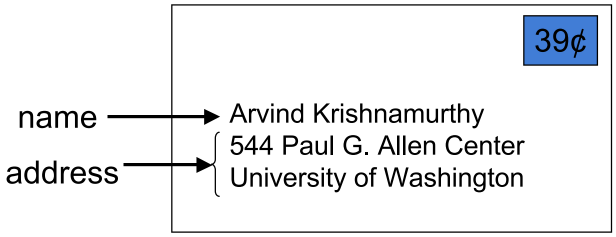
# Naming and the DNS

## Names and Addresses



- Names are identifiers for objects/services (high level)
- Addresses are locators for objects/services (low level)
- Binding is the process of associating a name with an address
- Resolution is the process of looking up an address given a name

# Internet Hostnames

- Hostnames are human-readable identifiers for end-systems based on an administrative hierarchy
  - uranium.cs.washington.edu is my desktop machine
- IP addresses are a fixed-length binary encoding for end-systems based on their position in the network
  - 128.208.2.50 is uranium’s IP address

- Original name resolution: HOSTS.TXT
- Current name resolution: Domain Name System
- Future name resolution: ?

# Original Hostname System

- When the Internet was really young …

- Flat namespace
  - Simple (host, address) pairs

- Centralized management
  - Updates via a single master file called HOSTS.TXT
  - Manually coordinated by the Network Information Center (NIC)

- Resolution process
  - Look up hostname in the HOSTS.TXT file

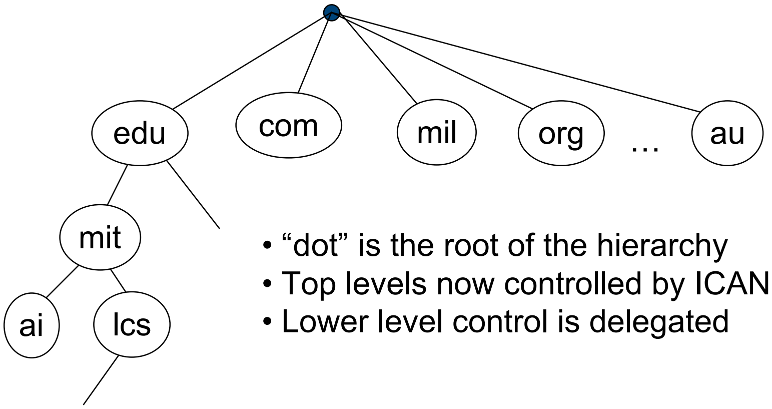
# Scaling Problems

- Coordination
  - Between all users to avoid conflicts
- Inconsistencies
  - Between update and distribution of new version
- Reliability
  - Single point of failure
- Performance
  - Competition for centralized resources

# Domain Name System (DNS)

- Designed by Mockapetris and Dunlap in the mid 80s
- Namespace is hierarchical
  - Allows much better scaling of data structures
  - e.g., uranium.cs.washington.edu
- Namespace is distributed
  - Decentralized administration and access
  - e.g., *.cs.washington.edu managed by CSE
- Resolution is by query/response
  - With replicated servers for redundancy
  - With heavy use of caching for performance

# DNS Hierarchy



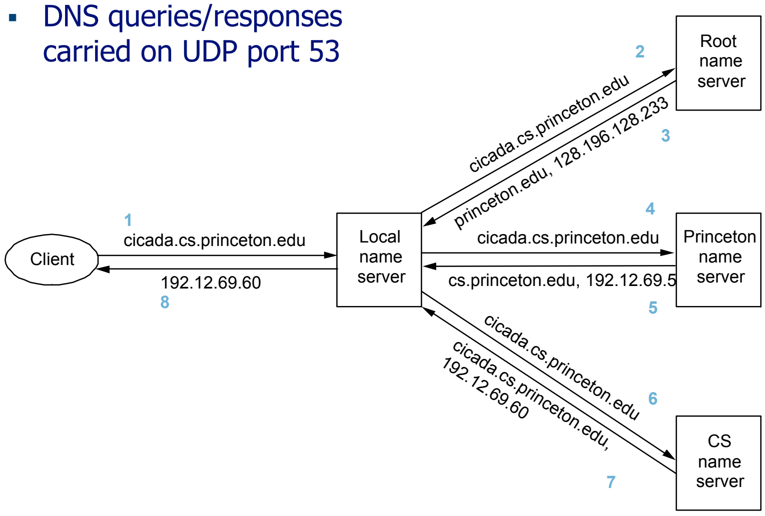
- “dot” is the root of the hierarchy
- Top levels now controlled by ICANN
- Lower level control is delegated

# DNS Distribution

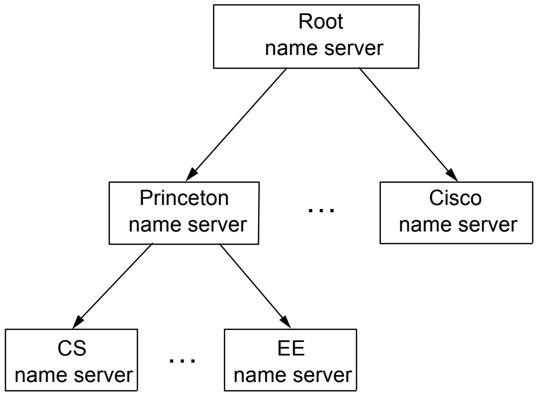
- Data managed by zones that contain resource records
  - Zone is a complete description of a portion of the namespace
  - e.g., all hosts and addresses for machines in washington.edu with pointers to subdomains like cs.washington.edu
- One or more nameservers manage each zone
  - Zone transfers performed between nameservers for consistency
  - Multiple nameservers provide redundancy
- Client resolvers query nameservers for specified records
  - Multiple messages may be exchanged per DNS lookup to navigate the name hierarchy

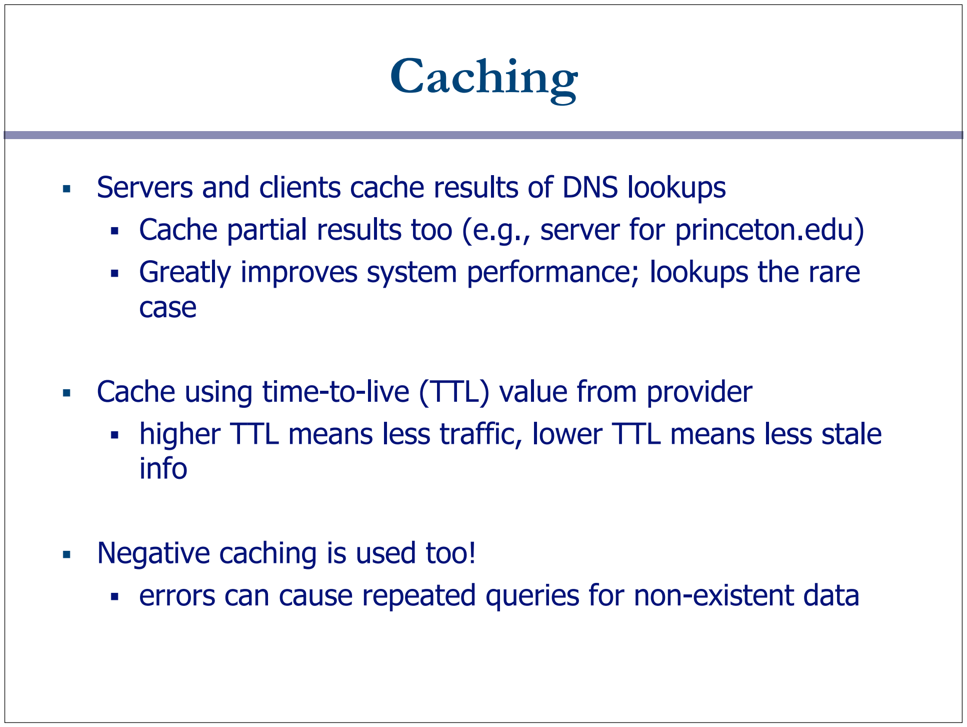
# DNS Lookups/Resolution

- DNS queries/responses carried on UDP port 53



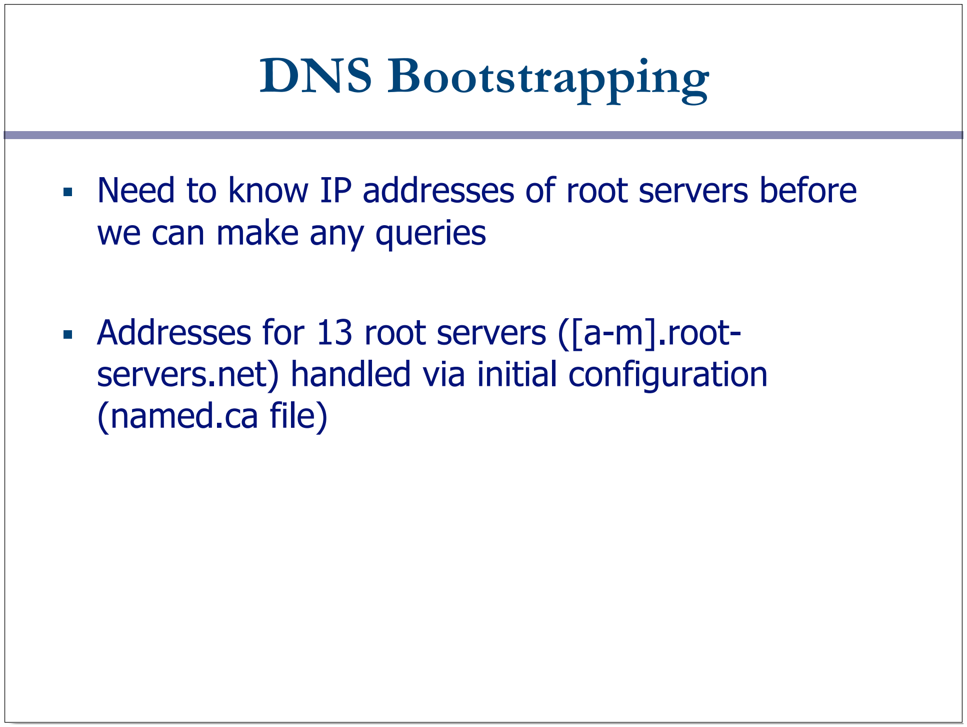
# Hierarchy of Nameservers





# Caching

- Servers and clients cache results of DNS lookups
  - Cache partial results too (e.g., server for princeton.edu)
  - Greatly improves system performance; lookups the rare case
- Cache using time-to-live (TTL) value from provider
  - higher TTL means less traffic, lower TTL means less stale info
- Negative caching is used too!
  - errors can cause repeated queries for non-existent data



# DNS Bootstrapping

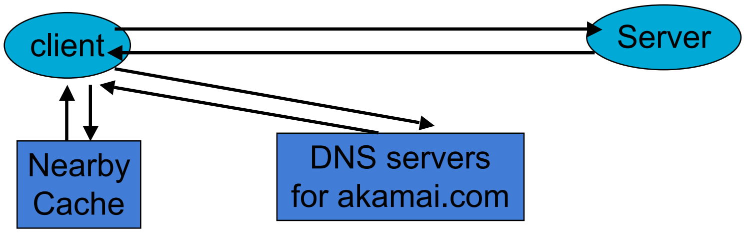
- Need to know IP addresses of root servers before we can make any queries
- Addresses for 13 root servers ([a-m].root-servers.net) handled via initial configuration (named.ca file)

# Future Evolution of the DNS

- Design constrains us in two major ways that are increasingly less appropriate
- Static host to IP mapping
  - What about mobility (Mobile IP)
- Location-insensitive queries
  - What if I don't care what server a Web page comes from, as long as it's the right page?
  - e.g., a yahoo page might be replicated

# Akamai

- Use the DNS to effect selection of a nearby Web cache



- Leverage separation of static/dynamic content

# DNS DoS Attacks

October 22, 2002

- The attack lasted for approximately one hour. Of the thirteen servers, nine were disabled
- The largest malfunction of the DNS servers before this event were seven machines in July 1997, due to a technical glitch

# DNS DoS Attacks

February 6, 2007

- The attack lasted about five hours. none of the servers crashed, two of the root servers "suffered badly", while others saw "heavy traffic".
- The botnet responsible for the attack has reportedly been traced to South Korea.

"If the United States found itself under a major cyberattack aimed at undermining the nation’s critical information infrastructure, the Department of Defense is prepared, based on the authority of the president, to launch a cyber counterattack or an actual bombing of an attack source."

# Announcements

- Exam in this room on Wed 8:30 AM
- Material: everything from beginning of the semester

- Similar to midterm
  - Open-book, open-notes

- Final project due next friday