CS 447/647

DNS & DHCP

DHCP Overview

What is DHCP?

How does DHCP work?

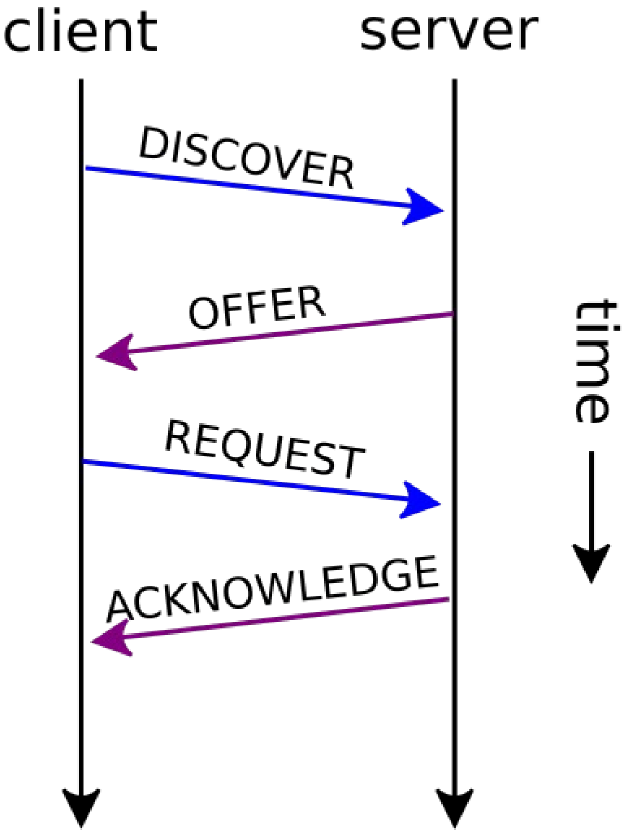
What are some common DHCP problems?

What is DHCP

- Dynamic Host Configuration Protocol (RFC 2131)
- Automatically assigns IP addresses to devices on a network
- Saves time that would be spent manually assigning IP addresses
- Prevents typos that cause network problems

DHCP Session

- Client broadcasts DHCPDISCOVER message
- DHCP server responds with a DHCPOFFER message containing an available IP address and network settings
- Client sends a DHCPREQUEST to accept the DHCP offer
- DHCP server confirms with a DHCPACK



DHCP Key Components

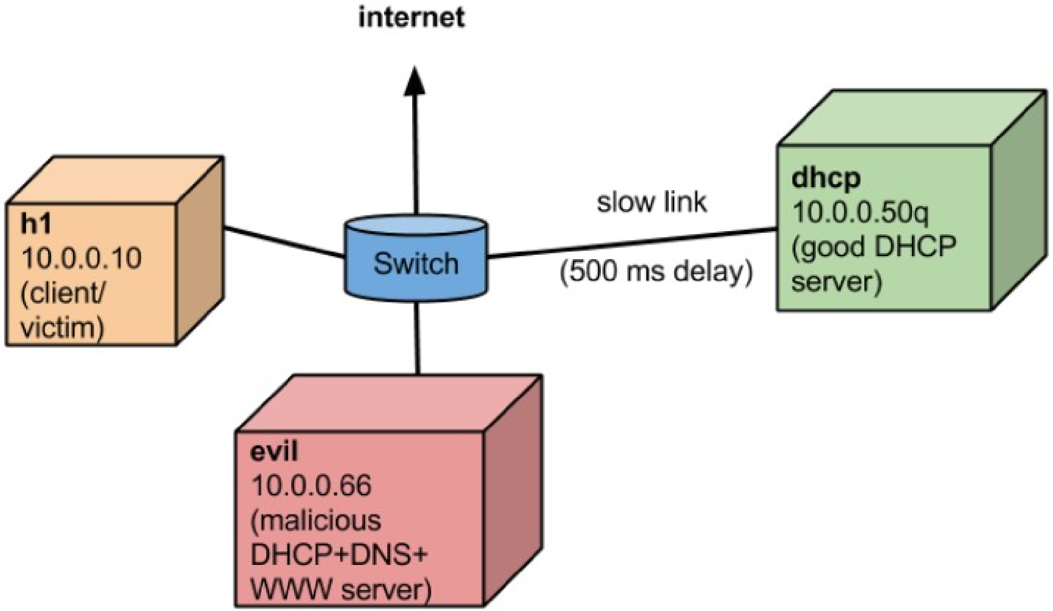
- DHCP Server
  - Assigns IP addresses
  - Manages network configurations
- DHCP Client
  - Requests and receives IP configuration from the DHCP server
- DHCP Relay Agent
  - Forwards DHCP messages across networks

Configuring a DHCP Server

- Defining IP Address Pools
  - Specify IP ranges available for dynamic assignment
  - Example: 192.168.0.100-192.168.0.199
- Setting lease durations
  - Default lease time
  - Max lease time
- Static IP reservations
  - Critical devices can have a static IP reservation
- Default route
- DNS domain
- Name servers

DHCP Security

- Rogue DHCP servers
  - Malicious DHCP server intercepts DHCP requests
- DHCP starvation attacks
  - Client spams DHCP requests with spoofed MAC addresses to exhaust all available IP addresses
- DHCP snooping
  - Security feature on network switches that blocks unauthorized DHCP servers



DNS Overview

What is DNS?

How is DNS managed?

What are some common DNS resource records?

What is the SOA record?

What command line tools help you query DNS?

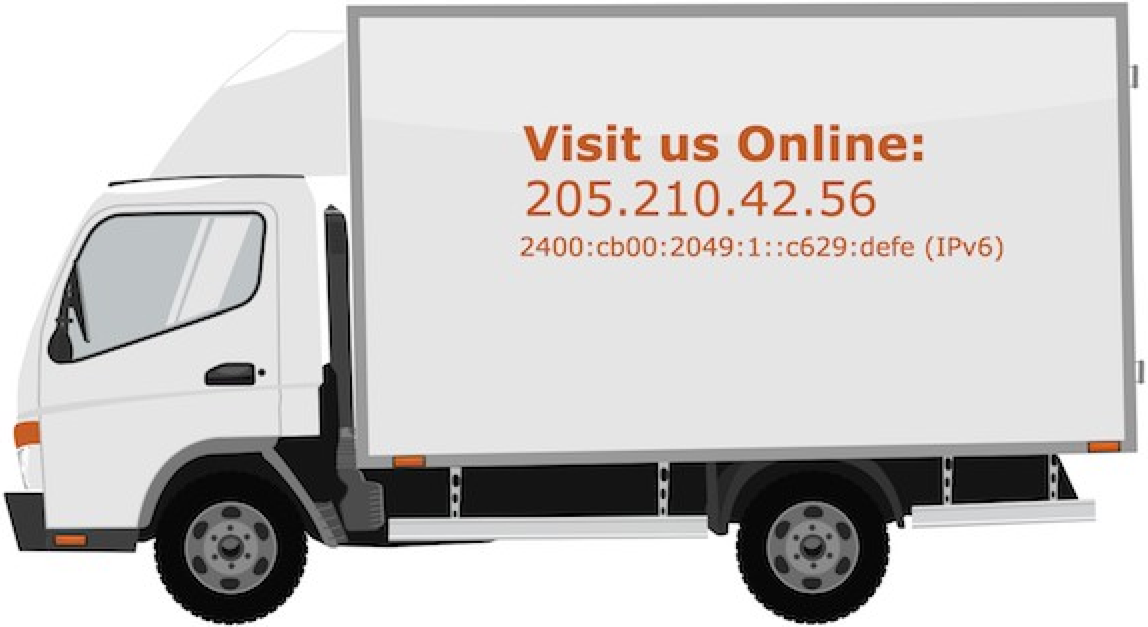
How to setup and manage dnsmasq and bind.

Domain Name System

- Maps a hostname to an IP
  - google.com -> 172.217.6.46
- Essential for the global Internet
- Used for:
  - Mail
  - Service Discovery
  - Authentication
  - SSL
  - WWW

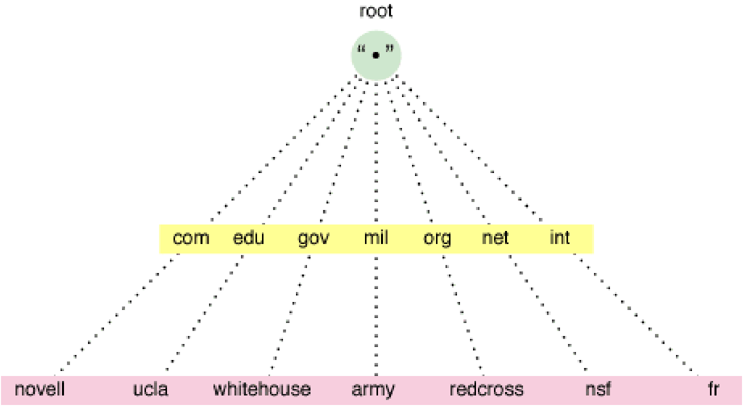
THE RUMORS ARE TRUE. GOOGLE WILL BE SHUTTING DOWN PLUS—
ALONG WITH HANGOUTS, PHOTOS, VOICE, DOCS, DRIVE, MAPS, GMAIL, CHROME, ANDROID, AND SEARCH—
TO FOCUS ON OUR CORE PROJECT:
THE 8.8.8.8 DNS SERVER.
Google

https://xkcd.com/1361/


Visit us Online:
205.210.42.56
2400:cb00:2049:1::c629:defe (IPv6)

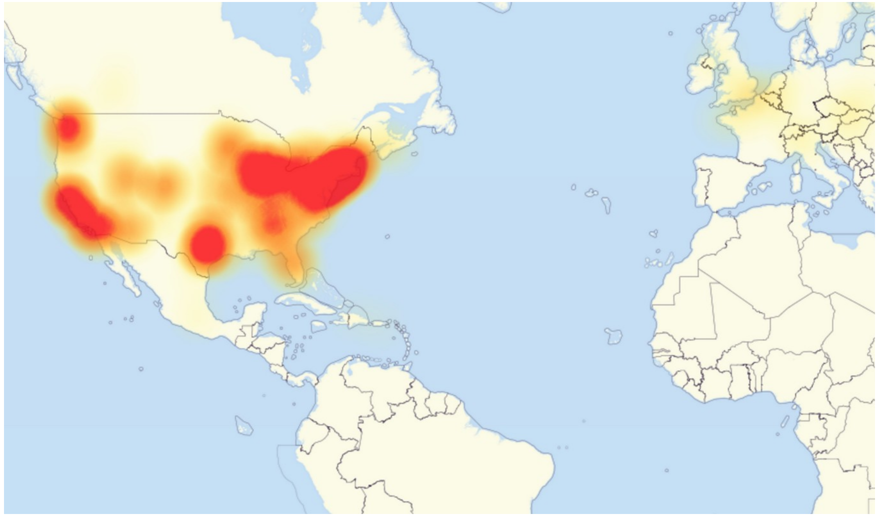
DNS Architecture

- Distributed Database
  - . is managed by a group of nonprofits and companies
    - ICANN operates one
    - *US Army*
    - *US DoD*
    - *NASA*
    - Verisign
    - 10/13 are in the US
- Each site maintains its own database
  - Company
  - University
  - Individual (zachest.com)
- Globally administered
  - IP network portion
  - Domain
- Local administrators must prevent duplicates



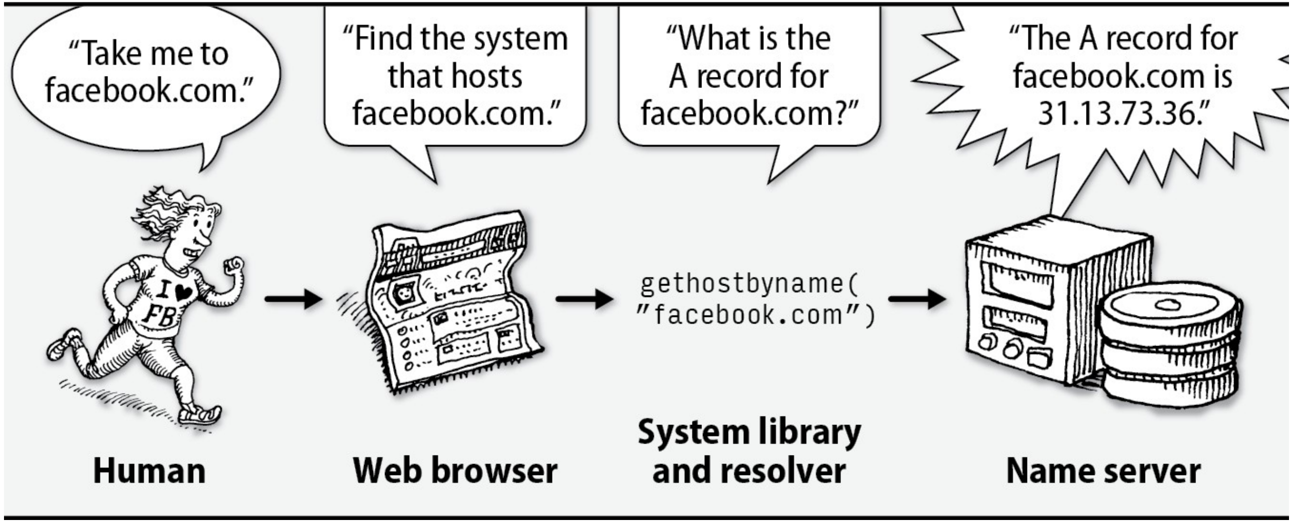
DNS Architecture

- DNS disappears, the Internet vanishes
- Mirai 2016 Distributed Denial of Service attack
  - DynDNS
  - Spotify, Twitter, Github, PayPal



DNS Architecture

- Query, two parts
  - Name: google.com
  - Record type: A
- Response
  - Resource Records



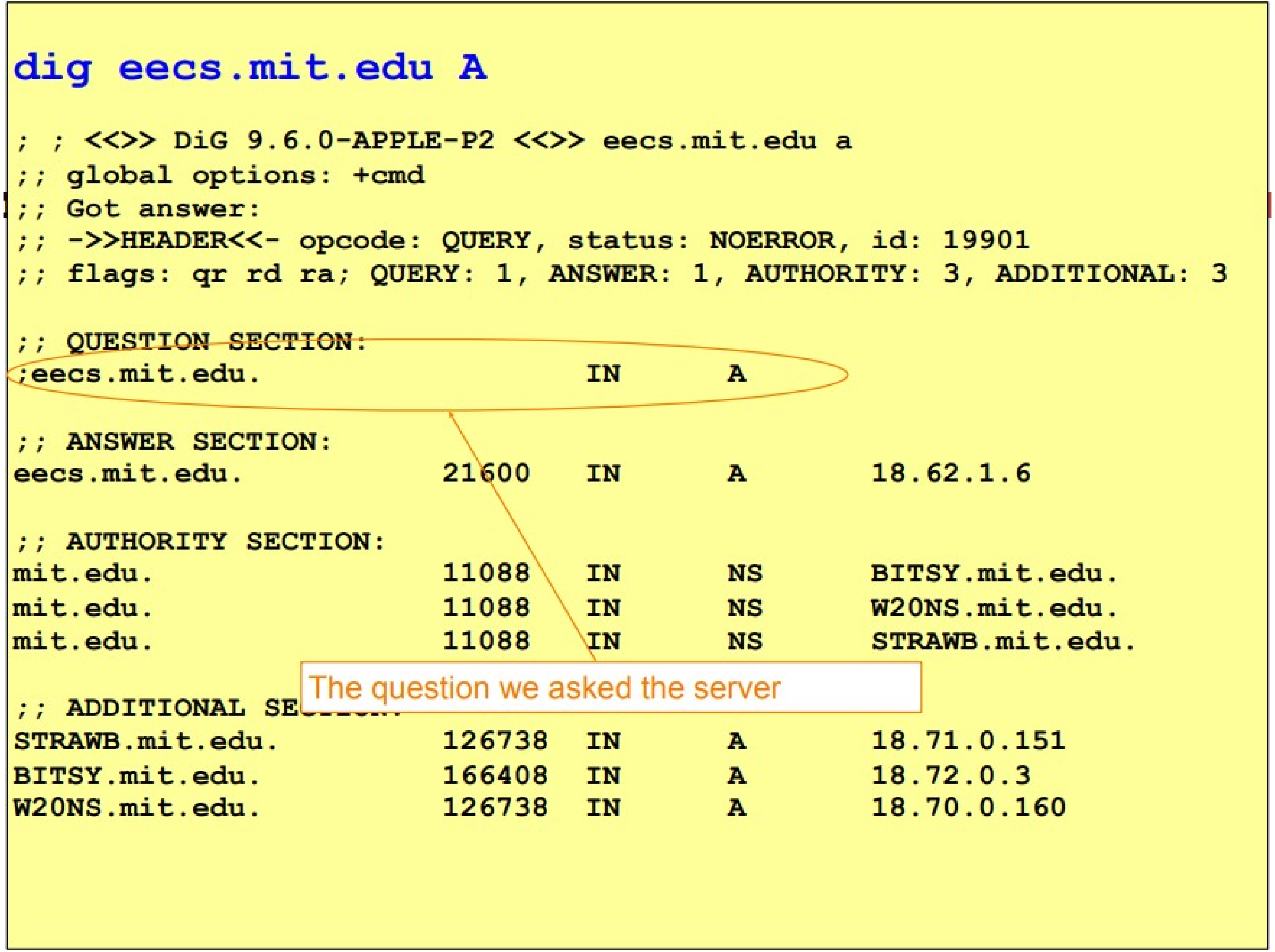
"Take me to facebook.com."
"Find the system that hosts facebook.com."
"What is the A record for facebook.com?"
"The A record for facebook.com is 31.13.73.36."
I ♥ FB
gethostbyname("facebook.com")
Human
Web browser
System library and resolver
Name server

```
dig eecs.mit.edu A
```

Use Unix “dig” utility to look up IP address (“A”) for hostname eecs.mit.edu via DNS

```
; ; <<>> DiG 9.6.0-APPLE-P2 <<>> eecs.mit.edu a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19901
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;eecs.mit.edu.                  IN      A

;; ANSWER SECTION:
eecs.mit.edu.           21600   IN      A       18.62.1.6

;; AUTHORITY SECTION:
mit.edu.                11088   IN      NS      BITSY.mit.edu.
mit.edu.                11088   IN      NS      W20NS.mit.edu.
mit.edu.                11088   IN      NS      STRAWB.mit.edu.

;; ADDITIONAL SECTION:
STRAWB.mit.edu.         126738  IN      A       18.71.0.151
BITSY.mit.edu.          166408  IN      A       18.72.0.3
W20NS.mit.edu.          126738  IN      A       18.70.0.160
```

dig eecs.mit.edu A



```
; ; <<>> DiG 9.6.0-APPLE-P2 <<>> eecs.mit.edu a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19901
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;eecs.mit.edu.                  IN      A

;; ANSWER SECTION:
eecs.mit.edu.           21600   IN      A       18.62.1.6

;; AUTHORITY SECTION:
mit.edu.                11088   IN      NS      BITSY.mit.edu.
mit.edu.                11088   IN      NS      W20NS.mit.edu.
mit.edu.                11088   IN      NS      STRAWB.mit.edu.

;; ADDITIONAL SE
STRAWB.mit.edu.         126738  IN      A       18.71.0.151
BITSY.mit.edu.          166408  IN      A       18.72.0.3
W20NS.mit.edu.          126738  IN      A       18.70.0.160
```

The question we asked the server

dig eecs.mit.edu A

```
; ; <<>> DiG 9.6.0-APPLE-P2 <<>> eecs.mit.edu a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19901
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;eecs.mit.edu.                  IN      A

;; ANSWER SECTION:
eecs.mit.edu.           21600

;; AUTHORITY SECTION:
mit.edu.                11088   IN      NS      BITSY.mit.edu.
mit.edu.                11088   IN      NS      W20NS.mit.edu.
mit.edu.                11088   IN      NS      STRAWB.mit.edu.

;; ADDITIONAL SECTION:
STRAWB.mit.edu.         126738  IN      A       18.71.0.151
BITSY.mit.edu.          166408  IN      A       18.72.0.3
W20NS.mit.edu.          126738  IN      A       18.70.0.160
```

A 16-bit **transaction identifier** that enables the DNS client (dig, in this case) to match up the reply with its original request

dig eecs.mit.edu A

```
; ; <<>> DiG 9.6.0-APPLE-P2 <<>> eecs.mit.edu a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode:
;; flags: qr rd ra; QUE                                         ONAL: 3

;; QUESTION SECTION:
;eecs.mit.edu.                  IN      A

;; ANSWER SECTION:
eecs.mit.edu.           21600   IN      A       18.62.1.6

;; AUTHORITY SECTION:
mit.edu.                11088   IN      NS      BITSY.mit.edu.
mit.edu.                11088   IN      NS      W20NS.mit.edu.
mit.edu.                11088   IN      NS      STRAWB.mit.edu.

;; ADDITIONAL SECTION:
STRAWB.mit.edu.         126738  IN      A       18.71.0.151
BITSY.mit.edu.          166408  IN      A       18.72.0.3
W20NS.mit.edu.          126738  IN      A       18.70.0.160
```

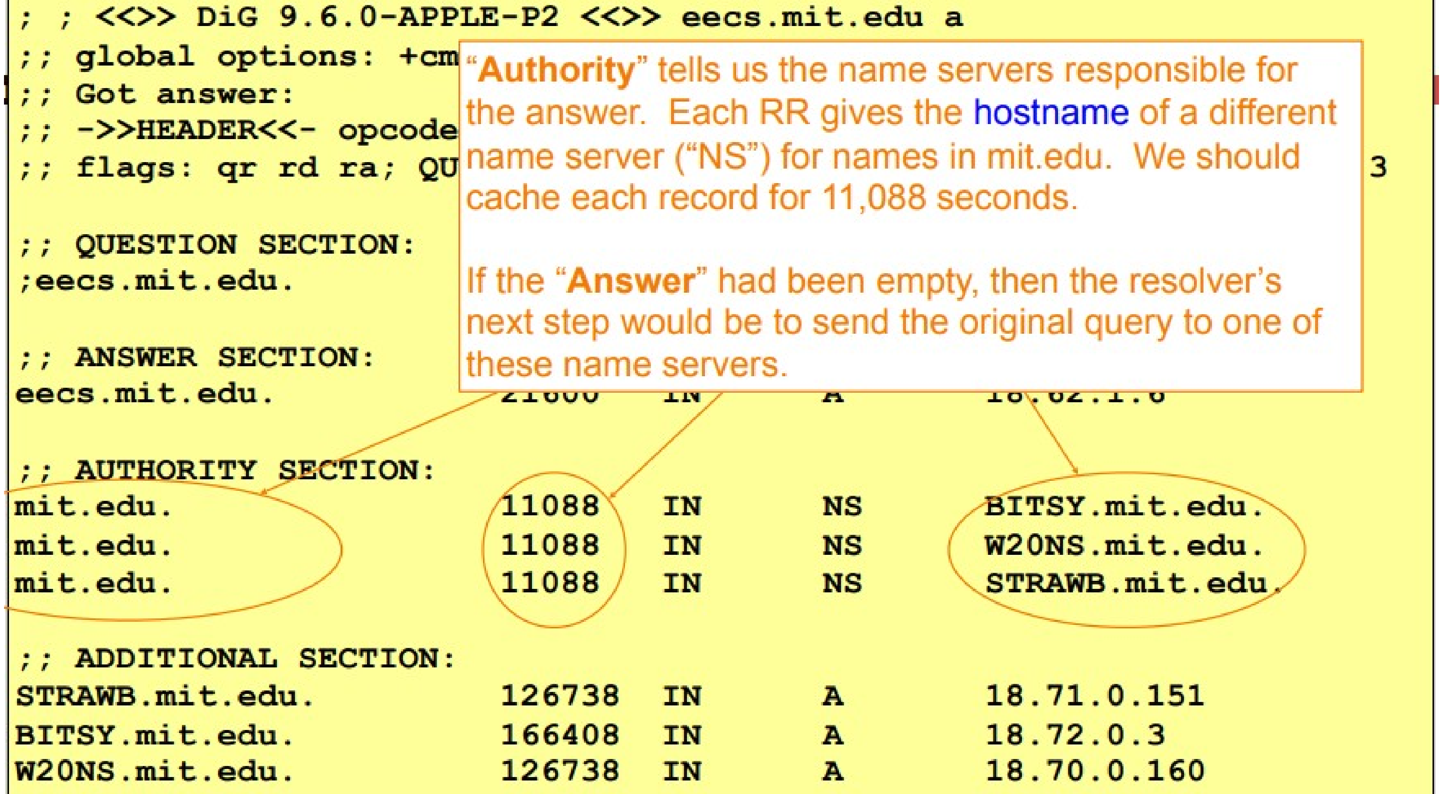
“**Answer**” tells us the IP address associated with eecs.mit.edu is 18.62.1.6 and we can cache the result for 21,600 seconds

dig eecs.mit.edu A

```
; ; <<>> DiG 9.6.0-APPLE-P2 <<>> eecs.mit.edu a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19901
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;eecs.mit.edu.                   IN      A

;; ANSWER SECTION:
eecs.mit.edu.            21600   IN      A       18.62.1.6

;; AUTHORITY SECTION:
mit.edu.                 11088   IN      NS      BITSY.mit.edu.
mit.edu.                                            du.
mit.edu.                                             edu.

;; ADDITIONAL SECTION
STRAWB.mit.edu.
BITSY.mit.edu.           166408  IN      A       18.72.0.3
W20NS.mit.edu.           126738  IN      A       18.70.0.160
```

In general, a single Resource Record (RR) like this includes, left-to-right, a DNS name, a time-to-live, a family (IN for our purposes - ignore), a type (A here), and an associated value

dig eecs.mit.edu A



```
; ; <<>> DiG 9.6.0-APPLE-P2 <<>> eecs.mit.edu a
;; global options: +cm
;; Got answer:
;; ->>HEADER<<- opcode
;; flags: qr rd ra; QU                                               3

;; QUESTION SECTION:
;eecs.mit.edu.

;; ANSWER SECTION:
eecs.mit.edu.            21600   IN     A       18.62.1.6

;; AUTHORITY SECTION:
mit.edu.                 11088   IN     NS      BITSY.mit.edu.
mit.edu.                 11088   IN     NS      W20NS.mit.edu.
mit.edu.                 11088   IN     NS      STRAWB.mit.edu.

;; ADDITIONAL SECTION:
STRAWB.mit.edu.          126738  IN     A       18.71.0.151
BITSY.mit.edu.           166408  IN     A       18.72.0.3
W20NS.mit.edu.           126738  IN     A       18.70.0.160
```

"**Authority**" tells us the name servers responsible for the answer. Each RR gives the hostname of a different name server ("NS") for names in mit.edu. We should cache each record for 11,088 seconds.

If the "**Answer**" had been empty, then the resolver's next step would be to send the original query to one of these name servers.

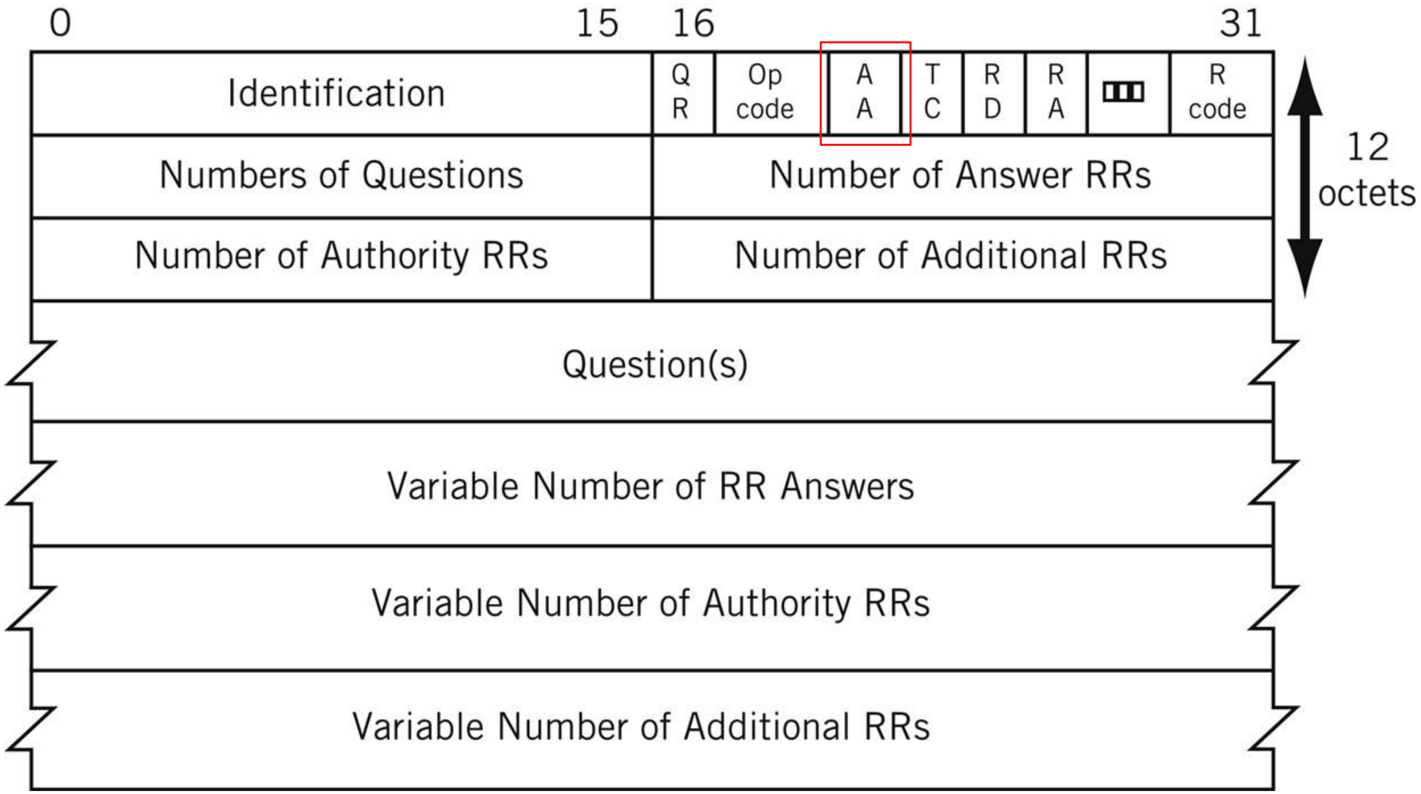
dig eecs.mit.edu A

```
; ; <<>> DiG 9.6.0-APPLE-P2 <<>> eecs.mit.edu a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19901
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;eecs.mit.edu.

;; ANSWER SECTION
eecs.mit.edu.

;; AUTHORITY SECT
mit.edu.                 11088    IN      NS      BITSY.mit.edu.
mit.edu.                 11088    IN      NS      W20NS.mit.edu.
mit.edu.                 11088    IN      NS      STRAWB.mit.edu.

;; ADDITIONAL SECTION:
STRAWB.mit.edu.          126738   IN      A       18.71.0.151
BITSY.mit.edu.           166408   IN      A       18.72.0.3
W20NS.mit.edu.           126738   IN      A       18.70.0.160
```

"**Additional**" provides extra information to save us from making separate lookups for it, or helps with bootstrapping.

Here, it tells us the IP addresses for the hostnames of the name servers. We add these to our cache.

DNS Request and Response (Same Format)



0 15 16 31

Identification | QR | Op code | AA | TC | RD | RA | ▯▯▯ | R code

Numbers of Questions | Number of Answer RRs

Number of Authority RRs | Number of Additional RRs

12 octets

Question(s)

Variable Number of RR Answers

Variable Number of Authority RRs

Variable Number of Additional RRs

DNS service providers

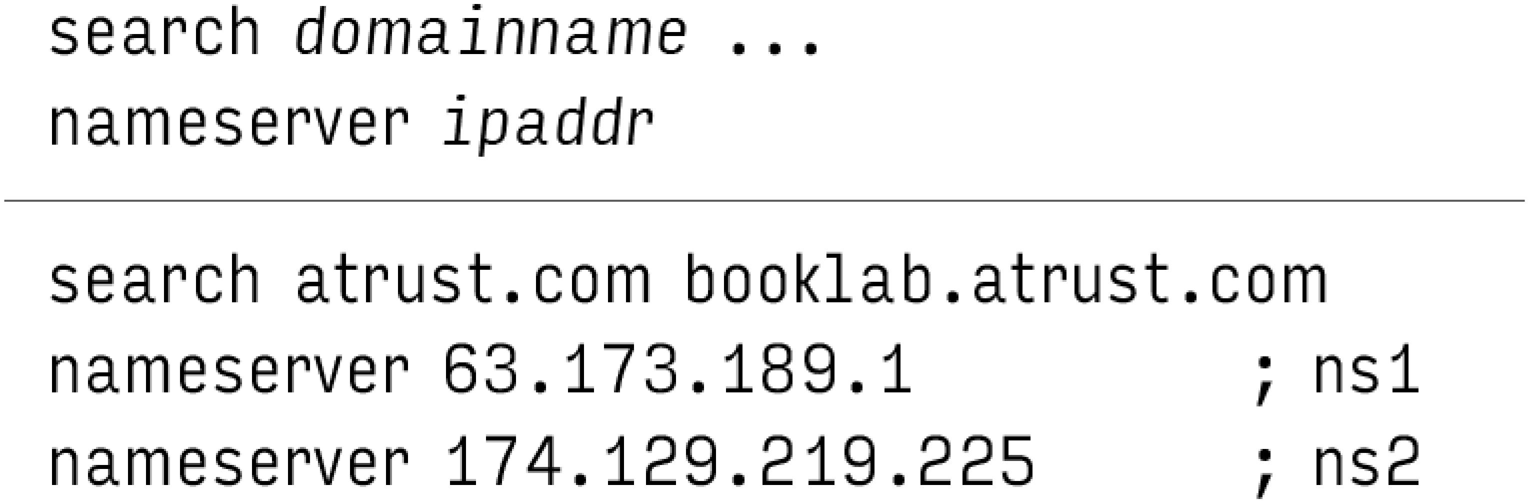
- DNS use to be a core sysadmin responsibility
- Products automate DNS
  - Microsoft Active Directory
  - Bluecat
  - Amazon Route 53
- Open Source DIY
  - BIND
  - Unbound
  - dnsmasq
- Still need to understand core concepts.
  - Troubleshooting

BIND

Berkeley Internet Domain Name

DNS for lookups

- Static
  - /etc/hosts
- Stub Resolver
  - /etc/resolv.conf

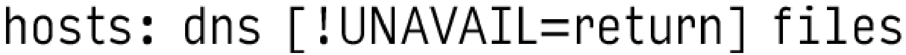


```
search domainname ...
nameserver ipaddr
```

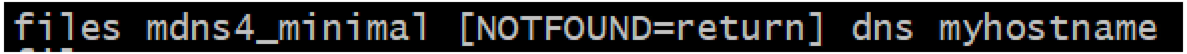
```
search atrust.com booklab.atrust.com
nameserver 63.173.189.1          ; ns1
nameserver 174.129.219.225       ; ns2
```

nsswitch

- Stored in /etc/nsswitch.conf
- Order of DNS services
  - Left to right



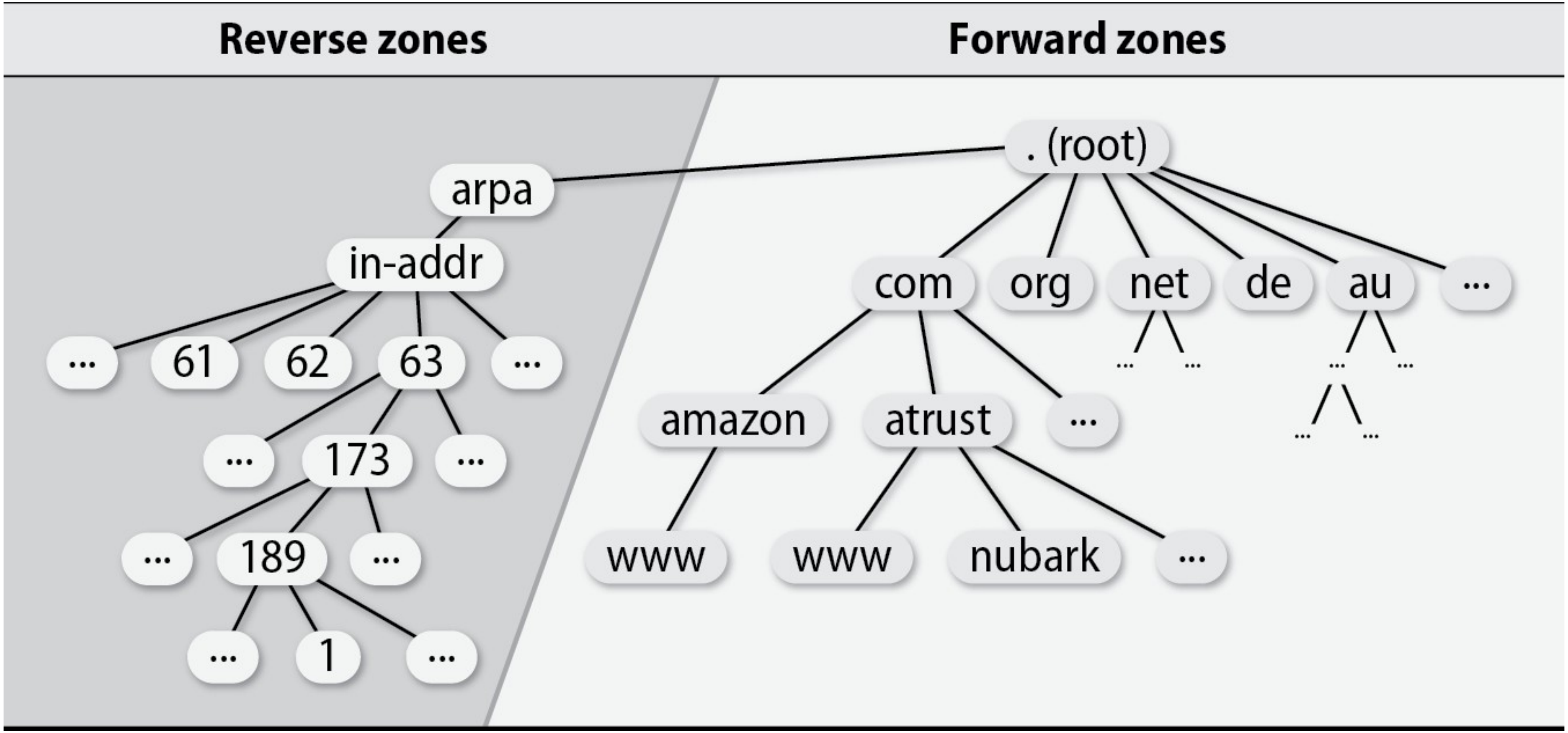
```
hosts: dns [!UNAVAIL=return] files
```



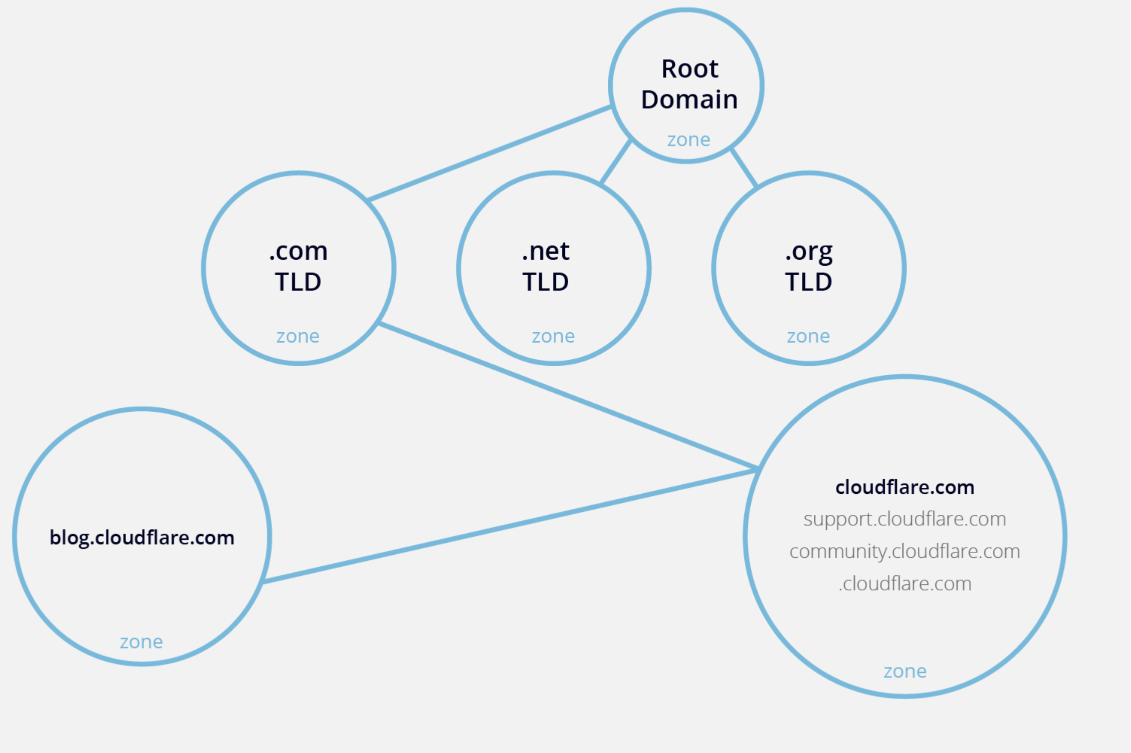
```
files mdns4_minimal [NOTFOUND=return] dns myhostname
```

The DNS namespace

- Maintains forward mappings
  - A Record
- Maintains reverse mappings
  - PTR Record - Pointer
  - Inverted IP address
  - 63.173.189.1
    - 1.189.173.63.in-addr.arpa.



http://www.internic.net/domain/root.zone - https://www.herenow.abbvie/



Root Domain

zone

.com TLD

zone

.net TLD

zone

.org TLD

zone

blog.cloudflare.com

zone

cloudflare.com

support.cloudflare.com

community.cloudflare.com

.cloudflare.com

zone

https://www.cloudflare.com/learning/dns/glossary/dns-zone/

The DNS namespace

- Two top-level domains
    - Country code domains
        - .us
        - .ru
        - .io
            - British Indian Ocean Territory
            - Uncertain of the future of .io
    - Generic top-level domains
        - .com
        - .org
        - .edu
        - .party
        - .dad
        - .lol
        - .ninja

ccTLDs Quiz

What Country owns these ccTLDs?

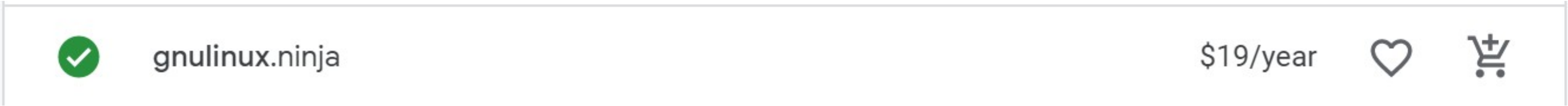
- .tv.
- .co.
- .ws.
- .ly.
- .re.

New TLDs

- .website
- .press
- .rocks
- .support
- .email
- .pics
- .lgbt
- .red
- .blue
- .wtf

The DNS namespace

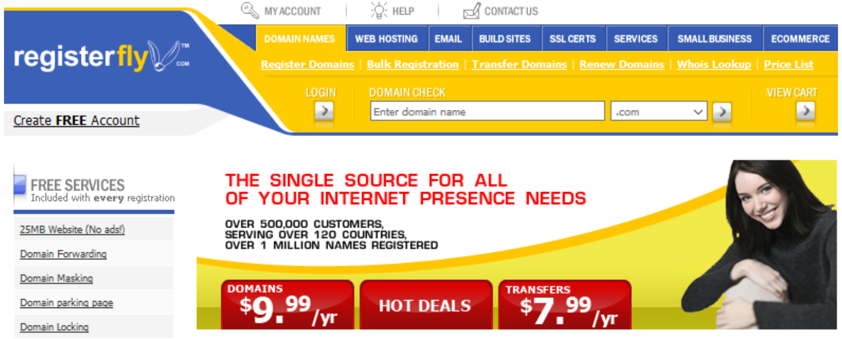
- Second level-domains
  - linux.ninja
- Apply at a top-level domain registrar
  - Costs money



gnulinux.ninja

$19/year

RegisterFly



THE SINGLE SOURCE FOR ALL OF YOUR INTERNET PRESENCE NEEDS

OVER 500,000 CUSTOMERS,
SERVING OVER 120 COUNTRIES,
OVER 1 MILLION NAMES REGISTERED

- Hosting and Domain Registrar
- Managed over 2,000,000 domains
- Split into RegisterFly.net and RegisterFly.com
  - Former business partners then estranged lovers
- Fraud, lawsuits, counter lawsuits, appeals, then total collapse
  - Liposuction and a $6,000 chihuahua
- Complete neglect of customers
- ICANN stripped the company of it’s registrar status

The DNS namespace

- Subdomains
  - .com = Top-level domain
  - bigcompany.com = Second-level domain
  - west.bigcompany.com = subdomain
- Two servers
  - Can work with one.

How DNS works

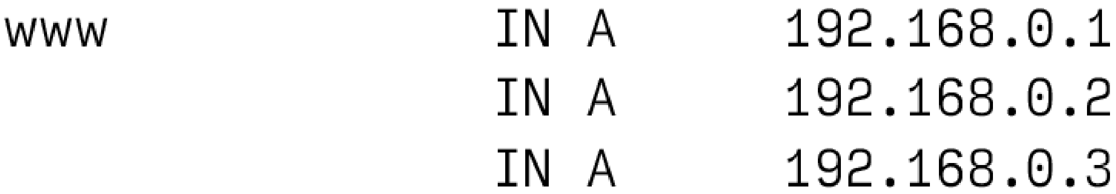
- Answers queries
  - hostnames and IP addresses
- Forwards requests
- Caches answers
- Synchronizes with other local servers

DNS Servers

- Authoritative
    - Responsible for a zone
        - IE: engr.unr.edu
    - Different Types
        - Primary (master) - Data is on disk
        - Secondary - Data is from master
        - Stub - Copy of zone with a subset of resource records
        - Distribution - Authoritative but not listed aka Stealth
        - Caching
        - Forwarding - Forwards requests, large cache
    - Recursive - Handles referrals
    - Nonrecursive - Sends referrals
        - `dig +recurse @8.8.8.8 www.google.hk`
        - `dig +norecurse @8.8.8.8 www.google.hk`

Resource Records

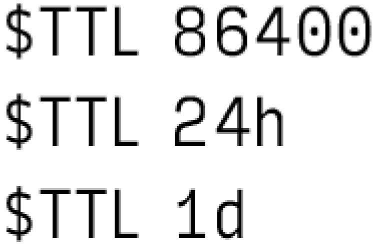
- Each server is responsible for its own zone
- Text files
- Record for each host
  - A - IPv4
  - AAAA - IPv6
- Load-balancing
  - round-robin



```
www                 IN A      192.168.0.1
                    IN A      192.168.0.2
                    IN A      192.168.0.3
```

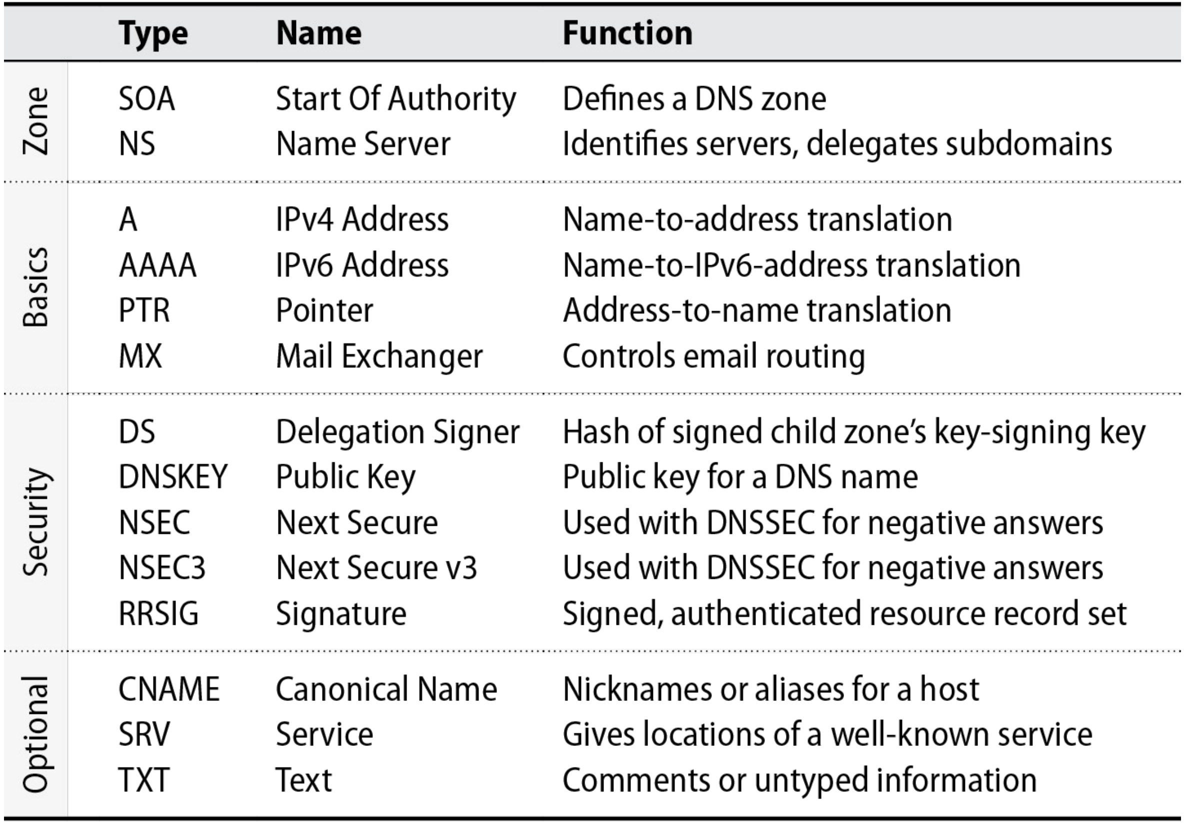
DNS Database

- Set of files
  - Zone Files
- $TTL - Time to live
  - Must be first line
- Resource Record
  - `[name] [ttl] [class] type data`
- Four Groups of Records
  - Zone Infrastructure Record
  - Basic Records
  - Security Records
  - Optional Records



```
$TTL 86400
$TTL 24h
$TTL 1d
```

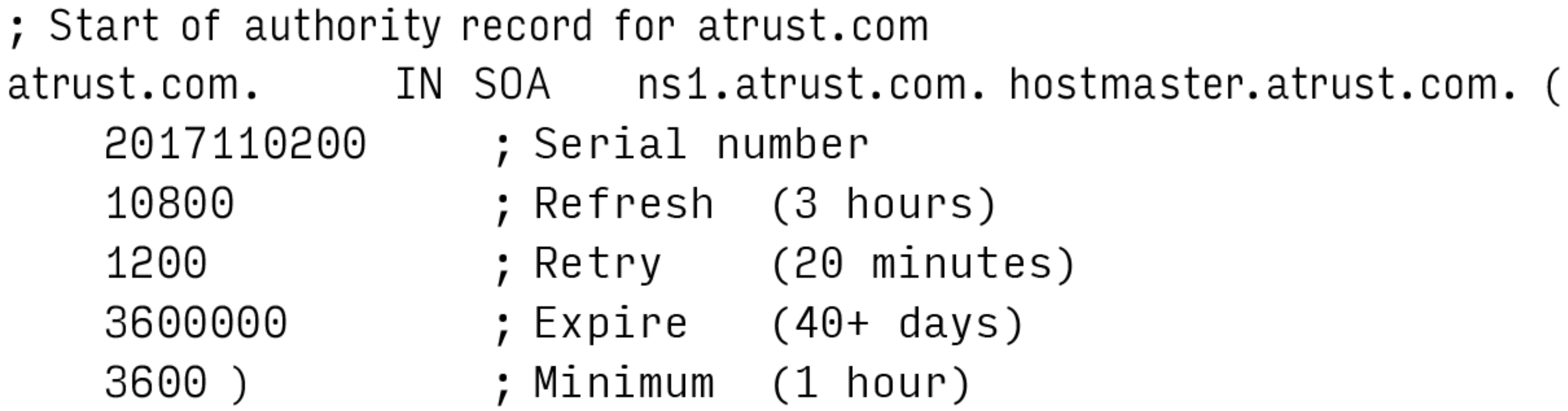
Record Types



	Type	Name	Function
Zone	SOA	Start Of Authority	Defines a DNS zone
	NS	Name Server	Identifies servers, delegates subdomains
Basics	A	IPv4 Address	Name-to-address translation
	AAAA	IPv6 Address	Name-to-IPv6-address translation
	PTR	Pointer	Address-to-name translation
	MX	Mail Exchanger	Controls email routing
Security	DS	Delegation Signer	Hash of signed child zone's key-signing key
	DNSKEY	Public Key	Public key for a DNS name
	NSEC	Next Secure	Used with DNSSEC for negative answers
	NSEC3	Next Secure v3	Used with DNSSEC for negative answers
	RRSIG	Signature	Signed, authenticated resource record set
Optional	CNAME	Canonical Name	Nicknames or aliases for a host
	SRV	Service	Gives locations of a well-known service
	TXT	Text	Comments or untyped information

Start of Authority Record (SOA)

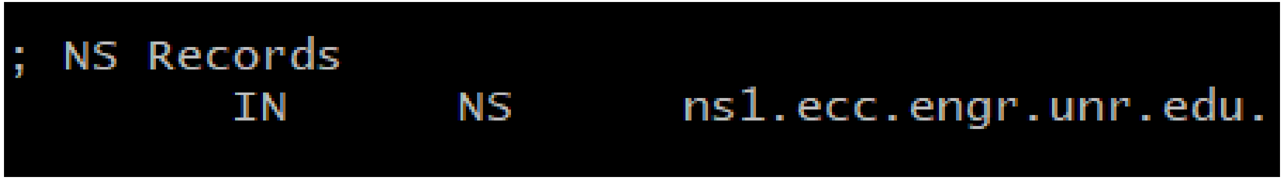
- Each zone has 1 SOA record
  - Name: atrust.com
  - Class: IN (Internet Record)
  - Type: SOA
  - Server: ns1.atrust.com.
  - Email: hostmaster.atrust.com. (hostmaster@atrust.com)



```
; Start of authority record for atrust.com
atrust.com.      IN  SOA    ns1.atrust.com. hostmaster.atrust.com. (
    2017110200      ; Serial number
    10800           ; Refresh  (3 hours)
    1200            ; Retry    (20 minutes)
    3600000         ; Expire   (40+ days)
    3600 )          ; Minimum  (1 hour)
```

Name Server Records (NS)

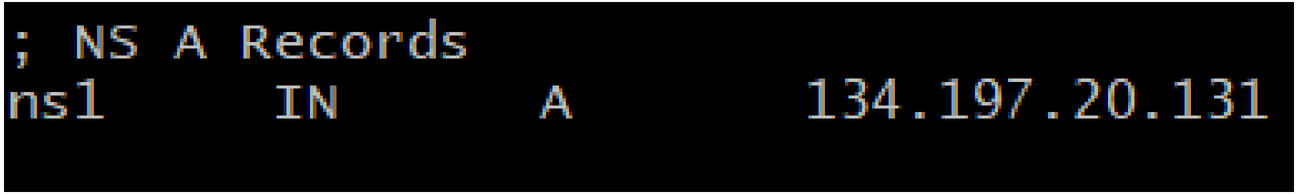
- Identify the servers that are authoritative for a zone
- Format:
    - `zone [ttl] [IN] NS hostname`



```
; NS Records
        IN      NS      ns1.ecc.engr.unr.edu.
```

Address Records (A) and (AAAA)

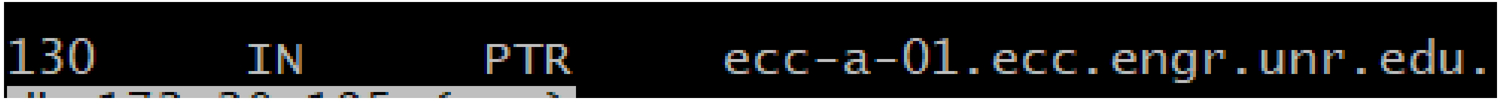
- Heart of the DNS database
- Format:
  - `hostname [ttl] [IN] A ip_address`
- "." denotes fully qualified name
  - No "." means the default domain is added.
- AAAA for IPv6



```
; NS A Records
ns1     IN      A       134.197.20.131
```

Pointer Records (PTR)

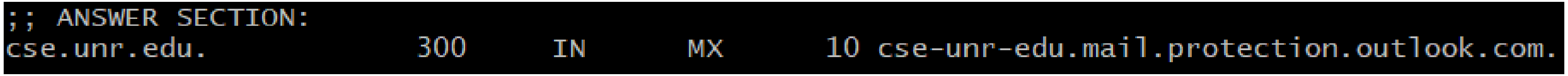
- Maps an IP* to a hostname
- Format:
    - `ip_address [ttl] [IN] PTR hostname`
    - `*130.195.20.172.in-addr.arpa`



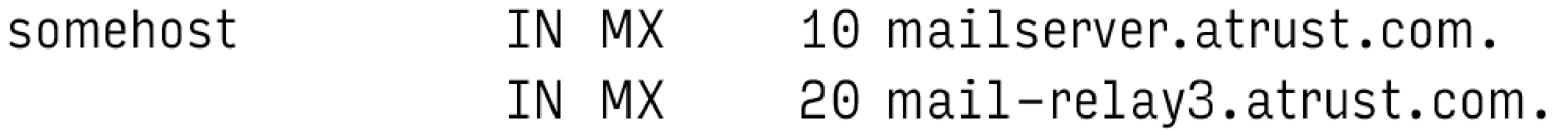
```
130       IN        PTR       ecc-a-01.ecc.engr.unr.edu.
```

Mail Exchanger Records (MX)

- Used for routing mail
- Format:
  - `name [ttl] [IN] MX preference hostname`
  - `dig MX cse.unr.edu @134.197.5.1`



```
;; ANSWER SECTION:
cse.unr.edu.            300     IN      MX      10 cse-unr-edu.mail.protection.outlook.com.
```

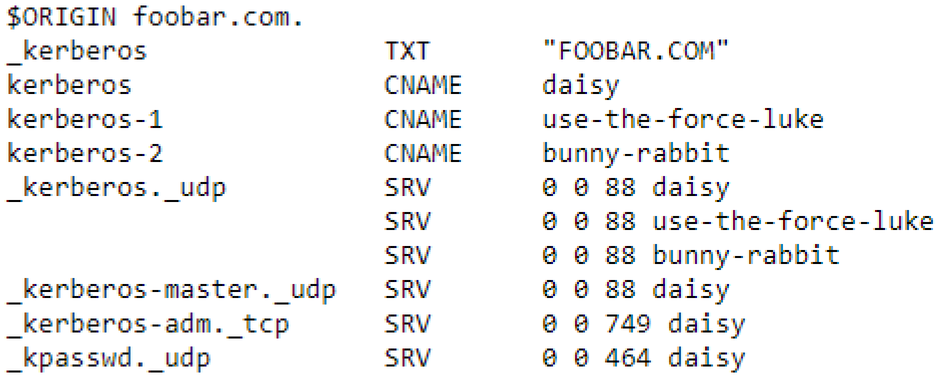


```
somehost            IN  MX    10 mailserver.atrust.com.
                    IN  MX    20 mail-relay3.atrust.com.
```

john@somehost.atrust.com.

Service Records (SRV)

- Specifies the location of services within a domain
- Format:
  service.proto.name [*ttl*] [IN] SRV *pri weight port target*
- Kerberos!



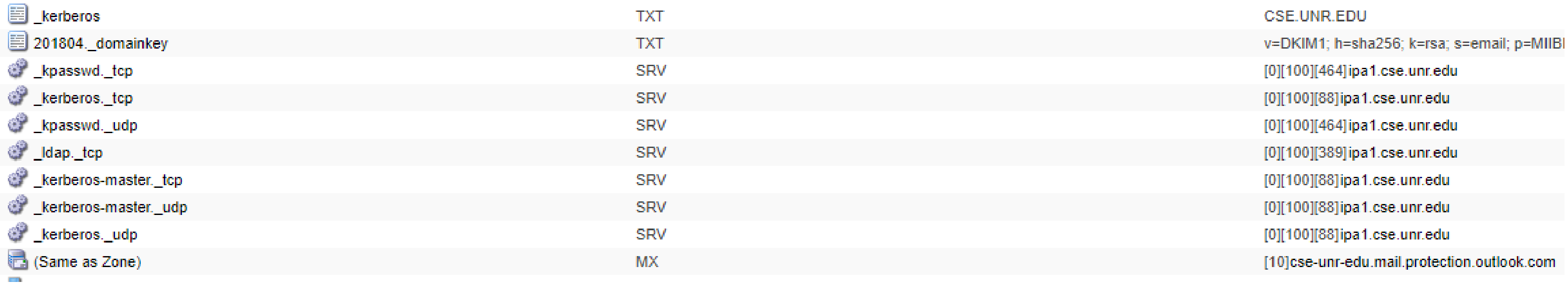
```
$ORIGIN foobar.com.
_kerberos                TXT       "FOOBAR.COM"
kerberos                 CNAME     daisy
kerberos-1               CNAME     use-the-force-luke
kerberos-2               CNAME     bunny-rabbit
_kerberos._udp           SRV       0 0 88 daisy
                         SRV       0 0 88 use-the-force-luke
                         SRV       0 0 88 bunny-rabbit
_kerberos-master._udp    SRV       0 0 88 daisy
_kerberos-adm._tcp       SRV       0 0 749 daisy
_kpasswd._udp            SRV       0 0 464 daisy
```

Text Records (TXT)

- Adds arbitrary text to a DNS record
- Format:

```
    name [ttl] [IN] TXT info ...
```

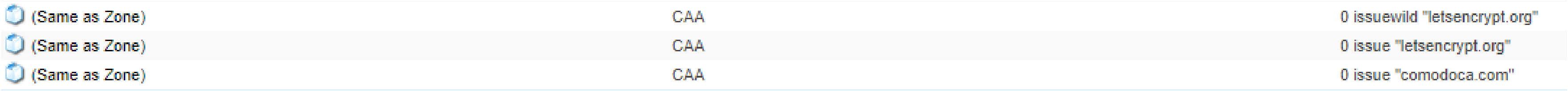
- Verification
    - Google Apps



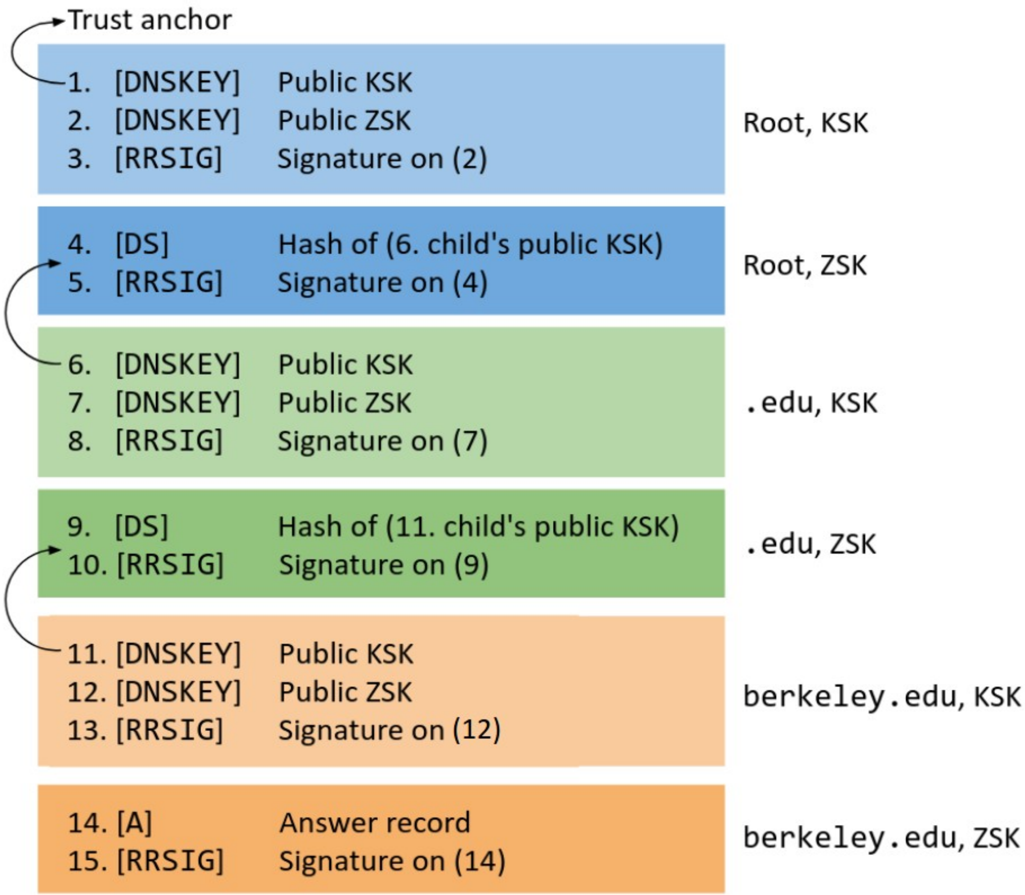
_kerberos	TXT	CSE.UNR.EDU
201804._domainkey	TXT	v=DKIM1; h=sha256; k=rsa; s=email; p=MIIBI
_kpasswd._tcp	SRV	[0][100][464]ipa1.cse.unr.edu
_kerberos._tcp	SRV	[0][100][88]ipa1.cse.unr.edu
_kpasswd._udp	SRV	[0][100][464]ipa1.cse.unr.edu
_ldap._tcp	SRV	[0][100][389]ipa1.cse.unr.edu
_kerberos-master._tcp	SRV	[0][100][88]ipa1.cse.unr.edu
_kerberos-master._udp	SRV	[0][100][88]ipa1.cse.unr.edu
_kerberos._udp	SRV	[0][100][88]ipa1.cse.unr.edu
(Same as Zone)	MX	[10]cse-unr-edu.mail.protection.outlook.com

Certificate Authority Authorization Record (CAA)

- Specifies Certificate Authorities(CA)
  allowed to issue certificates for the domain
- https://support.dnsimple.com/articles/caa-record/#what-is-a-caa-record



(Same as Zone)	CAA	0 issuewild "letsencrypt.org"
(Same as Zone)	CAA	0 issue "letsencrypt.org"
(Same as Zone)	CAA	0 issue "comodoca.com"



Trust anchor

1. [DNSKEY] Public KSK
2. [DNSKEY] Public ZSK
3. [RRSIG] Signature on (2)

Root, KSK

4. [DS] Hash of (6. child's public KSK)
5. [RRSIG] Signature on (4)

Root, ZSK

6. [DNSKEY] Public KSK
7. [DNSKEY] Public ZSK
8. [RRSIG] Signature on (7)

.edu, KSK

9. [DS] Hash of (11. child's public KSK)
10. [RRSIG] Signature on (9)

.edu, ZSK

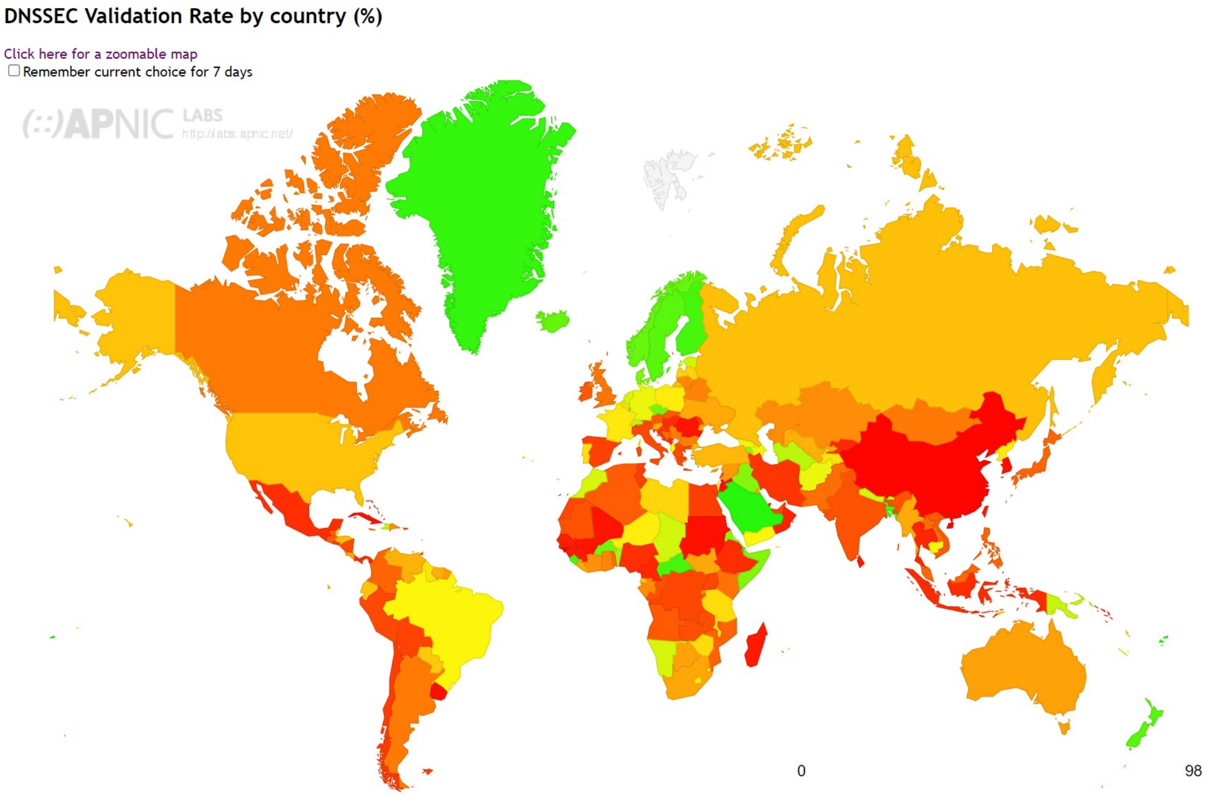
11. [DNSKEY] Public KSK
12. [DNSKEY] Public ZSK
13. [RRSIG] Signature on (12)

berkeley.edu, KSK

14. [A] Answer record
15. [RRSIG] Signature on (14)

berkeley.edu, ZSK

DNSSEC Adoption



DNSSEC Validation Rate by country (%)

Click here for a zoomable map

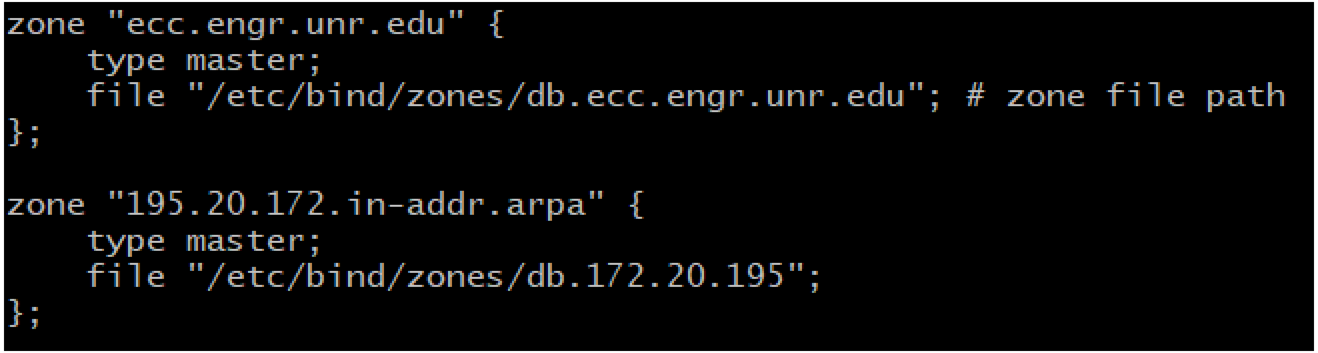
☐ Remember current choice for 7 days

The BIND software

- Berkeley Internet Name Domain system
  - bind9 latest stable version
  - bind10 under development
- Reference implementation for DNS
- Components
  - Named - DNS Server
  - Resolver libraries
  - Command line utilities: `dig`, `nslookup`, and `host`
- `Configuration`
  - `/etc/bind/named.conf`

Basic Bind configuration

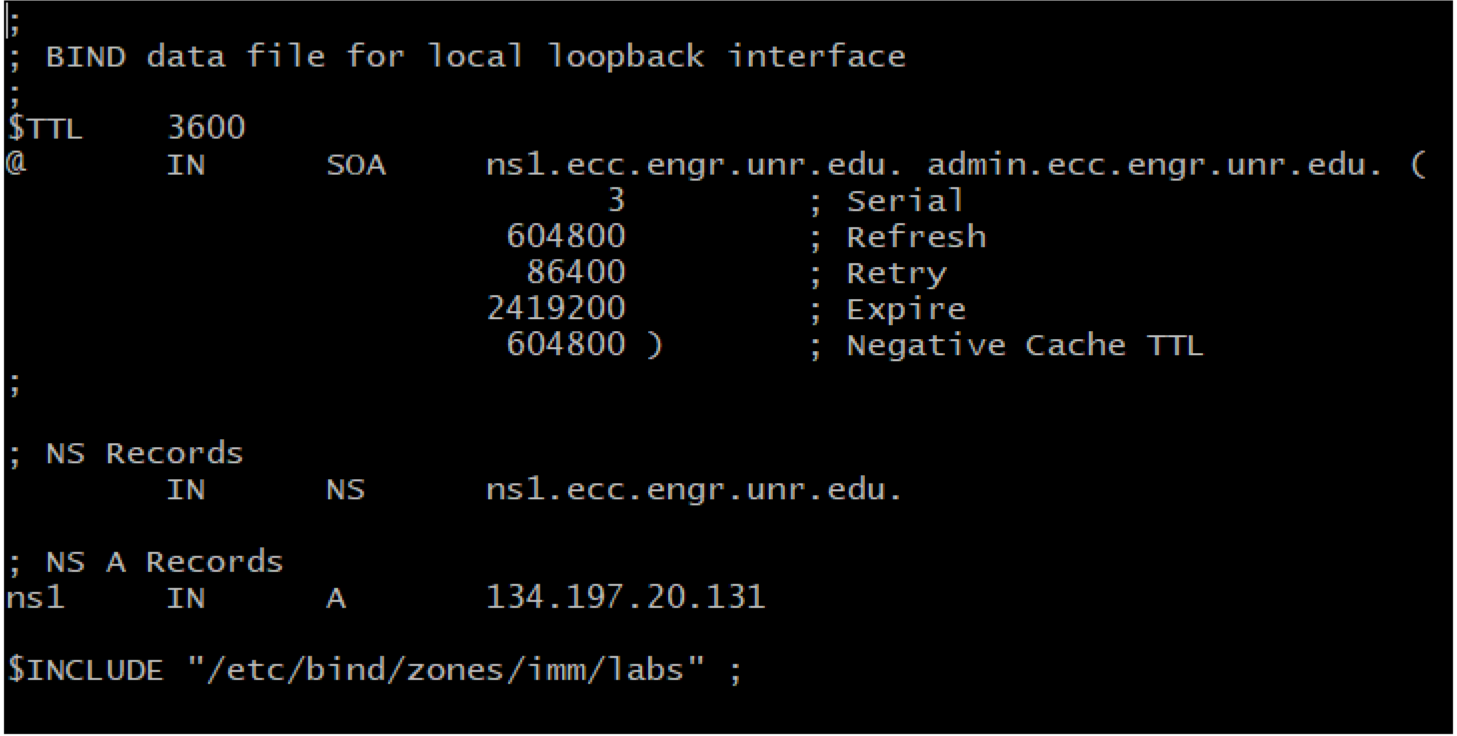
`/etc/bind/named.conf.local`



```
zone "ecc.engr.unr.edu" {
    type master;
    file "/etc/bind/zones/db.ecc.engr.unr.edu"; # zone file path
};

zone "195.20.172.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.172.20.195";
};
```

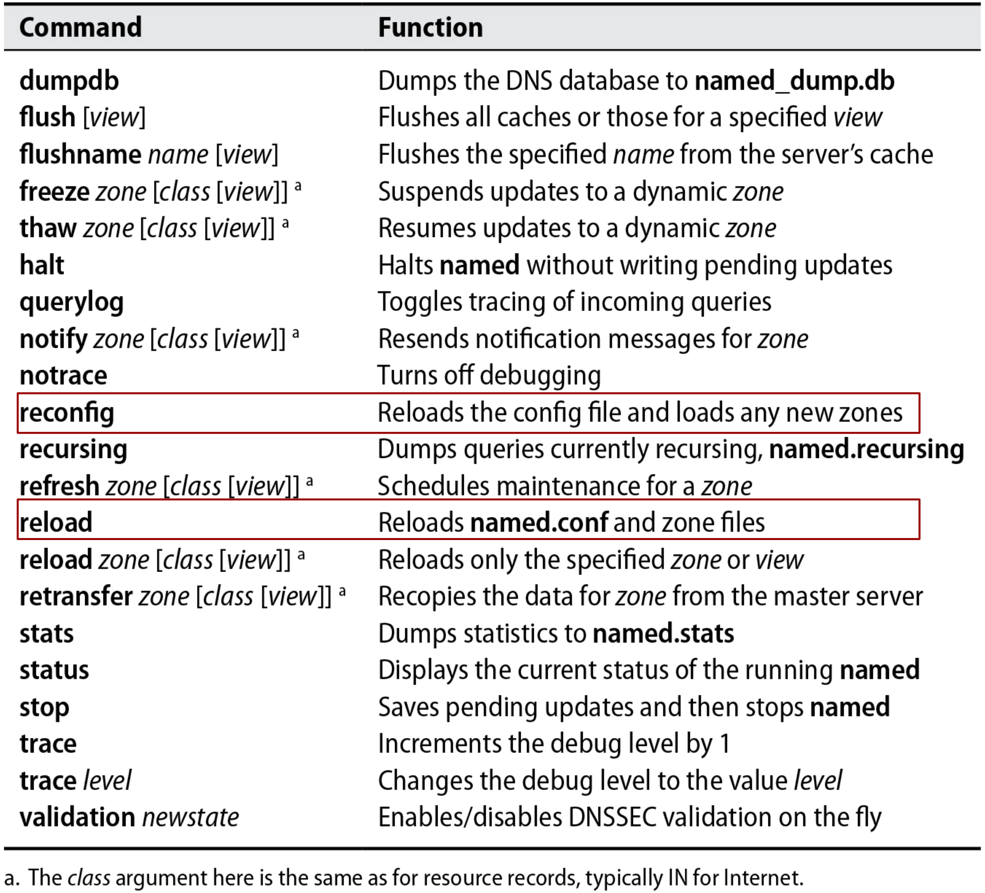
Basic Bind configuration

/etc/bind/zones/db.ecc.engr.unr.edu



```
;
; BIND data file for local loopback interface
;
$TTL    3600
@       IN      SOA     ns1.ecc.engr.unr.edu. admin.ecc.engr.unr.edu. (
                              3         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;

; NS Records
        IN      NS      ns1.ecc.engr.unr.edu.

; NS A Records
ns1     IN      A       134.197.20.131

$INCLUDE "/etc/bind/zones/imm/labs" ;
```

rndc



Command	Function
dumpdb	Dumps the DNS database to **named_dump.db**
flush [*view*]	Flushes all caches or those for a specified *view*
flushname *name* [*view*]	Flushes the specified *name* from the server's cache
freeze *zone* [*class* [*view*]] [a]	Suspends updates to a dynamic *zone*
thaw *zone* [*class* [*view*]] [a]	Resumes updates to a dynamic *zone*
halt	Halts **named** without writing pending updates
querylog	Toggles tracing of incoming queries
notify *zone* [*class* [*view*]] [a]	Resends notification messages for *zone*
notrace	Turns off debugging
reconfig	Reloads the config file and loads any new zones
recursing	Dumps queries currently recursing, **named.recursing**
refresh *zone* [*class* [*view*]] [a]	Schedules maintenance for a *zone*
reload	Reloads **named.conf** and zone files
reload *zone* [*class* [*view*]] [a]	Reloads only the specified *zone* or *view*
retransfer *zone* [*class* [*view*]] [a]	Recopies the data for *zone* from the master server
stats	Dumps statistics to **named.stats**
status	Displays the current status of the running **named**
stop	Saves pending updates and then stops **named**
trace	Increments the debug level by 1
trace *level*	Changes the debug level to the value *level*
validation *newstate*	Enables/disables DNSSEC validation on the fly

[a] The *class* argument here is the same as for resource records, typically IN for Internet.

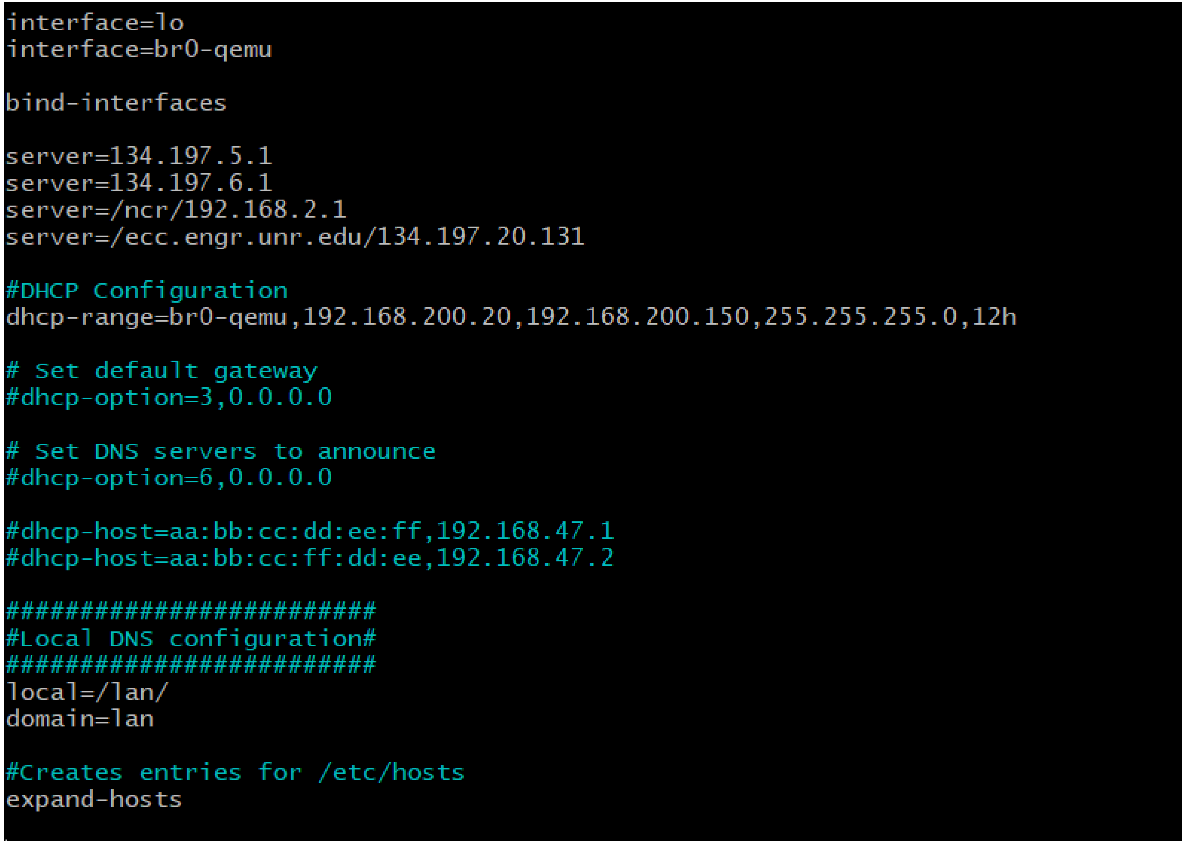
dnspython

```
pip install dnspython

answers = dns.resolver.query(record, rtype)

for rdata in answers:
   print('Host: {0}, Preference: {1}\n'.format(rdata, rdata))
```

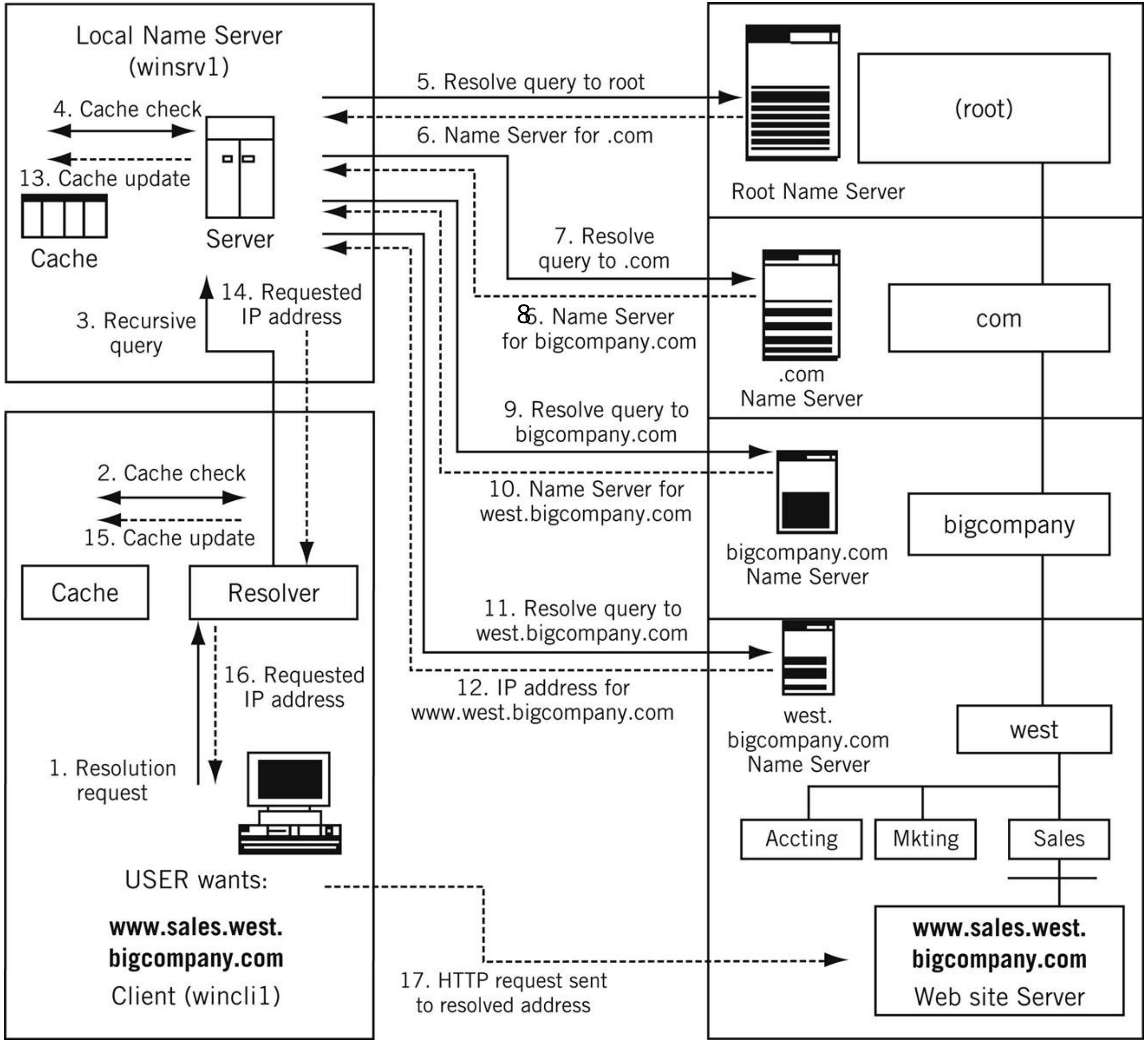
dnsmasq

```
apt install dnsmasq
$EDITOR /etc/dnsmasq.conf
systemctl disable systemd-resolved #Disable the systemd DNS
systemctl start dnsmasq #Enable our dnsmasq setup
```

dnsmasq configuration



```
interface=lo
interface=br0-qemu

bind-interfaces

server=134.197.5.1
server=134.197.6.1
server=/ncr/192.168.2.1
server=/ecc.engr.unr.edu/134.197.20.131

#DHCP Configuration
dhcp-range=br0-qemu,192.168.200.20,192.168.200.150,255.255.255.0,12h

# Set default gateway
#dhcp-option=3,0.0.0.0

# Set DNS servers to announce
#dhcp-option=6,0.0.0.0

#dhcp-host=aa:bb:cc:dd:ee:ff,192.168.47.1
#dhcp-host=aa:bb:cc:ff:dd:ee,192.168.47.2

#########################
#Local DNS configuration#
#########################
local=/lan/
domain=lan

#Creates entries for /etc/hosts
expand-hosts
```


Local Name Server
(winsrv1)
4. Cache check
13. Cache update
Server
Cache
3. Recursive query
14. Requested IP address
5. Resolve query to root
6. Name Server for .com
7. Resolve query to .com
86. Name Server for bigcompany.com
9. Resolve query to bigcompany.com
10. Name Server for west.bigcompany.com
11. Resolve query to west.bigcompany.com
12. IP address for www.west.bigcompany.com
Root Name Server
(root)
com
.com Name Server
bigcompany
bigcompany.com Name Server
west
west. bigcompany.com Name Server
Accting
Mkting
Sales
www.sales.west. bigcompany.com
Web site Server
2. Cache check
15. Cache update
Cache
Resolver
16. Requested IP address
1. Resolution request
USER wants:
www.sales.west. bigcompany.com
Client (wincli1)
17. HTTP request sent to resolved address

Additional Reading

The Illustrated Network

https://learning.oreilly.com/library/view/the-illustrated-network/9780128110287/xhtml/chp023.xhtml

Network #2: DNS

https://inst.eecs.berkeley.edu/~cs161/fa16/slides/network2_dns.key.pdf

https://dnsviz.net/