Lecture 17 (March 25, 2004)

Outline
Domain Name System

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

DNS Properties
- Size of Internet demands well devised naming mechanism
  - Specified in RFC 1034, 1035 (Mockapetris ‘87)
- 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?
- DNS for other purposes
  - Determines where user requests are routed

Examples of Mappings
- Hosts
  - pluto.cs.wisc.edu —> 192.12.69.17
- Files
  - /user/llp/tmp/foo —> (server, fileid)
- Users
  - Suman Banerjee —> suman@cs.wisc.edu

Examples (cont)
- Mailboxes
  - cs.wisc.edu
  - User
    - user@cs.wisc.edu
  - Mail program
    - 192.12.69.5
      - 3
    - TCP
      - 192.12.69.5
      - 4
      - IP
        - 192.12.69.5
        - 5

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

Domain Naming System
- Hierarchical name space for Internet objects
  - Each suffix in a domain name is a domain
  - mailbox.cs.wisc.edu, cs.wisc.edu, wisc.edu, edu

- Names are read from right to left separated by periods
**Name Servers**

- Partition hierarchy into zones (administrative authorities)

- Each zone implemented by two or more 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 the 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 types (other than NIC) to define types
  - IN: is what is used by the Internet

- TTL: how long the resource record is valid

**Root 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)`
- `(ecwisc.edu, dns.ecwisc.edu, NS, IN)`
- `(dns.ecwisc.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 the 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 is much 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

DNS Redirection and CDNs

• Up to now, we have assumed that there is a single mapping between a name and an IP
• Content delivery companies (Akamai) use DNS to direct client requests to mirror servers
  – Content Delivery Networks (CDN’s) attempt to push content closer to the edge of the network
    • Distributed network of mirror servers (caches/proxies)
    – How do clients find the closest mirror?
    – CDN’s take over company’s name server

DNS Redirection contd.

• Local DNS request gets routed to company’s name server
• CDN assumes client is “near” their local DNS
• CDN responds with IP of server which is closest to client’s local DNS
  – Enables much
  – Makes many assumptions

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