

## Chapter 26: Objective

The first section introduces the World Wide Web. It then discusses the HyperText Transfer Protocol, the most common client-server application program used in relation to the World Wide Web. The second section discusses the File Transfer Protocol which is the standard protocol provided by TCP/IP for copying a file from one host to another.

القسم الأول يقدم الشبكة العالمية. بعد ذلك يناقش بروتوكول نقل النص التشعبي، أكثر من غيرها المشتركة تطبيق العميل خادم التطبيق المستخدمة فيما يتعلق الشبكة العالمية.

ويناقش القسم الثاني بروتوكول نقل الملفات، وهو البروتوكول المعياري المقدم من قبل

The third section discusses electronic mail, which involves two protocols: SMTP and POP. As we will see, the nature of this application is different from the other two previous applications. We need two different protocols to handle electronic mail.

يناقش القسم الثالث البريد الإلكتروني، الذي يتضمن بروتوكولين: سمبت و بوب. كما سنرى، وطبيعة هذا التطبيق يختلف عن اثنين من التطبيقات السابقة الأخرى. نحن بحاجة إلى بروتوكولات مختلفة للتعامل معها بريد إلكتروني

The fourth section discusses TELNET, a general client-server program that allows users to log in to a remote

machine and use any application available on the remote host.

The fifth section discusses Secure Shell, which can be used as a secured TELNET, but it can also provide a secure tunnel for other applications.

القسم الرابع يناقش تيلنيت، وهو برنامج عميل للعميل الذي يسمح للمستخدمين بتسجيل الدخول إلى جهاز التحكم عن بعد آلة واستخدام أي تطبيق متاح على المضيف البعيد.

القسم الخامس يناقش سيكور شل، والتي يمكن استخدامها ك تيلنيت مضمونة، ولكنها يمكن أن توفر أيضا نفق آمن للتطبيقات الأخرى

The sixth section talks about the Domain Name System which acts as the directory system in the Internet. It maps the name of an entity to its IP address.

ويتناول القسم السادس نظام أسماء النطاقات، الذي يعمل بمثابة نظام الدليل في الإنترنت. فإنه يخطط اسم كيان إلى عنوان إب الخاص به.

### 1-26 WORLD WIDE WEB AND HTTP

World Wide Web (abbreviated WWW or Web)

Hyper-Text Transfer Protocol (HTTP), is the most common client-server application program used in relation to the Web.

الشبكة العالمية (مختصر ووو أو ويب)  
بروتوكول نقل النص فرط (هتت)، هو برنامج تطبيق خادم العميل الأكثر شيوعا المستخدمة فيما يتعلق بالويب

## 26.26.1 World Wide Web

The idea of the Web was first proposed by Tim Berners-Lee in 1989 at CERN, the European Organization for Nuclear Research, to allow several researchers at different locations throughout Europe to access each others' researches. The commercial Web started in the early 1990s

واقترح تيم فكرة الفكرة الأولى بيرنرز لي في عام ١٩٨٩ في سيرن، الأوروبي منظمة البحوث النووية، للسماح لعدة الباحثين في مواقع مختلفة في جميع أنحاء أوروبا للوصول إلى أبحاث بعضهم البعض. الشبكة التجارية التي بدأت في أوائل التسعينات

The Web today is a repository of information in which the documents, called web pages, are distributed all over the world and related documents are linked together

ويب هو اليوم مستودع للمعلومات التي يتم توزيع الوثائق، ودعا صفحات الويب، في جميع أنحاء العالم وترتبط الوثائق ذات الصلة معا

## World Wide Web Architecture

هندسة الشبكة العالمية

The WWW today is a distributed client-server service, in which a client using a browser can access a service using a server

The service provided is distributed over many locations called sites

Each site holds one or more web pages. Each web page can contain some links to other web pages in the same or other sites

\*Simple web page has no links to other web pages

\*Composite web page has one or more links to other web pages

Each web page is a file with a name and address

### Web Server

The web page is stored at the server. Each time a request arrives, the corresponding document is sent to the client

و و و هو اليوم هو خدمة العميل العميل الموزعة، حيث يمكن للعميل باستخدام مستعرض الوصول إلى خدمة باستخدام خادم يتم توزيع الخدمة المقدمة على العديد من المواقع تسمى المواقع

يحتوي كل موقع على صفحة ويب واحدة أو أكثر. يمكن أن تحتوي كل صفحة ويب على بعض الروابط لصفحات ويب أخرى في نفس المواقع أو غيرها

\*صفحة ويب بسيطة لا يوجد لديه روابط لصفحات الويب الأخرى

\* تحتوي صفحة الويب المركبة على رابط واحد أو أكثر إلى صفحات ويب أخرى

كل صفحة ويب هو ملف له اسم وعنوان

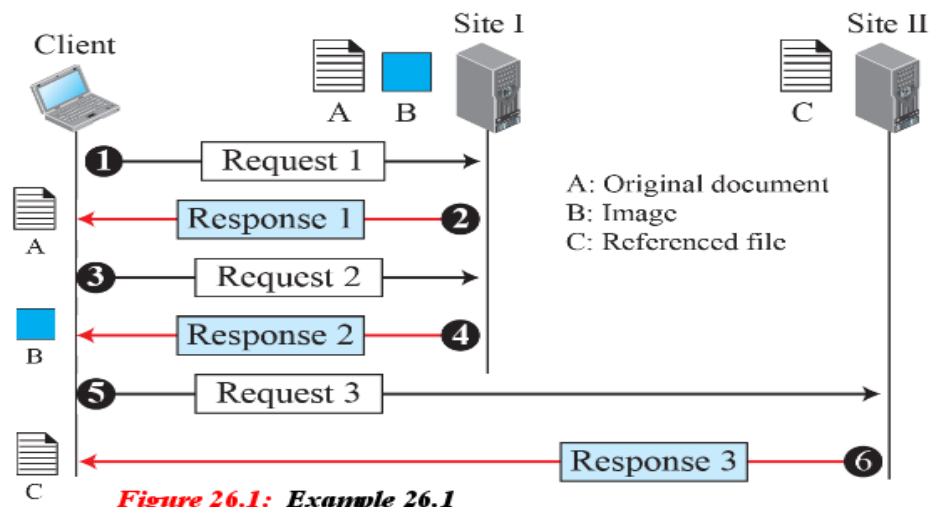
قاعدة بيانات للانترنت

يتم تخزين صفحة الويب على الخادم. في كل مرة يصل طلب، يتم إرسال المستند المقابل إلى العميل

## Example 26.1

Assume we need to retrieve a scientific document that contains one reference to another text file and one reference to a large image. Figure 26.1 shows the situation.

The main document and the image are stored in two separate files in the same site (file A and file B); the referenced text file is stored in another site (file C). Since we are dealing with three different files, we need three transactions if we want to see the whole document.

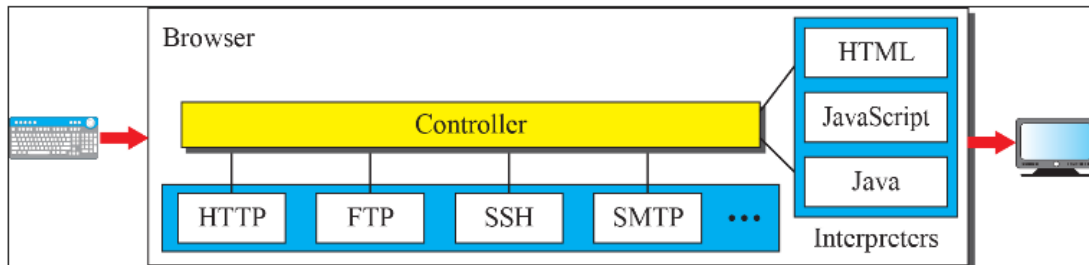


26.2

**Figure 26.2: Browser**

**browsers** interpret and display a web page.

**browsers usually consists of three parts:** a controller, client protocols, and interpreters.



- The controller receives input from the keyboard or the mouse
- The controller uses the client programs to access the document.
- The controller uses one of the interpreters to display the document on the screen.

**The client protocol:** HTTP or FTP.

**The interpreter:** HTML, Java, or JavaScript, depending on the type of document.

## Uniform Resource Locator (URL)

موقع محدد للمواقع

The uniform resource locator (URL) combine four identifiers to define the web page to distinguish it from other web pages:

- ▶ **Protocol:** the client-server program that we need in order to access the web page (HTTP or FTP)
- ▶ **Host:** IP address of the server or the unique name given to the server such as forouzan.com
- ▶ **Port:** the client-server application. If the HTTP protocol is used for accessing the web page, the well-known port number is 80. if a different port is used, the number can be explicitly given
- ▶ **Path:** The path identifies the location and the name of the file in the underlying operating system. For example, /top/next/last/myfile is a path that uniquely defines a file named myfile

protocol://host/path

Used most of the time

protocol://host:port/path

Used when port number is needed

يجمع محدد مواقع الموارد الموحد (ورل) أربعة معرفات لتحديد صفحة الويب لتمييزها عن صفحات الويب الأخرى:

► بروتوكول: برنامج خادم العميل الذي نحتاج إليه من أجل الوصول إلى صفحة الويب (هتب أو فتب)

► المضيف: عنوان إب للخادم أو الاسم الفريد المعطى للخادم مثل forouzan.com

► المنفذ: تطبيق خادم العميل. إذا تم استخدام بروتوكول هتب للوصول إلى صفحة ويب، رقم المنفذ المعروف هو ٨٠. إذا تم استخدام منفذ مختلف، يمكن إعطاء رقم صراحة

المسار: يحدد المسار موقع الملف واسمه في نظام التشغيل الأساسي. على سبيل المثال، / توب / نيكست / لاست / ميفيل هو مسار يعرف بشكل فريد ملف يسمى ميفيل

## Example 26.2

The URL <http://www.mhhe.com/compsci/forouzan/> defines the web page.

The string **www.mhhe.com** is the name of the computer in the McGraw-Hill company (the three letters **www** are part of the host name and are added to the commercial host).

The path is **compsci/forouzan/**, which defines Forouzan's web page under the directory **compsci** (computer science).

## 26.26.2 HyperText Transfer Protocol

بروتوكول نقل النص التشعبي

The HyperText Transfer Protocol (HTTP) is used to define how the client-server programs can be written to retrieve web pages from the Web. An HTTP client sends a request; an HTTP server returns a response. The server uses the port number 80; the client uses a temporary port number. HTTP uses the services of TCP, which, as discussed before, is a connection-oriented and reliable protocol.

يتم استخدام بروتوكول نقل النص التشعبي (هتب) لتحديد كيفية كتابة برامج خادم العميل لاسترداد صفحات الويب من الويب. يقوم عميل هتب بإرسال طلب؛ يقوم خادم هتب بإرجاع استجابة يستخدم الملفم رقم المنفذ ٨٠؛ يستخدم العميل رقم منفذ مؤقت. يستخدم هتب خدمات تكب، التي، كما نوقش من قبل، هو بروتوكول موجه نحو الاتصال وموثوق به

## Nonpersistent versus Persistent Connections

عدم الاتساق مقابل اتصالات دائمة

If the web pages are located on different servers, we must create a new TCP connection for retrieving each object

If the objects are located on the same server, we have two choices:

1-nonpersistent connection: retrieve each object using a new TCP connection

2-persistent connection: make a TCP connection and retrieve them all

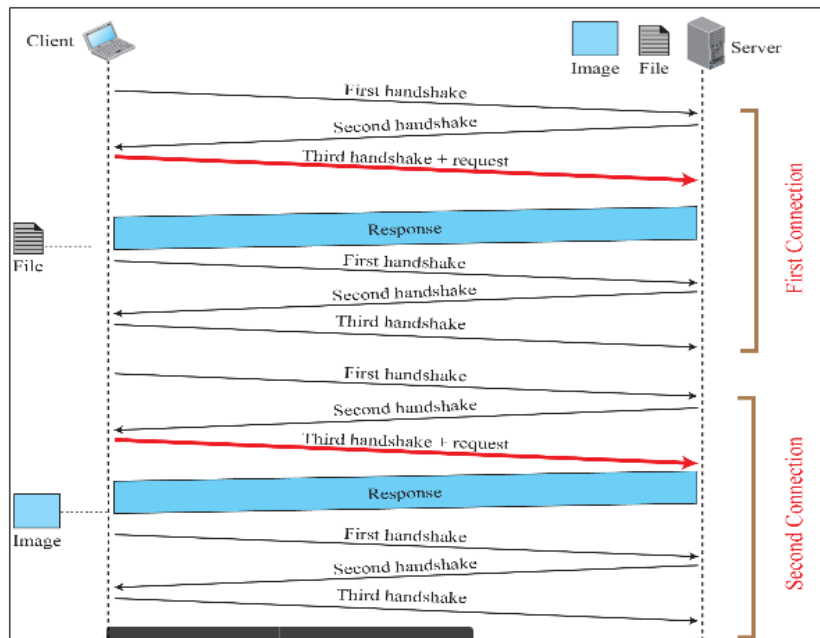
إذا كانت صفحات الويب موجودة على خوادم مختلفة، يجب علينا إنشاء اتصال تكب جديد لاسترداد كل كائن إذا كانت الكائنات موجودة على نفس الخادم، لدينا خياران:

- ١-اتصال غير نافذ: استرداد كل كائن باستخدام اتصال تكب جديد
- ٢-كونسنانت كونكتيون: قم بإجراء اتصال تكب واسترجاعها كلها

### Example 26.3

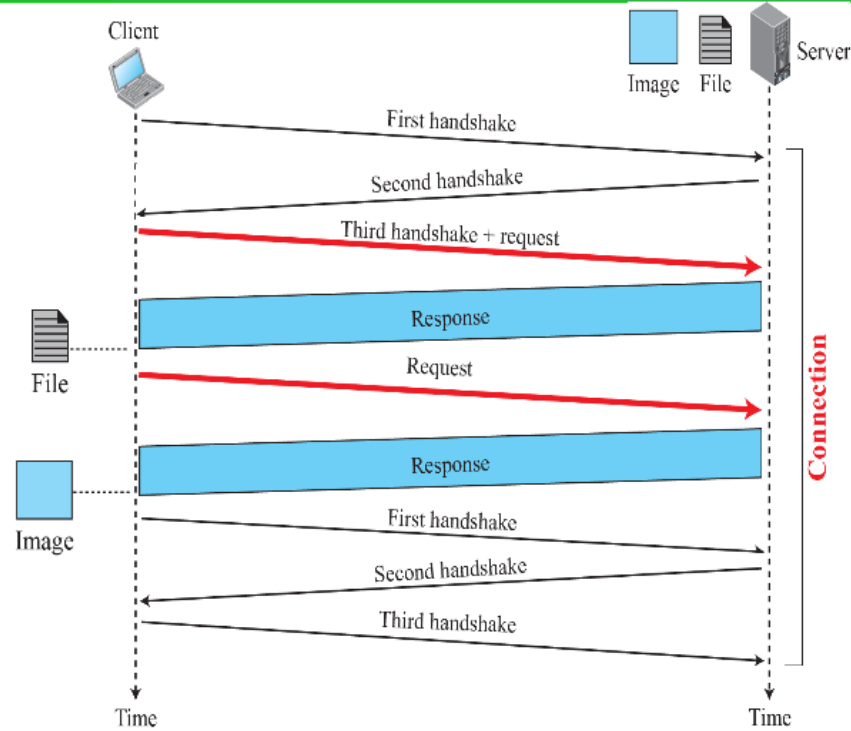
Figure 26.3 shows an example of a *nonpersistent* connection. The client needs to access a file that contains one link to an image. The text file and image are located on the same server.

Here we need two connections. For each connection, TCP requires at least three handshake messages to establish the connection, but the request can be sent with the third one. After the connection is established, the object can be transferred. After receiving an object, another three handshake messages are needed to terminate the connection.



## Example 26.4

Figure 26.4 shows the same scenario as in Example 26.3, but using a persistent connection. Only one connection establishment and connection termination is used, but the request for the image is sent separately.

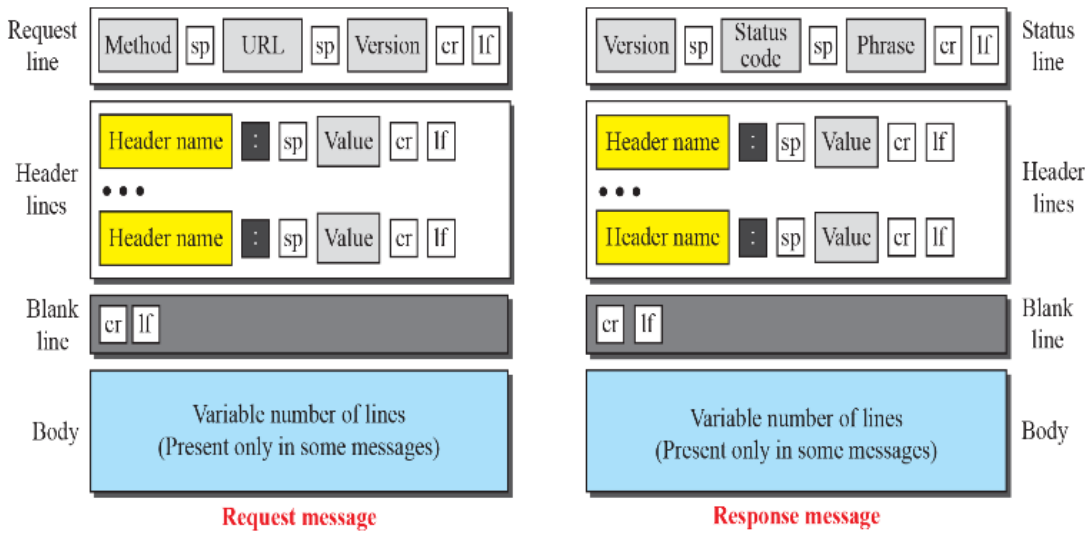


**Figure 26.4:** Example 26.4

26.3

**Figure 26.5:** Formats of the request and response messages

**Legend** sp: Space cr: Carriage Return lf: Line Feed



**Table 26.1: Methods**

<i>Method</i>	<i>Action</i>
GET	Requests a document from the server
HEAD	Requests information about a document but not the document itself
PUT	Sends a document from the client to the server
POST	Sends some information from the client to the server
TRACE	Echoes the incoming request
DELETE	Removes the web page
CONNECT	Reserved
OPTIONS	Inquires about available options

**Table 26.2: Request Header Names**

<i>Header</i>	<i>Description</i>
User-agent	Identifies the client program
Accept	Shows the media format the client can accept
Accept-charset	Shows the character set the client can handle
Accept-encoding	Shows the encoding scheme the client can handle
Accept-language	Shows the language the client can accept
Authorization	Shows what permissions the client has
Host	Shows the host and port number of the client
Date	Shows the current date
Upgrade	Specifies the preferred communication protocol
Cookie	Returns the cookie to the server (explained later)
If-Modified-Since	If the file is modified since a specific date

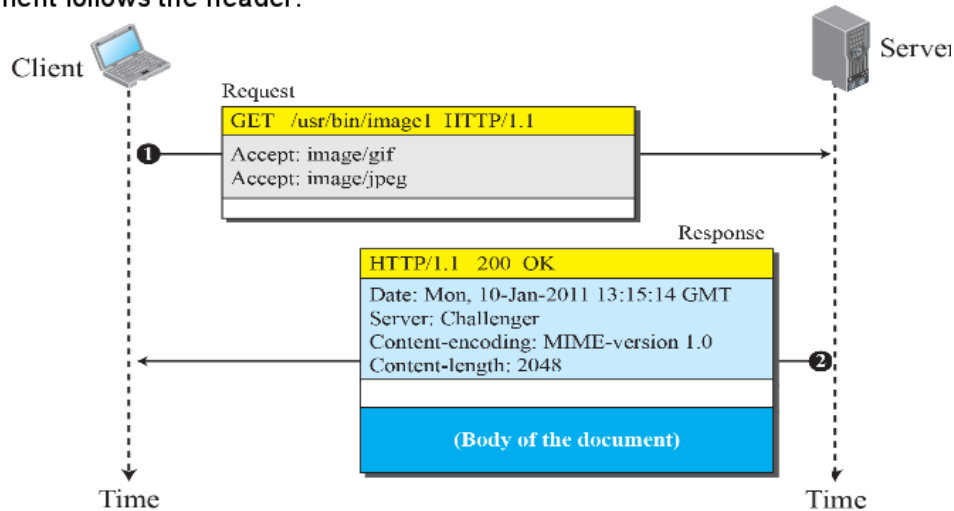
**Table 26.3: Response Header Names**

<i>Header</i>	<i>Description</i>
Date	Shows the current date
Upgrade	Specifies the preferred communication protocol
Server	Gives information about the server
Set-Cookie	The server asks the client to save a cookie
Content-Encoding	Specifies the encoding scheme
Content-Language	Specifies the language
Content-Length	Shows the length of the document
Content-Type	Specifies the media type
Location	To ask the client to send the request to another site
Accept-Ranges	The server will accept the requested byte-ranges
Last-modified	Gives the date and time of the last change



## Example 2656

This example retrieves a document . We use the GET method to retrieve an image with the path `/usr/bin/image1`. The request line shows the method (GET), the URL, and the HTTP version (1.1). The header has two lines that show that the client can accept images in the GIF or JPEG format. The request does not have a body. The response message contains the status line and four lines of header. The header lines define the date, server, content encoding and length of the document. The body of the document follows the header.



## Example 26.7

The following shows how a client imposes the modification data and time condition on a request.

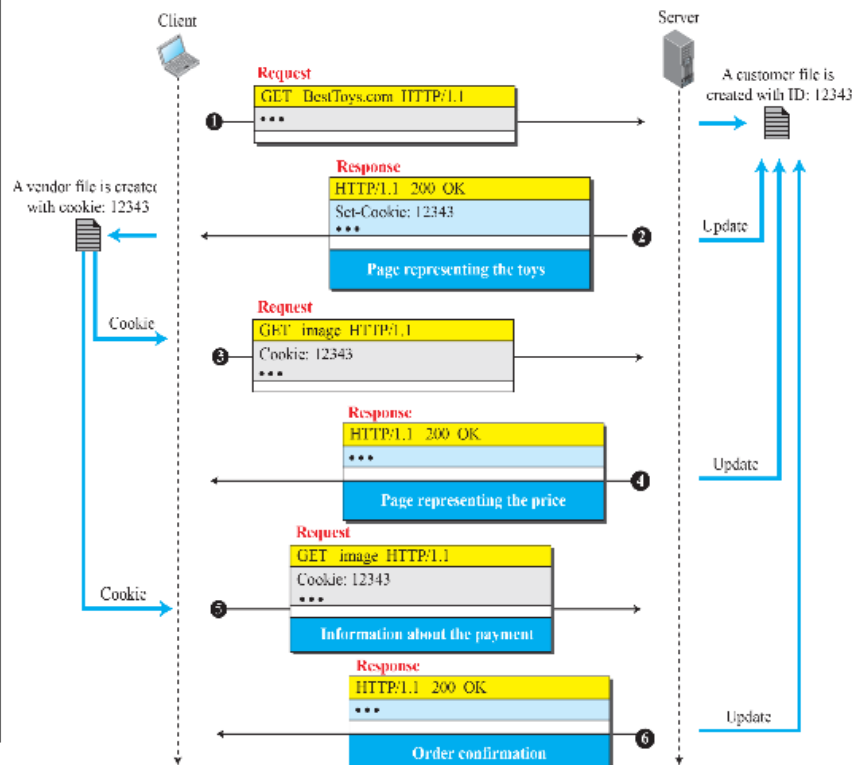
GET http://www.commonServer.com/information/file1 HTTP/1.1	<b>Request line</b>
If-Modified-Since: Thu, Sept 04 00:00:00 GMT	<b>Header line</b>
	<b>Blank line</b>

The status line in the response shows the file was not modified after the defined point in time. The body of the response message is also empty.

HTTP/1.1 304 Not Modified	<b>Status line</b>
Date: Sat, Sept 06 08 16:22:46 GMT	<b>First header line</b>
Server: commonServer.com	<b>Second header line</b>
	<b>Blank line</b>
(Empty Body)	<b>Empty body</b>

## Example 26.8

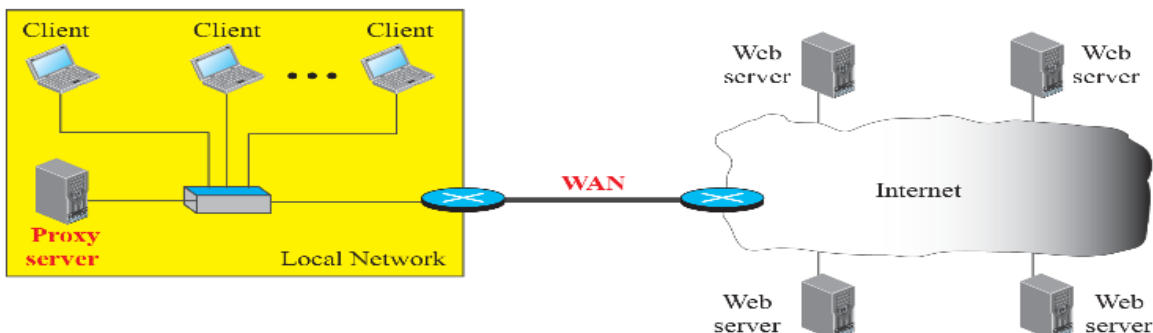
Figure 26.8 shows a scenario in which an electronic store can benefit from the use of cookies. Assume a shopper wants to buy a toy from an electronic store named BestToys. The shopper browser (client) sends a request to the BestToys server. The server creates an empty shopping cart (a list) for the client and assigns an ID to the cart (for example, 12343). The server then sends a response message, which contains the images of all toys available, with a link under each toy that selects the toy if it is being clicked. This response message also includes the Set-Cookie header line whose value is 12343. The client displays the images and stores the cookie value in a file named BestToys.



## Example 26.9

**Web Caching: Proxy Servers:** A proxy server is a computer that keeps copies of responses to recent requests.

Figure 26.9 shows an example of a use of a proxy server in a local network, such as the network on a campus or in a company. The proxy server is installed in the local network. When an HTTP request is created by any of the clients (browsers), the request is first directed to the proxy server. If the proxy server already has the corresponding web page, it sends the response to the client. Otherwise, the proxy server acts as a client and sends the request to the web server in the Internet. When the response is returned, the proxy server makes a copy and stores it in its cache before sending it to the requesting client.

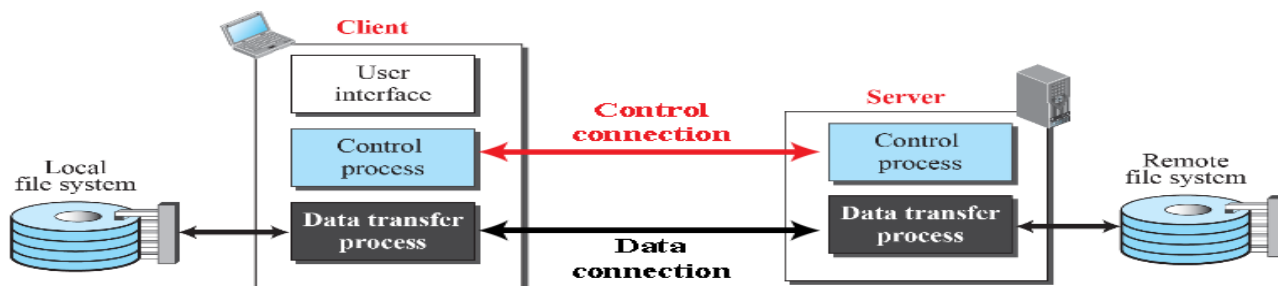


## 26.2 FTP

File Transfer Protocol (FTP) is the standard protocol provided by TCP/IP for copying a file from one host to another. Although transferring files from one system to another seems simple and straightforward, some problems must be dealt with first

بروتوكول نقل الملفات (فتب) هو البروتوكول القياسي الذي يوفره تكب / إب لنسخ ملف من مضيف إلى آخر. وعلى الرغم من أن نقل الملفات من نظام إلى آخر يبدو بسيطاً ومباشراً، فإنه يجب معالجة بعض المشاكل أولاً

**Figure 26.10: FTP**



basic model of FTP. The client has three components: the user interface, the client control process, and the client data transfer process.

The server has two components: the server control process and the server data transfer process.

The control connection is made between the control processes.  
The data connection is made between the data transfer processes.

### 26.2.1 Two Connections

The two connections in FTP have different lifetimes

- \*The control connection remains connected during the entire interactive FTP session
- \*The data connection is opened and then closed for each file transfer activity. It opens each time commands that involve transferring files are used, and it closes when the file is transferred

اثنين من الاتصالات في فتب لها عمر مختلف.  
يبقى اتصال التحكم متصلاً أثناء كامل جلسة فتب التفاعلية.  
يتم فتح اتصال البيانات ثم أغلق لكل نشاط نقل الملفات. فإنه يفتح كل الأوامر التي تنطوي على نقل الملفات المستخدمة، ويغلق عند نقل الملف

### 26.2.2 Control Connection

For control communication, FTP uses the same approach as TELNET (discussed later). It uses the NVT ASCII character set as used by TELNET  
Communication is achieved through commands and responses

commands are sent from the client to the server and responses are sent from the server to the client

This simple method is adequate for the control connection because we send one command (or response) at a time

Each line is terminated with a two-character carriage return and line feed) end-of-line token

ولتواصل التحكم، يستخدم بروتوكول نقل الملفات نفس النهج الذي يتبعه تلمنيت (الذي نوقش لاحقاً). ويستخدم مجموعة الأحرف نفت أسي كما تستخدم من قبل تلمنيت . يتم تحقيق الاتصالات من خلال الأوامر والردود  
يتم إرسال الأوامر من العميل إلى الملقم ويتم إرسال الردود من الملقم إلى العميل هذه الطريقة البسيطة كافية للاتصال التحكم لأننا نرسل أمر واحد (أو رد) في وقت واحد . يتم إنهاء كل سطر مع رمز إرجاع وخط تغذية من حرفين) رمز نهاية السطر

### Table 26.4: Some FTP commands

Commands, which are sent from the FTP client control process, are in the form of ASCII uppercase, which may or may not be followed by an argument

الأوامر، التي يتم إرسالها من عملية التحكم عميل فنتب، هي في شكل أسي الكبيرة، والتي قد أو قد لا يتبعها وسيطة.

Command	Argument(s)	Description
<b>ABOR</b>		Abort the previous command
<b>CDUP</b>		Change to parent directory
<b>CWD</b>	Directory name	Change to another directory
<b>DELE</b>	File name	Delete a file
<b>LIST</b>	Directory name	List subdirectories or files
<b>MKD</b>	Directory name	Create a new directory
<b>PASS</b>	User password	Password
<b>PASV</b>		Server chooses a port
<b>PORT</b>	port identifier	Client chooses a port
<b>PWD</b>		Display name of current directory
<b>QUIT</b>		Log out of the system
<b>RETR</b>	File name(s)	Retrieve files; files are transferred from server to client
<b>RMD</b>	Directory name	Delete a directory
<b>RNFR</b>	File name (old)	Identify a file to be renamed
<b>RNTO</b>	File name (new)	Rename the file
<b>STOR</b>	File name(s)	Store files; file(s) are transferred from client to server
<b>STRU</b>	<b>F, R, or P</b>	Define data organization ( <b>F</b> : file, <b>R</b> : record, or <b>P</b> : page)
<b>TYPE</b>	<b>A, E, I</b>	Default file type ( <b>A</b> : ASCII, <b>E</b> : EBCDIC, <b>I</b> : image)
<b>USER</b>	User ID	User information
<b>MODE</b>	<b>S, B, or C</b>	Define transmission mode ( <b>S</b> : stream, <b>B</b> : block, or <b>C</b> : compressed)

### Table 26.5: Some responses in FTP

Every FTP command generates at least one response. A response has two parts: three-digit number followed by text. The numeric part defines the code; the text part defines needed parameters or further explanations

كل أمر فتنب يولد استجابة واحدة على الأقل. الرد له جزأين: عدد من ثلاثة أرقام متبوعا بالنص. ويحدد الجزء الرقمي الرمز؛ ويحدد الجزء الخاص بالنص البارامترات المطلوبة أو التفسيرات الأخرى

<i>Code</i>	<i>Description</i>	<i>Code</i>	<i>Description</i>
125	Data connection open	250	Request file action OK
150	File status OK	331	User name OK; password is needed
200	Command OK	425	Cannot open data connection
220	Service ready	450	File action not taken; file not available
221	Service closing	452	Action aborted; insufficient storage
225	Data connection open	500	Syntax error; unrecognized command
226	Closing data connection	501	Syntax error in parameters or arguments
230	User login OK	530	User not logged in

### 26.2.3 Data Connection

The data connection uses the well-known port 20 at the server site. However, the creation of a data connection is different from the control connection.

The following shows the steps:

- 1-The client, not the server, issues a passive open using an ephemeral port
- 2-Using the PORT command the client sends this port number to the server
- 3-The server receives the port number and issues an active open using the well-known port 20 and the received ephemeral port number






يستخدم اتصال البيانات المنفذ المعروف ٢٠ في موقع الملقم. ومع ذلك، فإن إنشاء اتصال بيانات يختلف عن اتصال التحكم. وفيما يلي الخطوات التالية:

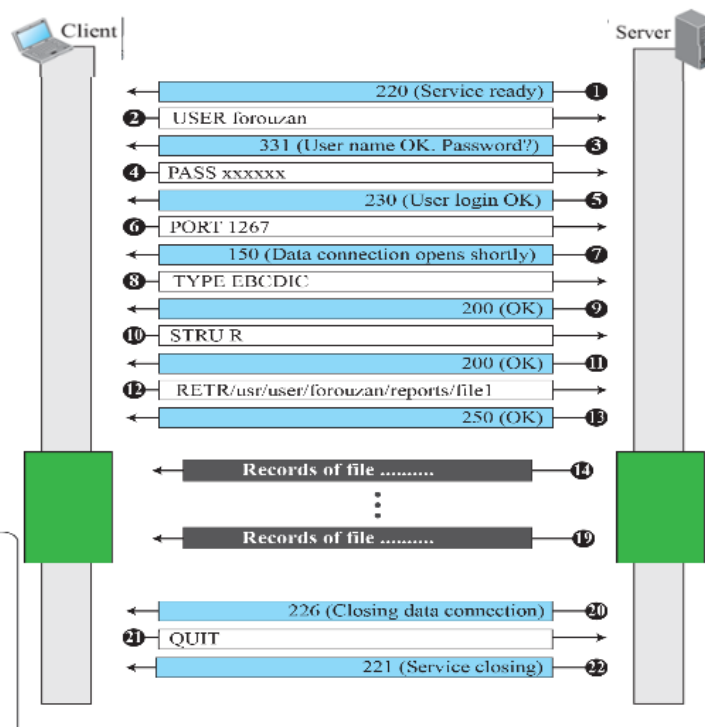
- ١-العميل، وليس الخادم، يصدر السلبي مفتوحا باستخدام منفذ سريع الزوال
- ٢-باستخدام الأمر بورت يقوم العميل بإرسال رقم المنفذ هذا إلى الملقم
- ٣-يتلقى الخادم رقم المنفذ ويصدر فتحا نشطا باستخدام المنفذ المعروف ٢٠ و رقم المنفذ السريع الزائد

## Example 26.10

The figure shows only one file to be transferred. The control connection remains open all the time, but the data connection is opened and closed repeatedly. We assume the file is transferred in six sections. After all records have been transferred, the server control process announces that the file transfer is done. Since the client control process has no file to retrieve, it issues the QUIT command, which causes the service connection to be closed.

### Legend

-  Control process (port 21)
-  Data transfer process (port 20)
-  Command
-  Response
-  Data transfer



## Example 26.11

The following shows an actual FTP session that lists the directories.

```
$ ftp voyager.deanza.fhda.edu
Connected to voyager.deanza.fhda.edu.
220 (vsFTPd 1.2.1)
530 Please login with USER and PASS.
Name (voyager.deanza.fhda.edu:forouzan): forouzan
331 Please specify the password.
Password:*****
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
227 Entering Passive Mode (153,18,17,11,238,169)
150 Here comes the directory listing.
drwxr-xr-x  2  3027  411  4096  Sep 24  2002  business
drwxr-xr-x  2  3027  411  4096  Sep 24  2002  personal
drwxr-xr-x  2  3027  411  4096  Sep 24  2002  school
226 Directory send OK.
ftp> quit
221 Goodbye.
```

## 26.2.4 Security for FTP

The FTP protocol was designed when security was not a big issue. Although FTP requires a password, the password is sent in plaintext (unencrypted), which means it can be intercepted and used by an attacker.

The data transfer connection also transfers data in plaintext, which is insecure. To be secure, one can add a Secure Socket Layer between the FTP application layer and the TCP layer. In this case FTP is called SSL-FTP.

We also explore some secure file transfer applications when we discuss SSH later in the chapter.

تم تصميم بروتوكول فنتب عندما لم يكن الأمن مشكلة كبيرة. على الرغم من أن فنتب يتطلب كلمة مرور، ويتم إرسال كلمة المرور في نص عادي (غير مشفرة)، مما يعني أنه يمكن اعتراضها واستخدامها من قبل مهاجم. نقل البيانات نقل أيضا البيانات في نص عادي، وهو غير آمن. لكي تكون آمنة، يمكن للمرء أن يضيف طبقة المقابس الآمنة بين طبقة تطبيق فنتب وطبقة تكب. في هذه الحالة يسمى فنتب سل-فنتب. نحن أيضا استكشاف بعض التطبيقات نقل الملفات آمنة عندما نناقش سش في وقت لاحق في الفصل

## 26.3 ELECTRONIC MAIL

Electronic mail (or e-mail) allows users to exchange messages. The nature of this application is different from other applications discussed so far. This means that the idea of client/server programming should be implemented in another way: using some intermediate computers (servers).

البريد الإلكتروني (أو البريد الإلكتروني) يسمح للمستخدمين لتبادل الرسائل. طبيعة هذا التطبيق يختلف عن التطبيقات الأخرى التي نوقشت حتى الآن. وهذا يعني أن فكرة البرمجة العميل / الخادم يجب أن تنفذ بطريقة أخرى: استخدام بعض الحواسيب المتوسطة (الخوادم).

### 26.3.1 Architecture

To explain the architecture of e-mail, we give a common scenario, as shown in Figure 26.12. Another possibility is the case in which Alice or Bob is directly connected to the corresponding mail server, in which LAN or WAN connection is not required, but this variation in the scenario does not affect our discussion.

ولشرح بنية البريد الإلكتروني، نقدم سيناريو مشترك، كما هو مبين في الشكل ٢٦،١٢. وثمة احتمال آخر هو الحالة التي يتصل فيها أليس أو بوب مباشرة بخادم البريد المقابل، حيث لا يلزم الاتصال بشبكة لان أو وان، ولكن هذا الاختلاف في السيناريو لا يؤثر على مناقشتنا.

### Figure 26.12: Common scenario

the sender and the receiver, Alice and Bob, are connected to two mail servers. The administrator has created one mailbox for each user. A mailbox is part of a server hard drive, a special file with permission restrictions. Only the owner of the mailbox has access to it. When Alice needs to send a message to Bob, she runs a user agent (UA) program to prepare the message and send it to her mail server. The mail server at her site uses a queue (spool) to store messages waiting to be sent. The message needs to be sent through the Internet from Alice's site to Bob's site using a message transfer agent (MTA). Here two message transfer agents are needed: one client and one server. The server needs to run all the time because it

does not know when a client will ask for a connection. The client, on the other hand, can be triggered by the system when there is a message in the queue to be sent.

يتم توصيل المرسل والمتلقي، أليس وبوب، إلى اثنين من خوادم البريد. أنشأ المشرف علبة بريد واحدة لكل مستخدم. صندوق البريد هو جزء من محرك الأقراص الثابتة الملقم، ملف خاص مع قيود الإذن. فقط مالك علبة البريد لديه حق الوصول إليه. عندما تحتاج أليس إلى إرسال رسالة إلى بوب، تدير برنامج وكيل المستخدم (وا) لإعداد الرسالة وإرسالها إلى خادم البريد. يستخدم خادم البريد في موقعها قائمة انتظار (التخزين المؤقت) لتخزين الرسائل في انتظار أن يتم إرسالها. يجب إرسال الرسالة عبر الإنترنت من موقع أليس لموقع بوب باستخدام وكيل نقل الرسائل (متا). هناك حاجة إلى اثنين من وكلاء نقل الرسائل: عميل واحد وخادم واحد. الخادم يحتاج إلى تشغيل في كل وقت لأنه لا يعرف متى يطلب عميل للاتصال. العميل، من ناحية أخرى، يمكن تشغيلها من قبل النظام عندما يكون هناك رسالة في قائمة الانتظار ليتم إرسالها.

The user agent at the Bob site allows Bob to read the received message. Bob later uses a message access agent client to retrieve the message from a message access agent server running on the second server.

يسمح وكيل المستخدم في موقع بوب ل بوب بقراءة الرسالة المستلمة. بوب لاحقاً يستخدم عميل عميل الوصول إلى الرسالة لاسترداد الرسالة من ملقم وكيل الوصول رسالة قيد التشغيل على الملقم الثاني

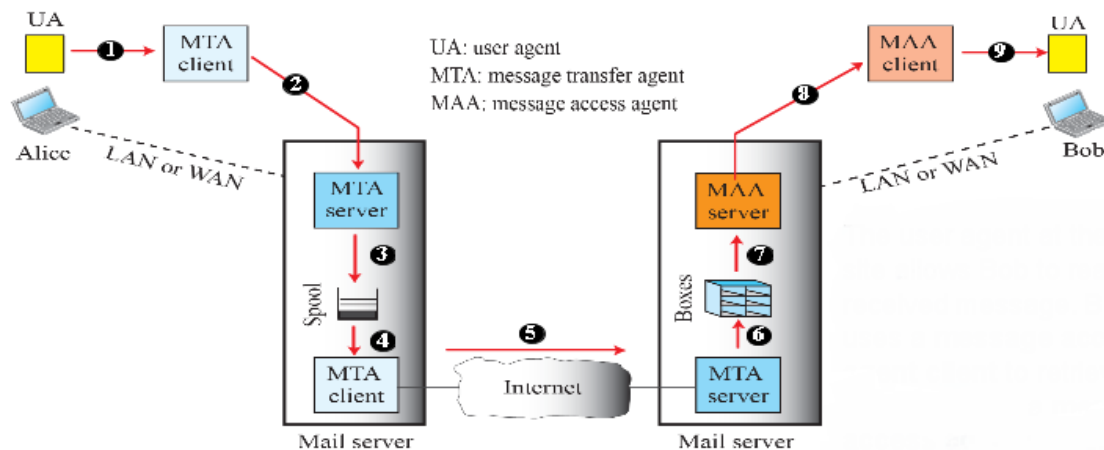
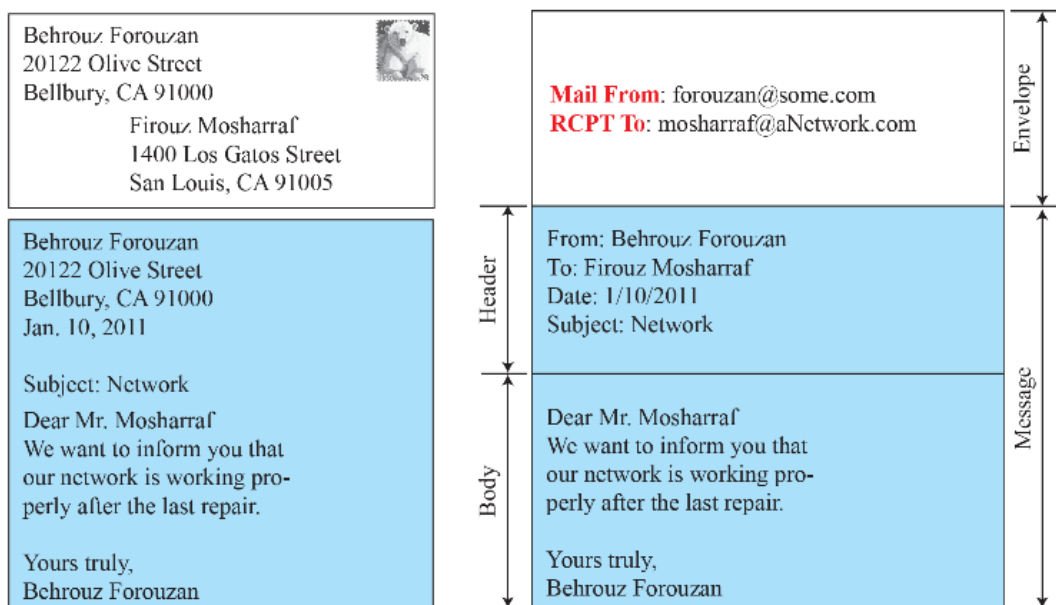


Figure 26.13: Format of an e-mail





**Figure 26.14: E-mail address**



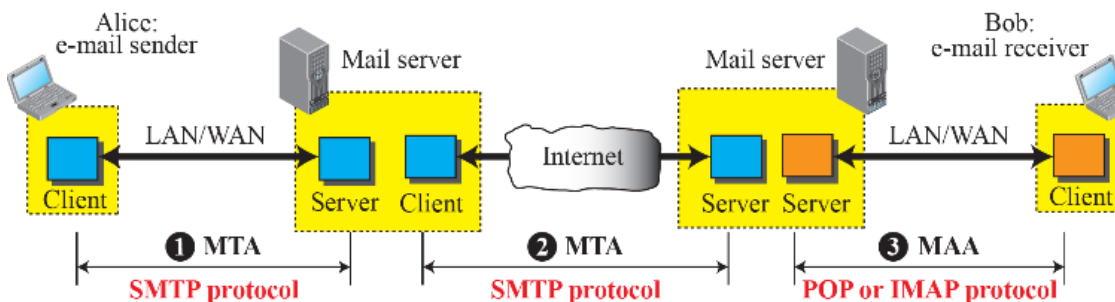
In the Internet, the address consists of two parts

**Local part:** defines the name of a special file, called the user mailbox, where all the mail received for a user is stored for retrieval by the message access agent.

**Domain name:** An organization usually selects one or more hosts to receive and send e-mail; they are sometimes called mail servers or exchangers.

في الإنترنت، يتكون العنوان من جزأين  
الجزء المحلي: يحدد اسم ملف خاص يسمى صندوق بريد المستخدم حيث يتم تخزين كل البريد المستلم للمستخدم لاسترجاعه بواسطة وكيل الوصول للرسالة.  
اسم النطاق: تقوم المؤسسة عادة بتحديد واحد أو أكثر من المضيفين لتلقي وإرسال البريد الإلكتروني؛ فإنها تسمى أحيانا خوادم البريد أو المبادلات.

**Figure 26.15: Protocols used in electronic mail**



For MTA, the message needs to be pushed from the client to the server (need a push (protocol) → Simple Mail Transfer Protocol (SMTP).

For MAA, the client must pull messages from the server (need a pull protocol) → POP and IMAP.

بالنسبة إلى مٲا، يجب أن يتم دفع الرسالة من العميل إلى الخادم (تحتاج إلى دفعة بروتوكول) → بروتوكول نقل البريد البسيط (سمتب).  
بالنسبة إلى ما، يجب على العميل سحب الرسائل من الخادم (تحتاج إلى بروتوكول سحب) → بوباماب.

## Table 26.6: SMTP Commands

The command is from an MTA client to an MTA server

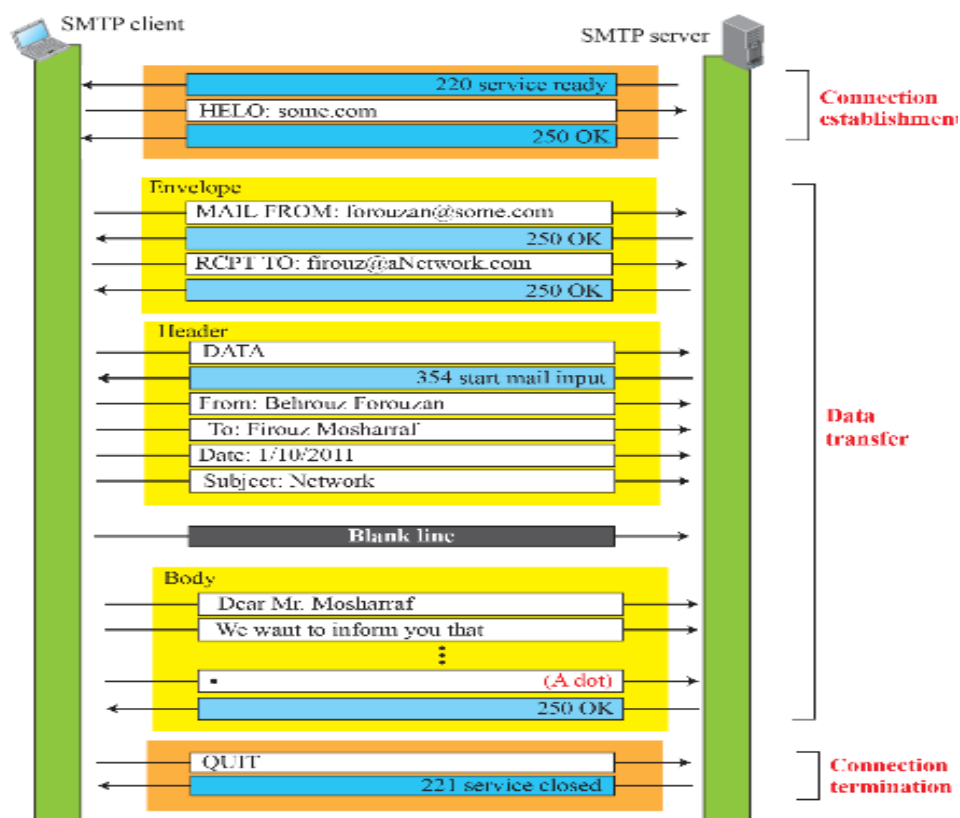
<i>Keyword</i>	<i>Argument(s)</i>	<i>Description</i>
HELO	Sender's host name	Identifies itself
MAIL FROM	Sender of the message	Identifies the sender of the message
RCPT TO	Intended recipient	Identifies the recipient of the message
DATA	Body of the mail	Sends the actual message
QUIT		Terminates the message
RSET		Aborts the current mail transaction
VRFY	Name of recipient	Verifies the address of the recipient
NOOP		Checks the status of the recipient
TURN		Switches the sender and the recipient
EXPN	Mailing list	Asks the recipient to expand the mailing list.
HELP	Command name	Asks the recipient to send information about the command sent as the argument
SEND FROM	Intended recipient	Specifies that the mail be delivered only to the terminal of the recipient, and not to the mailbox
SMOL FROM	Intended recipient	Specifies that the mail be delivered to the terminal <i>or</i> the mailbox of the recipient
SMAL FROM	Intended recipient	Specifies that the mail be delivered to the terminal <i>and</i> the mailbox of the recipient

## Table 26.7: SMTP responses (Continued)

The response is from an MTA server to the MTA client

Code	Description
<b>Positive Completion Reply</b>	
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
<b>Positive Intermediate Reply</b>	
354	Start mail input
<b>Transient Negative Completion Reply</b>	
421	Service not available
450	Mailbox not available
451	Command aborted: local error
452	Command aborted; insufficient storage
<b>Permanent Negative Completion Reply</b>	
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

### Example 26.12



The process of transferring a mail message occurs in three phases connection establishment, mail transfer, and connection termination

In the figure, we have separated the messages related to the envelope header, and body in the data transfer section

Note that the steps in this figure are repeated two times in each e-mail transfer

once from the e-mail sender to the local mail server

once from the local mail server to the remote mail server

The local mail server, after receiving

the whole e-mail message, may spool it and send it to the remote mail server at another time

تحدث عملية نقل رسالة بريدية في ثلاث مراحل إنشاء اتصال ونقل البريد وإنهاء الاتصال في الشكل، فمنا بفصل الرسائل المتعلقة رأس المغلف، والجسم في قسم نقل البيانات لاحظ أن الخطوات الواردة في هذا الشكل تتكرر مرتين في كل نقل البريد الإلكتروني مرة واحدة من مرسل البريد الإلكتروني إلى خادم البريد المحلي، مرة واحدة من خادم البريد المحلي إلى خادم البريد البعيد خادم البريد المحلي، بعد تلقي رسالة البريد الإلكتروني بأكملها، قد التخزين المؤقت وإرساله إلى خادم البريد البعيد في وقت آخر

### Figure 26.17: POP3

Post Office Protocol, version 3 (POP3)

Mail access starts with the client when the user needs to download its e-mail from 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 messages, one by one.

بروتوكول مكتب البريد، الإصدار ٣ (POP3)

يبدأ الوصول إلى البريد مع العميل عند

يحتاج المستخدم لتحميل البريد الإلكتروني من

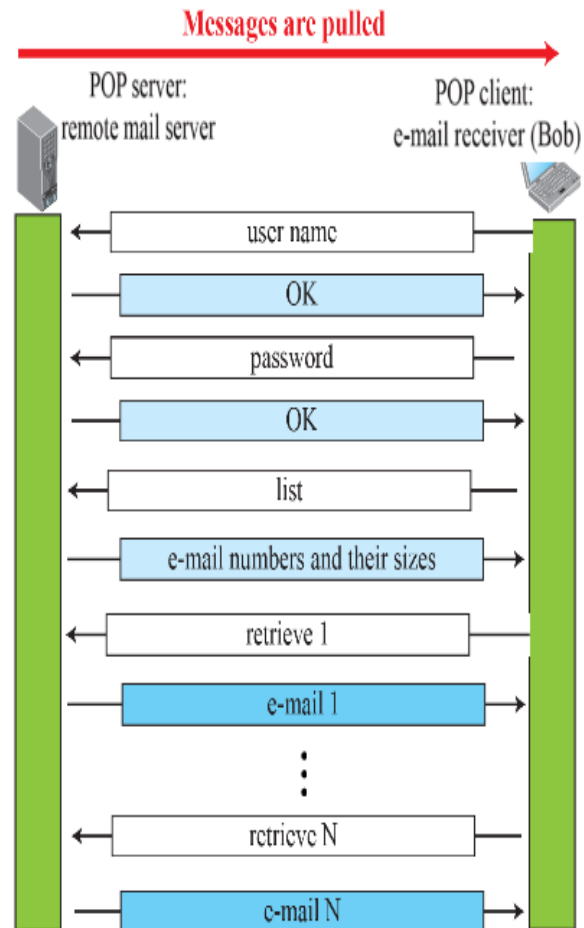
صندوق البريد على خادم البريد. يفتح العميل

اتصال بالملقم على منفذ تكب ١١٠.

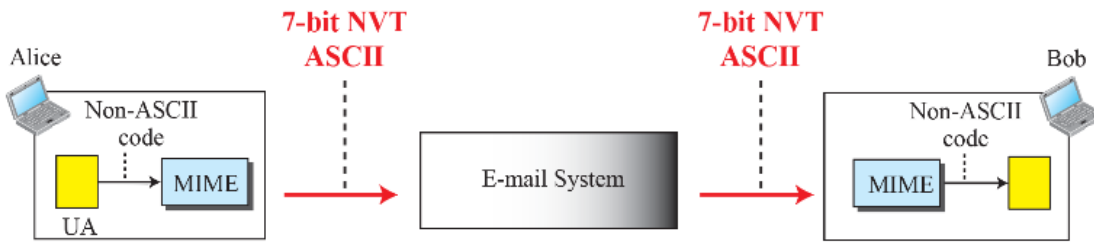
ثم يرسل اسم المستخدم وكلمة المرور ل

الوصول إلى علبة البريد. يمكن للمستخدم ثم قائمة و

استرداد رسائل البريد، واحدا تلو الآخر



**Figure 26.18: MIME**



Electronic mail can send messages only in NVT 7-bit ASCII format. It cannot be used for languages other than English or to send binary files or video or audio data

Multipurpose Internet Mail Extensions (MIME) is a supplementary protocol that transforms non-ASCII data at the sender site to NVT ASCII data and delivers it to the client MTA to be sent through the Internet. The message at the receiving site is transformed back to the original data

يمكن للبريد الإلكتروني إرسال رسائل فقط بتنسيق نبت ٧ بت نفت. لا يمكن استخدامه للغات غير الإنجليزية أو إرسال الملفات الثنائية أو بيانات الفيديو أو الصوت

تعد ملحقات بريد الإنترنت متعددة الأغراض (مايم) بروتوكول تكميلي يحول البيانات غير أسي في موقع المرسل إلى بيانات نبت أسي ويسلمها إلى متا العميل ليتم إرسالها عبر الإنترنت. يتم تحويل الرسالة في موقع الاستقبال مرة أخرى إلى البيانات الأصلية

**Figure 26.19: MIME header**

<b>MIME headers</b>	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

**Table 26.8: Data Types and Subtypes in MIME**

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

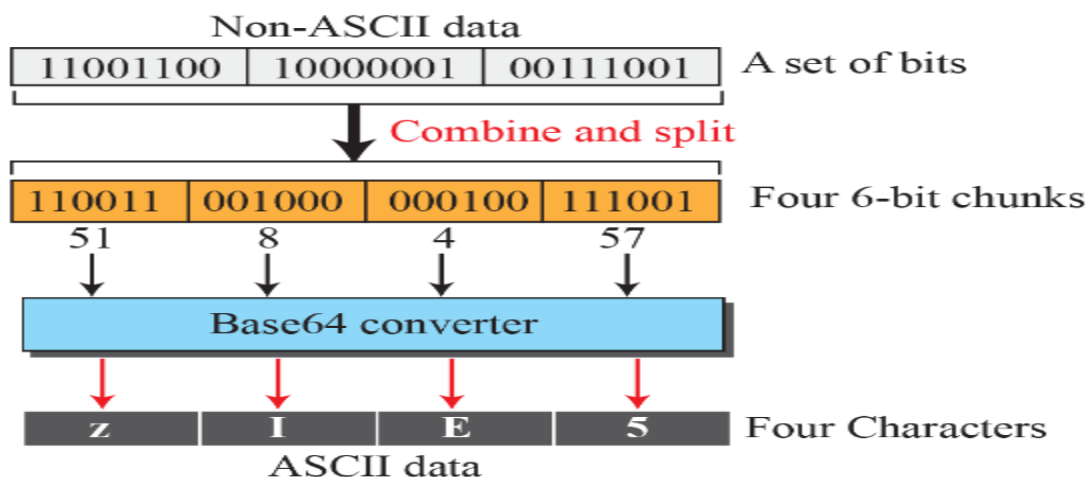
**Table 2.9: Methods for Content-Transfer-Encoding**

Type	Description
7-bit	NVT ASCII characters with each line less than 1000 characters
8-bit	Non-ASCII characters with each line less than 1000 characters
Binary	Non-ASCII characters with unlimited-length lines
Base64	6-bit blocks of data encoded into 8-bit ASCII characters
Quoted-printable	Non-ASCII characters encoded as an equal sign plus an ASCII code

Figure 26.20: Base64 conversion

In the Base64 encoding data is divided into 6-bit chunks. Each 6-bit section is then converted into an ASCII character according to Table 26.10

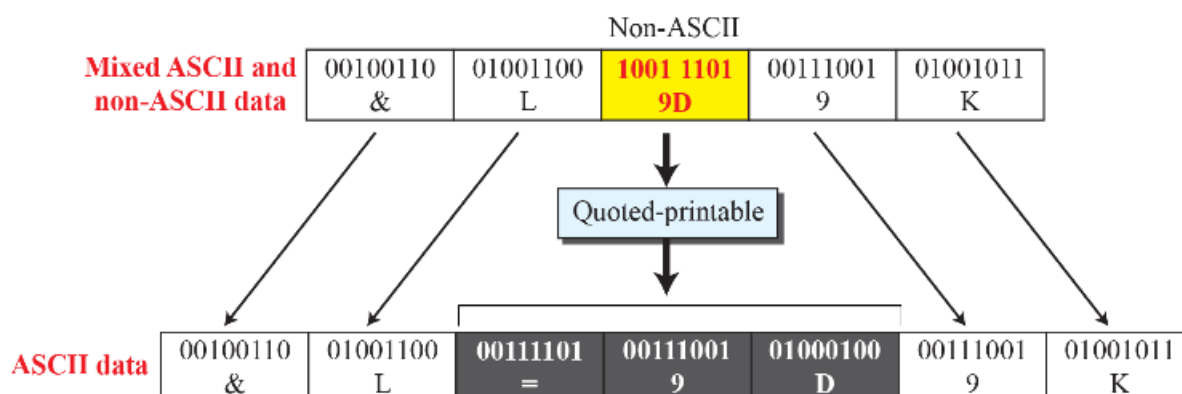
في قاعدة 64 يتم تقسيم البيانات ترميز إلى قطع 6 بت. ثم يتم تحويل كل قسم 6 بت إلى حرف أسي وفقا للجدول 26,10



**Table 26.10: Base64 Converting Table S**

Value	Code	Value	Code	Value	Code	Value	Code	Value	Code	Value	Code
0	A	11	L	22	W	33	h	44	s	55	3
1	B	12	M	23	X	34	i	45	t	56	4
2	C	13	N	24	Y	35	j	46	u	57	5
3	D	14	O	25	Z	36	k	47	v	58	6
4	E	15	P	26	a	37	l	48	w	59	7
5	F	16	Q	27	b	38	m	49	x	60	8
6	G	17	R	28	c	39	n	50	y	61	9
7	H	18	S	29	d	40	o	51	z	62	+
8	I	19	T	30	e	41	p	52	0	63	/
9	J	20	U	31	f	42	q	53	1		
10	K	21	V	32	g	43	r	54	2		

Figure 26.21: Quoted-printable



If the data consist mostly of ASCII characters with a small non-ASCII portion, we can use quoted-printable encoding.

if a character is ASCII, it is sent as is

If a character is not ASCII, it is sent as three characters. The first character is the equal sign (=). The next two characters are the hexadecimal representations of the byte .

In the Figure, the third character is a non-ASCII because it starts with bit 1. It is interpreted as two hexadecimal digits (9D)16, which is replaced by three ASCII characters (=, 9, and D)

إذا كانت البيانات تتكون في معظمها من أحرف أسي مع جزء صغير غير أسي، يمكننا استخدام ترميز قابل للطباعة. إذا كان الحرف أسي، يتم إرساله كما هو

إذا كان الحرف ليس أسي، يتم إرساله كثلاثة أحرف. الحرف الأول هو علامة المساواة (=). الحرفان التاليان هما التمثيل السداسي العشري للبايت.

في الشكل، الحرف الثالث هو غير أسي لأنه يبدأ بت 1. يتم تفسيره على أنه رقمين سداسي عشريين (9D) 16، الذي يتم استبدال ثلاثة أحرف أسي (=، 9، و D)

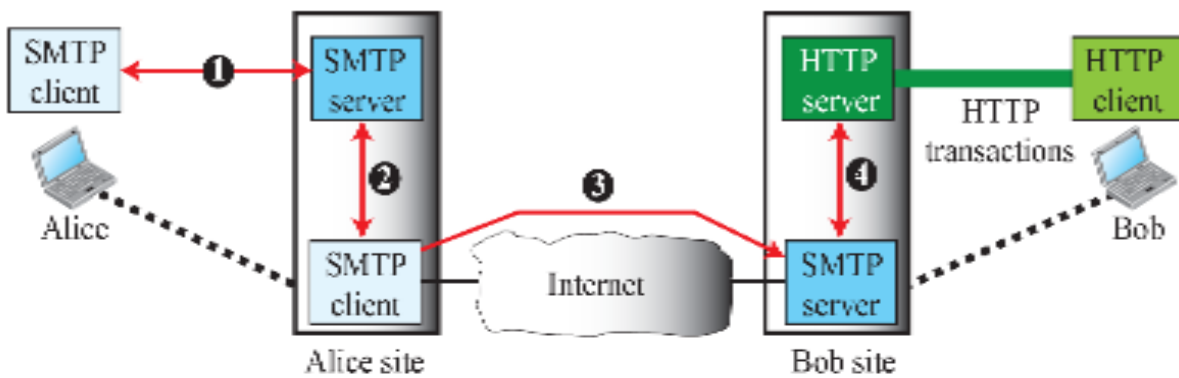
### 26.3.2 Web-Based Mail

E-mail is such a common application that some websites today provide this service to anyone who accesses the site.

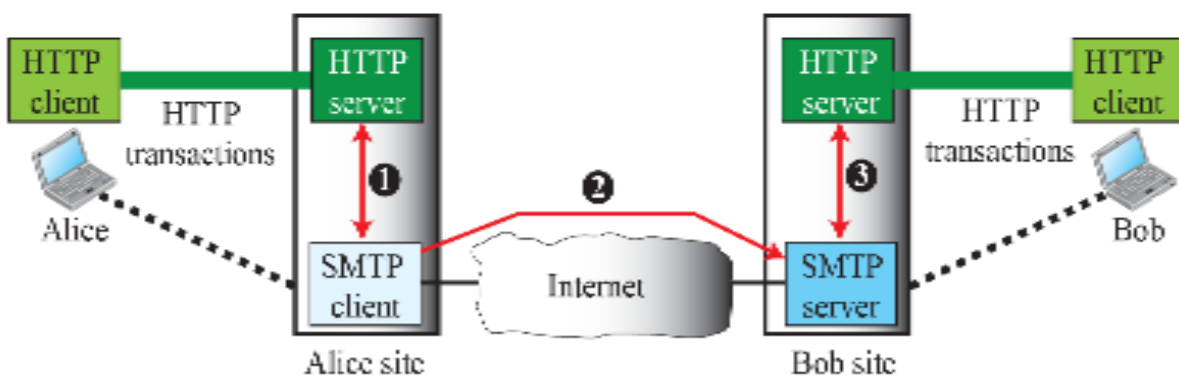
Three common sites are Hotmail, Yahoo, and Google mail. The idea is very simple. Figure 26.22 shows two cases.

البريد الإلكتروني هو مثل هذا التطبيق المشترك أن بعض المواقع اليوم تقديم هذه الخدمة إلى أي شخص الوصول إلى الموقع. هناك ثلاثة مواقع مشتركة هي هوميل وياهو و بريد غوغل. الفكرة بسيطة جدا. ويبين الشكل ٢٦-٢٢ حالتين

Figure 26.22: Web-based e-mail, cases I and II



Case 1: Only receiver uses HTTP



Case 2: Both sender and receiver use HTTP

Case I: Alice, uses a mail server; Bob, the receiver has an account on a web-based server  
 Mail transfer from Alice’s browser to her traditional mail serve, and from the sending mail server to the receiving mail server (the web server) to Bob’s browser is done through HTTP., instead of using POP3 or IMAP4  
 When Bob needs to retrieve his e-mails, he sends a request HTTP message to the website (Hotmail, for



example). The website sends a form to be filled in by Bob (the log-in name and the password) If the log-in name and password match, the list of e-mails is transferred from the web server to Bob's browser in HTML format.

Case 2: In the second case, both Alice and Bob use web servers. Alice sends an HTTP request message to her web server using the name and address of Bob's mailbox as the URL. The server at the Alice site passes the message to the SMTP client and sends it to the server at the Bob site using SMTP protocol.

Bob

receives the message using HTTP transactions. SMTP protocol. Is used to transfer the message from the server at the Alice site to the server at the Bob site.

E-Mail Security ٢٦,٣,٢

لحالة الأولى: أليس، تستخدم خادم بريد؛ بوب، المتلقي لديه حساب على خادم على شبكة الإنترنت نقل البريد من متصفح أليس إلى خدمة البريد التقليدية، ومن خادم البريد المرسل إلى استقبال خادم البريد من خلال سمتب. ومع ذلك، يتم إرسال الرسالة من خادم الاستلام (خادم الويب) إلى متصفح بوب عبر هتتب، بدلا من استخدام POP3 أو IMAP4 عندما يحتاج بوب لاسترداد رسائل البريد الإلكتروني، يرسل رسالة هتتب طلب إلى الموقع (هوتميل، ل مثال). يرسل الموقع نموذجا يتعين ملؤه بواسطة بوب (اسم تسجيل الدخول وكلمة المرور) إذا تطابق اسم تسجيل الدخول وكلمة المرور، يتم نقل قائمة من رسائل البريد الإلكتروني من ملقم ويب إلى بوب المتصفح بتنسيق هتتمل.

الحالة ٢: في الحالة الثانية، يستخدم كل من أليس وبوب خوادم الويب. ترسل أليس رسالة طلب هتتب إلى خادم الويب الخاص بها باستخدام اسم وعنوان صندوق بريد بوب كعنوان ورل. يقوم الخادم في موقع أليس بتمرير الرسالة إلى عميل سمتب ويرسلها إلى الخادم في موقع بوب باستخدام بروتوكول سمتب. تمايل يتلقى الرسالة باستخدام معاملات هتتب. بروتوكول سمتب. يستخدم لنقل الرسالة من الخادم في موقع أليس إلى الخادم في موقع بوب

### 26.3.2 E-Mail Security

The protocol discussed in this chapter does not provide any security provisions per se. However, e-mail exchanges can be secured using two application-layer securities designed in particular for e-mail systems.

Two of these protocols, Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME), are discussed in Chapter 32 after we have discussed basic network security.

والبروتوكول الذي نوقش في هذا الفصل لا ينص على أي أحكام أمنية في حد ذاتها. ومع ذلك، يمكن تأمين تبادل البريد الإلكتروني باستخدام اثنين من الأوراق المالية طبقة التطبيق المصممة خصيصا لأنظمة البريد الإلكتروني. ويناقش الفصلان ٣٢ من هذه البروتوكولات و "الخصوصية الجيدة الجيدة" و "ملحقات البريد الإلكتروني الأمانة / متعددة الأغراض" (S / مايم) بعد أن ناقشنا أمن الشبكات الأساسية.

### 26.4 TELNET

It is impossible to have a client/server pair for each type of service we need; the number of servers soon becomes intractable. The idea is not scalable. The solution is to have a specific client/server program for a set of common scenarios, but to have some generic client/server programs for the rest.

من المستحيل أن يكون زوج العميل / الخادم لكل نوع من أنواع الخدمات التي نحتاج إليها؛ يصبح عدد الخوادم قريبا مستعصية على الحل. الفكرة ليست قابلة للتطوير. الحل هو أن يكون برنامج عميل / خادم محدد لمجموعة من السيناريوهات المشتركة، ولكن لديك بعض عام برامج العميل / الخادم للباقي.

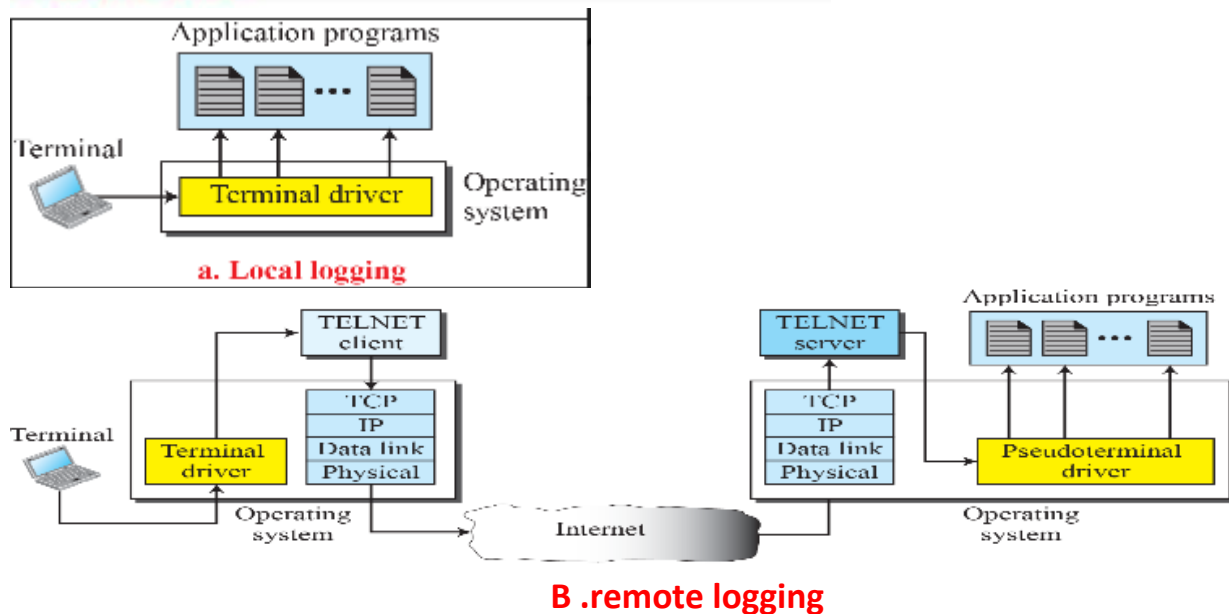
### 26. 4.1 Local versus Remote Logging

We first discuss the concept of local and remote logging as shown in Figure 26.23

نناقش أولاً مفهوم قطع الأشجار المحلية والبعيدة كما هو مبين في الشكل ٢٦،٢٣

When a user logs into a local system, it is called local logging. As a user types at a terminal or at a workstation running a terminal emulator, the keystrokes are accepted by the terminal driver. The terminal driver passes the characters to the operating system. The operating system interprets the combination of characters and invokes the desired application program or utility.

**Figure 2.23: Local versus remote logging**

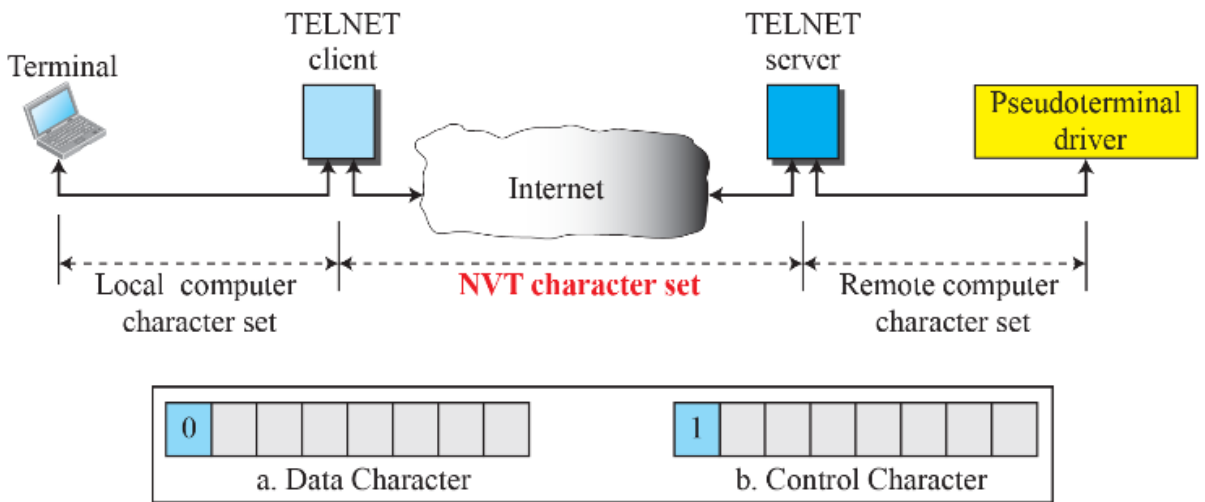


When a user wants to access an application program or utility located on a remote machine, she performs remote logging. The user sends the keystrokes to the terminal driver where the local operating system accepts the characters but does not interpret them. The characters are sent to the TELNET client, which transforms the characters into a universal character set called Network Virtual Terminal (NVT) characters and delivers them to the local TCP/IP stack. NVT 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 characters cannot be passed directly to the operating system because it is not designed to receive characters from a TELNET server; it is designed to receive characters from a terminal driver. The solution is to add a piece of software called a pseudo terminal driver, which

pretends that the characters are coming from a terminal. The operating system then passes the characters to the appropriate application program

عندما يقوم المستخدم بتسجيل الدخول إلى نظام محلي، يطلق عليه التسجيل المحلي. كما يكتب المستخدم في محطة أو في محطة عمل تشغيل جهاز محاكاة الطرفية، تكون ضغطات المفاتيح قبلت من قبل سائق المحطة الطرفية. سائق المحطة يمر الشخصيات إلى نظام التشغيل. يفسر نظام التشغيل مجموعة الأحرف واستدعاء برنامج التطبيق المطلوب أو الأداة المساعدة. عندما يريد المستخدم الوصول إلى برنامج تطبيق أو أداة موجودة على جهاز بعيد، تقوم بإجراء تسجيل بعيد. يرسل المستخدم ضغطات المفاتيح إلى برنامج التشغيل الطرفي حيث يقبل نظام التشغيل المحلي الأحرف ولكن لا يفسرها. يتم إرسال الأحرف إلى عميل تلمنيت، الذي يحول الأحرف إلى مجموعة أحرف عالمية تسمى شبكة نيتورك فيرتوال ترمينال (نفت) وتسليمها إلى مكندس تكب / إب المحلي. نفت السفر عبر الإنترنت والوصول إلى تكب / إب المكندس على الجهاز البعيد. هنا يتم تسليم الأحرف إلى نظام التشغيل ومررت إلى خادم تلمنيت، الذي يغير الأحرف إلى الأحرف المقابلة مفهومة بواسطة الكمبيوتر البعيد. ومع ذلك، لا يمكن تمرير الحروف مباشرة إلى نظام التشغيل لأنه غير مصمم لتلقي شخصيات من خادم تلمنيت؛ وهي مصممة لتلقي أحرف من برنامج تشغيل المحطة الطرفية. الحل هو إضافة قطعة من البرمجيات تسمى سائق محطة الزائفة، الذي يدعي أن الشخصيات تأتي من محطة. ثم يقوم نظام التشغيل بتمرير الحروف إلى برنامج التطبيق المناسب

**Figure 26.24: Concept of NVT**



**NVT character format**

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

NVT uses two sets of characters, one for data and one for control. Both are 8-bit bytes

تلمنيت العميل يترجم الأحرف (البيانات أو الأوامر) التي تأتي من المحطة المحلية في شكل نفت وتسليمها إلى الشبكة. خادم تلمنيت، من ناحية أخرى يترجم البيانات والأوامر من شكل نفت في شكل مقبول من قبل الكمبيوتر البعيد يستخدم نفت مجموعتين من الأحرف، واحدة للبيانات واحد للسيطرة. كلاهما بايت ٨ بت

**Table 26.11: Examples of interface commands S**

The operating system (UNIX, for example) defines an interface with user-friendly commands

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

## 26.5 SECURE SHELL (SSH)

Although Secure Shell (SSH) is a secure application program that can be used today for several purposes such as remote logging and file transfer, it was originally designed to replace TELNET. There are two versions of SSH. The first version, SSH-1, is now deprecated because of security flaws in it. In this section, we discuss only SSH-2

على الرغم من أن تأمين شل (سش) هو تطبيق تطبيق آمن التي يمكن استخدامها اليوم لعدة أغراض مثل قطع الأشجار عن بعد ونقل الملفات، تم تصميمه أصلا ليحل محل تلتنت. هناك إصداران من سش. النسخة الأولى، سش-1، تم إهمالها الآن بسبب عيوب أمنية فيها. في هذا القسم، نناقش فقط سش-2

### 26.5.1 Components

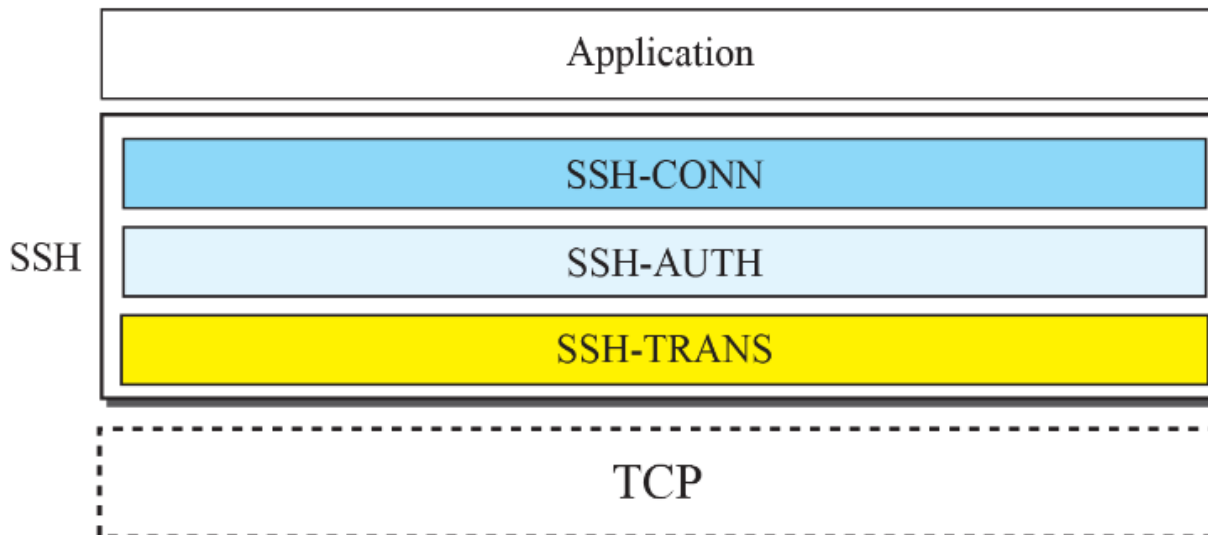
SSH is an application-layer protocol with three components, as shown in Figure 26.25

**Figure 26.25: Components of SSH**

**(SSH-CONN): SSH Connection Protocol.**

**(SSH-AUTH): SSH Authentication Protocol.**

**(SSH-TRANS): SSH Transport-Layer Protocol.**



### 26.5.2 Applications

Although SSH is often thought of as a replacement for TELNET, SSH is, in fact, a general-purpose protocol that provides a secure connection between a client and server

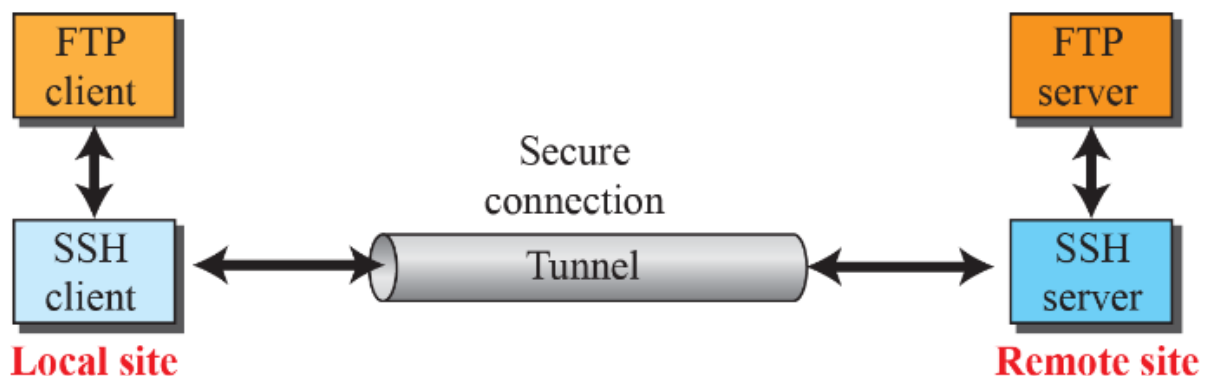
على الرغم من أن سش غالبا ما يعتبر كبديل ل تلتنيت، سش هو، في الواقع، بروتوكول للأغراض العامة يوفر اتصال آمن بين العميل والخادم

#### Figure 26.26: Port Forwarding

The SSH port forwarding mechanism creates a tunnel through which the messages belonging to other protocols can travel. For this reason, this mechanism is sometimes referred to as SSH tunneling.

We can use the secured channels to access an application program that does not provide security services

تقوم آلية إعادة توجيه منفذ سش بإنشاء نفق يمكن من خلاله نقل الرسائل التي تنتمي إلى بروتوكولات أخرى. ولهذا السبب، يشار أحيانا إلى هذه الآلية باسم نفق سش. يمكننا استخدام القنوات المضمونة للوصول إلى برنامج التطبيق الذي لا يوفر خدمات الأمان

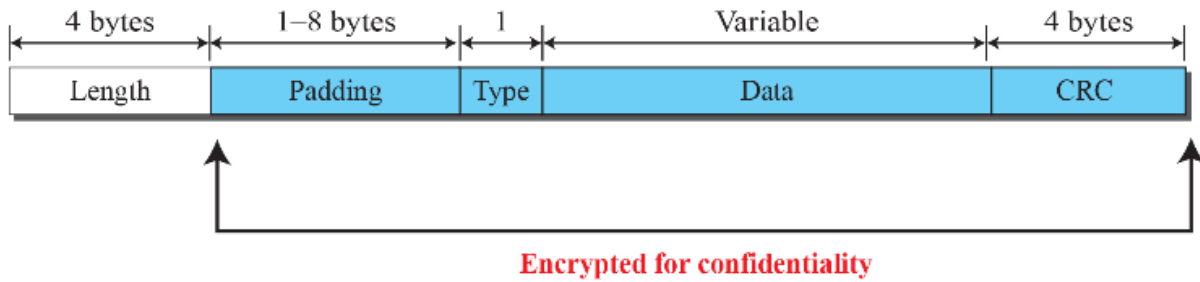


#### Figure 26.27: SSH Packet Format S

The length field defines the length of the packet but does not include the padding.

One to eight bytes of padding is added to the packet to make the attack on the security

provision more difficult. The CRC field is used for error detection. The type field designates the type of the packet used in different SSH protocols. The data field is the data transferred by the packet in different protocols



## 26.6 DOMAIN NAME SYSTEM (DNS)

The last client-server application program we discuss has been designed to help other application programs.

The Internet needs to have a directory system that can map a name to an address. This is analogous to the telephone network.

Figure 26.28 shows how TCP/IP uses a DNS client and a DNS server to map a name to an address

وقد تم تصميم آخر برنامج تطبيق العميل-الخادم مناقش لمساعدة برامج التطبيقات الأخرى. يحتاج الإنترنت إلى نظام الدليل الذي يمكن تعيين اسم إلى عنوان. وهذا مشابه لشبكة الهاتف. يوضح الشكل 26.28 كيفية استخدام تكب / إب عميل دنس وملقم دنس لتعيين اسم إلى عنوان

### Figure 26.28: Purpose of DNS

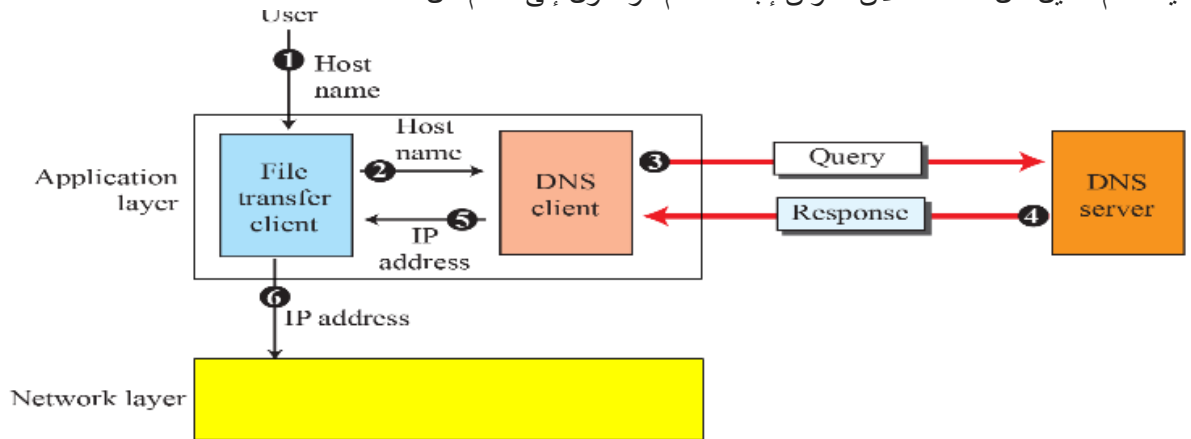
A user wants to use a file transfer client to access the corresponding file transfer server running on a remote host. The user knows only the file transfer server name, such as afilesource.com. However, the TCP/IP suite needs the IP address of the file transfer server to make the connection. The following six steps map the host name to an IP address:

- 1-The user passes the host name to the file transfer client
- 2-The file transfer client passes the host name to the DNS client
- 3-Each computer, after being booted, knows the address of one DNS server. The DNS client sends a message to a DNS server with a query that gives the file transfer server name using the known IP address of the DNS server
- 4-The DNS server responds with the IP address of the desired file transfer server
- 5-The DNS server passes the IP address to the file transfer client
- 6-The file transfer client now uses the received IP address to access the file transfer server

يريد المستخدم استخدام عميل نقل الملفات للوصول إلى خادم نقل الملفات المقابل الذي يعمل على جهاز تحكم عن بعد مضيف. المستخدم يعرف فقط اسم ملف نقل الملفات، مثل afilesource.com. ومع ذلك، تحتاج مجموعة تكب / إب عنوان إب ملقم نقل الملفات لإجراء الاتصال. تحدد الخطوات الست التالية اسم المضيف لعنوان إب:

- 1-يقوم المستخدم بتمرير اسم المضيف إلى عميل نقل الملفات
- 2-عميل نقل الملفات يمرر اسم المضيف إلى عميل دنس
- 3-كل كمبيوتر، بعد تمهيده، يعرف عنوان ملقم دنس واحد. يرسل عميل دنس رسالة إلى ملقم دنس مع استعلام يعطي اسم ملقم نقل الملفات باستخدام عنوان إب المعروف لخادم دنس

- ٤-يستجيب ملقم دنس مع عنوان إب لخدم نقل الملفات المطلوب
- ٥-يقوم خادم دنس بتمرير عنوان إب إلى عميل نقل الملفات
- ٦-يستخدم عميل نقل الملفات الآن عنوان إب المستلم للوصول إلى خادم نقل الملفات



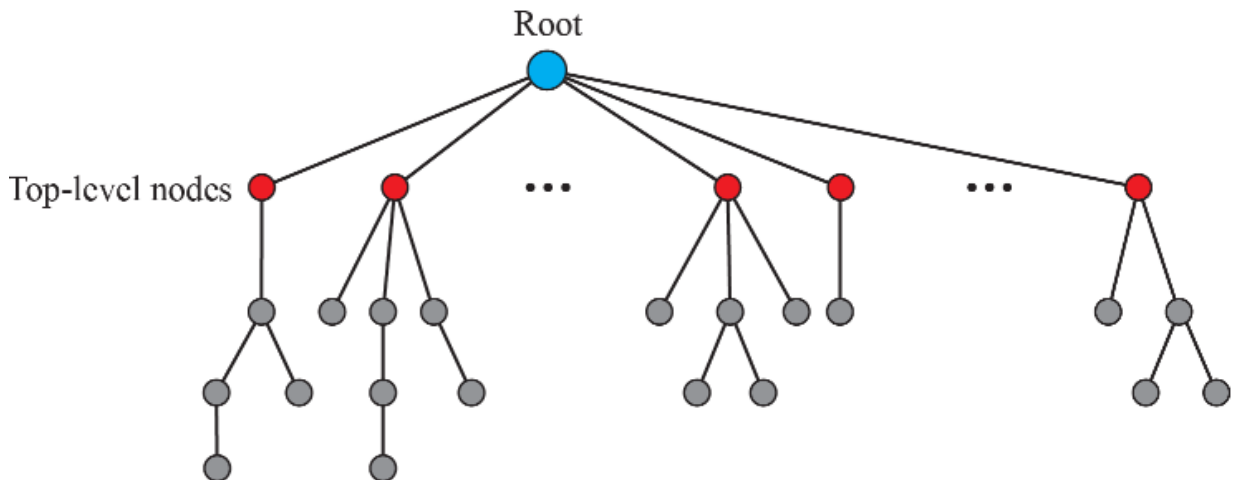
### 26.6.1 Name Space

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 names must be unique because the addresses are unique. A name space that maps each address to a unique name can be organized in two ways:

- 1-Flat: a name is assigned to an address. A name in this space is a sequence of characters without structure
- 2-Hierarchical name space, each name is made of several parts. The first part can define the nature of the organization, the second part can define the name of an organization, the third part can define departments in the organization, and so on.

ولكي تكون غامضة، يجب اختيار الأسماء المخصصة للآلات بعناية من مساحة اسم مع التحكم الكامل في الربط بين الأسماء وعناوين إب. وبعبارة أخرى، يجب أن تكون الأسماء فريدة لأن العناوين فريدة. يمكن تنظيم مساحة اسم تخزين كل عنوان إلى اسم فريد بطريقتين: شقة: يتم تعيين اسم إلى عنوان. اسم في هذا الفضاء هو تسلسل من الأحرف دون بنية مساحة اسم هرمي، كل اسم مصنوع من عدة أجزاء. الجزء الأول يمكن تحديد طبيعة المنظمة، والجزء الثاني يمكن تحديد اسم منظمة، والجزء الثالث يمكن تحديد الإدارات في المنظمة، وهم جرا

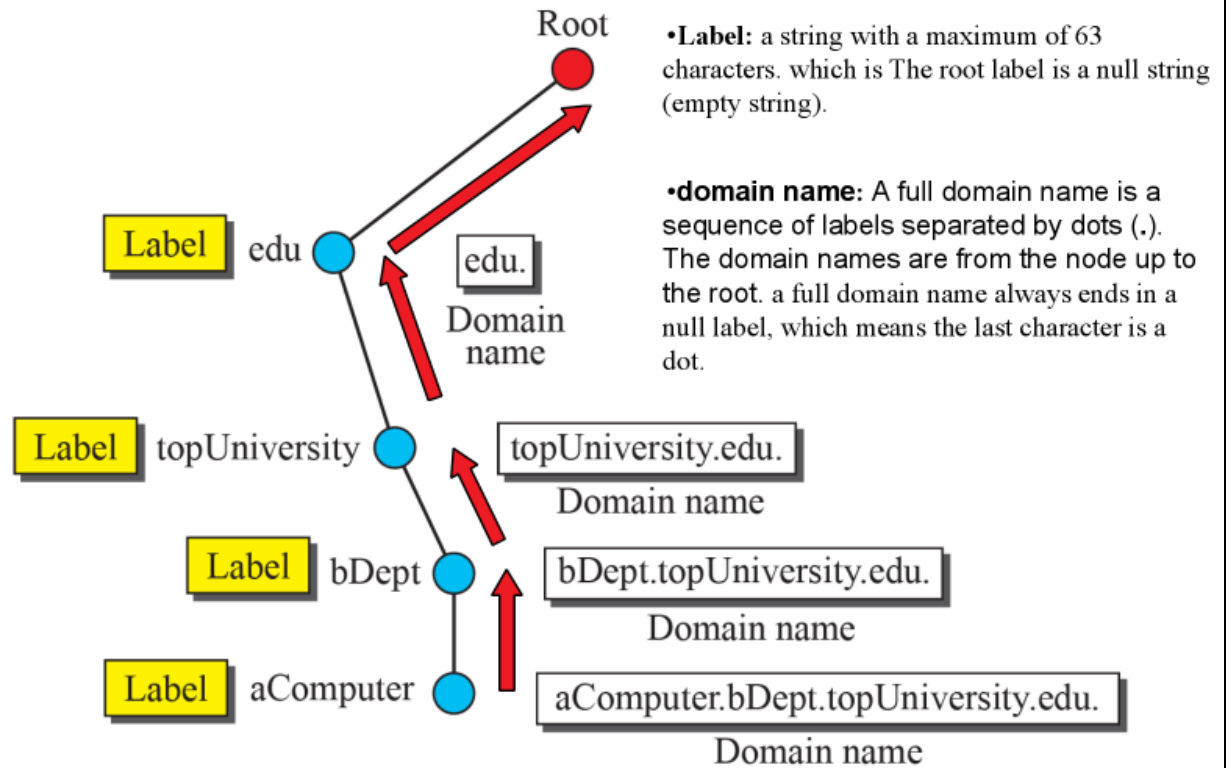
**Figure 26.29: Domain name space**



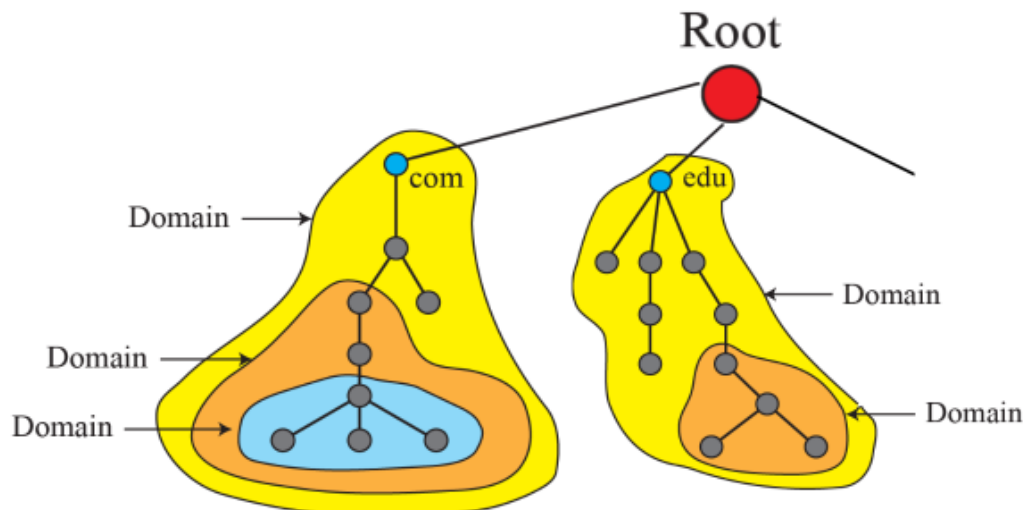
The names are defined in an inverted-tree structure with the root at the top. The tree can have only 128 levels: level 0 (root) to level 127

يتم تعريف الأسماء في هيكل شجرة مقلوب مع الجذر في الأعلى. الشجرة يمكن أن يكون فقط مستويات ١٢٨: المستوى ٠ (الجذر) إلى مستوى ١٢٧

**Figure 26.30: Domain names and labels**



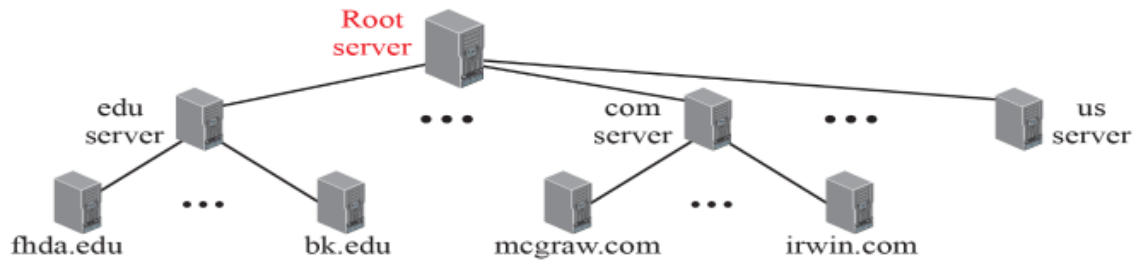
**Figure 26.31: Domains**



- **domain** is a subtree of the domain name space.
- The name of the domain is the name of the node at the top of the subtree.
- The domain may itself be divided into domains.



**Figure 26.32: Hierarchy of name servers**



The information contained in the domain name space must be stored. It is very inefficient to store it in one computer, because responding to requests from all over the world places a heavy load on the system. Also, It is not reliable because any failure makes the data inaccessible

The solution: Hierarchy of Name Servers:

distribute the information among many computers called DNS servers (How?)

\*by dividing the whole space into many domains → we let the root and create sub trees (first-level nodes)→ then domains can be divided further into smaller domains (sub domains)

\*Each server can be responsible (authoritative) for either a large or small domain

we have a hierarchy of servers in the same way that we have a hierarchy of names

يجب تخزين المعلومات الموجودة في مساحة اسم المجال. فمن غير فعالة جدا لتخزينها في جهاز كمبيوتر واحد، لأن الاستجابة لطلبات من جميع أنحاء العالم يضع حمولة ثقيلة على النظام. أيضا، أنها ليست موثوقة لأن أي فشل يجعل البيانات لا يمكن الوصول إليها الحل: التسلسل الهرمي لخوادم الاسم: توزيع المعلومات بين العديد من أجهزة الكمبيوتر التي تسمى ملقمات دنس (كيف؟)

من خلال تقسيم المساحة بأكملها إلى العديد من المجالات → نسمح للجذر وإنشاء أشجار فرعية (العقد من المستوى الأول) ← يمكن تقسيم النطاقات بعد ذلك إلى نطاقات أصغر (نطاقات فرعية)

يمكن أن يكون كل خادم مسؤولا (موثوق) عن نطاق كبير أو صغير لدينا التسلسل الهرمي للخوادم بنفس الطريقة التي لدينا التسلسل الهرمي للأسماء

**Figure 26.33: Zone**

What a server is responsible for or has authority over is called a **zone**.

**If a server does not divide the domain into smaller domains:**

The “domain” and the “zone” refer to the same thing.

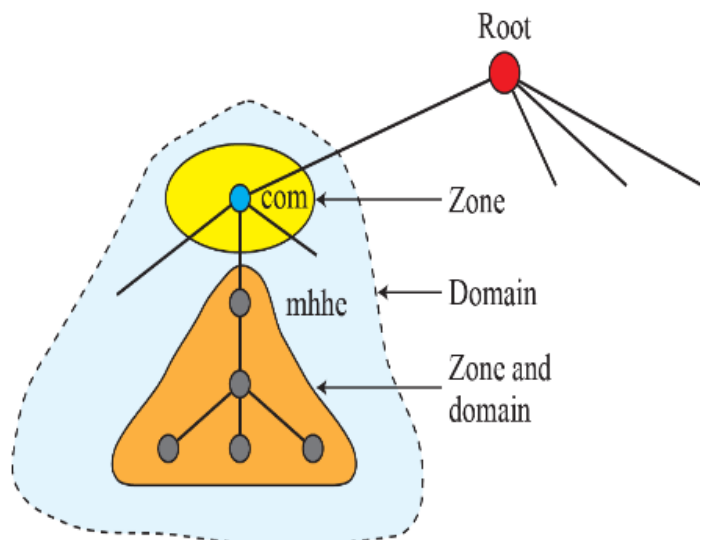
The server makes a database called a **zone file** and keeps all the information for every node under that domain.

**If a server divides its domain into subdomains and delegates part of its authority to other servers,**

“domain” and “zone” refer to different things.

The information about the nodes in the subdomains is stored in the servers at the lower levels, with the original server keeping some sort of reference to these lower-level servers.

Of course, the original server does not free itself from responsibility totally. It still has a zone, but the detailed information is kept by the lower-level servers.



### 26.6.2 DNS in the Internet

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

However, due to the rapid growth of the Internet, it became extremely difficult to keep track of the inverse domains, which could be used to find the name of a host when given the IP address. The inverse domains are now deprecated (see RFC 3425). We, therefore concentrate on the first two

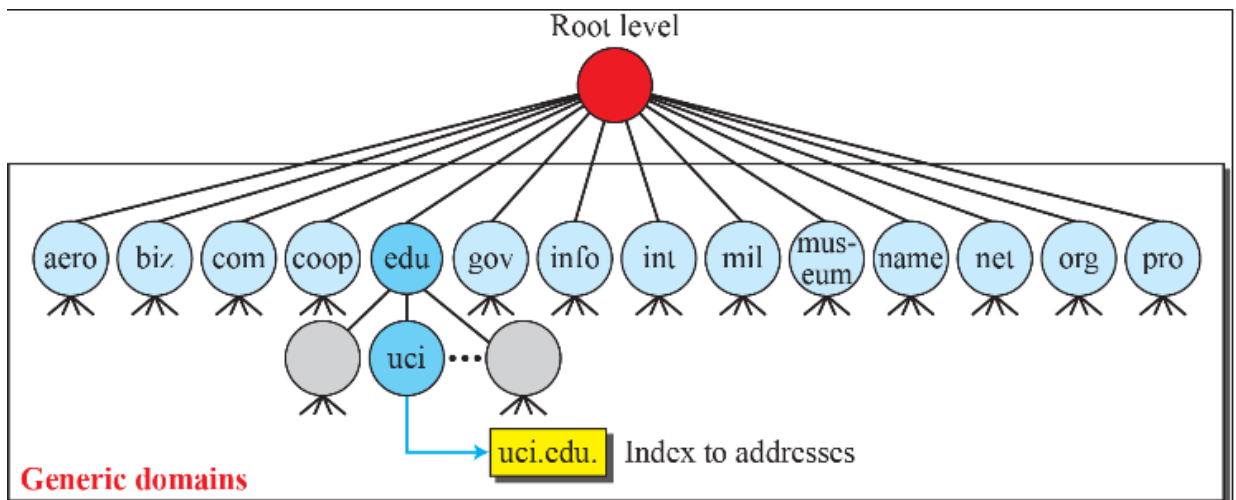
دنس هو بروتوكول يمكن استخدامه في منصات مختلفة. في الإنترنت، قسمت مساحة اسم النطاق (شجرة) في الأصل إلى ثلاثة أقسام مختلفة للنطاقات العامة، والنطاقات القطرية، والنطاقات العكسية.

ومع ذلك، نظرا للنمو السريع للإنترنت، أصبح من الصعب للغاية لتتبع المجالات العكسي، والتي يمكن استخدامها للعثور على اسم المضيف عند إعطاء عنوان إب. تم الآن إيقاف النطاقات العكسية (راجع رك ٣٤٢٥). ولذلك، فإننا نركز على الأولين

**Figure 26.34: Generic domains**

The generic domains define registered hosts according to their generic behavior. Each node in the tree defines a domain, which is an index to the domain name space database. Looking at the tree, we see that the first level in the generic domains section allows 14 possible labels. These labels describe the organization types as listed in Table 26.12

تحدد النطاقات العامة المضيفين المسجلين وفقا لسلوكهم العام. كل عقدة في شجرة تعريف مجال، وهو فهرس إلى قاعدة بيانات مساحة اسم المجال وعند النظر إلى الشجرة، نرى أن المستوى الأول في قسم النطاقات العامة يتيح ١٤ تصنيفا ممكنا. تصف هذه التصنيفات أنواع المؤسسة كما هو موضح في الجدول ٢٦،١٢



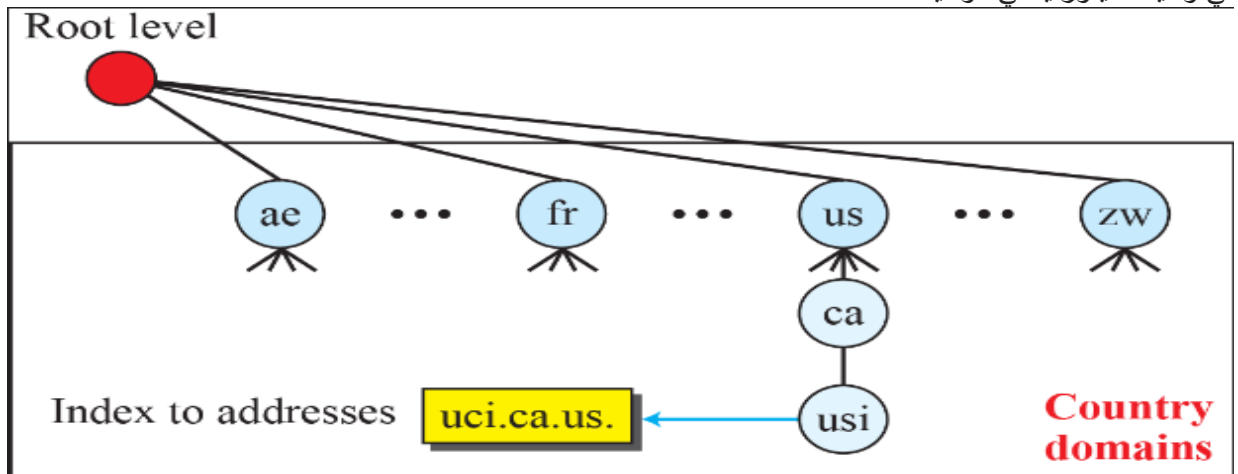
**Table 26.12: Generic domain labels**

Label	Description	Label	Description
<b>aero</b>	Airlines and aerospace	<b>int</b>	International organizations
<b>biz</b>	Businesses or firms	<b>mil</b>	Military groups
<b>com</b>	Commercial organizations	<b>museum</b>	Museums
<b>coop</b>	Cooperative organizations	<b>name</b>	Personal names (individuals)
<b>edu</b>	Educational institutions	<b>net</b>	Network support centers
<b>gov</b>	Government institutions	<b>org</b>	Nonprofit organizations
<b>info</b>	Information service providers	<b>pro</b>	Professional organizations

### Figure 26.35: Country domains

The country domains section uses two-character country abbreviations (us for United States) Second labels can be organizational, or they can be more specific national designations In the figure, the address uci.ca.us. can be translated to University of California in the state of California in the United States

يستخدم قسم نطاقات البلد الاختصارات القطرية المكونة من حرفين (الولايات المتحدة للولايات المتحدة) يمكن أن تكون التسميات الثانية تنظيمية، أو يمكن أن تكون تسميات وطنية أكثر تحديدا في الشكل، عنوان uci.ca.us. يمكن ترجمتها إلى جامعة كاليفورنيا في ولاية كاليفورنيا في الولايات المتحدة



### 26.6.3 Resolution

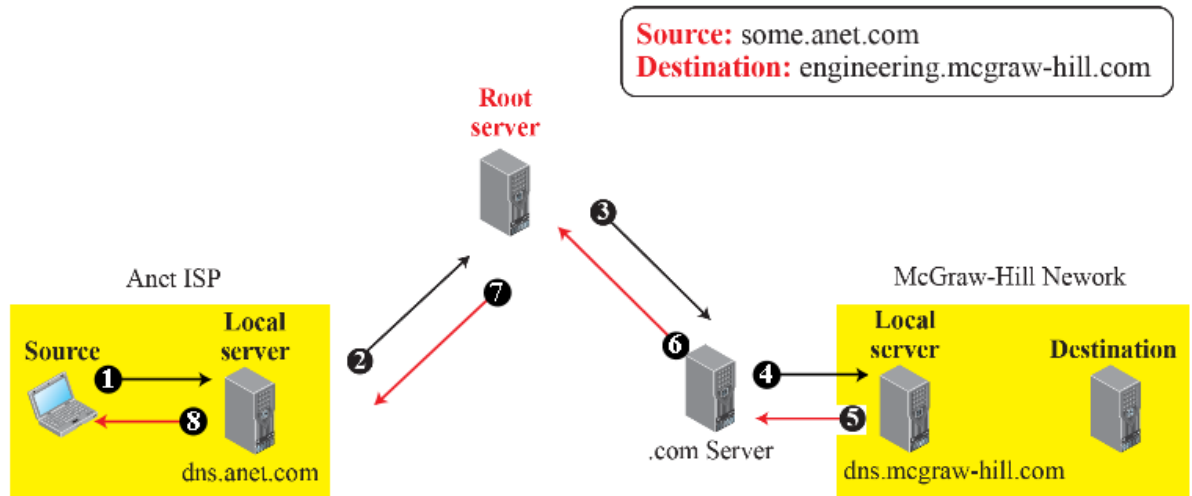
name-address resolution: Mapping a name to an address

DNS is designed as a client-server application. A host that needs to map an address to a name or a name to an address calls a DNS client named as 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.

اسم عنوان القرار: تعيين اسم إلى عنوان . تم تصميم نظام أسماء النطاقات كتطبيق خادم-عميل. المضيف الذي يحتاج إلى تعيين عنوان إلى اسم أو اسم إلى عنوان يدعو عميل دنس اسمه كمحلل يقوم المحلل بالوصول إلى أقرب ملقم دنس مع طلب تعيين. إذا كان الخادم لديه المعلومات، فإنه يرضي محلل؛ وإلا فإنه يشير إما إلى المحلل إلى خوادم أخرى أو يطلب من خوادم أخرى تقديم المعلومات.

**Figure 26.36: Recursive resolution**

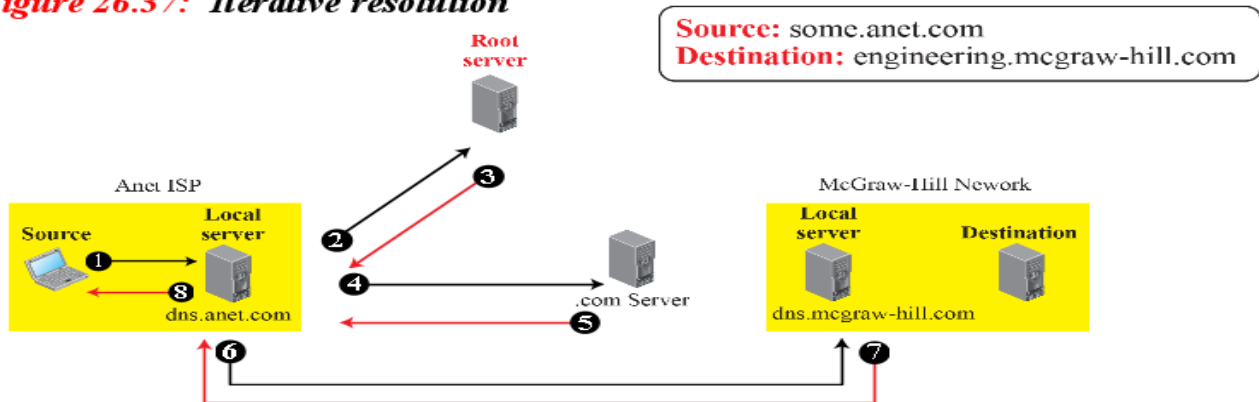


The Figure shows a simple example of a recursive resolution.

We assume that an application program running on a host named some.anet.com needs to find the IP address of another host named engineering.mcgraw-hill.com.

ويعين الشكل مثال بسيط على قرار العودية. نفترض أن برنامج تطبيق يعمل على مضيف اسمه some.anet.com يحتاج إلى العثور على عنوان إيب لمضيف آخر اسمه engineering.mcgraw-hill.com

**Figure 26.37: Iterative resolution**



In **iterative resolution**, each server that does not know the mapping sends the IP address of the next server back to the one that requested it. The messages shown by events 2, 4, and 6 contain the same query. The message shown by event 3 contains the IP address of the top-level domain server. The message shown by event 5 contains the IP address of the McGraw-Hill local DNS server. The message shown by event 7 contains the IP address of the destination.

## 26.6.4 Caching

Each time a server receives a query for a name that is not in its domain, it needs to search its database for a server IP address. Reduction of this search time would increase efficiency.

DNS handles this with a mechanism called caching:

When a server asks for a mapping from another server and receives the response, it stores this information in its cache memory before sending it to the client.

في كل مرة يتلقى ملقم استعلام عن اسم غير موجود في مجاله، فإنه يحتاج للبحث قاعدة البيانات الخاصة به لعنوان إيب الملقم. ومن شأن تقليل وقت البحث هذا أن يزيد من الكفاءة. يتعامل نظام أسماء النطاقات مع آلية تسمى التخزين المؤقت:

عندما يطلب الملقم تعيين من ملقم آخر ويتلقى الاستجابة، فإنه يخزن هذه المعلومات في ذاكرة التخزين المؤقت قبل إرسالها إلى العميل.

### 26.6.5 Resource Records

The zone information associated with a server is implemented as a set of resource records. In other words, a name server stores a database of resource records. A resource record is a 5-tuple structure, as shown below

يتم تنفيذ معلومات المنطقة المرتبطة بملقم كمجموعة من سجلات الموارد. وبعبارة أخرى، يقوم خادم اسم بتخزين قاعدة بيانات لسجلات الموارد. سجل الموارد هو بنية 5-تول، كما هو مبين أدناه

## (Domain Name, Type, Class, TTL, Value)

**Table 26.13: DNS types**

Type	Interpretation of value
A	A 32-bit IPv4 address (see Chapter 4)
NS	Identifies the authoritative servers for a zone
CNAME	Defines an alias for the official name of a host
SOA	Marks the beginning of a zone
MX	Redirects mail to a mail server
AAAA	An IPv6 address (see Chapter 4)

### 26.6.6 DNS Messages

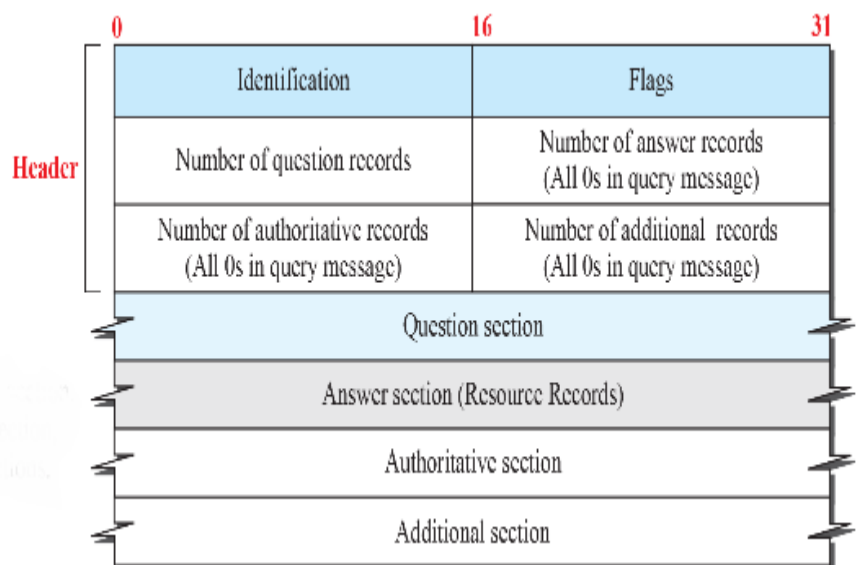
To retrieve information about hosts, DNS uses two types of messages: query and response. Both types have the same format as shown in Figure 26.38

لاسترداد المعلومات حول المضيفين، يستخدم دنس نوعين من الرسائل: الاستعلام والاستجابة. وكلا النوعين له نفس الشكل كما هو مبين في الشكل ٢٦-٣٨

**Figure 26.38: DNS message**

**Note:**

The query message contains only the question section. The response message includes the question section, the answer section, and possibly two other sections.



\*Identification is used by the client to match the response with the query

\*Flag defines whether the message is a query or response

- \*The next four fields in the header define the number of each record type in the message
- \*Question section consists of one or more question records→ in both query and response messages
- \*Answer section consists of one or more resource records→ only in response messages
- \*Authoritative section gives information (domain name) about one or more authoritative servers for the query
- \*Additional section provides additional information that may help the resolver

- \* يتم استخدام التعريف من قبل العميل لمطابقة الاستجابة مع الاستعلام
- \* يحدد العلم ما إذا كانت الرسالة عبارة عن استعلام أو استجابة
- \* تحدد الحقول الأربعة التالية في الرأس عدد كل نوع سجل في الرسالة
- \* يتكون قسم السؤال من واحد أو أكثر من سجلات الأسئلة → في كل من الاستعلام والاستجابة الرسائل
- \* يتكون قسم الإجابة من واحد أو أكثر من سجلات الموارد → فقط في رسائل الاستجابة
- \* يعطي القسم الموثوق معلومات (اسم المجال) عن واحد أو أكثر من خوادم موثوقة للاستعلام
- \* يوفر قسم إضافي معلومات إضافية قد تساعد المحلل

## Example 26.13

In UNIX and Windows, the nslookup utility can be used to retrieve address/name mapping. The following shows how we can retrieve an address when the domain name is given.

```
$nslookup www.forouzan.biz
Name: www.forouzan.biz
Address: 198.170.240.179
```

### 26.6.7 Registrars

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

كيف تتم إضافة نطاقات جديدة إلى نظام أسماء النطاقات؟ ويتم ذلك من خلال أمين السجل، وهو كيان تجاري معتمد من إيكان. يقوم المسجل أولاً بالتحقق من أن اسم النطاق المطلوب فريد ومن ثم يدخله في قاعدة بيانات دنس

### 26.6.8 DDNS

When the DNS was designed, no one predicted that there would be so many address changes. In DNS, when there is a change, such as adding a new host, removing a host, or changing an IP address, the change must be made to the DNS master file. These types of changes involve a lot of manual updating. The size of today's Internet does not allow for this kind of manual operation. The DNS master file must be updated dynamically. The Dynamic Domain Name System (DDNS) therefore was devised to respond to this need.

عندما تم تصميم نظام أسماء النطاقات، لم يتنبأ أحد بأنه سيكون هناك الكثير من التغييرات في العناوين. في دنس، عندما يكون هناك تغيير، مثل إضافة مضيف جديد أو إزالة مضيف أو تغيير عنوان إيب، يجب إجراء التغيير إلى ملف دنس الرئيسي. هذه الأنواع من التغييرات تنطوي على الكثير من التحديث اليدوي. حجم الإنترنت اليوم لا يسمح لهذا النوع من التشغيل اليدوي. يجب تحديث ملف دنس الرئيسي ديناميكياً. ولذلك تم وضع نظام أسماء النطاقات الديناميكية (دنز) للاستجابة لهذه الحاجة

### 26.6.9 Security of DNS

DNS is one of the most important systems in the Internet infrastructure; it provides crucial services to Internet users. Applications such as Web access or e-mail are heavily dependent on the proper operation of DNS

DNS can be attacked in several ways (how?). a technology named DNS Security (DNSSEC) protect DNS by providing message origin authentication and message integrity using a security service called digital signature

دنس هو واحد من أهم الأنظمة في البنية التحتية للإنترنت. فإنه يوفر خدمات حاسمة لمستخدمي الإنترنت. تعتمد تطبيقات مثل الوصول إلى الويب أو البريد الإلكتروني بشكل كبير على التشغيل الصحيح لنظام أسماء النطاقات يمكن الهجوم على نظام أسماء النطاقات بعدة طرق (كيف؟). تحمي تقنية اسمها دنس سيكوري (دسيك) دنس من خلال توفير مصادقة أصل الرسالة وسلامة الرسائل باستخدام خدمة أمان تسمى التوقيع الرقمي

تم بحمد الله

---

دعواتكم لي بالتوفيق  
شاديه السلمي