ECE 2305: Chap 24.2 - Domain Name System Basics

D.R. Brown III

Worcester Polytechnic Institute
(Some figures from Stallings Data and Computer Communications textbook)

D-term

What is the Domain Name System (DNS)?

- TCP/IP uses IP addresses, e.g., 130.215.36.26, to route packets between hosts.
- Users prefer friendly and memorable names, e.g., www.wpi.edu.
- DNS provides a standard naming convention and a distributed database of mappings between hostnames and IP addresses for locating IP-based computers.
- Critically, the database is distributed (servers all over the world) and redundant.
- Every computer is assigned a DNS server (typically via DHCP, although you can manually set up your DNS server as well).

Four Components of DNS

- **Domain name space**: DNS uses a tree-structured name space to identify resources on the Internet.
- **DNS database**: Each node and leaf in the name space tree structure has a set of information (e.g., IP address, type of resource) that is contained in a resource record (RR). The collection of all RRs is organized into a distributed database.
- **Name servers**: These are computers (or clusters of computers) that hold information about a portion of the domain name tree structure and the associated RRs.
- **Resolvers**: These are programs that extract information from name servers in response to client requests. A typical client request is for an IP address corresponding to a given domain name.

Domain Name Space

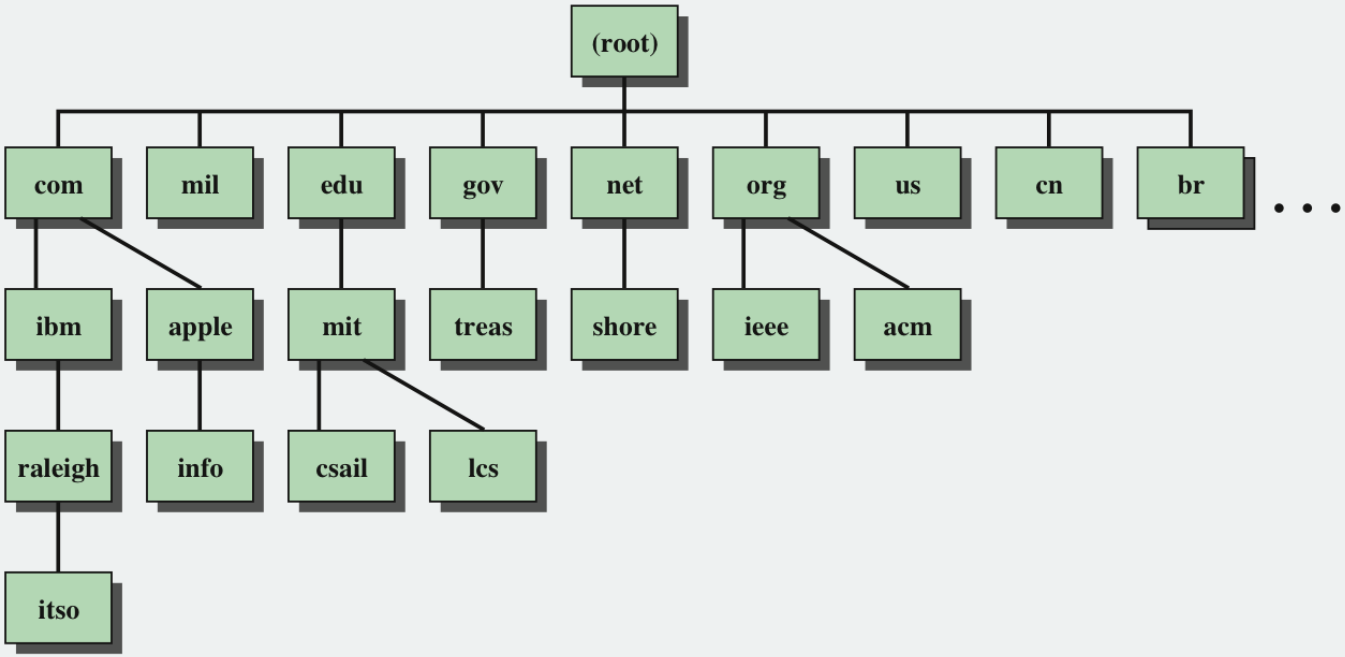

Figure 24.4 Portion of Internet Domain Tree

Creation and assignment of top-level and second-level names handled by ICANN (a non-profit corporation).

DNS Database: Resource Records

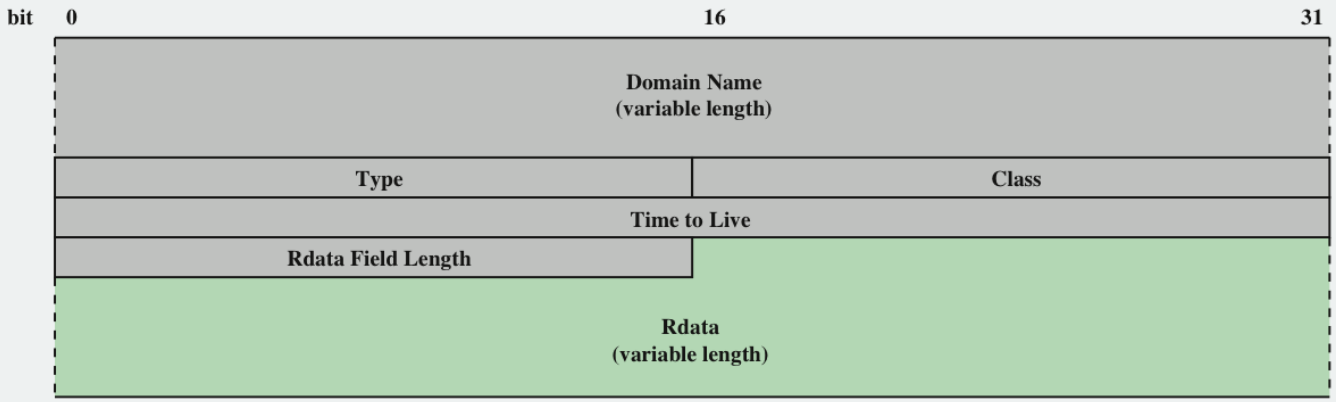

Figure 24.5 DNS Resource Record Format

- Domain Name: human readable name, labels separated by periods
- Type: Type of resource described by this resource record (table on next slide)
- Class: Protocol family (almost always IN=Internet)
- Time-to-live: The time interval that the RR may be cached.

Resource Record Types

Type	Description
A	A host address. This RR type maps the name of a system to its IPv4 address. Some systems (e.g., routers) have multiple addresses, and there is a separate RR for each.
AAAA	Similar to A type, but for IPv6 addresses.
CNAME	Canonical name. Specifies an alias name for a host and maps this to the canonical (true) name.
HINFO	Host information. Designates the processor and operating system used by the host.
MINFO	Mailbox or mail list information. Maps a mailbox or mail list name to a host name.
MX	Mail exchange. Identifies the system(s) via which mail to the queried domain name should be relayed.
NS	Authoritative name server for this domain.
PTR	Domain name pointer. Points to another part of the domain name space.
SOA	Start of a zone of authority (which part of naming hierarchy is implemented). Includes parameters related to this zone.
SRV	For a given service provides name of server or servers in domain that provide that service.
TXT	Arbitrary text. Provides a way to add text comments to the database.
WKS	Well-known services. May list the application services available at this host.

Name Servers

Root name servers:

Server	Operator	Cities	IP Addr
A	VeriSign Global Registry Services	6 sites in the United States, Germany, Hong Kong	IPv4: 198.41.0.4 IPv6: 2001:503:BA3E::2:30
B	Information Sciences Institute	Marina Del Rey, CA, U.S.	IPv4: 192.228.79.201 IPv6: 2001:478:65::53
C	Cogent Communications	6 sites in the United States, Germany, Spain	192.33.4.12
D	University of Maryland	College Park, MD, U.S.	128.8.10.90
E	NASA Ames Research Center	Mountain View, CA, U.S.	192.203.230.10
F	Internet Software Consortium	49 sites in the United States and other countries	IPv4: 192.5.5.241 IPv6: 2001:500::1035
G	U.S. DOD Network Information Center	6 sites in United States, Japan, Germany, Italy	192.112.36.4
H	U.S. Army Research Lab	Aberdeen, MD, U.S. San Diego, CA, USA	IPv4: 128.63.2.53 IPv6: 2001:500:1::803f:235
I	Netnod	38 sites in the United States and other countries	IPv4: 192.36.148.17 IPv6: 2001:7fe::53
J	VeriSign Global Registry Services	70 sites in the United States and other countries	IPv4: 192.58.128.30 IPv6: 2001:503:C27::2:30
K	Reseaux IP Europeens - Network Coordination Centre	18 sites in the United States and other countries	IPv4: 193.0.14.129 IPv6: 2001:7fd::1
L	Internet Corporation for Assigned Names and Numbers	55 sites in the United States and other countries	IPv4: 199.7.83.42 IPv6: 2001:500:3::42
M	WIDE Project	6 sites in the United States, Japan, Korea, France	IPv4: 202.12.27.33 IPv6: 2001:dc3::35

If your computer does not have the appropriate RR in its cache, it sends a DNS query to the local DNS server, which either returns an address immediately or forwards the query to one or more other servers. Resolvers use UDP for single queries and TCP for group queries.

Big Picture

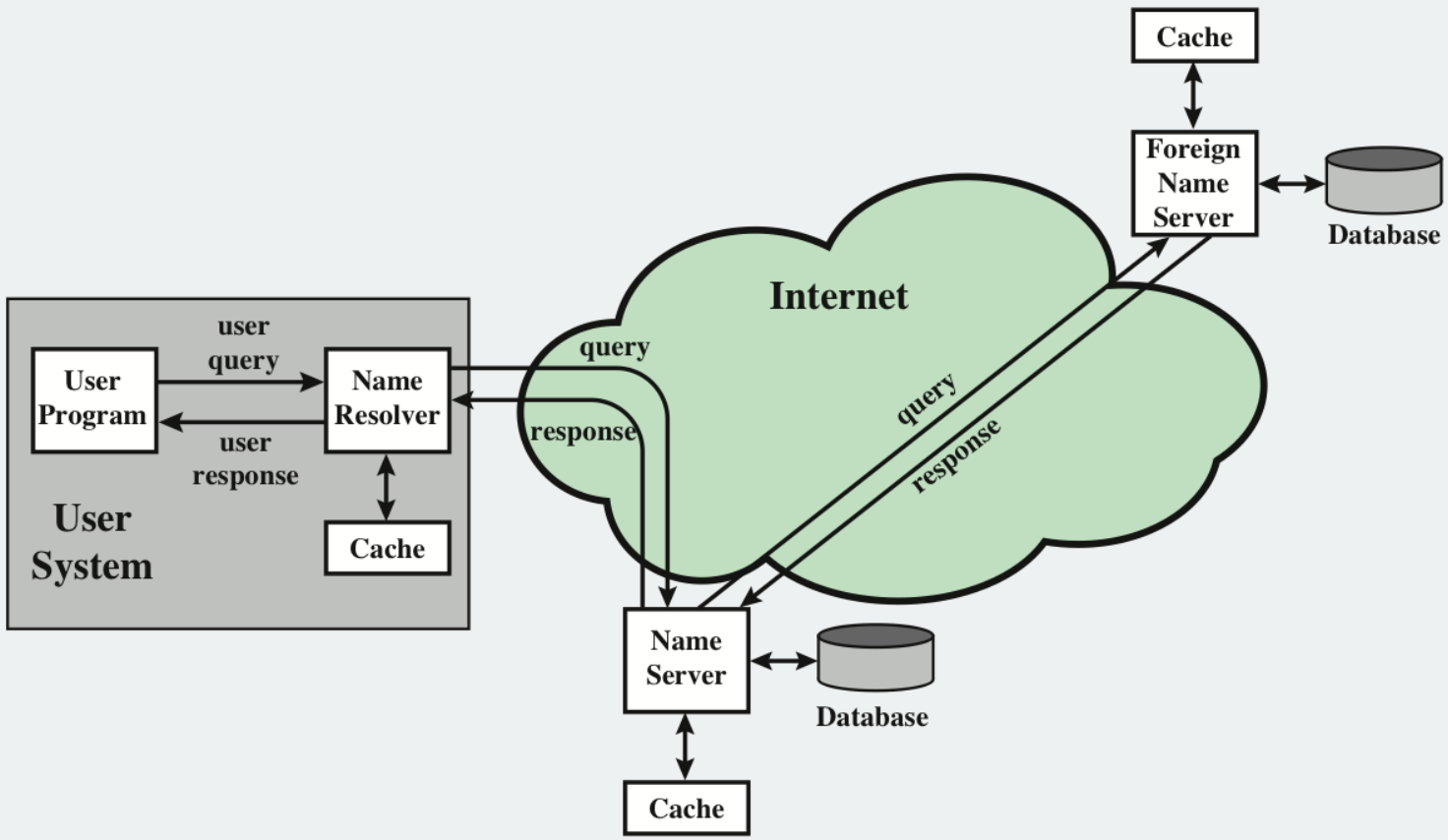

Figure 24.6 DNS Name Resolution

Local DNS Cache Example (Windows)

```
C:\Users\drb>ipconfig /displaydns

Windows IP Configuration

    download.windowsupdate.com
    ----------------------------------------
    Record Name . . . . . : download.windowsupdate.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 19
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    CNAME Record  . . . . : download.windowsupdate.nsatc.net

    update.microsoft.com
    ----------------------------------------
    Record Name . . . . . : update.microsoft.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 30
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    CNAME Record  . . . . : update.microsoft.com.nsatc.net

    www.wpi.edu
    ----------------------------------------
    Record Name . . . . . : www.wpi.edu
    Record Type . . . . . : 5
    Time To Live  . . . . : 586
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    CNAME Record  . . . . : THOLIAN.wpi.edu
```

Typical Steps

1. A user program requests an IP address for a domain name.
2. A resolver module in the local host checks the local DNS cache and uses it if a valid RR is present.
3. If the RR is not cached, one or more DNS servers are queried from the host's DNS server table.
4. The queried server checks to see if the name is in its local database or cache, and, if so, returns the IP address to the requestor. Otherwise, the name server queries other available name servers, going to the root server if necessary.
5. When a response is received at the queried name server, it stores the name/ address mapping in its local cache and may maintain this entry for the amount of time specified in the time to live field of the retrieved RR.
6. The user program that originated the request is given the IP address or an error message.

Wireshark Capture: `nslookup www.aiit.or.kr 8.8.8.8`