DNS Lab

James

Brief Intro

What is DNS?

Domain Name Service - Translates between domain name and IP

For example :

csie.ntu.edu.tw -> 140.112.30.28

google.com -> 172.217.160.78

DNS hierarchy

- Distributed storage

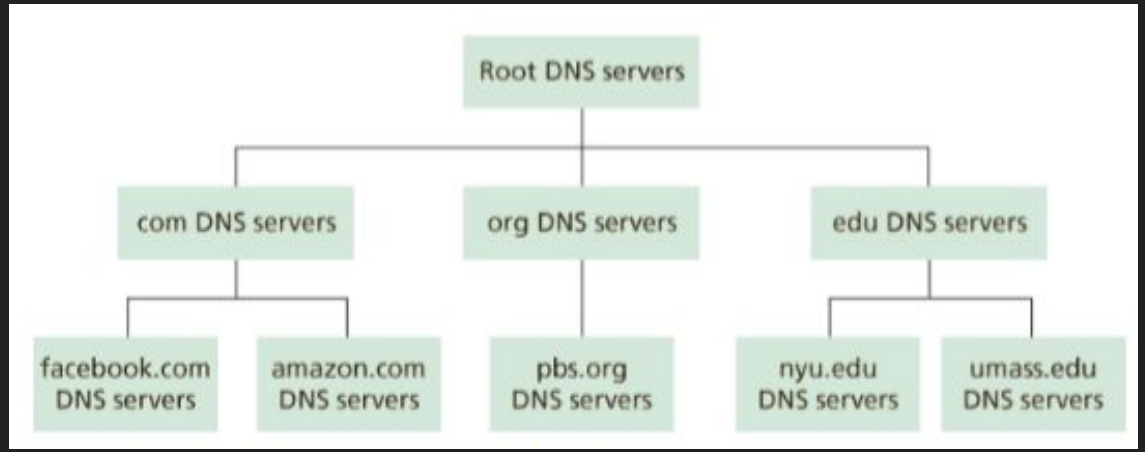

Image from Computer-Networking-A-Top-Down-Approach-7th-Edition textbook

How DNS works

- Authoritative servers

  Stores records of owned domain

  Can be found in hierarchy from previous page

- Recursive servers

  Servers that ‘serve’ DNS queries from users

  Will not be found in the DNS hierarchy

Recursive Querying

- Caching Possible

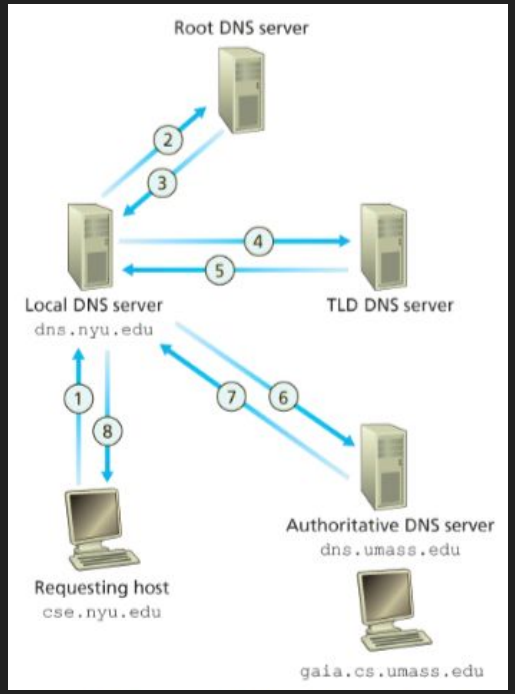

Image from Computer-Networking-A-Top-Down-Approach-7th-Edition textbook

Lab

Set up your own authoritative DNS

Resource Records

Information about DNS are stored in zone files as resource records

Common fields are shown in table below

A	ipv4 address
CNAME	canonical name
NS	name server
MX	mail server
PTR	reverse ip
TXT	text record
AAAA	ipv6 address

Zone File

Zone File = SOA(start of authority) record + other records

Typical SOA record :

```
;@ domain_zone, Internet, SOA, responsive server, admin mail
@ csie.ntu.edu.tw. IN SOA dns.csie.ntu.edu.tw. ta221.csie.ntu.edu.tw.  (
                                1999051401      ; Serial
                                3600            ; Refresh
                                300             ; Retry
                                3600000         ; Expire
                                3600 )          ; Minimum
```

Zone File

Typical resource records:

```
www         IN    A          192.168.0.10  ;www is without period, so it expands to www.csie.ntu.edu.tw
@           IN    AAAA ::1                 ;"@" means this zone(indicated in SOA)
            IN    NS         csman2        ;but "@" can be omitted sometimes
www1 IN     CNAME      www
@           IN    MX    1    mx1.csie.ntu.edu.tw.        ; 1 is TTL that overides the original expire time
            IN    PTR   im.the.one.         ;putting PTR records in a different zone file is recommended
@           IN    TXT   "v=spf1 mx a:example.mx -all"
```

Configuration Files

named.conf: For including other conf files. Try not to add anything here.

named.conf.options: bind9 options and global options, like version, forwarders, rate-limit, allow-query-cache, allow-recursion, etc.

named.conf.local: Include zone files along with local (to zone) options here.

Requirements

1. Create a zone [id].com
2. Map multiple IPs to your zone [id].com
3. Map “alias.[id].com” to “[id].com”
4. Secure your server such that only list of allowed IPs can use it as DNS resolver
5. Set your zone such that anyone can query for it

Bonus : set up query logs

Environment setup

1. Download centos VM
2. Install bind9

   yum install bind

   yum install bind-utils #for checkconf/checkzone commands

Add zone

1. In /etc/named.conf, add the following

   ```
   zone “[id].com”
   {
   type master;
   file “/var/named/named.[id]”;
   };
   ```

2. Create zone file named.[id] in /var/named/ and modify records to meet requirements 1,2,3

Limited access

1. Look up “allow-recursion” option and try to modify it to meet requirement 4
2. Look up “allow-query” option and try to modify it to meet requirement 5

Useful Commands

named-checkconf /etc/named.conf
named-checkzone -i local [domain] /var/named/[zone_file]
systemctl start named
dig [ip] @[authorative_server_ip]