The Domain Name System

Greg Horie

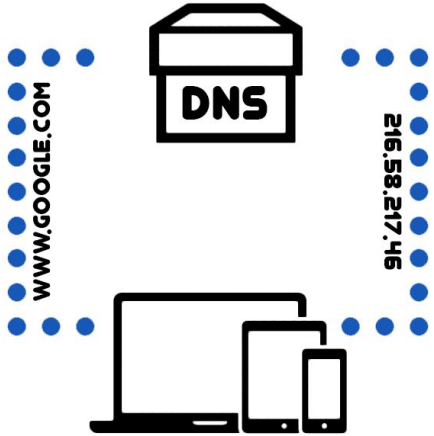
DNS - What is it?

DNS is ...

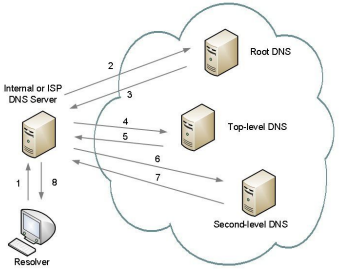
- A naming hierarchy for the Internet.
- A service for looking up Internet resource records.
  - Typically domain names to IP addresses.
- A protocol that enables name resolution.
  - RFC 1034 and RFC 1035.

Analogy …

- DNS is a phone book for your network.
- Given a name, you can look up an address.



DNS - Why do we need it?



- Domain names provide a abstraction over the Internet Protocol.
  - Names are easy to remember compared with IPs.
    - e.g. vicpimakers.ca vs. 2607:7b00:3000:4::597e:ebad
  - Names provide flexibility
    - e.g. IP can change, but domain name stays the same.
    - e.g. Multiple IPs assigned to the same name to serve in different geo-locations or for redundancy.
  - Names hide IP protocol version
    - I.e. Same domain name used to reference both IPv4 and IPv6

DNS Records Types

- Some common DNS record types:

DNS Type	Record	Function
A	IPv4 address	IPv4 address lookup using hostname.
AAAA	IPv6 address	IPv6 address lookup using hostname.
MX	Mail exchange	Maps domain name to a mail transfer host(s).
NS	Name server	Maps a DNS zone to an authoritative name server.
CNAME	Canonical name	Alias to another domain name record.
PTR	Pointer to canonical	Typically used for reverse lookups (IP to hostname)

Setup - dig

On Ubuntu:

```
$ sudo apt install dnsutils
```

On Centos:

```
$ sudo dnf install bind-utils
```

On Arch:

```
$ sudo pacman -Sy dnsutils
```

Fun with dig - Simple lookup

```
$ dig vicpimakers.ca AAAA
...
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55405
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
vicpimakers.ca.     14400   IN      AAAA    2607:7b00:3000:4::597e:ebad
```

More fun with dig

```
$ dig www.vicpimakers.ca AAAA
...
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24996
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
www.vicpimakers.ca.     14400   IN      CNAME   vicpimakers.ca.
vicpimakers.ca.         14400   IN      AAAA    2607:7b00:3000:4::597e:ebad
```

DNS configs - /etc/nsswitch.conf

- Configuration file that orders the name resolution data sources.
- For name resolution, we typically see:

```
$ grep hosts /etc/nsswitch.conf
hosts:      files dns
```

  - List order is relevant.
  - In this example, lookup start with **`/etc/hosts`** then reaches out to DNS.
  - Allow you to override DNS with your local configuration.
- To trace nsswitch.conf, use the following:

```
$ getent ahosts mydummyhost
```

- Host also uses **`/etc/nsswitch.conf`** for other services.
  - e.g. passwd, shadow, group entries

DNS configs - /etc/resolv.conf

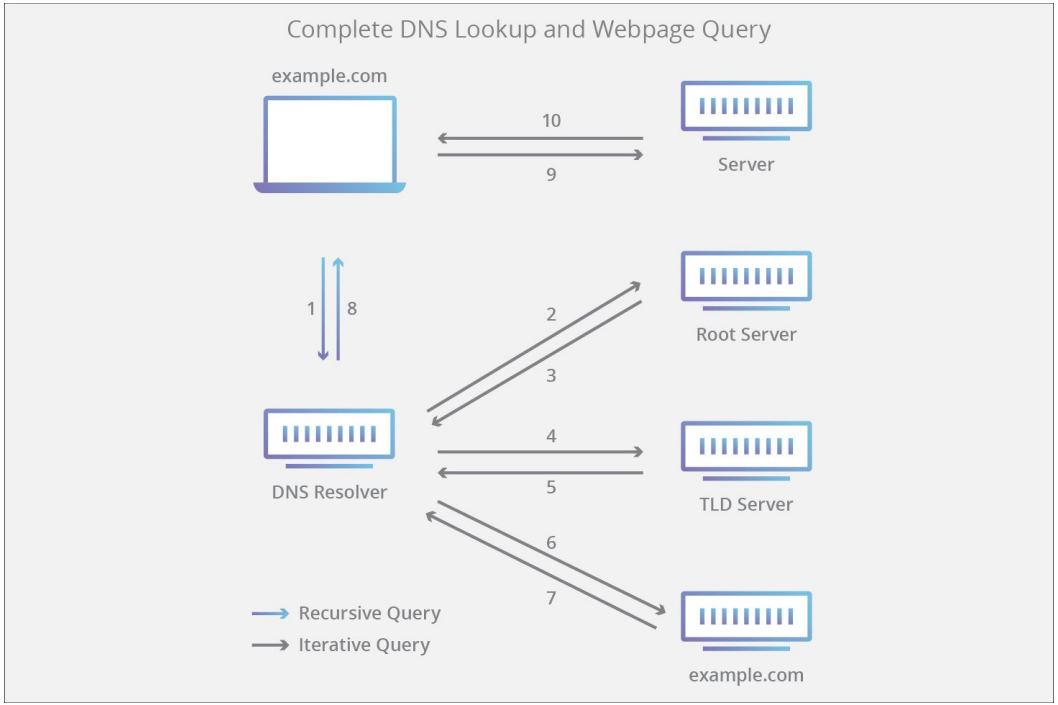
- DNS configuration for a linux host.

```
$ cat /etc/resolv.conf
nameserver 1.1.1.1
nameserver 8.8.8.8
nameserver 208.67.222.222
```

- Can be configured by DHCP (IPv4 / IPv6) or RAs (IPv6 only).
- Manual entry is also possible.
- More to come in Craig's presentation.

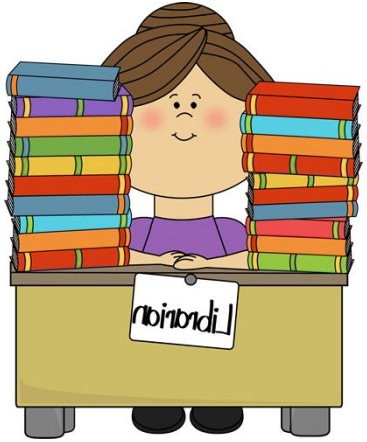
The Name Resolution Process

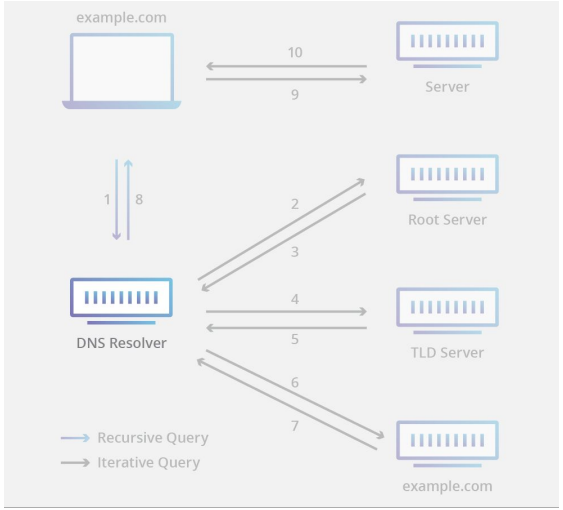
- https://www.cloudflare.com/learning/dns/what-is-dns/



Recursive Name Servers (Resolver)

- The first stop in most DNS client requests.
- If possible, response with cached records.
- If not, it goes on a recursive journey for the record.
  - Queries other DNS servers to on behalf of the client.
- Recursors typically in ISPs, enterprises, or public DNS.
  - Public (open) resolvers will respond any source.
  - e.g. cloudflare @ 1.1.1.1 or google @ 8.8.8.8
- Most recursive servers also cache DNS records
  - These records are valid for the length of the TTL.





Fun with dig - TTL

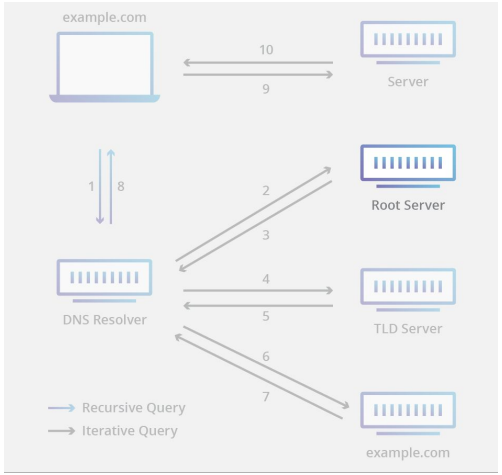
```
$ watch 'dig vicpimakers.ca A | grep -A 1 "ANSWER SECTION"'
;; ANSWER SECTION:
vicpimakers.ca.         14308   IN      A       23.111.74.233
```

What is TTL?

- TTL = Time to Live.
- TTL is set in seconds.
- Mechanism that limits the lifespan of a cached record in the Domain Naming System.
- Set by an authoritative DNS server for particular resource record.
- Used by recursive DNS servers to time out cached records.

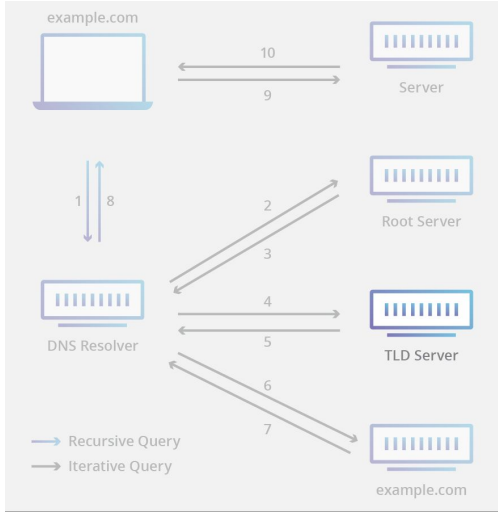
Root Name Servers

- DNS is structured in a hierarchy.
- Root name servers are at the top of this hierarchy.
  - There are 13 IP addresses for these root name servers.
  - Using anycast IPs, so actually hosted on many servers.
- Each recursive server knows the 13 IPs for root.
  - When a DNS lookup is initiated, the first recursive communication is with one of these 13 IP addresses.
- The root name servers refer recursive requests to the appropriate TLD (top-level domain) servers.
  - e.g. the root name servers tell us a vicpimakers.ca request will continue its search in the *.ca-servers.ca TLD name servers.
- https://root-servers.org/



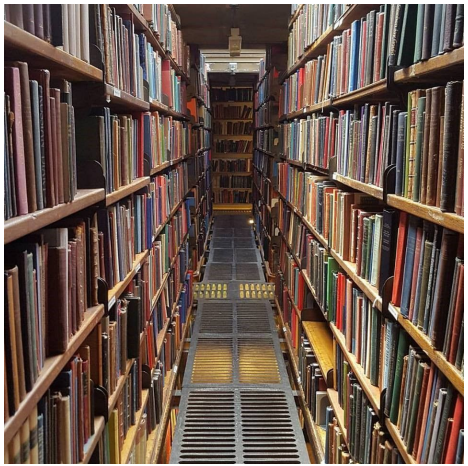
TLD Name Servers

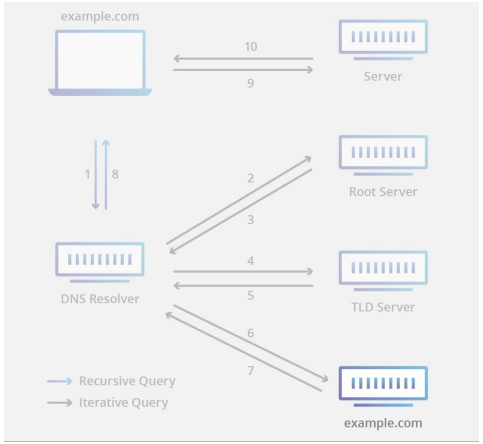
- TLD = Top-Level Domain
- The TLD name servers refer recursive requests to the appropriate authoritative name servers.
  - e.g. The *.ca-servers.ca TLD servers respond with ns1.cozyhost.space and ns2.cozyhost.space as the authoritative name servers for vicpimakers.ca.
- TLD is the highest level of names the DNS hierarchy.
  - E.g. vicpimakers.**CA** is the CA TLD.
- There are many groupings for TLD name servers.
  - Original generic TLDs = .COM, .EDU, .NET, .ORG, etc.
  - Country code TLDs = .CA, .US, .UK, etc.
  - New generic top-level domains = .BEER, .FYI, .WTF, etc.
    - Only $200K USD



Authoritative Name Servers

- Typically the final name server in the recursive query.
- If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS recursor (the librarian) that made the initial request.
    - e.g. The ns1.cozyhost.space name server responds with the vicpimakers.ca A record at 23.111.74.233.





Fun with dig - Find the authoritative NS

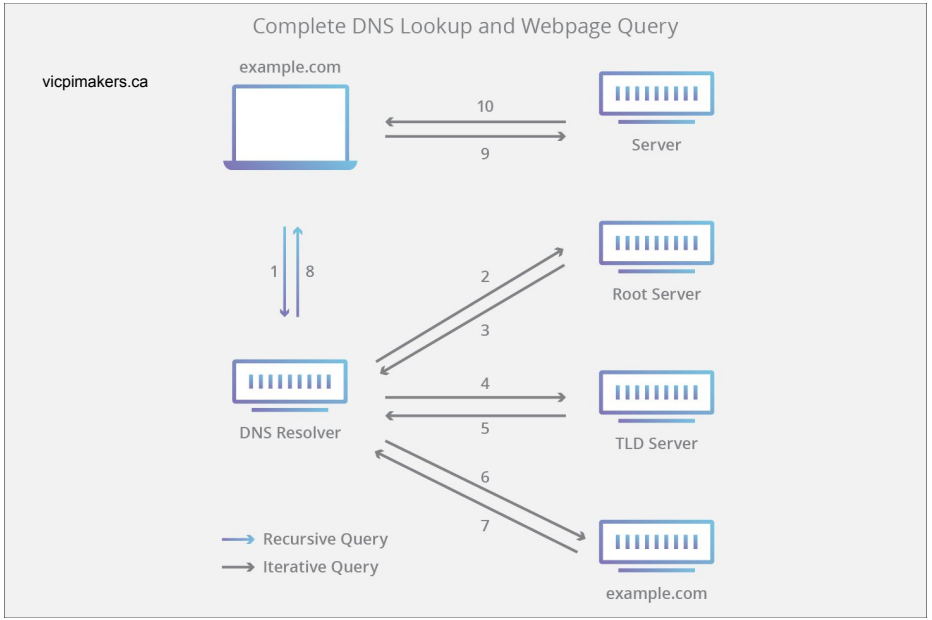
```
$ dig vicpimakers.ca NS
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59433
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
vicpimakers.ca.         86400   IN      NS      ns3.cozyhost.space.
vicpimakers.ca.         86400   IN      NS      ns2.cozyhost.space.
vicpimakers.ca.         86400   IN      NS      ns1.cozyhost.space.
vicpimakers.ca.         86400   IN      NS      ns4.cozyhost.space.
```

Fun with dig - Query the authoritative NS

```
$ dig @ns1.cozyhost.space vicpimakers.ca A
...
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54672
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9
;; WARNING: recursion requested but not available
...
;; ANSWER SECTION:
vicpimakers.ca.      14400   IN   A   23.111.74.233
```

Fun with dig - trace

```
$ dig +trace vicpimakers.ca A
```



To Be Continued ...

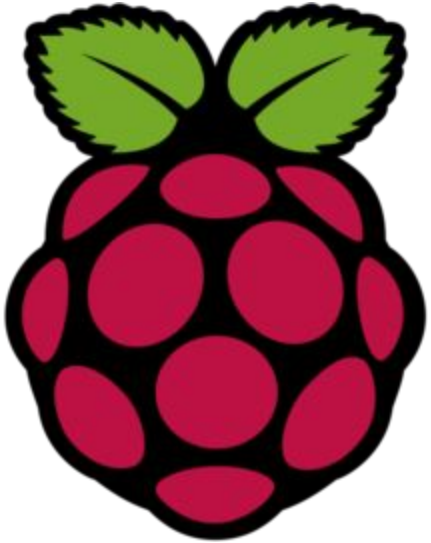
- More fun with DNS in July NetSIG
- Craig will present on:
  - How does a host get it DNS configuration?
  - The DNS search list.
  - Captive portals - Redirecting DNS requests.
  - DNS over HTTP
  - DNS for SOHO
  - And much more!

Possible Future Discussions

- Vulnerability scanning / Pen-testing
  - e.g. Metasploit, OpenVAS, etc.
- Intrusion Detection
  - e.g. Snort, etc.
- Network monitoring
  - e.g. Prometheus, Elastic Stack, Nagios, Cactus, etc.
- Honey Pots
- IPv6 with containers - k8s w/ calico ?
- Other ideas welcome!

VicPiMakers and Others Slack

- Please let us know if you want an invite to this Slack group



Backup Slides