CS 640 Introduction to Computer Networks

Lecture 3

CS 640

Today's lecture

- Domain Name System
  - Overview
  - The hierarchy of domain names
  - DNS records
  - The resolution process

CS 640

Domain Name System Overview

- What are names used for in general?
  - identify objects
  - locate objects
  - define membership in a group
  - …
- Basic Terminology
  - ***Name space***
    - defines set of possible names
    - consists of a set of name to value *bindings*
  - ***Resolution mechanism***
    - when invoked with a name returns corresponding value

CS 640

DNS Properties

- Size of Internet demands robust naming mechanism
  - Specified in RFC 1034, 1035 (Mockapetris '87)
  - Scalability through caching and hierarchy
  - Reliability through caching and redundancy
- Names versus addresses
  - Human readable versus router readable
  - Location transparent versus location-dependent
- Hierarchical
  - Names are divided into components
- Global versus local
  - What is the scope of naming?

CS 640

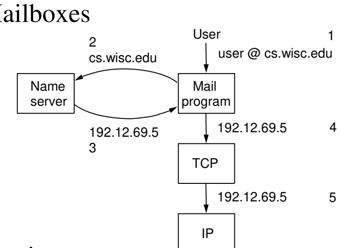
Examples of Mappings

- Hosts
  `pluto.cs.wisc.edu` → `192.12.69.17`
  `192.12.69.17` → `80:23:A8:33:5B:9F`
- Files
  `/usr/llp/tmp/foo` → `(server, fileid)`
- Users
  `Suman Banerjee` → `suman@cs.wisc.edu`

CS 640

Examples (cont)

- Mailboxes

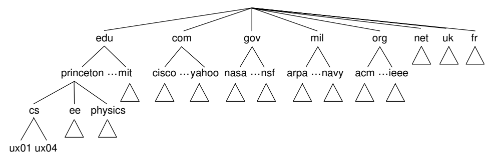


- Services
  `nearby ps printer with short queue and 2MB`

CS 640

Domain Naming System

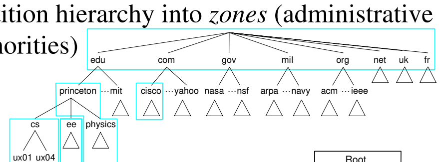
- Hierarchical name space for Internet objects



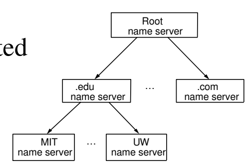
- Names are read from right to left separated by periods
  - Each suffix in a domain name is a domain
    `wail.cs.wisc.edu, cs.wisc.edu, wisc.edu, edu`

Name Servers

- Partition hierarchy into *zones* (administrative authorities)



- Each zone implemented by two or more *authoritative name servers*



Resource Records

- Each name server maintains a collection of *resource records*
  `(Name, Value, Type, Class, TTL)`
  - Each record is a translation based on type
  - Name/Value: not necessarily host names to IP addresses
- Type (some examples)
  - A: Name = full domain name, Value = IP address
  - NS: Value gives domain name for host running name server that knows how to resolve names within specified domain.
  - CNAME: Value gives canonical name for particle host; used to define aliases.
  - MX: Value gives domain name for host running mail server that accepts messages for specified domain.
- Class: allow other entities (other than NIC) to define types
  - IN is what is used by the Internet
- TTL: how long the resource record is valid

gTLD Name Server

May contain the following resource records:

```
(wisc.edu, dns.wisc.edu, NS, IN)
(dns.wisc.edu, 128.105.12.11, A, IN)

(cisco.com, thumper.cisco.com, NS, IN)
(thumper.cisco.com, 128.96.32.20, A, IN)
```

…

Wisconsin Server

May contain the following resource records:

```
(cs.wisc.edu, dns.cs.wisc.edu, NS, IN)
(dns.cs.wisc.edu, 128.105.2.10, A, IN)

(ece.wisc.edu, dns.ece.wisc.edu, NS, IN)
(dns.ece.wisc.edu, 128.105.40.12, A, IN)

(host1.cs.wisc.edu, 128.105.9.103, A, IN)
(host2.cs.wisc.edu, 128.105.9.13, A, IN)
```

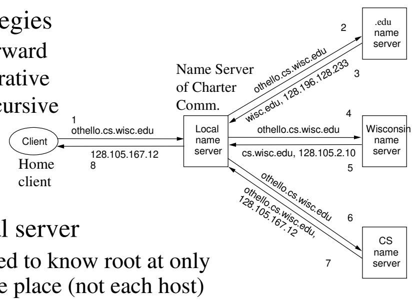

CS Server

CS server may contain following resource records:

```
(cs.wisc.edu, norm.cs.wisc.edu, MX, IN)
(norm.cs.wisc.edu, 128.105.8.45, A, IN)
(n.cs.wisc.edu, norm.cs.wisc.edu, CNAME, IN)
(othello.cs.wisc.edu, 128.105.167.12, A, IN)
(o.cs.wisc.edu, othello.cs.wisc.edu, CNAME, IN)
```

Name Resolution

- Strategies
  - forward
  - iterative
  - recursive



- Local server
  - need to know root at only one place (not each host)
  - site-wide cache

DNS Issues

- Top level domain names are tightly controlled
- Before an institution is granted authority for a second-level domain, it must agree to operate a DNS server that meets Internet standards.
  - Eg. all DNS info must be replicated on separate systems
- DNS is *very* important in the Internet
  - Security of this system is strict
- DNS lookups can affect performance
- In practice DNS more complicated than you might think

PTR Record

- Used for IP to name resolution
- For IP address: a.b.c.d
  - PTR record stored at: d.c.b.a.in-addr.arpa.
- All PTR records are stored under in-addr.arpa. domain
- Consider the zone: 105.128.in-addr.arpa
  - This will typically be under control of CS dept of Wisconsin (since 128.105/16 belongs to the CS dept)
- PTR zone and the usual namespace zone may be inconsistent

Resilience of DNS to attacks

- January 2001 flooding attack against Microsoft's name servers
  - Service went down because they were all on the same subnet
- October 2002 flooding attack on the 13 root name servers
  - 4 servers survived

Other Naming Protocols

- X.500
  - Naming system designed to identify people
  - Each person is defined by attributes
    - Name
    - Title
    - …
  - Too cumbersome
- Lightweight Directory Access Protocol (LDAP)
  - Evolved from X.500
  - System for learning about users