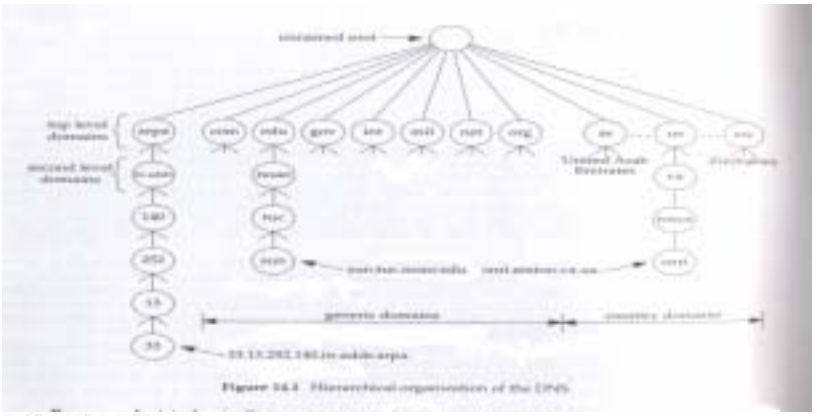
Chapter 14:
DNS: The Domain Name System

Introduction

- **The *Domain Name System* is a distributed database.**
- **To map between hostnames and IP address, and to provide electronic mail routing information.**
- **From an application's point of view, access to the DNS is through a *resolver*. (Ref. Page 55)**
- **The resolver is normally part of the application, rather than part of the operating system kernel (as are the TCP/IP protocols).**
- **The TCP/IP protocols within the kernel know nothing about the DNS.**
- **The most commonly used implementation of the DNS, both resolver and name server, is called BIND (the Berkeley Internet Name Domain server). The server is called *named*.**

DNS Basics

- The DNS name space is hierarchical.



DNS Basic (Cont.)

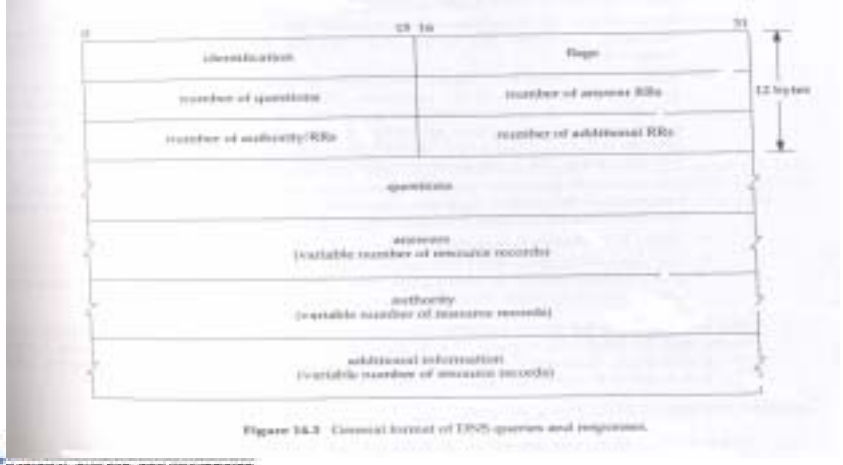
- Every node has a label of up to 63 characters.
- The root of the tree is a special node with a null label.
- Any comparison of labels considers uppercase and lowercase characters the same.
- The domain name of any node in the tree is the list of labels,starting at that node, working up to the root, using a period (“dot”) to separate the labels.
- A domain name that ends with a period is called an *absolute domain name* or a *fully qualified domain name* (FQDN).
- arpa is a special domain used for address-to-name mapping.
- A zone is a subtree of the DNS tree that is administered separately.
- A name server is said to have authority for one zone or multiple zones.

DNS Basics (Cont.)

- There will be one *primary name server* for a zone, and one or more *secondary name servers*.
- Primary name server loads all the information for the zone from disk files.
- Secondary name servers obtain all the information from the primary (*zone transfer*).
- Every name server must know how to contact the *root name server*.
- Root name servers: as of April 1993 there were 8 root servers and all the primary servers must know the IP address of each root server.
- Iterative query process: the requesting name server must contact a root server. The root server tells the requesting server to contact another server, and so on.

DNS Message Format

- A fundamental property of the DNS is *caching*.



flags Field in the DNS Header

- QR: 0 means the message is query, 1 means response
- opcode: the normal value is 0 (a stand query), 1 (an inverse query), 2 (server status request).
- AA: authoritative answer.
- TC: truncated .
- RD: recursion desired.
- RA: recursion available.
- There is a 3-bit field that must be 0
- rcode: the common value are 0 (no error) and 3 (name error).

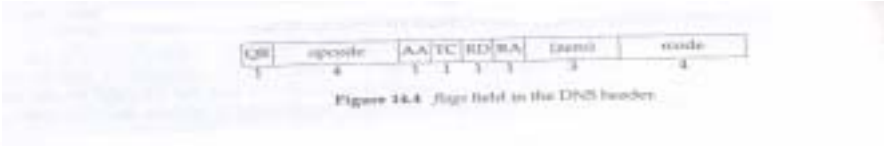


Figure 14.4 flags field in the DNS header

Question Portion of DNS Query Message

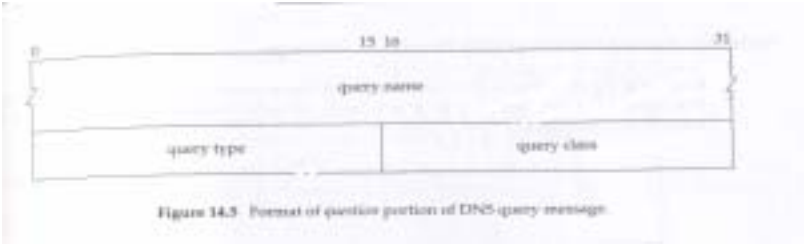


Figure 14.5 Format of question portion of DNS query message

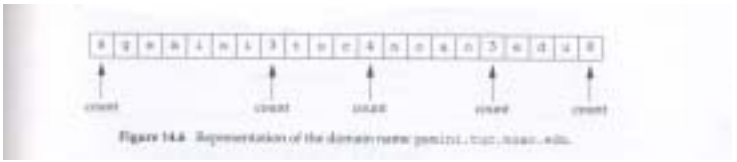


Figure 14.6 Representation of the domain name

Question Portion of DNS Query Message (Cont.)

- **The *query name* is name being looked up.**
- **The most common query type is *A* type: IP address is desired for the *query name*.**
- **A *PTR* query requests the names corresponding to an IP address. (反查)**

Question Portion of DNS Query Message (Cont.)

Name	Numeric value	Description	*type?*	*query type?*
A	1	IP address	•	•
NS	2	name server	•	•
CNAME	5	canonical name	•	•
PTR	12	pointer record	•	•
HINFO	13	host info	•	•
MX	15	mail exchange record	•	•
AXFR	252	request for zone transfer		•
* or ANY	255	request for all records		•

Figure 14.7 *type* and *query type* values for DNS questions and responses.

Resource Record Portion of DNS Response Message

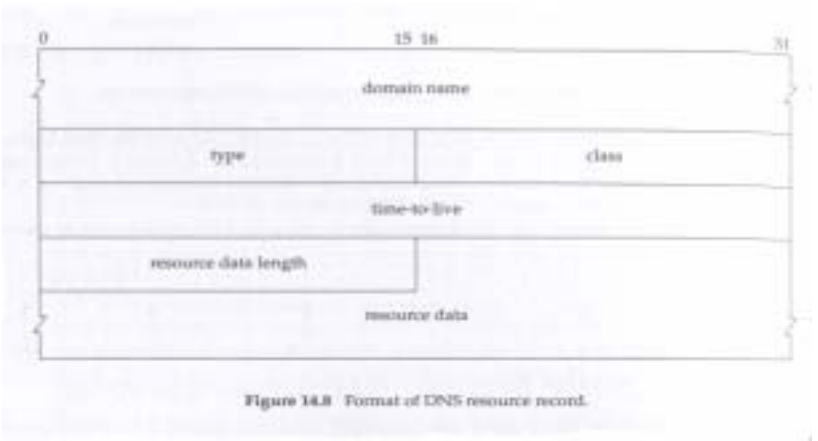


Figure 14.8 Format of DNS resource record.

A Simple Example

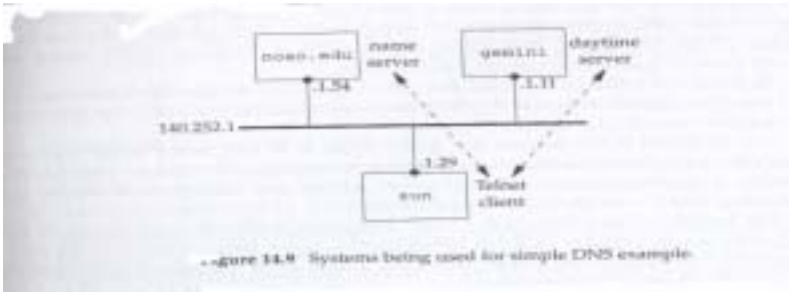


Figure 14.9 Systems being used for simple DNS example.

```
sun % cat /etc/resolv.conf
nameserver 140.252.1.54
domain tuc.noao.edu
```

A Simple Example (Cont.)

- Port 1447 is the ephemeral port used by the client.
- Port 53 is the well-know port for the name server.
- 1 means the identification.
- + means the RD flag is set.
- A means the query type is A (want an IP address)
- ? Means it is a query.
- 37 is length of user data in UDP datagram as 37 bytes.

```
1  0.0                    140.252.1.29.1447 > 140.252.1.54.53: 1+ A?
                          gemini.tuc.noao.edu. (37)

2  0.290820 (0.2908)      140.252.1.54.53 > 140.252.1.29.1447: 1* 2/0/0 A
                          140.252.1.11 (69)
```

Figure 14.10 tcpdump output for name server query of the hostname gemini.tuc.noao.edu

A Simple Example (Cont.)

- 1 is identification field.
- * means the AA flag (authoritative answer) is set.
- 2/0/0 shows the number of resource records in the final variable length fields in the response: 2 answer RRs, 0 authority RRs, and 0 additional RRs.
- 69 the size of the UDP data in the reply .

```
1  0.0                    140.252.1.29.1447 > 140.252.1.54.53: 1+ A?
                          gemini.tuc.noao.edu. (37)

2  0.290820 (0.2908)      140.252.1.54.53 > 140.252.1.29.1447: 1* 2/0/0 A
                          140.252.1.11 (69)
```

Figure 14.10 tcpdump output for name server query of the hostname gemini.tuc.noao.edu

A Simple Example (Cont.)

```
sun % host gemini
gemini.tuc.noao.edu      A       140.252.1.11
gemini.tuc.noao.edu      A       140.252.3.54
```

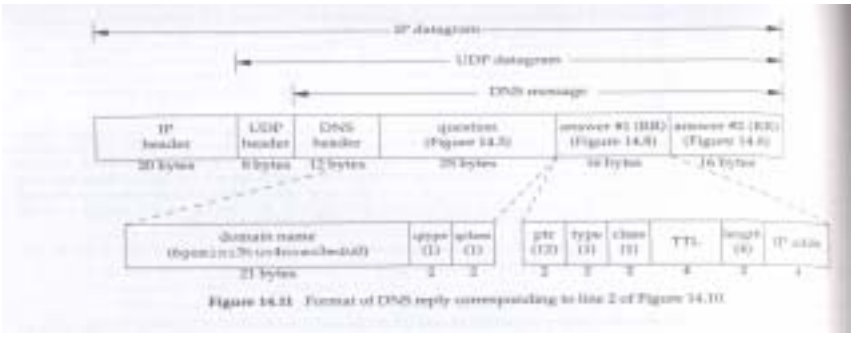


Figure 14.11 Format of DNS reply corresponding to line 2 of Figure 14.10.

Pointer Queries

- Pointer queries: given an IP address, return the name (or names) corresponding to that address.
- arpa top-level domain and in-addr domain.
- The DNS name for host *sun* is 33.13.252.140.in-addr.arpa
- What is passed from the resolver to the name server from a pointer query is the domain name 34.13.252.140.in-addr.arpa.

```
sun % host 140.252.13.34
Name: svr4.tuc.noao.edu
Address: 140.252.13.34

1  0.0                  140.252.1.29.1610 > 140.252.1.54.53: 14 PTR?
                        34.13.252.140.in-addr.arpa. (44)

2  0.332288 (0.3323)    140.252.1.54.53 > 140.252.1.29.1610: 14 1/0/0 PTR
                        svr4.tuc.noao.edu. (75)
```

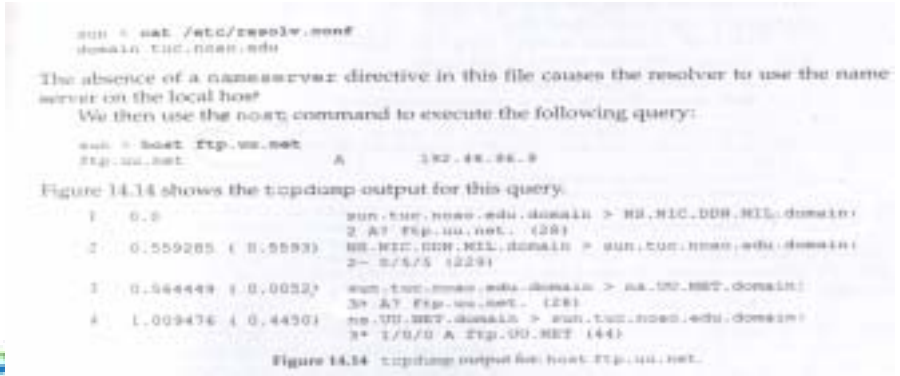
Figure 14.12 tcpdump output for a pointer query.

Resource Records

- A: an A record defines an IP address.
- PTR: this is the pointer record used for pointer queries.
- CHAME: this stands for “canonical name” (often called *alias*).
- HINFO: host information, two arbitrary character strings specifying the CPU and operating system.
- MX: mail exchange records.
- NS: name server record.

Caching

- To reduce the DNS traffic on the Internet, all name servers employ a cache.
- The cache is maintained in the server, not the resolver.
- Delete the name server directive from resolver file.



Caching (Cont.)

```
sun % host -v ftp.uu.net
Query about ftp.uu.net for record types A
Trying ftp.uu.net ...
Query done, 1 answer, status: no error
The following answer is not authoritative:
ftp.uu.net              19109   IN      A       192.48.96.9
Authoritative nameservers:
UU.NET                  170308  IN      NS      NS.UU.NET
UU.NET                  170308  IN      NS      UUNET.UU.NET
UU.NET                  170308  IN      NS      UUCP-GW-1.PA.DEC.COM
UU.NET                  170308  IN      NS      UUCP-GW-2.PA.DEC.COM
UU.NET                  170308  IN      NS      NS.EU.NET
Additional information:
NS.UU.NET               170347  IN      A       137.39.1.3
UUNET.UU.NET            170347  IN      A       192.48.96.2
UUCP-GW-1.PA.DEC.COM    170347  IN      A       16.1.0.18
UUCP-GW-2.PA.DEC.COM    170347  IN      A       16.1.0.19
NS.EU.NET               170347  IN      A       192.16.202.11
```


Another Example

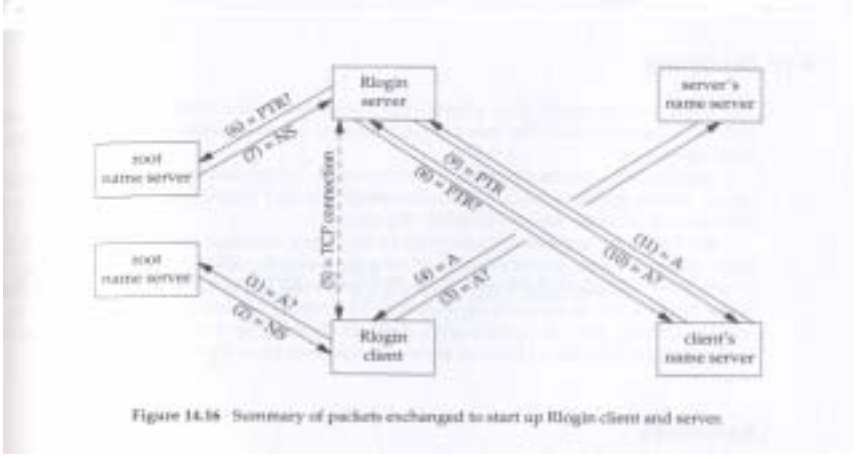


Figure 14.16 Summary of packets exchanged to start up Rlogin client and server.

Summary

- The DNS is an essential part of any host connected to the Internet and widely used in private internets.
- Application contacts resolver to convert a hostname to an IP address, and vice versa .
- All DNS quires and responses have the same message format. This message contains questions and possibly answer resource records RRs, authority RRs and additional RRs.