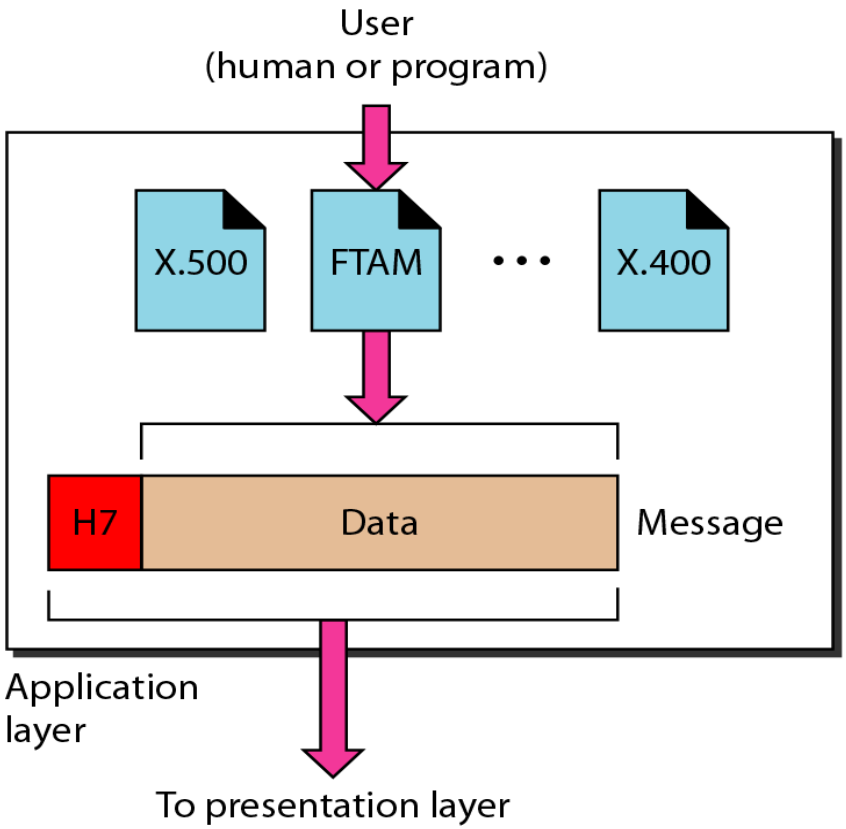
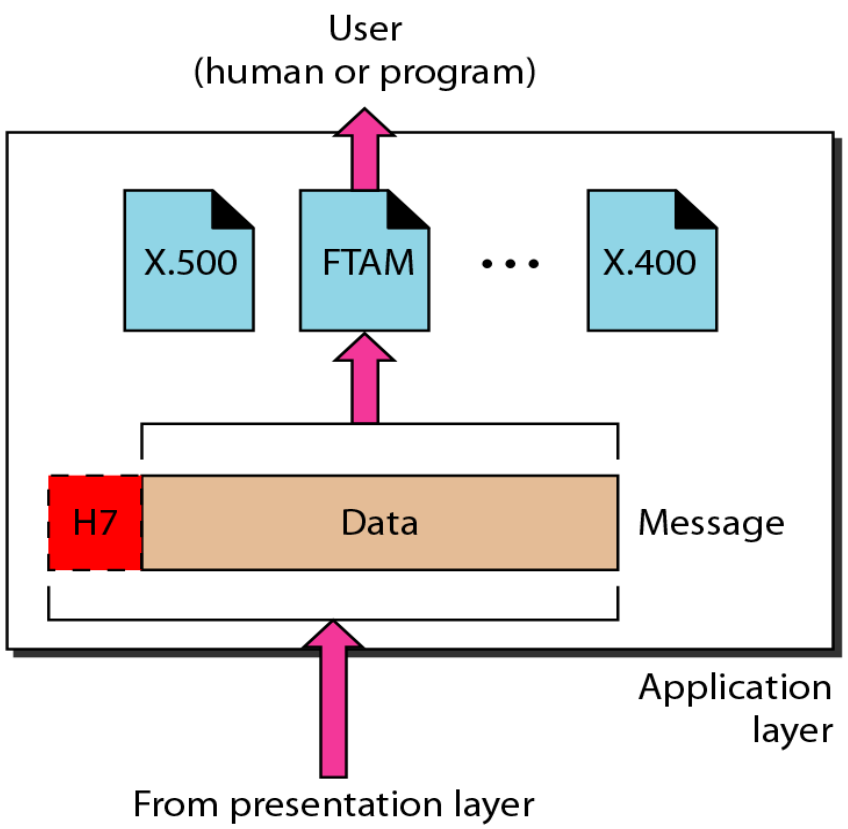
- **Unit- 6**

- **Application Layer**

- *Application layer*

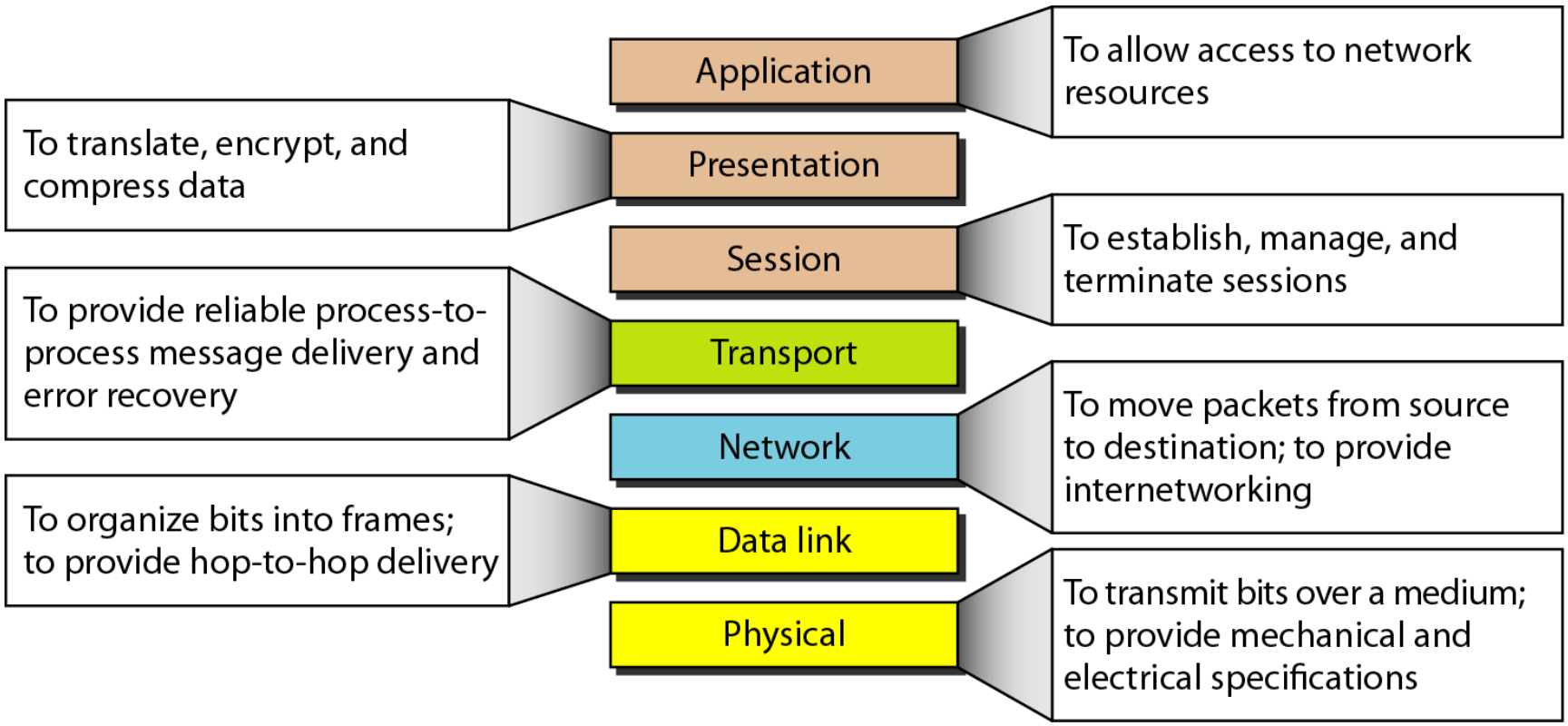




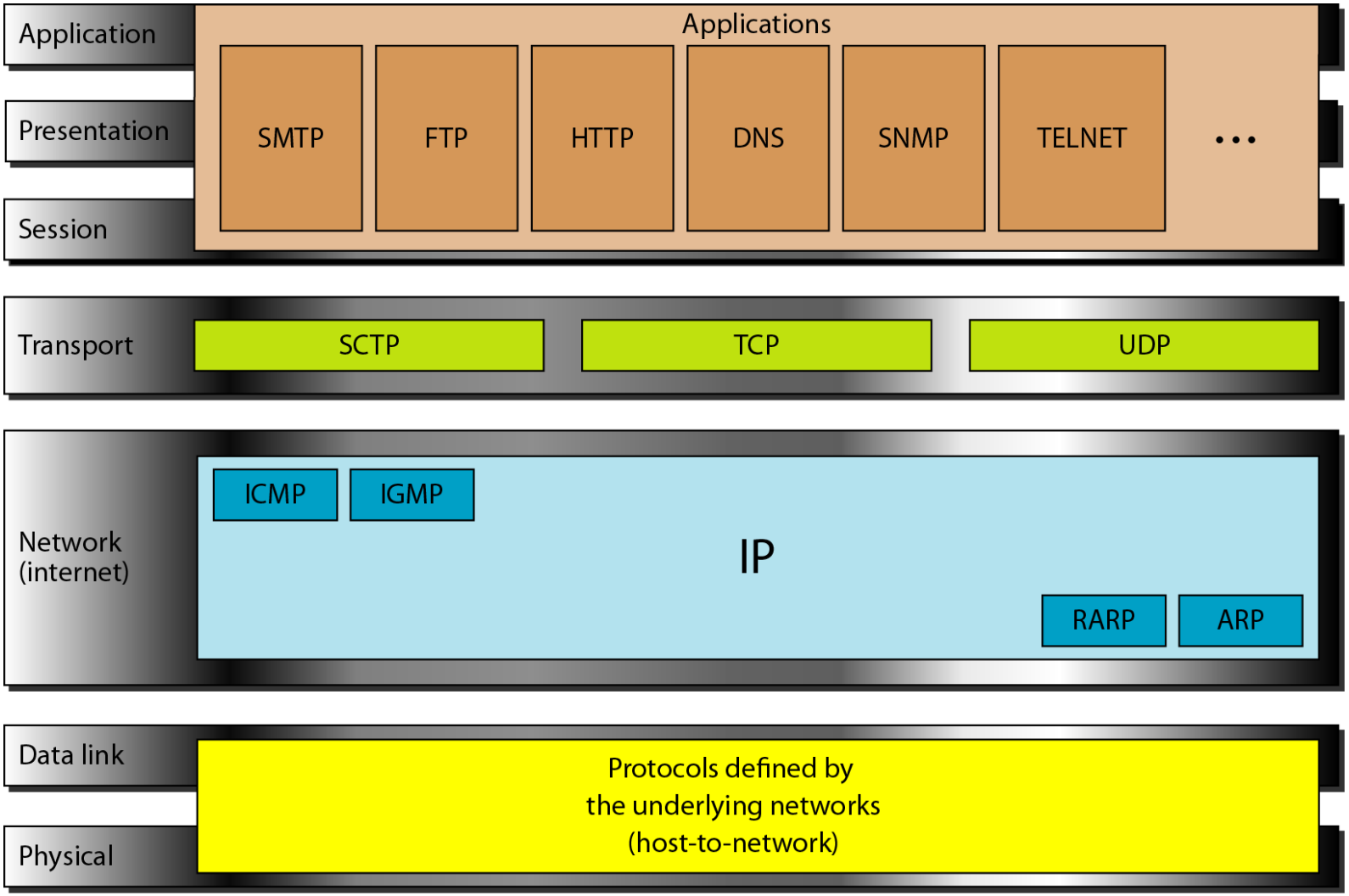
- *Note*

The application layer is responsible for providing services to the user.

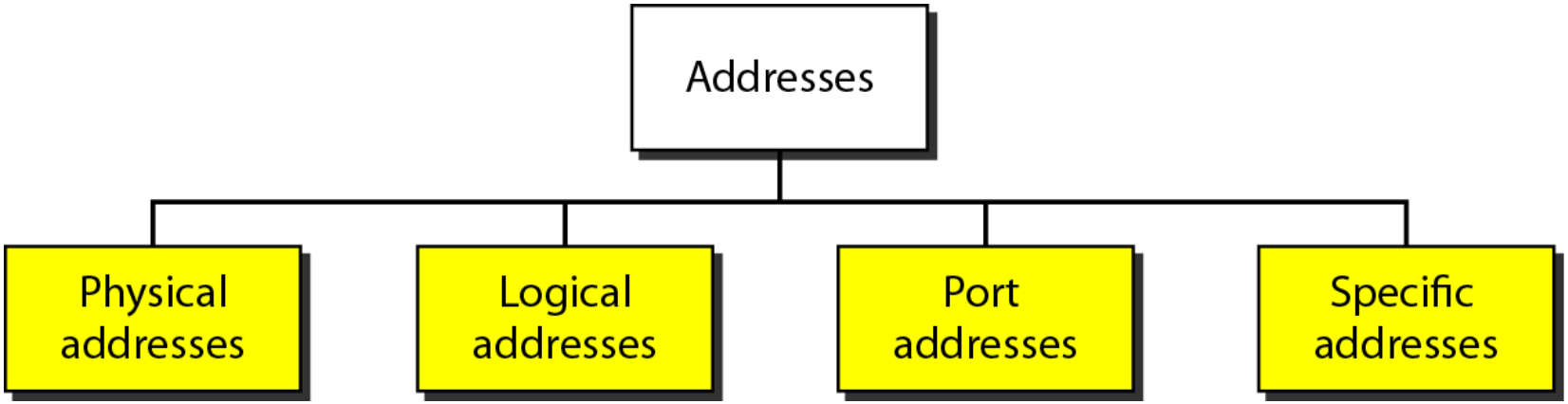
- Fig. *Summary of layers*



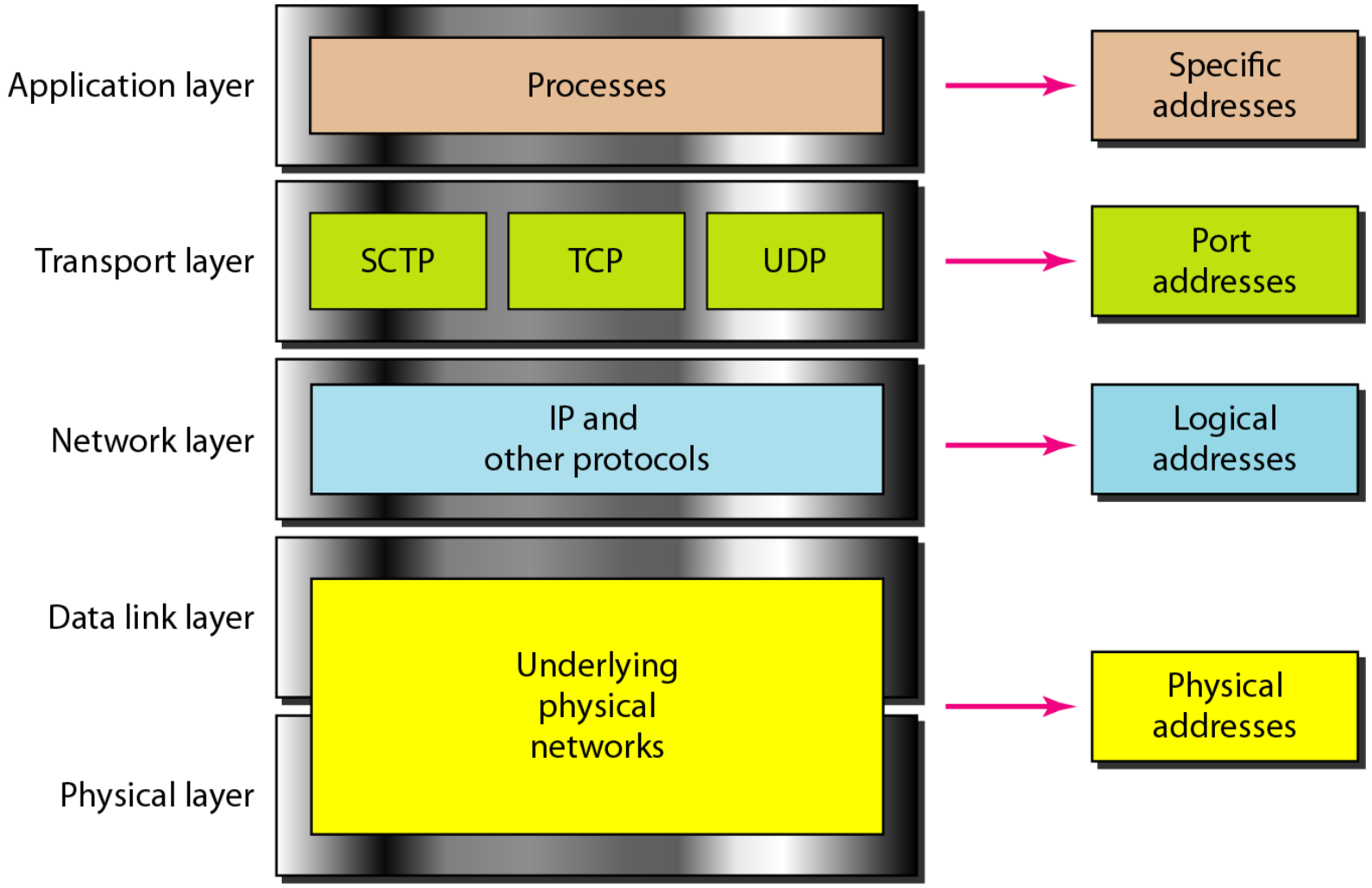
- Fig. *TCP/IP and OSI model*



- Fig. *Addresses in TCP/IP*



- Fig. *Relationship of layers and addresses in TCP/IP*



Network Architecture:

- Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data.

- Simply we can say that how computers are organized and how tasks are allocated to the computer.

- Two of the most widely used types of network architecture are:

1. Peer-to-Peer architecture

2. Client/Server architecture

1. Peer-to-Peer architecture (P2P architecture):

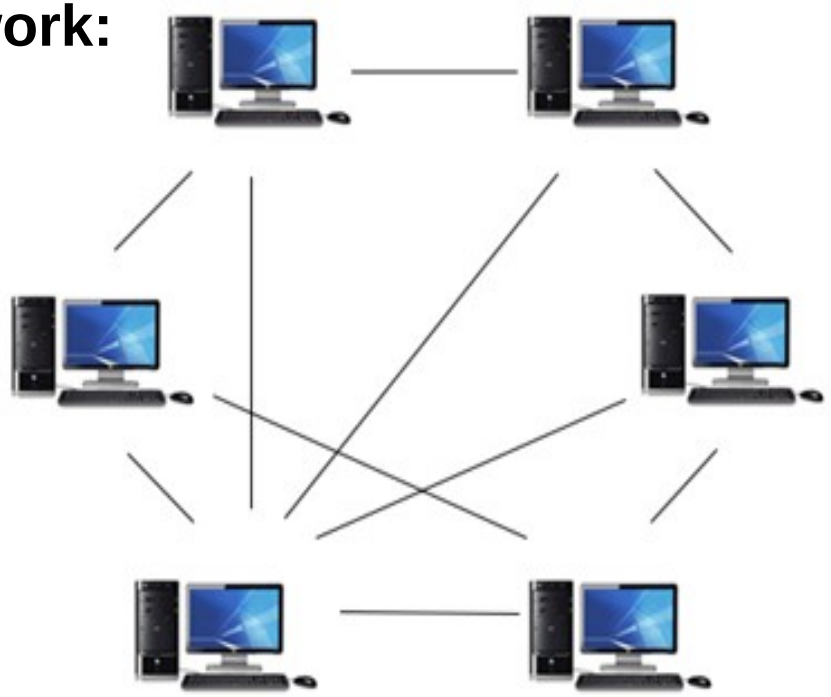
- It is a commonly used computer networking architecture in which each workstation, or node, has the same capabilities and responsibilities.

- Peer-To-Peer network is useful for small environments, usually up to 10 computers.

- Peer-To-Peer network has no dedicated server.

- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.

Advantages Of Peer-To-Peer Network:



- It is less costly as it does not contain any dedicated server.

- If one computer stops working but, other computers will not stop working.

- It is easy to set up and maintain as each computer manages itself.

Disadvantages Of Peer-To-Peer Network:

- In the case of Peer-To-Peer network, it does not contain the centralized system . Therefore, it cannot back up the data as the data is different in different locations.

- It has a security issue as the device is managed itself.

2. Client/Server Architecture:

- It is a network model designed for the end users i.e clients, to access the resources such as songs, video, etc. from a central computer i.e. Server.

-The central controller is known as a server while all other computers in the network are called clients.

- A server performs all the major operations such as security and network management.

- A server is responsible for managing all the resources such as files, directories, printer, etc.

- All the clients communicate with each other through a server.

- Eg., if client 1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.

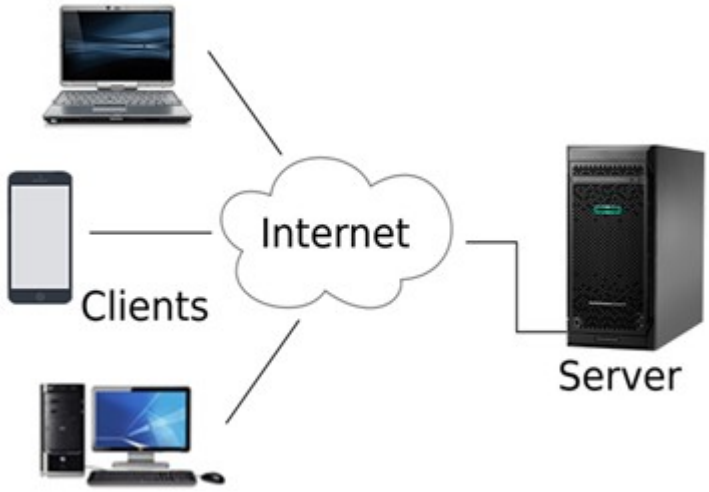
Advantages Of Client/Server network:

- It contains the centralized system. Therefore we can back up the data easily.

- It has a dedicated server that improves the overall performance of the whole system.

- Security is better in Client/Server network as a single server administers the shared resources.

- It also increases the speed of the sharing resources.



Disadvantages Of Client/Server network:

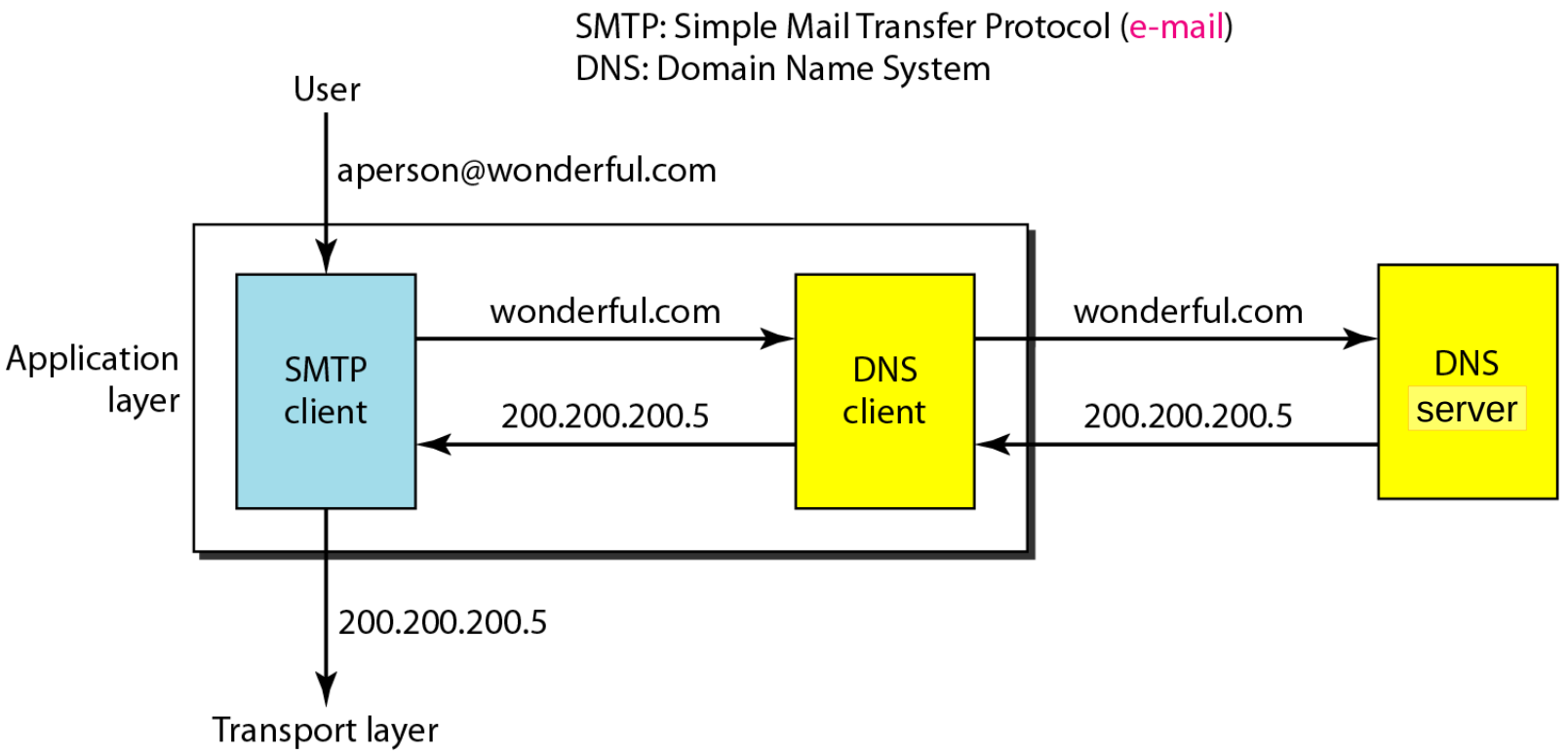
- It is expensive as it requires the server with large memory.

- A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.

- It requires a dedicated network administrator to manage all the resources.

- Domain Name System

- Figure *Example of using the DNS service*



• 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.*

It is organized into 2 ways:

- Flat Name Space:

- - Name is assigned to an address.
- - The name in this space is a sequence of characters without
- structure.

- Disadvantage:

- - It cannot be used in a Internet because it must be centrally
- controlled to avoid ambiguity and duplication.

- Hierarchical Name Space

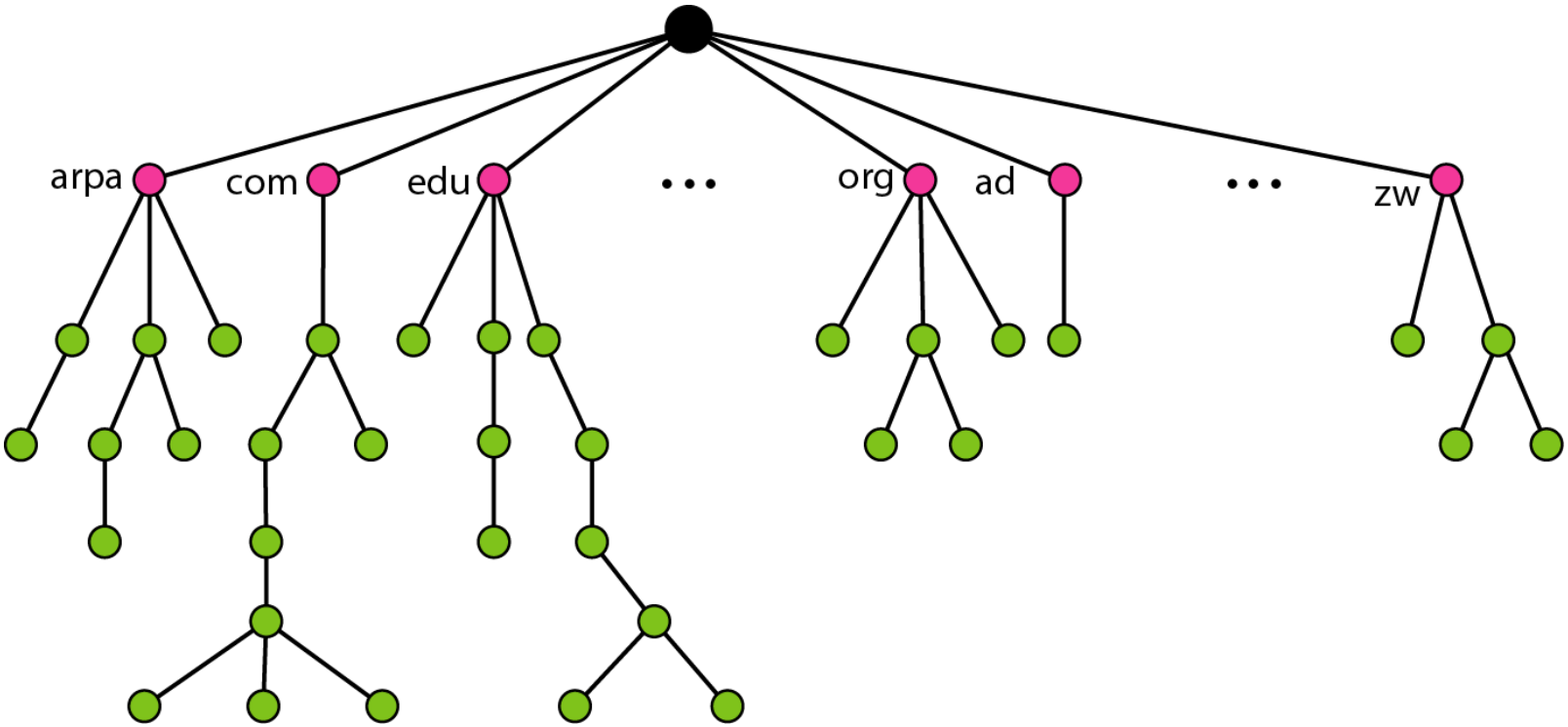
- - Name is made of several parts.
- - 1st part define nature of organization.
- - 2nd part define name of organization.
- - 3rd part define department of organization
  - and so on.
- - Central authority assign the part of the name that nature of organization and the name of the organization.

• DOMAIN NAME SPACE

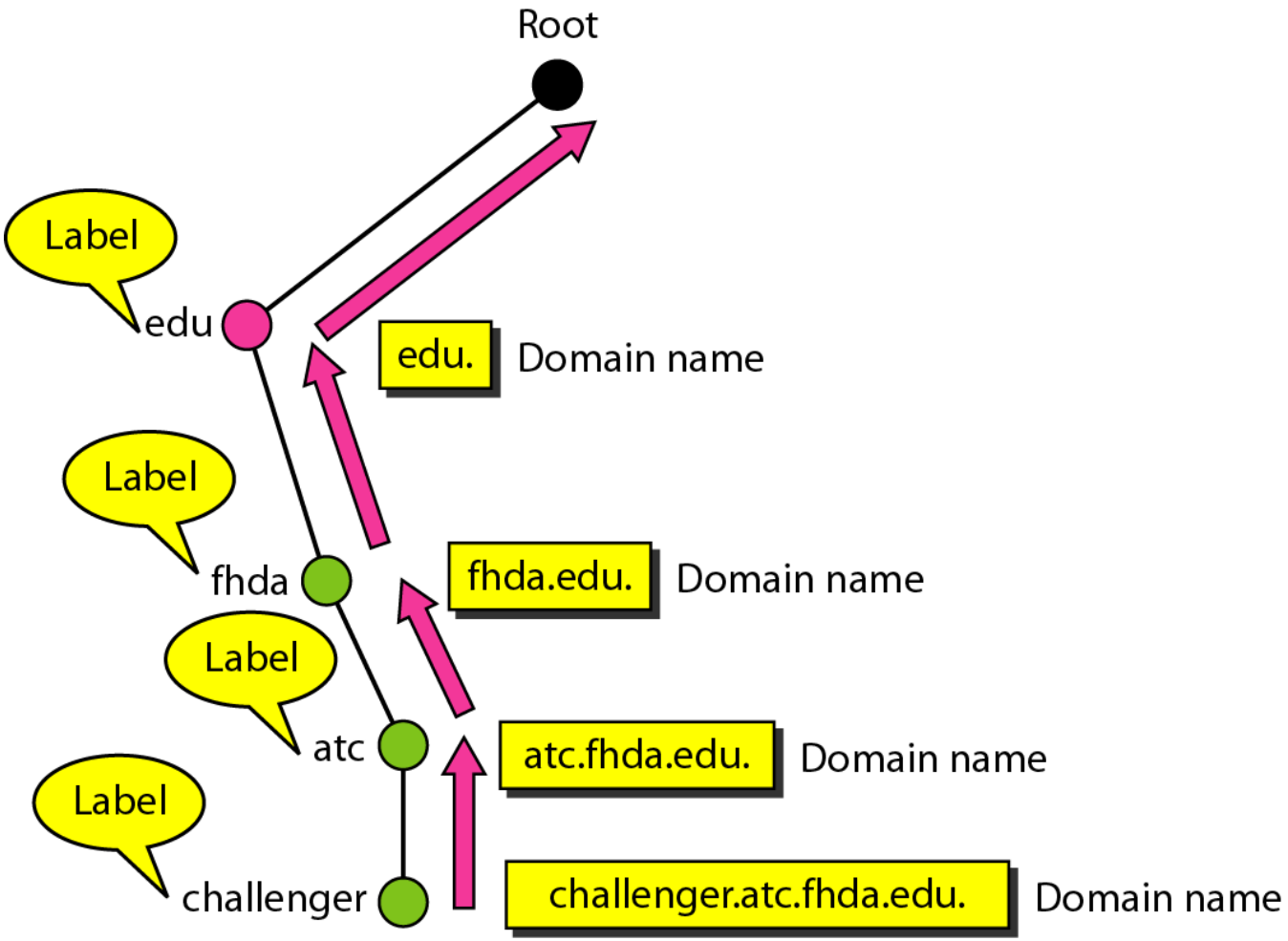
- *To have a hierarchical name space, a domain name space was designed. In this design the names are defined in an inverted-tree structure with the root at the top. The tree can have only 128 levels: level 0 (root) to level 127.*

Label
Domain Name
Domain

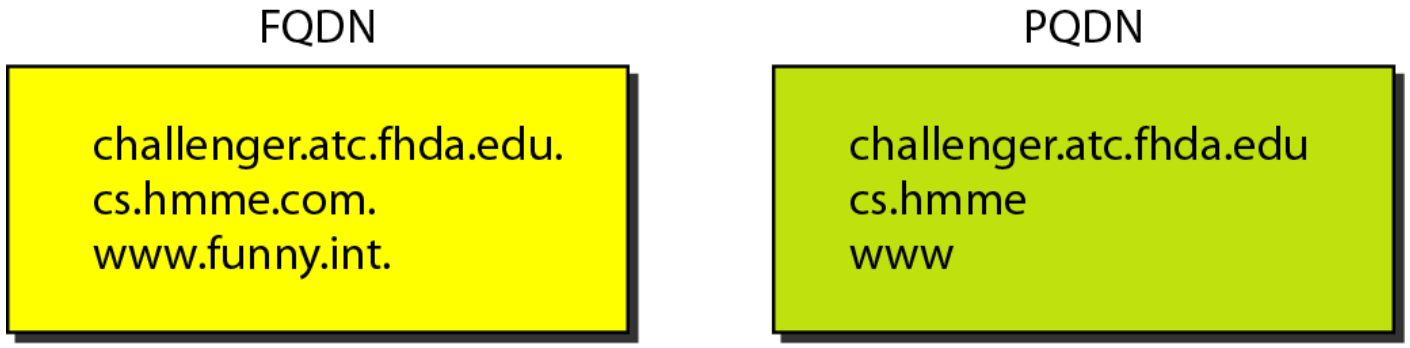
- Figure *Domain name space*



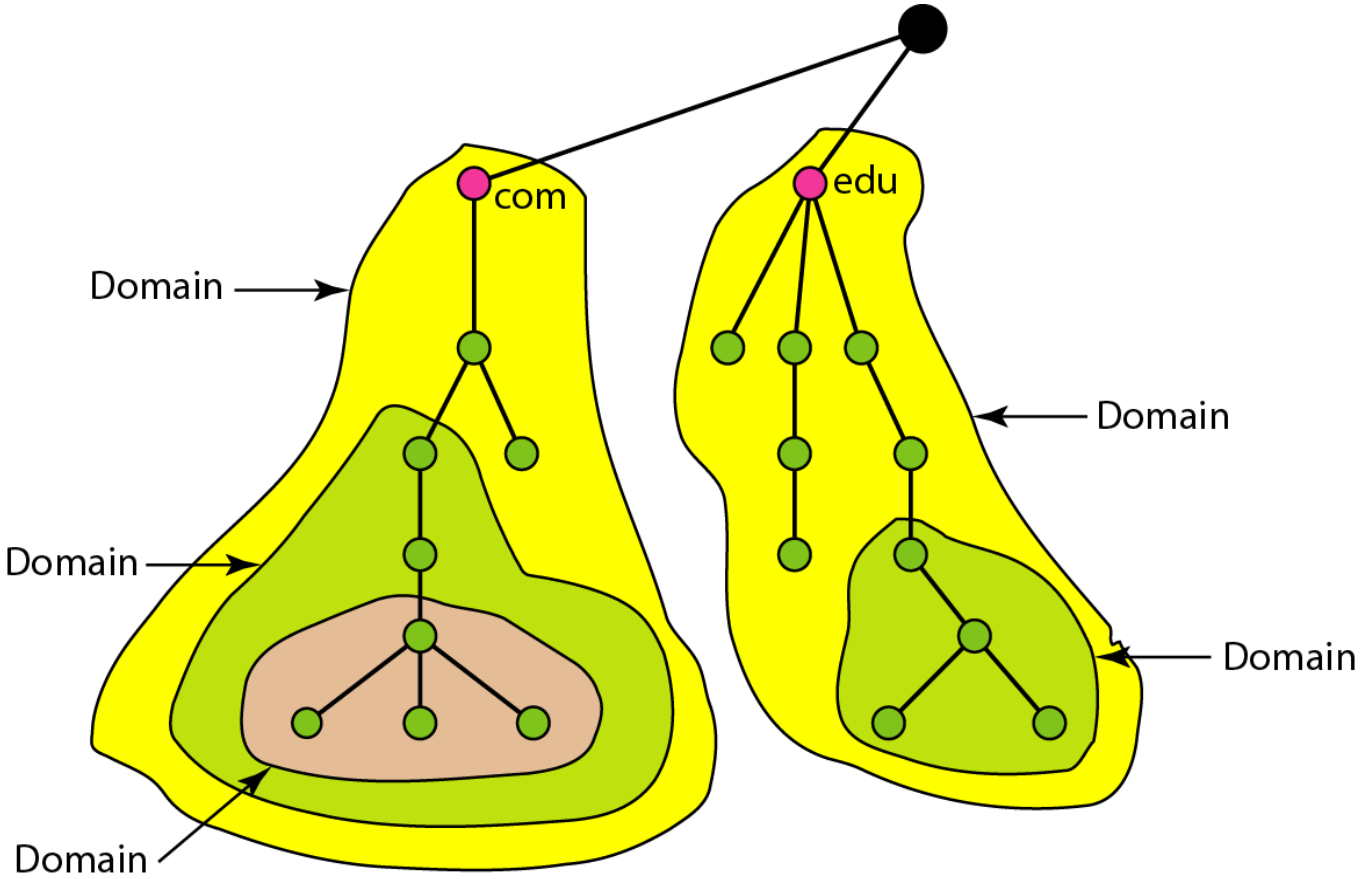
- Figure *Domain names and labels*



- Figure *FQDN and PQDN*



- Figure *Domains*

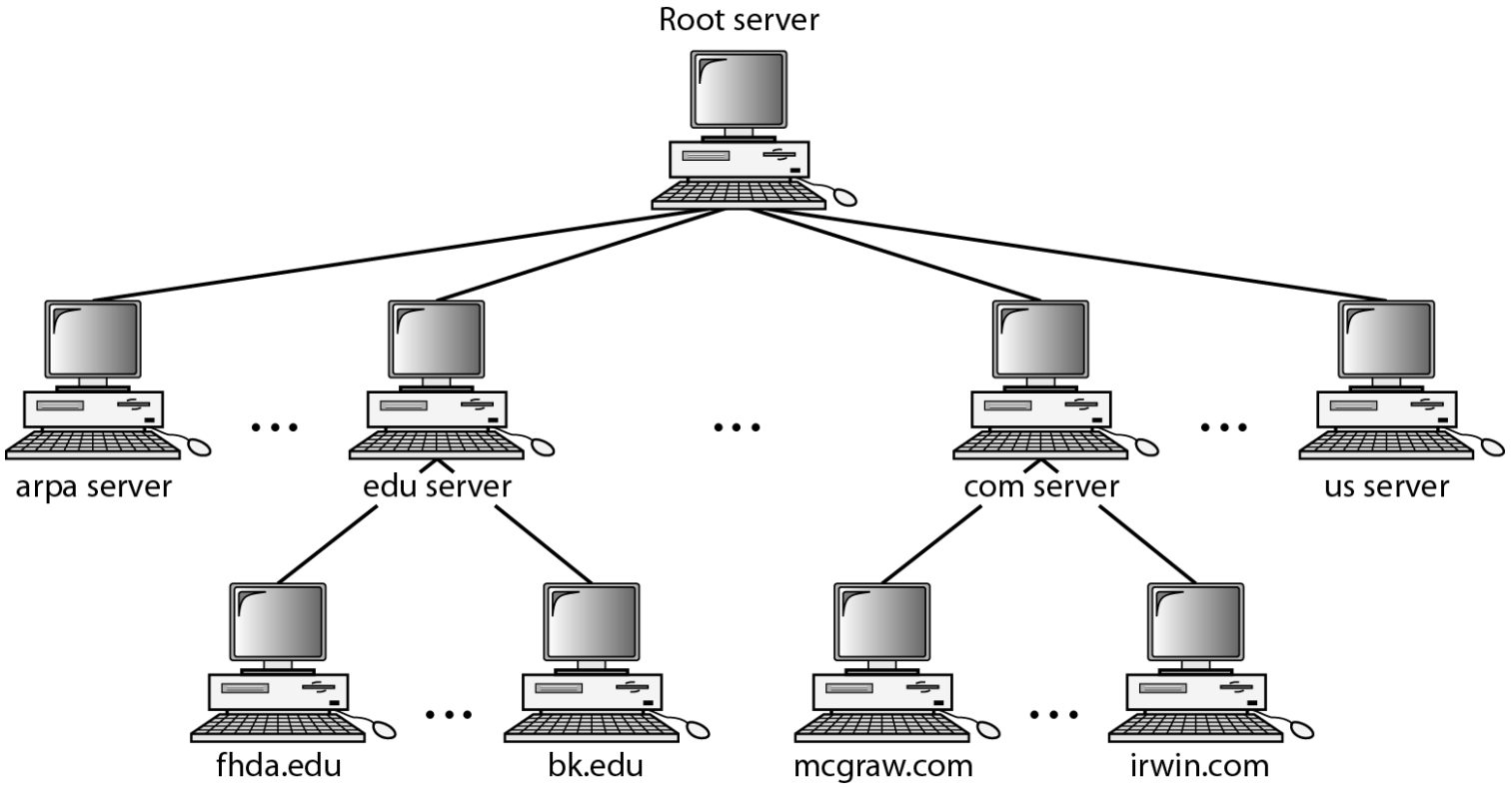


• DISTRIBUTION OF NAME SPACE

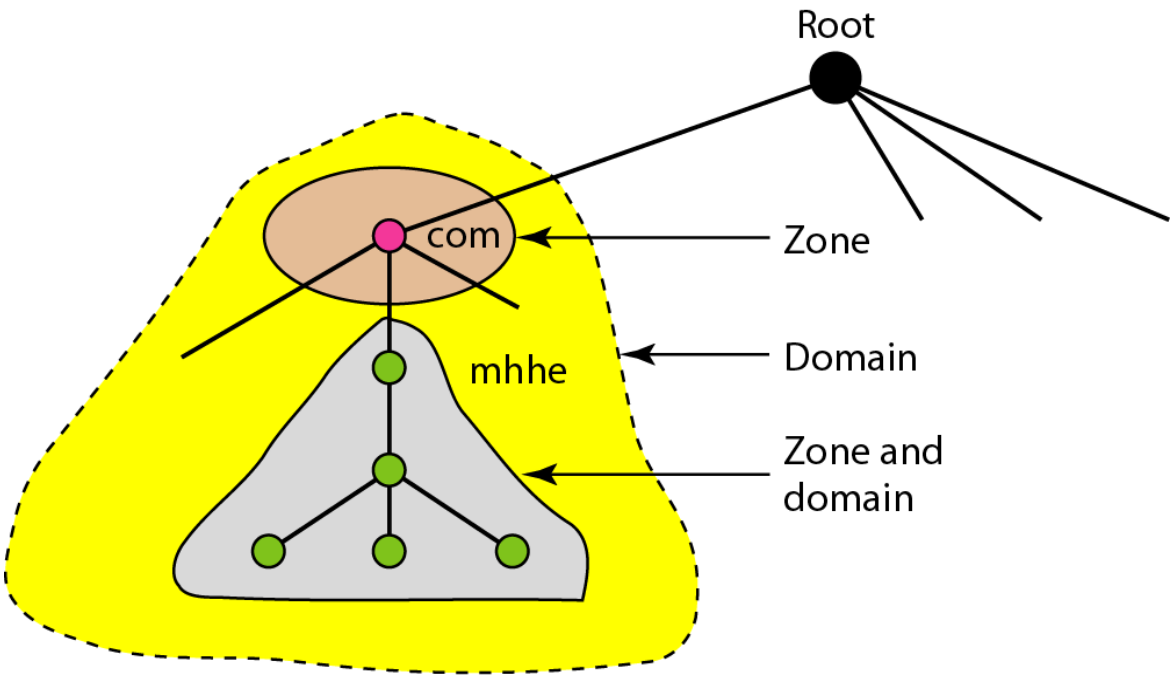
- *The information contained in the domain name space must be stored. However, it is very inefficient and also unreliable to have just one computer store such a huge amount of information.*

- Hierarchy of Name Servers
- Zone
- Root Server
- Primary and Secondary Servers

- Figure. *Hierarchy of name servers*



- Figure. *Zones and domains*



• *Note*

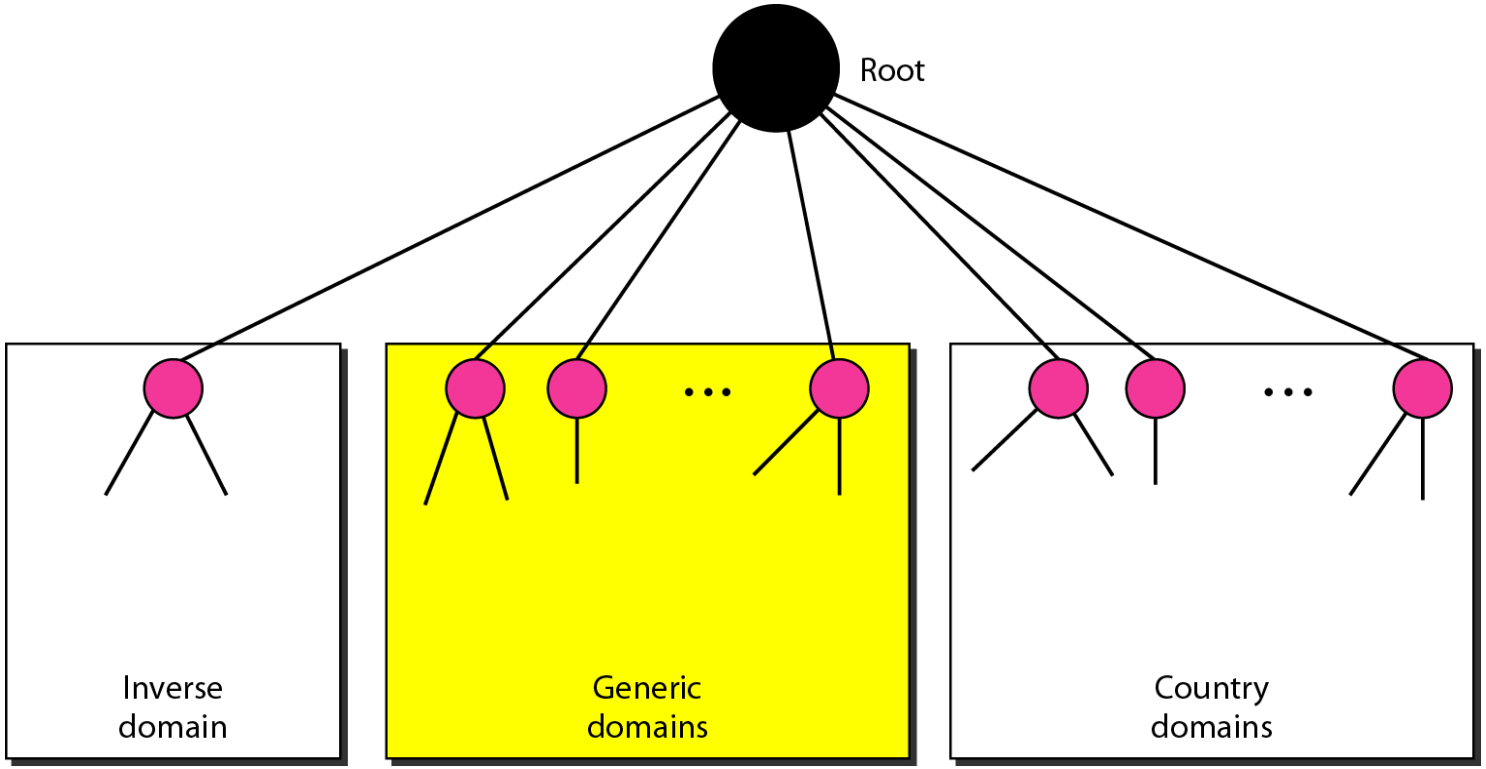
- A primary server loads all information from the disk file, it is responsible for creating, maintaining and updating the zone file.
-
- The secondary server loads all information from the primary server.
- When the secondary downloads information from the primary, it is called zone transfer.

• DNS IN THE INTERNET

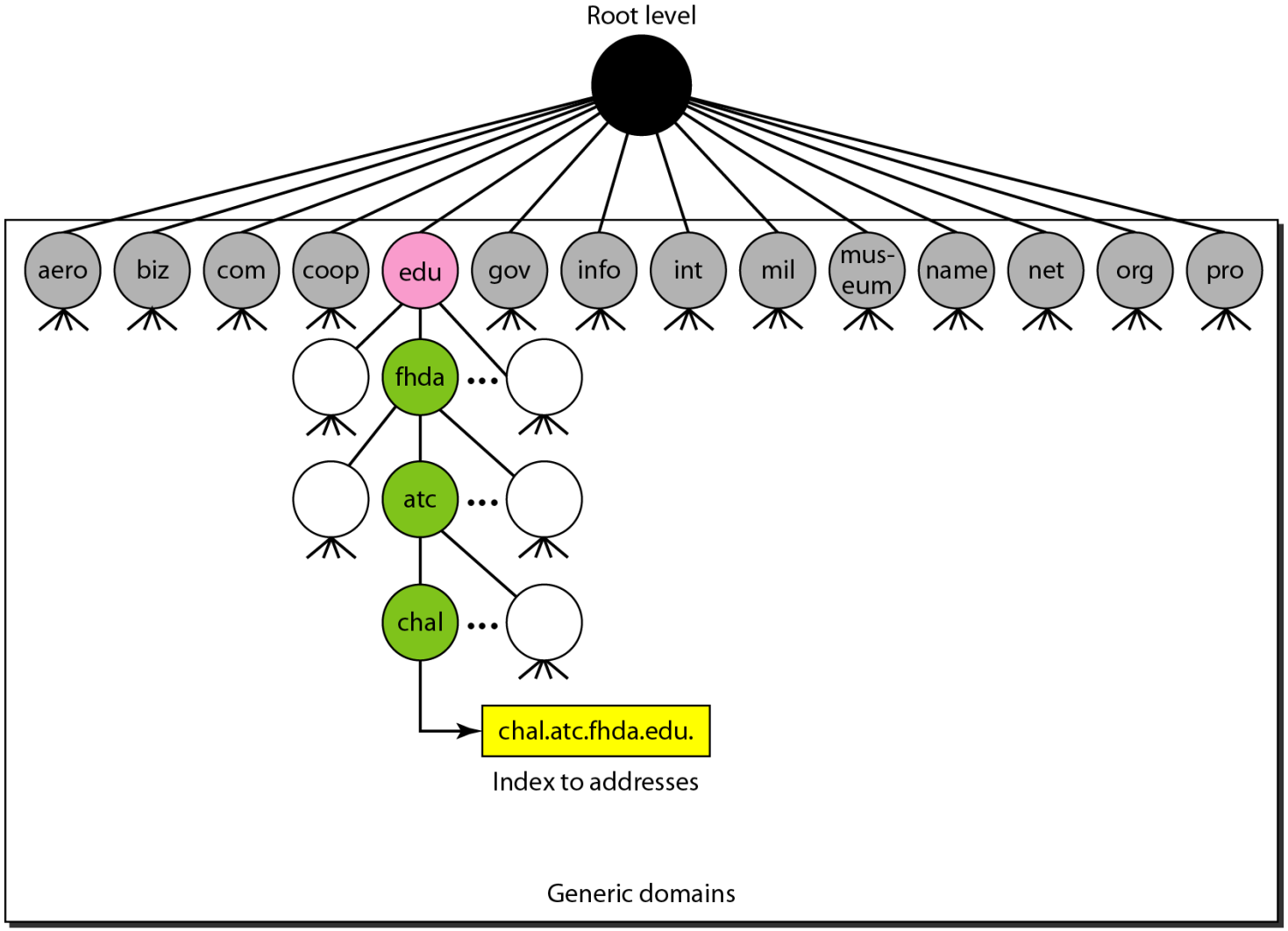
- *DNS is a protocol that can be used in different platforms. In the Internet, the domain name space (tree) is divided into three different sections: generic domains, country domains, and the inverse domain.*

- Generic Domain:
- It defines registered host according to their behavior.
- Country Domain:
- It section uses 2 character country abbreviations and second labels Can bé organizational or national désignations.
- Inverse Domain:
- It is used to map an address to a name.
- Servers has list of client with IP address.
- Server ask to its Resolver to send a query to the DNS server to map an address to a name in its list.

- *DNS IN THE INTERNET*



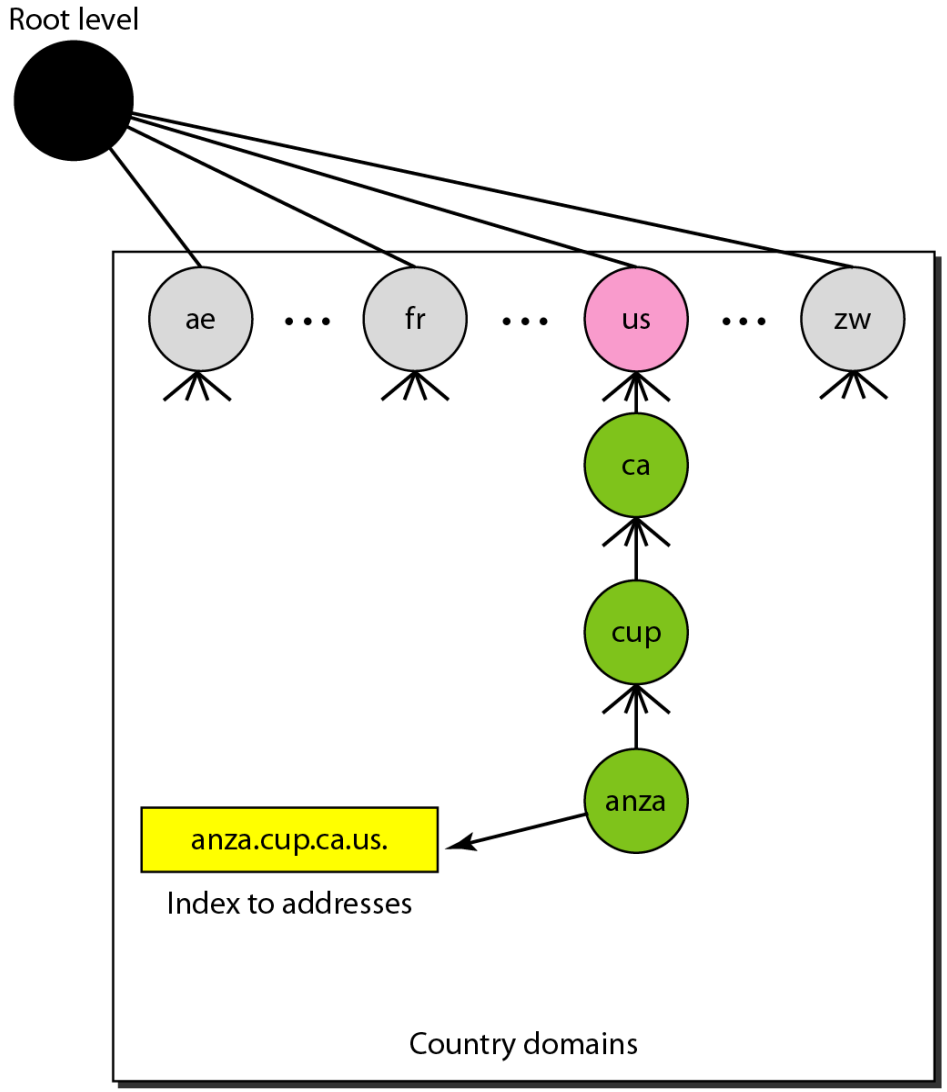
- *Generic domains*



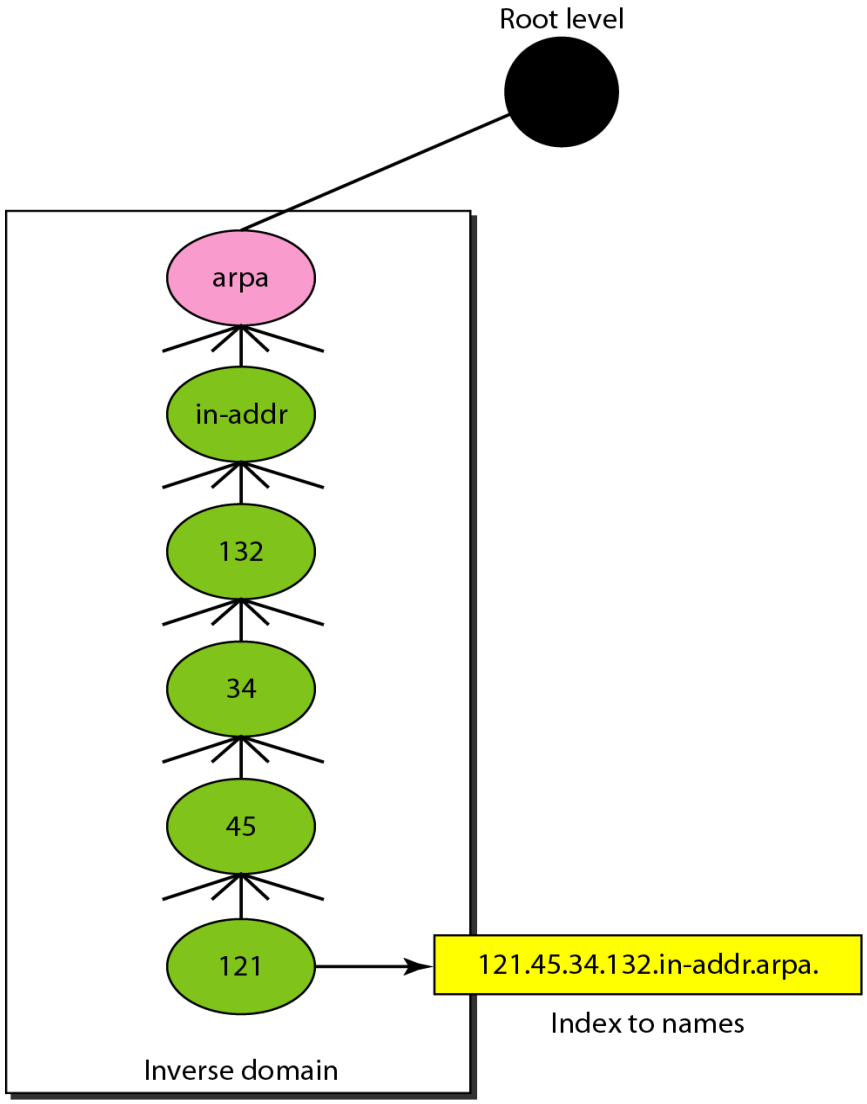
- *Generic domain labels*

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*



- *Inverse domain*

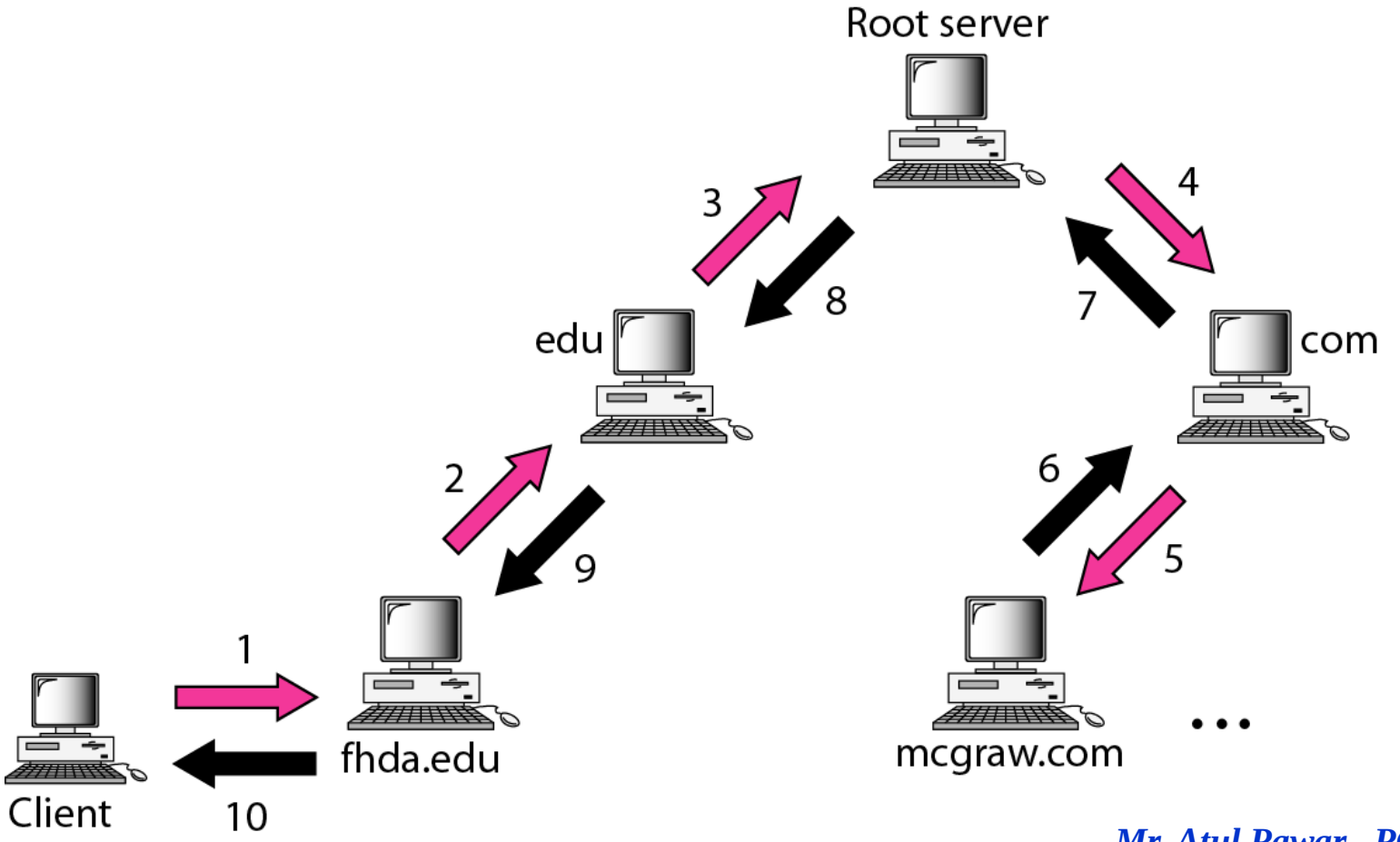


• RESOLUTION

- *Mapping a name to an address or an address to a name is called name-address resolution.*
- Resolver:
- A host that needs to map an address to a name or a name to an address calls a DNS client called a resolver.
- Mapping Names to Addresses:
- Resolver gives a domain name to the server and ask for the corresponding address. Server checks Country and Generic domain for mapping.
- Mapping Addresses to Names:
- Client send IP address for mapping a domain name.
- It use the Inverse domain.
- The resolver first invers IP address and then adds the two
- labels before sending.
- Eg.: Resolver recieves IP 132.34.45.121
- After inversion and adding labels 121.45.34.132.in-addr.arpa

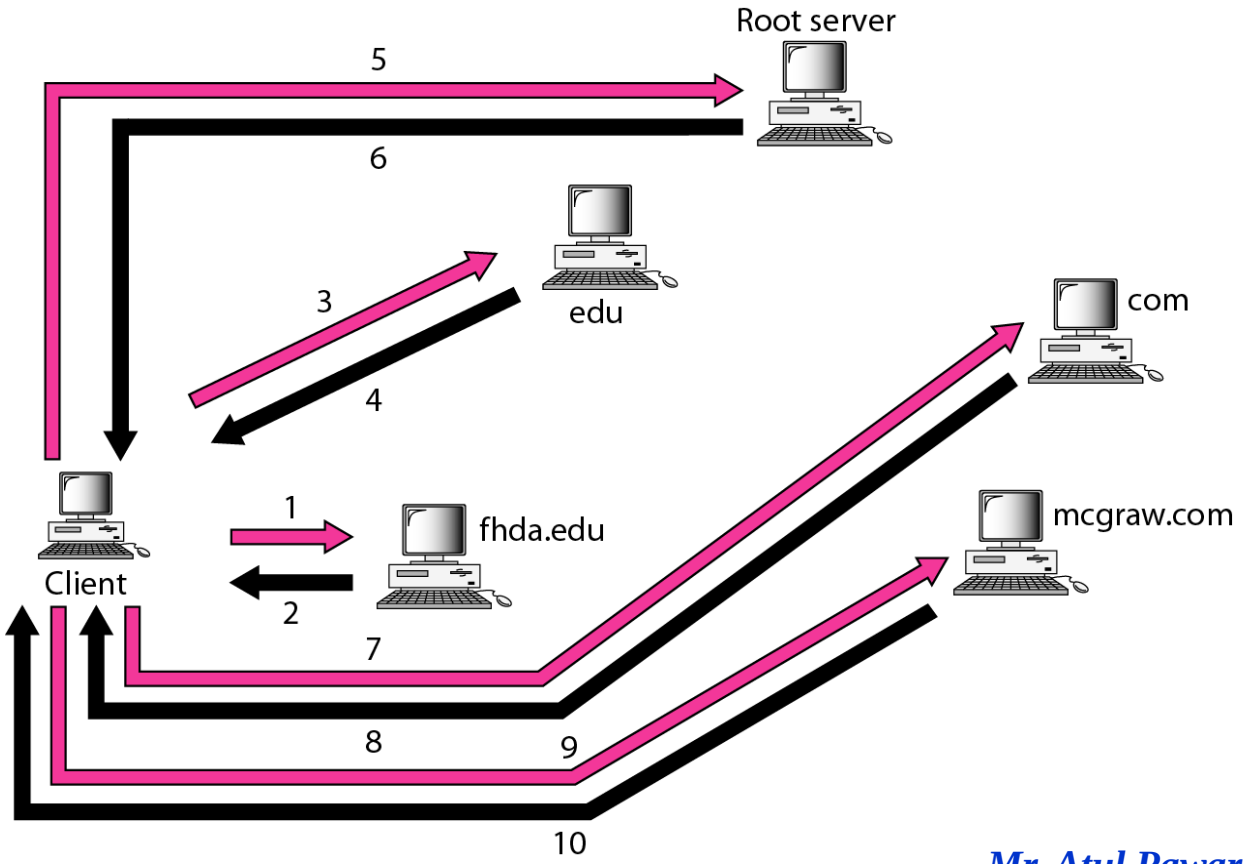
• Recursive Resolution

- Client (Resolver) send query to server, it checks
- Database and respond. If he do not have that domain name then he forward query to another server and so on.



Iterative Resolution

- Client repeats the same query to multiple server.
- If server do not have Domain name, it returns
- the IP address of the server that it thinks can
- resolve the query.



Caching

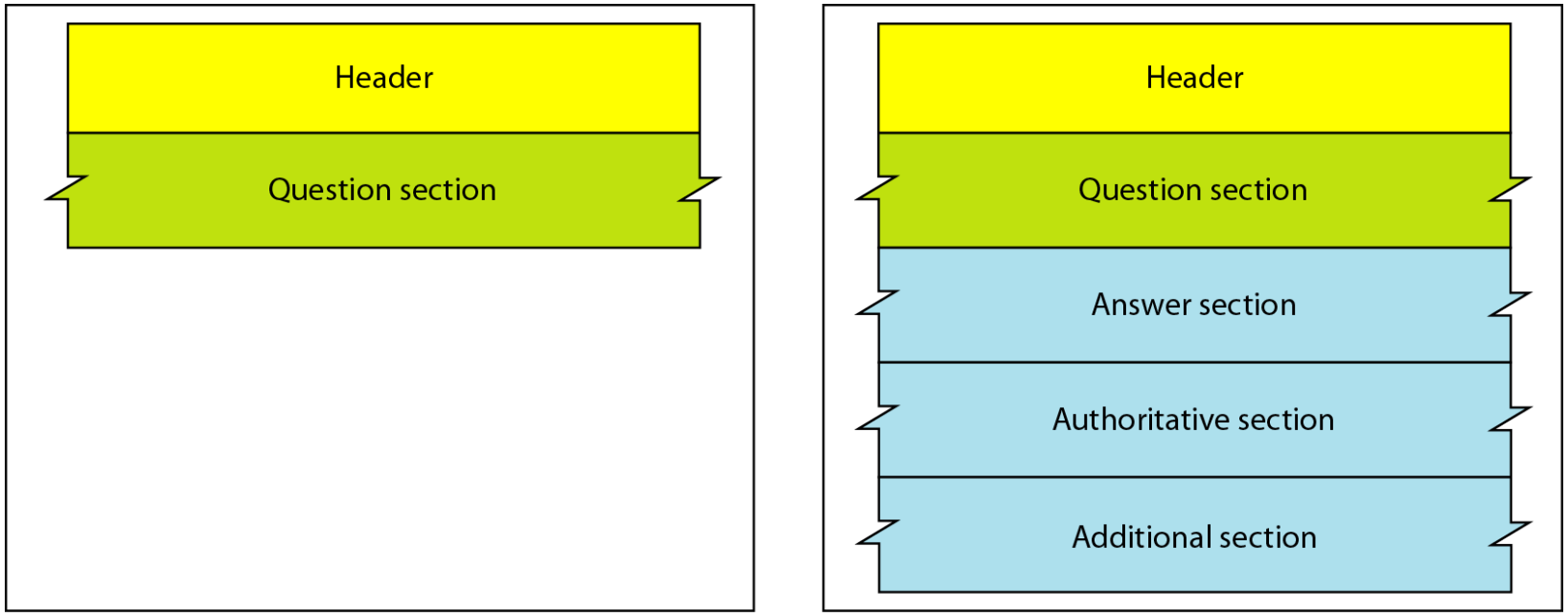
- When a server ask for a mapping from another server and receives the response, it stores this information in its cache memory before sending it to the client.
- Caching speed up resolution.

- Disadvantage:
  - Long term cache send outdated mapping to the client.
  - Time To Live (TTL) is used to overcome this problem.

• DNS MESSAGES

- *DNS has two types of messages: query and response. Both types have the same format. The query message consists of a header and question records; the response message consists of a header, question records, answer records, authoritative records, and additional records.*

- Figure. *Query and response messages*



a. Query

b. Response

• Header:

- Both Query and Response messages have the
- same header format of size 12 bytes.

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)

TYPES OF RECORDS

- *Two types of records are used in DNS. The question records are used in the question section of the query and response messages. The resource records are used in the answer, authoritative, and additional information sections of the response message.*

- Question Record
- Resource Record

• REGISTRARS

- *How are new domains added to DNS? This is done through a registrar, a commercial entity accredited by ICANN (Internet Corporation for Assign Names and Numbers). A registrar first verifies that the requested domain name is unique and then enters it into the DNS database. A fee is charged.*

- *http://www.intenic.net*

• ENCAPSULATION

- *DNS can use either UDP or TCP. In both cases the well-known port used by the server is port 53.*
- *UDP is used when the size of the response message is less than 512 bytes because most UDP packages have a 512-byte packet size limit.*
- *If the size of the response message is more than 512 bytes, a TCP connection is used.*

- *Note*

- DNS can use the services of UDP or TCP using the well-known port 53.

• 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.
- RTT (Round Trip Time) contains different delays.
- HTTP uses the services of TCP on well-known port 80.
- Non-Persistent Connections:
- Client Server configuration required.
- Disadvantages:
- New connection required for each request.
- Each object suffers a delivery delay of 2 RTT's, 1 RTT to
- TCP connection and 1 RTT to request and receive an object.

Persistent Connections:

It is a default mode for HTTP

TCP connection is open after a response.

2 versions of Persistence Connections:

Without Pipelining:

Client issues new request only when the previous response has been received.

Disadvantage:

Server become idle after response object.

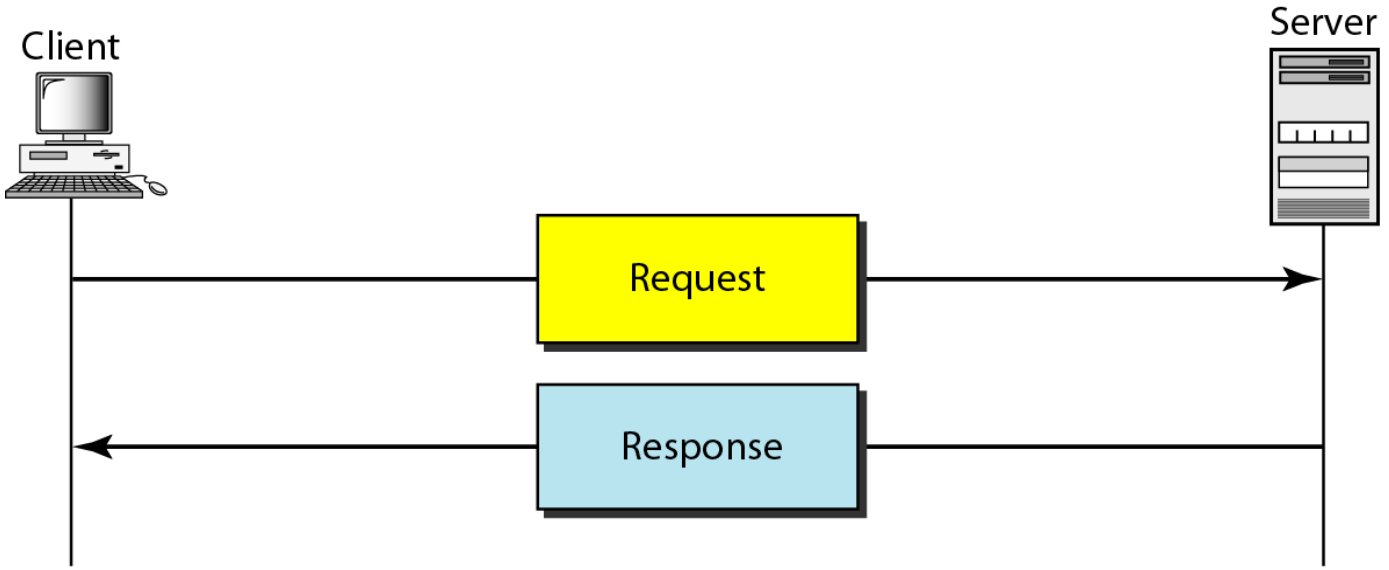
2) With Pipelining:

Default mode of HTTP.

Client make back-to-back request for objects.

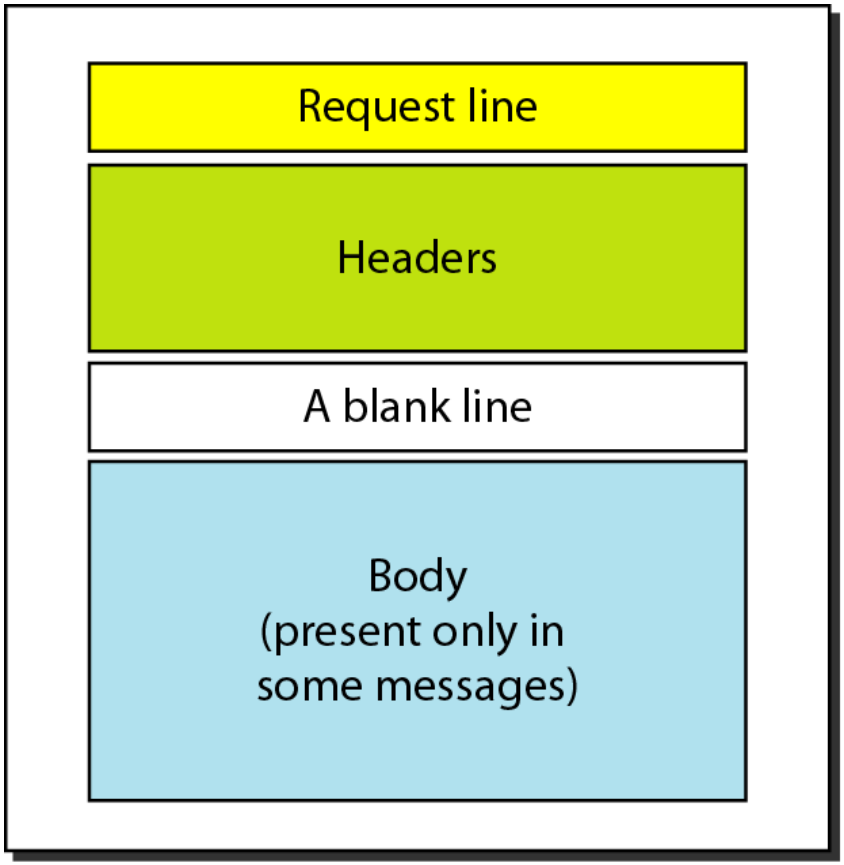
Server sends objects back-to-back.

- Fig. *HTTP transaction*

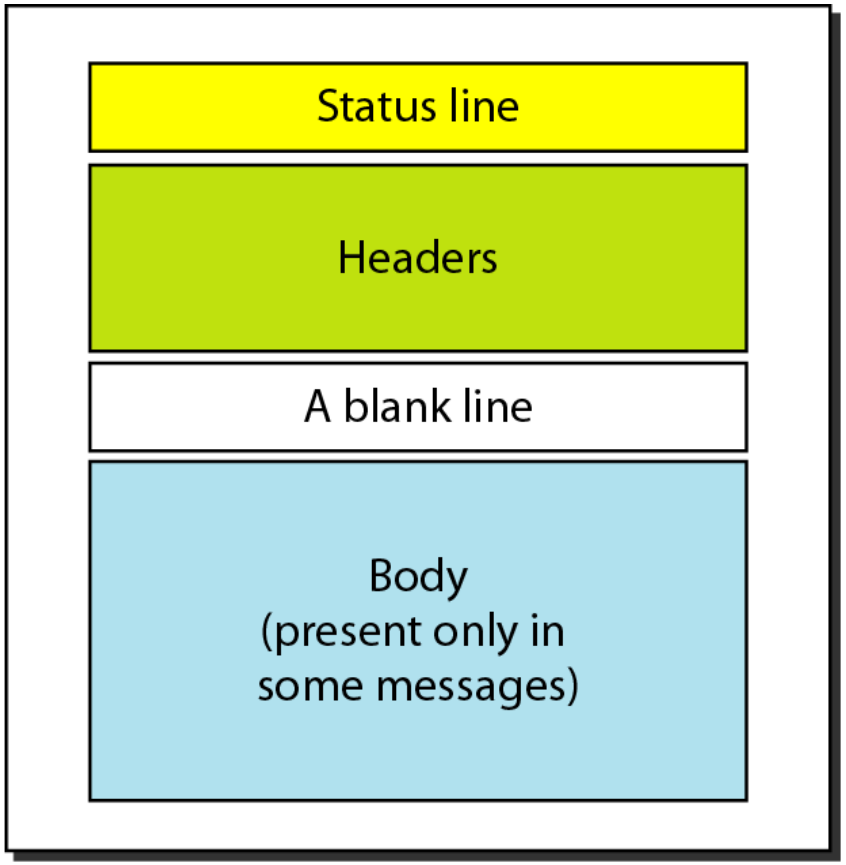


HTTP is a stateless protocol, because the connection between the browser and the server is lost once the transaction ends.

- HTTP Request and response messages

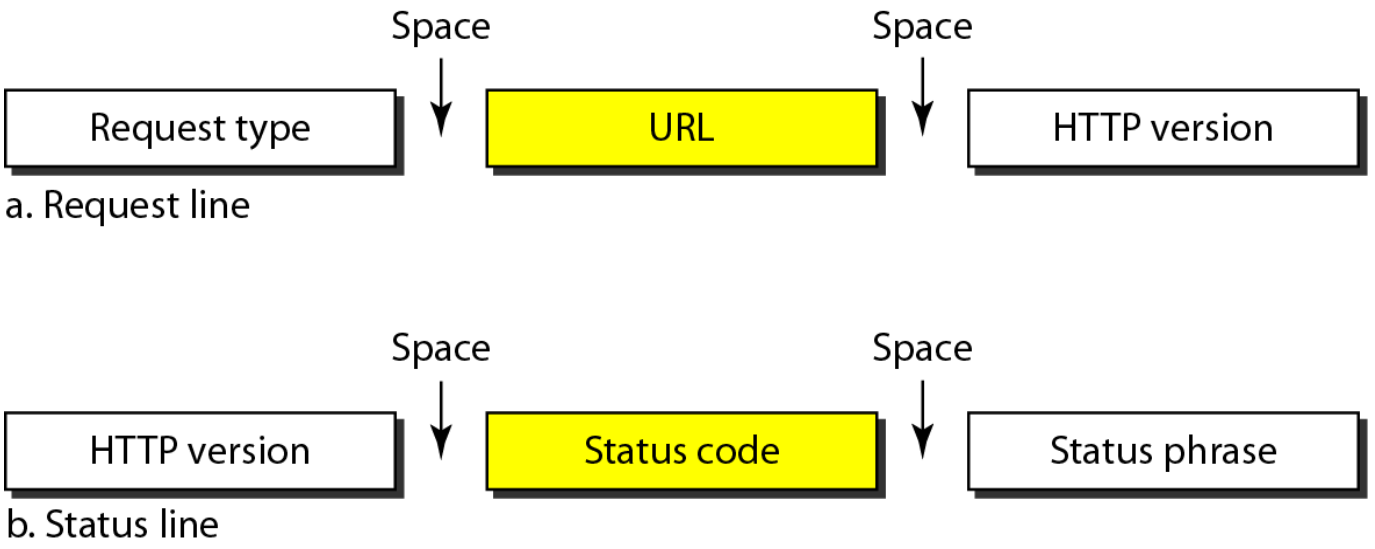


Request message



Response message

- Fig. *Request and status lines*



- Table. Request Type (*Methods)*

Method	*Action*
GET	Requests a document from the server
HEAD	Requests information about a document but not the document itself
POST	Sends some information from the client to the server
PUT	Sends a document from the server to the client
TRACE	Echoes the incoming request
CONNECT	Reserved
OPTION	Inquires about available options

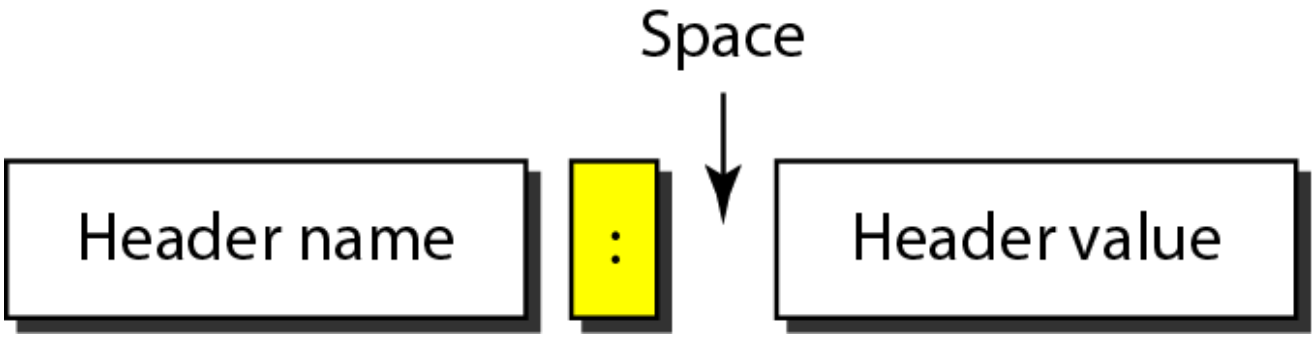
- Table. *Status codes*

Code	*Phrase*	*Description*
	Informational	
100	Continue	The initial part of the request has been received, and the client may continue with its request.
101	Switching	The server is complying with a client request to switch protocols defined in the upgrade header.
	Success	
200	OK	The request is successful.
201	Created	A new URL is created.
202	Accepted	The request is accepted, but it is not immediately acted upon.
204	No content	There is no content in the body.

- Table. *Status codes (continued)*

Code	*Phrase*	*Description*
Redirection		
301	Moved permanently	The requested URL is no longer used by the server.
302	Moved temporarily	The requested URL has moved temporarily.
304	Not modified	The document has not been modified.
Client Error		
400	Bad request	There is a syntax error in the request.
401	Unauthorized	The request lacks proper authorization.
403	Forbidden	Service is denied.
404	Not found	The document is not found.
405	Method not allowed	The method is not supported in this URL.
406	Not acceptable	The format requested is not acceptable.
Server Error		
500	Internal server error	There is an error, such as a crash, at the server site.
501	Not implemented	The action requested cannot be performed.
503	Service unavailable	The service is temporarily unavailable, but may be requested in the future.

- Fig. *Header format*



- Table. *General headers*

Header	*Description*
Cache-control	Specifies information about caching
Connection	Shows whether the connection should be closed or not
Date	Shows the current date
MIME-version	Shows the MIME version used
Upgrade	Specifies the preferred communication protocol

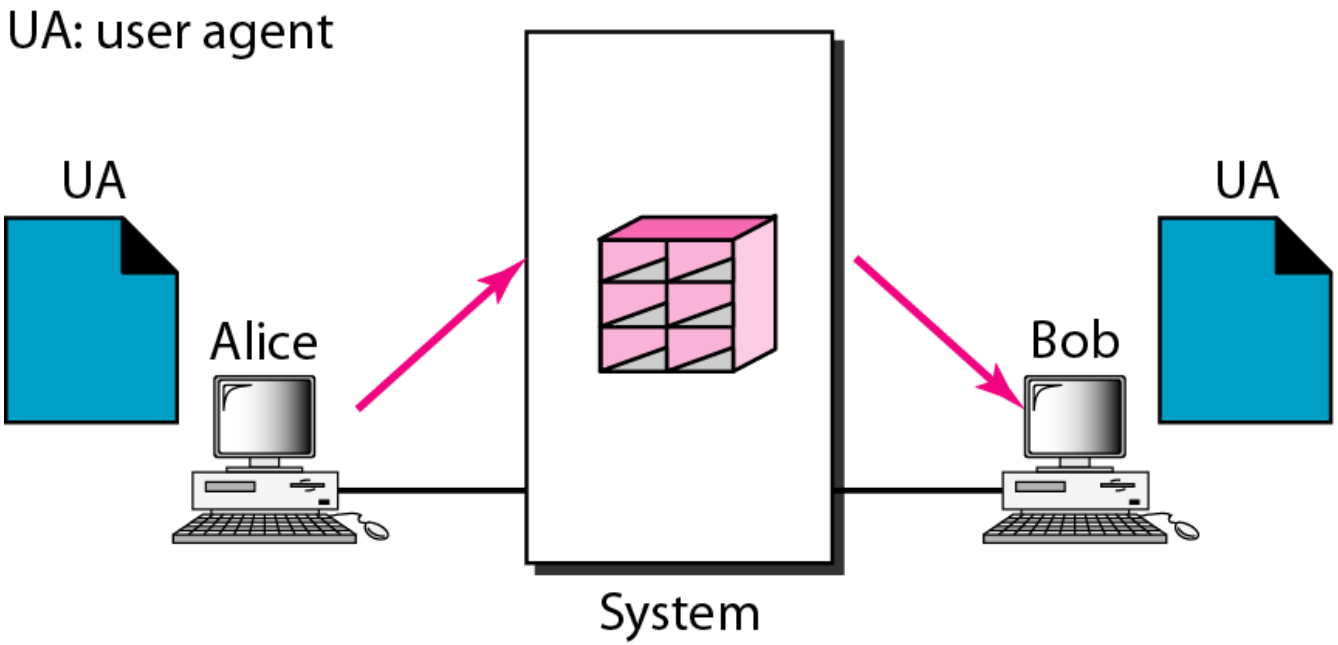
ELECTRONIC MAIL

- ***One of the most popular Internet services is electronic mail (e-mail). The designers of the Internet probably never imagined the popularity of this application program. Its architecture consists of several components that we discuss in this chapter.***

Topics discussed in this section:

Architecture
User Agent
Message Transfer Agent: SMTP
Message Access Agent: POP and IMAP
Web-Based Mail

Figure 26.6 *First scenario in electronic mail*

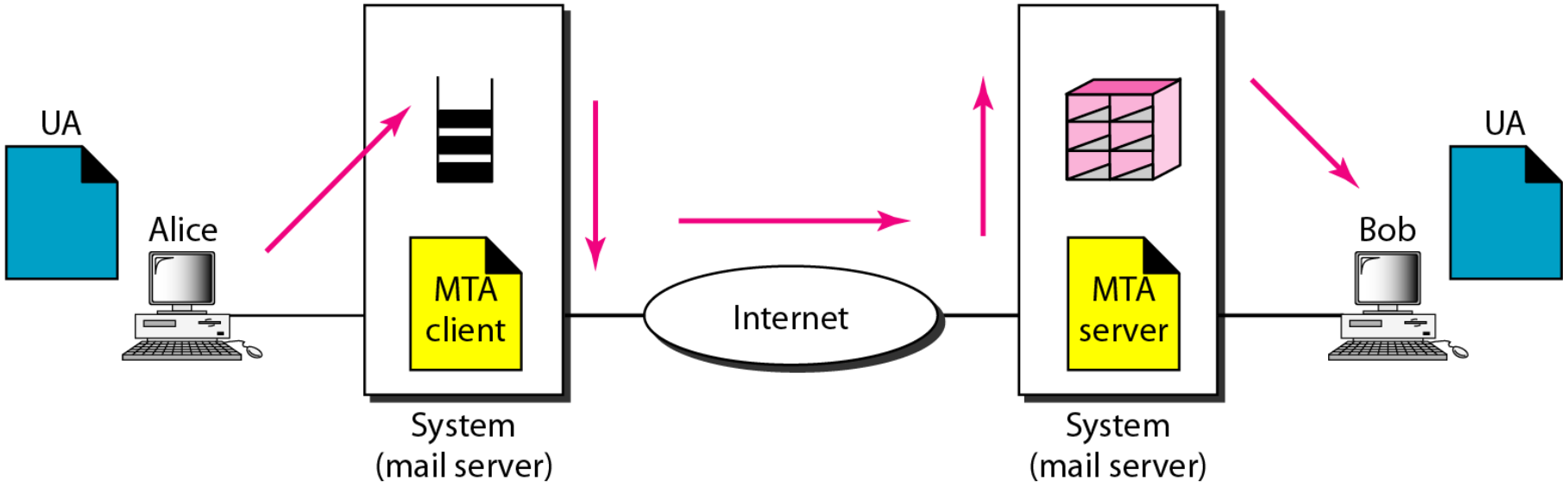


Note

When the sender and the receiver of an e-mail are on the same system, we need only two user agents.

Second scenario in electronic mail

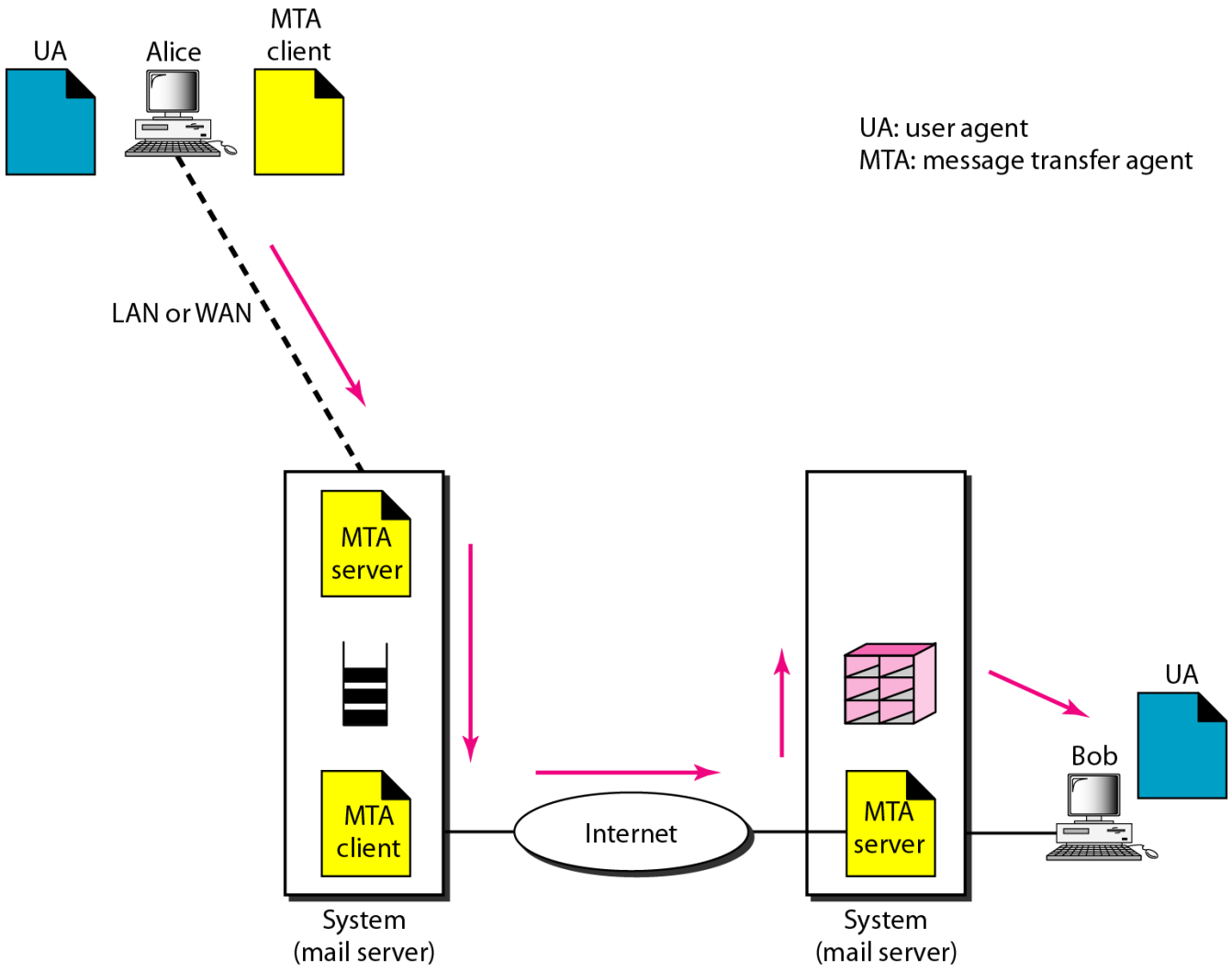
UA: user agent
MTA: message transfer agent



Note

When the sender and the receiver of an e-mail are on different systems, we need two UAs and a pair of MTAs (client and server).

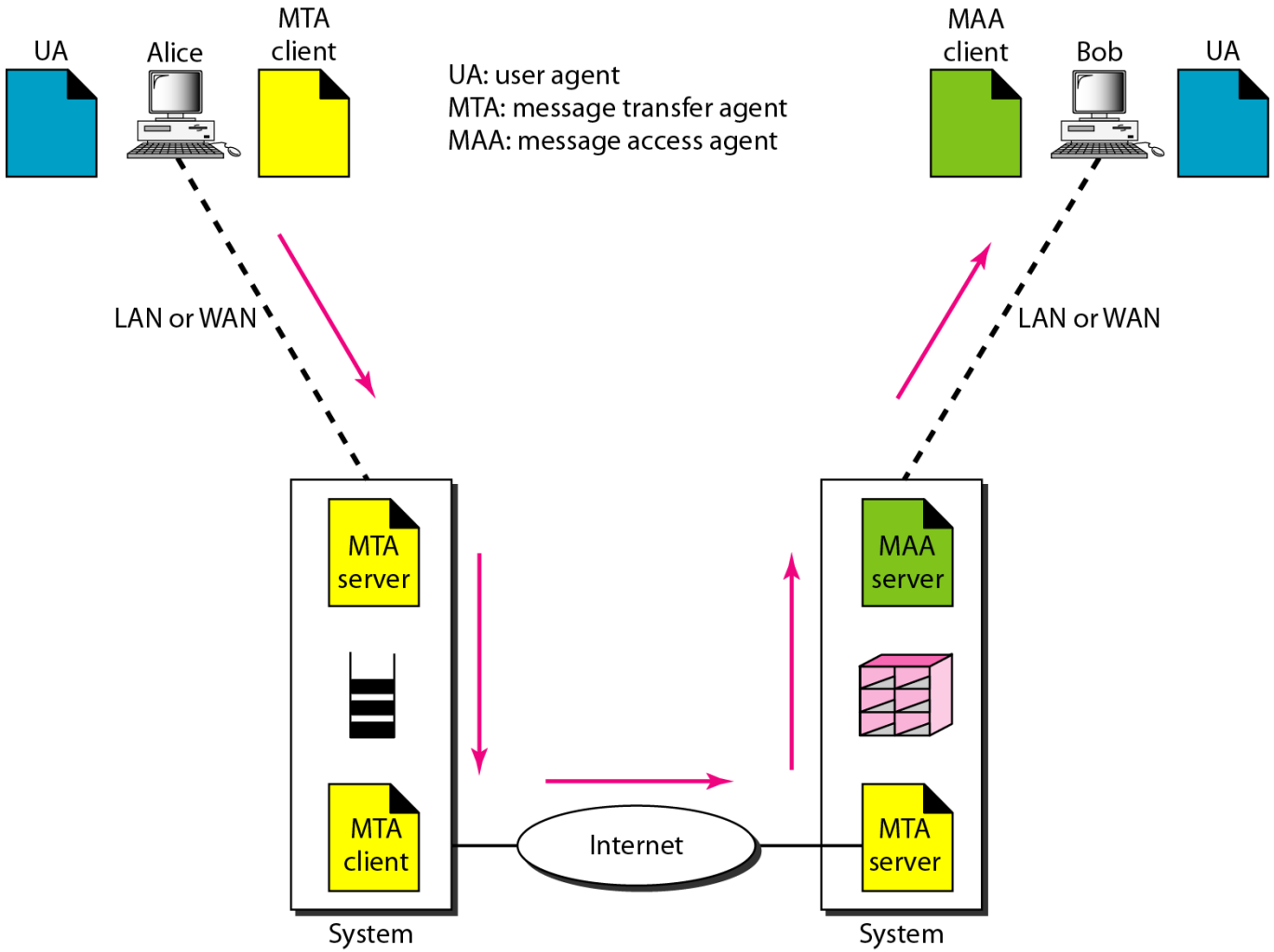
Third scenario in electronic mail



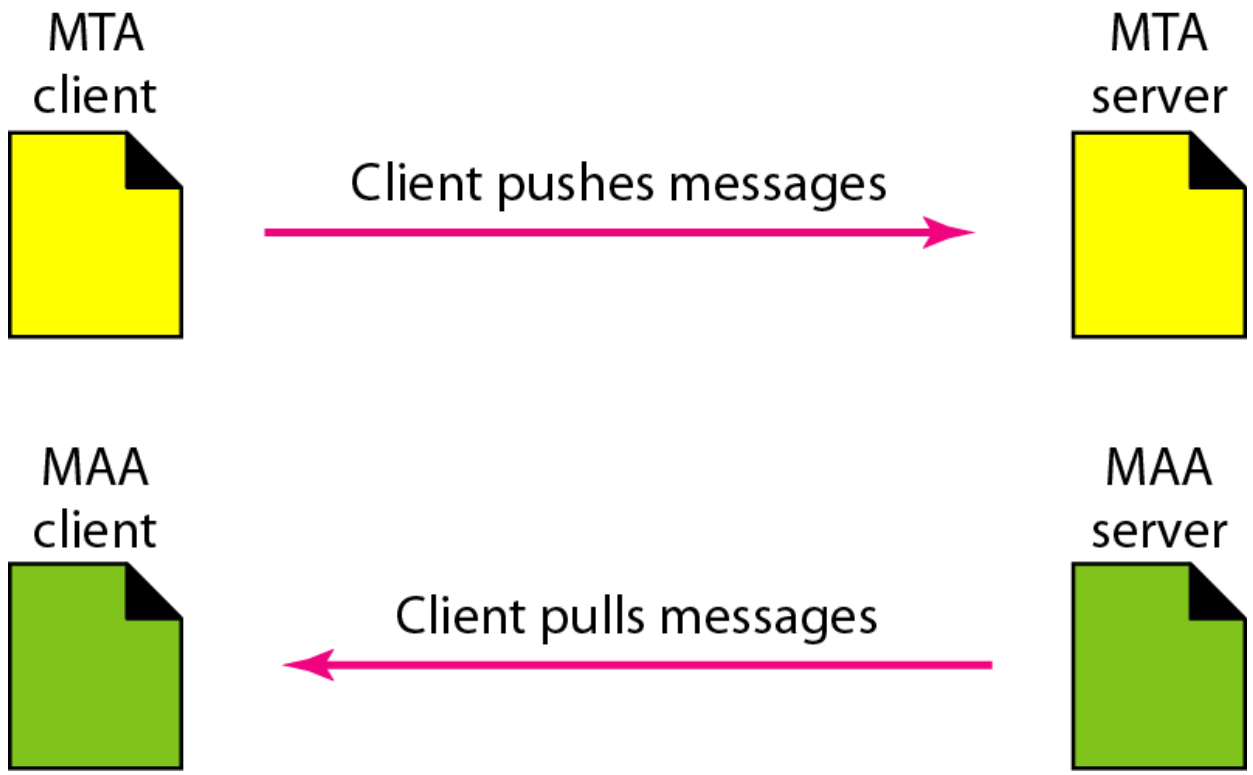
Note

When the sender is connected to the mail server via a LAN or a WAN, we need two UAs and two pairs of MTAs (client and server).

Fourth scenario in electronic mail



Push versus pull in electronic email

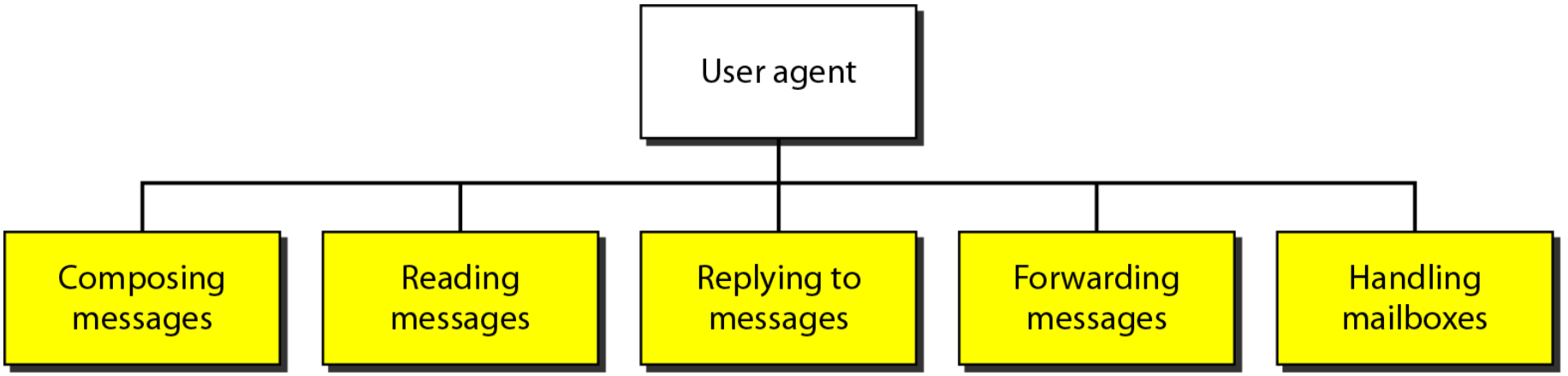


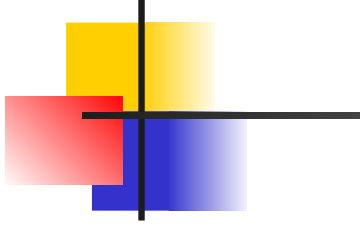
Note

When both sender and receiver are connected to the mail server via a LAN or a WAN, we need two UAs, two pairs of MTAs and a pair of MAAs.

This is the most common situation today.

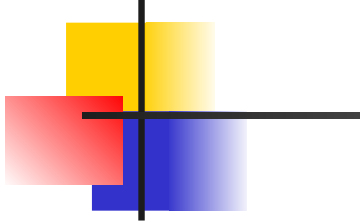
Services of user agent





Note

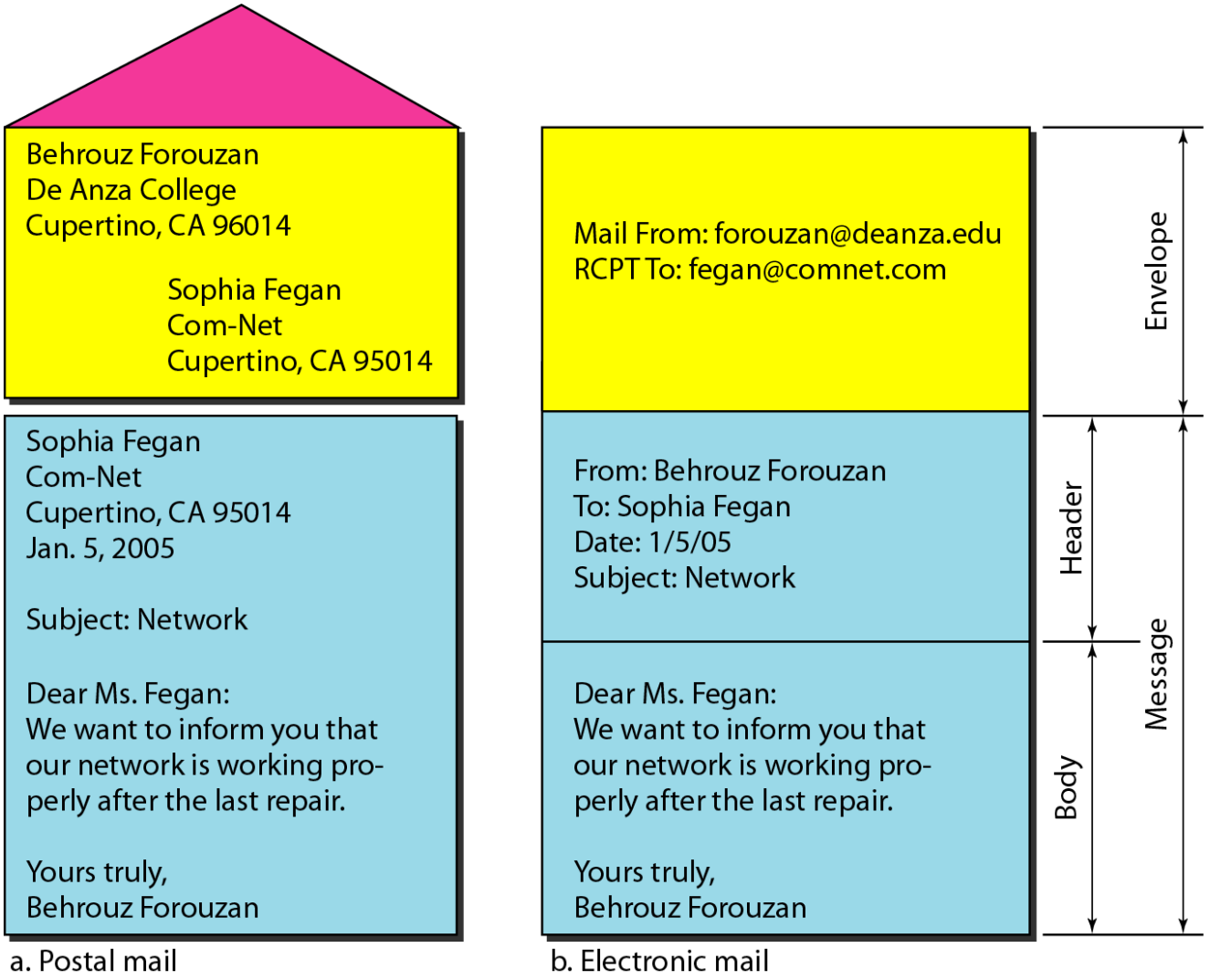
Some examples of command-driven user agents are *mail*, *pine*, and *elm*.



Note

Some examples of GUI-based user agents are *Eudora*, *Outlook*, and *Netscape*.

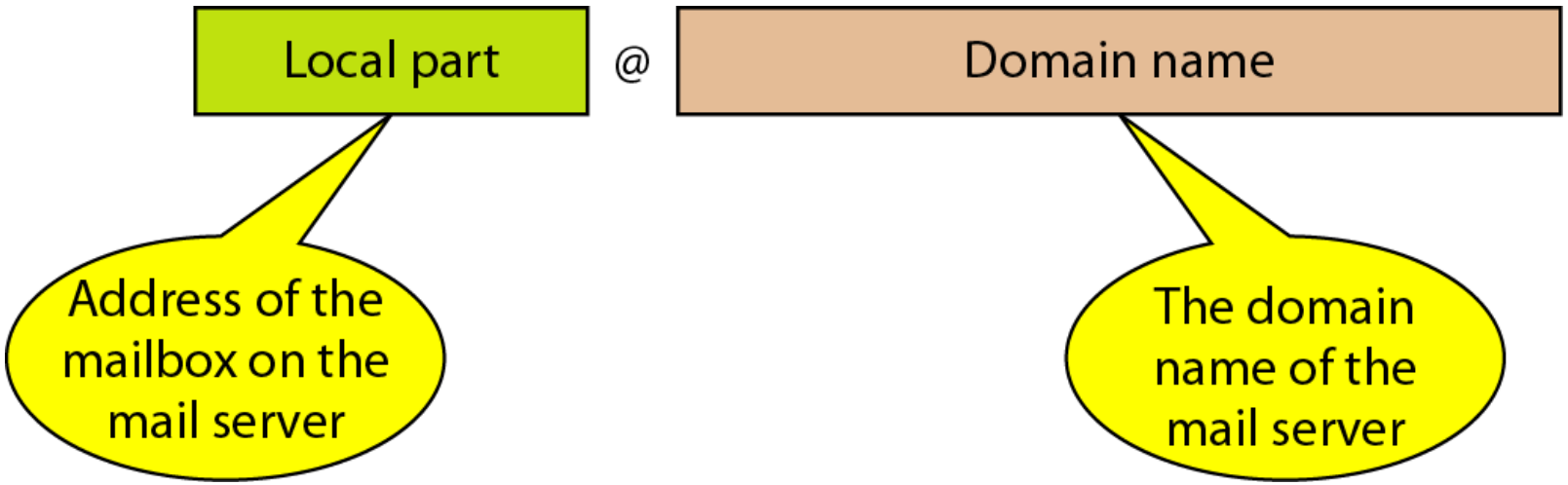
Format of an e-mail



a. Postal mail

b. Electronic mail

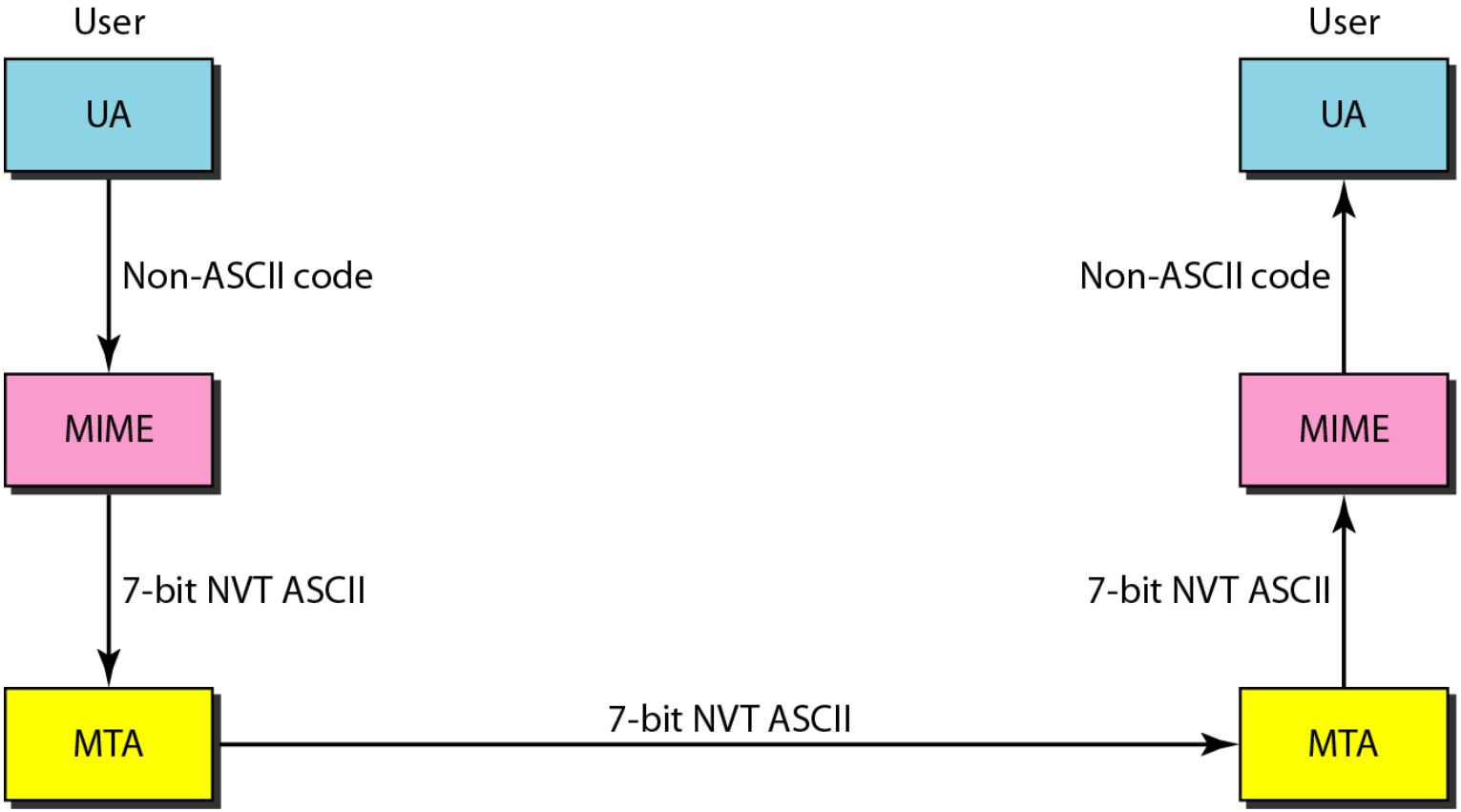
E-mail address



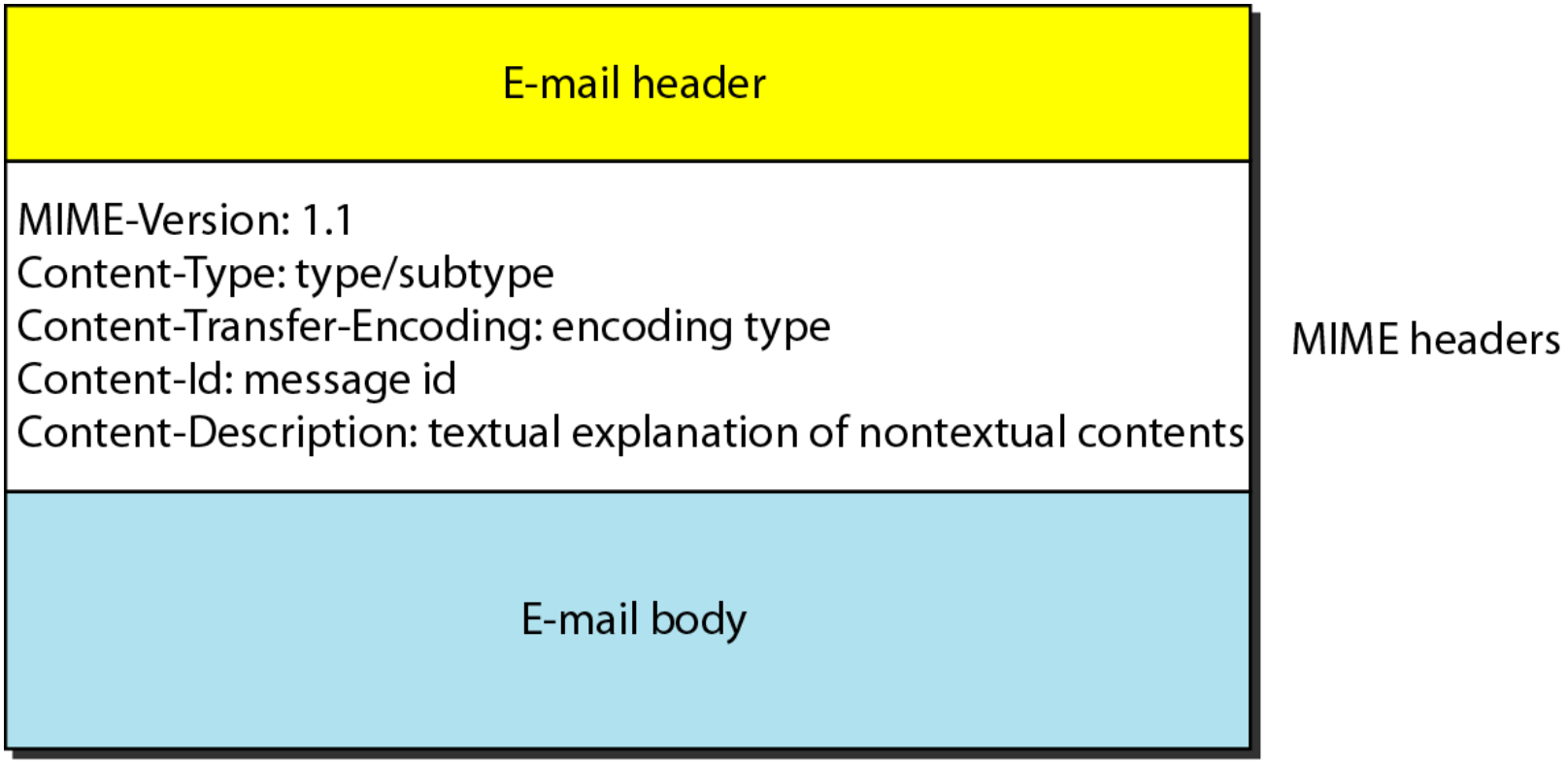
Multipurpose Internet Mail Extensions (MIME):

- Electronic mail has a simple structure. Its simplicity, comes at a price.
- It can send messages only in NVT 7-bit ASCII format.
- In other words, it has some limitations.
- For example, it cannot be used for languages that are not supported by 7-bit ASCII characters (such as French, German, Hebrew, Russian, Chinese, and Japanese).
- Also, it cannot be used to send binary files or video or audio data.
- **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 them to the client MTA to be sent through the Internet.
- The message at the receiving side is transformed back to the original data.
- We can think of MIME as a set of software functions that transforms non-ASCII data (stream of bits) to ASCII data and vice versa.

MIME


User
UA
Non-ASCII code
MIME
7-bit NVT ASCII
MTA
7-bit NVT ASCII
User
UA
Non-ASCII code
MIME
7-bit NVT ASCII
MTA

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

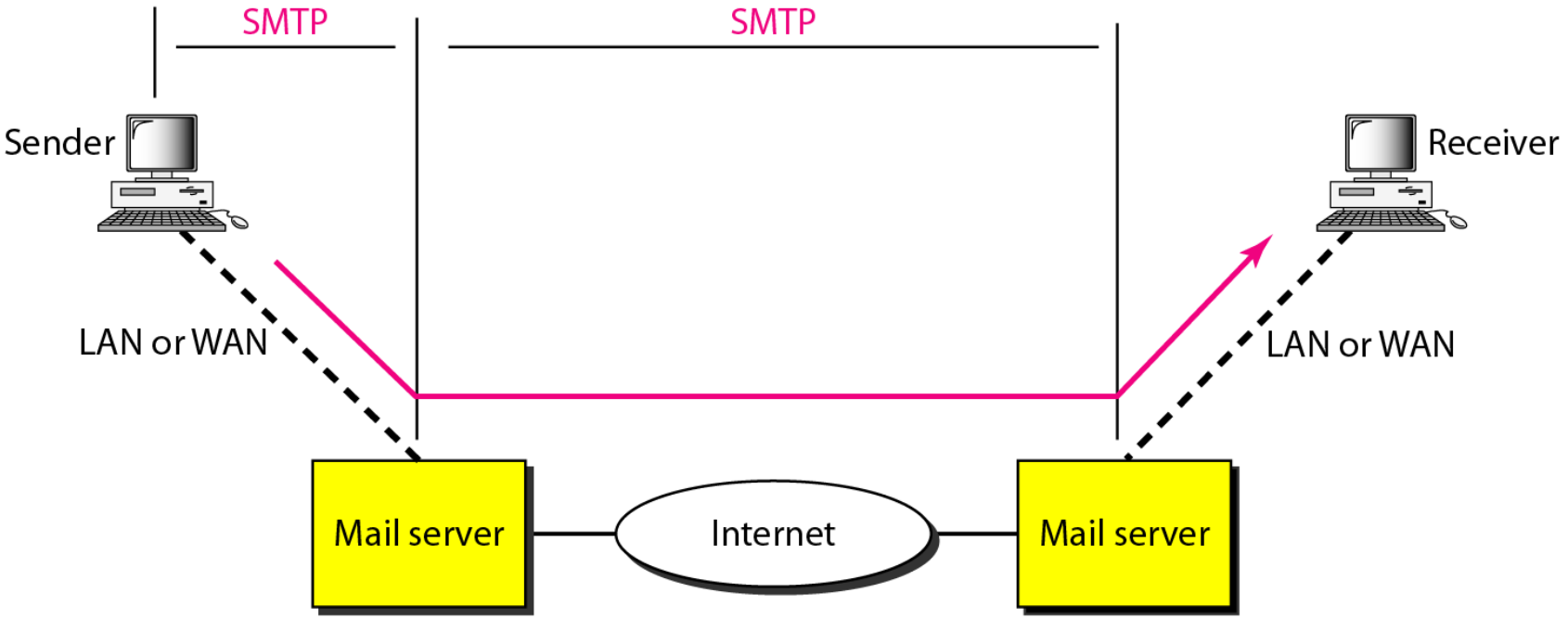
Data types and subtypes in MIME

Type	*Subtype*	*Description*
Text	Plain	Unformatted
	HTML	HTML format (see Chapter 27)
Multipart	Mixed	Body contains ordered parts of different data types
	Parallel	Same as above, but no order
	Digest	Similar to mixed subtypes, 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 (8-bit bytes)

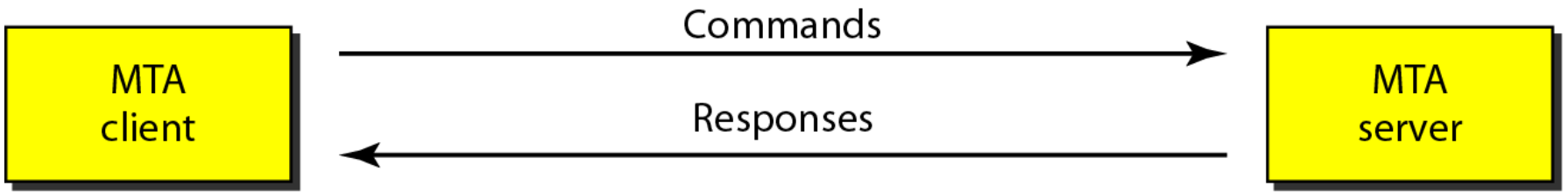
Content-transfer-encoding

Type	*Description*
7-bit	NVT ASCII characters and short lines
8-bit	Non-ASCII characters and short lines
Binary	Non-ASCII characters with unlimited-length lines
Base-64	6-bit blocks of data encoded into 8-bit ASCII characters
Quoted-printable	Non-ASCII characters encoded as an equals sign followed by an ASCII code

- SMTP


SMTP
SMTP
Sender
Receiver
LAN or WAN
LAN or WAN
Mail server
Internet
Mail server

- *Commands and responses*



- Figure . *Command format*

- Table *Commands*

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

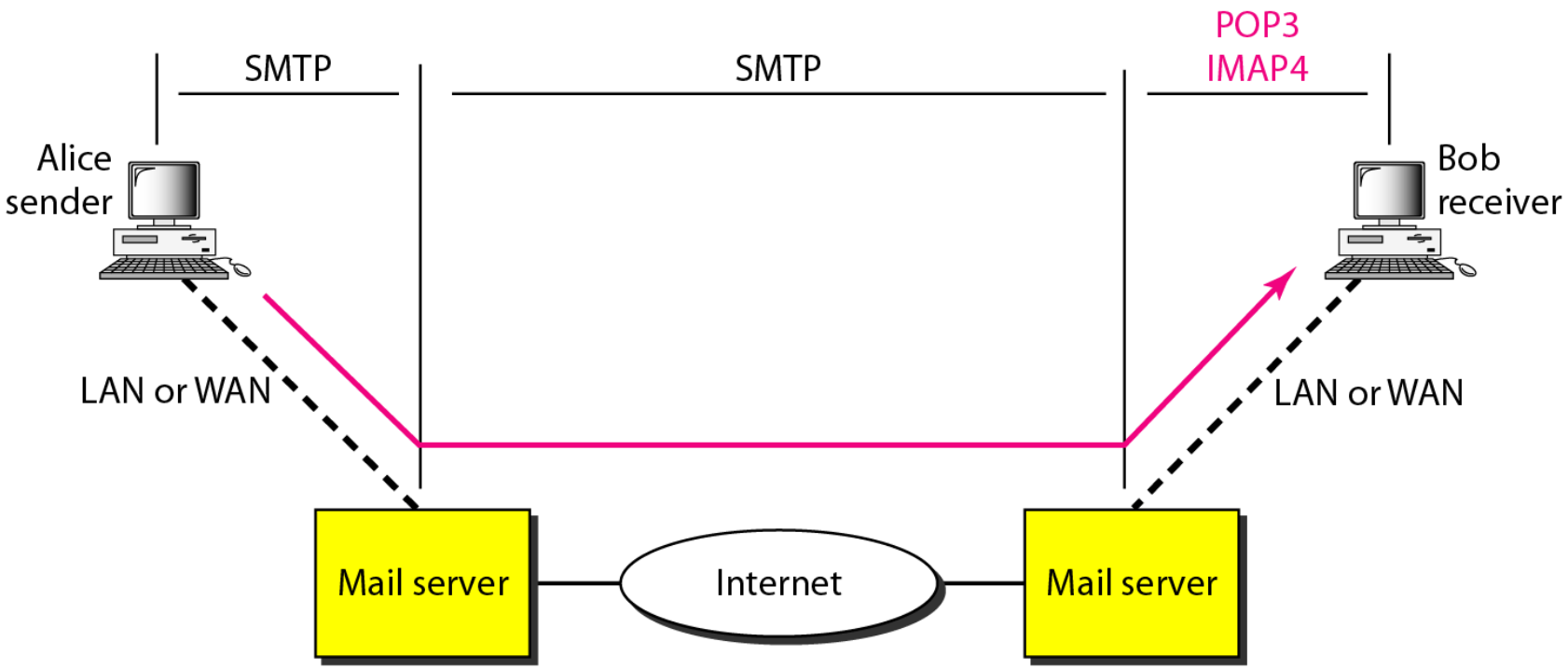
- Table *Responses*

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

- Table *Responses* *(continued)*

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

- *POP3 and IMAP4*



Comparison between IMAP4 & POP3

- IMAP4 is used to download, read and manage emails, while POP3 is used only for downloading emails.
- IMAP4 is newer and more popular than POP3, especially when mailboxes are huge, or multiple clients access the same account.
- With IMAP4, the server retains the master copy and all devices and apps that are configured for the email account sync with the server. With POP3, there is no such synchronization.
- With IMAP4, any changes (such as deleting mail) made on one device are automatically reflected in any other app or device syncing to the same account.
- With POP3, you can download all email from the server on to your device and choose to either delete the copy on the server or retain it.

	IMAP4	POP3
Speed	Slow	Fast
Storage of content	Always on server	Downloaded onto local device, unless ‘keep a copy on the server’ selected.
Mail Syncing	Yes	No
Direction	Bi-directional - Whatever changes you make on server or device, the other side shows the changes too.	One-direction - Changes made on device have no effect on server content.
Port used by server	PORT 143	PORT 110
Keep messages on the server	Required	Possible

Web-Based Mail

-Eg. Gmail, Hotmail and Yahoo.

- Mail transfer from Sender's browser to sender's mail server is done through HTTP.

- The transfer of the message from the sending mail server to the receiving mail server is still through SMTP.

- Finally, the message from the receiving server (the Webserver) to receiver's browser is done through HTTP.

- The last phase is very interesting. Instead of POP3 or IMAP4, HTTP is normally used.

- The website sends a form to be filled in by user, which includes the log-in name and the password.

- If the log-in name and password match, the e-mail is transferred from the Web server to user's browser in HTML format.

• FILE TRANSFER

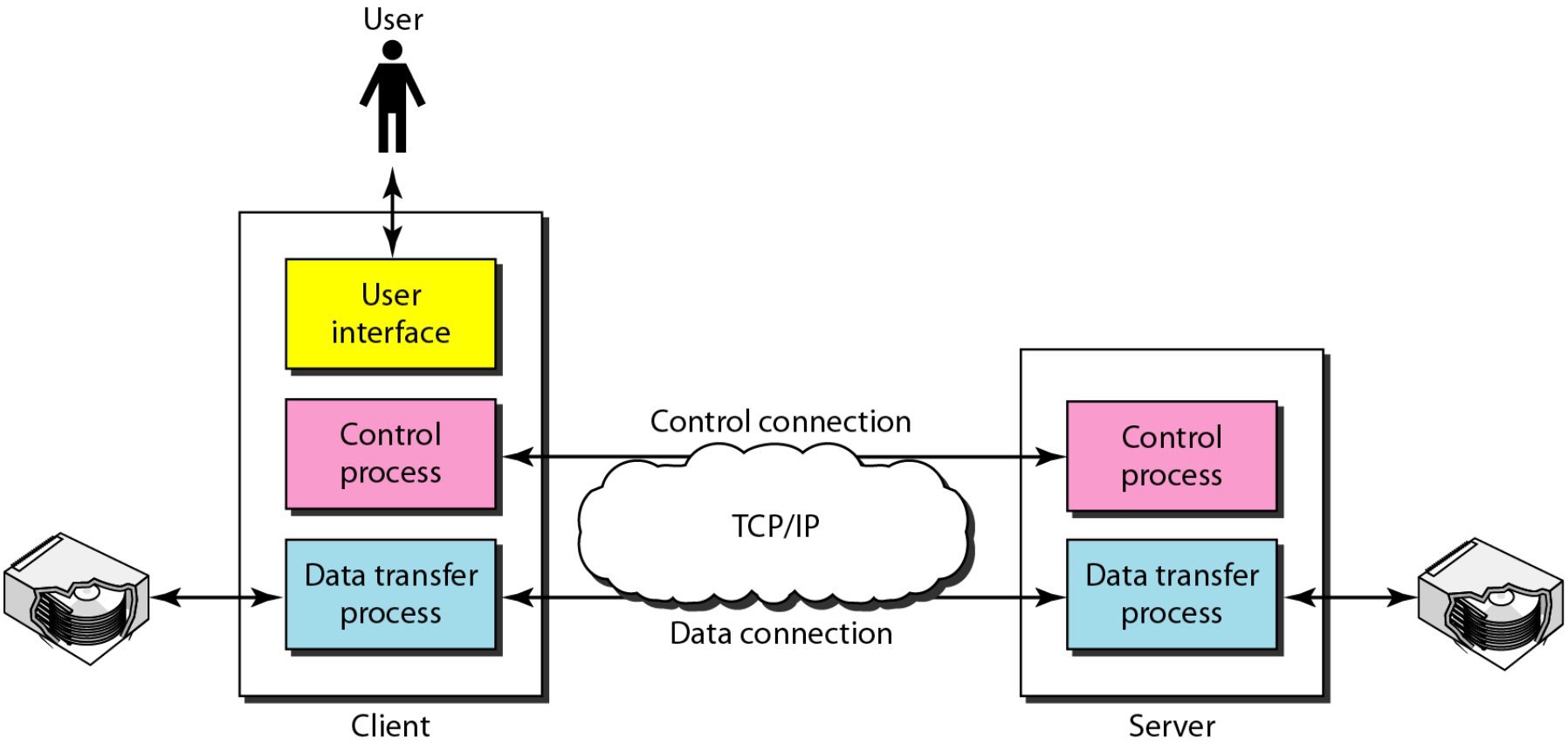
- *Transferring files from one computer to another is one of the most common tasks expected from a networking or internetworking environment. As a matter of fact, the greatest volume of data exchange in the Internet today is due to file transfer.*

- File Transfer Protocol (FTP)
- Use to transfer différent file formats.

- *Note*

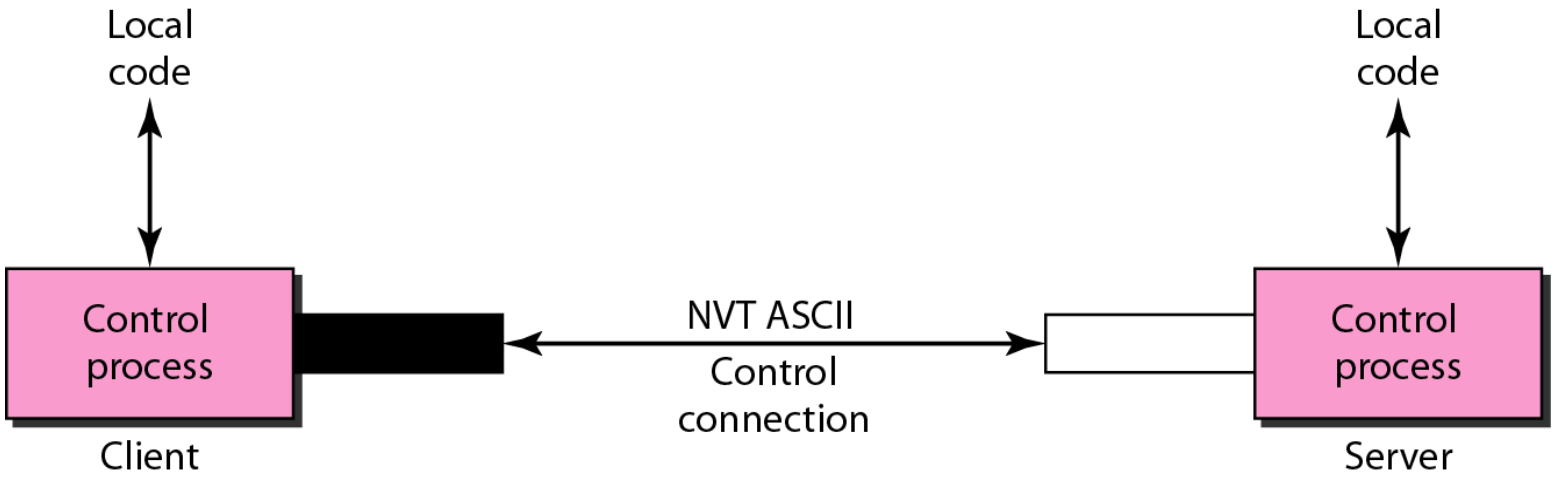
- FTP uses the services of TCP. It needs two TCP connections.
- The well-known port 21 is used for the control connection and the well-known port 20 for the data connection.

- Figure. *FTP*



- The control connection remains connected during the entire interactive.
- The Data connection is opened and then closed for each file transferred.

- Figure. *Using the control connection*



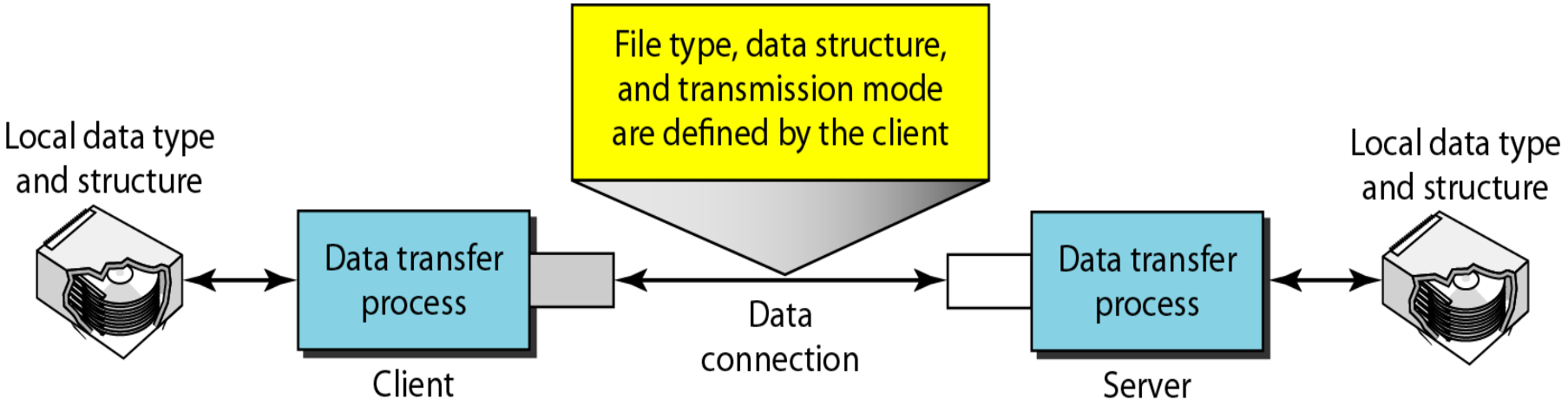
Communication over Data Connection

- File transfer occurs over the data connection under the control of the commands sent over the control connection.
- However, we should remember that file transfer in FTP means one of three things:

1. A file is to be copied from the server to the client. This is called retrieving a file. It is done under the supervision of the RETR command.
2. A file is to be copied from the client to the server. This is called storing a file. It is done under the supervision of the STOR command.
3. A list of directory or file names is to be sent from the server to the client. This is done under the supervision of the LIST command.

Note that FTP treats a list of directory or file names as a file. It is sent over the data connection.

- Figure. *Using the data connection*



File Type: ASCII file, EBCDIC file, image file etc.

Data Structure : File structure, record structure & page structure.

Transmission mode : Stream mode, block mode, compressed mode.

Anonymous FTP :

- To use FTP, a user needs an account (user name) and a password on the remote server.
- Some sites have a set of files available for public access, to enable anonymous FTP.
- To access these files, a user does not need to have an account or password.
- Instead, the user can use anonymous as the user name and guest as the password.
- User access to the system is very limited. Some sites allow anonymous users only a subset of commands.
- For example, most sites allow the user to copy some files, but do not allow navigation through the directories.

• REMOTE LOGGING

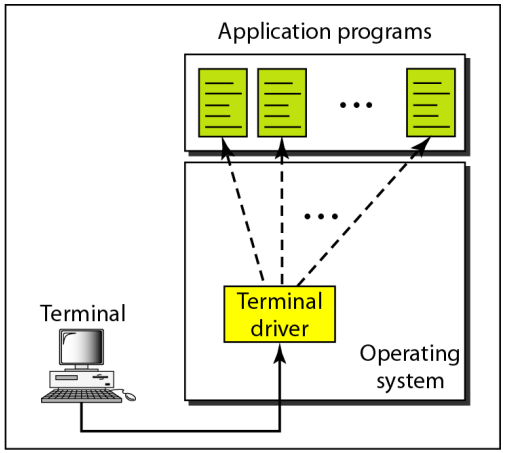
- *It would be impossible to write a specific client/server program for each demand. The better solution is a general-purpose client/server program that lets a user access any application program on a remote computer.*

- TELNET (TErminaL NETwork)

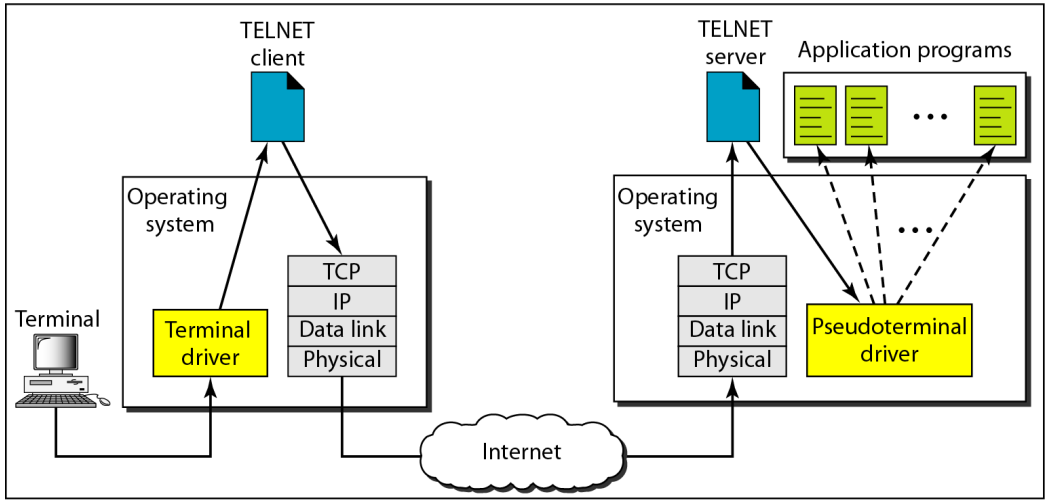
  - TELNET is a general-purpose client/server application program.

- Timesharing Environment.
- Logging:
  - Local log-in: (No use of TELNET).
  - Remote log-in: (Use of TELNET).

- *Local and remote log-in*

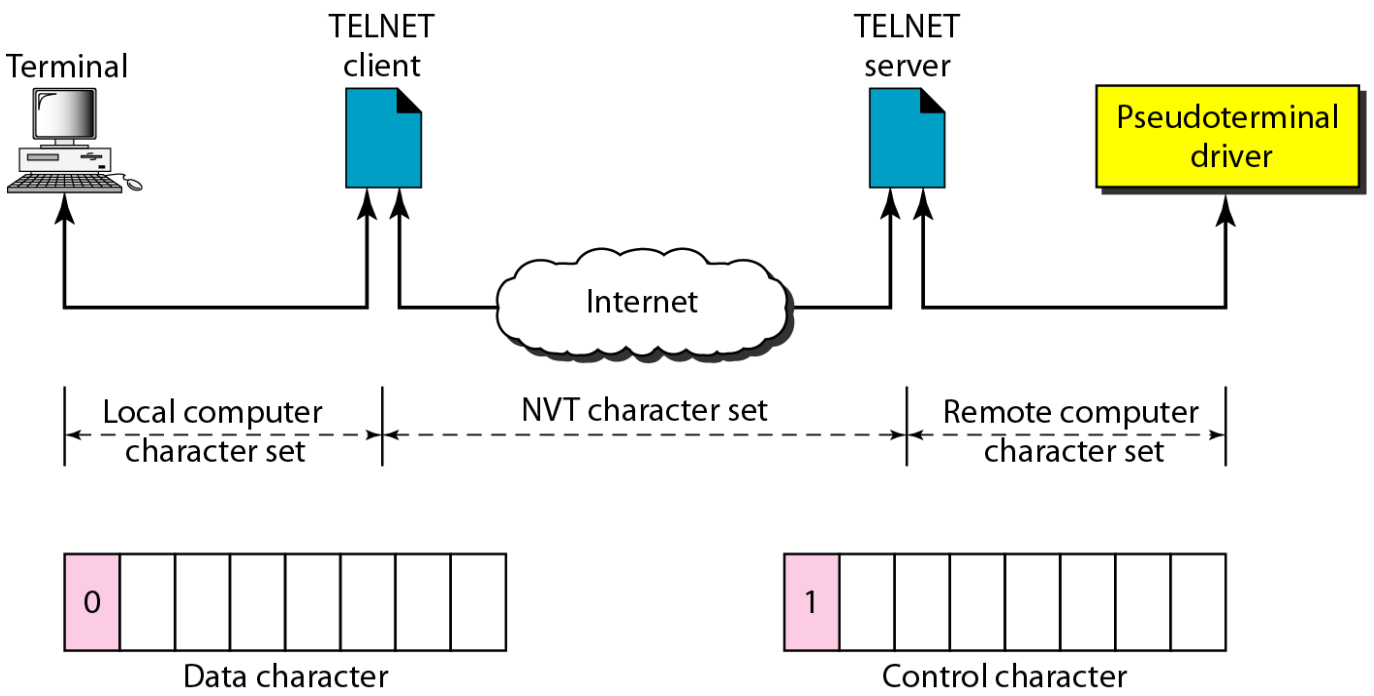


a. Local log-in



b. Remote log-in

- *Concept of NVT*

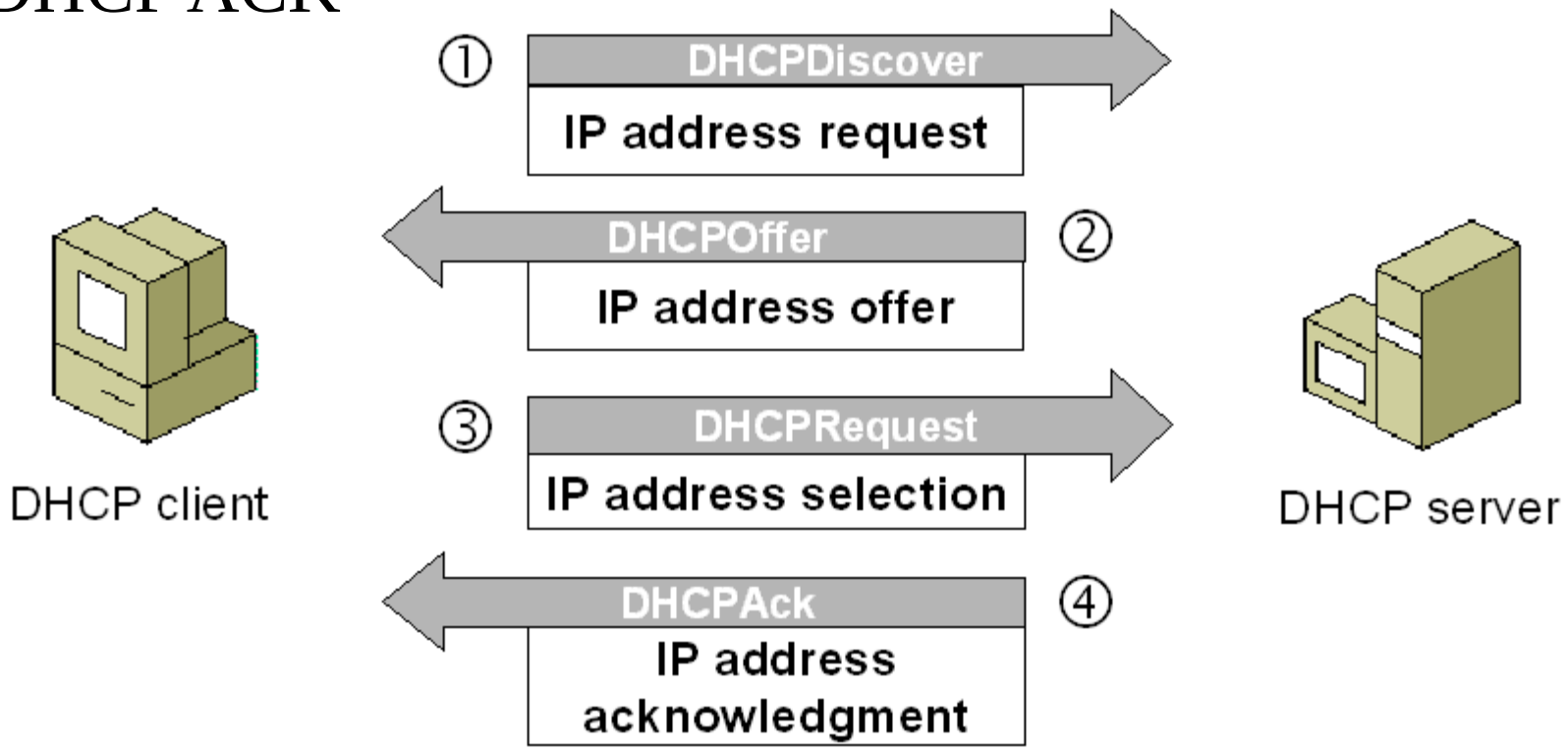


DHCP (*Dynamic Host Configuration Protocol*)

- DHCP is a Client-Server protocol provides static and dynamic address allocation that can be manual or automatic.
- DHCP provides temporary IP addresses for a limited time (Lease time).
- If lease expire, client must either stop use of IP or renew the lease.

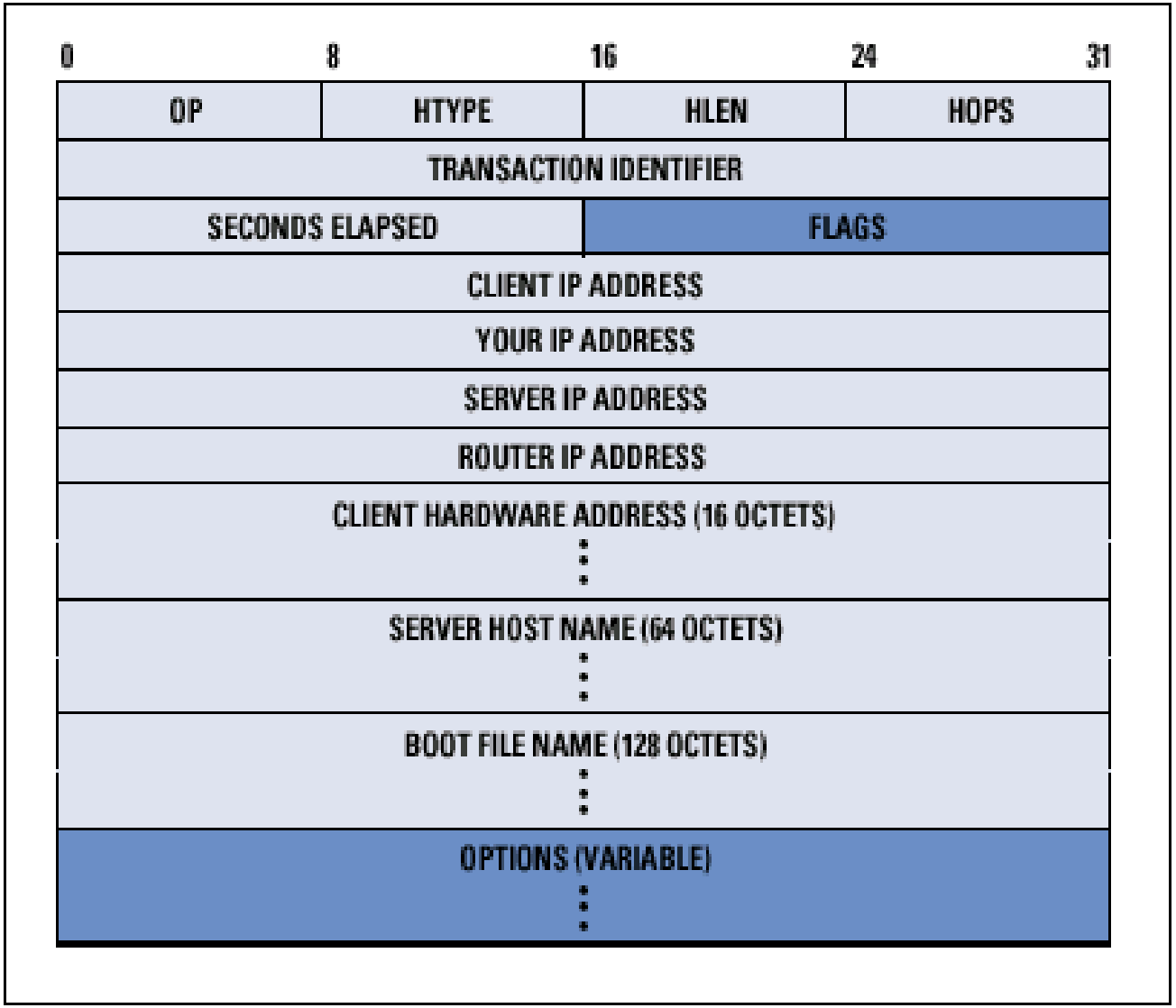
It is a 4 step process:

1.DHCP discover
2.DHCP offer
3.DHCP request
4.DHCP ACK



- DHCP Header

Figure 2: DHCP Message Format



- **(There are >100 different options)**

OpCode: *1 (Request), 2(Reply)*

Hardware Type: *1 (for Ethernet)*

Hardware address length: *6 (for Ethernet)*

Hop count: *set to 0 by client*

Transaction ID: *Integer (used to match reply to response)*

Seconds: *number of seconds since the client started to boot.*
Flags : *2 bytes- 1 bit is Broadcast bit=1- used to braodcast request, remaining 15 bits = 0, unused*

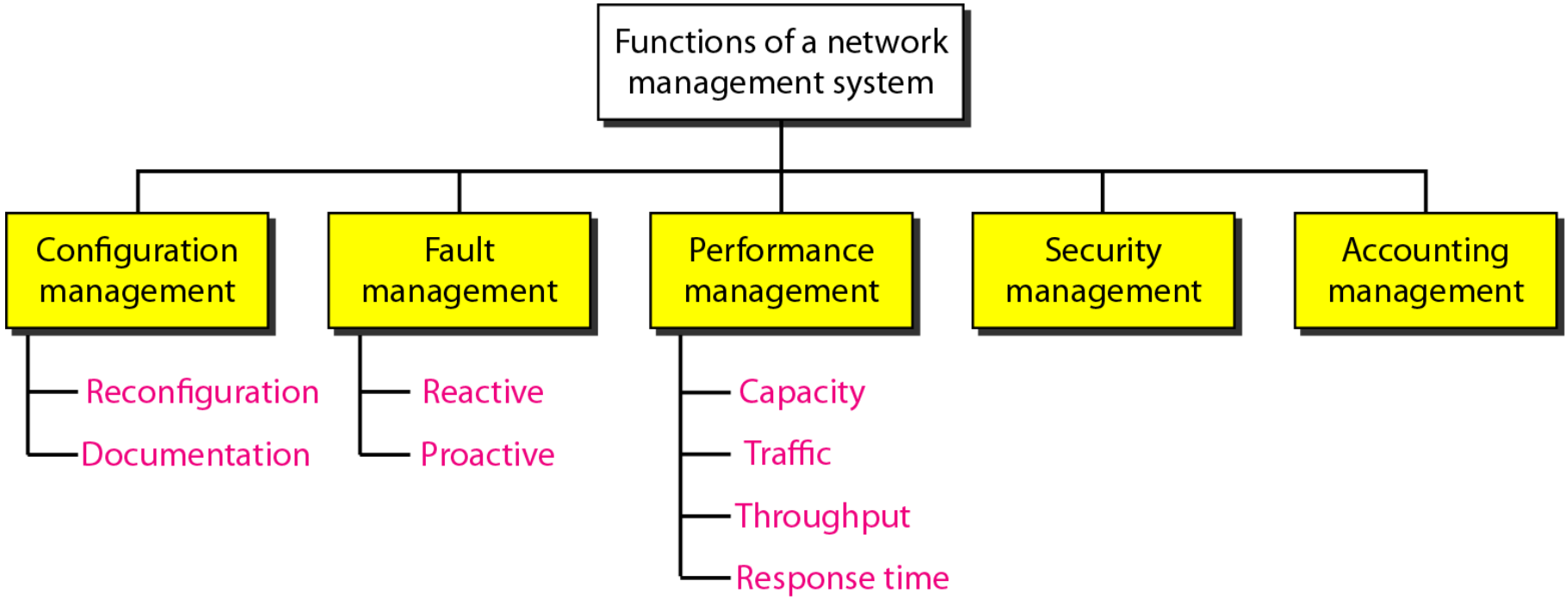
Client IP address, Your IP address, server IP address, Gateway IP address, client hardware address, server host name, boot file name: *client fills in the information that it has, leaves rest blank.*

NETWORK MANAGEMENT SYSTEM

- ***We can say that the functions performed by a network management system can be divided into five broad categories: configuration management, fault management, performance management, security management, and accounting management.***

Configuration Management
Fault Management
Performance Management
Security Management
Accounting Management

Functions of a network management system



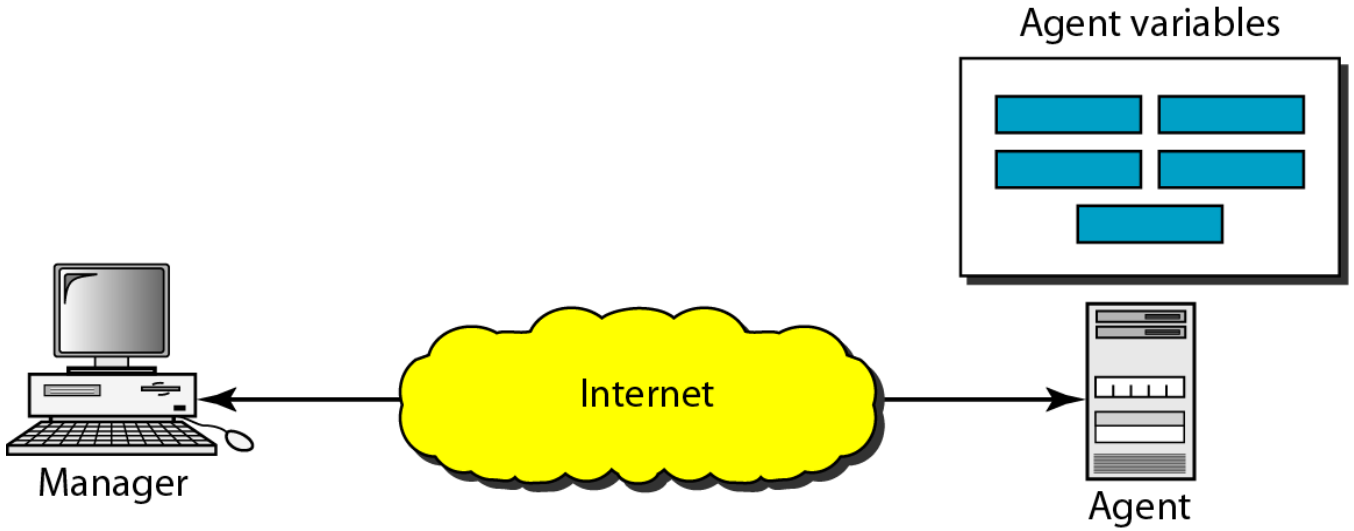
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

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

Topics discussed in this Protocol:

Concept
Management Components
Structure of Management Information (SMI)
Management Information Base (MIB)
SNMP

SNMP concept



SNMP uses the concept of manager and agent. That is, a manager, usually a host, controls and monitors a set of agents, usually routers or servers.

- SNMP is an application-level protocol in which a few manager stations control a set of agents.
- The protocol is designed at the application level so that it can monitor devices made by different manufacturers and installed on different physical networks.
- SNMP frees management tasks from both the physical characteristics of the managed devices and the underlying networking technology.
- It can be used in a heterogeneous internet made of different LANs and WANs connected by routers made by different manufacturers.

Managers and Agents

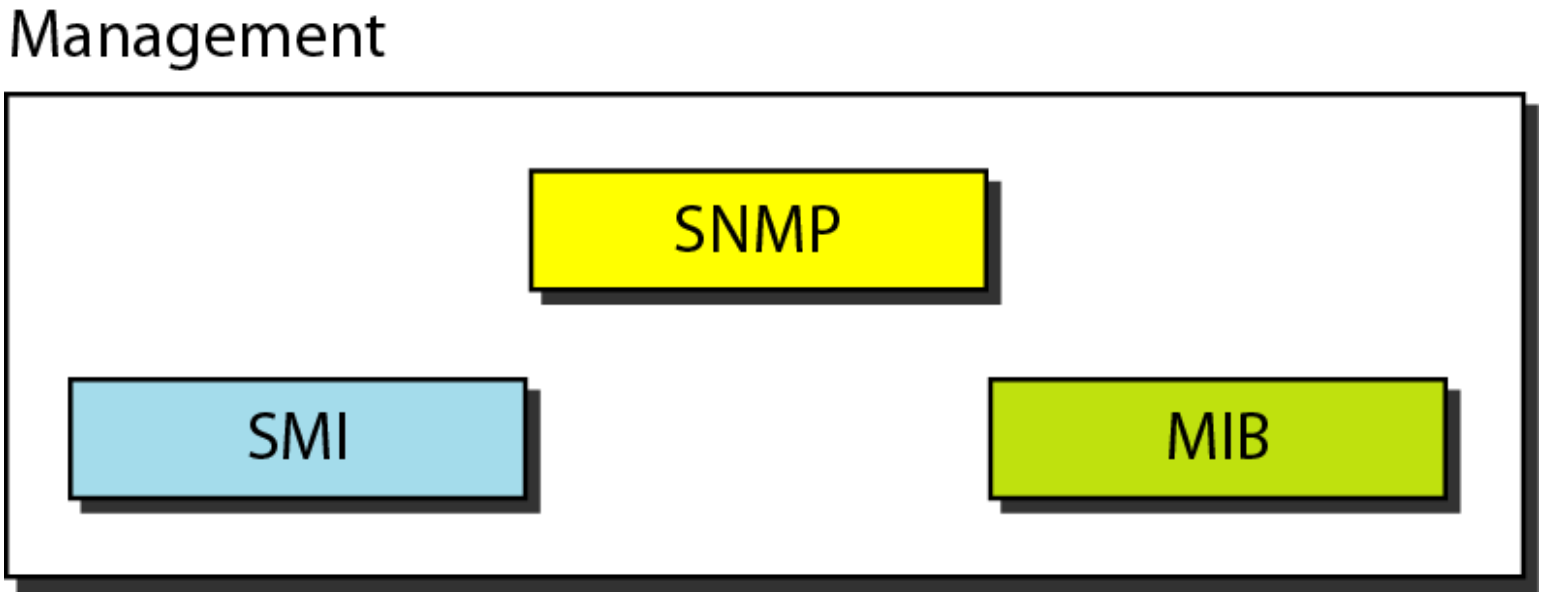
- A management station, called a manager, is a host that runs the SNMP client program.
- A managed station, called an agent, is a router (or a host) that runs the SNMP server program.
- Management is achieved through simple interaction between a manager and an agent.
- The agent keeps performance information in a database. The manager has access to the values in the database.
- For example, a router can store in appropriate variables the number of packets received and forwarded. The manager can fetch and compare the values of these two variables to see if the router is congested or not.
- The manager can also make the router perform certain actions.
- For example, a use this feature to reboot the agent remotely at any time. It simply sends a packet to force a 0 value in the counter.

Agents can also contribute to the management process. The server program running on the agent can check the environment, and if it notices something unusual, it can send a warning message, called a trap, to the manager.

In other words, management with SNMP is based on three basic ideas:

1. A manager checks an agent by requesting information that reflects the behavior of the agent.
2. A manager forces an agent to perform a task by resetting values in the agent database.
3. An agent contributes to the management process by warning the manager of an unusual situation.

Components of network management on the Internet



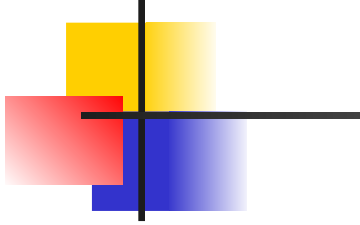
Structure of Management Information (SMI)
Management Information Base (MIB).

Note

SNMP defines the format of packets exchanged between a manager and an agent. It reads and changes the status (values) of objects (variables) in SNMP packets.

Note

SMI defines the general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values.



Note

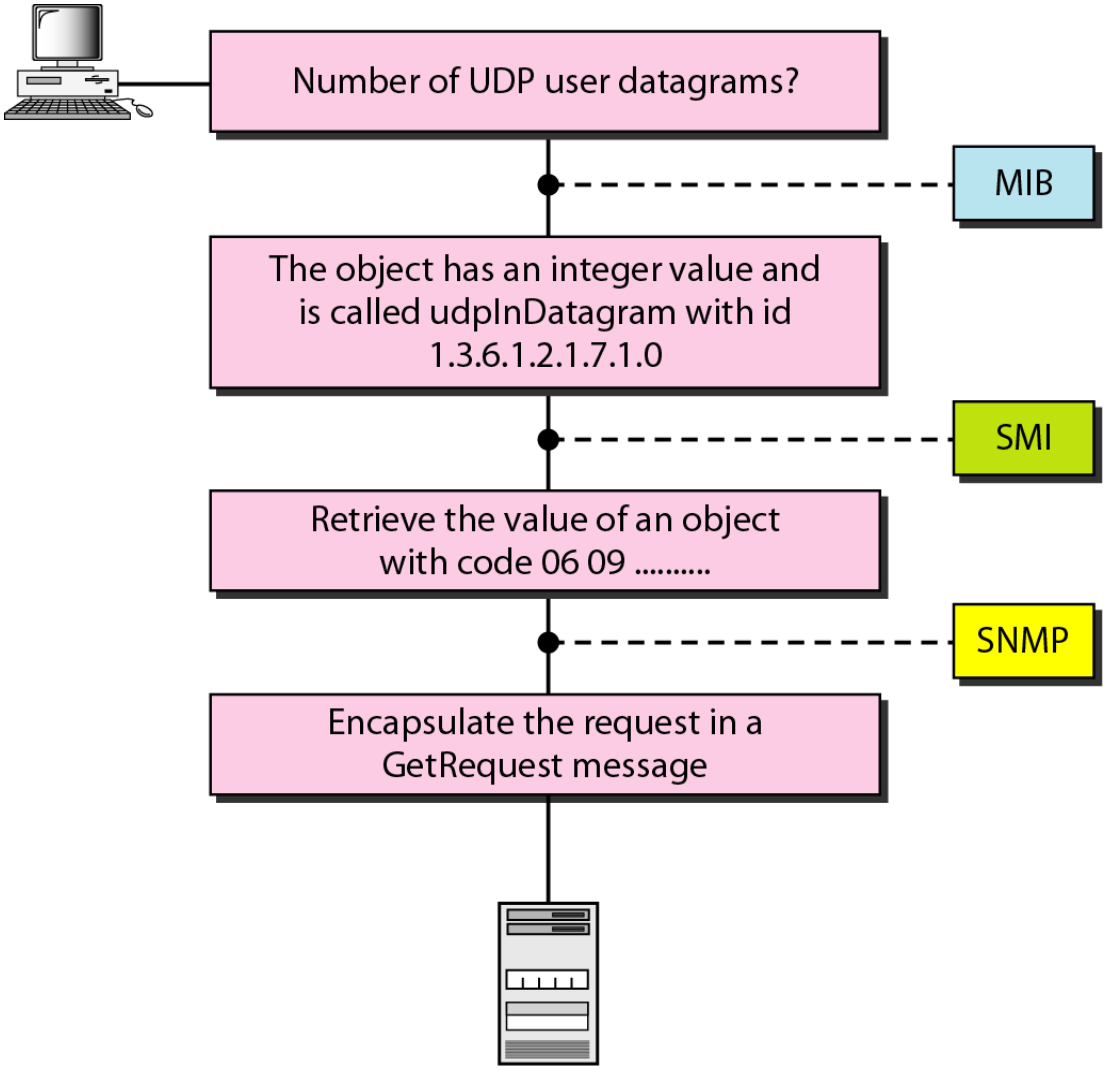
MIB creates a collection of named objects, their types, and their relationships to each other in an entity to be managed.

Note

We can compare the task of network management to the task of writing a program.

- **Both tasks need rules. In network management this is handled by SMI.**
- **Both tasks need variable declarations. In network management this is handled by MIB.**
- **Both tasks have actions performed by statements. In network management this is handled by SNMP.**

Management overview



SNMP

- SNMP uses both SMI and MIB in Internet network management. It is an application program that allows:

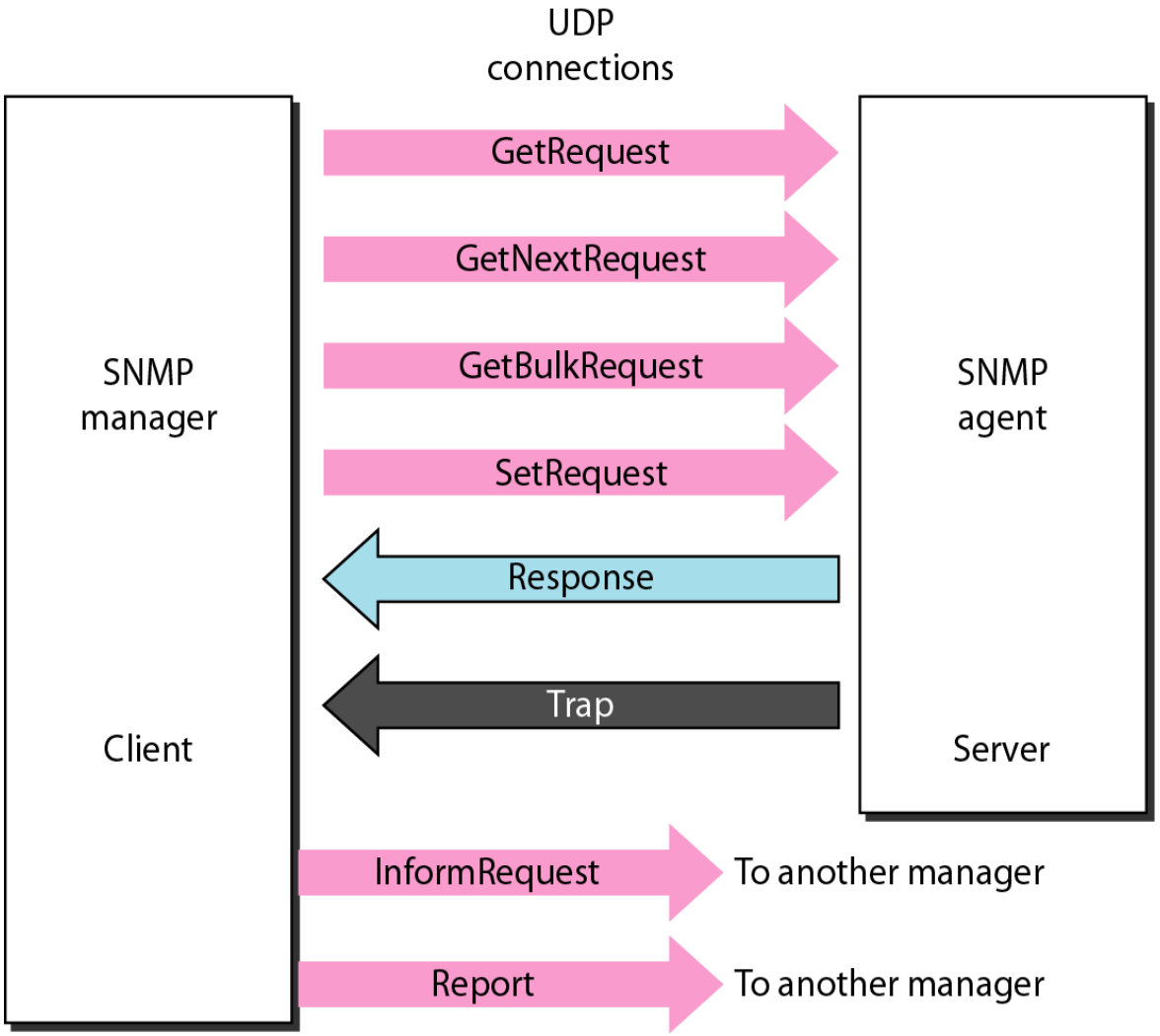
1. A manager to retrieve the value of an object defined in an agent.
2. A manager to store a value in an object defined in an agent.
3. An agent to send an alarm message about an abnormal situation to the manager.

Protocol Data Unit's (PDUs)

SNMPv3 defines eight types of packets (or PDUs):

GetRequest, GetNextRequest, GetBulkRequest, SetRequest, Response, Trap, InformRequest,and Report.

SNMP PDUs


UDP
connections
SNMP
manager
SNMP
agent
GetRequest
GetNextRequest
GetBulkRequest
SetRequest
Response
Trap
Client
Server
InformRequest
To another manager
Report
To another manager

GetRequest: To retrieve the value of a variable or a set of variables.

GetNextRequest: To retrieve the value of a variable. The retrieved value is the value of the object following the defined Objectid in the PDU. It is mostly used to retrieve the values of the entries in a table.

GetBulkRequest: To retrieve a large amount of data. It can be used instead of multiple GetRequest and GetNextRequest.

SetRequest: To set (store) a value in a variable.

Response: The Response sent to a manager in response to GetRequest or GetNextRequest. It contains the value(s) of the variable(s) requested by the manager.

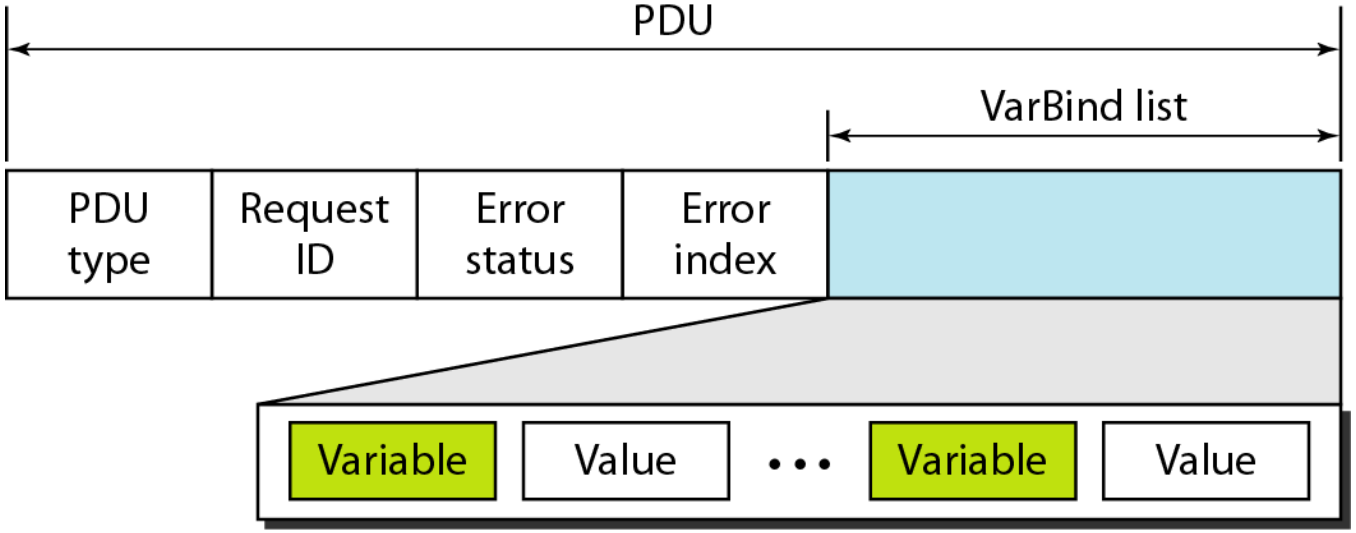
Trap: The Trap (also called SNMPv2 Trap to distinguish it from SNMPv 1 Trap) PDU is sent to report an event. For example, if the agent is rebooted, it infonns the manager and reports the time of rebooting.

InformRequest: It is sent to get the value of some variables from agents under the control of the remote manager. The remote manager responds with a Response PDU.

Report: The Report POD is designed to report some types of errors between managers.

It is not yet in use.

SNMP PDU format



Differences:

1. Error status and error index values are zeros for all request messages except GetBulkRequest.
2. Error status field is replaced by nonrepeater field and error index field is replaced by max-repetitions field in GetBulkRequest.

Codes for SNMP messages

Data	*Class*	*Format*	*Number*	*Whole Tag (Binary)*	*Whole Tag (Hex)*
GetRequest	10	1	00000	**10100000**	**A0**
GetNextRequest	10	1	00001	**10100001**	**A1**
Response	10	1	00010	**10100010**	**A2**
SetRequest	10	1	00011	**10100011**	**A3**
GetBulkRequest	10	1	00101	**10100101**	**A5**
InformRequest	10	1	00110	**10100110**	**A6**
Trap (SNMPv2)	10	1	00111	**10100111**	**A7**
Report	10	1	01000	**10101000**	**A8**

Request ID: This field is a sequence number used by the manager in a Request PDU and repeated by the agent in a response. It is used to match a request to a response.

Error status: This is an integer that is used only in Response PDUs to show the types of errors reported by the agent. Its value is 0 in Request PDUs.

Nonrepeaters: This field is used only in GetBulkRequest and replaces the error status field, which is empty in Request PDUs.

Error index: The error index is an offset that tells the manager which variable caused the error.

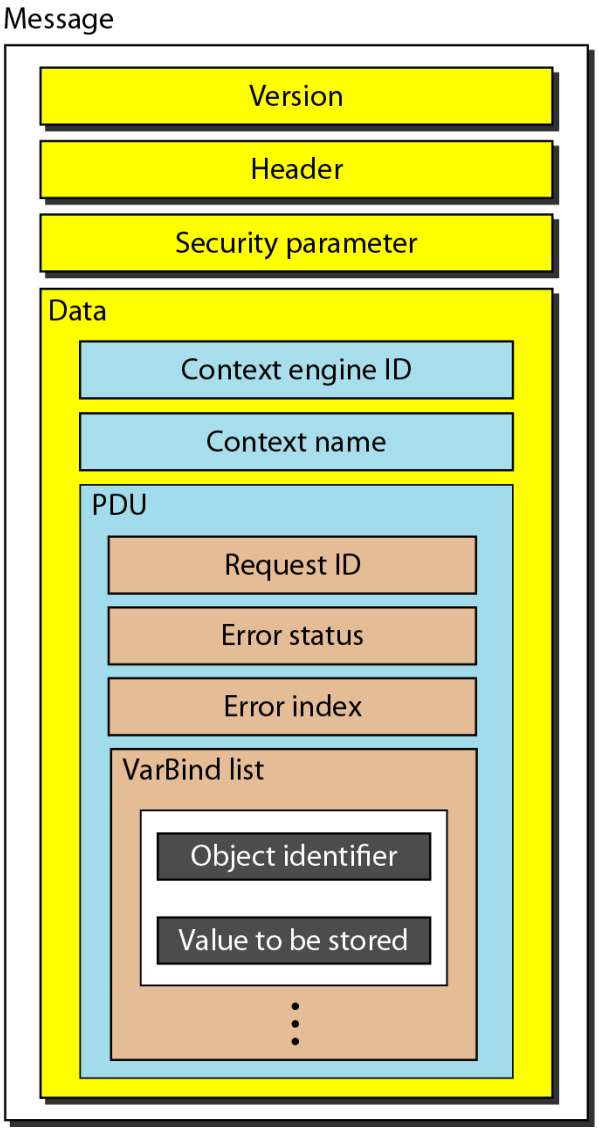
Max-repetition: This field is also used only in GetBulkRequest and replaces the error index field, which is empty in Request PDUs.

VarBind list: This is a set of variables with the corresponding values the manager wants to retrieve or set. The values are null in GetRequest and GetNextRequest. In a Trap PDU, it shows the variables and values related to a specific PDU.

Types of errors

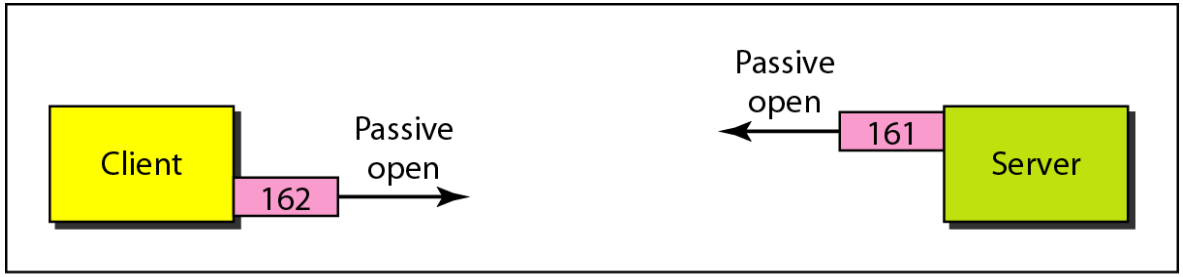
Status	*Name*	*Meaning*
0	noError	No error
1	tooBig	Response too big to fit in one message
2	noSuchName	Variable does not exist
3	badValue	The value to be stored is invalid
4	readOnly	The value cannot be modified
5	genErr	Other errors

SNMP message

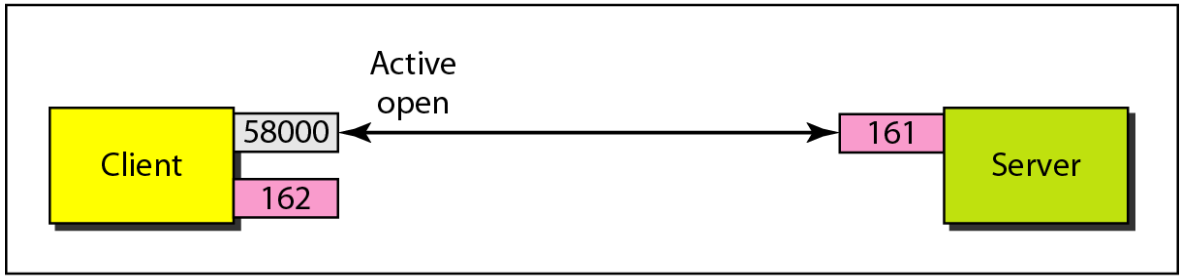


Port numbers for SNMP

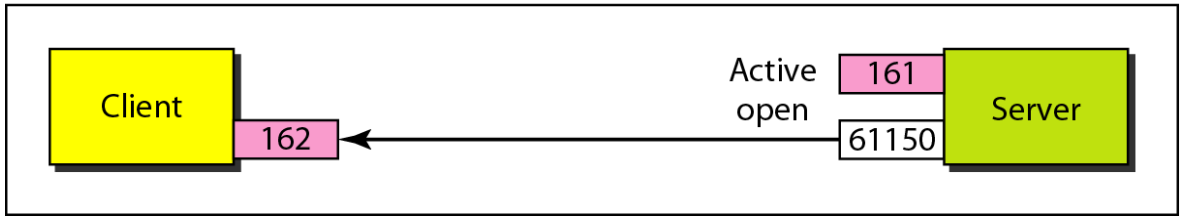
SNMP uses the services of UDP on two well-known ports, 161 and 162. The wellknown port 161 is used by the server (agent), and the well-known port 162 is used by the client (manager).



a. Passive open by both client and server



b. Exchange of request and response messages



c. Server sends trap message