CS 348
Computer Networks
Lec 13

Spring 2020 IIT Goa

Course Instructor: Dr. Neha Karanjkar

Disclaimer: These slides are based on the content in “Computer Networking: A Top-down Approach by Kurose & Ross, 7th ed” and some specific topics are referenced from Wikipedia.

Questions

- What is the “Interface” between applications and the Internet? How can applications use services of the layers below? **The Sockets API**
- Some popular applications, how they work, protocols they use:
  - **The Web** and HTTP, Email, Peer-to-peer applications

How can “names” be translated to IP addresses? DNS

The Need for Different kinds of Names

- IP Addresses
  - Purpose: routing
- Domain names
  - Purpose: mnemonics, for humans to remember
  - Example: mail.google.com, www.bbc.co.uk, www.iitgoa.ac.in

Need a mechanism for translating domain names to IP addresses

The Domain Name System (DNS)

- **What is DNS?**

  A global, distributed **directory-service** for translating Domain names to IP addresses

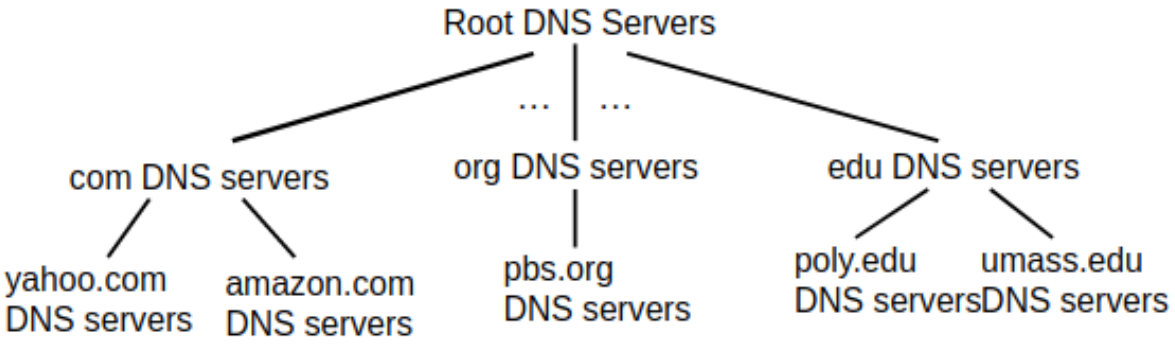
- **What is its purpose?**
  - Translation of domain/host names to IP addresses
  - Some other functions it serves:
    - translate simple hostnames to canonical hostnames

      Example:
    - load distribution (one hostname, many IP addresses)

The Domain Name System (DNS)

- **What does the DNS system consist of?**
  - A **distributed database** maintained in a hierarchy of name servers
  - The **DNS protocol**: an application layer protocol for querying for translations
    - A DNS-client application sends requests to a DNS-server for translations, the server sends a response.
      - Query: “What is the IP addr of www.google.com?”
      - Response: “216.58.203.4”
    - The DNS protocol **operates over UDP**

Distributed, hierarchical database

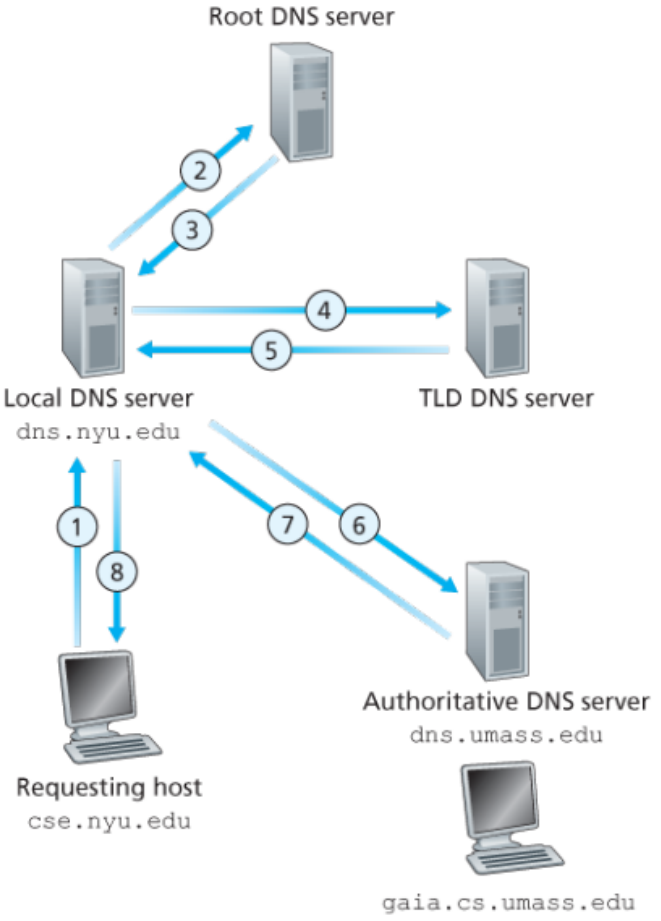


client wants IP for www.amazon.com; 1st approx:

- client queries root server to find com DNS server
- client queries .com DNS server to get amazon.com DNS server
- client queries amazon.com DNS server to get IP address for www.amazon.com

There are currenty 13 root-DNS servers (https://www.iana.org/domains/root/servers)

DNS queries: Iterative and Recursive



Distributed, hierarchical database

- **Root-level Servers:**
  - contacted by local name server that can not resolve name
  - In-turn contacts authoritative name server if name mapping not known, gets mapping and returns mapping to local name server
- **Top-Level domain (TLD) servers:**
  - responsible for com, org, net, edu, aero, jobs, museums, and all top-level country domains, e.g.: uk, fr, ca, jp
- **Authoritative DNS servers:**
  - organization’s own DNS server(s), providing authoritative hostname to IP mappings for organization’s named hosts
  - can be maintained by organization or service provider

Distributed, hierarchical database

- **Local DNS Servers:**
  - does not strictly belong to hierarchy
  - each ISP (residential ISP, company, university) has one, also called “default name server”
  - when host makes DNS query, query is sent to its local DNS server
  - **Caching**: has local cache of recent name-to-address translation pairs (but may be out of date!). Acts as proxy, forwards query into hierarchy

Caching DNS records

- Once (any) name server learns mapping, it can keep a cached copy
- IP addresses of TLD servers typically cached in local name servers, thus root name servers not often visited
- Cache entries timeout (disappear) after some time (TTL)
- Cached entries may be out-of-date ! If name host changes IP address, may not be known Internet-wide until all TTLs expire

Find Out ...

- Who maintains the Root-level and TLD servers?
- Does iitgoa have an Authoritative DNS server?
- If you wish to purchase a domain name for your buisiness, how should you go about this? Who is responsible for selling/giving out domain names?
- What is the IP address of your Local DNS server?
- Can you see the cached DNS records on your computer? How?
- **What happens if the IP address of a domain changes?**
  - How can the Authoritative DNS records be updated?
  - How will the “old” cached records get updated?
- Check out: https://en.wikipedia.org/wiki/ICANN

Format of DNS records

DNS: distributed db storing resource records (RR)

RR format: `(name, value, type, ttl)`

type=A

- **name** is hostname
- **value** is IP address

type=NS

- **name** is domain (e.g., foo.com)
- **value** is hostname of authoritative name server for this domain

type=CNAME

- **name** is alias name for some "canonical" (the real) name
- `www.ibm.com` is really `servereast.backup2.ibm.com`
- **value** is canonical name

type=MX

- **value** is name of mailserver associated with **name**

- Types of DNS records: https://en.wikipedia.org/wiki/List_of_DNS_record_types

DNS Attacks

- **DDoS attacks:**
  - Bombard root servers with ICMP ping traffic: Not very successful because of Traffic Filtering, Local DNS servers cache IPs of TLD servers, allowing root server bypass
- **Bombard TLD servers with requests**
- **Redirect attacks**
  - Man-in-middle : Intercept queries
- **DNS poisoning :** Send bogus relies to DNS server, which caches it
- **Exploit DNS for DDoS:** Send queries with spoofed source address: target IP

So far...

- Structure and Physical components of the Internet
- Design of the Internet: Layering and Encapsulation
- The Applications Layer:
  - Sockets Interface
  - The Web and HTTP
  - DNS

→ **The Transport Layer: how it works**

References and Reading Assignment

- **Kurose and Ross 6th ed**
  - **Section 2.5: DNS**