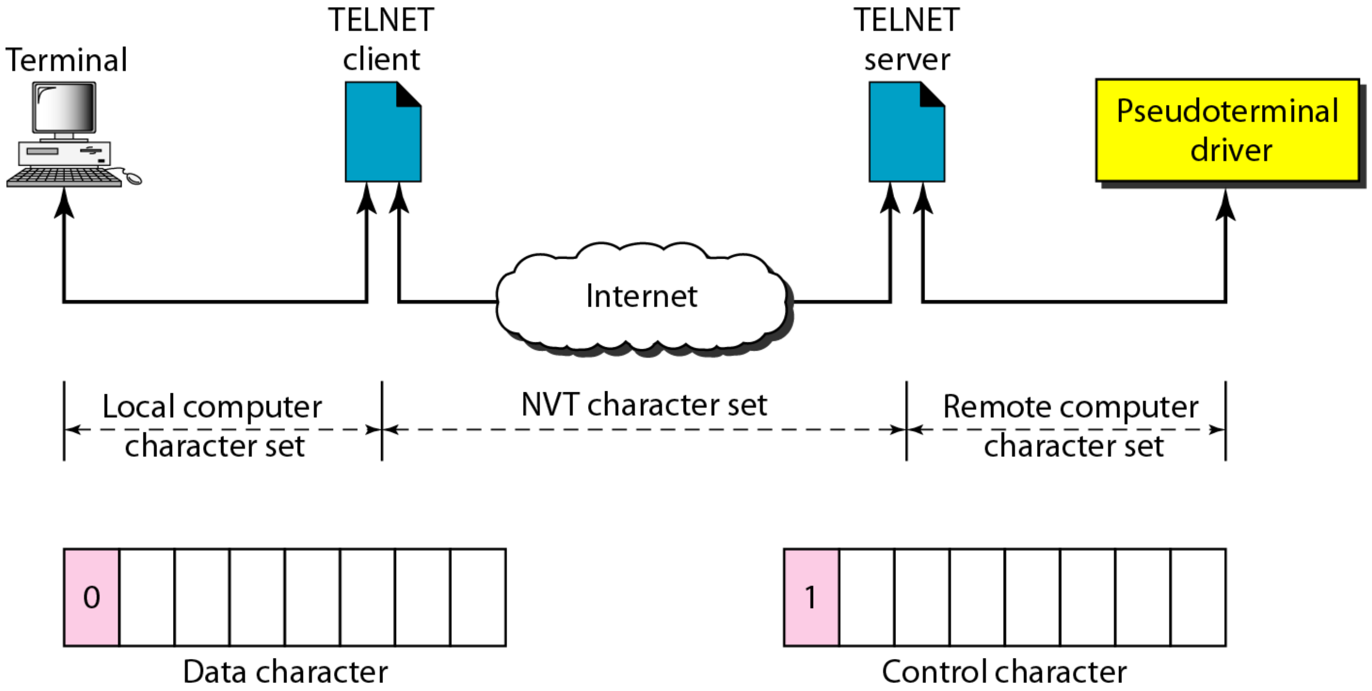
- When a user logs into a local timesharing system, it is called local log-in.
- When a user types at a terminal, the keystrokes are accepted by the terminal driver.
- The terminal driver passes the characters to the operating system.
- The operating system, in turn, interprets the combination of characters and invokes the desired application program or utility.

Remote Log-in

- When user access an application program or utility located on a remote machine, it is called remote log-in, in which telnet client and server comes in use.
- The users sends the keystrokes to the terminal driver, when the local operating system accepts the characters but does not interpret them. The characters are send to the TELNET client, which transforms the characters to a universal character set called **network virtual terminal (NVT)** characters and delivers them to the local TCP/IP protocol stack.
- The commands or text, in NVT form, travel through the internet and arrive at the TCP/IP stack at the remote machine. Here the characters are delivered to the operating system and passed to the TELNET server, which changes the characters to the corresponding characters understandable by the remote computer.
- However, the character cannot directly passed to OS because remote OS are not designed to receive the characters from a TELNET server. The software called ***pseudo terminal driver*** is used which pretends that the characters are coming from the a terminal. The OS then passed the characters to the appropriate application.

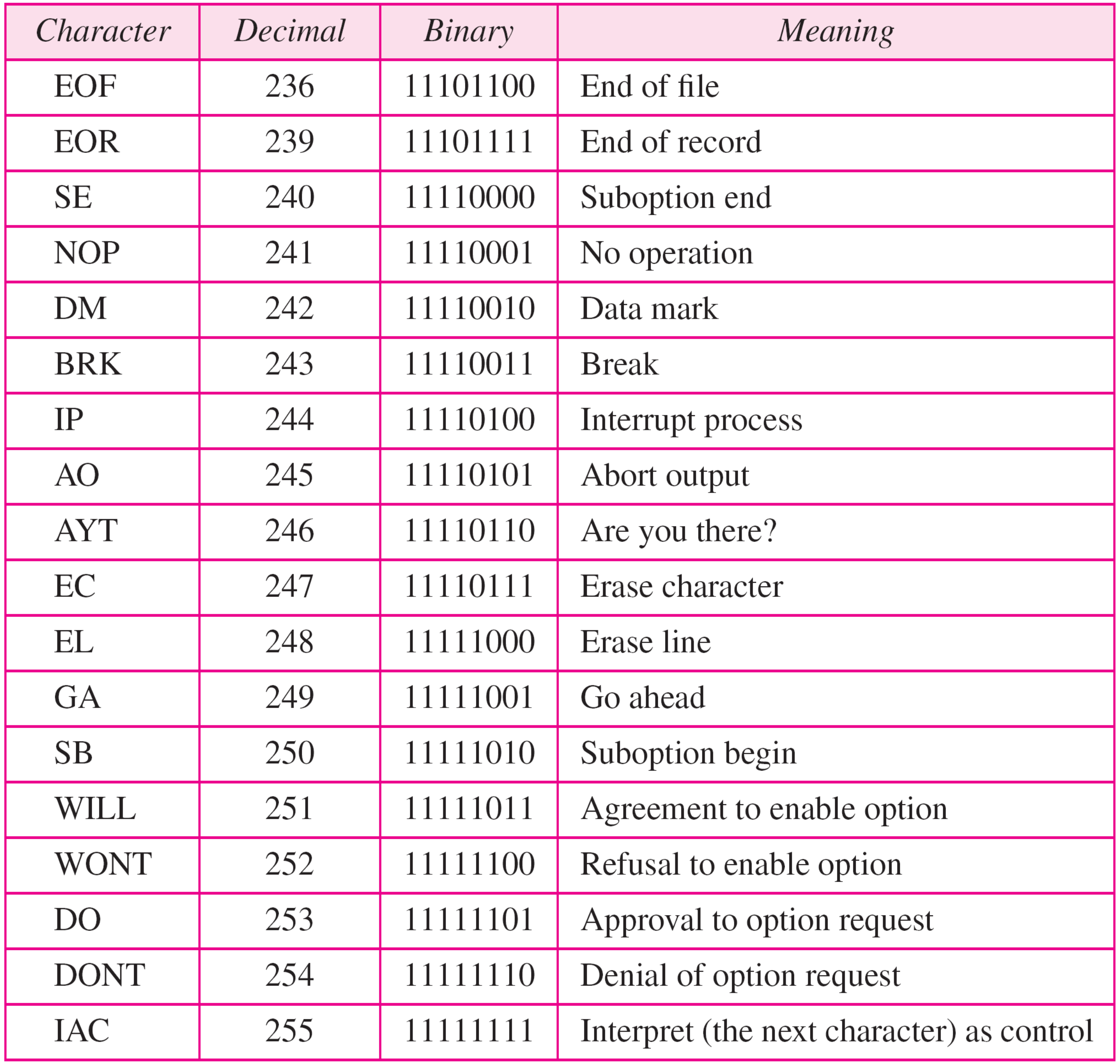
Network Virtual Terminal (NVT)

- TELNET uses the network virtual terminal (NVT) system to encode the characters on the local system. On the server machine, NVT decodes the characters to a form acceptable to the remote machine.
- NVT uses the set of characters for data and a set of characters for control.
- Control characters are embedded in the data stream and preceded by the *interpret as control (IAC)* control character.



NAT character set

- Uses to set of characters: one for data and one for control
- Both are 8-bit
- For data, 7 lowest bit are the same as ASCII and the highest order is 0.
- For control, 7 lowest bit are the same as ASCII and the highest order is 1.



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

Figure: NVT control character set

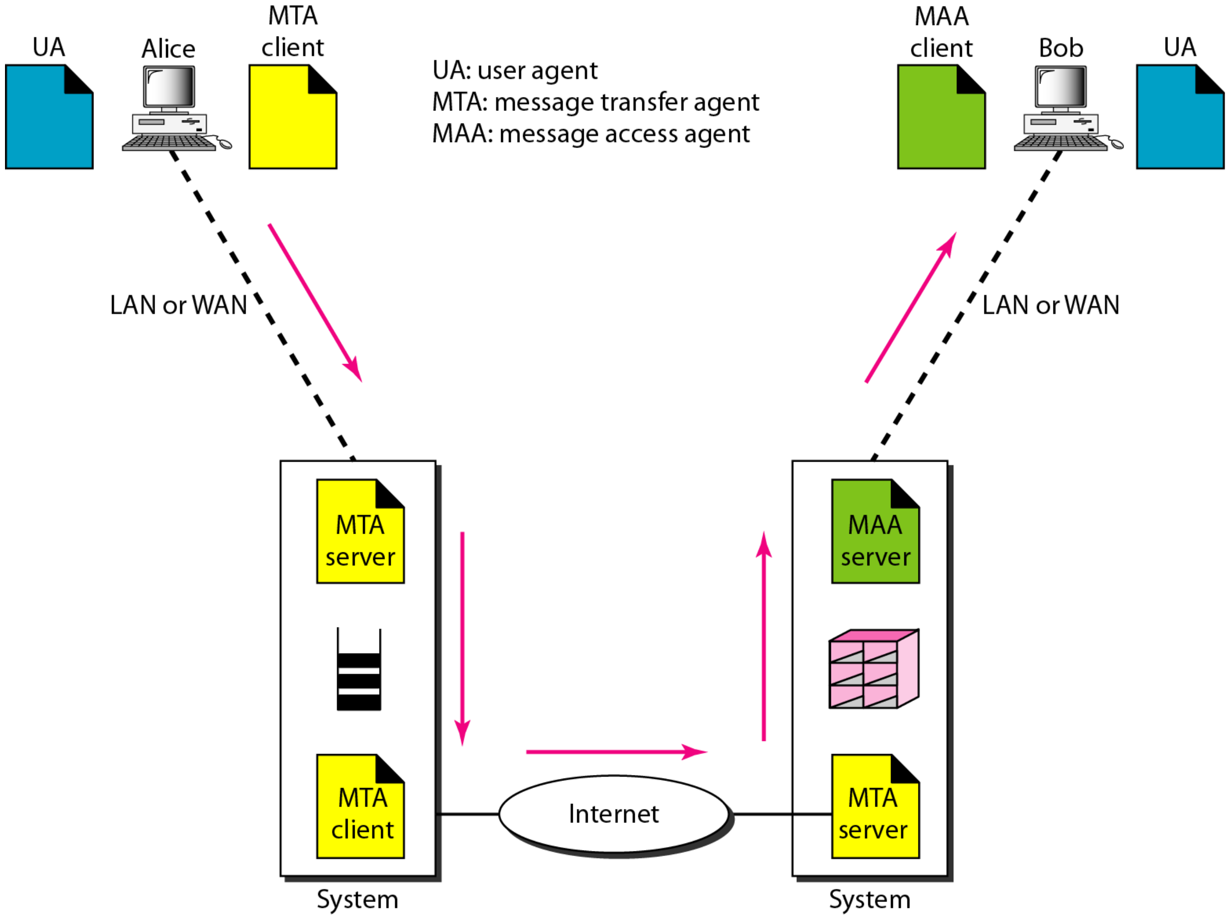
Mail Protocol

- SMTP
- POP
- IMAP

Electronic Mail (E-mail) Architecture

Three parts:

1. User Agent
2. Message Transfer Agent
3. Message Access Agent



Introduction

- Alice (the user) uses a user agent to prepare a message. Then message is send through LAN or WAN to the mail server using MTA, which in turn calls the MTA client.
- The MTA client established the a connection with the MTA server on the system, which is running all the time. The system at Alice's site queues all messages received. It then uses MTA to send to mail server of BOB's system.
- BOB uses an Messages Access Agent client to retrieve mail from mail server. The client sends a request to the MAA server, which is running all the time, and requests the transfer of the messages.

User Agent

- The first component of an e-mail is the user agent (UA).
- It is a software package (program) that provides the services to the user.

Services of user agent are:

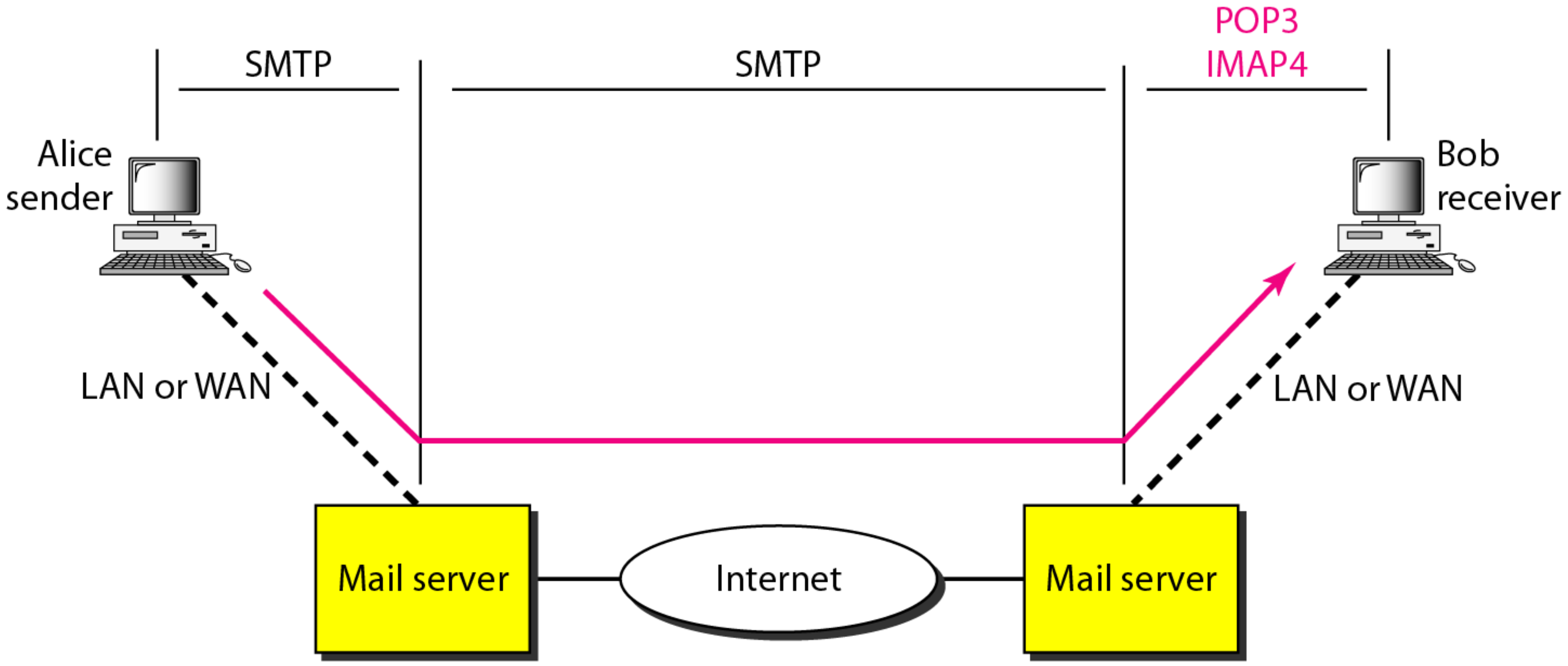
- ➢Composing messages
- ➢Reading messages
- ➢Replying to messages
- ➢Forwarding the messages
- ➢Handling mailbox

Types of agents

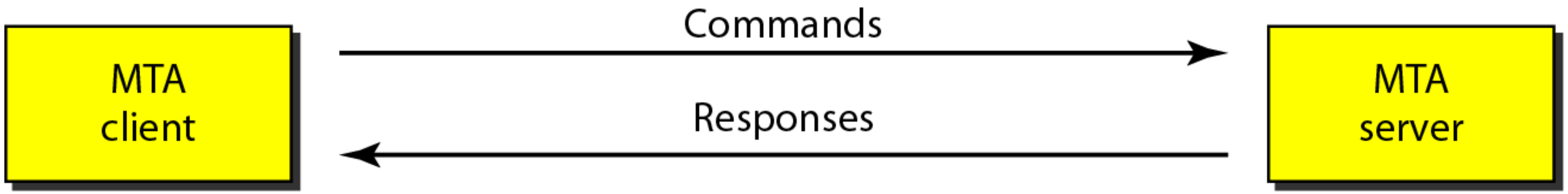
- Command driven: e.g. *mail, pine, and elm*
- GUI-based: e.g. *Eudora, Outlook, and Netscape*

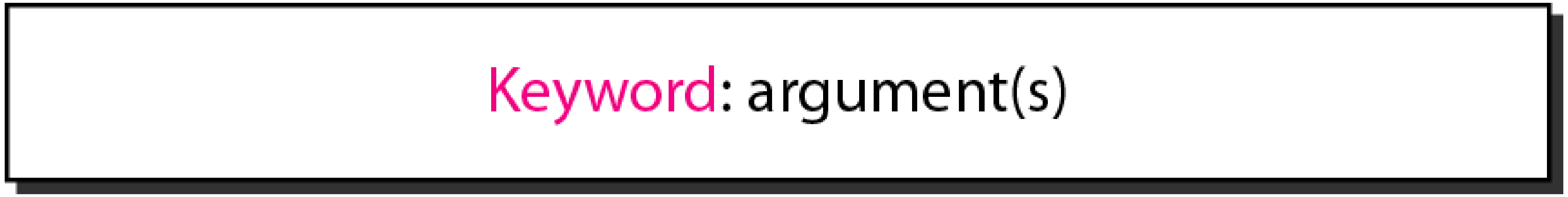
Message Transfer Agent (MTA)

- The actual mail transfer is done through the MTA.
- To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA.
- The protocol that defines the MTA client and server in the internet is SMPT (Simple Mail Transfer Protocol).
- SMTP is the standard protocol for transferring mail between hosts in the TCP/IP suite. SMTP uses the TCP port 25.

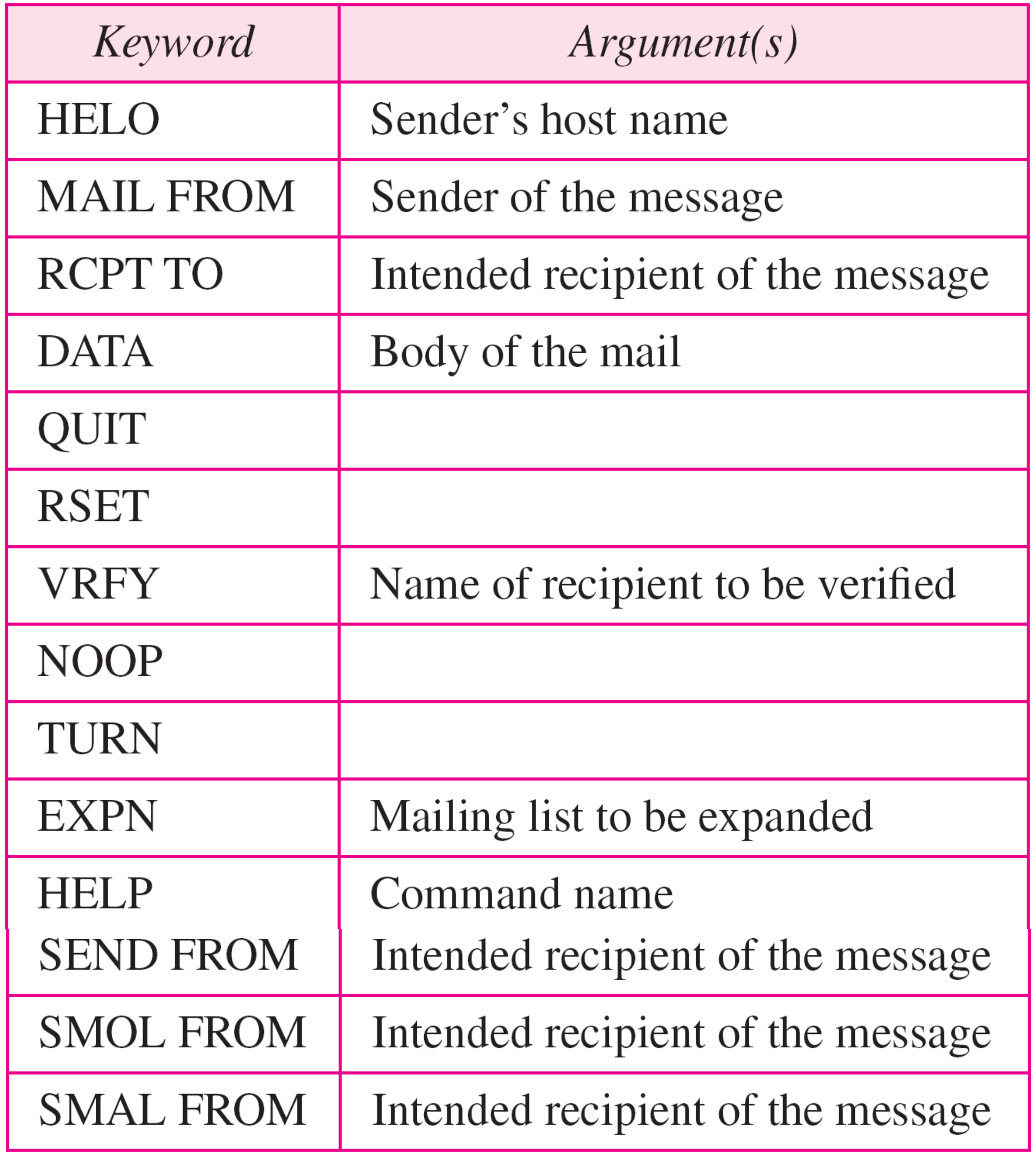


- SMPT uses the commands and response to transfer messages between an MTA client and an MTA server.

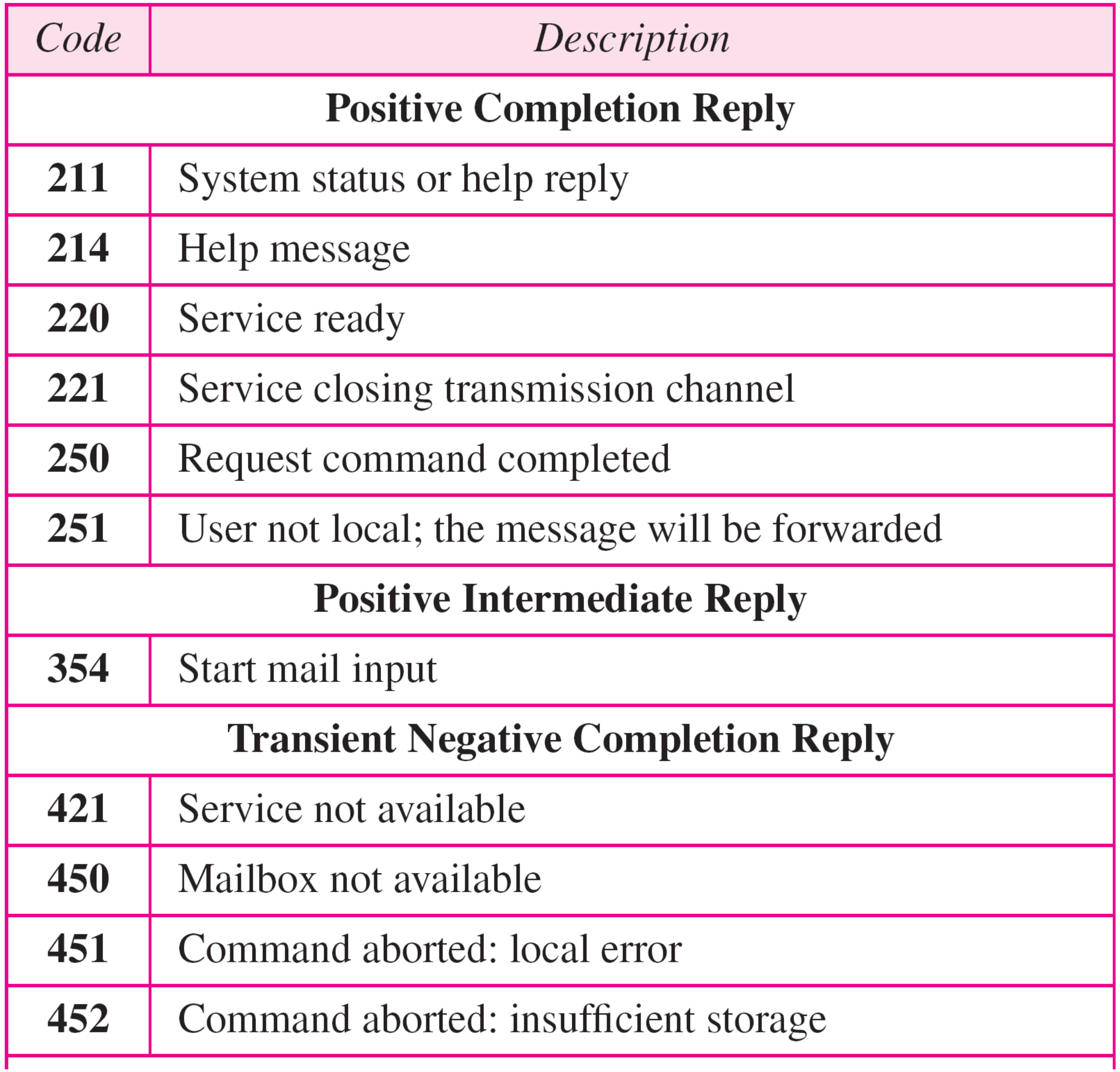




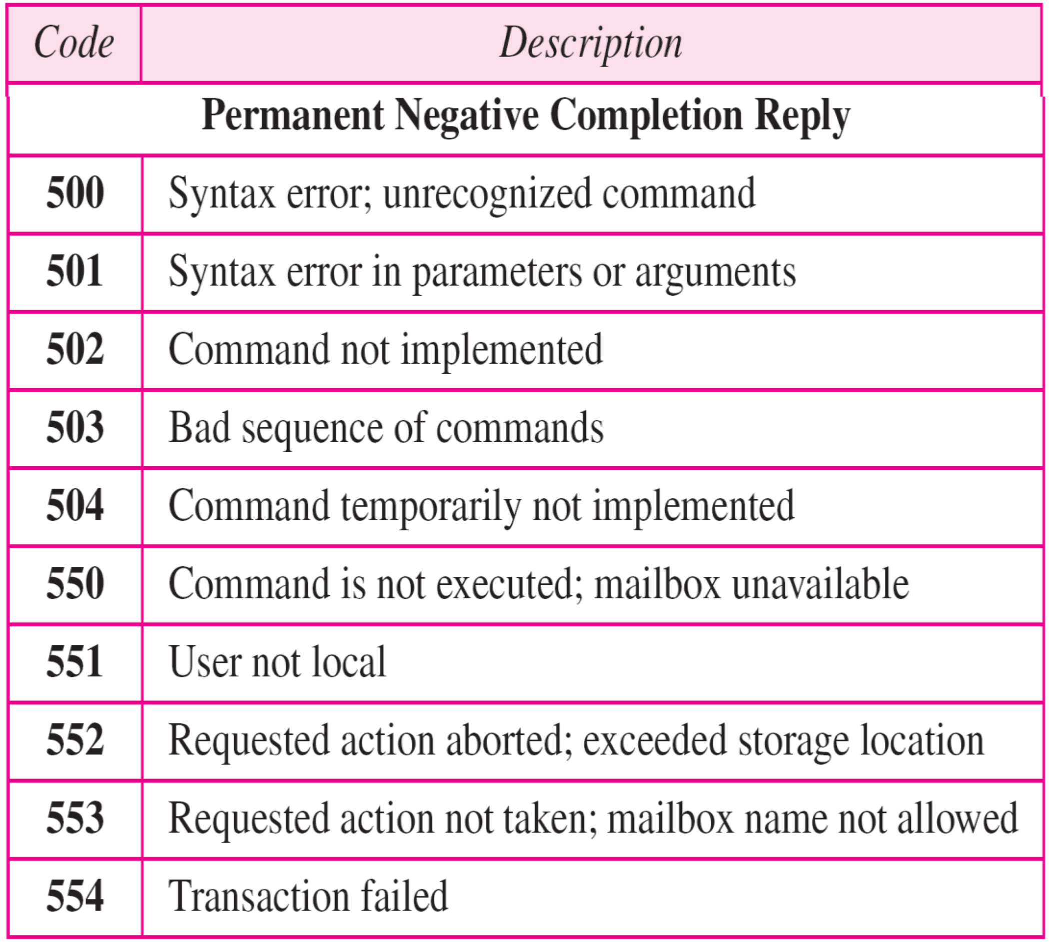
Command Format



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



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



Code	*Description*
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: three digit code

Mail Transfer Phases

- The process of transferring a mail message occurs in three phases:
    1. Connection establishment
    2. Mail transfer
    3. Connection termination → Uses POP and IMAP

Uses SMTP

Message Access Agent (MAA) :POP and IMAP

- It is pull protocol, that is, the client must pull messages from the server and used in the third stage.
- Two protocols are used as MAA:
    1. POP3
    2. IMAP4

POP3

- Stands for Post Office Protocol, version 3, simple and limited in functionality.
- The client POP3 is installed on the recipient computer, the server POP3 software is installed on the mail server.

Process

- Mail access starts with the client when the user needs to download e-mail form the mailbox on the mail server.
- The client opens a connection to the server on TCP port 110.
- it then sends its user name and password to access the mailbox.
- The user can then list and retrieve the mail message, one by one.

Two mode of POP3

1. The delete mode
   - ➢ Mail is deleted from the mail box after each retrieval
2. The keep mode
   - ➢ The mail remains in the mailbox after retrieval

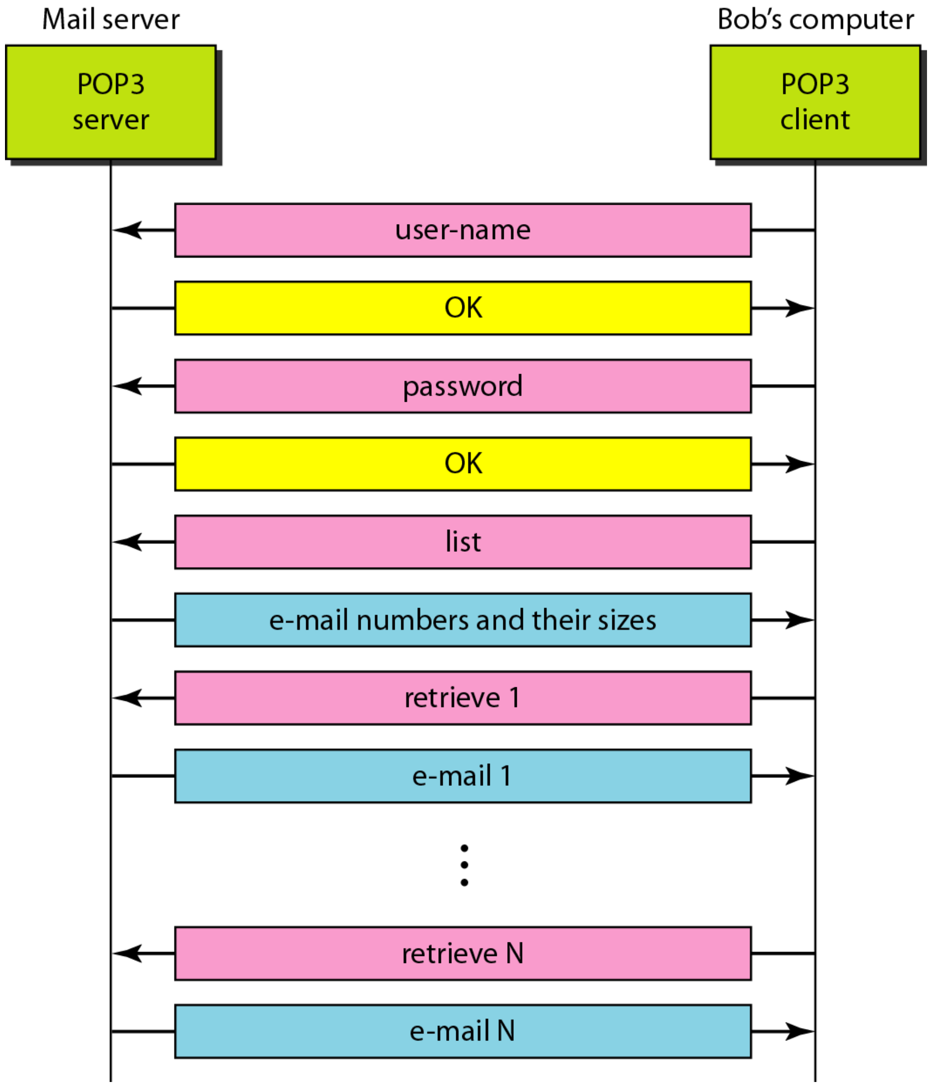


Figure: The exchange of commands and responses in POP3

Drawbacks of POP3

- It does not allow the user to organize her mail on the server; the user cannot have different folders on the server.
- It does not allow the user to partially check the contents of the mail before downloading.

IMAP4

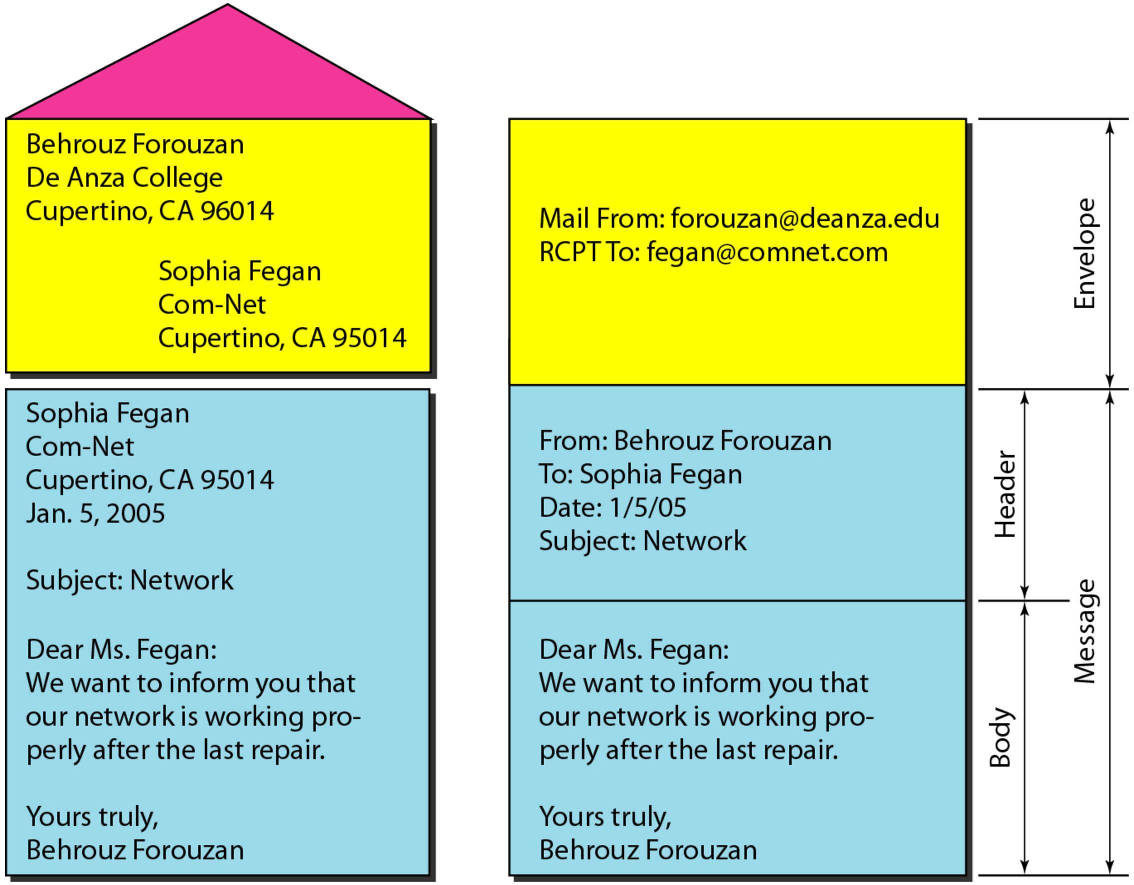
- Stands for Internet Mail Access Protocol, version 4.
- Similar to POP3, but it has more features than POP3; more powerful and complex.

IMAP4 provides the following extra functions:

- A user can check their 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 create, delete, or rename mailboxes on the mail server.
- A user can create a hierarchy of mailboxes in a folder for e-mail storage

Two parts:

1. **Envelope**: contains sender and receiver address
2. **Message**: contains the header and the body



Behrouz Forouzan
De Anza College
Cupertino, CA 96014

Sophia Fegan
Com-Net
Cupertino, CA 95014

Sophia Fegan
Com-Net
Cupertino, CA 95014
Jan. 5, 2005

Subject: Network

Dear Ms. Fegan:
We want to inform you that our network is working properly after the last repair.

Yours truly,
Behrouz Forouzan

a. Postal mail

Mail From: forouzan@deanza.edu
RCPT To: fegan@comnet.com

From: Behrouz Forouzan
To: Sophia Fegan
Date: 1/5/05
Subject: Network

Dear Ms. Fegan:
We want to inform you that our network is working properly after the last repair.

Yours truly,
Behrouz Forouzan

b. Electronic mail

Figure: Format of mail

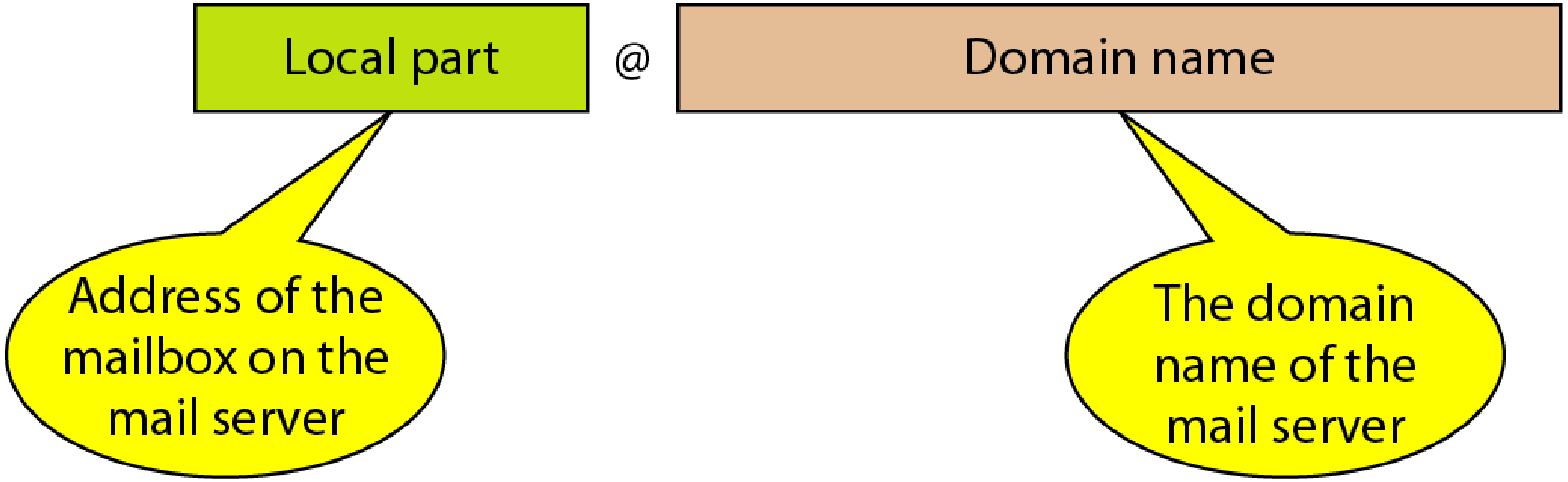

Local part
@
Domain name
Address of the mailbox on the mail server
The domain name of the mail server

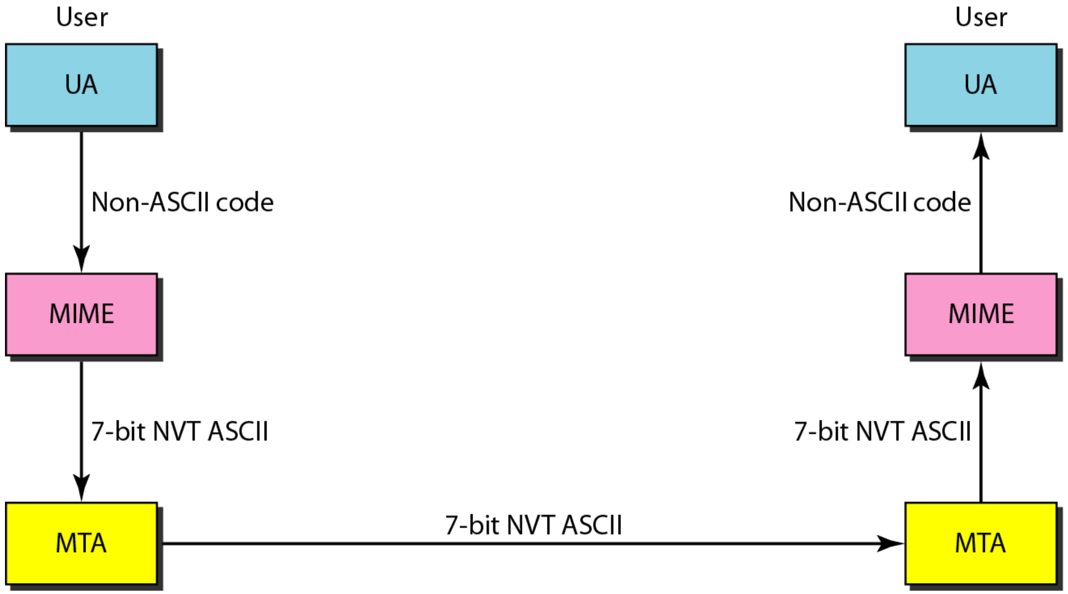
Figure: E-mail Address

Limitation of E-mail

- Can send message only in NVT 7 bit ASCII format. That is, it cannot be used for languages that are not supported by 7-bit ASCII characters (such as French, Germany, Russian, Chinese etc.)
- Also, it cannot be used to send binary files or videos or audio data.

MIME: Multipurpose Internet Mail Extension (MIME)

- MIME is a supplementary protocol that allows non-ASCII data to be send through e-mail. i.e. it allows the transfer of multimedia messages.
- MIME transforms non-ASCII data at the sender site to NVT ASCII data and delivers them to the client MTA to be sent through the internet. The messages at the receiving side is transformed back to the original data.



FTP : File Transfer Protocol

- One of the programs used for file transfer in the Internet is File Transfer Protocol (FTP).
- It uses the service of TCP and needs two TCP connections; the well-known TCP port 20 is used for data connection, and the well-known TCP port 21 is used for the control connection.

The client has three components:

1. User interface
2. Control process
3. Data transfer process

The server has two components:

1. Control process
2. Data transfer process

- The control connection is made between control process. It is connected the entire interactive FTP session.
- The data connection is made between the data transfer processes. It is opened and then closed for each file transferred.

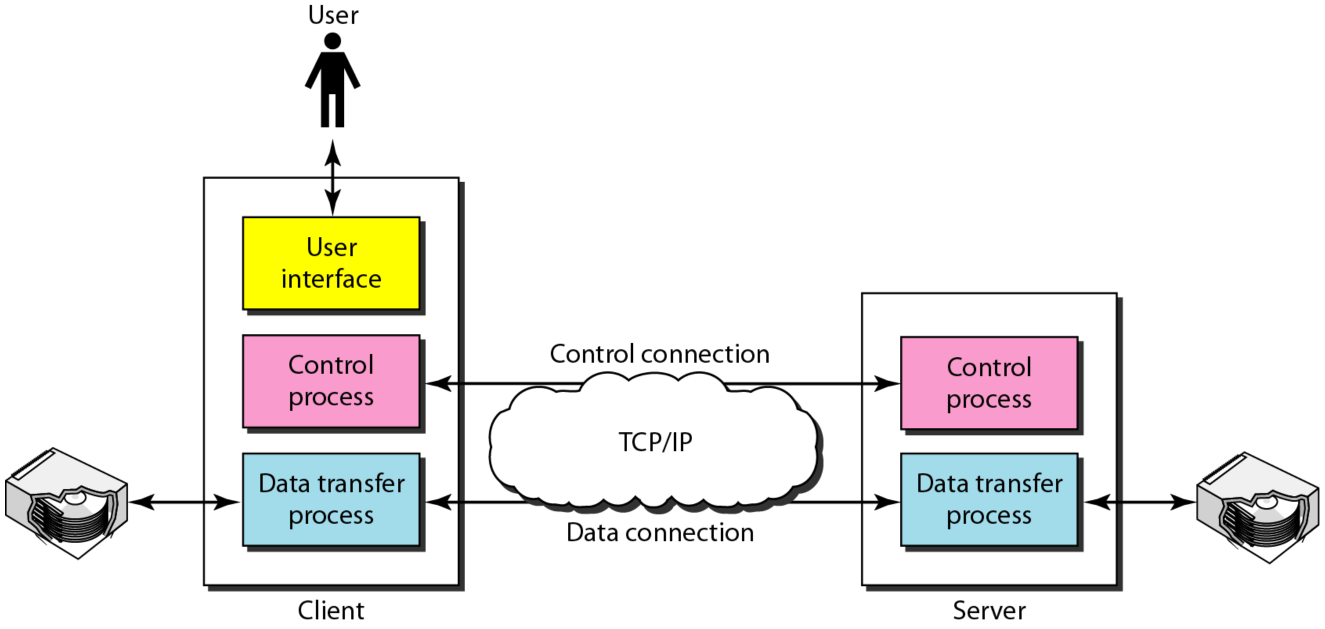
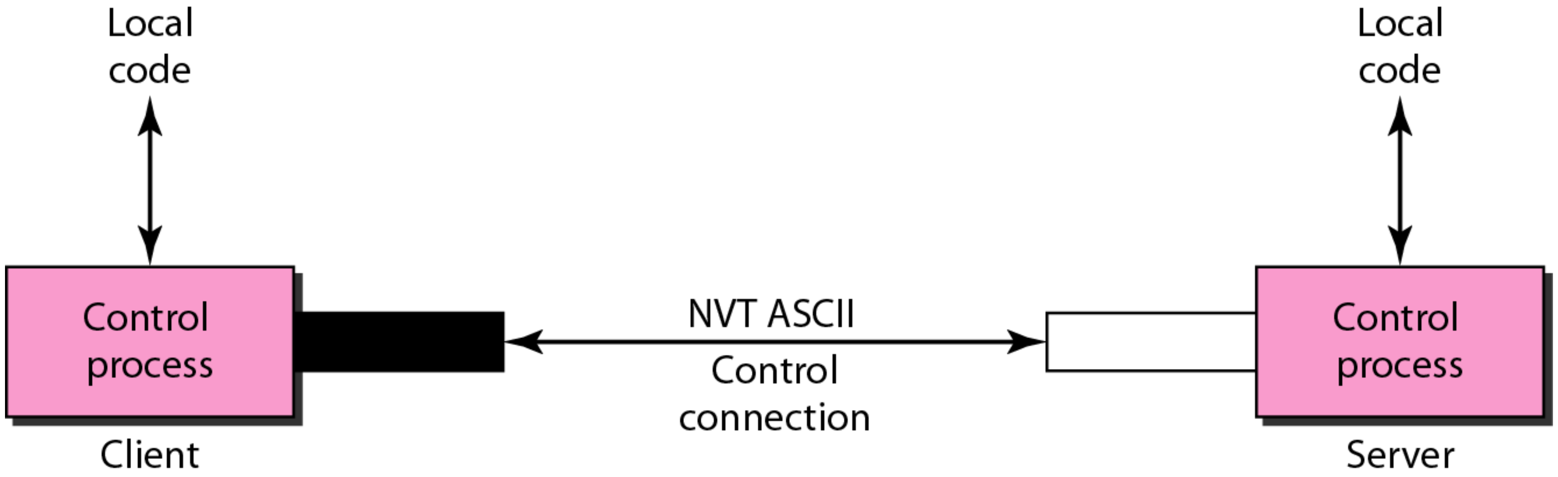


Figure: The Basic Model of FTP

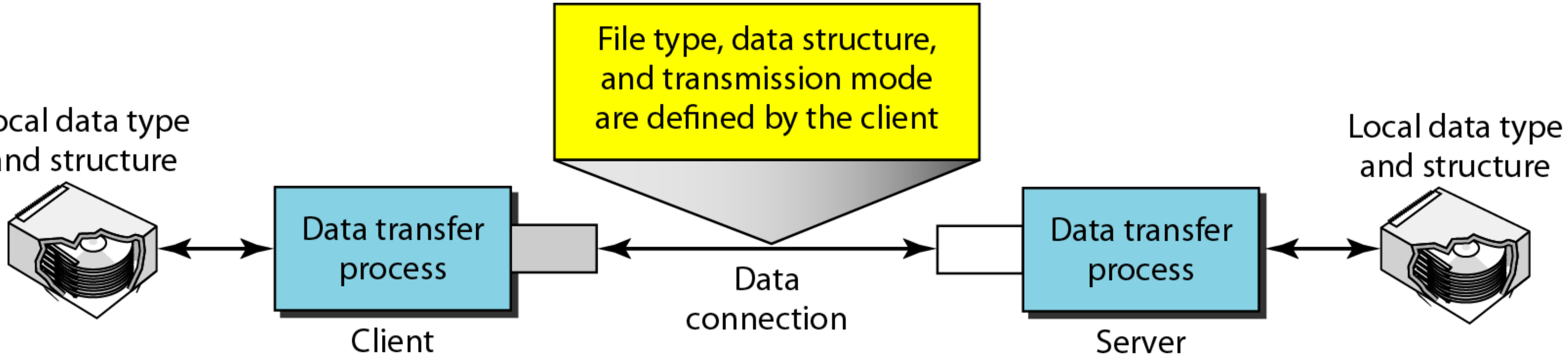
Communication over Control Connection

- Uses the 7 bit NVT ASCII character set
- Achieved through commands and responses.



Communication over data connection

- File transfer occurs over the data connection under the control of commands sent over the control connection.
- Prior to actual data transfer of files, the file type, data structure, and transmission mode are defined by the client through the control connection.
- There are three types of file transfer
  1. A file is copied from the server to the client
  2. A file is copied from the client to the server.
  3. A list of directories of file names is sent from the server to the client.


File type, data structure, and transmission mode are defined by the client
Local data type and structure
Data transfer process
Client
Data connection
Data transfer process
Server
Local data type and structure

File type

- ASCII file
- EBCDIC file
- Image file

Data Structure

- File structure
- Record structure
- Page structure

Transmission Mode

- Stream mode
- Block mode
- Compressed mode

WWW Service

- WWW
- HTTP
- HTTPS
- FTP

WWW: World Wide Web

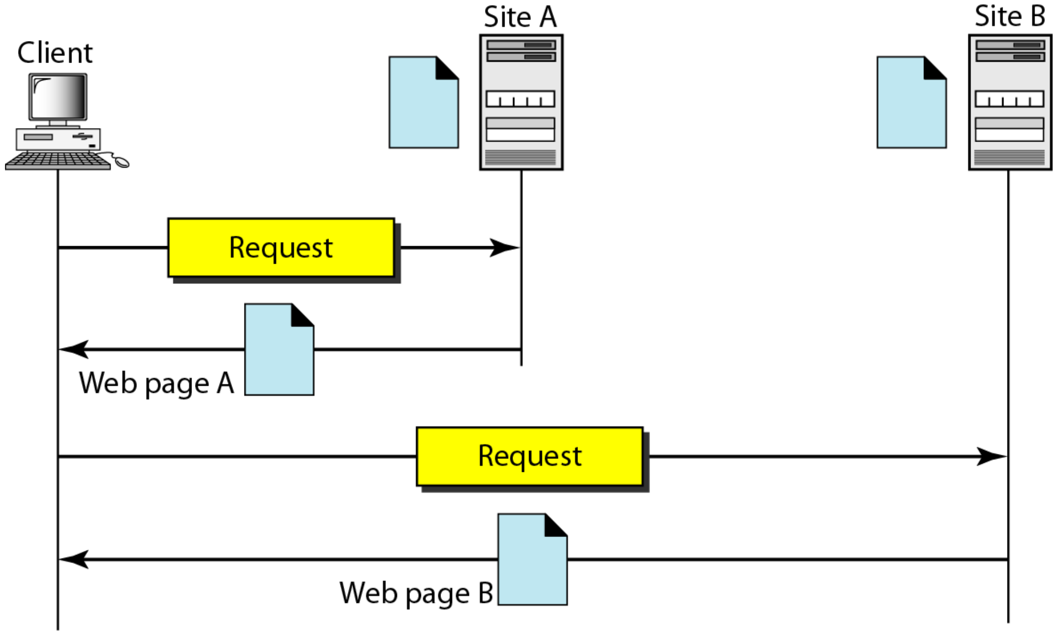
- It is a repository of information linked together from points all over the world.
- It consists of a vast, worldwide collection of documents or **web pages**. Each page may contain link to other pages anywhere in the world, called **hyperlink**.
- The pages are retrieved and viewed by using a **browser**.

Architecture of WWW

- The WWW today is a distributed client/server service, in which a client using a browser can access a service using a server. However, the service provided is distributed over many locations called sites.

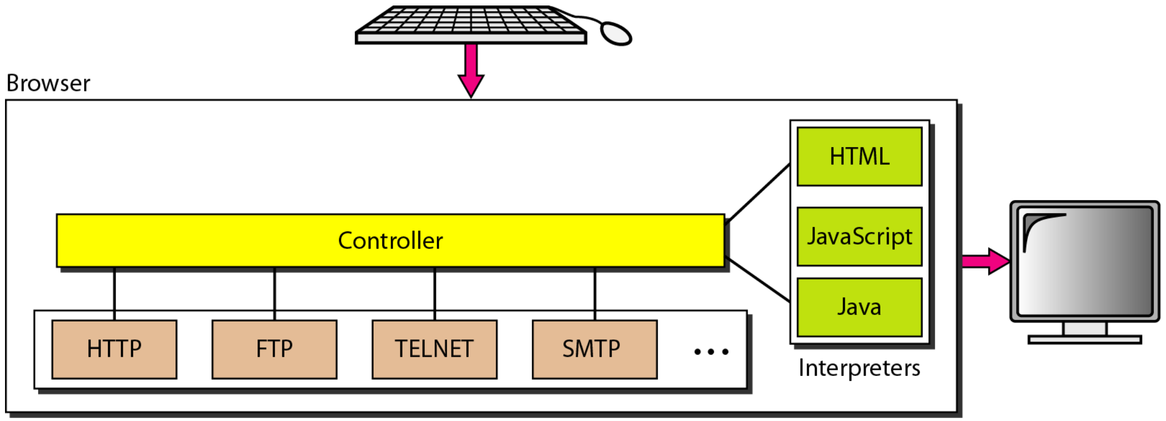
Description

- Suppose the client needs to see some information that it belongs to site A.
- It sends a request through its browser. A request consists of URL.
- The server at site A finds the documents and send to client.
- When the document is viewed, there is some references to other documents which is at site B.
- The clients sends another request to the new site, and the new page is viewed.



Browser

- A browser is an application program that interpret and display the contents of web pages.
- Each browser has three parts: a controller, client protocol, and interpreter.
  - A controller
    - ➢ receives input from keyboard or mouse and uses the client program to access the document.
    - ➢ Use interpreter to display the content of web page
  - Client protocol : HTTP, FTP, FILE etc.
  - Interpreter : HTML, Java, Javascript etc.

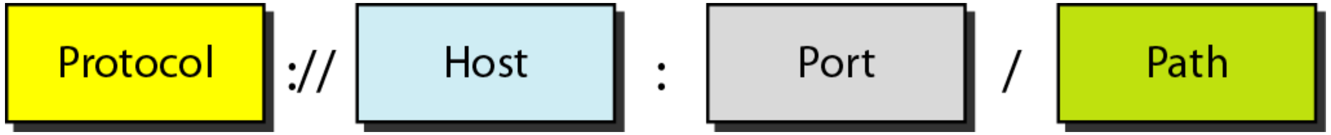


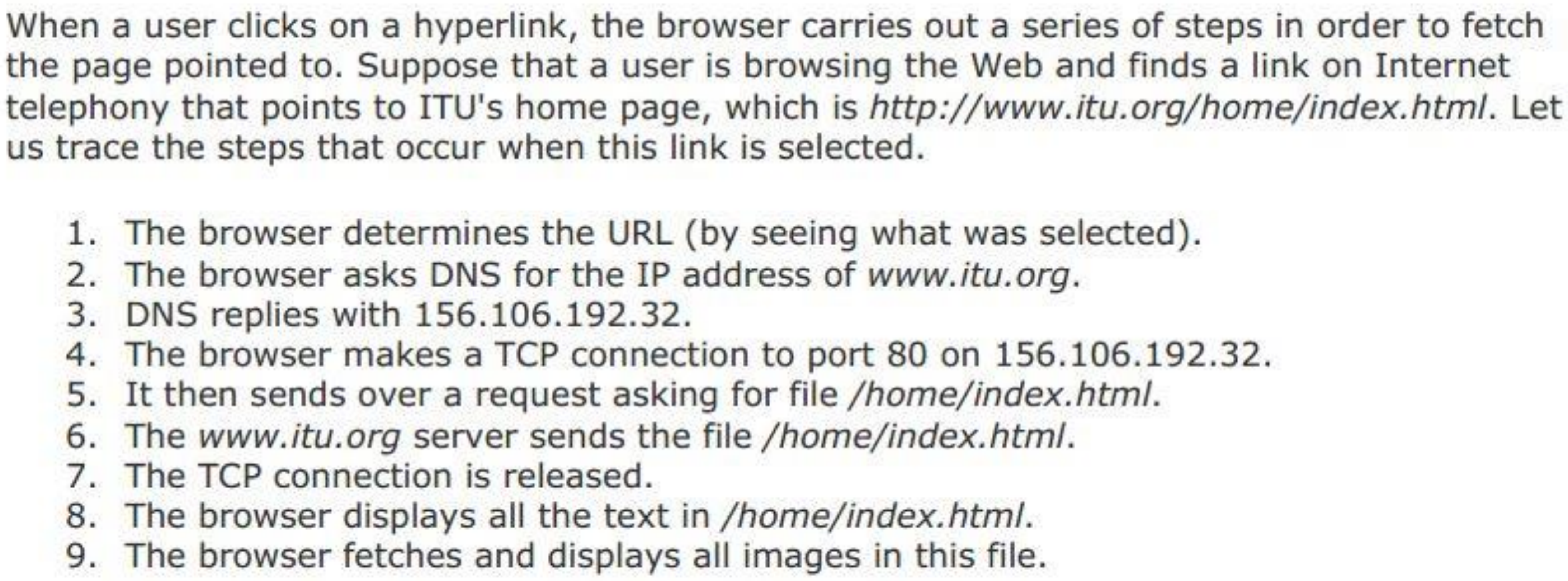
Server

- The web pages is stored in the server.
- Each time a client request arrives, the corresponding document is sent to the client.

URL : Universal Resource Locator

- It is the address of a web page. Each page has its own unique web address (URL) in the internet. This is how your computer locates the web page that you are trying to find.
- An example of a URL is: http://funbrain.com/index.html. In this example URL, funbrain.com is called the domain name. The "index.html" refers to the specific page.
- URL defines four thing: protocol, host computer, port, and path.





When a user clicks on a hyperlink, the browser carries out a series of steps in order to fetch the page pointed to. Suppose that a user is browsing the Web and finds a link on Internet telephony that points to ITU's home page, which is *http://www.itu.org/home/index.html*. Let us trace the steps that occur when this link is selected.

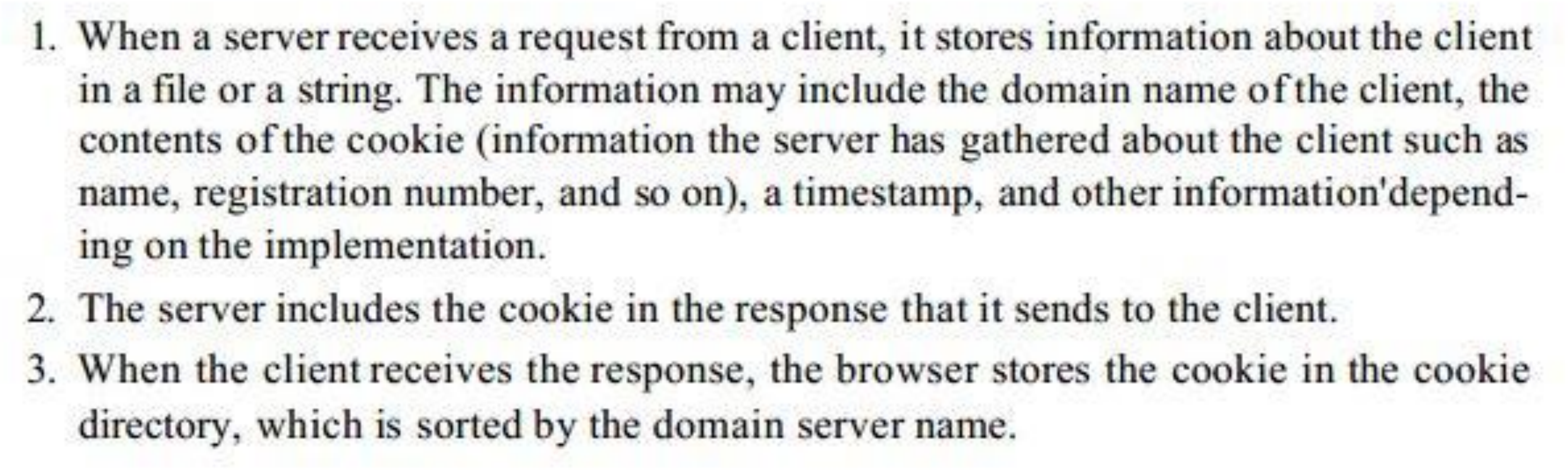
1. The browser determines the URL (by seeing what was selected).
2. The browser asks DNS for the IP address of *www.itu.org*.
3. DNS replies with 156.106.192.32.
4. The browser makes a TCP connection to port 80 on 156.106.192.32.
5. It then sends over a request asking for file */home/index.html*.
6. The *www.itu.org* server sends the file */home/index.html*.
7. The TCP connection is released.
8. The browser displays all the text in */home/index.html*.
9. The browser fetches and displays all images in this file.

Cookies

- **HTTP** is a stateless protocol because an HTTP server maintains no information about the clients. That is, a client sends a request; a server responds. Their relationship is over.
- If a particular client asks for the same object twice in a period of a few seconds, the server does not respond by saying that it just served the object to the client; instead, the server resends the object, as it has completely forgotten what it did earlier.

- **HTTP cookies**, sometimes known as **web cookies** or just **cookies**, are parcels of text sent by a server to a web browser and then sent back unchanged by the browser each time it accesses that server.
- HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences and the contents of their electronic shopping carts etc.

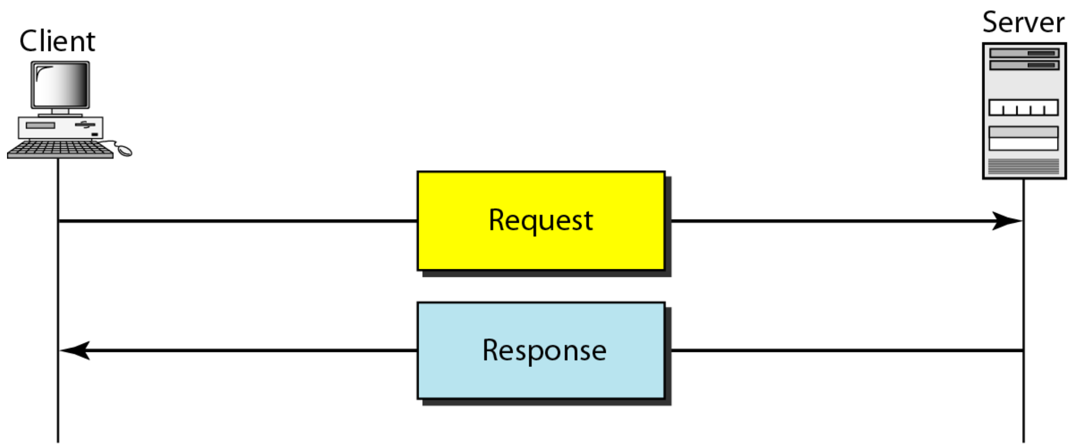
Creation and storage of cookies



1. When a server receives a request from a client, it stores information about the client in a file or a string. The information may include the domain name of the client, the contents of the cookie (information the server has gathered about the client such as name, registration number, and so on), a timestamp, and other information'depending on the implementation.
2. The server includes the cookie in the response that it sends to the client.
3. When the client receives the response, the browser stores the cookie in the cookie directory, which is sorted by the domain server name.

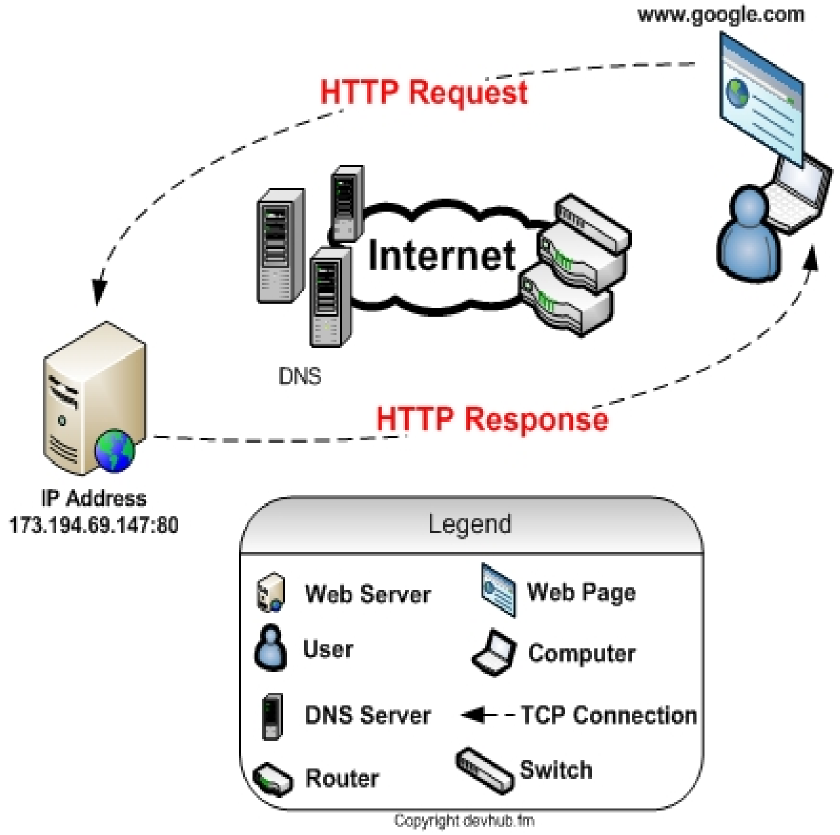
HTTP : Hyper Text Transfer Protocol

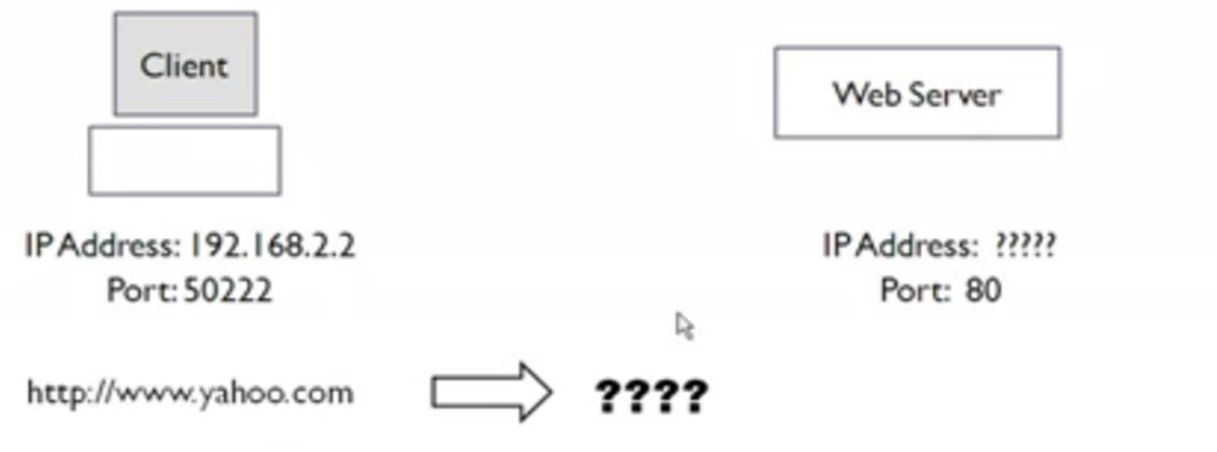
- HTTP is used mainly to access data on the WWW.
- HTTP uses the services of TCP on well-known port 80.



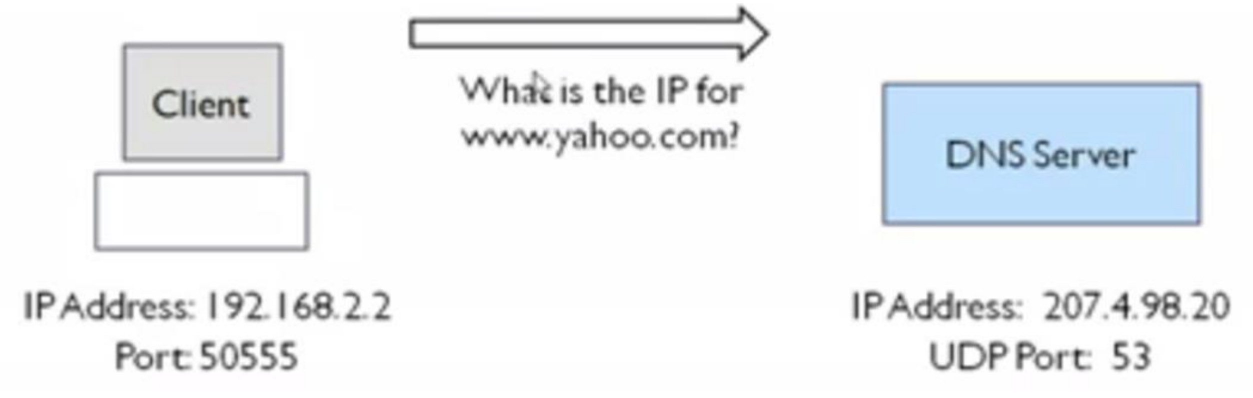
How does HTTP works?

- HTTP is implemented in two programs: a client program and a server program, executing on different end systems, talk to each other by exchanging HTTP messages.
- The HTTP client first initiates a TCP connection with the server. Once the connection is established, the browser and the server processes access TCP through their socket interfaces.

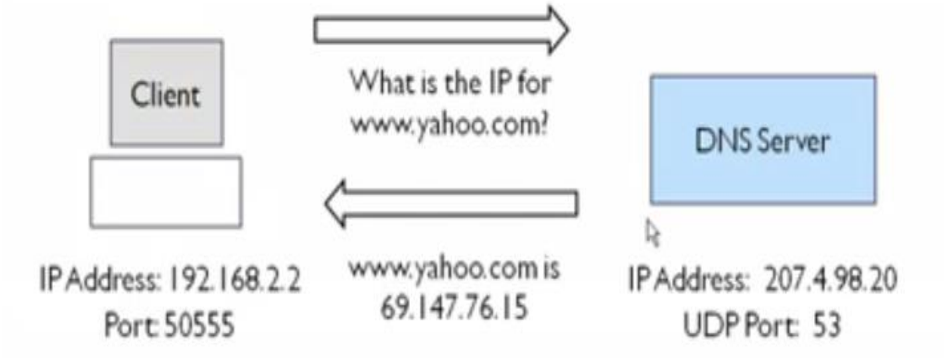




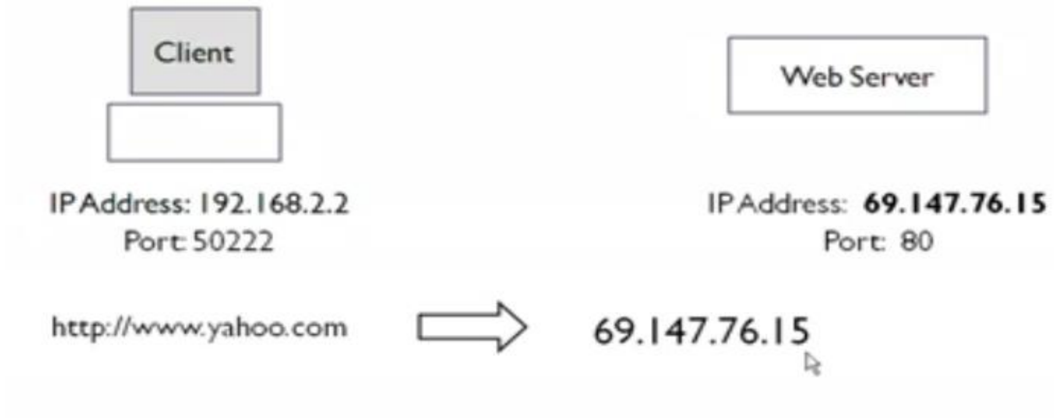
Step:1



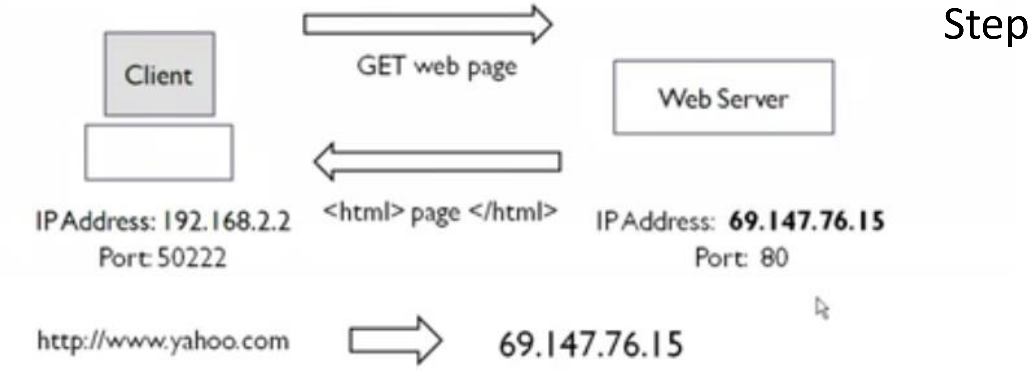
Step:2



Step:3

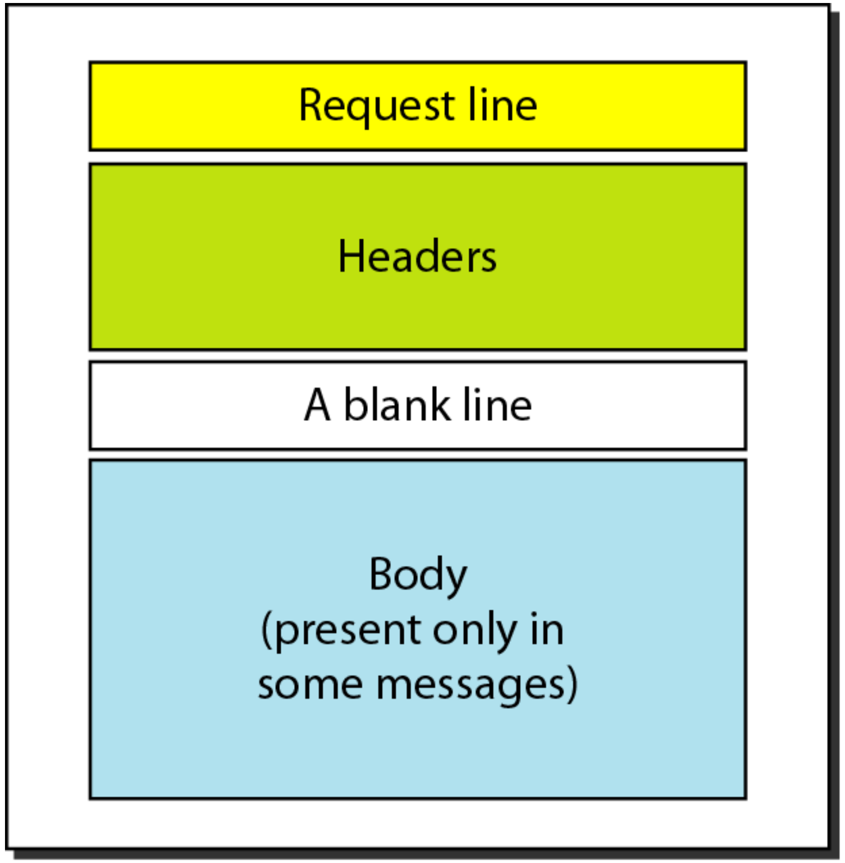


Step:4



Step:5

Request and Response Message



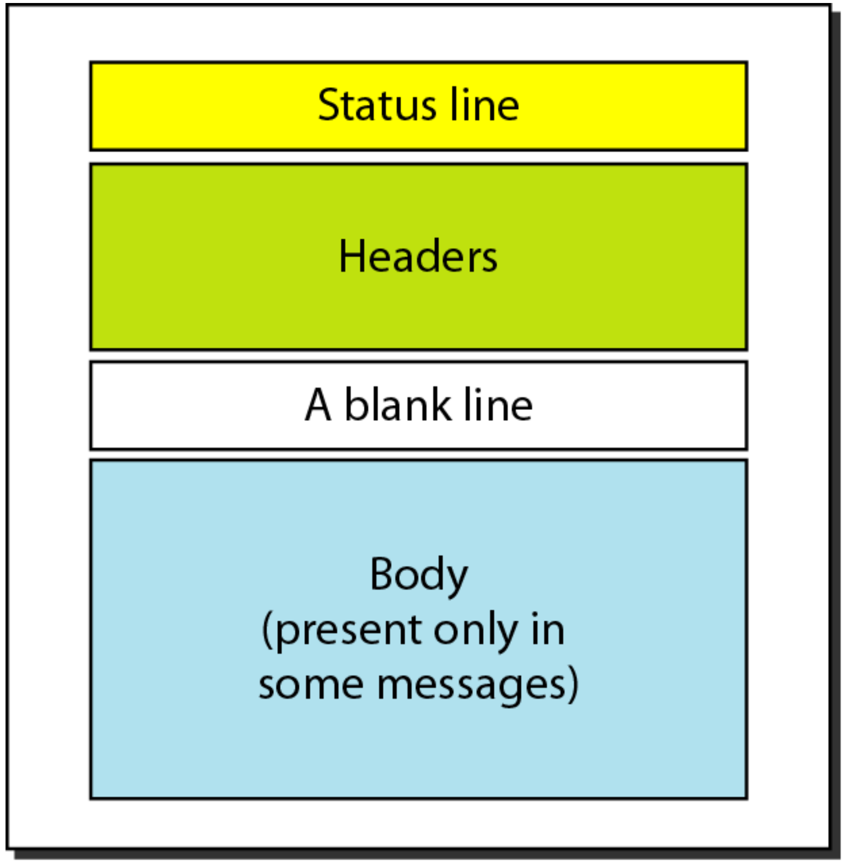
Request line

Headers

A blank line

Body
(present only in
some messages)

Request message



Status line

Headers

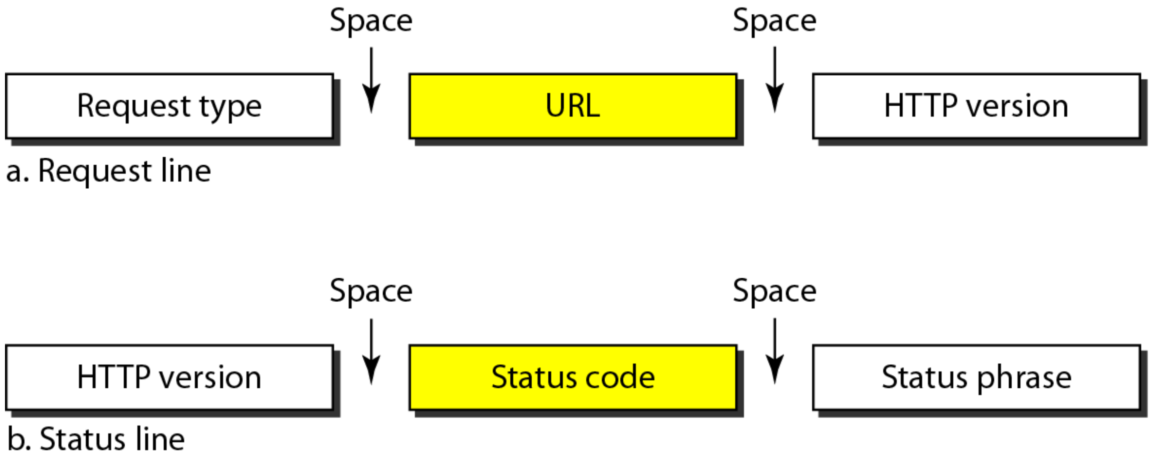
A blank line

Body
(present only in
some messages)

Response message

Request and Status Lines

- Request and status lines



- Request type (Methods) : GET, HEAD, POST, PUT, TRACE, CONNECT, OPTION
- Status codes: 3 digits code similar to FTP an SMTP

Persistent and non-persistent connection

Persistent connection

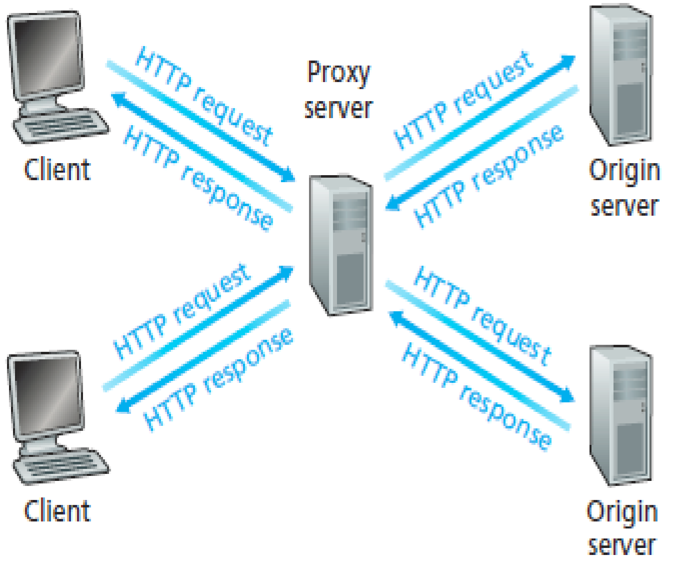
- In a persistent connection, the server leaves the connection open for more requests after sending a response.
- The server can close the connection at the request of a client or if a time-out has been reached.

Nonperistent connection

- In non-persistent connection, one TCP connection is made for each request/response.
- The following list the steps in this strategy:
  1. The client opens a TCP connection and sends a request.
  2. The server sends the response and close the connection.
  3. The client reads the data until it encounters end-of-file marker; it then closes the connection

Proxy Server/Web Caching

- Proxy server is a computer that keeps the copies of responses to recent requests.
- The HTTP client sends request to the proxy server. The proxy server checks its cache. It the response is not stored in the cache, the proxy server sends the request to the corresponding server. Incoming responses are sent to the proxy server and stored for future requests from other clients.
- The proxy server reduces the load on the original server, decreases traffic, and improves latency.



Clients requesting objects through a Web cache

HTTPS: Hyper Text Transfer Protocol Secure

Background

- Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to.
- The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are encrypted.
- HTTPS is often used to protect highly confidential online transactions like online banking and online shopping order forms.
- Web browsers such as Internet Explorer, Firefox and Chrome also display a padlock icon in the address bar to visually indicate that a HTTPS connection is in effect.

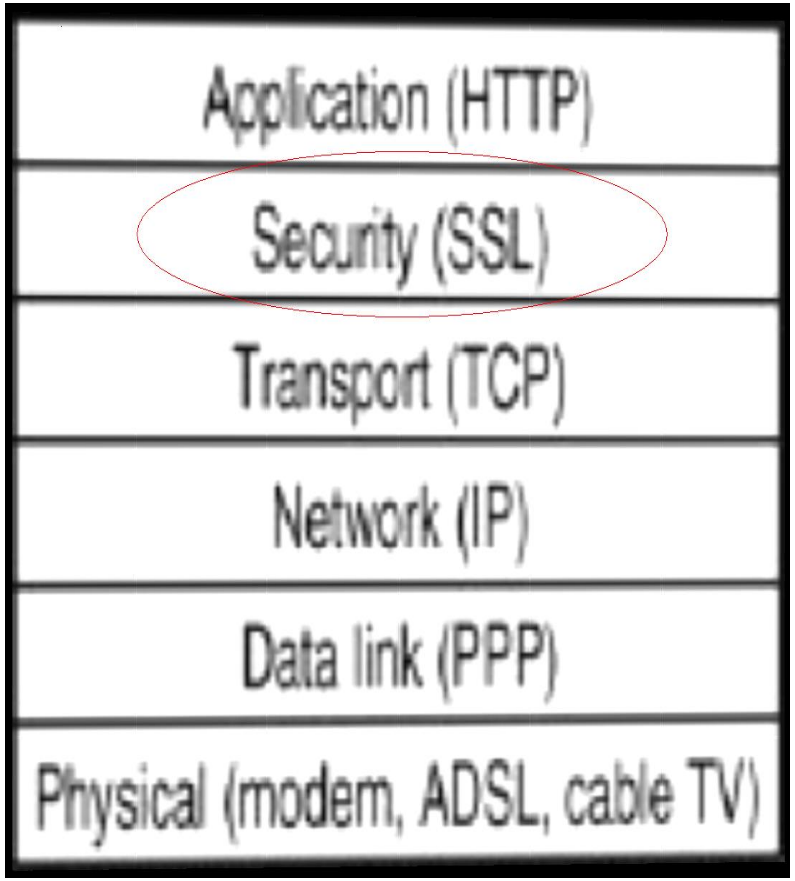
Definition

- HTTPS stands for Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL.

  SSL acts like a sub layer under regular HTTP application layering.
- HTTPS encrypts an HTTP message prior to transmission and decrypts a message upon arrival.
- HTTPS by default uses port 443 as opposed to the standard HTTP port of 80.

- URL's beginning with HTTPS indicate that the connection between client and browser is encrypted using SSL

  e.g.: https://login.yahoo.com/config/login_verify2?&.src=ym



Application (HTTP)

Security (SSL)

Transport (TCP)

Network (IP)

Data link (PPP)

Physical (modem, ADSL, cable TV)

SSL: Secure Socket Layer

- **Secure Sockets Layer** (**SSL**), are cryptographic protocols that provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers.
- URL pattern – https://
- For HTTPS, normally use port 443.
- Need SSL if…
    - you have an online store or accept online orders and credit cards
    - you offer a login or sign in on your site
    - you process sensitive data such as address, birth date, license, or ID numbers
    - you need to comply with privacy and security requirements

DHCP : Dynamic Host Configuration Protocol

- Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.
- With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.