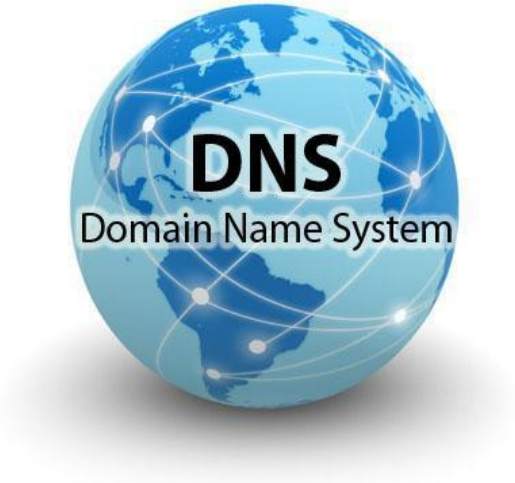
Computer Networks Advanced Course

DNS Protocol

Barak Gonen
Some slides from Jim Kurose

Lesson Goals

- The purpose of the DNS protocol
- Domain name hierarchy
  - Root
  - TLD
  - Zone
- Query types
  - A, AAAA, PTR, CNAME
  - Iterative, recursive
- Hand On
  - Analysis of DNS packets using Wireshark
  - Creation of DNS packets using Scapy

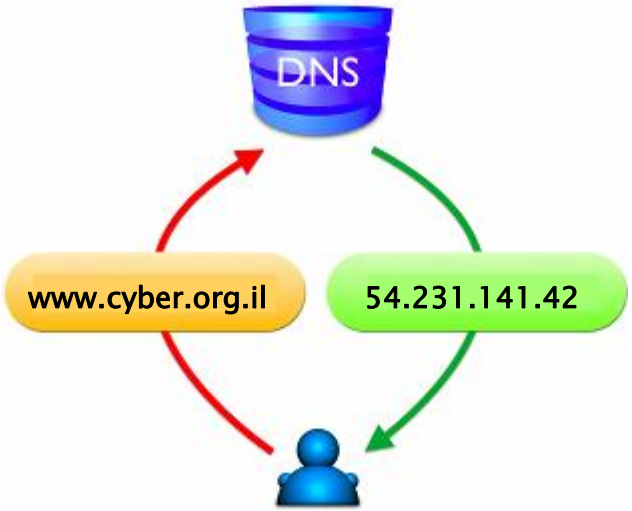


Domain Names

- Why are domain names even required?

DNS Goals

- DNS - Domain Name System
- DNS is an application layer protocol
- Maps domain name to IP addresses
- Without DNS, it is impossible to maintain the Internet
- Why?



Hands On

- Fire up cmd
- Fire up wireshark
- Execute: nslookup www.jct.ac.il

Imagine the world without DNS

- Storage of domain-IP records on every device
  - Storage Volume
  - Keeping the store updated

- Hands on
  - C:\Windows\system32\drivers\etc\hosts

Imagine a Single Global DNS Server

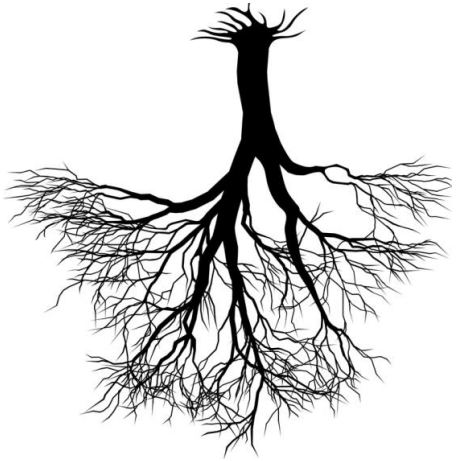
- One server, holding all DNS records
- What are the problems?

Imagine a Single Global DNS Server

- One server, holding all DNS records
- What are the problems?
  - Single point of failure
  - Volume of records
  - Search / response times

Domain Names Hierarchy

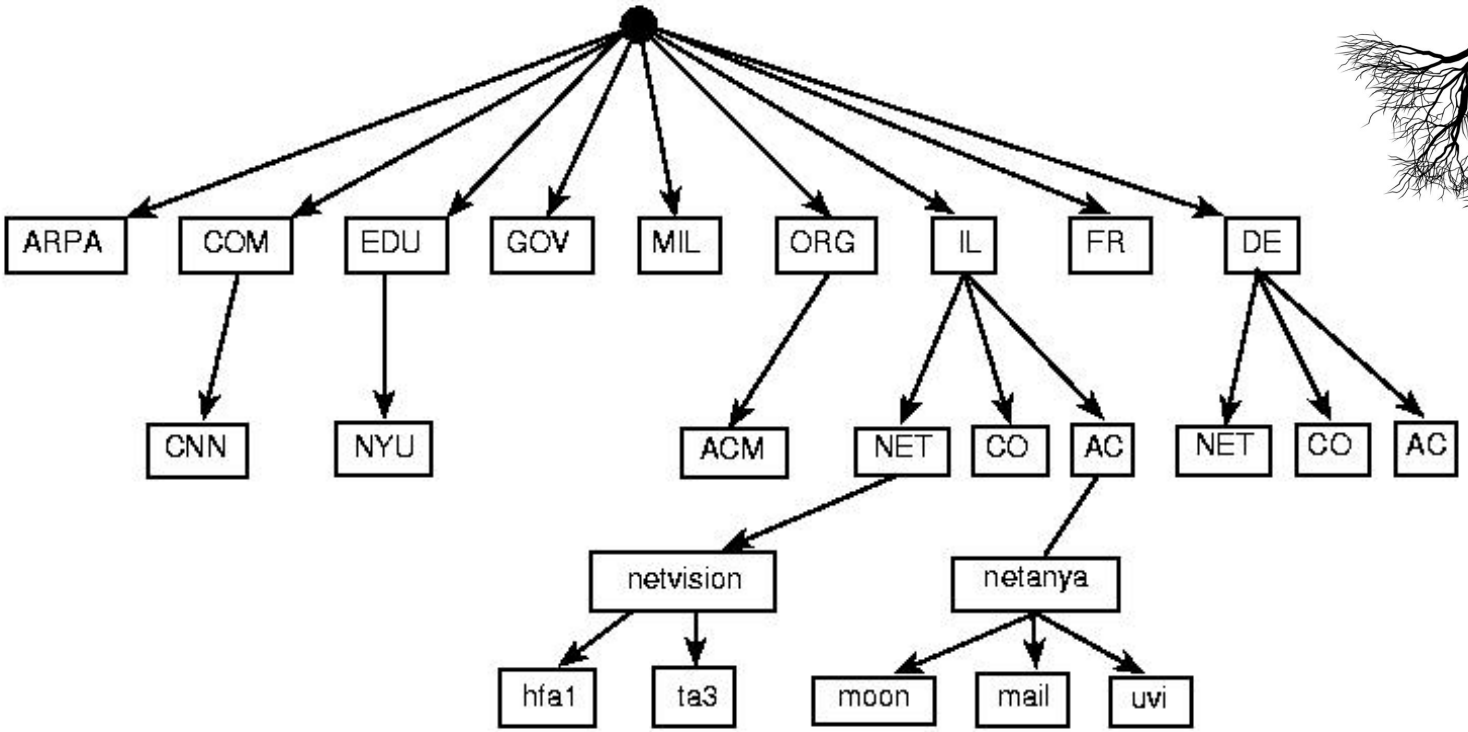
- Principles
  - Multiple servers
  - Each server responsible for a subset of domain names
  - Redundancy
- Domain names are set to levels
- Each DNS server knows only the IPs of domain names in its own level
- “Upside down tree”

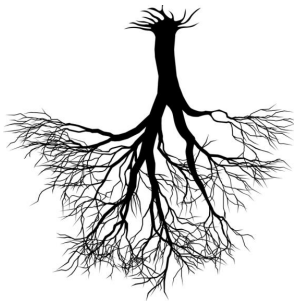


Domain Names Hierarchy – cont.

- **Root server** is the base:
  - Address is "."
  - Belongs to ICANN – Internet Corporation of Assigned Numbers and Names
  - There are few https://www.iana.org/domains/root/servers
- **TLD** – Top Level domain:
  - Country codes – il, us, uk, ru …
  - Generic – com, gov, edu, org, net …
- Zones
- DNS server which "owns" a domain name

Domain Names Hierarchy – Example



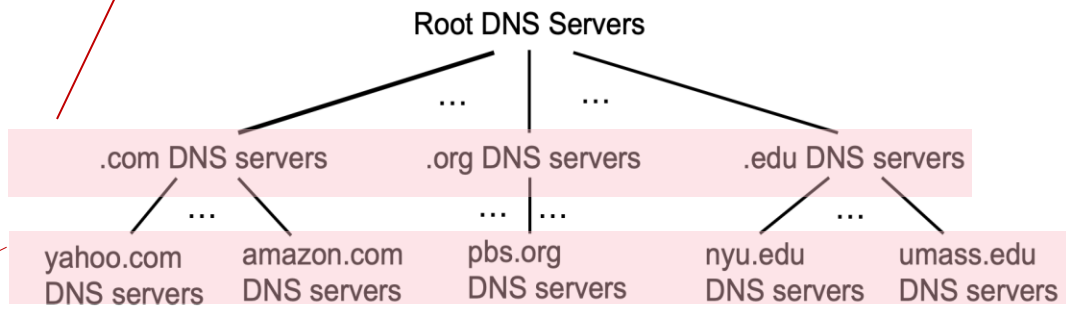


Source :http://mars.netanya.ac.il/~unesco/cdrom/booklet/HTML/NETWORKING/node100.html

Top-Level Domain, and Authoritative Servers

Top-Level Domain (TLD) servers:

- Responsible for .com, .org, .net, .edu, .aero, .jobs, .museums, and all top-level country domains, e.g.: .cn, .uk, .fr, .ca, .jp
- Network Solutions: authoritative registry for .com, .net TLD
- Educause: .edu TLD



Authoritative DNS servers:

- Organization's own DNS server(s), providing authoritative hostname to IP mappings for the organization's named hosts
- Maintained by organization or service provider

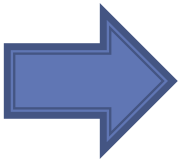
Question

- Do these domains map to the same IP address?
  - www.cyber.org.il
  - www.cyber.il.org

Domain Names Hierarchy – cont.

- Hierarchy is right to left
  - Root, “.”, is not written
  - Dot separates between levels
  - Left- the type of service (default is www)

www.google.co.il



root
il
co
google

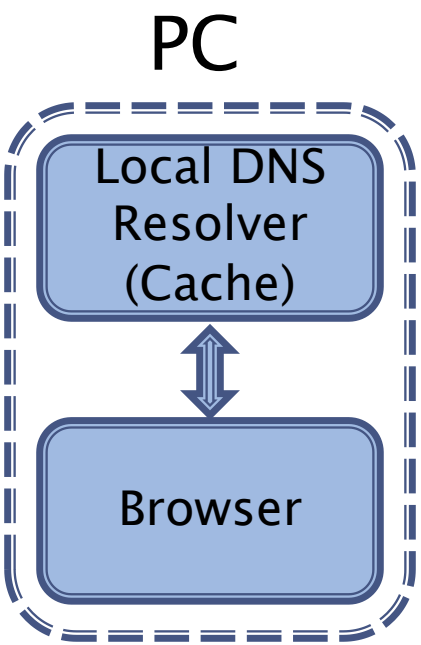
Domain Names Hierarchy – cont.

- Root knows IPs of TLDs
- A TLD server knows only IPs of one level below
  - Ex: www.cyber.org.il, the “il” DNS server knows org.il but not cyber.org.il
- Advantage: A server manages a short list of IPs
  - Simple search
  - Less updates
- A protocol is required to find IPs

DNS Protocol Operation

Stage 1: Browser requests domain name

- Operating system checks if IP is in the cache
- If yes – return IP address(es)



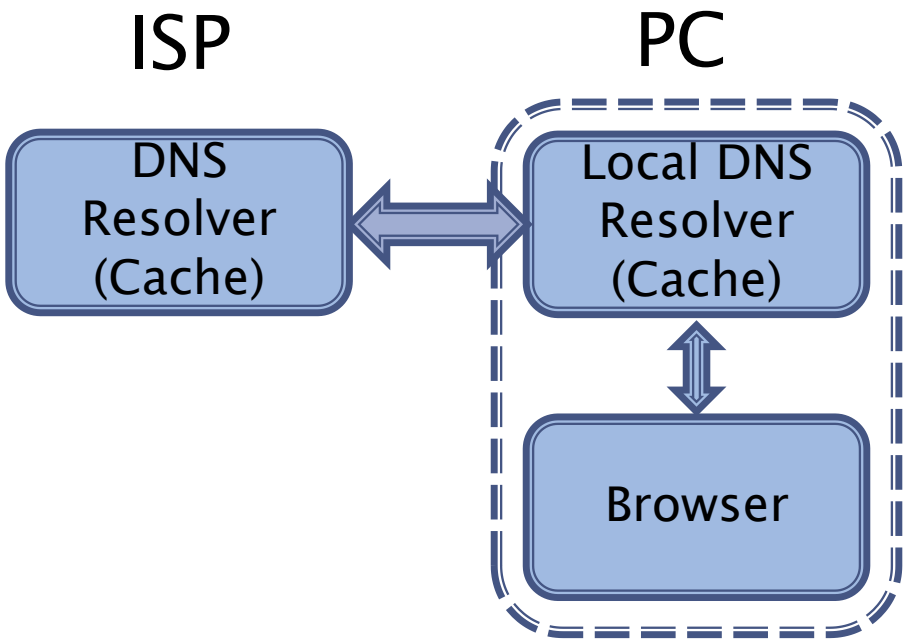
DNS Cache

- Ipconfig /displaydns

```
www.jct.ac.il
----------------------------------------
Record Name . . . . . : www.jct.ac.il
Record Type . . . . . : 1
Time To Live  . . . . : 55815
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 185.186.66.220
```

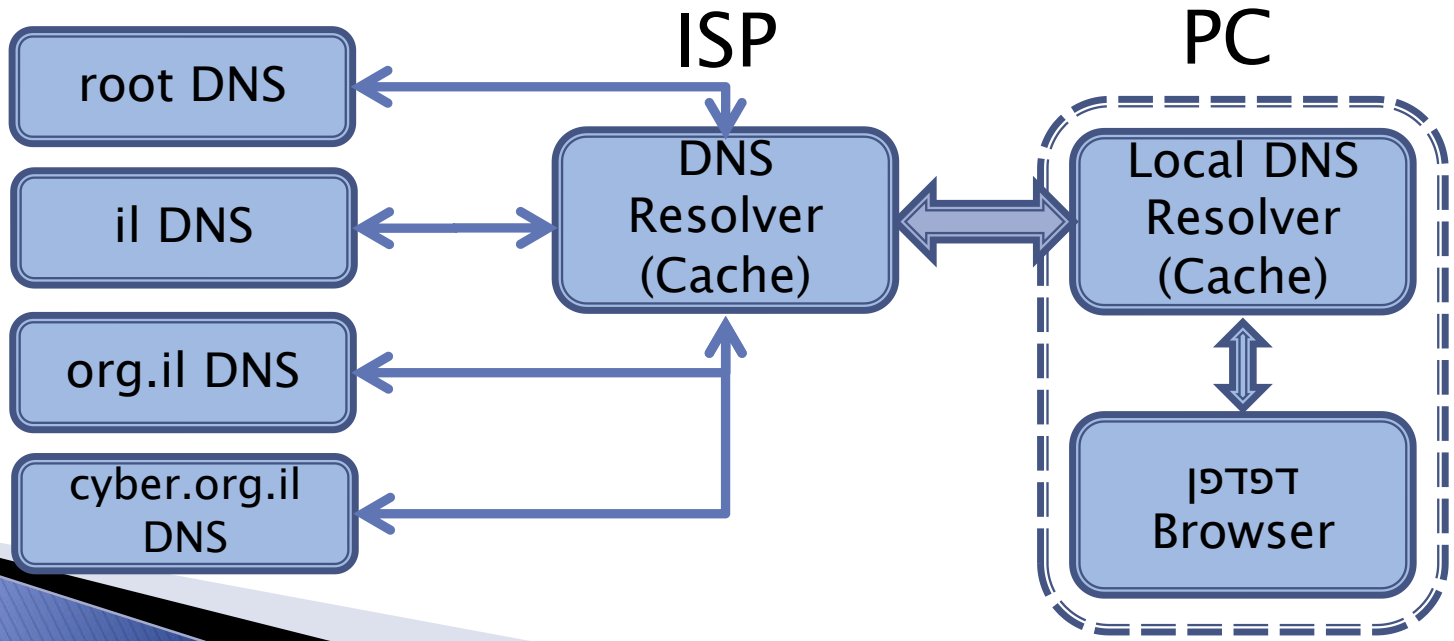
DNS Protocol Operation – cont.

- **Stage 2**: PC makes DNS request to server
  - Typically, ISP server (defined in browser)
  - Named "DNS resolver"
  - Has cache
  - If IP found – return IP address(es)



DNS Protocol Operation – cont.

- **Stage 3:** DNS resolver seeks IP using other DNS servers
- For example, for www.cyber.org.il:
  - From root, requests IP address of “il” DNS server
  - From “il” DNS server, requests IP address of “org.il” DNS server
  - From “org.il” DNS server, requests IP address of “cyber.org.il” DNS server



Bypassing the ISP

- The ISP can spy on us
- Use simple browser setting to bypass
- Demo

DNS Query Types

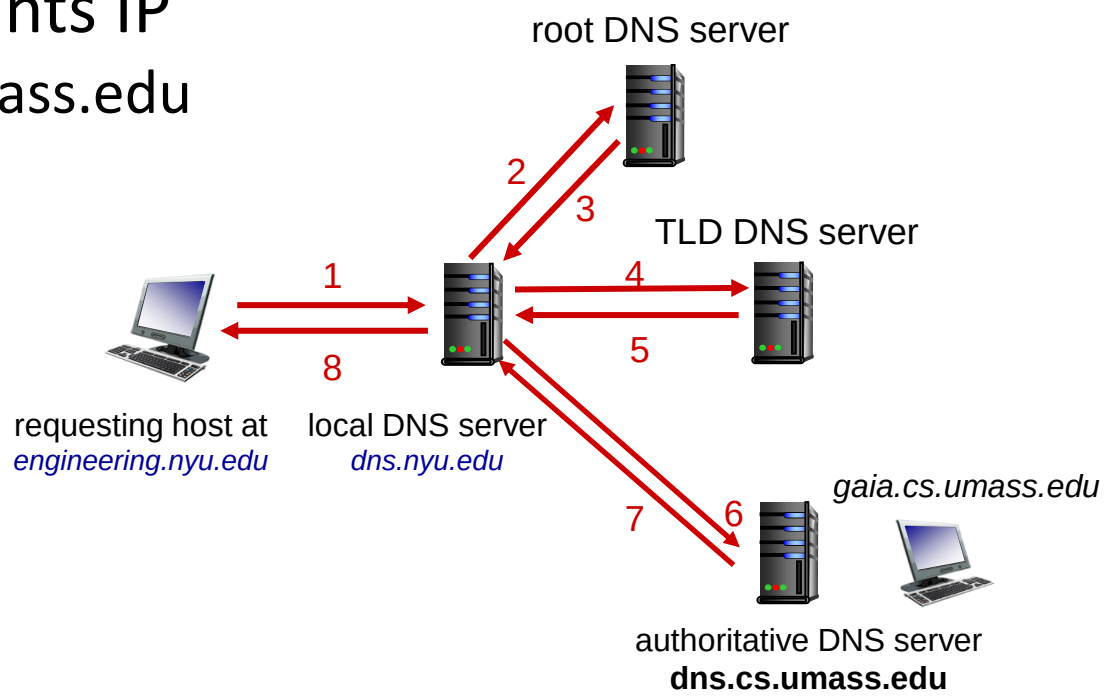
- The DNS resolver returns final IP address(es)
  - Iterative query will return “full service”
- The other servers return only next server’s IP
  - Recursive query
- Protocol field: Recursion Desired (RD flag)
- Perform ex. 4.14 and look for the flag

DNS name resolution: iterative query

Example: host at engineering.nyu.edu wants IP address for gaia.cs.umass.edu

Iterative query:

- contacted server replies with name of server to contact
- "I don't know this name, but ask this server"

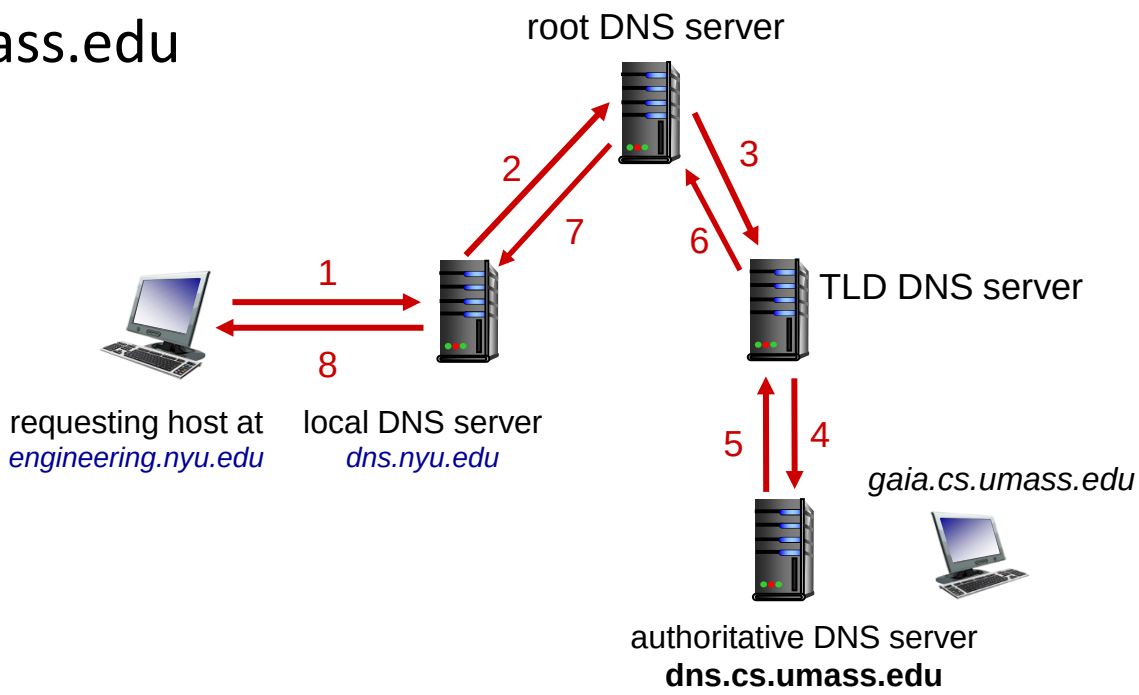


DNS name resolution: recursive query

Example: host at engineering.nyu.edu wants IP address for gaia.cs.umass.edu

Recursive query:

- puts burden of name resolution on contacted name server
- heavy load at upper levels of hierarchy?



DNS Iterative Queries

- Demo – how to find:
  - www.jct.ac.il
  - www.facebook.com
- Hands on – find:
  - www.palmach.org.il
  - www.amazon.com

Reverse Mapping

- Query type:
  - Type ‘A’: Domain -> IP
  - Type ‘PTR’: IP -> Domain
- Perform ex 4.15
  - What is the domain name of IP 8.8.8.8?

DNS records

DNS: distributed database 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 (canonical name)
- `value` is canonical name

type=MX

- `value` is name of SMTP mail server associated with `name`

TTL– Time To Live

- How can the DNS resolver in our PC / ISP tell if DNS cache is updated?
  - DNS response has TTL field
  - Perform ex. 4.16, find TTL field in DNS response

Getting your info into the DNS

Example: new startup "Network Utopia"

- register name networkuptopia.com at *DNS registrar* (e.g., Network Solutions)
  - provide names, IP addresses of authoritative name server (primary and secondary)
  - registrar inserts NS, A RRs into .com TLD server:

    `(networkutopia.com, dns1.networkutopia.com, NS)`

    `(dns1.networkutopia.com, 212.212.212.1, A)`
- create authoritative server locally with IP address `212.212.212.1`
  - type A record for www.networkuptopia.com
  - type MX record for networkutopia.com

Summary

- DNS hierarchy
- DNS query types
- Iterative / recursive query
- DNS cache
- Reverse mapping
- TTL