Domain Name System (DNS)

Tejas Parikh (t.parikh@northeastern.edu)
Spring 2018

CSYE 6225
Northeastern University
https://spring2018.csye6225.com

What is DNS?

- The Domain Name System
- The mechanism by which internet software translate name to attributes such as addresses
- A globally distributed, stateless, scalable, reliable database

DNS Components

DNS is comprised of three components

- Name space (TLDs)
- Name Servers
- Resolvers

Why DNS?

- Human-friendly
  - Is this easy to remember - https://216.58.219.196 ?
  - How about this - https://www.google.com ?
- De-centralized Administration

Global Distribution

- Data is maintained locally, but retrievable globally
  - No single server has all the DNS data
- Remote DNS data is locally cacheable to improve performance

Loose Coherency

- Each version of a subnet of the database (a zone) has a serial number which is incremented on each database change
- Changes to the master copy of the database are propagated to replicas
- Cached data expires according to the timeout set (TTL)

Scalability

- No limit on the size of the database
- No limit to the number of queries
- Queries distributed among masters, slaves, and caches

Reliability

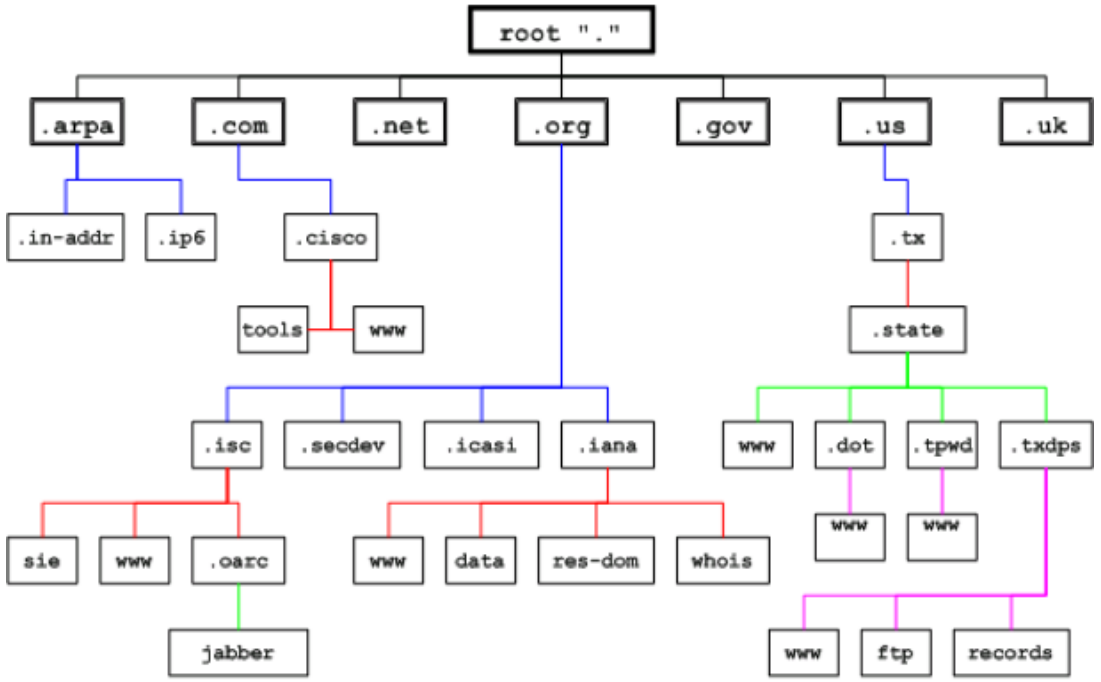
- Data is replicated
- Client can query master or any of the slave servers
- Client will typically query local caches

Dynamicity

- Database on master can be updated dynamically
- Modification of the master database triggers replication

The Name Space

- The **name space** is the structure of the DNS database
  - An inverted tree with the root node at the top
- Each node has a label
- The root node has a **null** label written as "."



.arpa: primarly used for address to host mappings

.com, **.net**, **.org**, **.org**: are generic TLDs (gTLD)

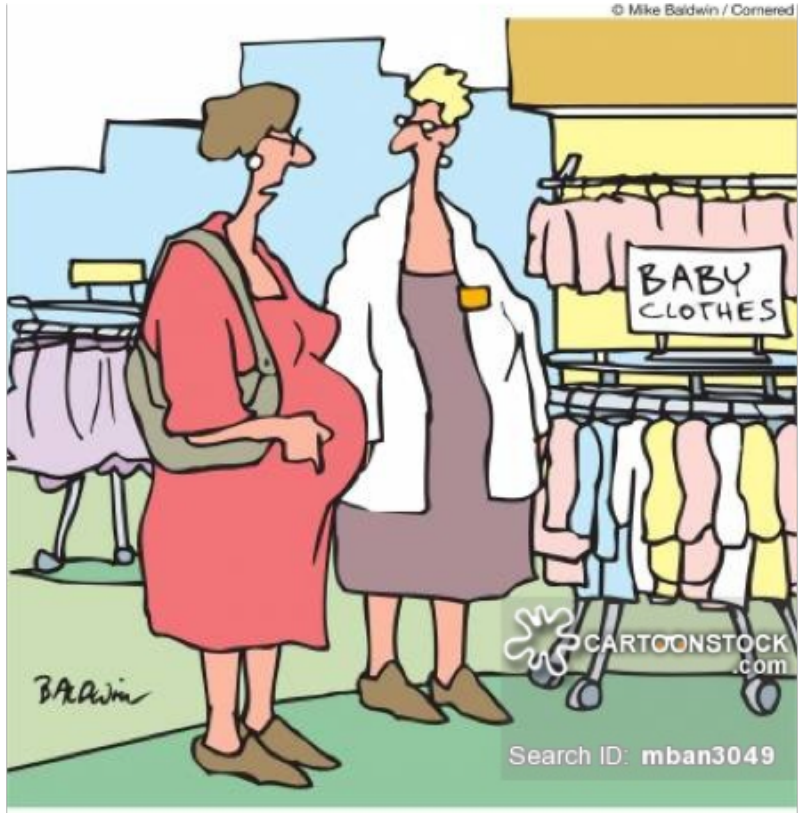
.us, **.uk**: are country code TLDs (ccTLD)

Labels

- Each node in the tree must have label
- A label is a string of up to 63 bytes
- RFCs 852 and 1123 define legal character for hostname
- A-Z, 0-9 and "-" are the only valid characters. A-Z and a-z are treated the same. Hostnames are case-insensitive
- Sibling node must have unique label
- The **null** label is reserved for the root node

Domain Names

- A **domain name** is the sequence of labels from a node to the root, separated by dots ("."s) read left to right
- Domain names are limited to 255 characters in length
- Top-Level Domains (TLDs)
- gTLDs and ccTLDs
- N-level domains - The name space has a maximum depth of 127 levels
- Subdomains



Subdomains

A subdomain is a domain that is part of a larger domain; the only domain that is not also a subdomain is the root domain. For example, **west.example.com** and **east.example.com** are subdomains of the **example.com** domain, which in turn is a subdomain of the **com** top-level domain (TLD).

Name Servers

- Run the software (BIND, BIND 9, NSD) which receive and respond to DNS queries
- Name servers store information about the name space in units called "zone"
- Usually, more than one name server are authoritative for the same zone ensuring redundancy and load balancing
- A single name server may be authoritative for many zones

Types of Name Servers

- Two main types of name servers
  - **Authoritative** – maintains the data
    - Master – where the data is edited
    - Slave – where the data is replicated to
  - **Caching** – stores data obtained from authoritative server
- No special hardware is needed to run name servers

Zones

- Name space having an administrator
- Each zone is defined in a Zone File
- Zone file has Resource Records (RRs)

Zone File Example

```
; SOA Record
example.com.    3600    IN  SOA ns69.domaincontrol.com. dns.jomax.net (
                2016122100
                28800
                7200
                604800
                600
                )

; A Records
@   600 IN  A   154.45.18.26

; CNAME Records
www 3600    IN  CNAME   @
email   3600    IN  CNAME   email.secureserver.net

; MX Records
@   3600    IN  MX  10  mailstore1.secureserver.net
@   3600    IN  MX  0   smtp.secureserver.net

; TXT Records
@   3600    IN  TXT "site-verification-1213fasd12312414asda"

; NS Records
@   3600    IN  NS  ns69.domaincontrol.com
@   3600    IN  NS  ns70.domaincontrol.com
```

DNS Resource Record Types

- **A** - The value for an A record is an IPv4 address in dotted decimal notation
- **AAAA** - The value for a AAAA record is an IPv6 address in colon-separated hexadecimal format
- **CAA** - A CAA record lets you specify which certificate authorities (CAs) are allowed to issue certificates for a domain or subdomain.
- **CNAME** - A CNAME Value element is the same format as a domain name
- **MX** - A mail exchanger record (MX record) is a type of resource record in the Domain Name System that specifies a mail server responsible for accepting email messages on behalf of a recipient's domain
- **NS** - An NS record identifies the name servers for the hosted zone
- **SOA** - A start of authority (SOA) record provides information about a domain and the corresponding hosted zone
- **SPF** - SPF records were formerly used to verify the identity of the sender of email messages.
- **TXT** - A TXT record contains a space-separated list of double-quoted strings
- and many more types

TTL (Time to Live)

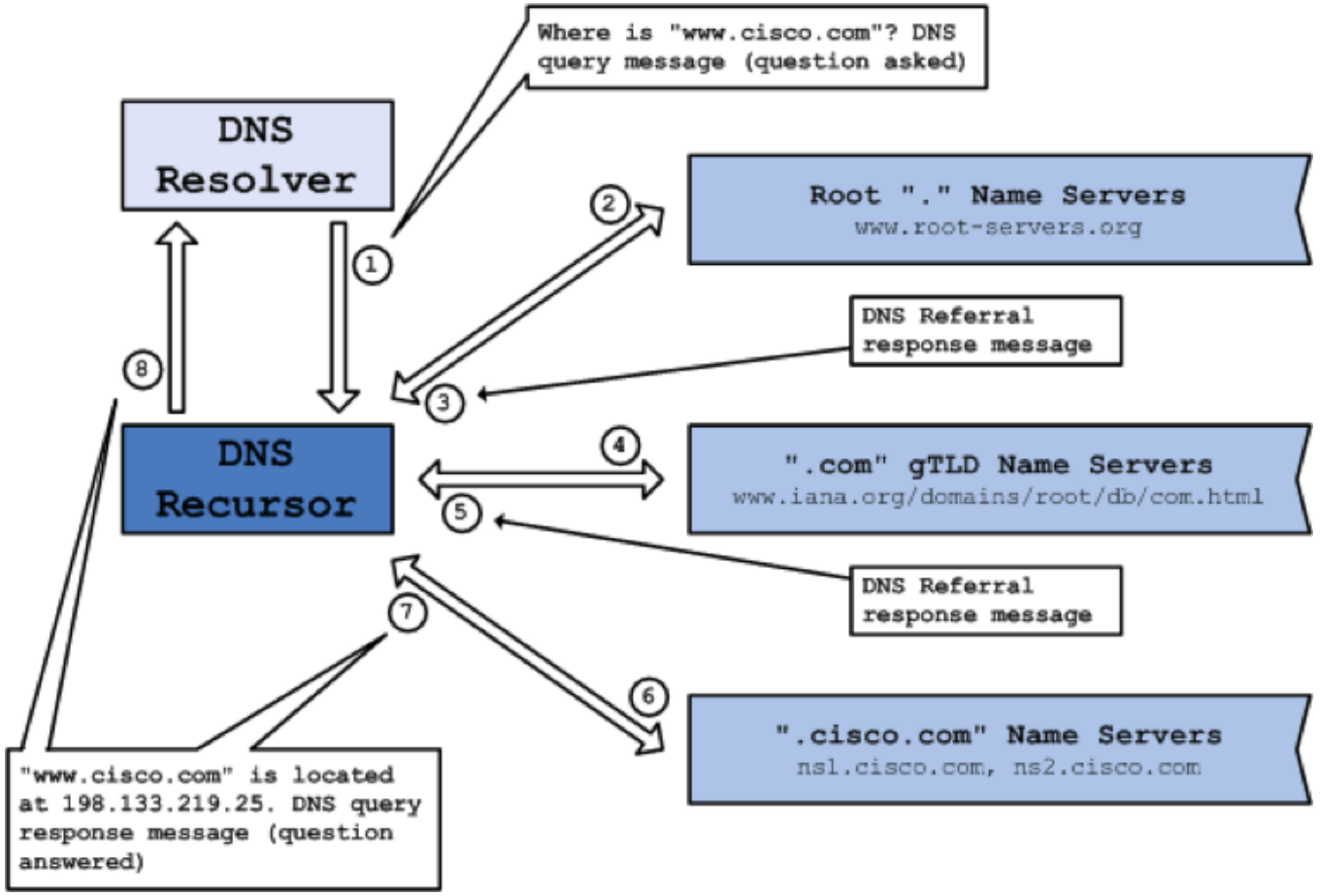
- The amount of time, in seconds, that you want DNS recursive resolvers to cache information about this resource record set.
- If you specify a longer value (for example, 172800 seconds, or two days it often takes longer for changes to the resource record set (for example, a new IP address) to take effect because recursive resolvers use the values in their cache for longer periods instead of querying.

I'll tell you a DNS joke but be advised, it could take up to 24 hours for everyone to get it.

Name Resolution

- Name resolution is the process by which resolvers and name space servers cooperate to find data in the name space
- A DNS query has three parameters:
  - A domain name (e.g. www.example.com)
  - A class (e.g IN), and
  - A type (e.g. A)
- Upon receiving a query from a resolver, a name server will
  1. look for answer in its authoritative data and its cache
  2. if step 1 fails, the answer must be looked up

Recursive Query



DNS Query Resolution Process Example

```
sh-3.2# dig +trace @8.8.8.8 www.northeastern.edu
; <<>> DiG 9.8.3-P1 <<>> +trace @8.8.8.8 www.northeastern.edu
; (1 server found)
;; global options: +cmd
.            160738   IN   NS   c.root-servers.net.
.            160738   IN   NS   l.root-servers.net.
.            160738   IN   NS   m.root-servers.net.
.            160738   IN   NS   b.root-servers.net.
.            160738   IN   NS   f.root-servers.net.
.            160738   IN   NS   i.root-servers.net.
.            160738   IN   NS   a.root-servers.net.
.            160738   IN   NS   h.root-servers.net.
.            160738   IN   NS   k.root-servers.net.
.            160738   IN   NS   g.root-servers.net.
.            160738   IN   NS   d.root-servers.net.
.            160738   IN   NS   j.root-servers.net.
.            160738   IN   NS   e.root-servers.net.
;; Received 228 bytes from 8.8.8.8#53(8.8.8.8) in 38 ms

edu.         172800   IN   NS   c.edu-servers.net.
edu.         172800   IN   NS   l.edu-servers.net.
edu.         172800   IN   NS   d.edu-servers.net.
edu.         172800   IN   NS   f.edu-servers.net.
edu.         172800   IN   NS   g.edu-servers.net.
edu.         172800   IN   NS   a.edu-servers.net.
;; Received 273 bytes from 192.228.79.201#53(192.228.79.201) in 89 ms

northeastern.edu.   172800   IN   NS   ns20.customer.level3.net.
northeastern.edu.   172800   IN   NS   ns29.customer.level3.net.
northeastern.edu.   172800   IN   NS   nb4276.neu.edu.
northeastern.edu.   172800   IN   NS   nb4277.neu.edu.
;; Received 205 bytes from 192.26.92.30#53(192.26.92.30) in 15 ms

www.northeastern.edu.   600    IN   A    155.33.17.68
northeastern.edu.   3600   IN   NS   ns20.customer.level3.net.
northeastern.edu.   3600   IN   NS   ns29.customer.level3.net.
northeastern.edu.   3600   IN   NS   nb4276.neu.edu.
northeastern.edu.   3600   IN   NS   nb4277.neu.edu.
```

```
www.northeastern.edu.   600    IN   A    155.33.17.68
northeastern.edu.   3600   IN   NS   ns20.customer.level3.net.
northeastern.edu.   3600   IN   NS   ns29.customer.level3.net.
northeastern.edu.   3600   IN   NS   nb4276.neu.edu.
northeastern.edu.   3600   IN   NS   nb4277.neu.edu.
;; Received 189 bytes from 155.33.16.201#53(155.33.16.201) in 9 ms
```

Demo

dig +trace @8.8.8.8 csye6225.com

Internet Corporation for Assigned Names and Numbers (ICANN)

- Not-for-profit corporation
- Manages the IP namespace
- Controls the Top-level names
- Manages/oversees the root servers

The Root Name Servers

- The root zone file lists the name and IP addresses of the authoritative DNS servers for all top-level domains (TLDs)
- The root zone file is published on 13 root servers. However, as there are an incredible number of names to resolve every minute, each of these servers is actually mirrored. The interesting thing about this set up is that each of the mirrors for a single root server share the same IP address. When requests are made for a certain root server, the request will be routed to the nearest mirror of that root server.
- The Root name server operations is currently provided by volunteer efforts by a very diverse set of organizations.

Registries, Registrars, and Registrants

- A Registrant’s domain gets registered by a Registrar who is accredited by a Registry.
- Registries - gTLD and ccTLD Registries.
- Registrars - GoDaddy, 1&1, Namecheap, etc.

DNSSec

- Uses public key cryptography to sign DNS answers.
- Allows the resolvers to validate responses.
- Four main new RRs: DNSKEY, RRSIG, DS, NSEC3.
- Slow adaptation.

DNS Related Outages

- https://www.cnet.com/news/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/
- https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/
- http://www.zdnet.com/article/global-dns-outage-hits-microsoft-azure-customers/
- http://www.businessinsider.com/google-is-down-2015-3
- https://www.digitalocean.com/company/blog/update-on-the-march-24-2016-dns-outage/
- https://www.wired.com/2012/09/godaddy-goes-down/

THE RUMORS ARE TRUE. GOOGLE WILL BE SHUTTING DOWN PLUS—
ALONG WITH HANGOUTS, PHOTOS, VOICE, DOCS, DRIVE, MAPS, GMAIL, CHROME, ANDROID, AND SEARCH—
TO FOCUS ON OUR CORE PROJECT:
THE 8.8.8.8 DNS SERVER.
Google

Additional Resources

https://spring2018.csye6225.com/