

## TCP/IP 通訊協定及應用

Spring 2002  
中央大學 吳曉光博士  
<http://wmlab.csie.ncu.edu.tw/course/tcp>

Wireless & Multimedia Network Laboratory™

## Chapter 14: DNS: The Domain Name System

Wireless & Multimedia Network Laboratory™

### Introduction

- ♦ The **Domain Name System** is a distributed database that is used by TCP/IP applications 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*.

Wireless & Multimedia Network Laboratory™

### DNS Basics

- ♦ The DNS name space is hierarchical.

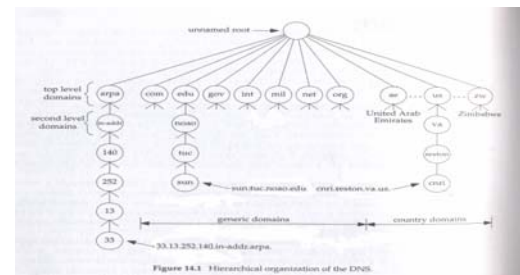


Figure 14.1 Hierarchical organization of the DNS.

Wireless & Multimedia Network Laboratory™

### DNS Basic

- ♦ 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.
- ♦ 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.

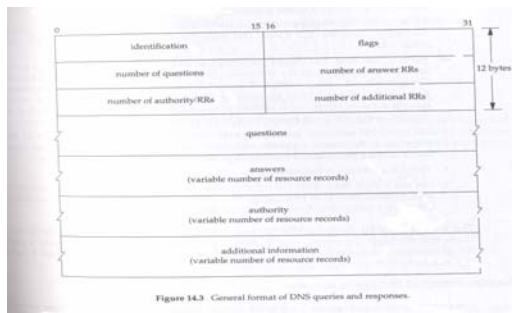
Wireless & Multimedia Network Laboratory™

### DNS Basics

- ♦ Primary name server loads all the information for the zone from disk files.
- ♦ Secondary name servers obtain all the information from the primary.
- ♦ Root name servers : as of April 1993 there were eight root servers and all the primary servers must know the IP address of each root server.

Wireless & Multimedia Network Laboratory™

## DNS Message Format

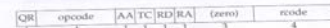


Wireless & Multimedia Network Laboratory™



## DNS Message Format

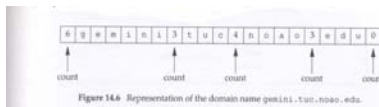
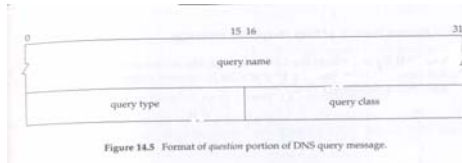
- QR : 0 means the message is query, 1 means response
- opcode : the normal value is 0 ( a stand query ) , 1 ( a n inverse query ), 2 ( server status request ).
- AA means authoritative answer.
- TC means truncated .
- RD means recursion desired.
- RA means recursion available.
- There is a 3-bit field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



Wireless & Multimedia Network Laboratory™



## Question Portion of DNS Query Message



Wireless & Multimedia Network Laboratory™



## Question Portion of DNS Query Message

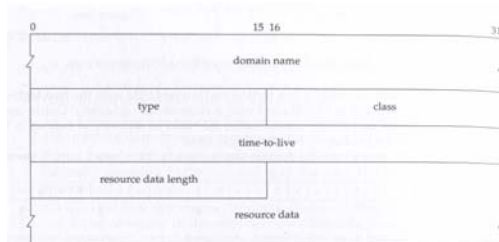
Name	Numeric value	Description	type?	query type?
A	1	IP address	*	*
NS	2	name server	*	*
CNAME	5	canonical name	*	*
PTR	12	pointer record	*	*
HINFO	13	host info	*	*
MX	15	mail exchange record	*	*
AXFR	252	request for zone transfer		*
* or ANY	255	request for all records		*

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

Wireless & Multimedia Network Laboratory™



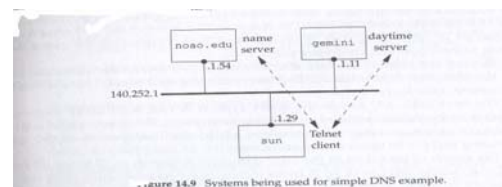
## Resource Record Portion of DNS Response Message



Wireless & Multimedia Network Laboratory™



## A Simple Example



```
sun % cat /etc/resolv.conf
nameserver 140.252.1.154
domain tuc.noao.edu
```

Wireless & Multimedia Network Laboratory™



## A Simple Example

- 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

- 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

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

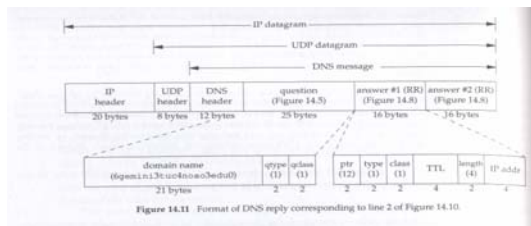


Figure 14.11 Format of DNS reply corresponding to line 2 of Figure 14.10.

## 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.

```
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: 1* PTR?
34.13.252.140.in-addr.arpa. (44)

2 0.332288 (0.3323) 140.252.1.54.53 > 140.252.1.29.1610: 1* 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".
- 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.

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

The absence of a nameserver directive in this file causes the resolver to use the name
server on the local host.
We then use the nslookup command to execute the following query:

sun % host ftp.uu.net
ftp.uu.net A 192.48.96.9
```

Figure 14.14 shows the tcpdump output for this query.

```
1 0.0 sun.tuc.noao.edu.domain > NS.NIC.DON.MIL.domain:
2 0.559285 (0.5593) NS.NIC.DON.MIL.domain > sun.tuc.noao.edu.domain:
2- 0/5/5 (229)
3 0.564449 (0.0052) sun.tuc.noao.edu.domain > NS.UU.NET.domain:
3- A7 ftp.uu.net. (28)
4 1.009476 (0.4450) ns.UU.NET.domain > sun.tuc.noao.edu.domain:
3- 1/0/0 A ftp.uu.net (44)
```

Figure 14.14 tcpdump output for host ftp.uu.net.

## Caching

CS'E

```

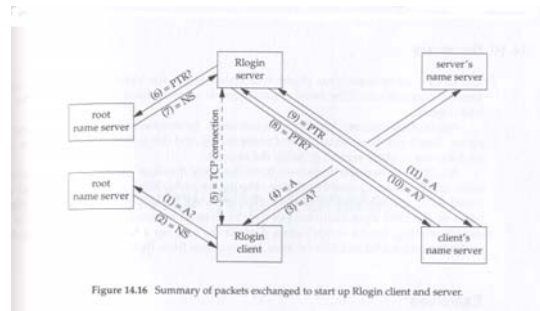
sun % host -v ftp.uu.net
Query about ftp.uu.net for record types A
Trying ftp.uu.net ...
Query done, 1 answer, status: no error
The following answer is not authoritative:
ftp.uu.net. 19109 IN A 192.48.96.9
Authoritative nameservers:
UU.NET 170308 IN NS NS.UU.NET
UU.NET 170308 IN NS UUNET.UU.NET
UU.NET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

Wireless & Multimedia Network Laboratory™



## Another Example

CS'E



Wireless & Multimedia Network Laboratory™



## Summary

CS'E

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

Wireless & Multimedia Network Laboratory™

