Computer Networks

— Unit - 5 —

— Application Layer —

- Domain Name System (DNS), DDNS, TELNET, EMAIL, File Transfer Protocol (FTP), WWW, HTTP, SNMP, Bluetooth, Firewalls, Basic concepts of Cryptography

Domain Name System

25.1 Name Space

Flat Name Space

Hierarchical Name Space

25-2 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

25.2 Domain Name Space

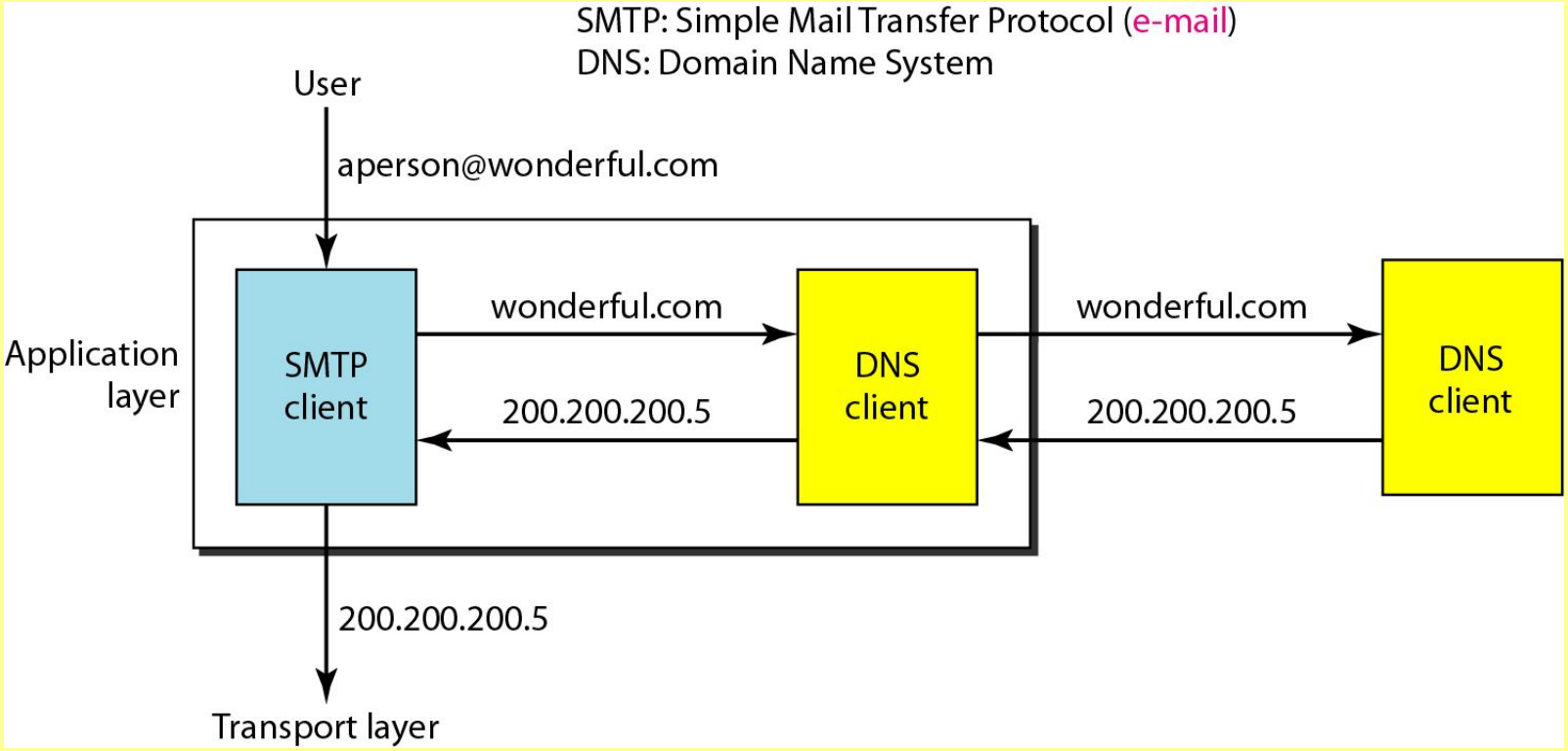


Figure 25.1 Domain name space

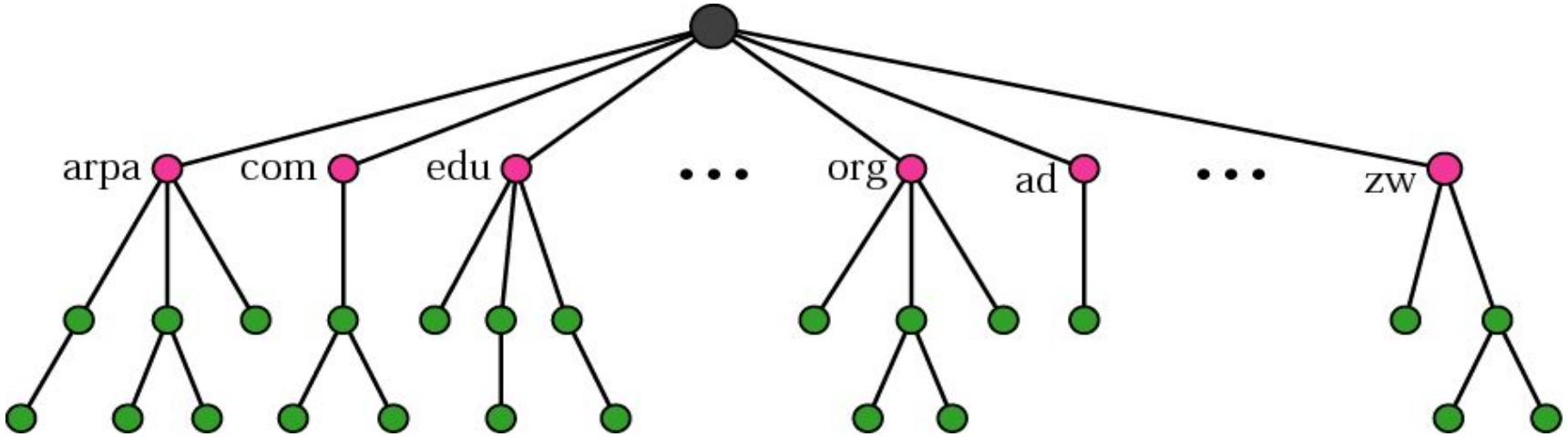


Figure 25.5 Hierarchy of name servers

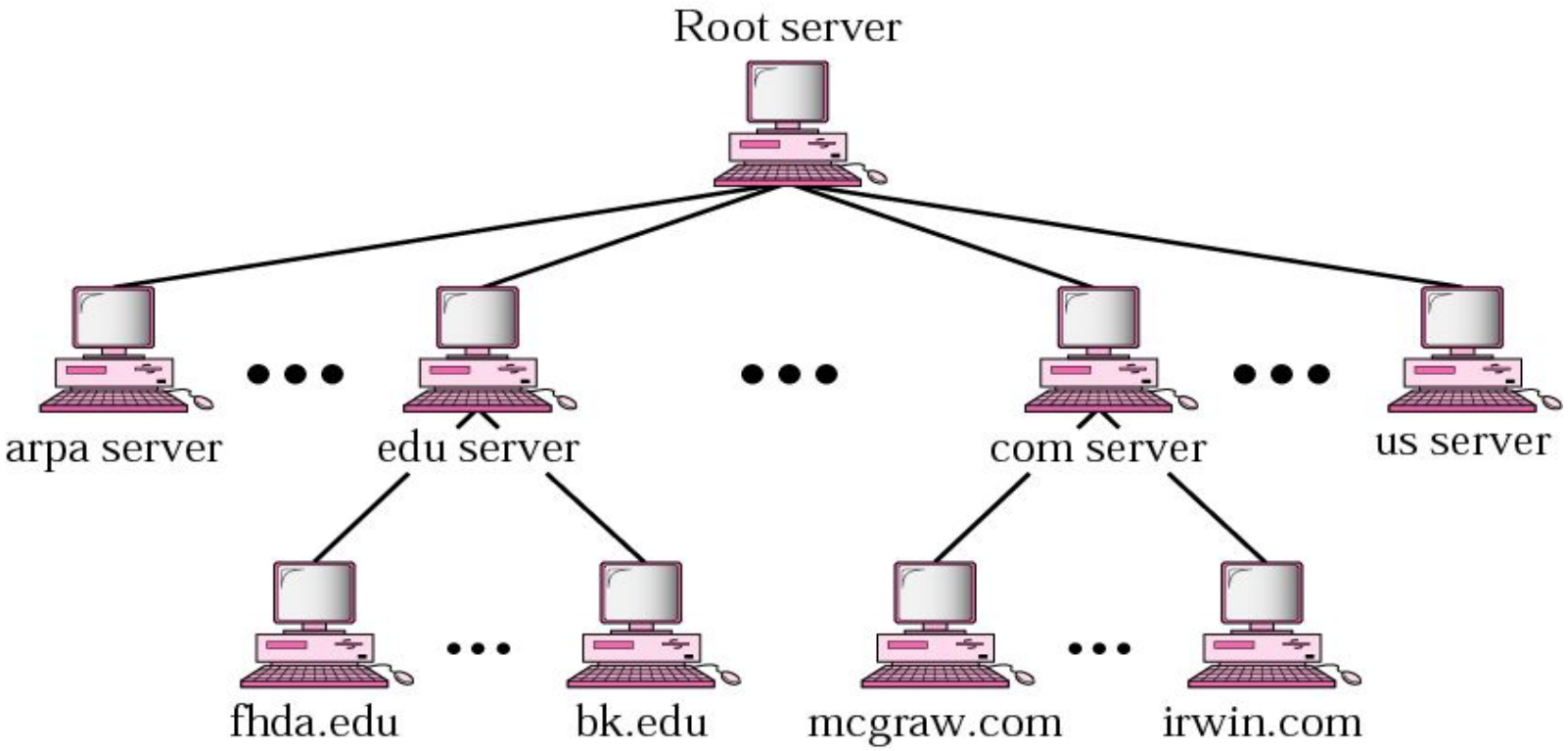


Figure 25.2 Domain names and labels

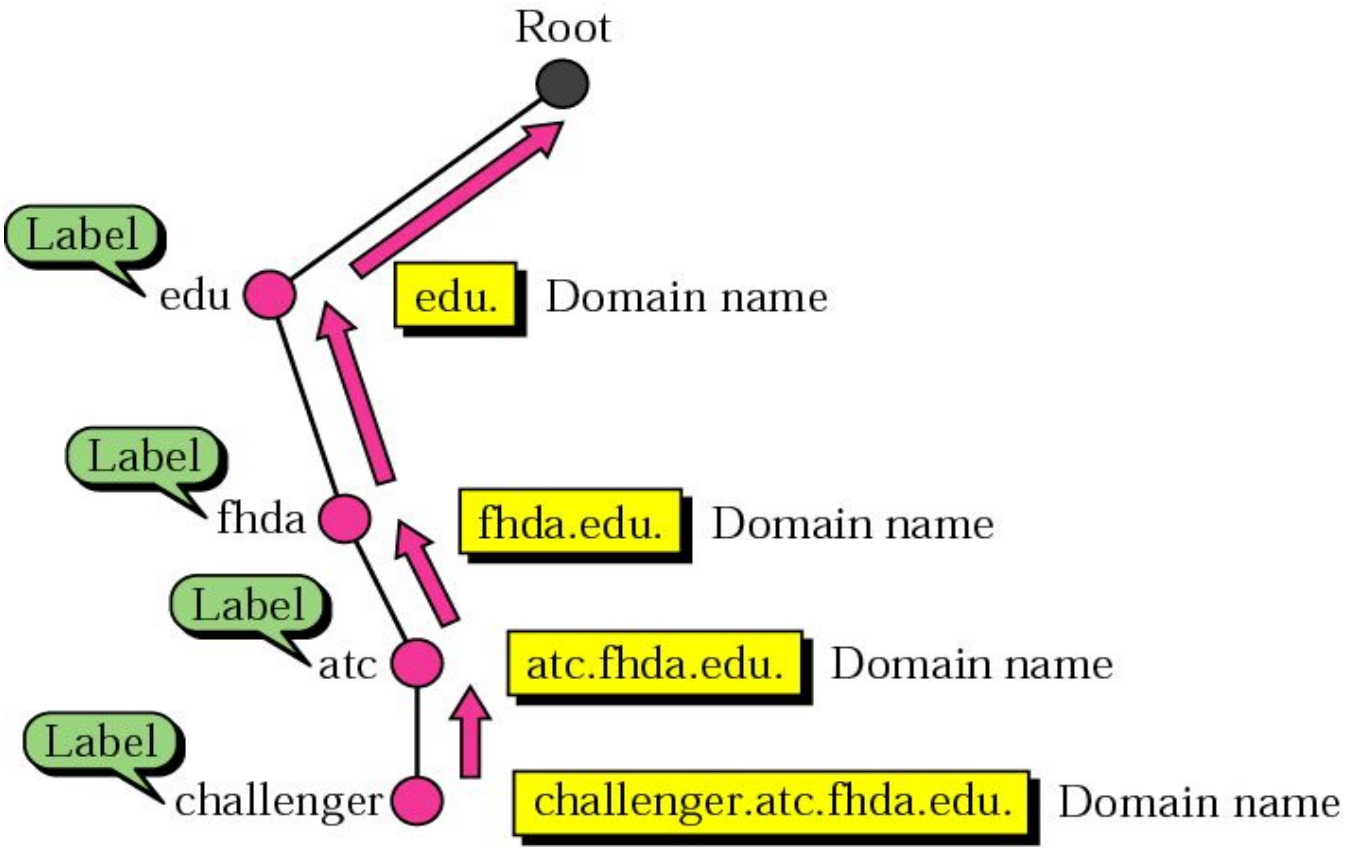
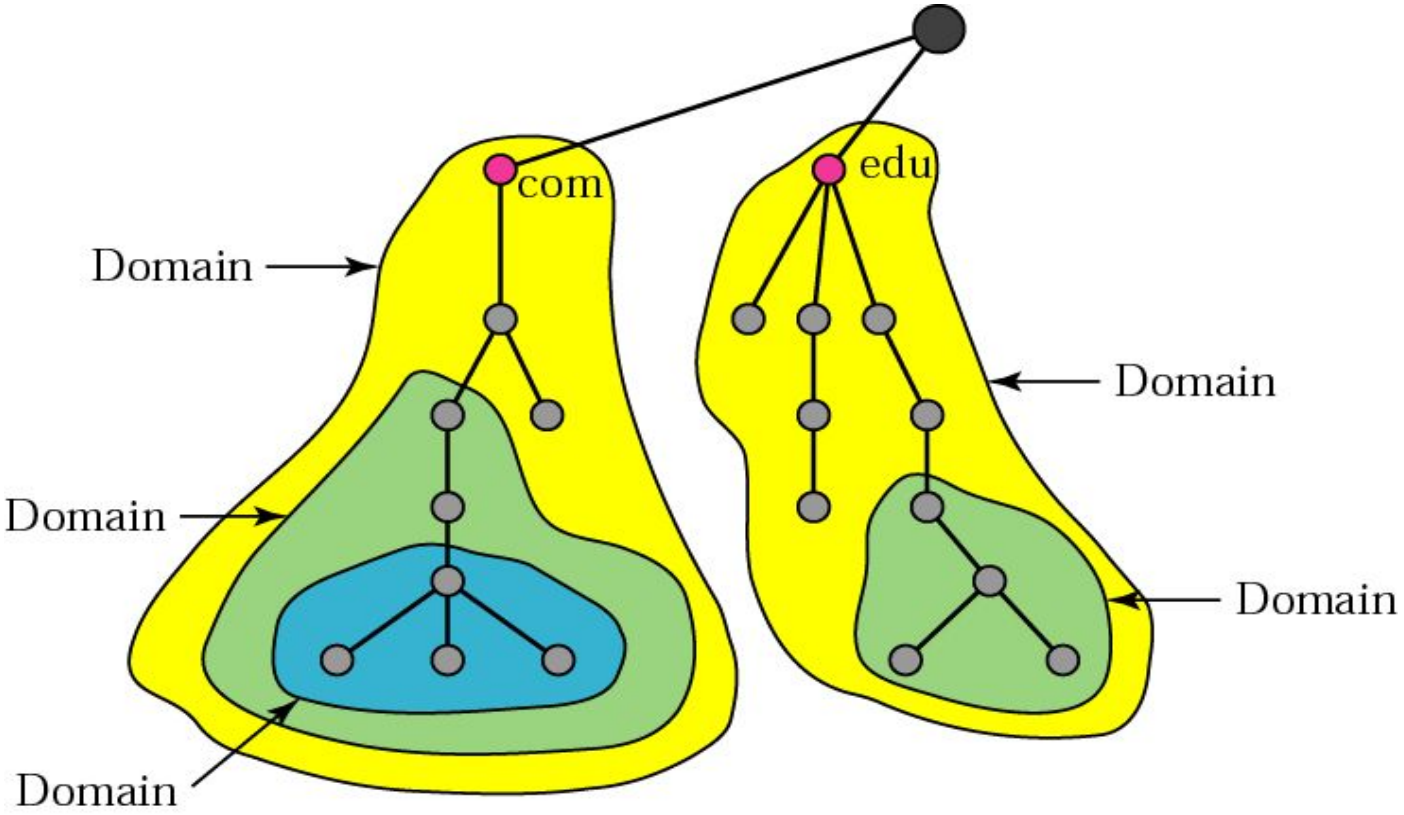


Figure 25.4 Domains



25.3 Distribution of Name Spaces

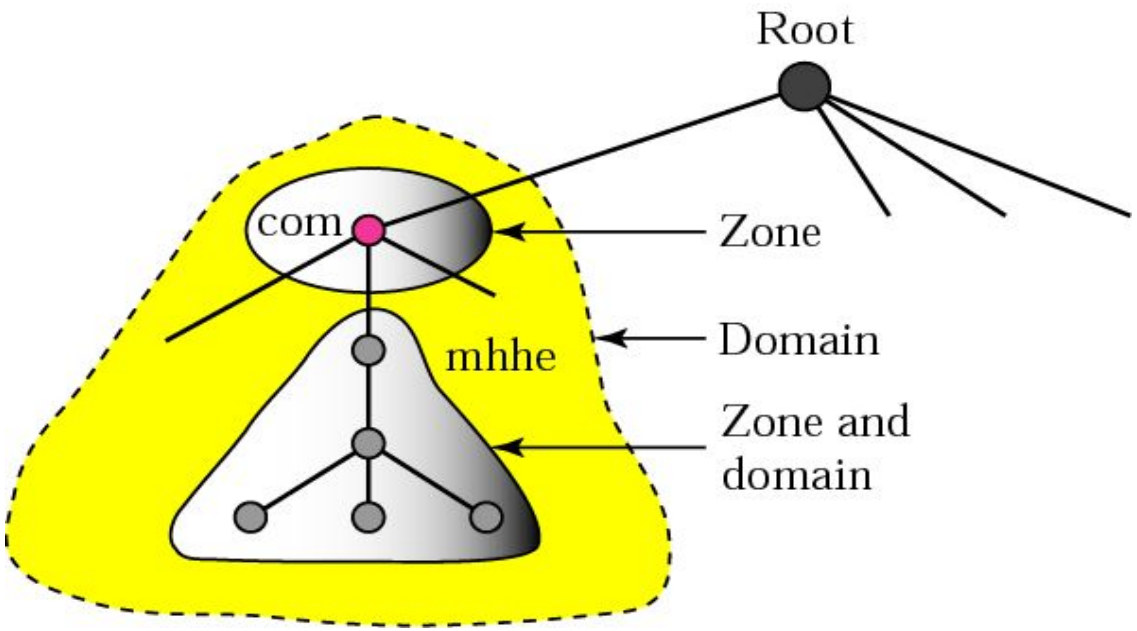
Hierarchy of Name Servers

Zone

Root Server

Primary and Secondary Servers

Figure 25.6 Zones and domains



25.4 DNS In The Internet

Generic Domain

Country Domain

Inverse Domain

Figure 25.7 DNS in the Internet

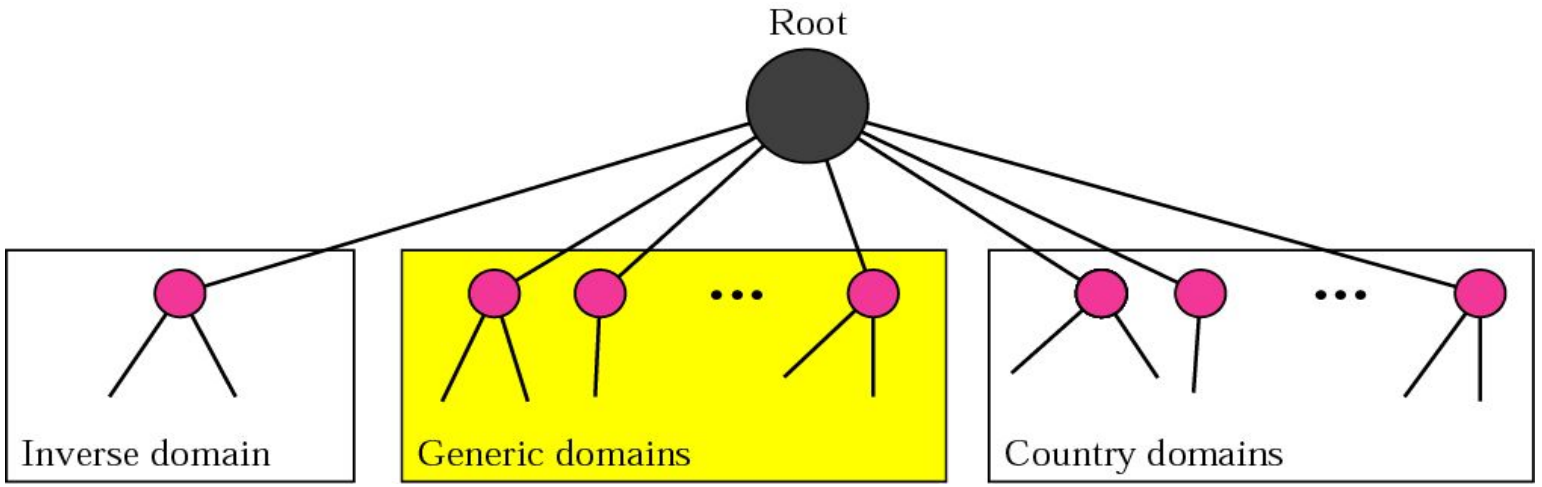


Figure 25.8 Generic domains

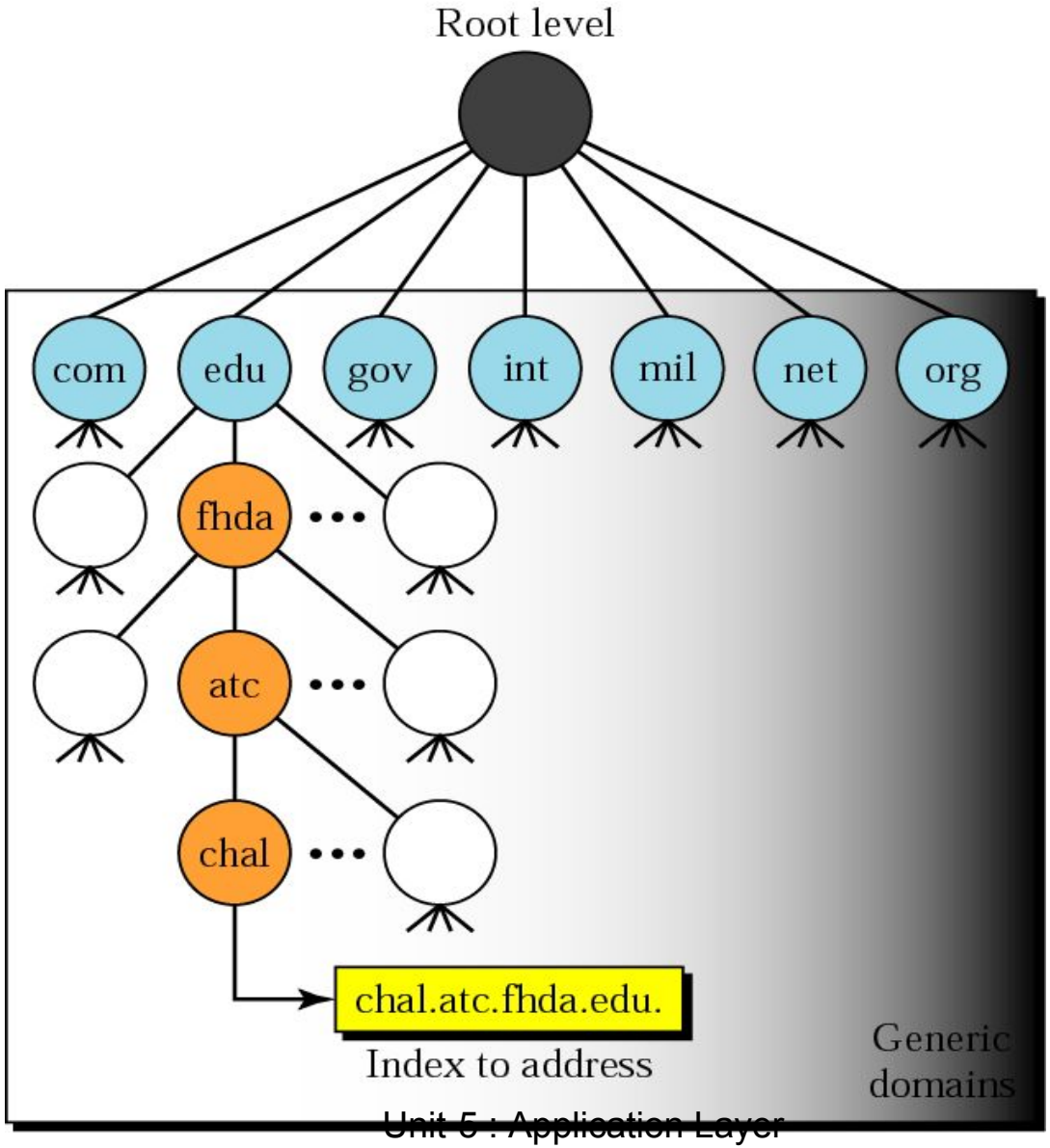
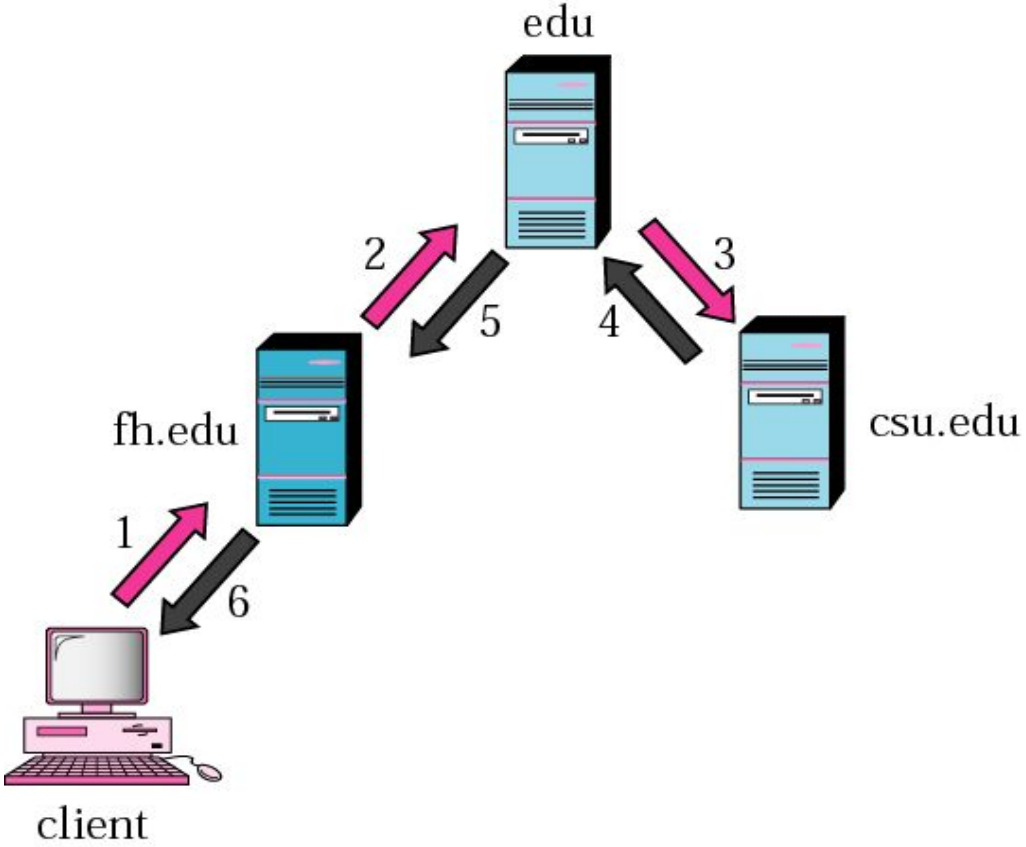


Table 25.1 Generic domain labels

Label	Description
com	Commercial organizations
edu	Educational institutions
gov	Government institutions
int	International organizations
mil	Military groups
net	Network support centers
org	Nonprofit organizations

Figure 25.11 Recursive resolution



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

SMTP and FTP

26.1 Electronic Mail

SMTP stands for Simple Mail Transfer Protocol.

It is a program used for sending messages to other computer users based on e-mail addresses.

Figure 26.2 Email address

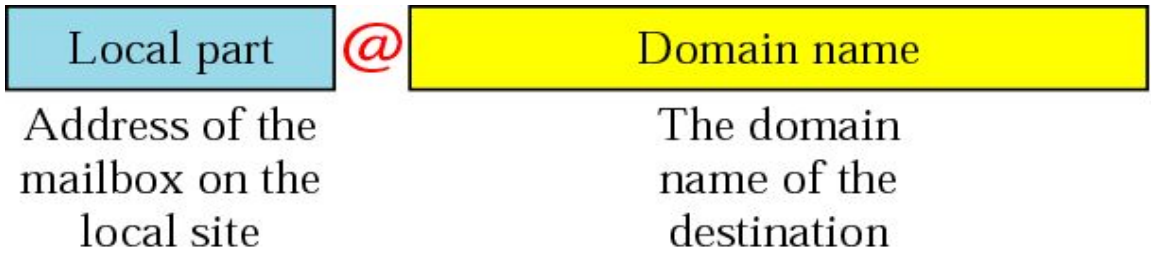


Figure 26.3 User agent

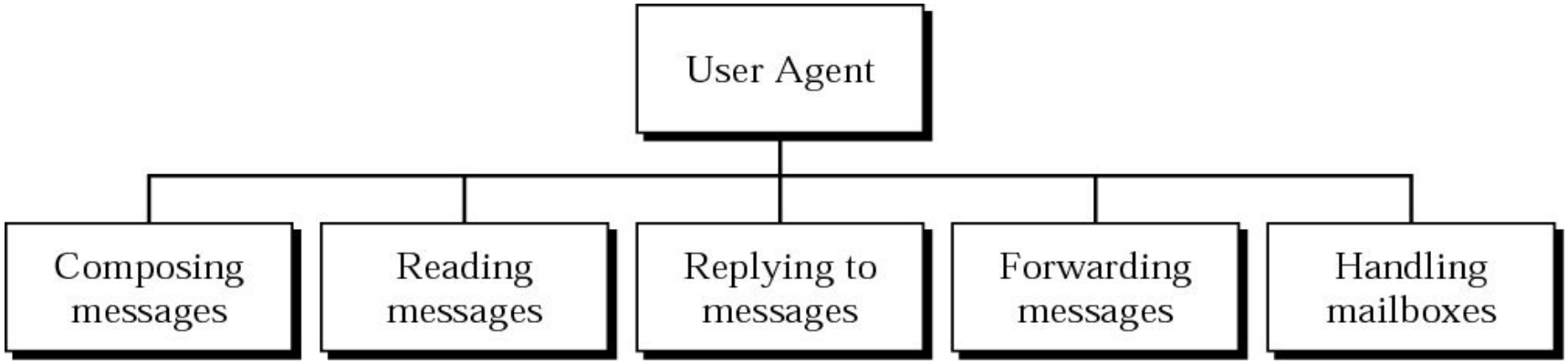


Figure 26.4 MIME

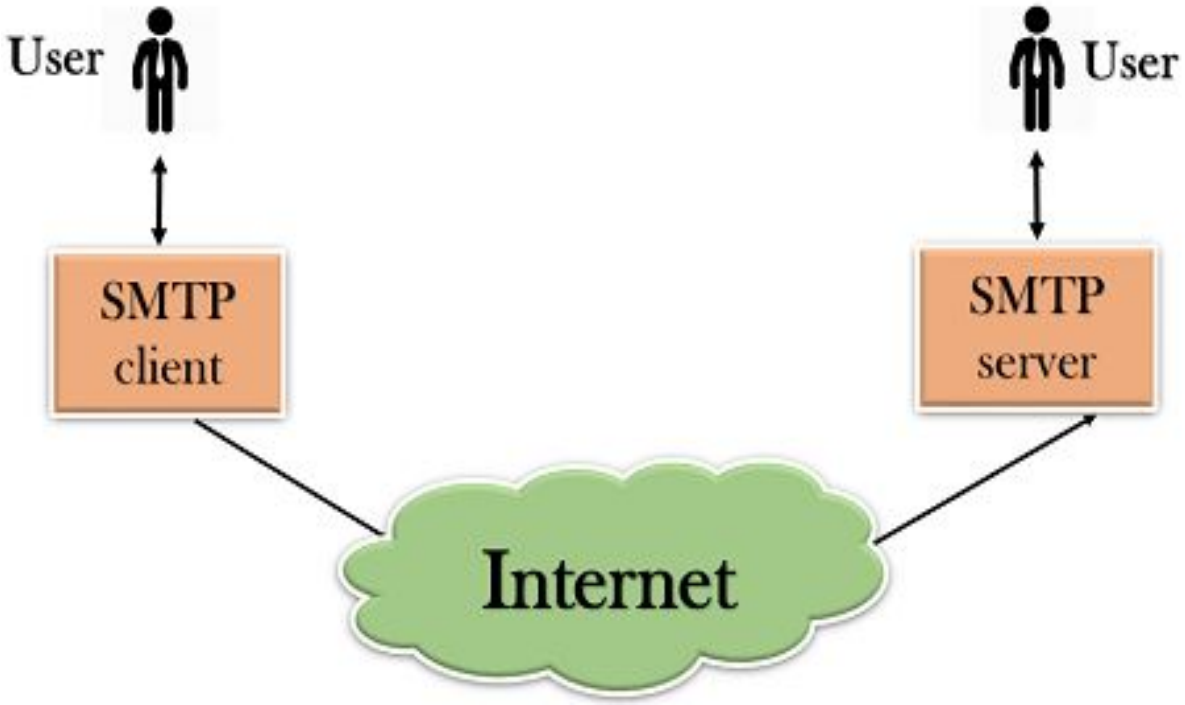


Figure 26.4 MIME

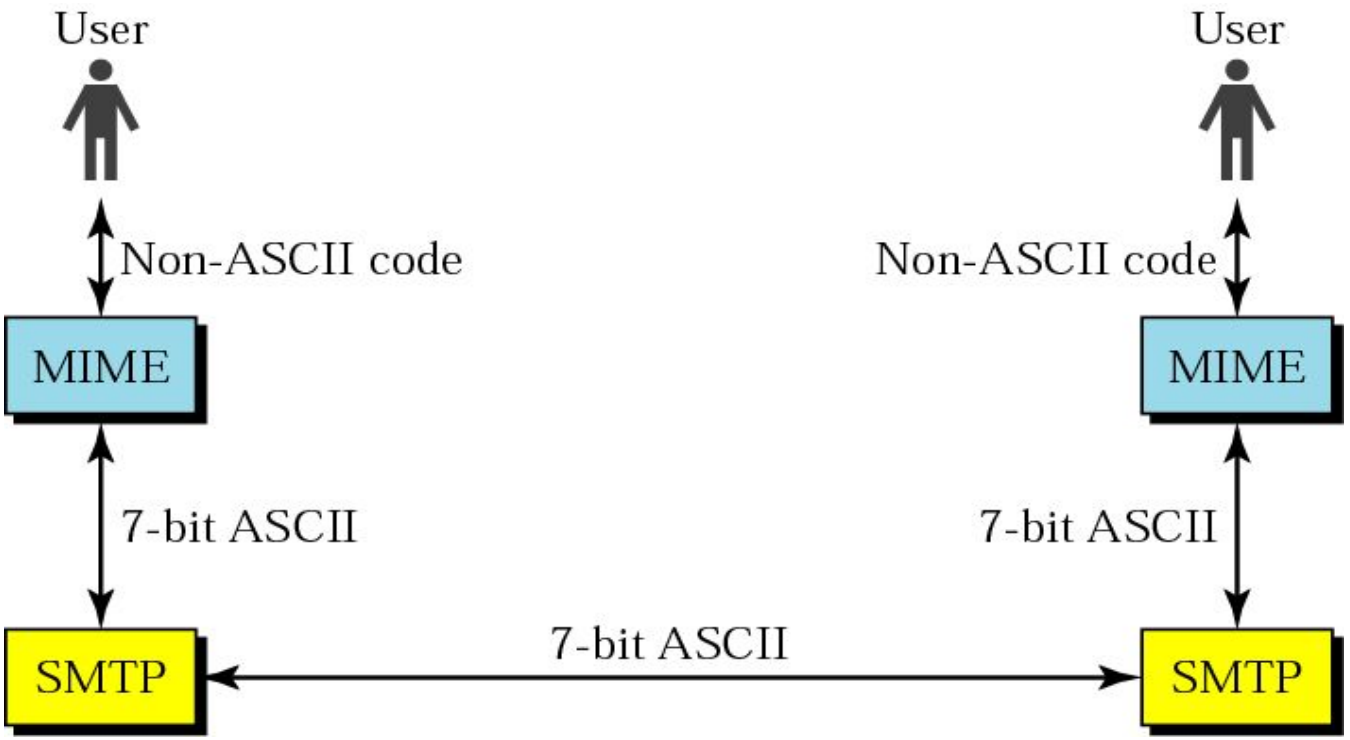


Figure 26.8 MTA client and server

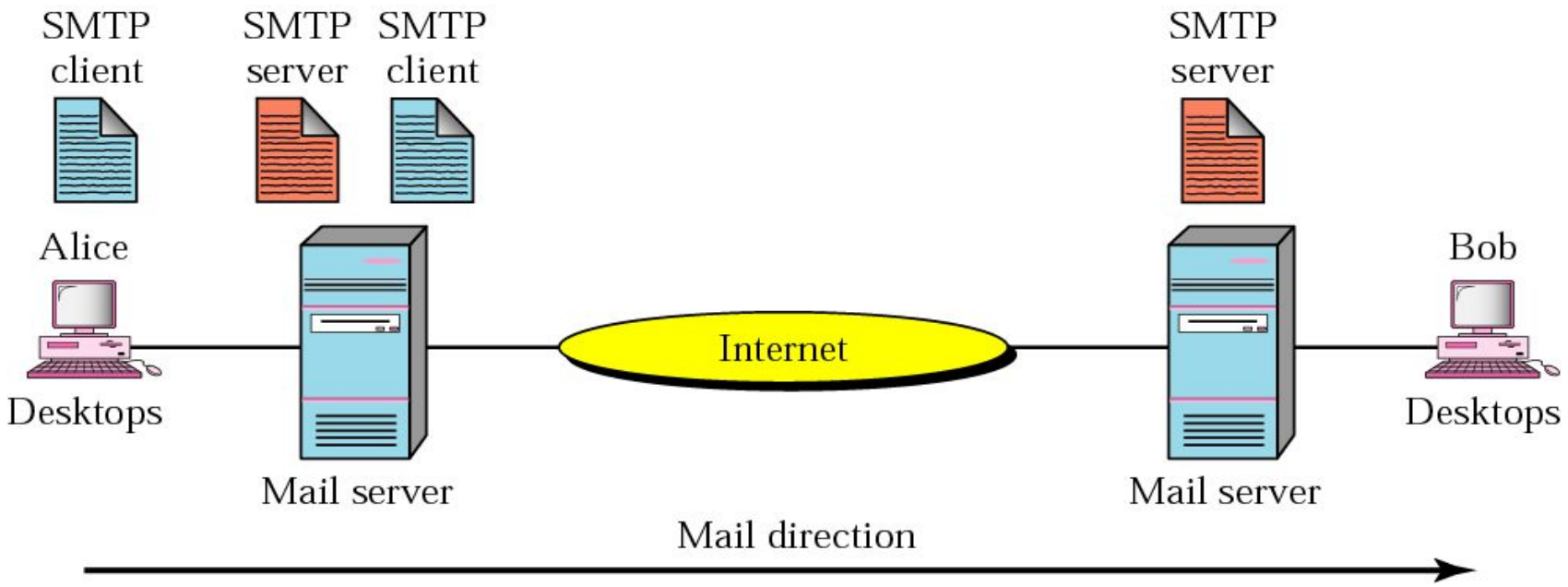


Figure 26.9 Commands and responses

The user agent (UA) prepares the message, creates the envelope and then puts the message in the envelope. The mail transfer agent (MTA) transfers this mail across the internet.

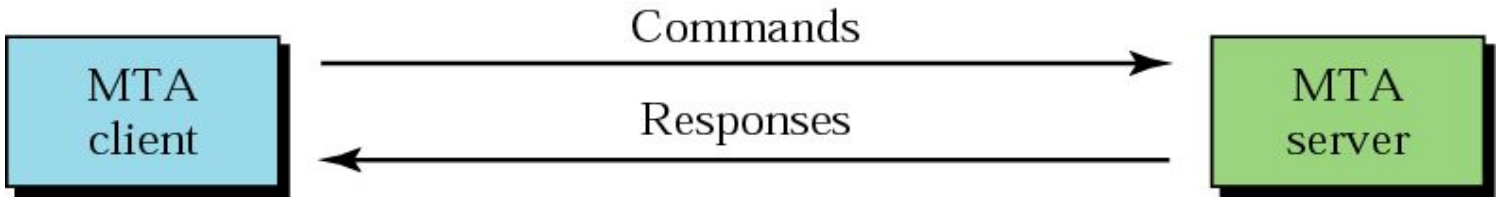
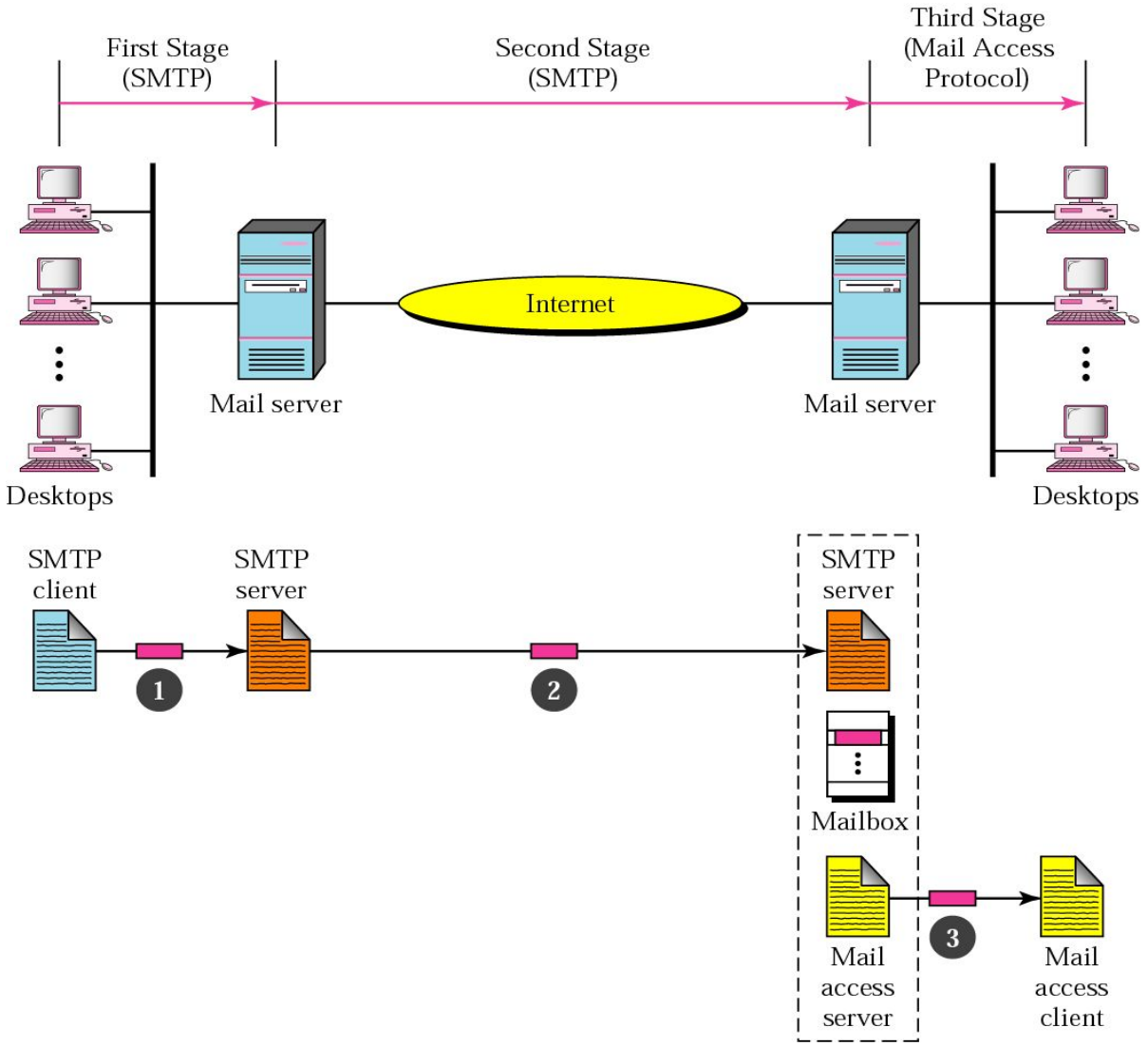


Figure 26.10 Email delivery



Post Office Protocol (POP):
It enables the clients to receive or download the emails from their remote mail server.

Internet Mail Access Protocol(IMAP):
IMAP allows the client program to manipulate the e-mail message on the server without downloading them on the local computer.

Post Office Protocol (POP):

POP allows you to read the mail only after downloading it.

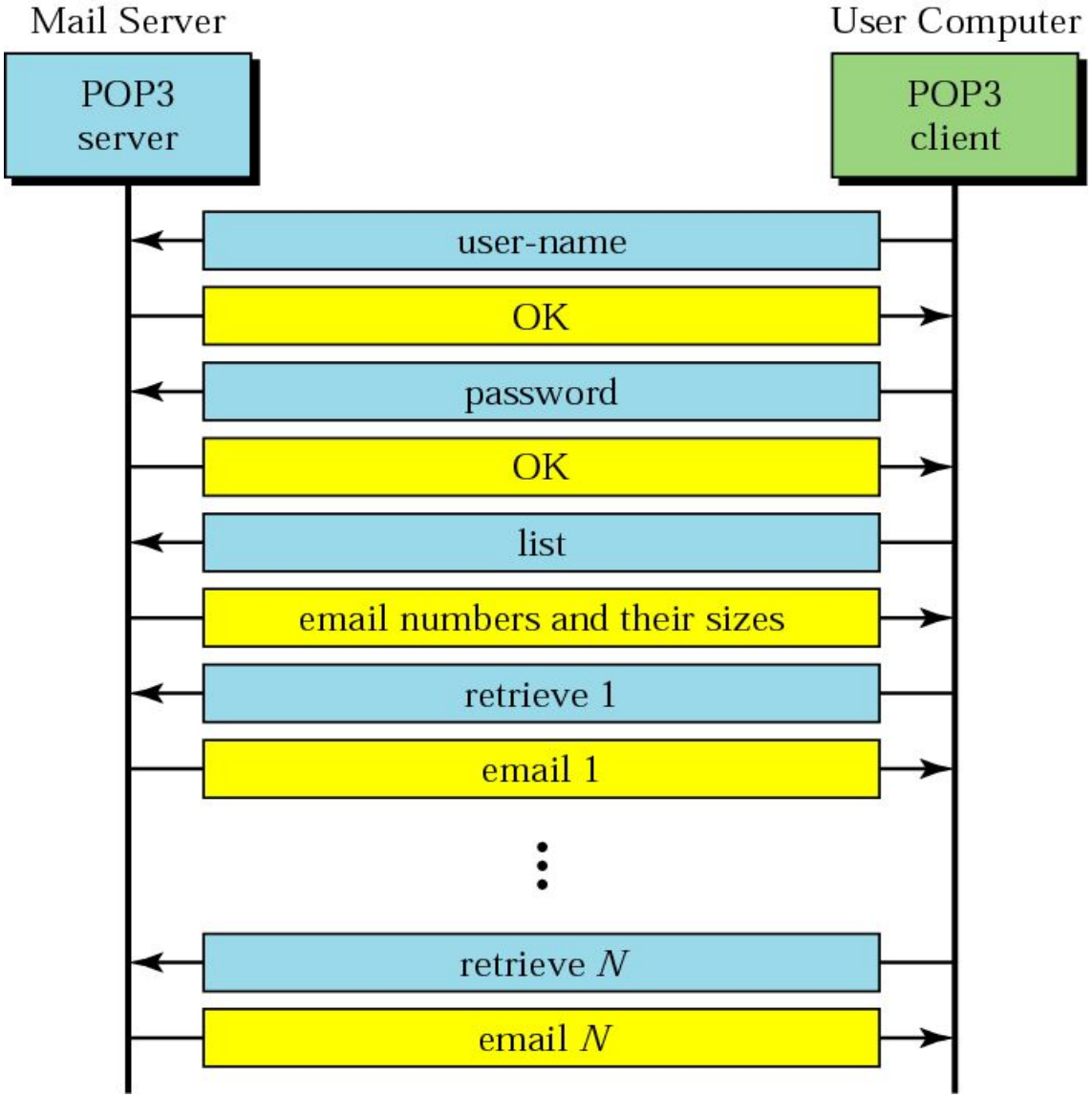
POP is a pull protocol.

Internet Mail Access Protocol(IMAP):

IMAP allows you to check the mail content before downloading.

So, with IMAP you can choose to download your messages or just delete them.

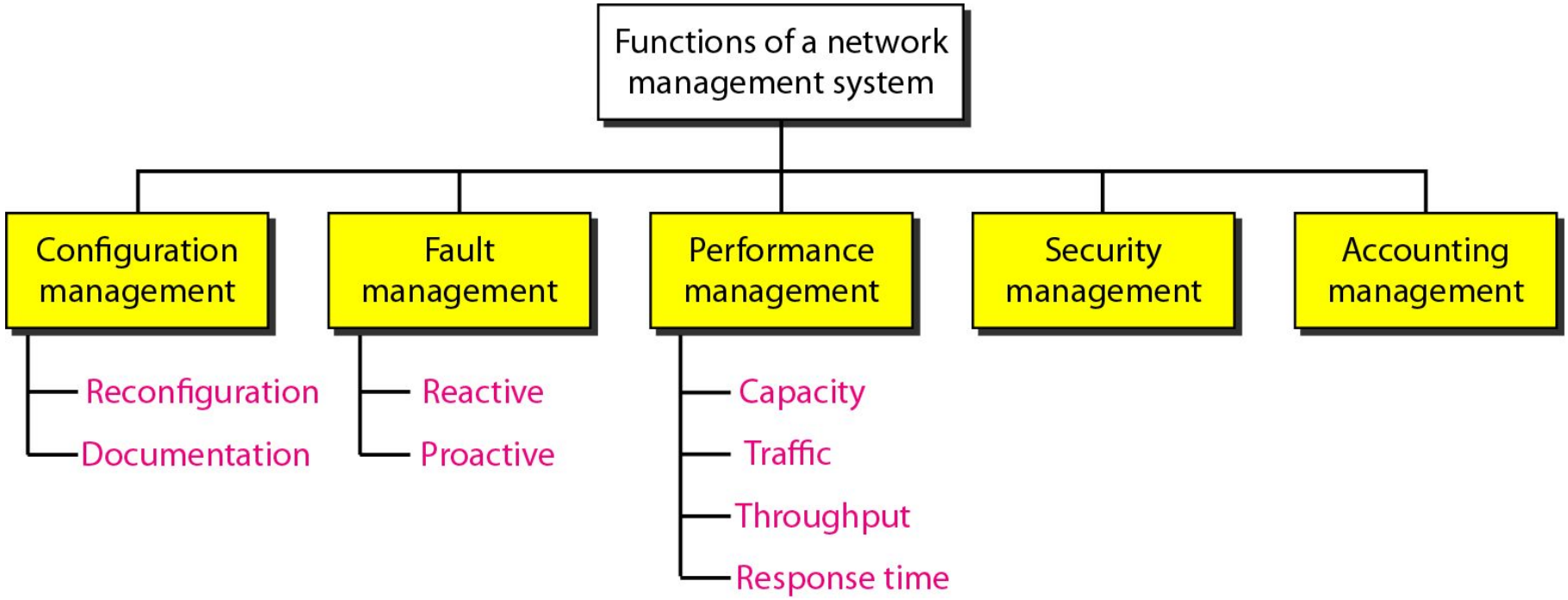
Figure 26.11 POP3



26.2 SNMP

Simple Network Management Protocol (SNMP) is an application-layer protocol used to manage and monitor network devices.

Functions of a network management system



26.2 Telnet

Telnet is an abbreviation for **Terminal Network**.
The user access any application program on a remote computer.
Telnet provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side.

26.2 File Transfer

Connections

Communication

File Transfer

User Interface

Anonymous

26.2 File Transfer

FTP is short for **File Transfer Protocol**.

It is used for exchanging files over the internet.
It enables the users to upload and download the files from the internet.

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 is used for the data connection.

Figure 26.12 FTP

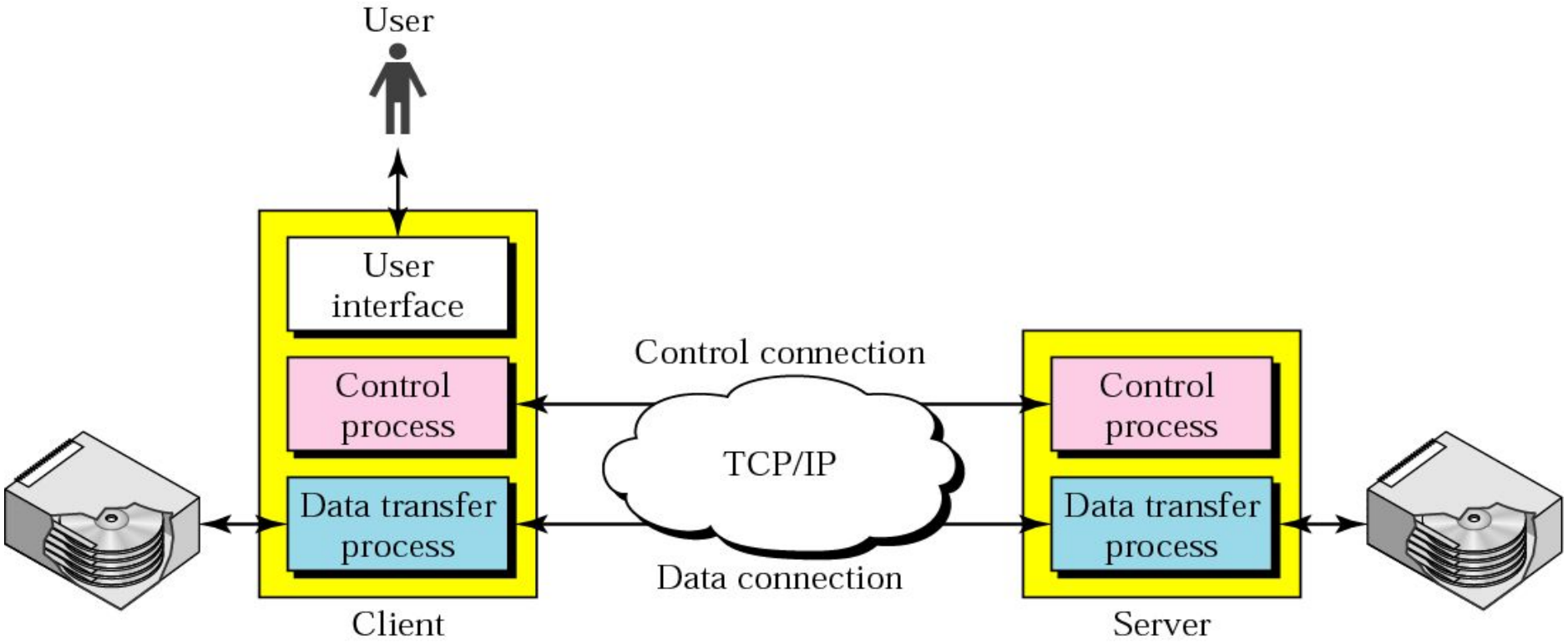


Figure 26.14 Using the data connection

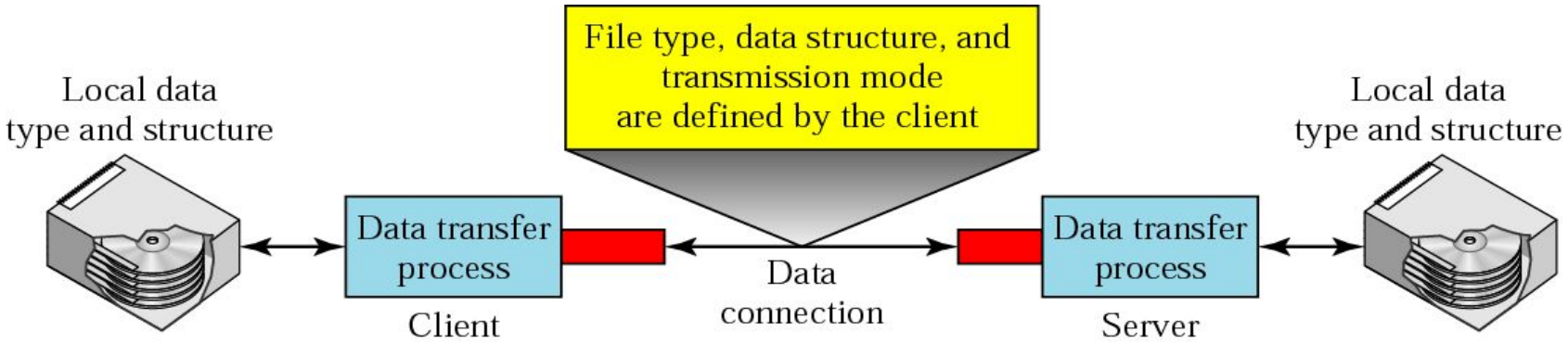
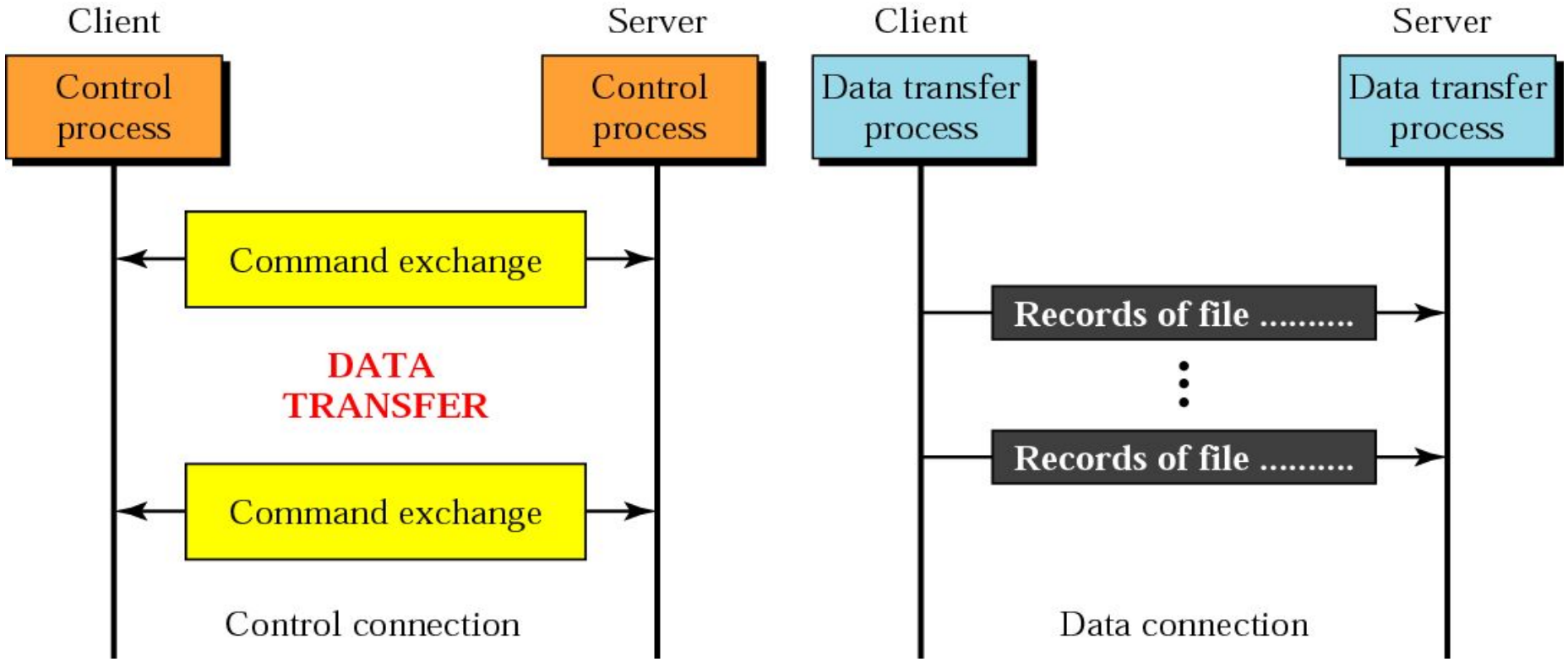


Figure 26.16 Example 1



HTTP and WWW

27.1 HTTP

HTTP is a stateless protocol.
HTTP server does not maintain any state.
It forgets about the client after sending the response.
It treats every new request independently.

27.1 HTTP

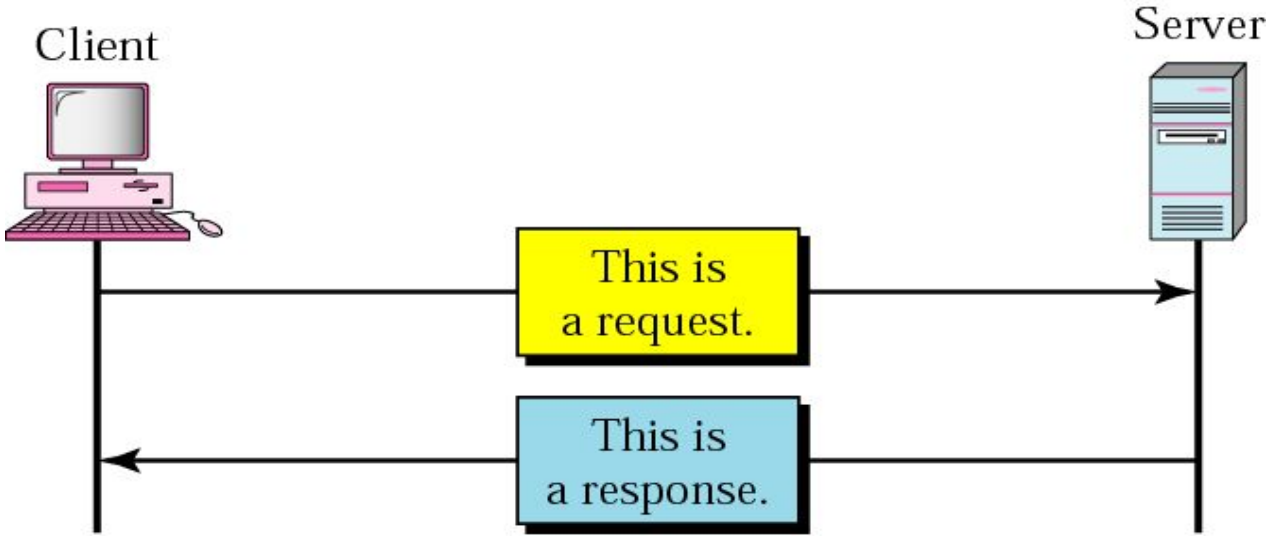
HTTP is short for **Hyper Text Transfer Protocol**

HTTP uses a client-server model

Non-persistent HTTP connection is one that is used for serving exactly one request and sending one response.

Persistent HTTP connection is one that can be used for serving multiple requests.

Figure 27.1 HTTP transaction



27.1 HTTP

Transaction

Request Message

Response Message

Headers

HTTP uses the services of TCP on well-known port 80.

Figure 27.3 Request line

Figure 27.4 URL

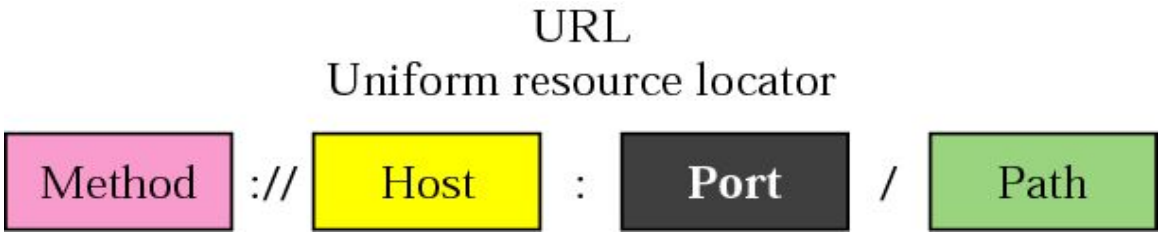
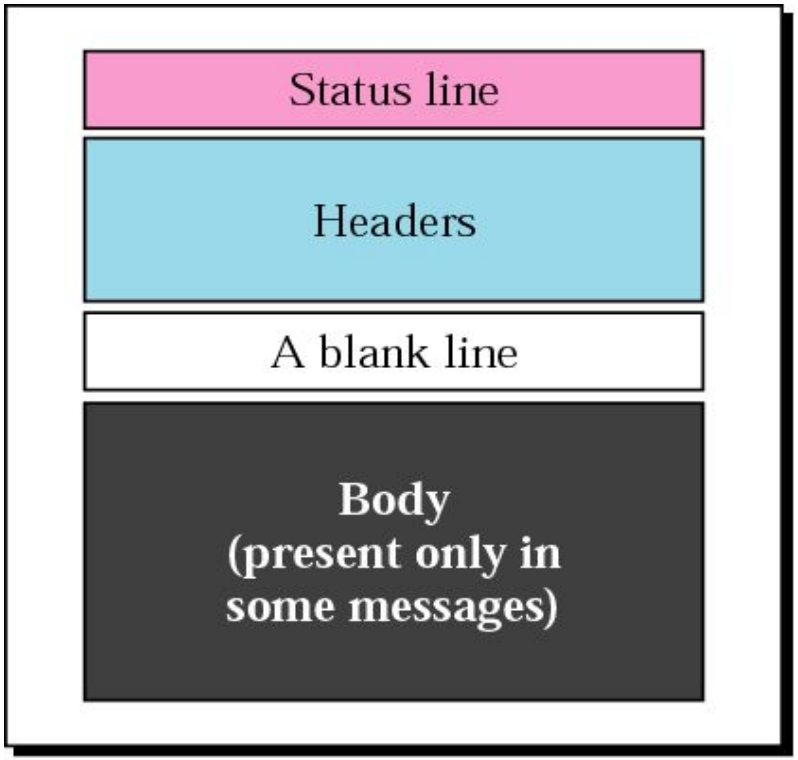


Figure 27.5 Response message



Response message

Figure 27.11 Distributed services

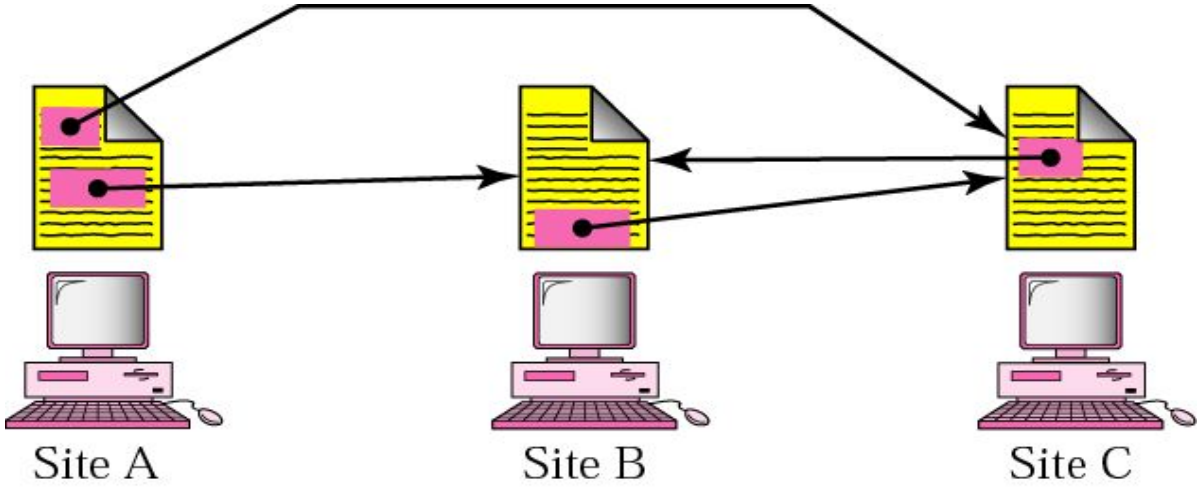
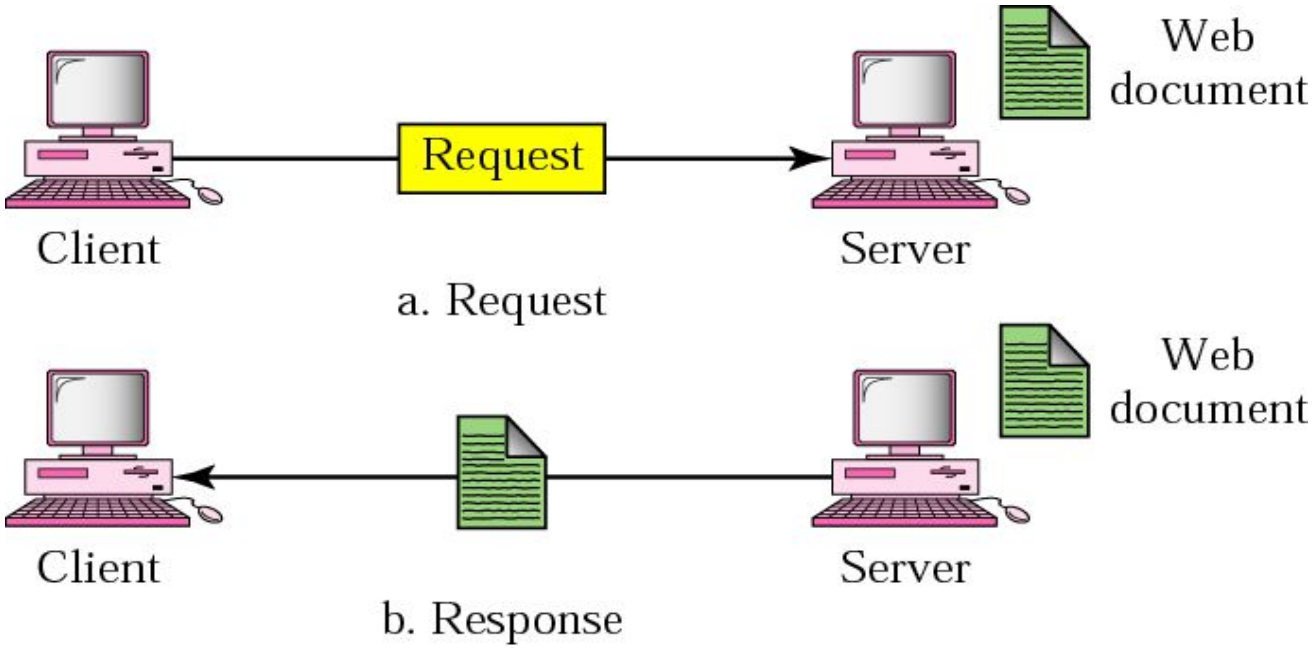


Figure 27.15 Static document



27.1 Firewall

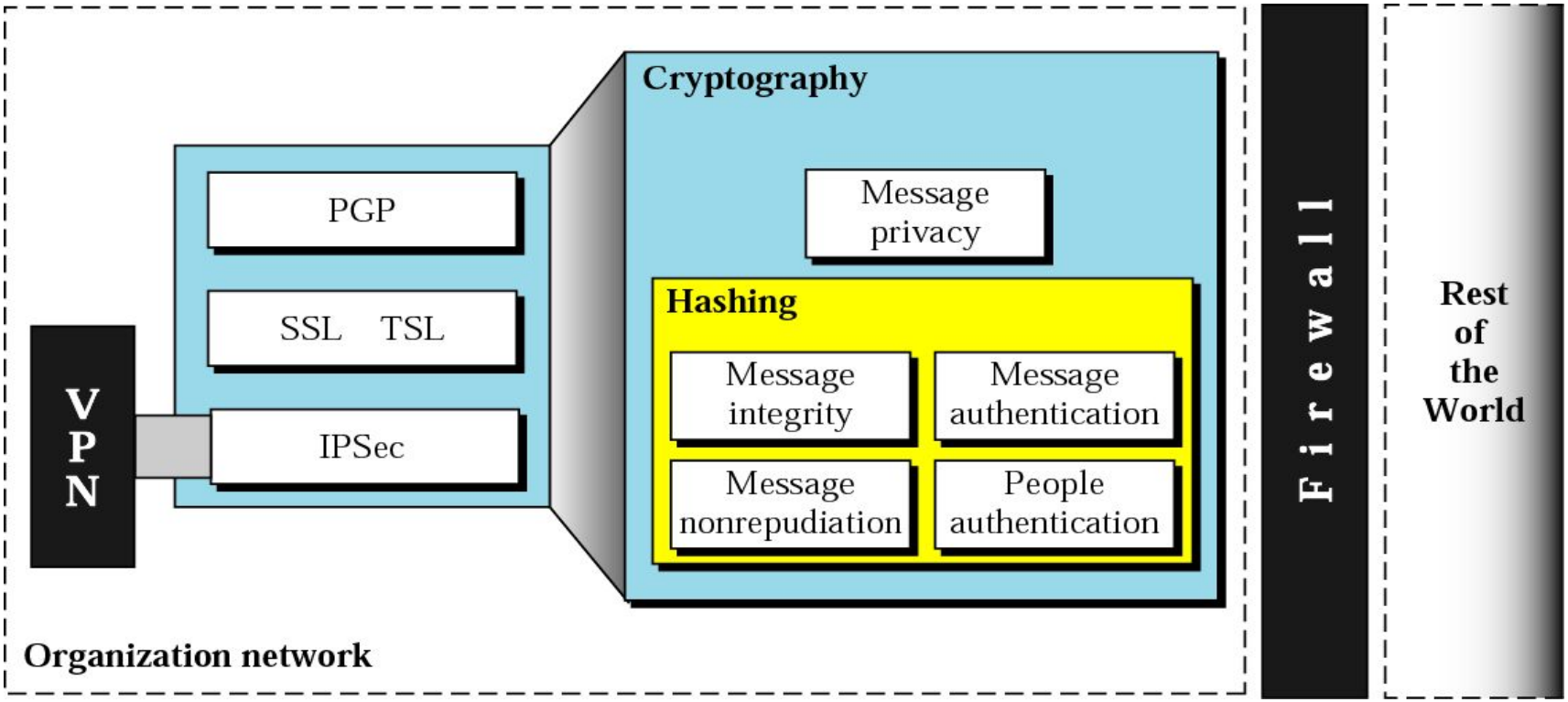
A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

A *firewall* is a network security system designed to prevent unauthorized access

Accept : allow the traffic

Reject : block the traffic but reply with an "unreachable error"

Security Topics



Cryptography

29.1 Introduction

Introduction to Cryptography

Figure 29.1 Cryptography components

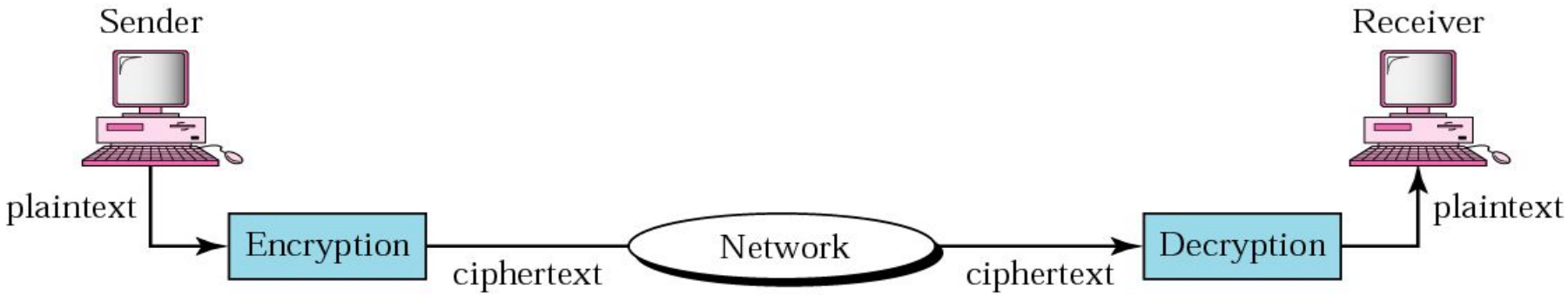
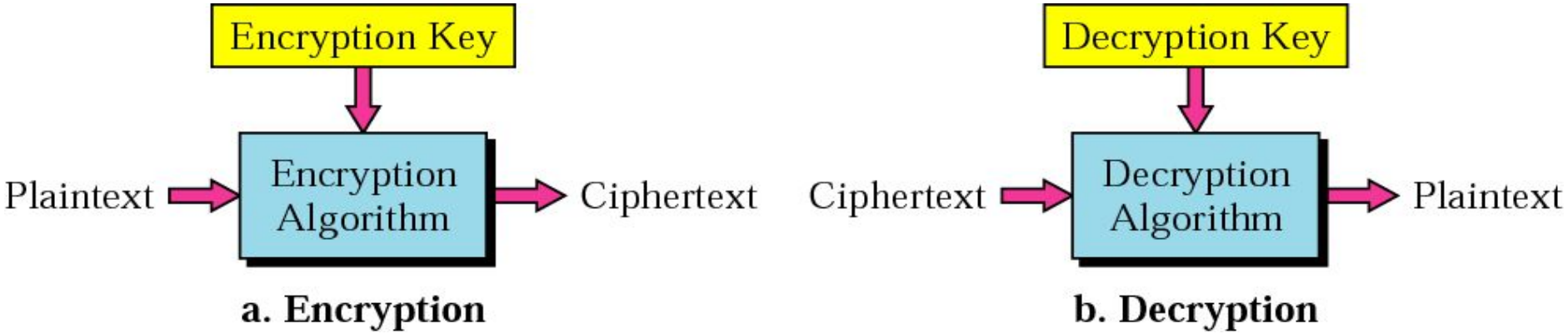
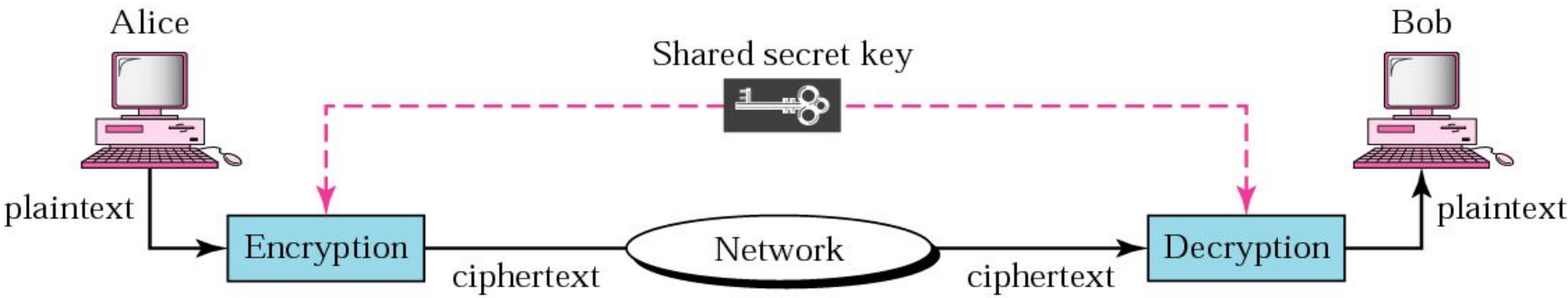


Figure 29.2 Encryption and decryption



In cryptography, the encryption/decryption algorithms are public; the keys are secret.

Figure 29.3 Symmetric-key cryptography



In symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.

Note:

In symmetric-key cryptography, the same key is used in both directions.

Symmetric-key cryptography is often used for long messages.

Figure 29.4 Caesar cipher

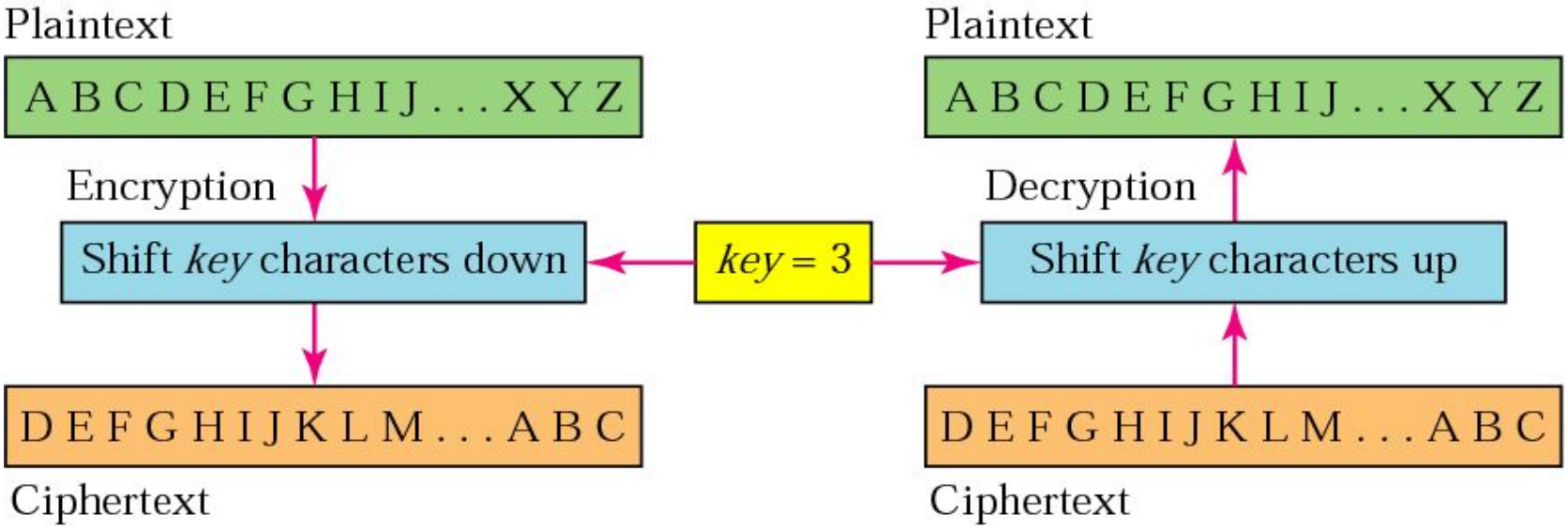


Figure 29.5 Example of monoalphabetic substitution

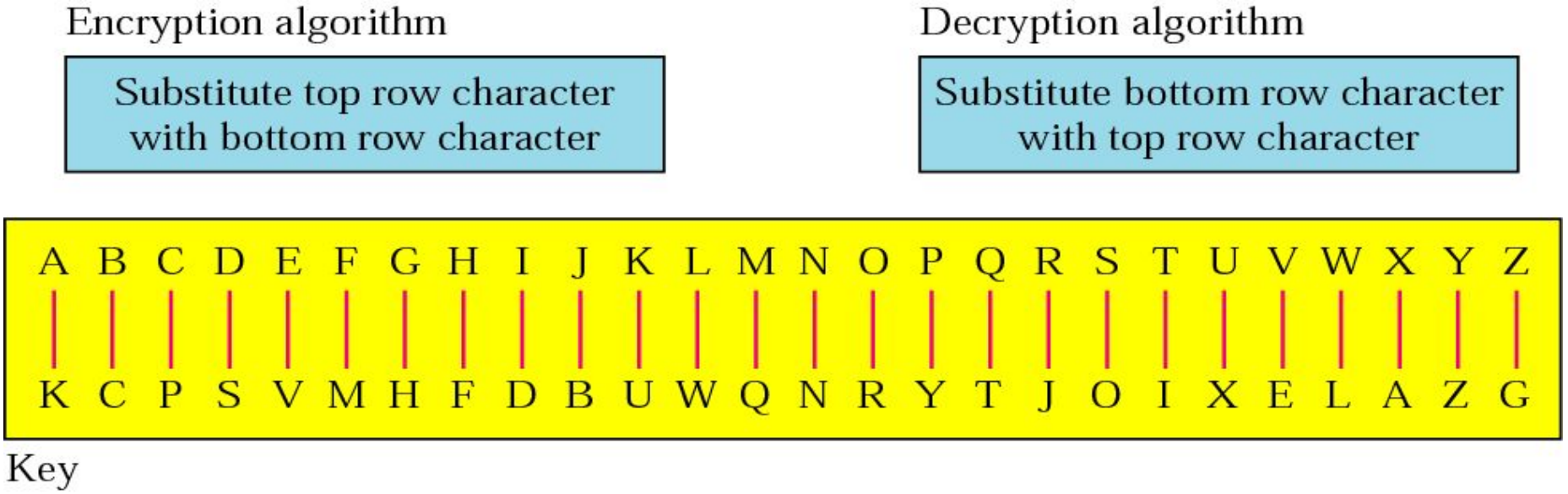


Figure 29.8 Block cipher

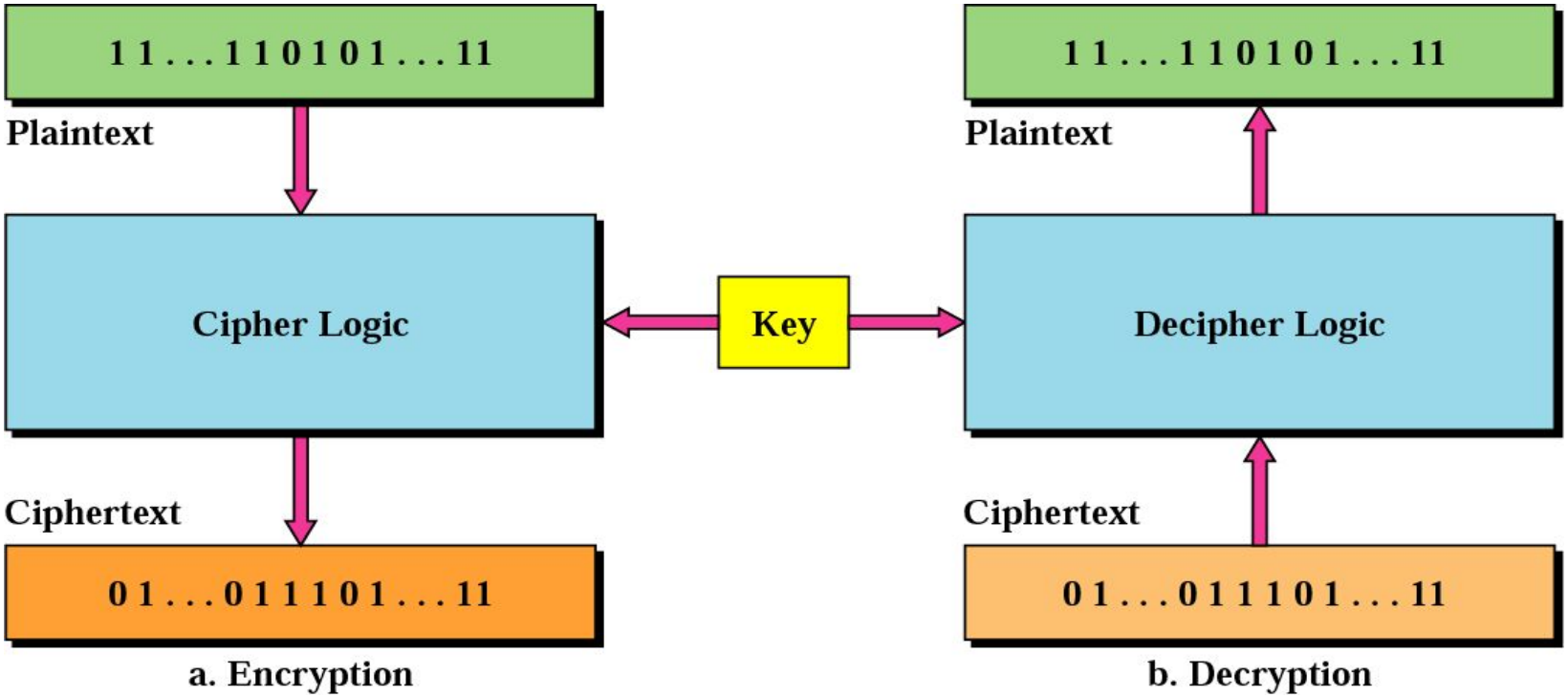


Figure 29.16 ECB mode

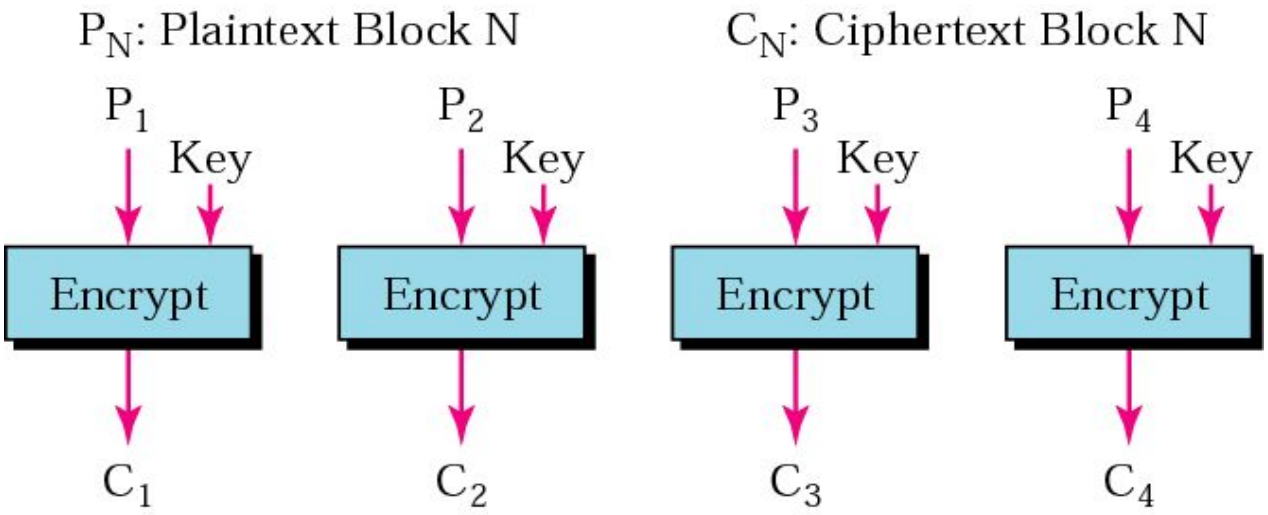


Figure 29.17 CBC mode

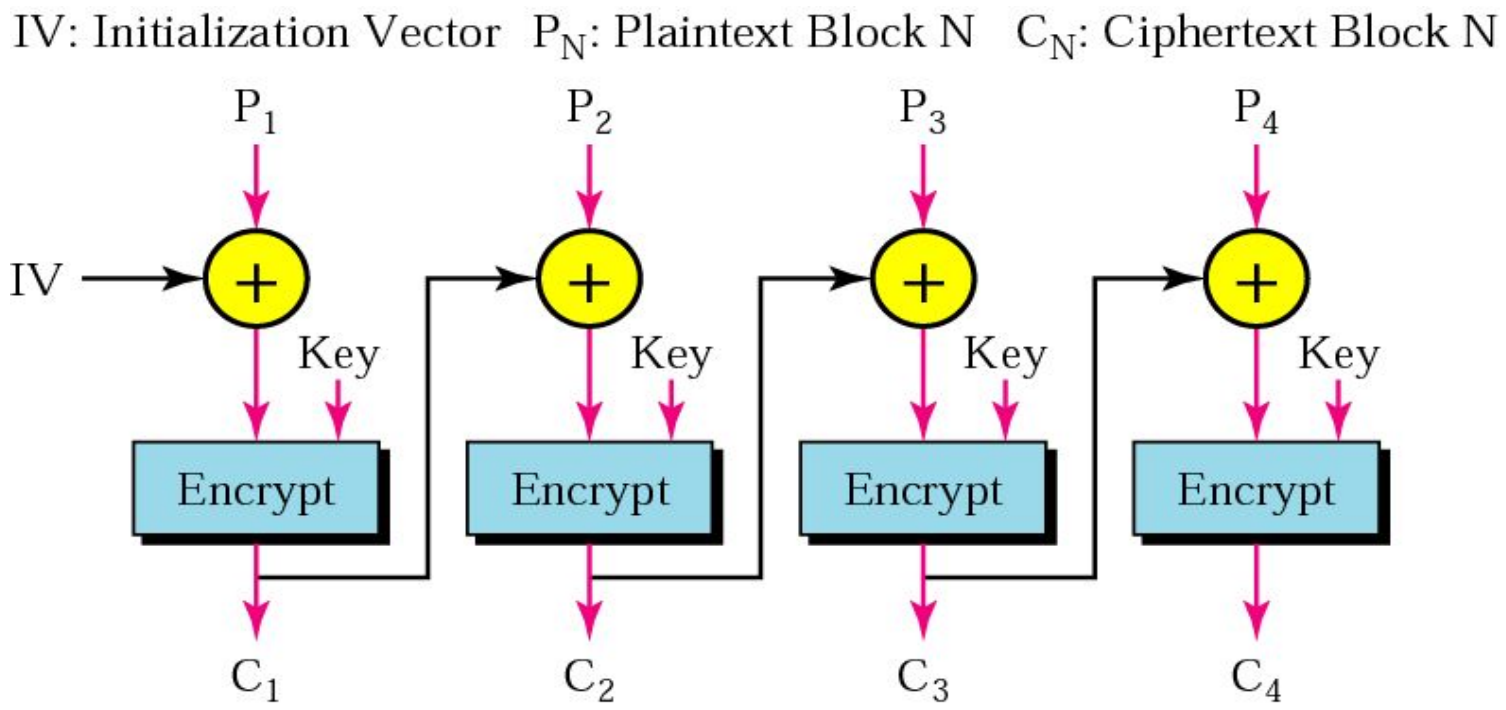
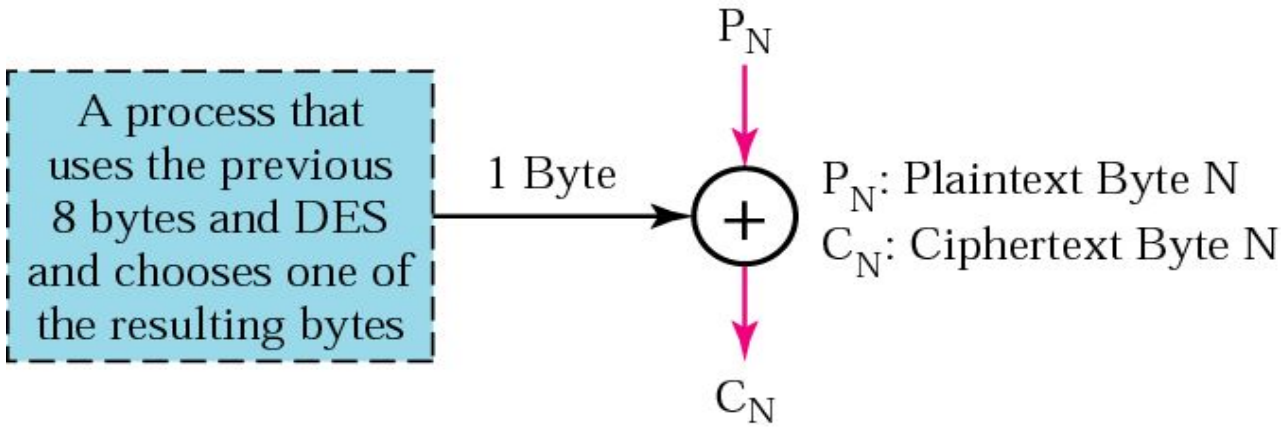


Figure 29.18 CFM

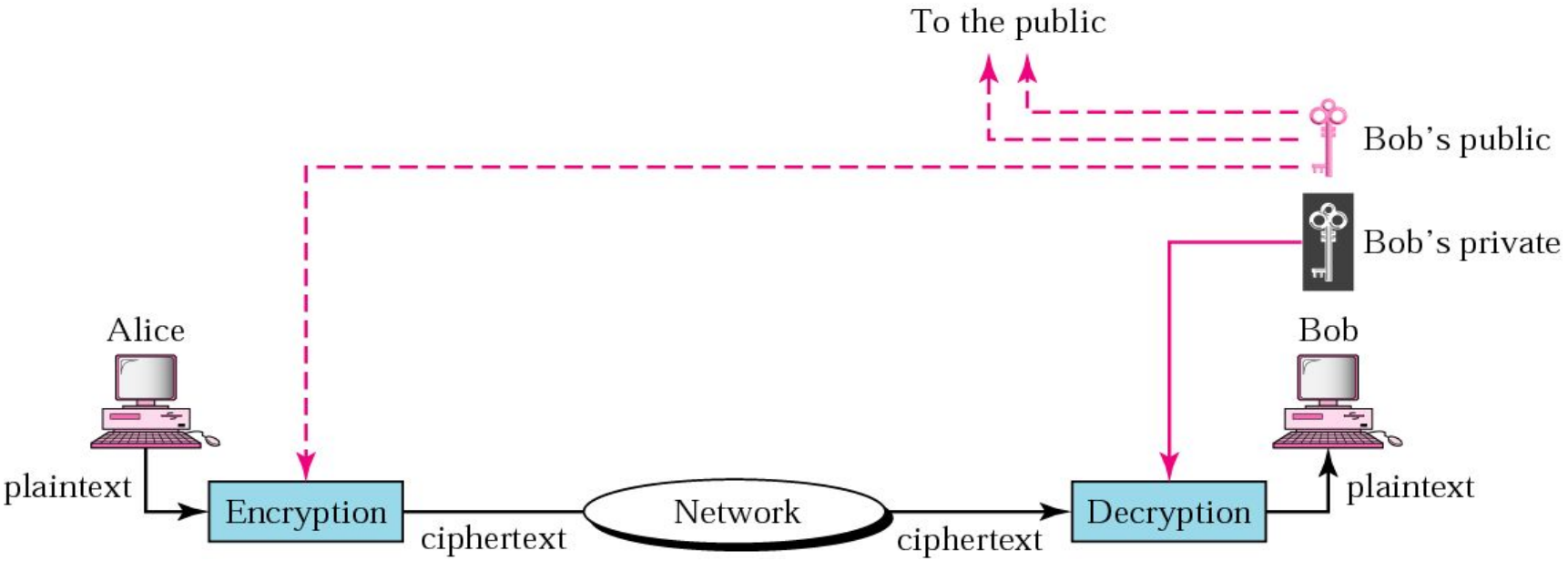


29.3 Public-Key Cryptography

RSA

Choosing Public and Private Keys

Figure 29.20 Public-key cryptography



Public-key algorithms are more efficient for short messages.