CSIS 4222

Ch 4: The Domain Name System (DNS)

Names or Numbers

IP assigns 32-bit addresses to hosts (interfaces)
- Easy for computers
- Hard for humans:

```
http://66.220.145.11
```

- All applications use IP addresses through the TCP/IP protocol software
- The *Domain Name System* (DNS) provides translation between symbolic names and IP addresses

Domain Name Syntax

Alphanumeric *segments* separated by dots

Examples

Top Level Domain

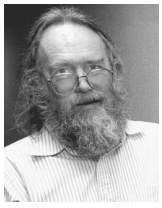
```
www.netbook.cs.purdue.edu
loki.stockton.edu
```

Fully Qualified Domain Name (FQDN)
- Includes complete domain, subdomain, and host name to make it unique

Domain Name System (DNS)

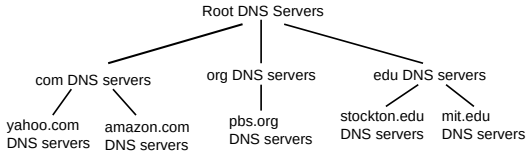
Originally, the Internet was small and mapping between names and addresses was accomplished using a centrally-maintained file called *hosts.txt*

Adding a name or changing an address required contacting the central administrator, updating the table, and distributing it to all the other sites



Jon Postel

Distributed Hierarchical Database



Client wants IP for www.amazon.com:
- Query a root server to find `com` DNS server
- Query `com` DNS server to get `amazon.com` DNS server
- Query `amazon.com` DNS server to get IP address for `www.amazon.com`

DNS Servers

- Each DNS server is the *authoritative server* for the names it manages
- If request contains a name managed by the receiving server, that server replies directly
- Otherwise, request must be forwarded to the appropriate authoritative server
  - DNS request is forwarded to a root name server, which points at next server to use
  - Eventually, the authoritative server is located and IP address is returned

DNS Root name servers are contacted when the local name server cannot resolve the name itself

Root name server:

- contacts authoritative name server if name mapping is not known
- gets mapping
- returns mapping to local name server

13 root name servers worldwide

TLD Servers

Top-level domain (TLD) servers: Responsible for `com`, `org`, `net`, `edu`, etc. and top-level country domains such as `uk`, `fr`, `ca`, `tv`

Countries define their own internal hierarchy:
`ac.uk` and `edu.au` are used for academic organizations in the United Kingdom and Australia

Figure 4.16
Example top-level domains and the group to which each is assigned

Domain Name	Assigned To
aero	Air transport industry
arpa	Infrastructure domain
asia	For or about Asia
biz	Businesses
com	Commercial organizations
coop	Cooperative associations
edu	Educational institutions
gov	United States Government
info	Information
int	International treaty organizations
jobs	Human resource managers
mil	United States military
mobi	Mobile content providers
museum	Museums
name	Individuals
net	Major network support centers
org	Non-commercial organizations
pro	Credentialed professionals
travel	Travel and tourism
country code	A sovereign nation

Local Name Server

- Does not strictly belong to the hierarchy
- Each ISP (residential ISP, company, university) has one
  - Also called “default name server”
- When a host makes a DNS query, it is sent to its local DNS server
  - Acts as a proxy, forwards query into hierarchy

Primary Name Servers

A *primary name server* knows the names and addresses of the hosts in one organization

- It is the authority for its *zone* (info kept in a config file)
- Can delegate authority to a secondary name server (for backup and to reduce load) that gets its info from primary name server
- Caching name servers also reduce load, by keeping copies of info obtained from previous queries (temporary, not stored on disk and expires periodically)

DNS Functionality

- Given
  Name of a computer
- Returns
  Computer’s internet address
- Method
  - Distributed lookup
  - Client contacts server(s) as necessary

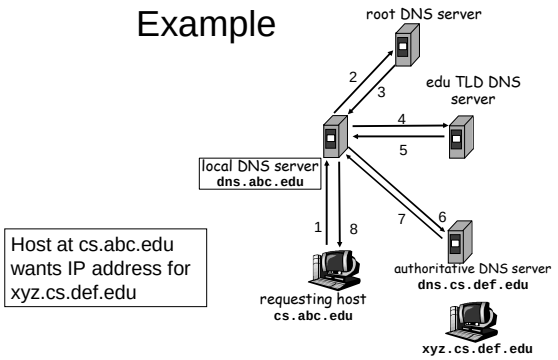
Resolver

- Application programs like web browsers, ftp, etc. that need IP addresses contain calls to resolver routines

Resolver: Software that converts a client's request for address info to a query to a name server

– Resolver needs to know the IP of at least one local domain server

Example



Obtaining a Domain Name

An organization

– Chooses desired name (must be unique)

– Registers with a central authority (ICANN designates domain registrars to administer top-level domains and approve specific names)

– Placed under one *top-level domain*

`stockton.edu`

`yahoo.com`

Names subject to international law for

– Trademarks

– Copyright

Example Name Structure

`candy.foobar.com`

- Most significant level is *.com*
- Second level is company name: *Foobar*
- Third level is division within company: *Candy* and *Soap*
- Fourth level might be
  – Company subdivision or individual computer

Each domain is delegated authority to create new *subdomains*

Example, cont.

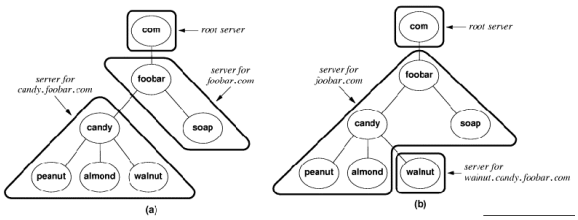
Names in soap division have the form

computer`.soap.foobar.com`

Names in candy division have the form

computer.subdivision`.candy.foobar.com`

Two possible choices for DNS hierarchies within the organization



DNS Client-Server Interaction

- Name servers are the programs that actually manage the name space.
- The name space is divided into *zones of authority*, and a name server is said to be *authoritative* for all domain names within its zone.
- Name servers can *delegate* responsibility for a *subdomain* to another name server, allowing a large name space to be divided into several smaller ones.

Inter-Server Links

All domain name servers are linked together to form a unified system. Each server knows how to reach a root server and how to reach servers that are authorities for names further down the hierarchy.

Name Resolution

- Calling program is *client*
  - Constructs DNS protocol message - a *DNS request*
  - Sends message to local DNS server
  - DNS request contains name to be resolved
- DNS *server* resolves name
  - Constructs DNS protocol message - a *DNS reply*
  - DNS reply contains IP address for the name in the request
  - Sends reply to client program and waits for the next request
- DNS queries/responses carried in UDP datagrams (more about these later).

Caching in DNS Servers

DNS applies the *locality of reference principle* that forms the basis for caching:

- *Spatial*: A user tends to look up the names of local computers more often than the names of remote computers
- *Temporal*: A user tends to look up the same set of domain names repeatedly

- A name resolver contacts a local server first
- DNS server caches all lookups

Caching In DNS

DNS resolution can be **very** inefficient

- Every host referenced by name triggers a DNS request
- Every DNS request for the address of a host in a different organization goes through the root server

Servers and hosts use *caching* to reduce the number of DNS requests

- Cache is a list of recently resolved names and IP addresses
- Authoritative server includes *time-to-live* with each reply

DNS Types

Each entry in server database consists of

- Domain name
- DNS type for name
- Value to which name corresponds

During lookup, client must supply

- Name
- Type

Server

- Matches both name and type

DNS Record Types

Type *A (Address)*
- Value is IP address for a named computer

Type NS *(Name Server)*
- Value is hostname of authoritative name server for this domain

Type *MX (Mail eXchanger)*
- Value is IP address of computer with mail server for name

Type *CNAME (Computer NAME)*
- Value is another domain name
- Used to establish an alias *(www)*

Domain Name Abbreviation

- DNS lookup uses full names
- Users might use abbreviations
- Technique
  - Configure resolver with a list of suffixes
  - Try suffixes one at a time

Example suffixes:
```
foobar.com
candy.foobar.com
```
User enters name `walnut`

Resolver tries
```
walnut
walnut.foobar.com
walnut.candy.foobar.com
```

whois

Get info on Stockton's name servers with

```
whois stockton.edu
```

Or a website such as:

http://www.arin.net/