Networking

DNS

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Domain Name System (DNS)

- Translates domain names to IP addresses
  - User can remember “google.com” instead of “142.250.72.206”

1. User types www.google.com

2. The system asks a DNS server for the IP address of www.google.com

3. The DNS server looks up the IP address for www.google.com

4. The server responds with the corresponding IP address

The Root Servers

- The root servers control the DNS data
  - They are located around the planet
  - ICANN is the authority that sets the bylaws for the organizations who control the root servers

You can find the specific root server locations here: https://root-servers.org/

Letter	Organization	Number of Sites (As of March 2022)
A	Verisign	16
B	University of Southern California (ISI)	6
C	Cogent Communications	12
D	University of Maryland	175
E	NASA	254
F	Internet Systems Consortium	302
G	Defense Information Systems Agency	6
H	US Army	12
I	Netnod	68
J	Verisign	118
K	RIPE NCC	82
L	ICANN	197
M	WIDE Project	8

DNS Records

- DNS Record – Types of data stored on a DNS server

- **Address (A vs AAAA)**
  - A is the IPv4 Address
  - AAAA is the IPv6 Address

```
┌──(kali@10.1.17.234)-[~]
└─$ nslookup -query=A cyber.org
Server:         10.3.0.2
Address:        10.3.0.2#53

Non-authoritative answer:
Name:   cyber.org
Address: 23.185.0.2
```

CYBER.ORG's A record

```
┌──(kali@10.1.17.234)-[~]
└─$ nslookup -query=AAAA cyber.org
Server:         10.3.0.2
Address:        10.3.0.2#53

Non-authoritative answer:
Name:   cyber.org
Address: 2620:12a:8000::2
Name:   cyber.org
Address: 2620:12a:8001::2
```

CYBER.ORG's AAAA record

DNS Records

- **MX** – How emails should be routed for the domain

```
┌──(kali@10.1.17.234)-[~]
└─$ nslookup -query=MX cyber.org
Server:         10.3.0.2
Address:        10.3.0.2#53

Non-authoritative answer:
cyber.org       mail exchanger = 0 cyber-org.mail.protection.outlook.com.
```

CYBER.ORG's MX record

- **SOA** – Provides information about the administrator of the domain

```
┌──(kali@10.1.17.234)-[~]
└─$ nslookup -query=SOA cyber.org
Server:         10.3.0.2
Address:        10.3.0.2#53

Non-authoritative answer:
cyber.org
        origin = ns15.domaincontrol.com
        mail addr = dns.jomax.net
        serial = 2022021501
        refresh = 28800
        retry = 7200
        expire = 604800
        minimum = 600
```

Notice: dns.jomax.net is what GoDaddy uses for their administrator email. GoDaddy is who controls the CYBER.ORG domain

CYBER.ORG's SOA record

DNS Records

- **TXT** – Notes for administrators, helps prevent spam for the domain

```
┌──(kali@10.1.17.234)-[~]
└─$ nslookup -query=TXT cyber.org
Server:         10.3.0.2
Address:        10.3.0.2#53

Non-authoritative answer:
cyber.org       text = "v=spf1 ip4:66.76.161.60 include:spf.protection.outlook.com -all"
cyber.org       text = "google-site-verification=TY__YSRdbvoIzq8AQezKJPxB79tV-qykxSue5hDL5_E"
```

CYBER.ORG's TXT record

- **NS** – The name server that contains the actual DNS information

```
┌──(kali@10.1.17.234)-[~]
└─$ nslookup -query=NS cyber.org
Server:         10.3.0.2
Address:        10.3.0.2#53

Non-authoritative answer:
cyber.org       nameserver = ns16.domaincontrol.com.
cyber.org       nameserver = ns15.domaincontrol.com.
```

Notice: CYBER.ORG's DNs records are located on two different DNS servers

CYBER.ORG's NS record

DNS Records

- CNAME – When a domain name is an alias for another domain name
  - For example, if you go to www.nicerc.org, you will be redirected to www.cyber.org
- PTR – This returns the domain name
  - It is used when someone does a reverse lookup, or they search with the IP address, instead of a domain name
- SRV – Designates the IP address and specific port numbers
  - In case the server needs to be serviced

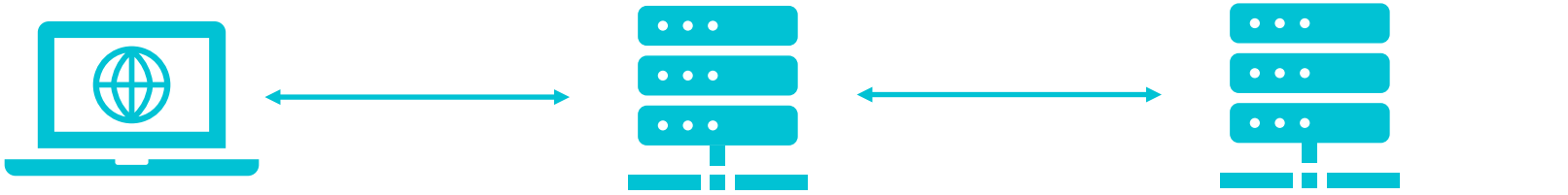
How DNS Actually Works

1. User types a URL
2. A query is created by that system
   - The query's job is to find the IP address associated with the domain
3. The first place checked is cache on the system
   - DNS Cache is stored DNS information from previous visits

1. User types URL
2. Systems creates Query
3. System checks DNS cache

How DNS Actually Works

4. Query checks the Internet service provider's lists
   - Most popular way to locate IP address
   - Known as an iterative or recursive lookup
5. Next place to check is the authoritative/root servers
   - Start with the top-level domains and work their way down



1. User types URL
2. Systems creates Query
3. System checks DNS cache

4. Query checks ISP lists

5. Query checks the root servers
6. The root servers start at the top and work their way to the specific server
7. The query is returned to the user's system

DNS Terms

- **Time to Live (TTL)** – When the recursive lists recheck the domain records for a specific domain

- **Internal vs. External** – Internal domains are only valid within a local network while external domains are all the domains connected to the WAN

- **Zone Transfers** – Server will download an entire DNS from a DNS server
  - Helps create backups and the recursive lists

DNS Terms

- **Reverse DNS/Reverse Lookup** – A query that sends an IP address to find the domain name associated with the IP address

- **Forward Lookup** – A query that sends the domain name to find the IP address associated with that domain name