Domain Name System (DNS)

Tejas Parikh (t.parikh@northeastern.edu)

CSYE 6225
Northeastern University

What is Domain Name System (DNS)?

- DNS, or the Domain Name System is the networking system in place that allows us to resolve human-friendly names to unique IP addresses.
- DNS can be thought of as the phonebook of the Internet.
  - Humans access information online through domain names, like nytimes.com or espn.com.
  - Web browsers interact through Internet Protocol (IP) addresses.
  - DNS translates domain names to IP addresses so browsers can load Internet resources.
- DNS is a globally distributed, stateless, scalable, reliable database.

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 primary, secondary, 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

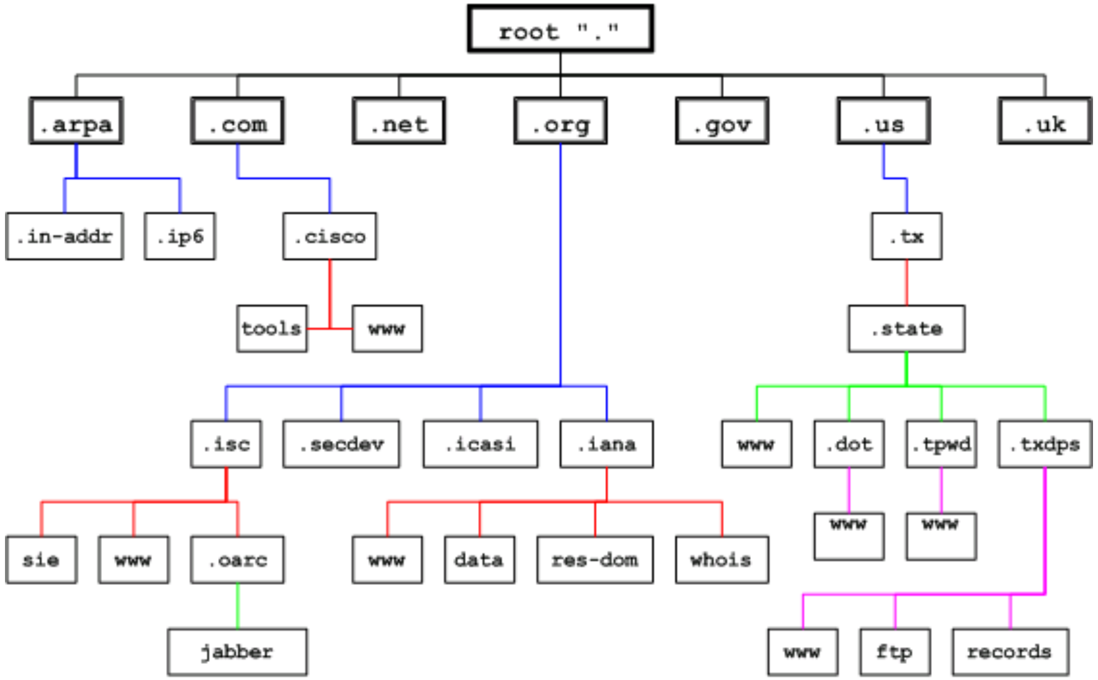
DNS Components

DNS is comprised of three components

- Name space (TLDs)
- Name Servers
- Resolvers

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)

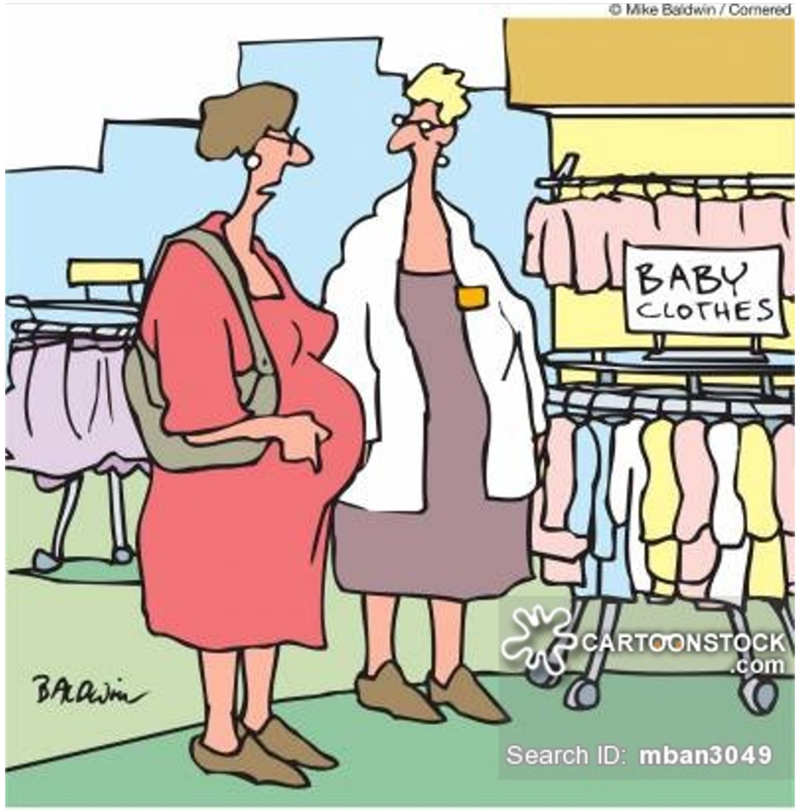
.us, **.uk**: are country code TLDs (ccTLD)

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 (".") read left to right
- Domain names are limited to 255 characters in length
- Top-Level Domains (TLDs)
    - gTLDs: Generic top-level domain
    - ccTLDs: Country code top-level domain
- N-level domains - The name space has a maximum depth of <u>127 levels</u>
- Subdomains



"It's our first. Don't know where to begin. Haven't even picked out a domain name."

Top-Level Domain

- A top-level domain, or TLD, is the most general part of the domain.
- The top-level domain is the furthest portion to the right (as separated by a dot).
- Common top-level domains are “com”, “net”, “org”, “gov”, “edu”, and “io”.
- Top-level domains are at the top of the hierarchy in terms of domain names.

Country code top-level domain

- A country code top-level domain (ccTLD) is an Internet top-level domain generally used or reserved for a country, sovereign state, or dependent territory identified with a country code.
- All ASCII ccTLD identifiers are two letters long, and all two-letter top-level domains are ccTLDs.
- There are 312 ccTLDs in active use totally.
    - The .cn, .tk, .de and .uk ccTLDs contain the highest number of domains.

Subdomains

- DNS works in a hierarchy.
- TLDs can have many domains under them.
  - For instance, the “com” TLD has both “google.com” and “ubuntu.com” underneath it.
- 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).

Fully Qualified Domain Name

- A fully qualified domain name, often called FQDN, is what we call an absolute domain name.
- Domains in the DNS system can be given relative to one another, and as such, can be somewhat ambiguous.
- A FQDN is an absolute name that specifies its location in relation to the absolute root of the domain name system.
- A proper FQDN ends with a dot, indicating the root of the DNS hierarchy. An example of a FQDN is **mail.google.com.**

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

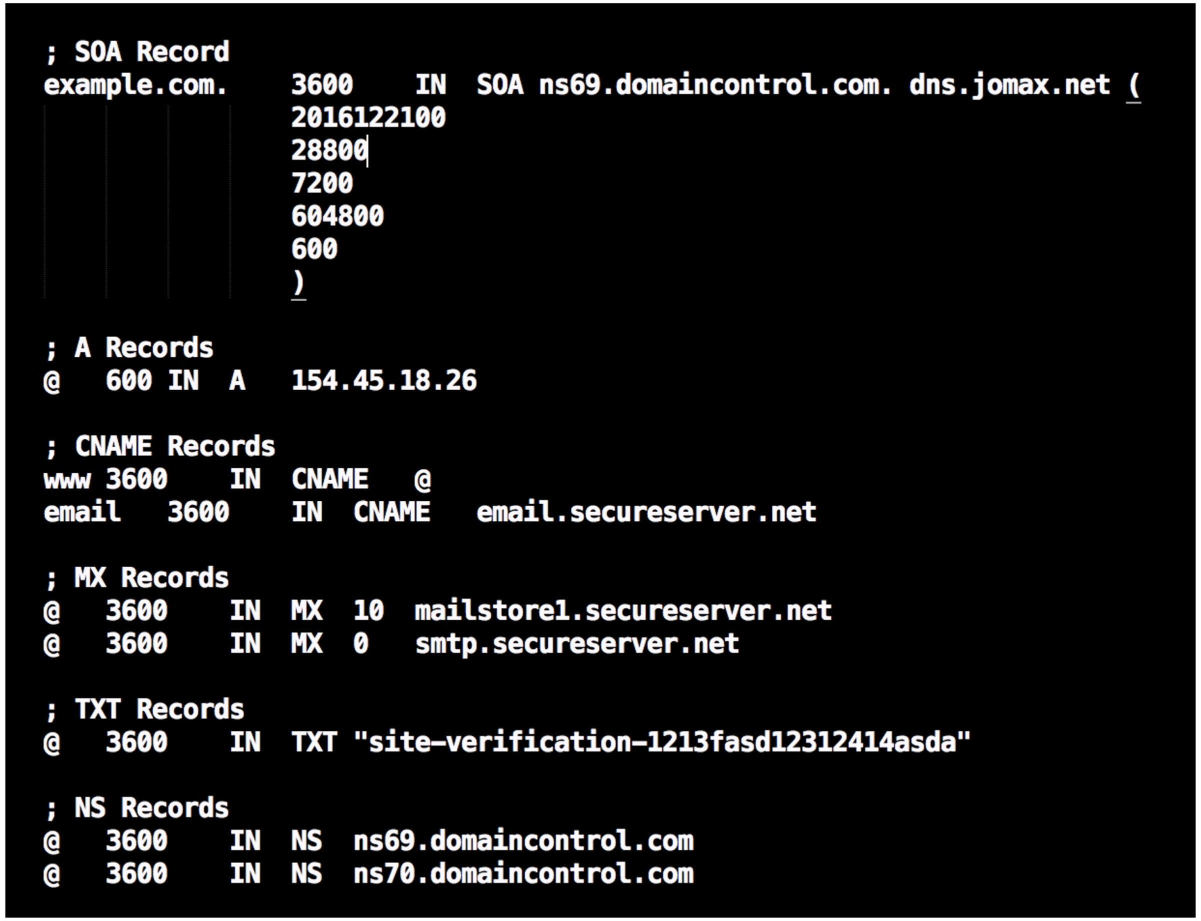
Types of Name Servers

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

Zones

- The DNS is broken up into many different zones.
- These zones differentiate between distinctly managed areas in the DNS namespace.
- A DNS zone is a portion of the DNS namespace that is managed by a specific organization or administrator.
- A DNS zone is an administrative space which allows for more granular control of DNS components, such as authoritative nameservers.
- The domain name space is a hierarchical tree, with the DNS root domain at the top.
- A DNS zone starts at a domain within the tree and can also extend down into subdomains so that multiple subdomains can be managed by one entity.

Zone File Example



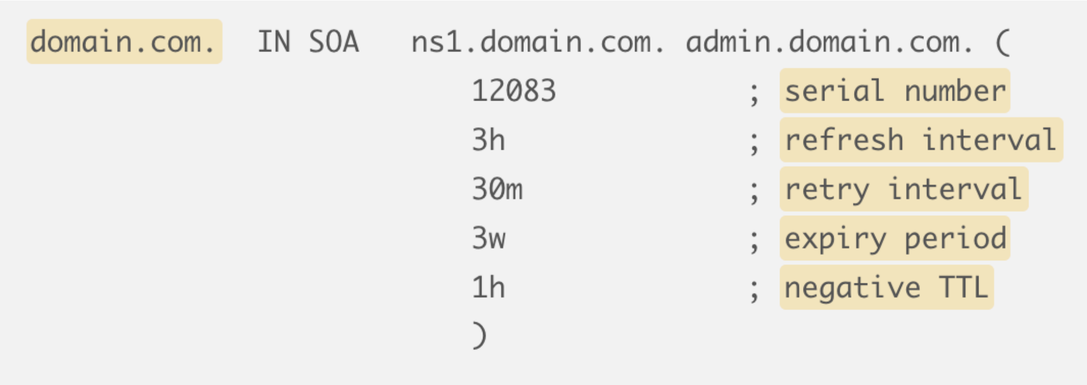
```
; SOA Record
example.com.    3600    IN  SOA ns69.domaincontrol.com. dns.jomax.net (
                2016122100
                28800
                7200
                604800
                600
                )

; 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

SOA record

- The DNS "start of authority" (SOA) record stores important information about a domain or zone such as the email address of the administrator, when the domain was last updated, and how long the server should wait between refreshes.



```
domain.com.  IN SOA  ns1.domain.com. admin.domain.com. (
                          12083          ; serial number
                          3h             ; refresh interval
                          30m            ; retry interval
                          3w             ; expiry period
                          1h             ; negative TTL
                          )
```

A Record

- The ‘A’ stands for ‘address’ and this is the most fundamental type of DNS record: it indicates the IP address of a given domain.
- **A** records hold IPv4 addresses.
- The most common usage of **A** records is IP address lookups: matching a domain name to an IPv4 address.

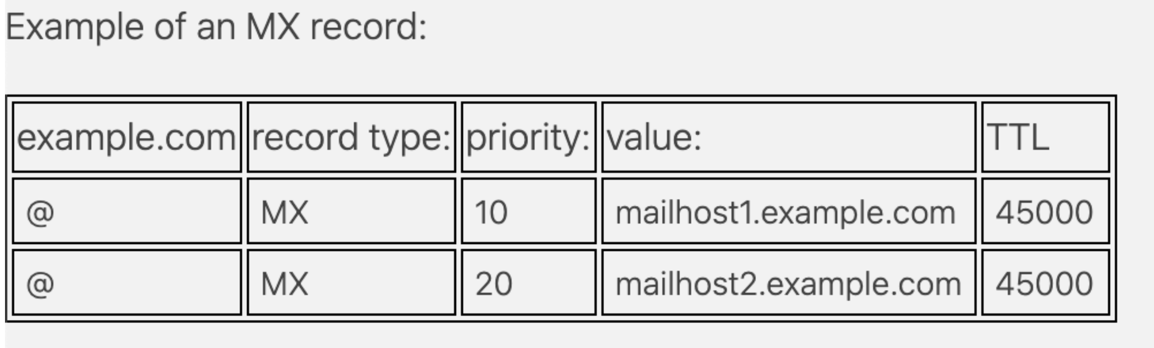
AAAA Record

- **AAAA** records hold IPv6 addresses.

CNAME Record

- The ‘canonical name’ (CNAME) record is used in lieu of an A record, when a domain or subdomain is an alias of another domain.
- All CNAME records must point to a domain, never to an IP address.

MX Record



Example of an MX record:

example.com	record type:	priority:	value:	TTL
@	MX	10	mailhost1.example.com	45000
@	MX	20	mailhost2.example.com	45000

- A DNS 'mail exchange' (MX) record directs email to a mail server.
- The MX record indicates how email messages should be routed in accordance with the Simple Mail Transfer Protocol (SMTP, the standard protocol for all email).
- Like CNAME records, an MX record must always point to another domain.
- The 'priority' numbers before the domains for these MX records indicate preference; the lower 'priority' value is preferred.
    - The server will always try mailhost1 first because 10 is lower than 20.
    - In the result of a message send failure, the server will default to mailhost2.

TXT Record

- The DNS ‘text’ (TXT) record lets a domain administrator enter text into the Domain Name System (DNS).
- One domain can have many TXT records.
- Today, two of the most important uses for DNS TXT records are email spam prevention and domain ownership verification, although TXT records were not designed for these uses originally.

NS Record

- NS stands for ‘nameserver,’ and the nameserver record indicates which DNS server is authoritative for that domain (i.e. which server contains the actual DNS records).
- NS records tell the Internet where to go to find out a domain's IP address.
- A domain often has multiple NS records which can indicate primary and backup nameservers for that domain.
- Without properly configured NS records, users will be unable to load a website or application.

CAA Record

- This is the ‘certification authority authorization’ record, it allows domain owners state which certificate authorities can issue certificates for that domain.
- If no CAA record exists, then anyone can issue a certificate for the domain.
- These records are also inherited by subdomains.

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

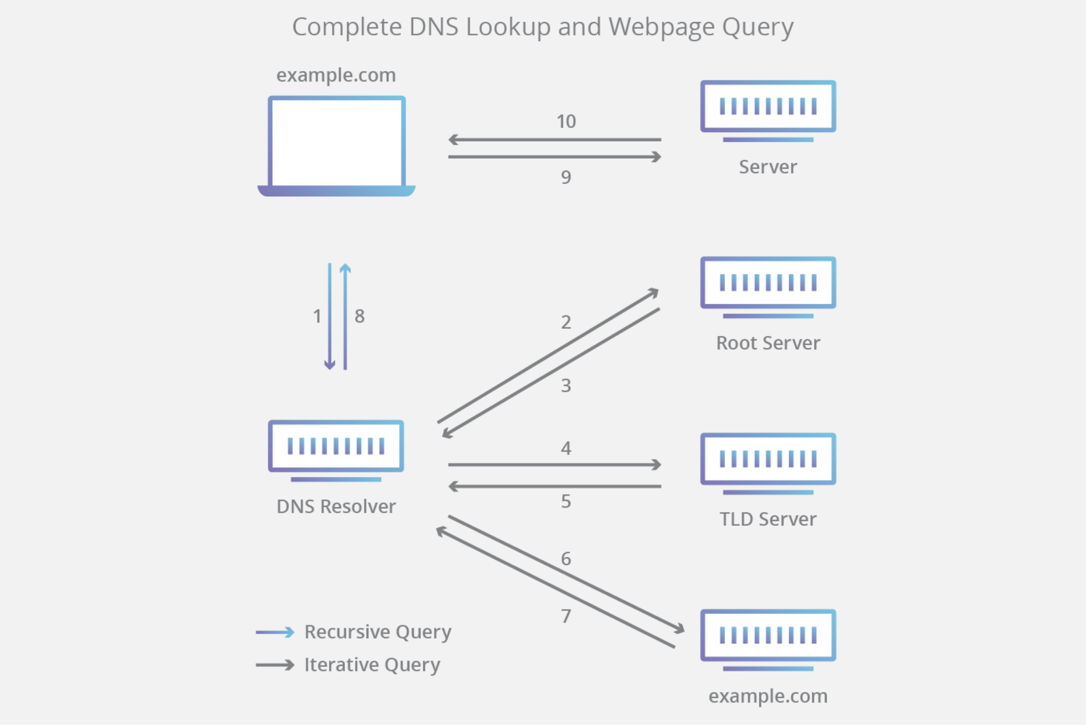
- Name resolution is the process by which resolvers and name space servers cooperate to find data in the name space
- A DNS query has three parameters:
  - A domain name (e.g., www.example.com)
  - A class (e.g., IN), and
  - A type (e.g., A)
- Upon receiving a query from a resolver, a name server will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

The 8 steps in a DNS lookup

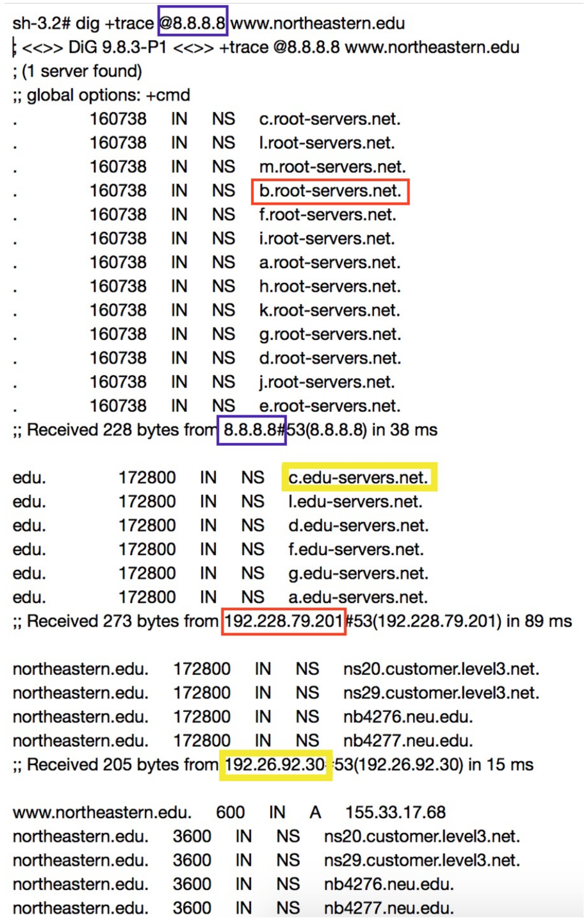
1. A user types ‘example.com’ into a web browser and the query travels into the Internet and is received by a DNS recursive resolver.
2. The resolver then queries a DNS root nameserver (.).
3. The root server then responds to the resolver with the address of a Top-Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD.
4. The resolver then makes a request to the .com TLD.
5. The TLD server then responds with the IP address of the domain’s nameserver, example.com.
6. Lastly, the recursive resolver sends a query to the domain’s nameserver.
7. The IP address for example.com is then returned to the resolver from the nameserver.
8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially.

Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser is able to make the request for the web page:

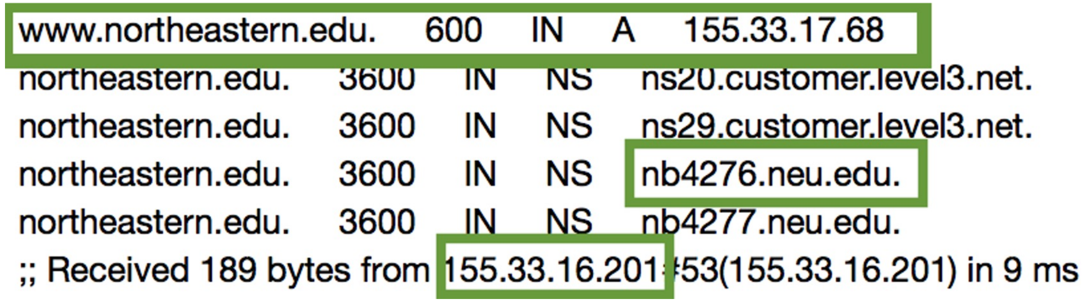
- The browser makes a HTTP request to the IP address.
- The server at that IP returns the webpage to be rendered in the browser (step 10).



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
```

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

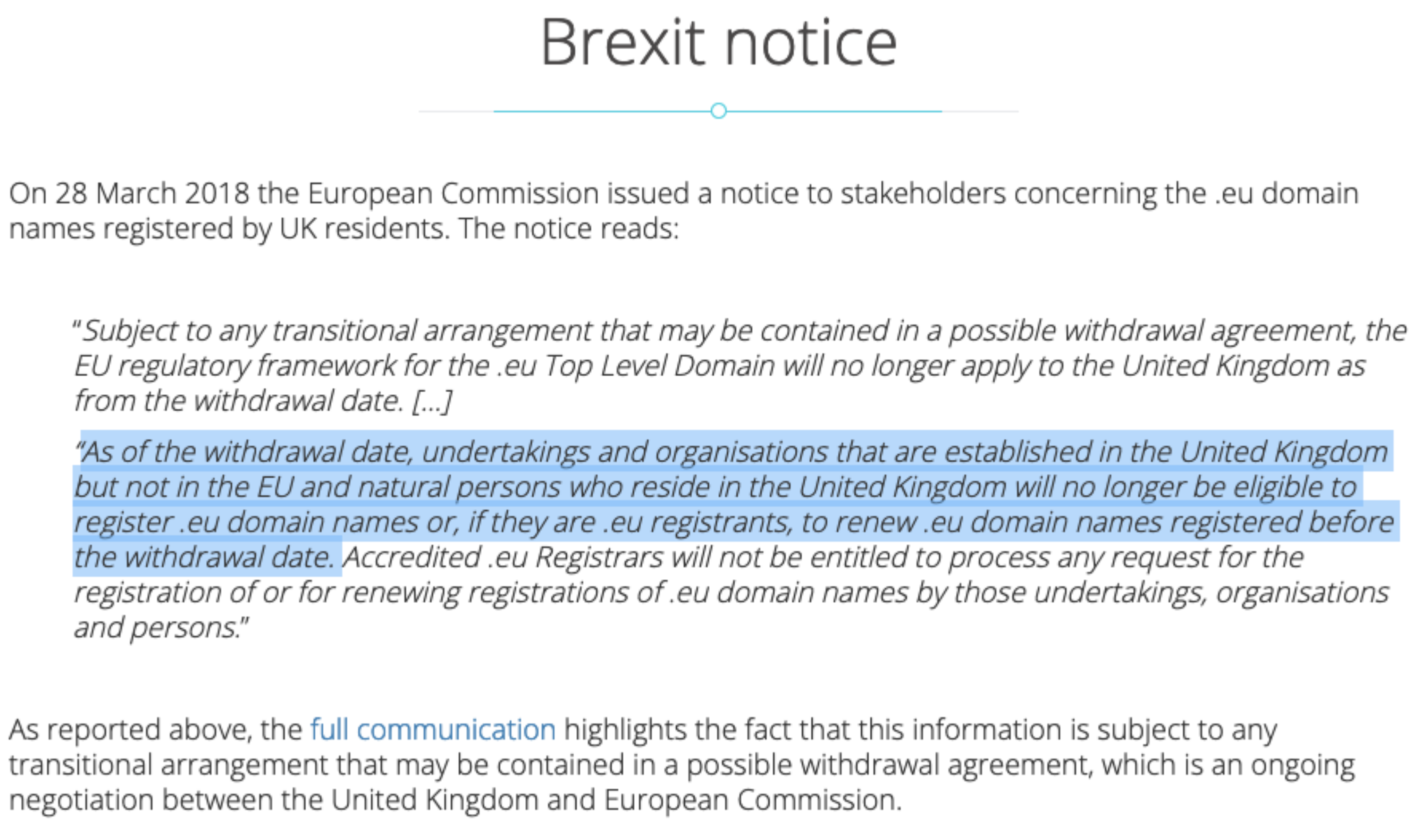
- The root zone file lists the name and IP addresses of the authoritative DNS servers for all top-level domains (TLDs).
- The root zone file is published on 13 root servers.
  - However, as there are an incredible number of names to resolve every minute, each of these servers is mirrored.
  - The interesting 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.

Risks of ccTLD

https://eurid.eu/en/register-a-eu-domain/brexit-notice/

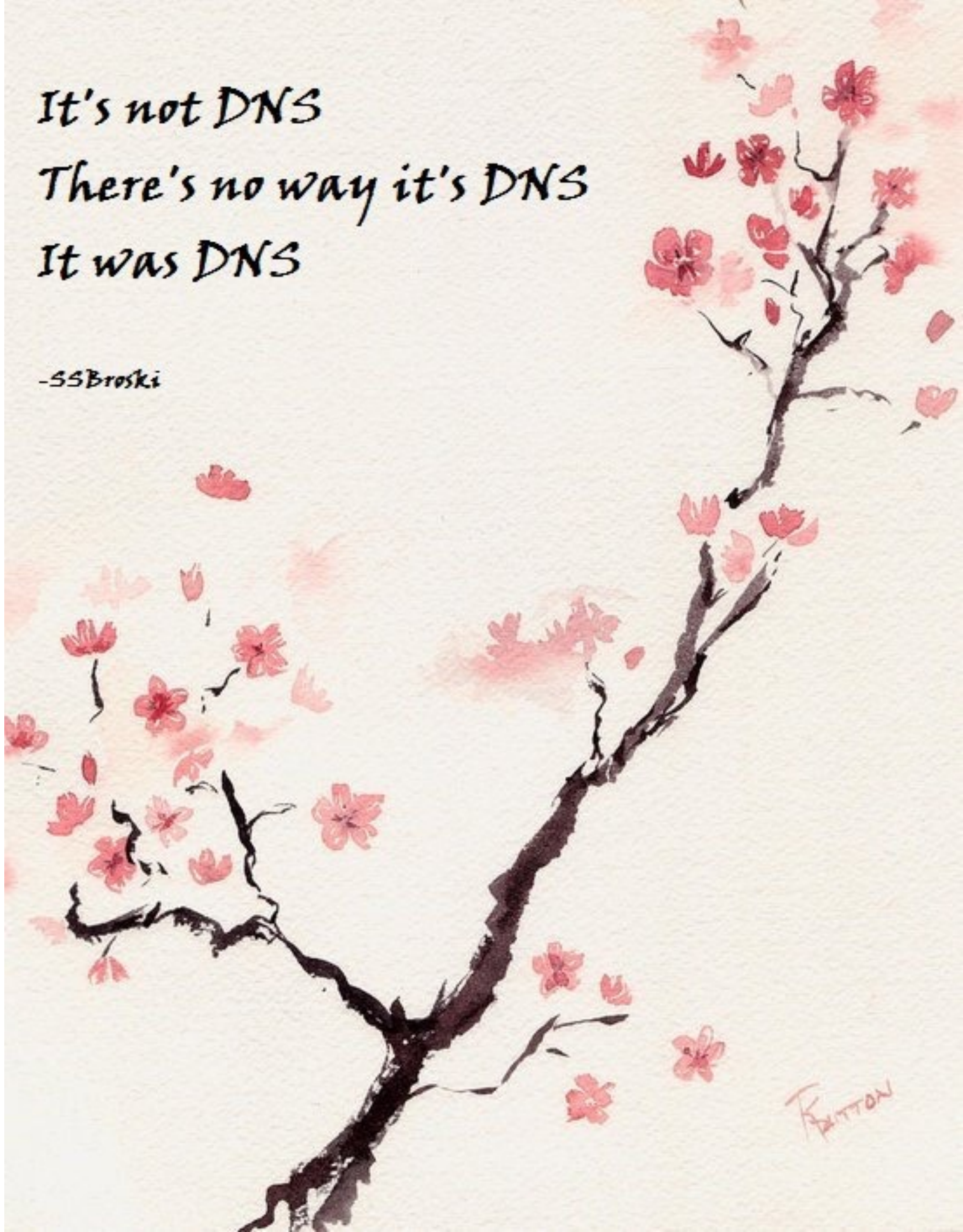


Brexit notice

On 28 March 2018 the European Commission issued a notice to stakeholders concerning the .eu domain names registered by UK residents. The notice reads:

> "*Subject to any transitional arrangement that may be contained in a possible withdrawal agreement, the EU regulatory framework for the .eu Top Level Domain will no longer apply to the United Kingdom as from the withdrawal date. [...]*
>
> *"As of the withdrawal date, undertakings and organisations that are established in the United Kingdom but not in the EU and natural persons who reside in the United Kingdom will no longer be eligible to register .eu domain names or, if they are .eu registrants, to renew .eu domain names registered before the withdrawal date. Accredited .eu Registrars will not be entitled to process any request for the registration of or for renewing registrations of .eu domain names by those undertakings, organisations and persons."*

As reported above, the full communication highlights the fact that this information is subject to any transitional arrangement that may be contained in a possible withdrawal agreement, which is an ongoing negotiation between the United Kingdom and European Commission.



It's not DNS
There's no way it's DNS
It was DNS

-SSBroski

References

- https://www.cloudflare.com/learning/dns/what-is-dns/
- https://www.digitalocean.com/community/tutorials/an-introduction-to-dns-terminology-components-and-concepts
- https://www.ibm.com/cloud/learn/dns
- https://github.com/ahupowerdns/hello-dns

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/
- https://nakedsecurity.sophos.com/2019/02/01/dns-outage-turns-tables-on-azure-database-users/

Additional Resources

See Lecture Page