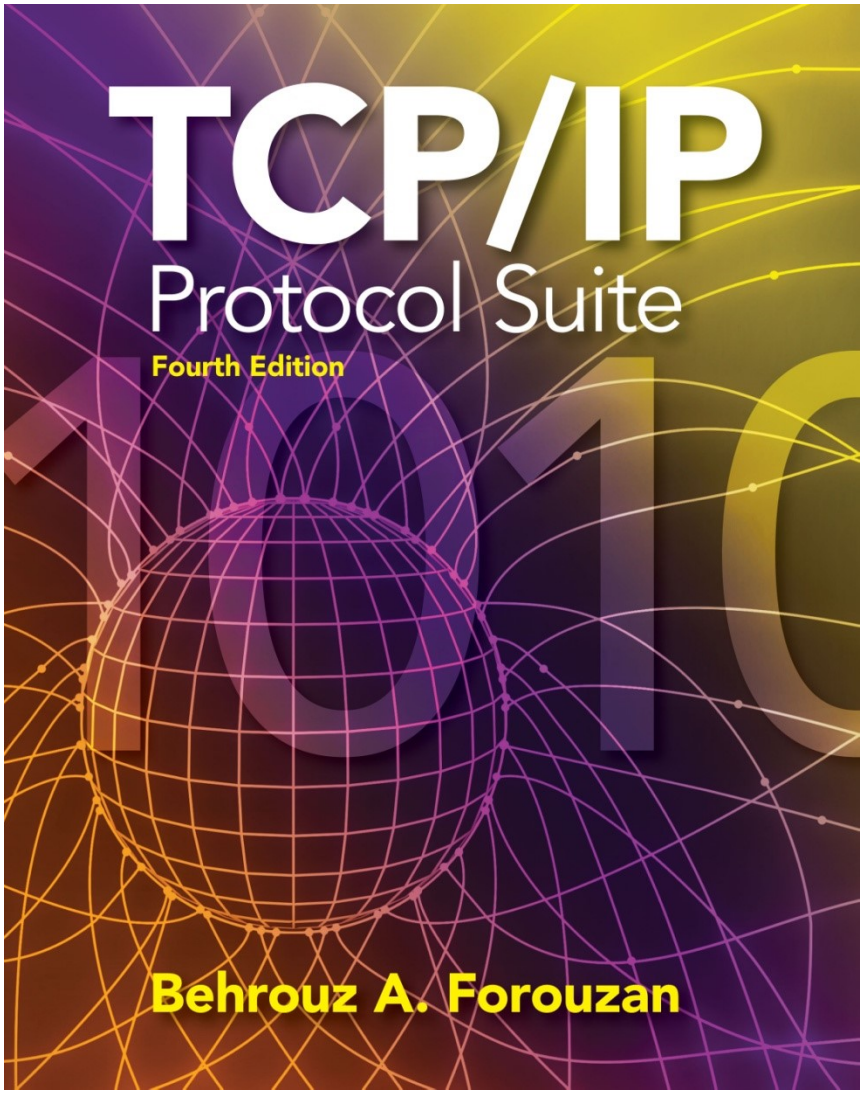
The McGraw-Hill Companies

Chapter 19

Domain Name System (DNS)



OBJECTIVES:

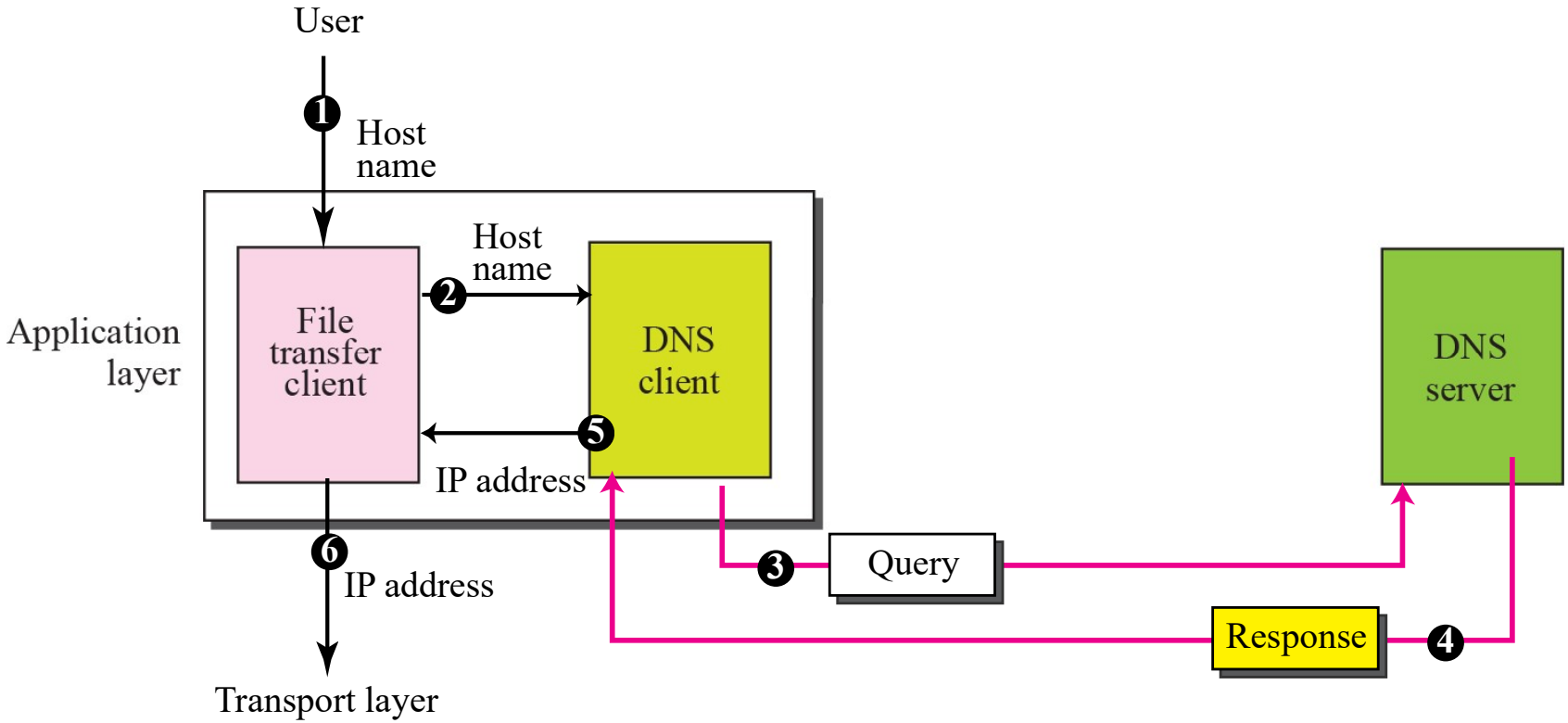
- To describe the purpose of DNS.
- To define the concept of domains and domain name space.
- To describe the distribution of name spaces and define zones.
- To discuss the use of DNS in the Internet and describe three categories of domains: generic, country, and reverse.
- To discuss name-address resolution and show the two resolution methods: recursive and iterative.
- To show the format of DNS message and how they can be compressed.
- To discuss DDNS and DNSSEC..

Chapter Outline

19-1 NEED FOR DNS

To identify an entity, TCP/IP protocols use the IP address, which uniquely identifies the connection of a host to the Internet. However, people prefer to use names instead of numeric addresses. Therefore, we need a system that can map a name to an address or an address to a name.

Figure 19.1 *Purpose of DNS*



19-2 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: flat or hierarchical.

Topics Discussed in the Section

- ✓ **Flat Name Space**
- ✓ **Hierarchical Name Space**
- ✓ **Domain Name Space**
- ✓ **Domain**
- ✓ **Distribution of Name Space**

Figure 19.2 *Domain name space*

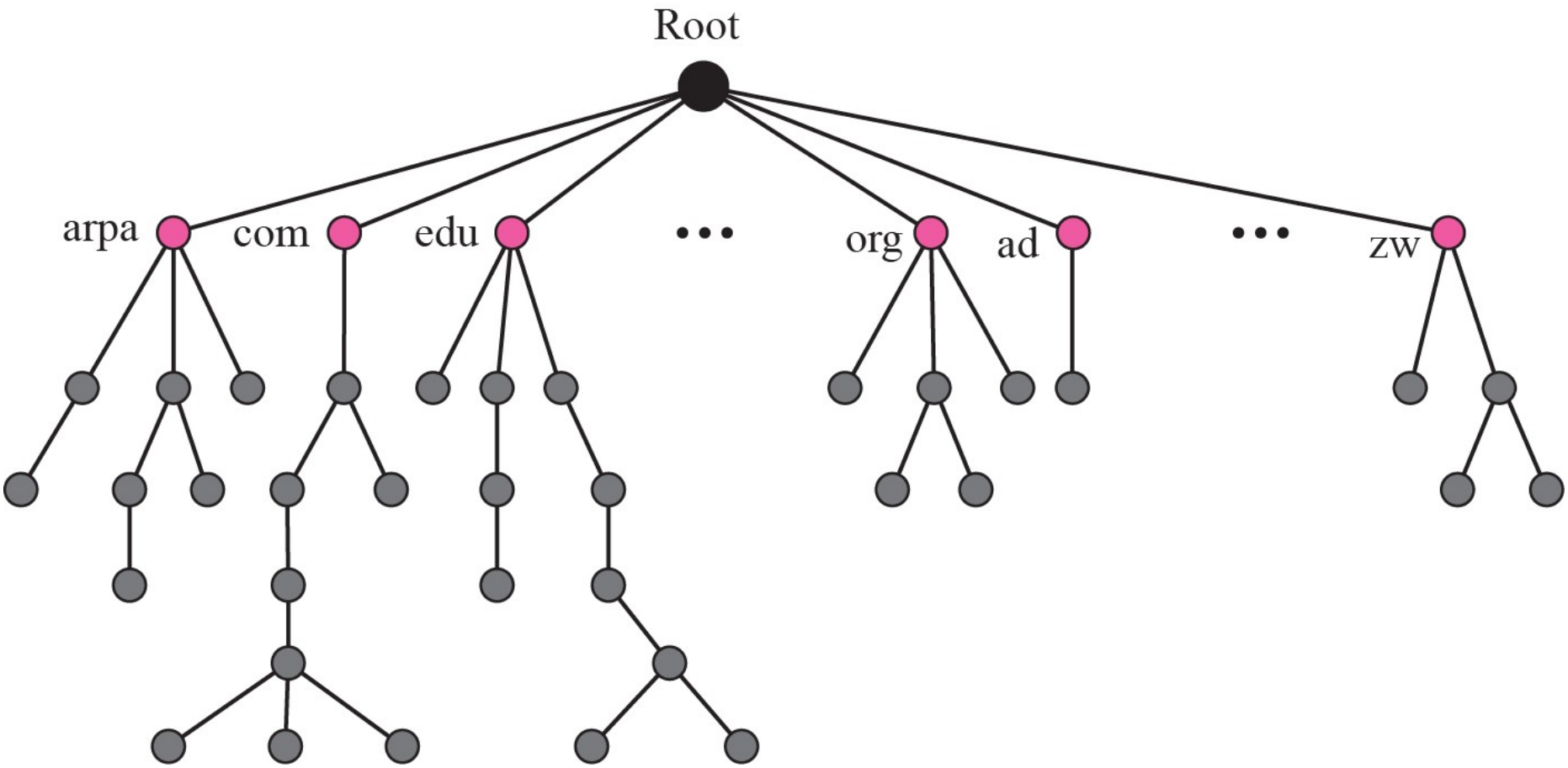


Figure 19.3 *Domain names and labels*

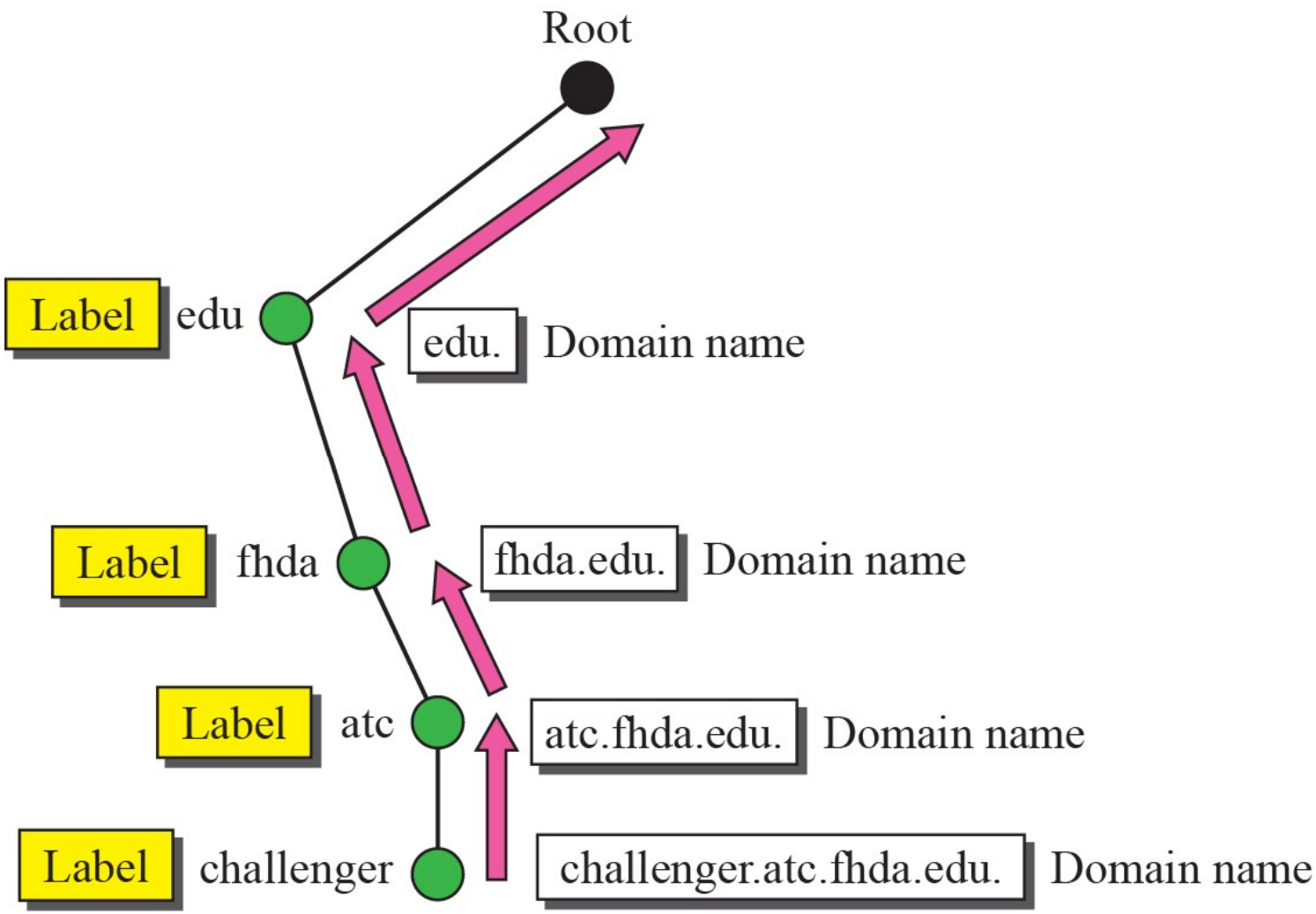


Figure 19.4 *FQDN and PQDN*

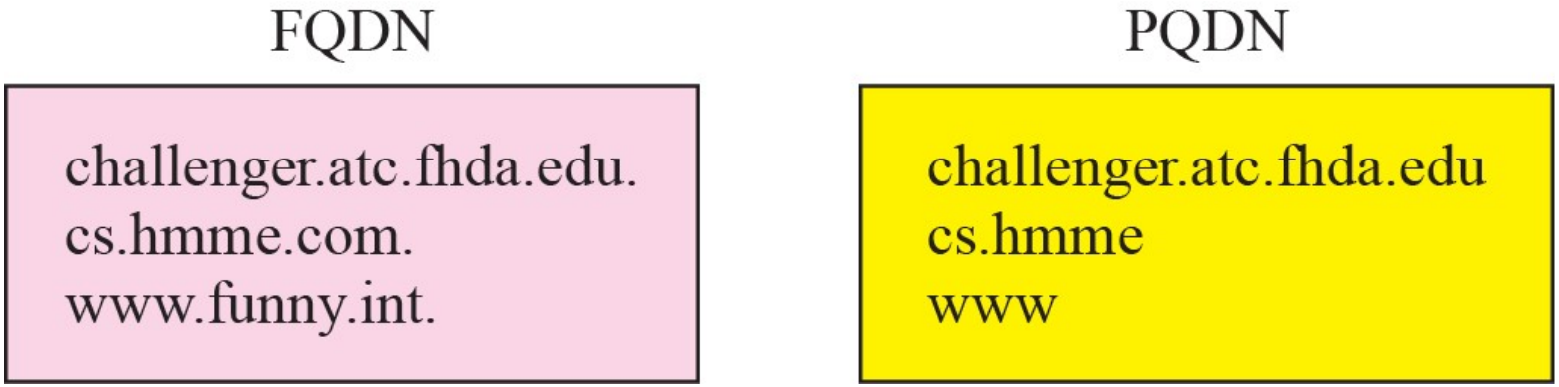


Figure 19.5 *Domains*

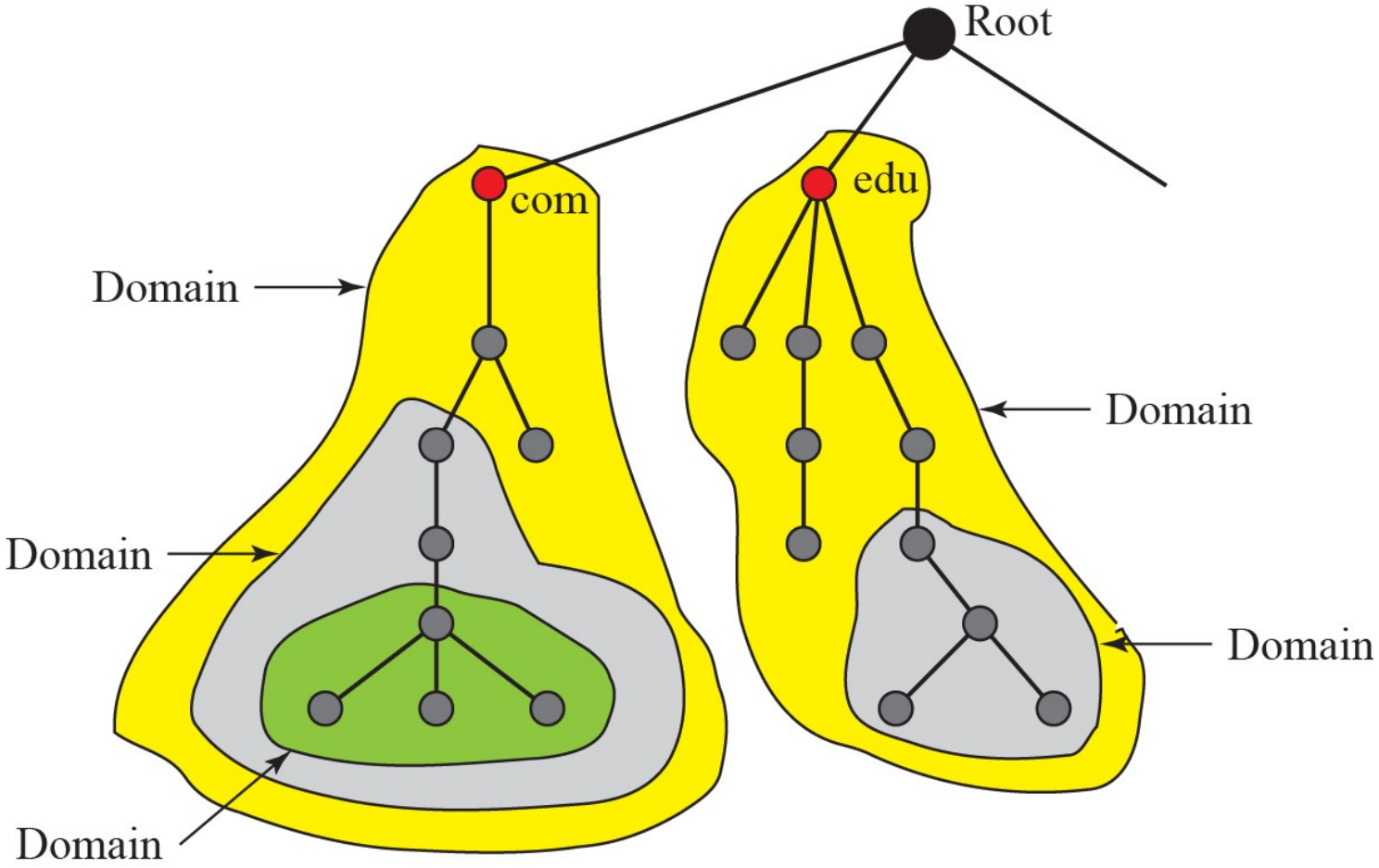


Figure 19.6 *Hierarchy of name servers*

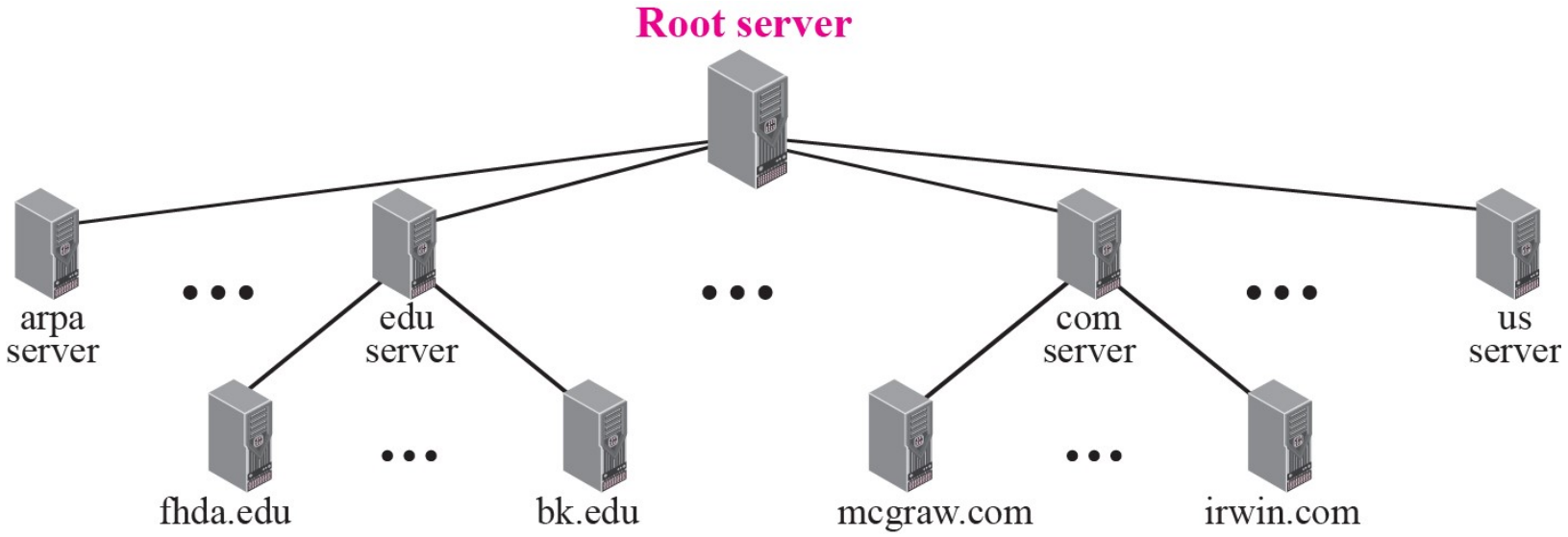
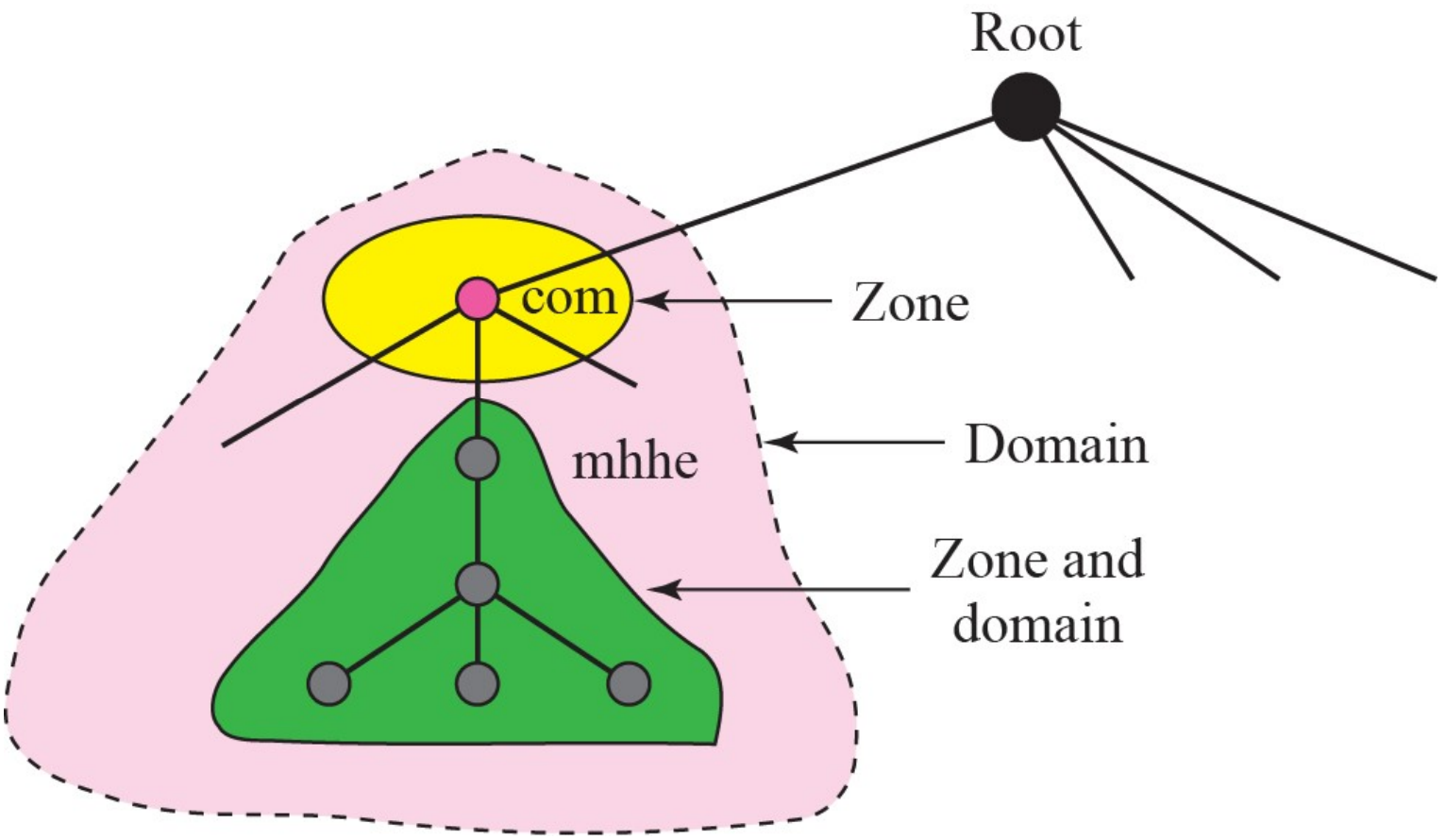


Figure 19.7 *Zones and domains*



Note

A primary server loads all information from the disk file; the secondary server loads all information from the primary server.

When the secondary downloads information from the primary, it is called zone transfer.

19-3 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 (see Figure 19.8).

Topics Discussed in the Section

- ✓ **Generic Domains**
- ✓ **Country Domains**
- ✓ **Inverse Domain**
- ✓ **Registrar**

Figure 19.8 *DNS used in the Internet*

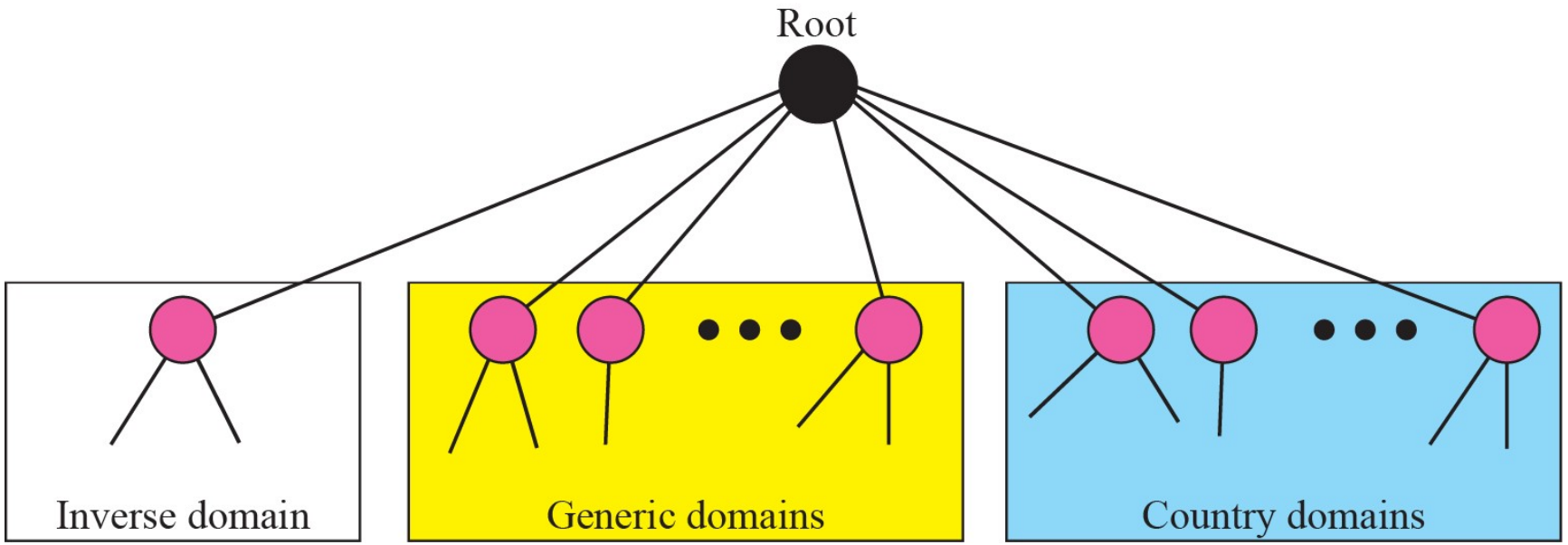


Figure 19.9 *Generic domains*

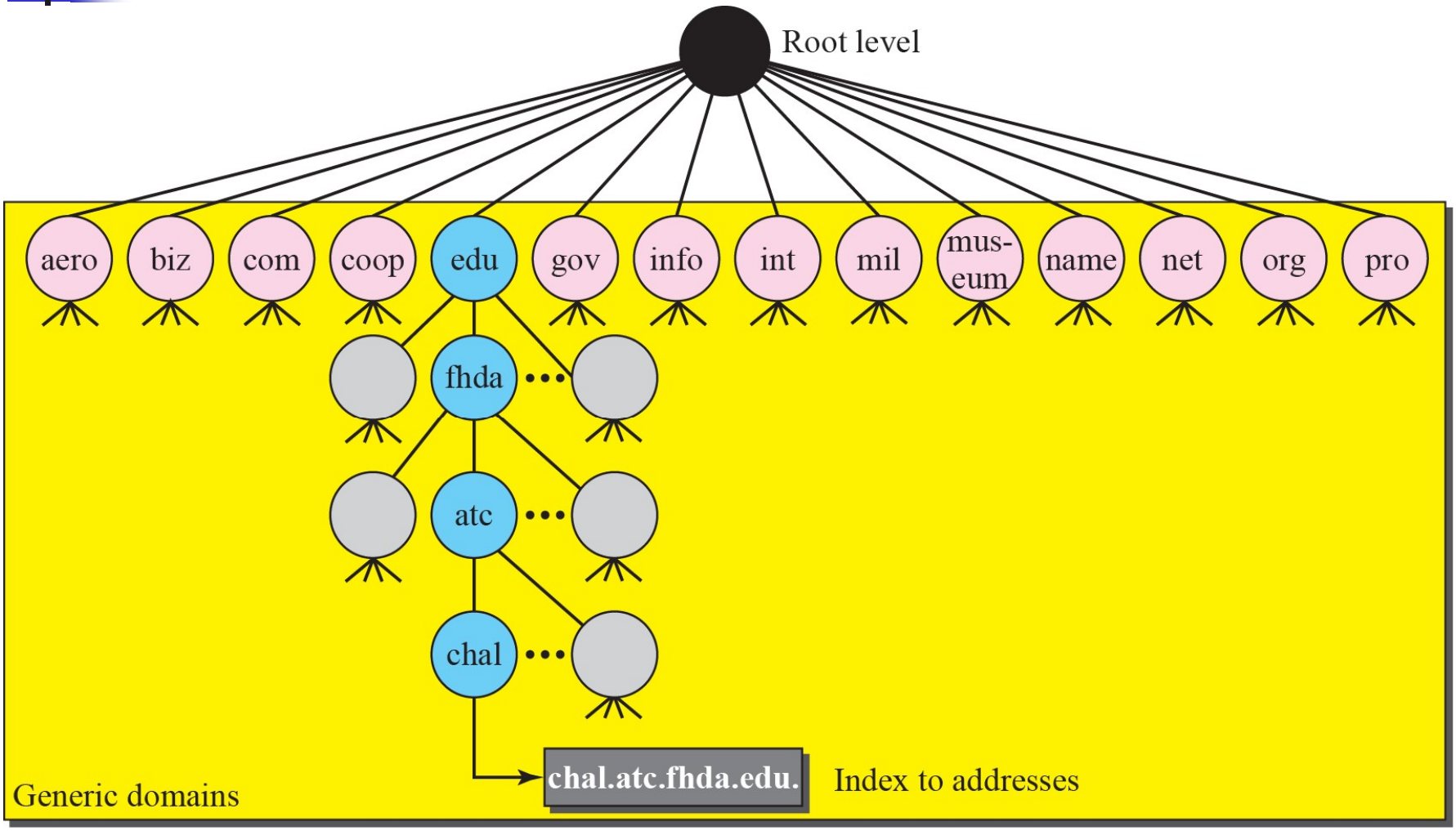


Table 19.1 *Generic domain labels*

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

Figure 19.10 *Country domains*

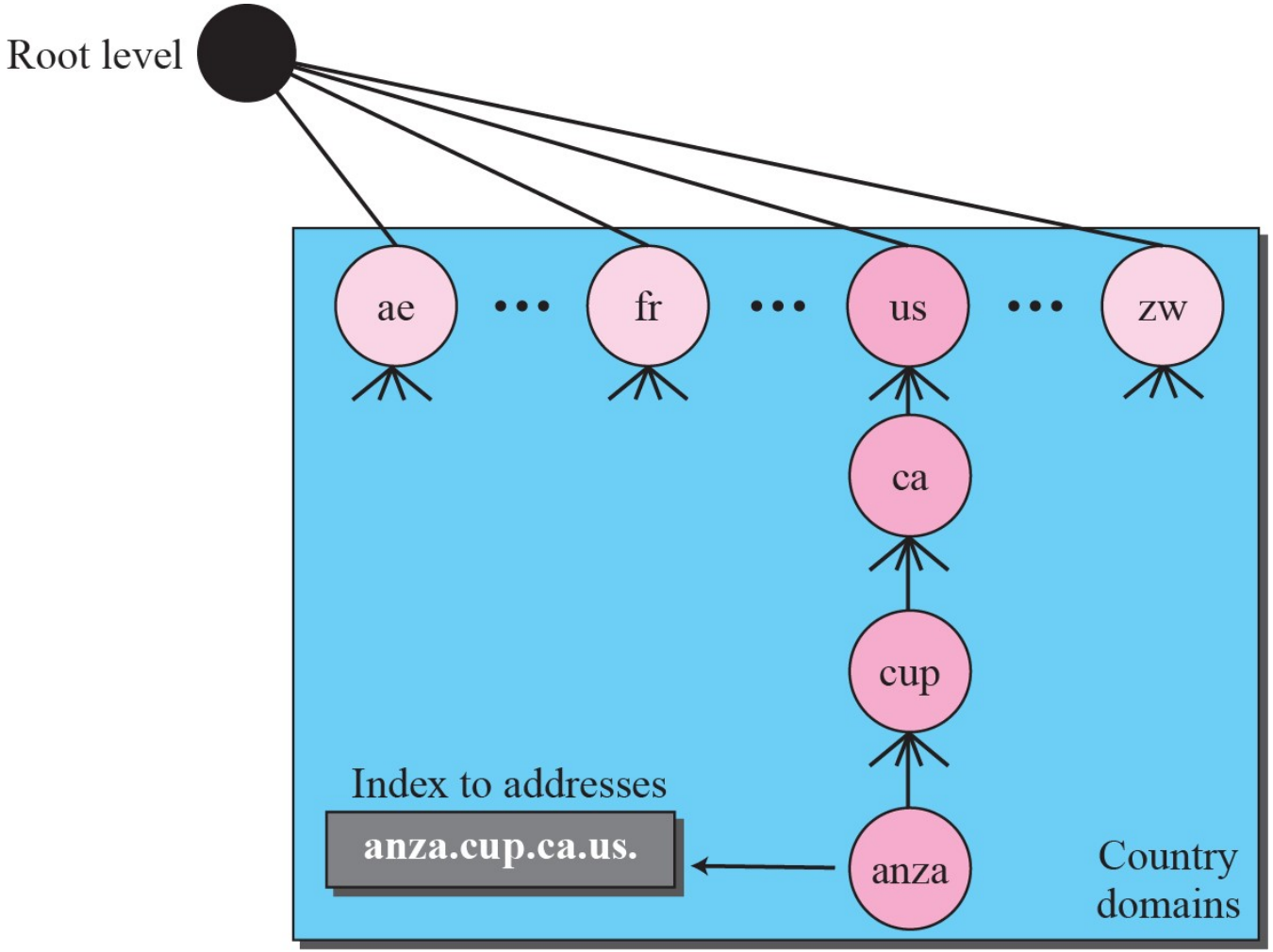
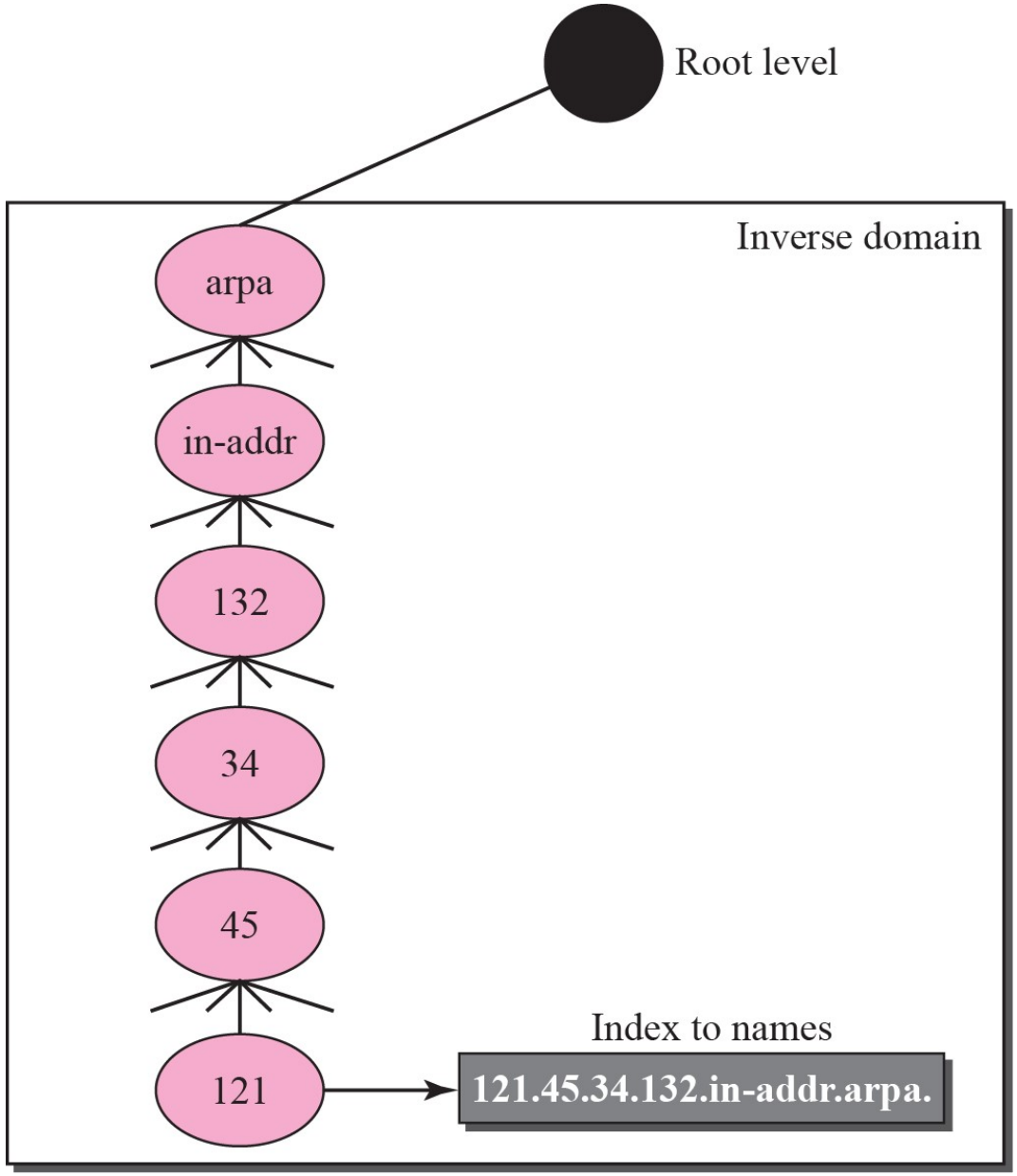


Figure 19.11 *Inverse domain*



19-4 RESOLUTION

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

Topics Discussed in the Section

- ✓ **Resolver**
- ✓ **Mapping Names to Addresses**
- ✓ **Mapping Addresses to Names**
- ✓ **Recursive Resolution**
- ✓ **Iterative Resolution**
- ✓ **Caching**

Figure 19.12 *Recursive resolution*

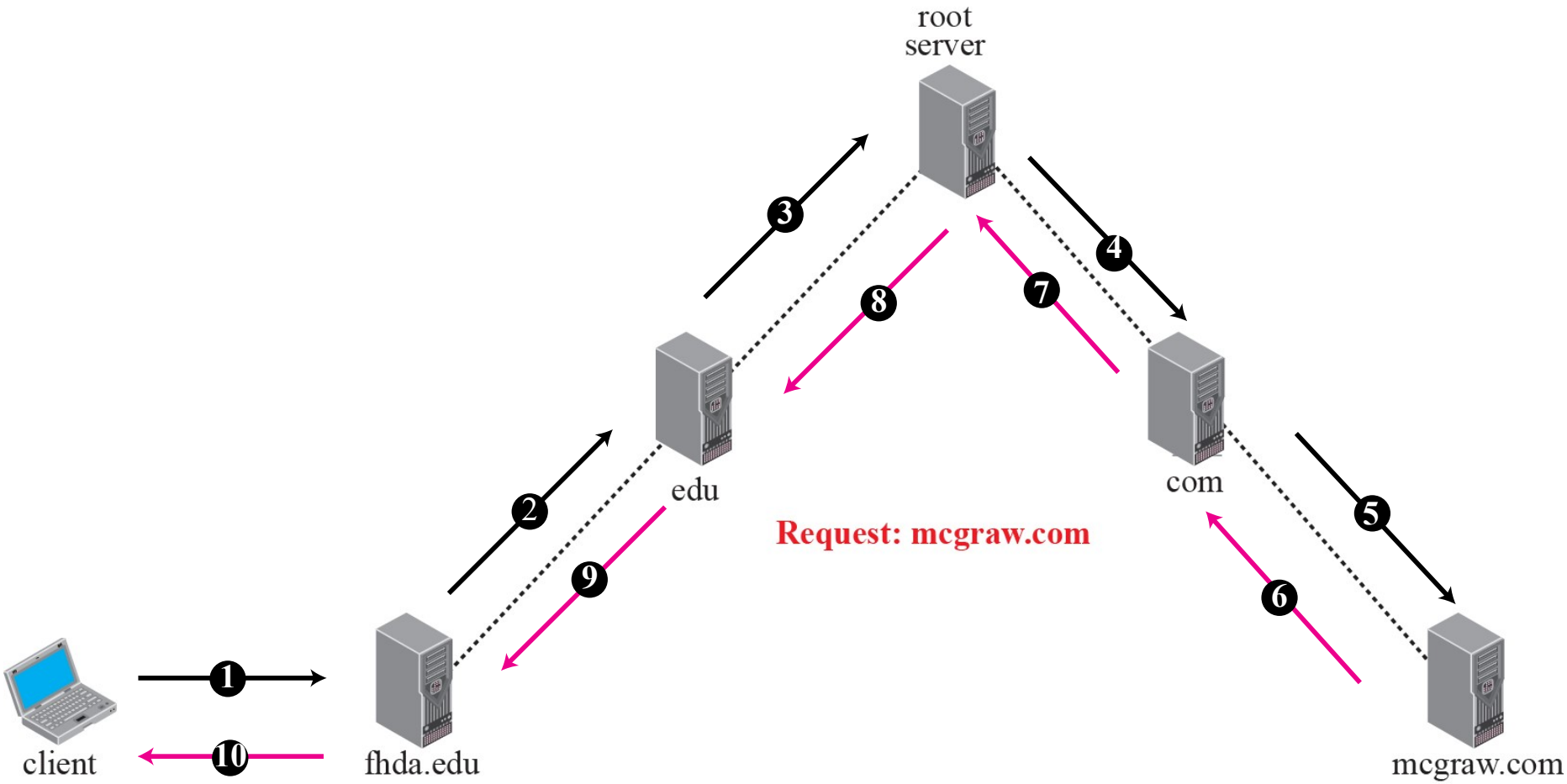
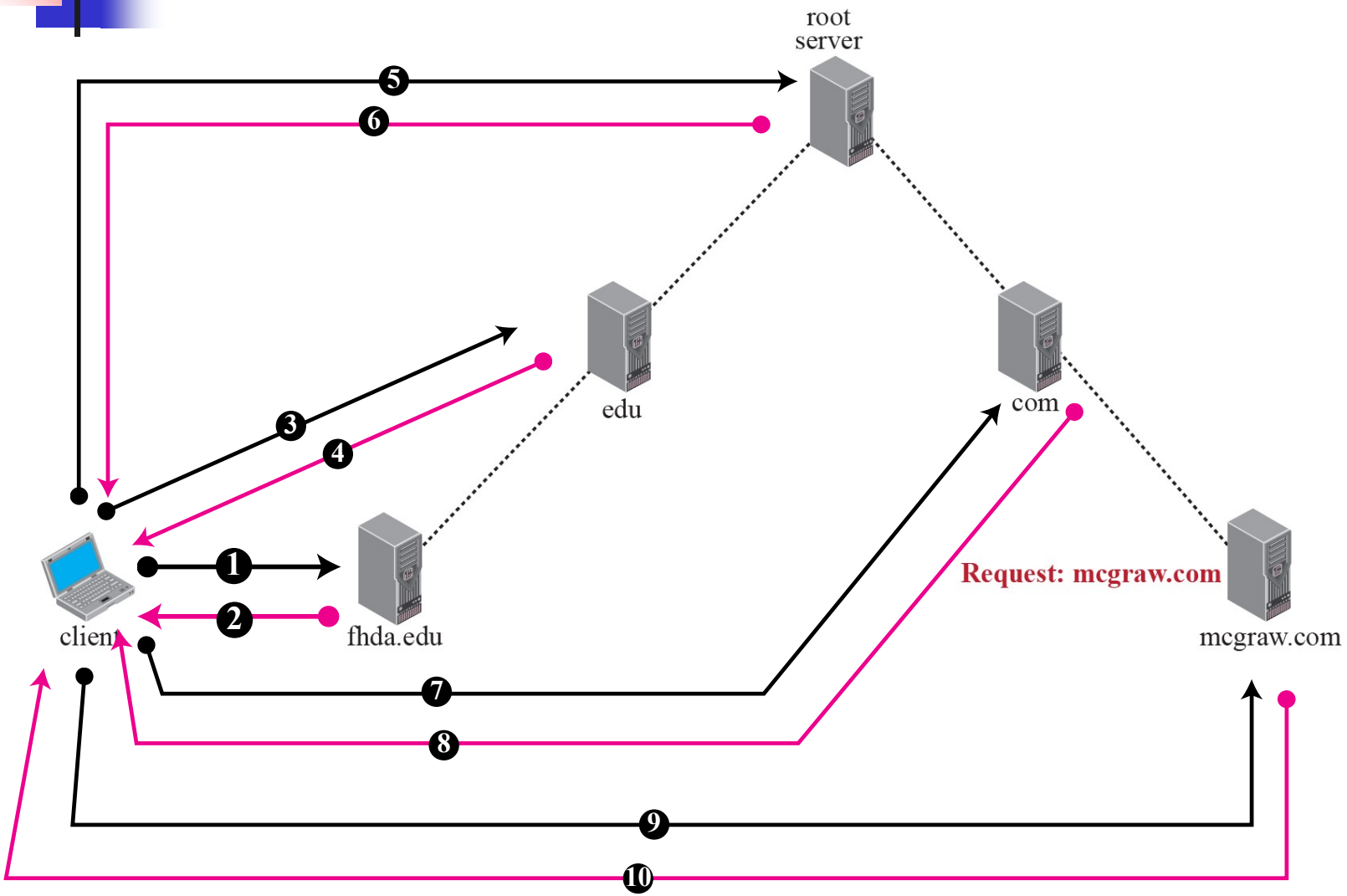


Figure 19.13 *Iterative resolution*



19-5 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 (see Figure 19.14).

Topics Discussed in the Section

- ✓ **Header**

Figure 19.14 *Query and response messages*

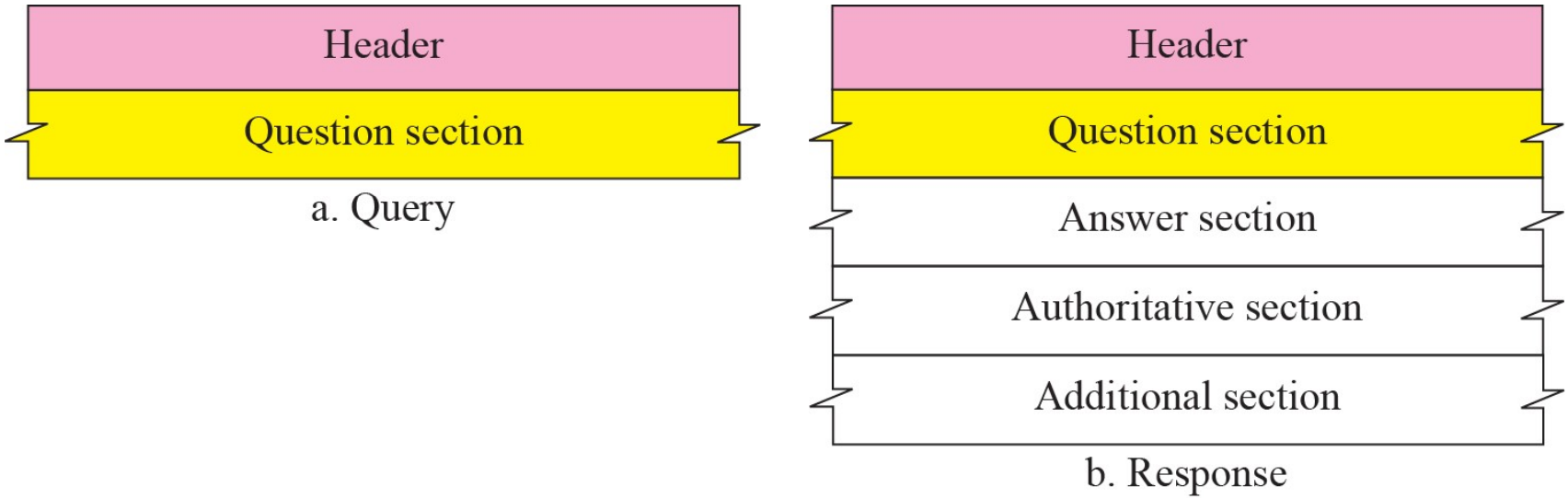


Figure 19.15 *Header format*

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)

Figure 19.16 *Flags field*

Table 19.2 *Values of rCode*

Value	*Meaning*	*Value*	*Meaning*
0	No error	4	Query type not supported
1	Format error	5	Administratively prohibited
2	Problem at name server	6–15	Reserved
3	Domain reference problem		

19-6 TYPES OF RECORDS

As we saw in the previous section, 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.

Topics Discussed in the Section

- ✓ **Question Record**
- ✓ **Resource Record**

Figure 19.17 *Question record format*

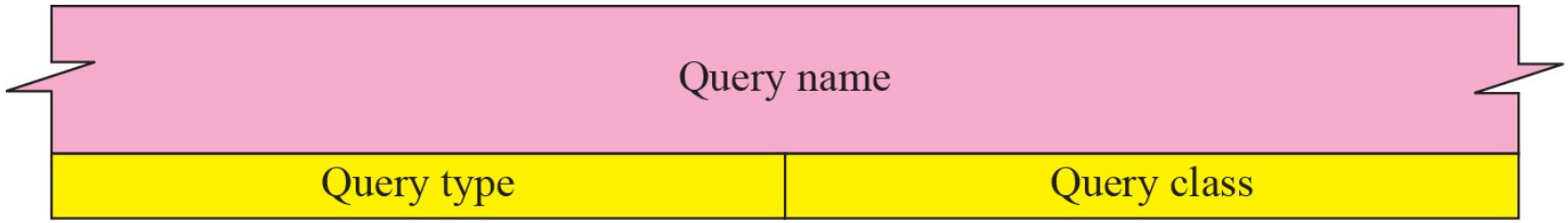


Figure 19.18 *Query name format*

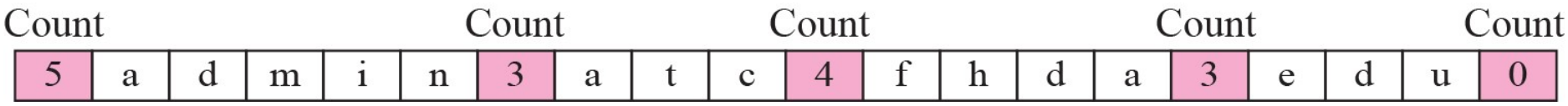


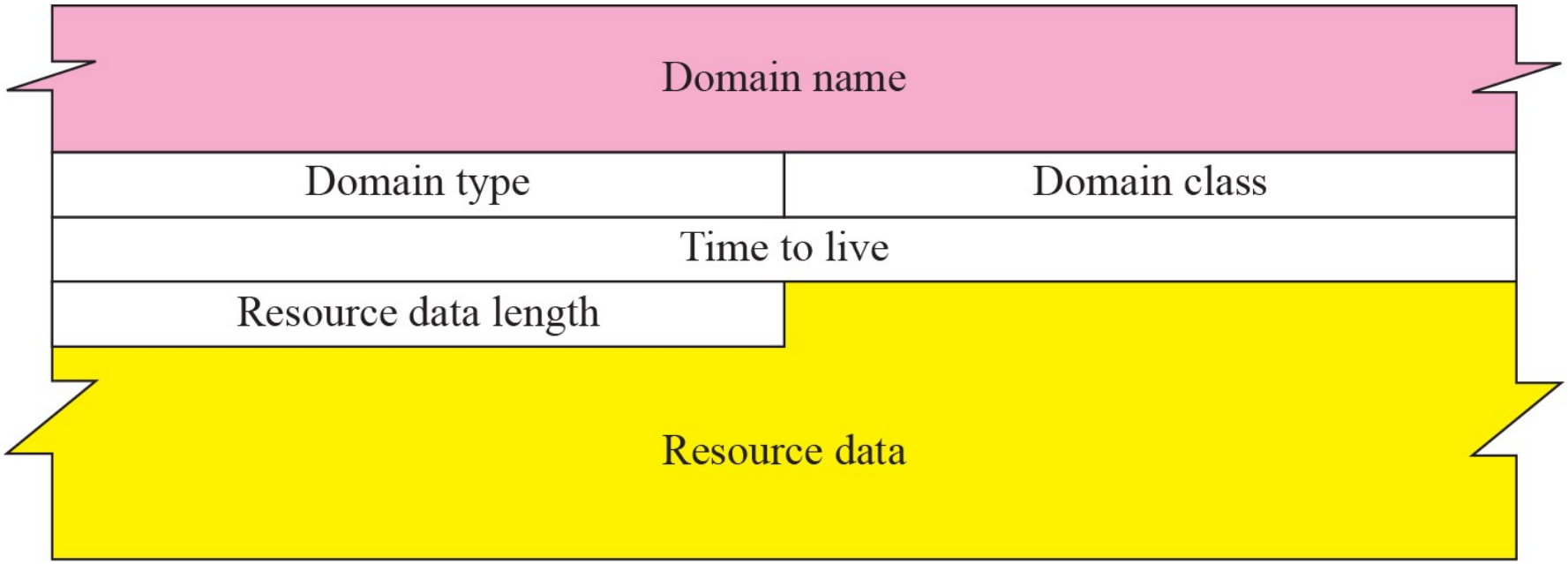
Table 19.3 *Types*

Type	*Mnemonic*	*Description*
1	A	**Address.** A 32-bit IPv4 address. It converts a domain name to an address.
2	NS	**Name server.** It identifies the authoritative servers for a zone.
5	CNAME	**Canonical name.** It defines an alias for the official name of a host.
6	SOA	**Start of authority.** It marks the beginning of a zone.
11	WKS	**Well-known services.** It defines the network services that a host provides.
12	PTR	**Pointer.** It is used to convert an IP address to a domain name.
13	HINFO	**Host information.** It defines the hardware and operating system.
15	MX	**Mail exchange.** It redirects mail to a mail server.
28	AAAA	**Address.** An IPv6 address (see Chapter 26).
252	AXFR	A request for the transfer of the entire zone.
255	ANY	A request for all records.

Table 19.4 *Classes*

Class	*Mnemonic*	*Description*
1	IN	Internet
2	CSNET	CSNET network (obsolete)
3	CS	The COAS network
4	HS	The Hesiod server developed by MIT

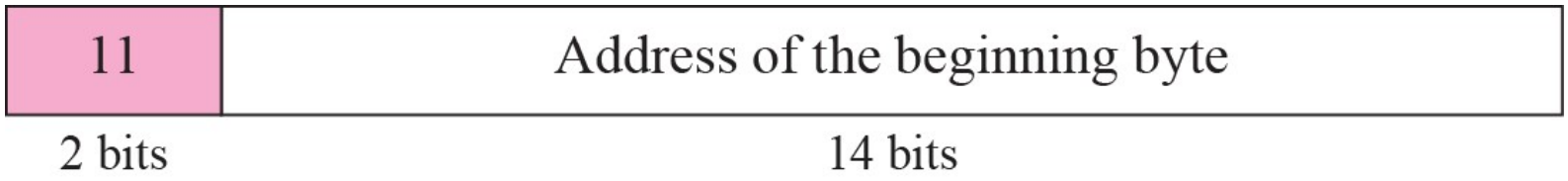
Figure 19.19 *Resource record format*



19-7 COMPRESSION

DNS requires that a domain name be replaced by an offset pointer if it is repeated. For example, in a resource record the domain name is usually a repetition of the domain name in the question record. For efficiency, DNS defines a 2-byte offset pointer that points to a previous occurrence of the domain or part of it. The format of the field is shown in Figure 19.20.

Figure 19.20 *Format of an offset pointer*

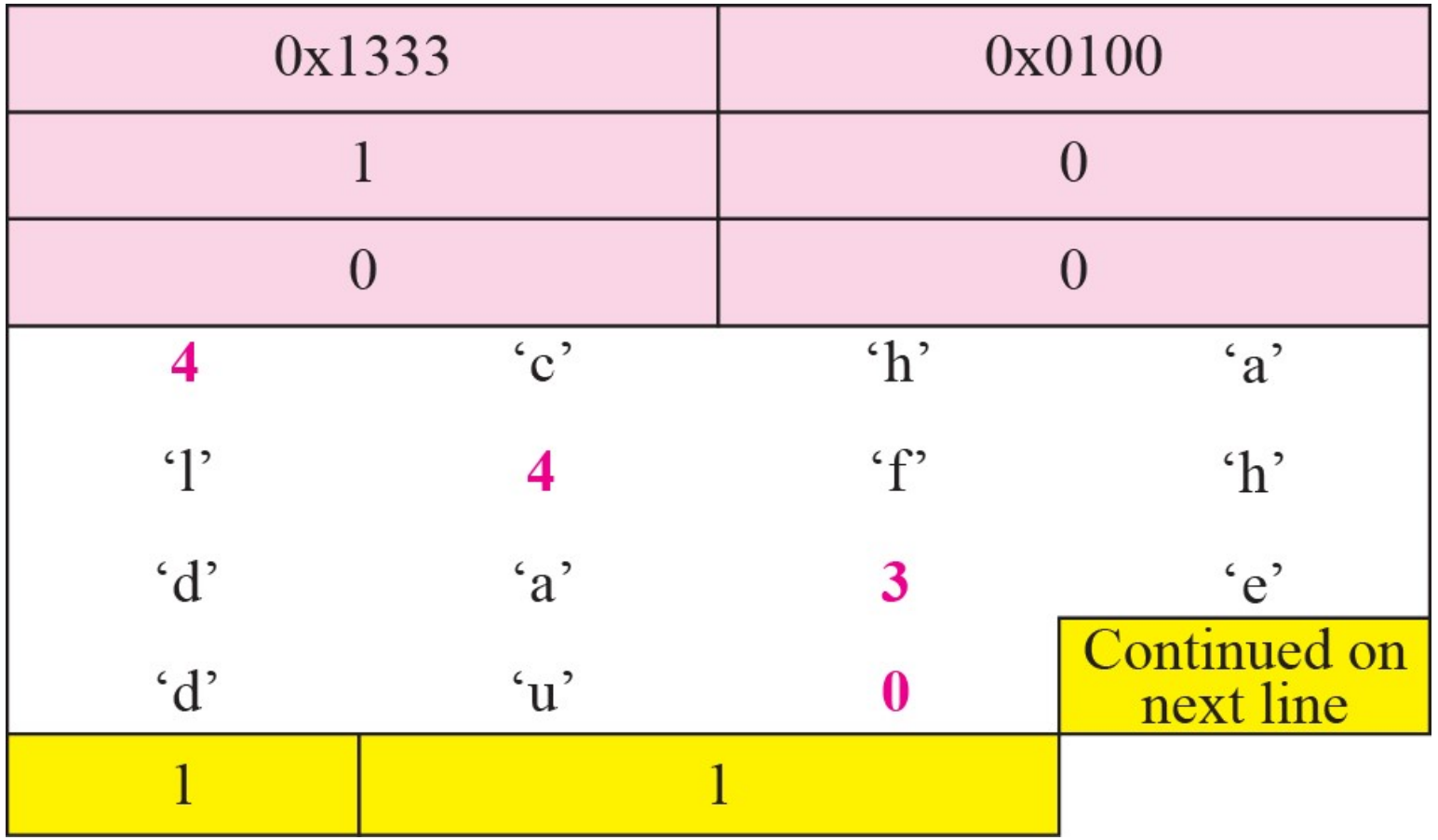


Example 19.1

A resolver sends a query message to a local server to find the IP address for the host "chal.fhda.edu.". We discuss the query and response messages separately. Figure 19.21 shows the query message sent by the resolver. The first 2 bytes show the identifier $(1333)_{16}$. It is used as a sequence number and relates a response to a query. The next bytes contain the flags with the value of 0x0100 in hexadecimal. In binary it is 0000000100000000, but it is more meaningful to divide it into the fields as shown below:

QR	OpCode	AA	TC	RD	RA	Reserved	rCode
0	0000	0	0	1	0	000	0000

Figure 19.21 *Example 19.1: Query message*

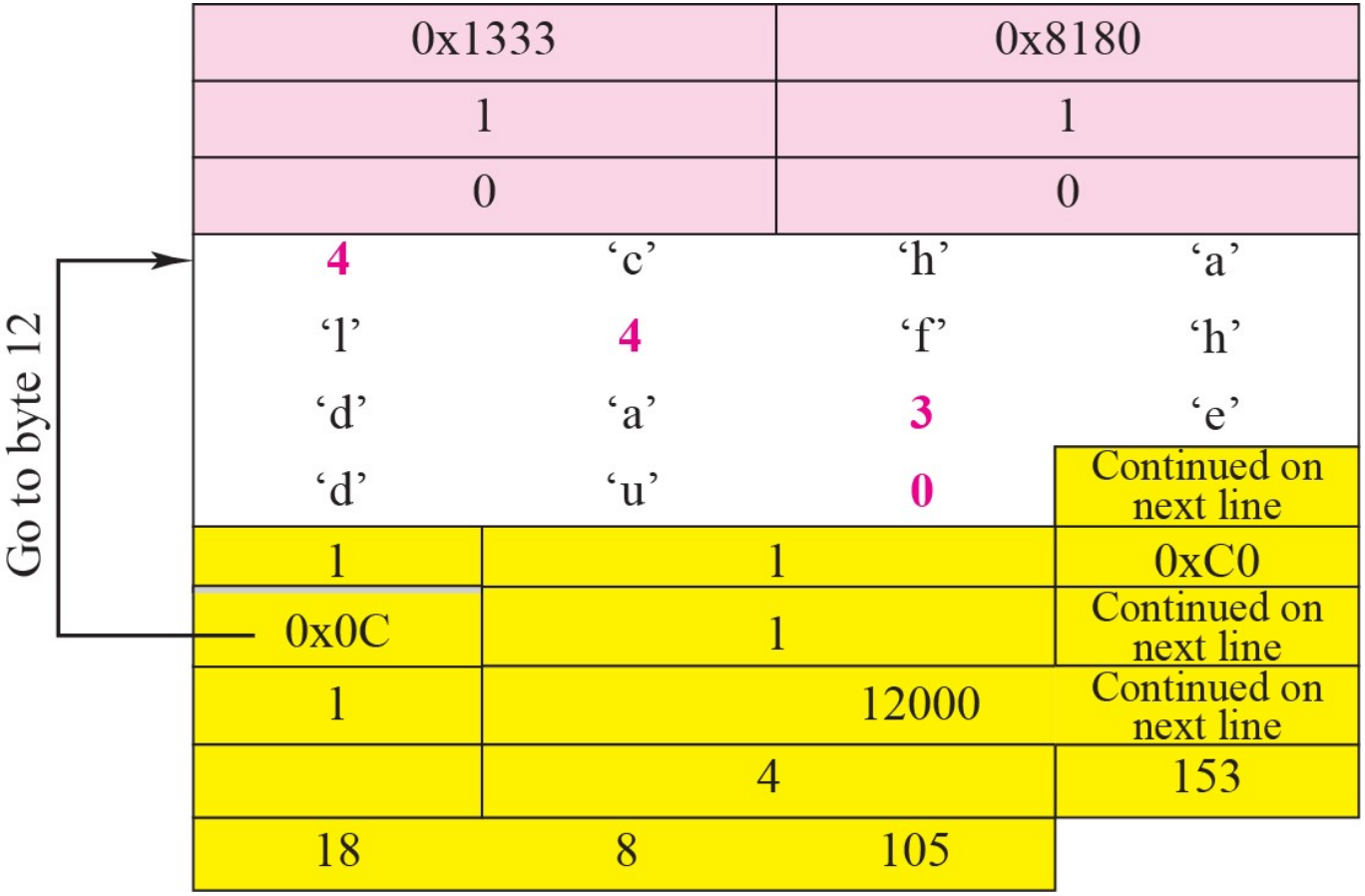


Example 19.1 *Continued*

Figure 19.22 shows the response of the server. The response is similar to the query except that the flags are different and the number of answer records is one. The flags value is 0x8180 in hexadecimal. In binary it is 1000000110000000, but again we divide it into fields as shown below:

QR	OpCode	AA	TC	RD	RA	Reserved	rCode
1	0000	0	0	1	1	000	0000

Figure 19.22 *Example 19.1: Response message*



Example 19.2

An FTP server has received a packet from an FTP client with IP address 153.2.7.9. The FTP server wants to verify that the FTP client is an authorized client. The FTP server can consult a file containing the list of authorized clients. However, the file consists only of domain names. The FTP server has only the IP address of the requesting client, which was the source IP address in the received IP datagram. The FTP server asks the resolver (DNS client) to send an inverse query to a DNS server to ask for the name of the FTP client. We discuss the query and response messages separately. Figure 19.23 shows the query message sent from the resolver to the server.

Figure 19.23 *Example 19.2: Inverse query message*

0x1200		0x0900	
1		0	
0		0	
1	‘9’	**1**	‘7’
1	‘2’	**3**	‘l’
‘5’	‘3’	**7**	‘i’
‘n’	‘-’	‘a’	‘d’
‘d’	‘r’	**4**	‘a’
‘r’	‘p’	‘a’	**0**
12		1	

Example 19.2 *Continued*

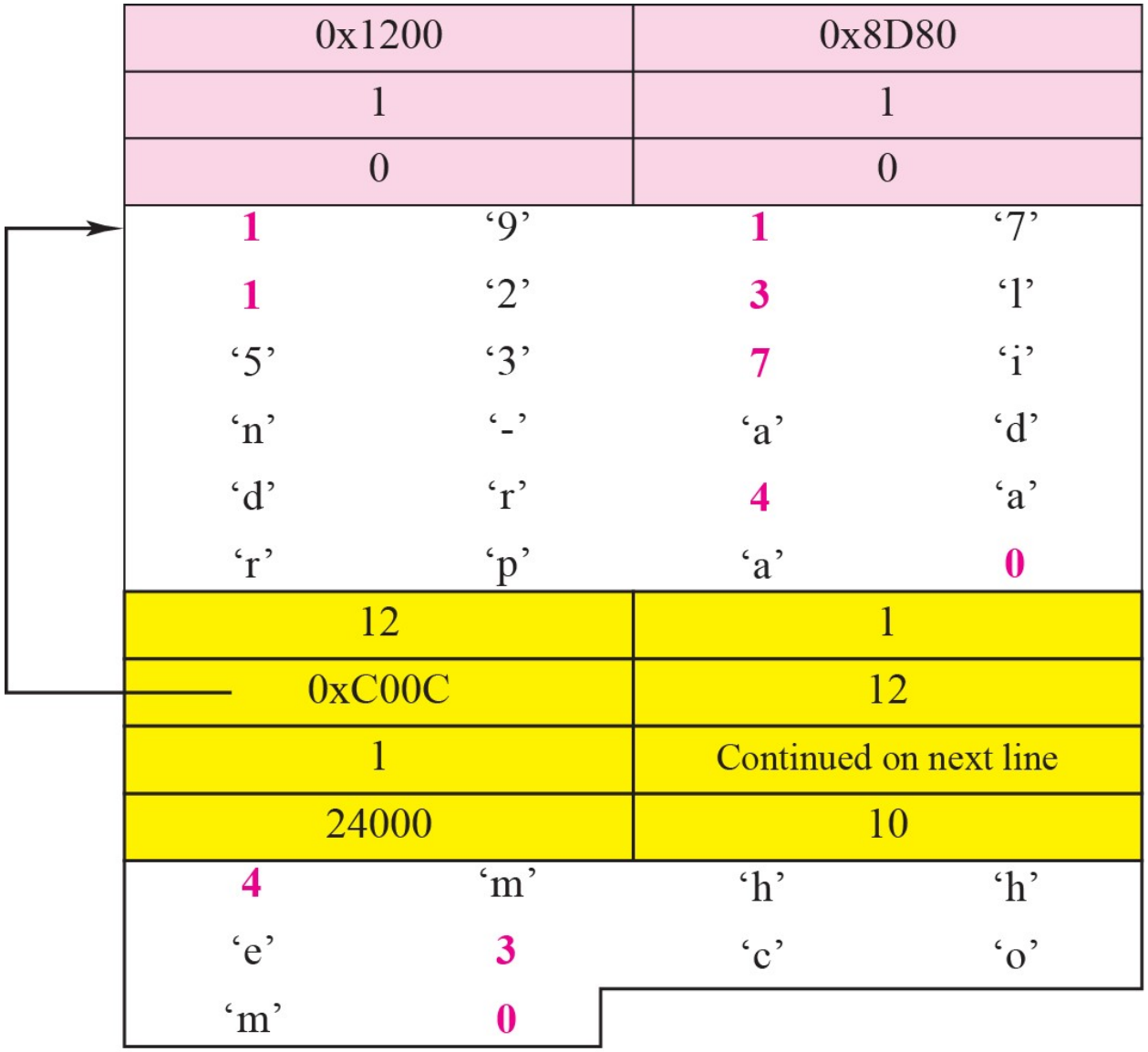
The first 2 bytes show the identifier (0x1200). The flags value is 0x0900 in hexadecimal. In binary it is 0000100100000000, and we divide it into fields as shown below:

QR	OpCode	AA	TC	RD	RA	Reserved	rCode
0	0001	0	0	1	0	000	0000

The OpCode is 0001, which defines an inverse query. The message contains only one question record. The domain name is 19171231537in-addr4arpa. The next 2 bytes define the query type as PTR, and the last 2 bytes define the class as the Internet. Figure 19.24 shows the response. The flags value is 0x8D80 in hexadecimal. In binary it is 1000110110000000, and we divide it into fields as shown below:

QR	OpCode	AA	TC	RD	RA	Reserved	rCode
1	0001	1	0	1	0	000	0000

Figure 19.24 *Example 19.2: Inverse response message*



0x1200		0x8D80	
1		1	
0		0	
1	'9'	1	'7'
1	'2'	3	'l'
'5'	'3'	7	'i'
'n'	'-'	'a'	'd'
'd'	'r'	4	'a'
'r'	'p'	'a'	0
12		1	
0xC00C		12	
1		Continued on next line	
24000		10	
4	'm'	'h'	'h'
'e'	3	'c'	'o'
'm'	0		

Example 19.3

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  fhda.edu
Name:    fhda.edu
Address: 153.18.8.1
```

The nslookup utility can also be used to retrieve the domain name when the address is given as shown below:

```
$ nslookup 153.18.8.1
1.8.18.153.in-addr.arpa name = tiptoe.fhda.edu.
```

19-8 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. In that case, one of two scenarios can occur:

19-9 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. A fee is charged.

19-10 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. The DNS master file must be updated dynamically. The Dynamic Domain Name System (DDNS) therefore was devised to respond to this need.

19-11 SECURITY OF DNS

DNS is one of the most important systems in the Internet infrastructure; it provides crucial services to the 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.

To protect DNS, IETF has devised a technology named DNS Security (DNSSEC) that provides the message origin authentication and message integrity using a security service called digital signature (See Chapter 29).