Module 2: Application Layer (Lecture – 4)

Dr. Nirnay Ghosh
Assistant Professor
Department of Computer Science & Technology
IIEST, Shibpur

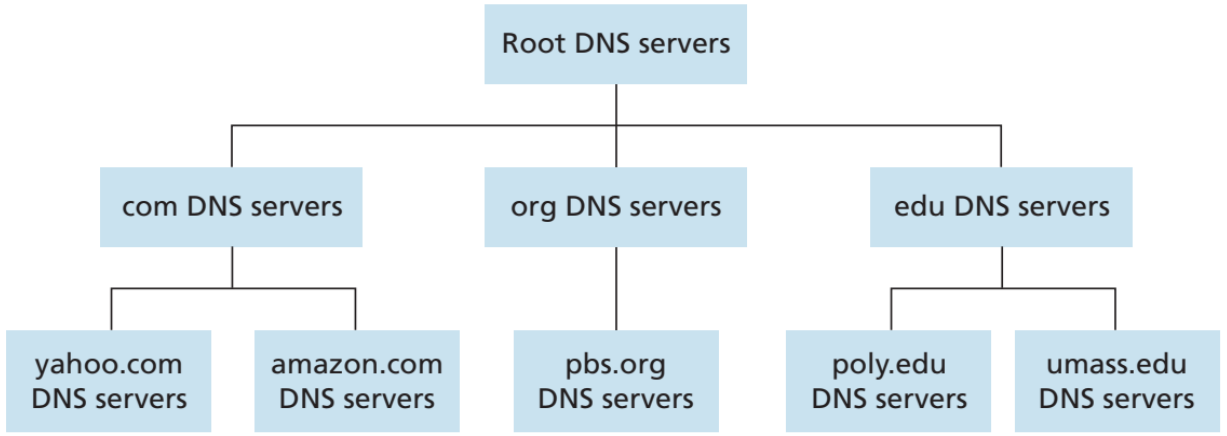
Domain Name System (DNS)

- DNS services other than hostname-to-IP address translation
  - Host aliasing
    - A host with complicated hostname (canonical hostname) can have one or more alias names
    - Alias name: typically more mnemonic than canonical hostnames
      - Example: relay1.west-coast.enterprise.com (canonical name) can have enterprise.com or www.enterprise.com as alias names
    - DNS can be invoked by an application to obtain canonical hostname for a supplied alias hostname as well as the IP address of the host
  - Load distribution
    - Performs load distribution among replicated servers (e.g., replicated Web servers) running on different end system and each having different IP address
    - DNS database contains the list of replicated servers
    - In response to typical name-to-address translation query, DNS server responds with the entire set of IP addresses – changes the ordering of the addresses with each reply
    - Client typically sends HTTP request message to the IP address listed first in the set – distributes traffic among replicated servers

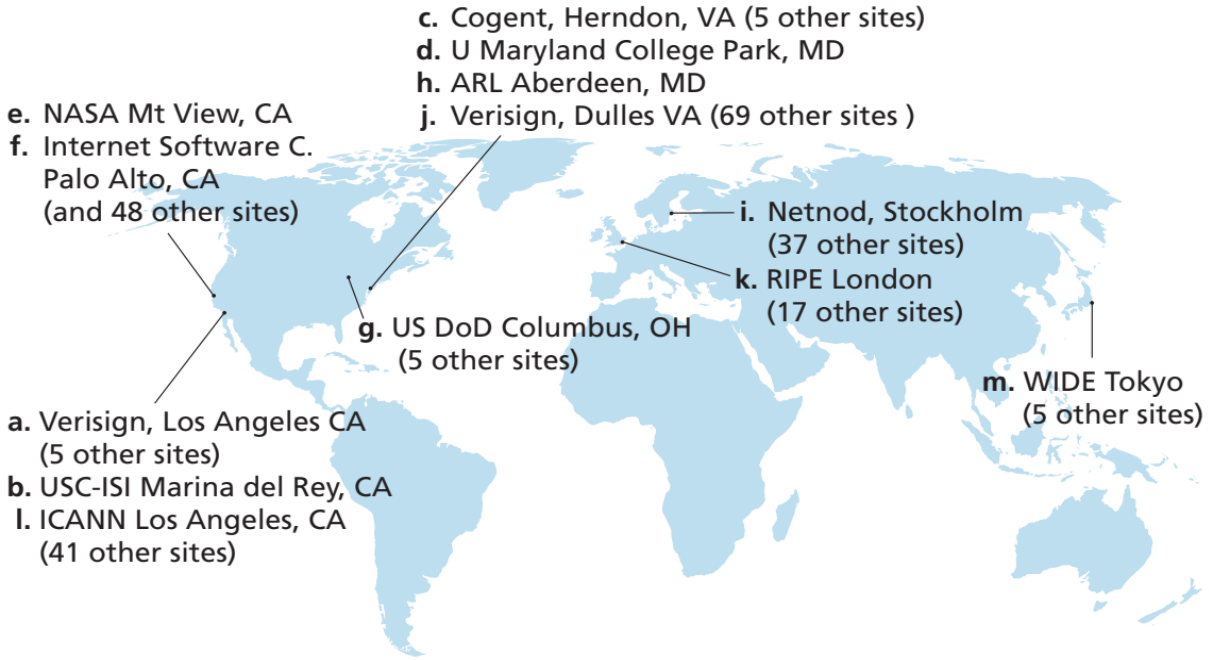
- DNS: both service and protocol
  - Service: a simple straight-forward name-to-address translation service
    - Complex in nature, consists of a large number of DNS servers distributed across the globe/Internet
  - Protocol: an application-layer protocol that specifies how the DNS servers and querying hosts communicate
- Why is DNS distributed by design?
  - Centralized DNS server: does not scale
    - A single point of failure: if the DNS server crashes, so does the entire Internet
    - Traffic volume: has to handle all DNS queries across the Internet
    - Distant centralized database: cannot be “close” to all querying clients - significant delays for clients who far away
    - Maintenance: have to maintain a huge database for all Internet hosts – need to update frequently to account for every new join and leave

DNS: A distributed, hierarchical data

- DNS: uses a large number of databases; organized in a hierarchical fashion; distributed around the world
- No single DNS server has all of the mappings for all hosts in the Internet
- Three classes of DNS servers are organized hierarchically (see fig.):
  - Root DNS servers
  - Top-level domain (TLD) DNS servers
  - Authoritative DNS servers
- Root DNS Servers
  - 13 root DNS servers exist in the Internet (as of 2012)
  - Each server is actually a network of replicated servers for both security and reliability



Portion of the Hierarchy of DNS Servers



DNS Root Servers in 2012 (Name, Organization, Location)

DNS: A distributed, hierarchical database

- Top-level Domain (TLD) DNS Servers
  - Responsible for top level domains – com, org, net, edu, gov, and all country top-level domains (uk, fr, ca, jp, in, etc.)
  - Verisign Global Registry: maintains the TLD servers for the "com" top-level domain
  - Educause: maintains the TLD servers for the "edu" top-level domain
- Authoritative DNS Servers
  - Contain organization-specific DNS records
  - Map the names of publicly accessible hosts (such as Web servers and mail servers) on the Internet to IP addresses
  - Most universities and large companies implement and maintain their own primary and secondary (backup) authoritative DNS servers
  - Alternatively, the organizations can pay to have these records stored in the authoritative DNS server of some service provider

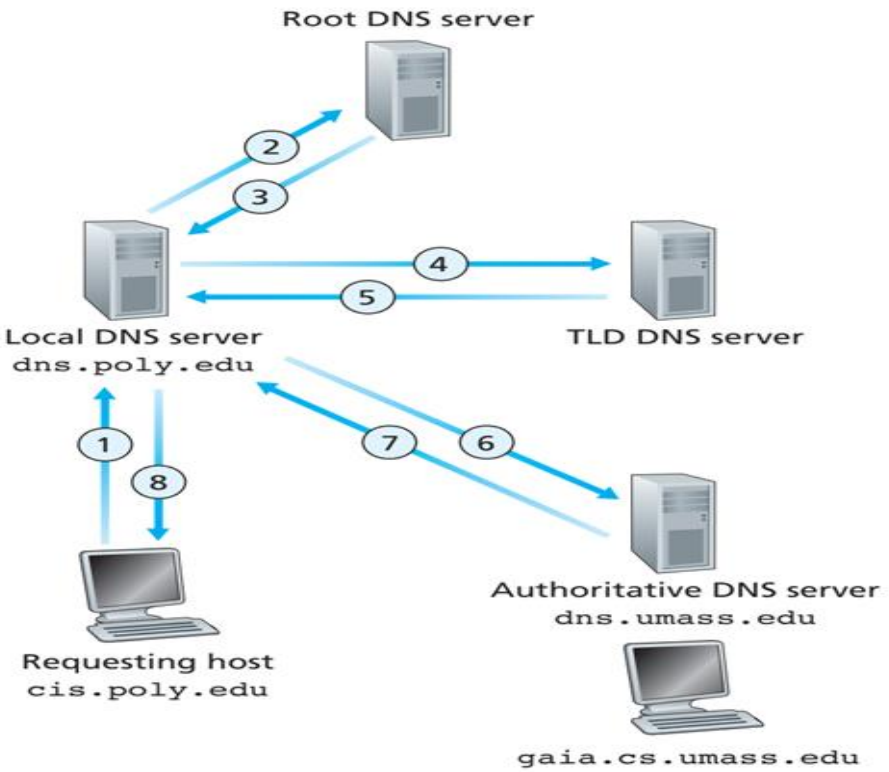


Fig.1: Interaction of various DNS Servers (Iterative)

- Local DNS Server
  - Does not strictly belong to the hierarchy of servers, but is nevertheless central to the DNS architecture
  - Each ISP (e.g., a university, company, etc.) has a local DNS server (also called default name server)
  - When a host connects an ISP, the ISP provides the IP address of one or more of its local DNS servers (typically through DHCP)
  - Local DNS server: close to the host
  - Acts as a proxy to a host's DNS query and forwards it into the DNS server hierarchy

DNS: A distributed, hierarchical database

- Local DNS Server
  - Makes use of both recursive and iterative queries
  - In Fig. 1, query sent from the requesting host (cis.poly.edu) to the local DNS server (dns.poly.edu) is recursive - query asks the local DNS server to obtain mapping on behalf of the host
    - The rest of the queries are iterative as all the replies are directly returned to the local DNS server
  - Fig. 2 shows a DNS query chain for which all of the queries are recursive
  - In practice, the queries typically follow the pattern in Fig. 1
    - Query from the requesting host to the local DNS server is recursive, and the remaining queries are iterative
- DNS Caching
  - Exploits caching in order to improve the delay performance and to reduce the number of DNS messages in the Internet
  - Local DNS server can cache a received mapping (from hostname to IP address) in its memory
  - If a query arrives for the name hostname, the DNS server can provide the desired IP address from its local cache (even if the DNS server is not authoritative for the hostname)
  - Discards cache information after period of time as mapping between hostname and IP address is not permanent
  - Local DNS server can also cache IP addresses of TLD servers – by passes visit to the root DNS servers in the query chain

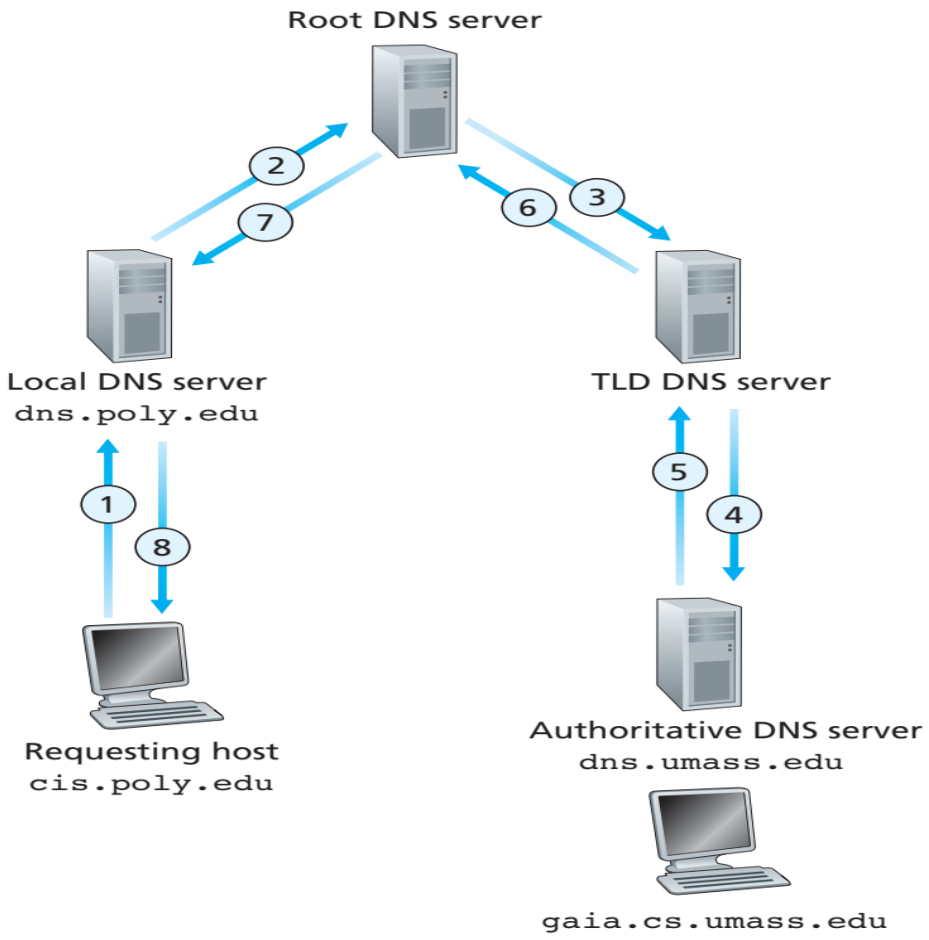


Fig.2: Recursive Queries in DNS

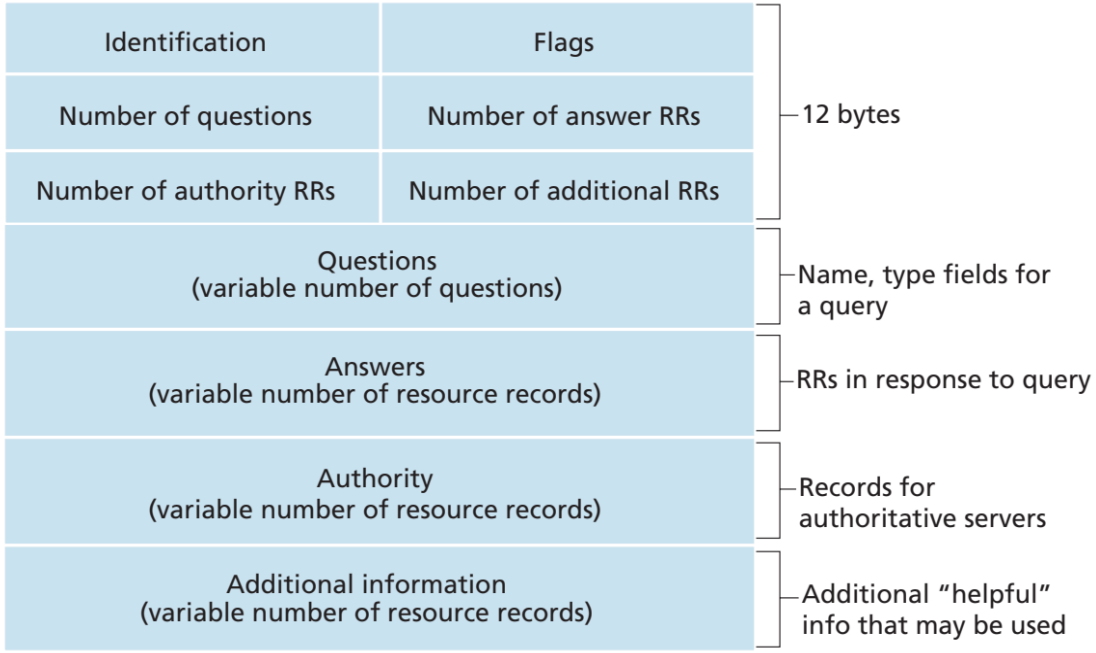
DNS Resource Records

- DNS distributed databases store resource records (RR) including RRs that provide hostname-to-IP address mappings
- Each DNS reply message carries one or more resource records
- Resource record: a four-tuple containing the following fields: *(Name, Value, Type, TTL)*
- TTL: time-to-live of the resource record – determines when a resource record should be removed from the cache
- Different types of resource records that are replied back through DNS messages are tabularized below:

Type	Name	Value	Response Message (Example)
A	Hostname	IP address	*relay1.bar.foo.com, 145.37.93.126, A*
NS	Domain (foo.com)	Hostname of an authoritative DNS server that knows how to obtain the IP addresses for the hosts in the domain	*foo.com, dns.foo.com, NS*
CNAME	Alias hostname	Canonical hostname	*foo.com, relay1.bar.foo.com, CNAME*
MX	Alias hostname of a mail server	Canonical hostname of the mail server	*foo.com, mail.bar.foo.com, MX*

DNS Messages

- Header section (12-bytes)
  - Identification (16-bit): identifies the query – copied into the reply message to a query for client's convenience
  - Flags: consists of a number of flags; some of them are:
    - A 1-bit query/reply flag: query (0) or reply (1)
    - A 1-bit authoritative flag: set in a reply message if a DNS server is an authoritative server for a queried name
    - A 1-bit recursive-desired flag: set when a client (host or DNS server) desires that the DNS server performs recursion if it doesn't have the record
    - A 1-bit recursion-available field: set in a reply if the DNS server supports recursion
  - Four "number-of" fields: number of occurrences of the four types of data sections that follow the header
- Question section: contains information about the query that is being made
  - Name field (contains the name being queried)
  - Type field (type of question being asked about the name)



DNS Message Format

- Answer section: contains the resource records for the name that was originally queried
  - Resource record – Type, Value, TTL
  - A reply can have multiple RRs in the answer since a hostname can have multiple IP addresses (e.g., replicated Web server)
- Authority section: contains information of other authoritative servers
- Additional section: contains other helpful records
  - Reply to MX query – providing the canonical hostname of a mail server
  - Type A record – IP address of the canonical hostname of the mail server

Inserting Records into the DNS Database

- For any new startup company, the first step is to register its domain name
- Registrar: commercial entity that verifies the uniqueness of the domain name
  - Accredited by the Internet Corporation for Assigned Names and Numbers (ICANN)
  - Responsible for entering the domain name into the DNS database at the cost of fees
- Organization needs to provide the registrar with the names and IP addresses of its primary and secondary authoritative DNS servers
- Registrar makes sure that a Type NS (name) record and a Type A (IP address) record are entered into the corresponding TLD servers (e.g., "com")
- Example: for a startup domain *somecompany.com*, following RRs are entered -
  - *(somecompany.com, dns1. somecompany.com, NS)*
  - *(dns1. somecompany.com, 212.212.212.1, A)*
  - *(dns2.somecompany.com, 212.212.212.2, A)*
- Type A RR for the Web server (*www.somecompany.com*) and the Type MX RR for the mail server (*mail.somecompany.com*) are entered into the authoritative DNS servers
  - Configured statically by the system manager