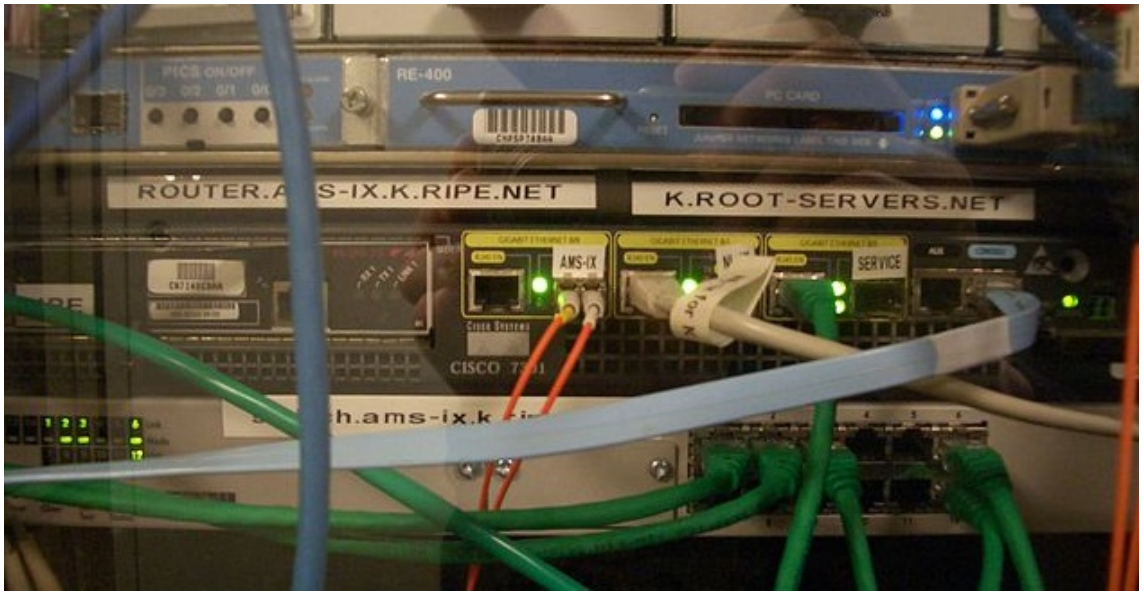
# COMP 175

## System Administration and Security


# DOMAIN NAME SERVICE

# Objectives

- Understanding of the Domain Name Service
- History and Evolution
- How DNS Functions
- DNS Configuration
- Importance of Accuracy
- Security Issues



# In the long, long ago time…

- A *hosts* file mapped hostnames to IP addresses
- Prior to DNS – SRI maintained master hosts.txt file (see RFC 952)
  - 1981 – 213 hosts
    - New one added every 20 days
  - Feb. 1988 – 11,631 hosts
  - Not going to scale very well
  - Staff were overwhelmed
  - Centralized location not a good idea either

# In the long, long ago time...

Pre-www Information display mechanism

# In the long, long ago time...

- Sites copied it nightly to get latest version
  - Bandwidth insufficient
- Easy to introduce errors
  - "Fate Sharing" model wrong
  - Impacted sites couldn't change database
- Huge flat name space – unique server names

- DNS distributed the maintenance
- Fate – you make errors in your own namespace
- **/etc/hosts file lives on!**

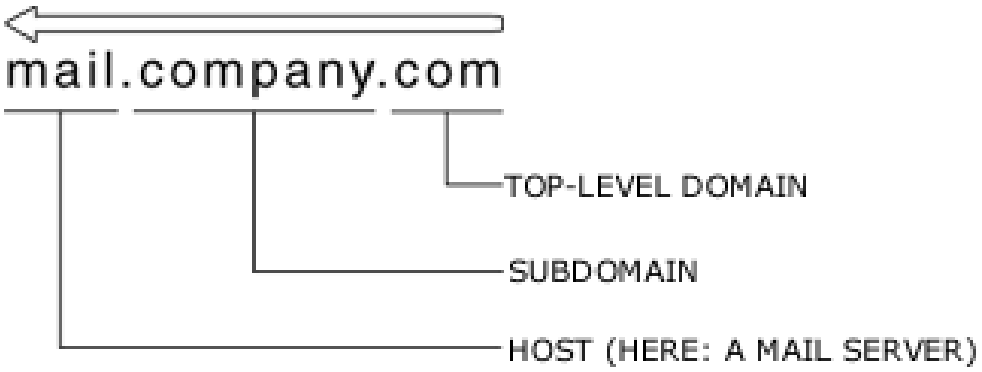
# Domain Name System

- Domain Name System (DNS)
- Application layer protocol
- A (1)hierarchical (2)distributed naming system for computers, services, or any resource connected to the Internet or a private network
- DNS provides the translation function between the two **Internet namespaces**:
  - The domain name hierarchy
  - The Internet Protocol (IP) address space

  i.e. *Resolves* domain names to IP addresses
- Abstracts URL's and email addresses

# DNS

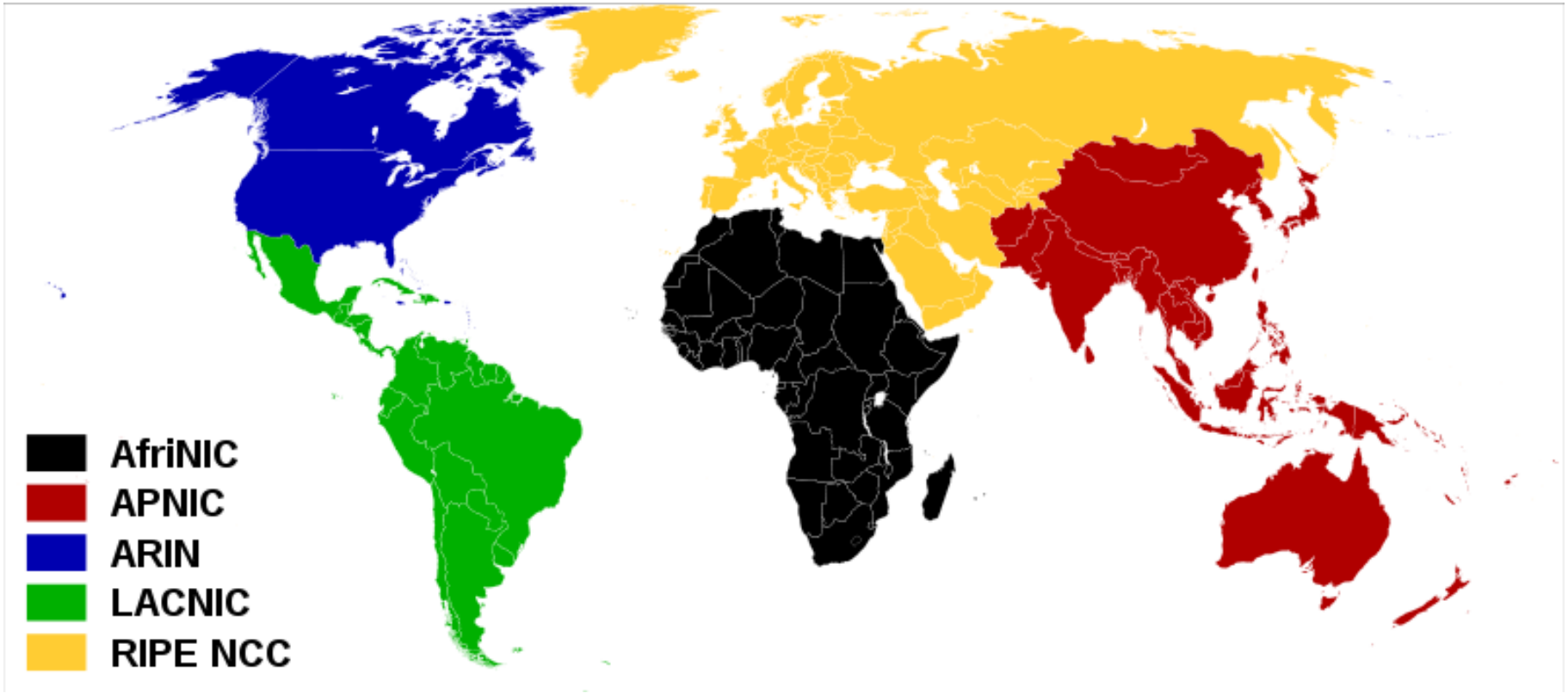
- First implementation - 1983
- BIND written – 1984  Usable (2.0)  August 1985
- ISC BIND is the most widely used DNS software
  - On Unix systems it is the de facto standard
- Domain name consists of dot delimited *labels*
- FQDN – Fully.Qualified.Domain.Name.
- Right-most label is the Top Level Domain (TLD)



# Oversight

- Internet Corporation for Assigned Names and Numbers
  - ICANN (Policy)
- Responsible for the coordination IP address spaces
- Address block assignment to regional Internet registries
- Maintaining registries of Internet protocol identifiers
- Managing top-level domain name space (DNS root zone)
- Including the operation of root nameservers
- Internet Assigned Numbers Authority
  - IANA (Technical)

# Regional Internet Registries




AfriNIC.net African Internet Address Registry
APNIC.net Asian Pacific Internet Address Registry
ARIN.net American Registry for Internet Numbers
LACNIC.net Latin American and Caribbean Internet Address Registry
RIPE.net Réseaux IP Européens

# DNS Distributed Database

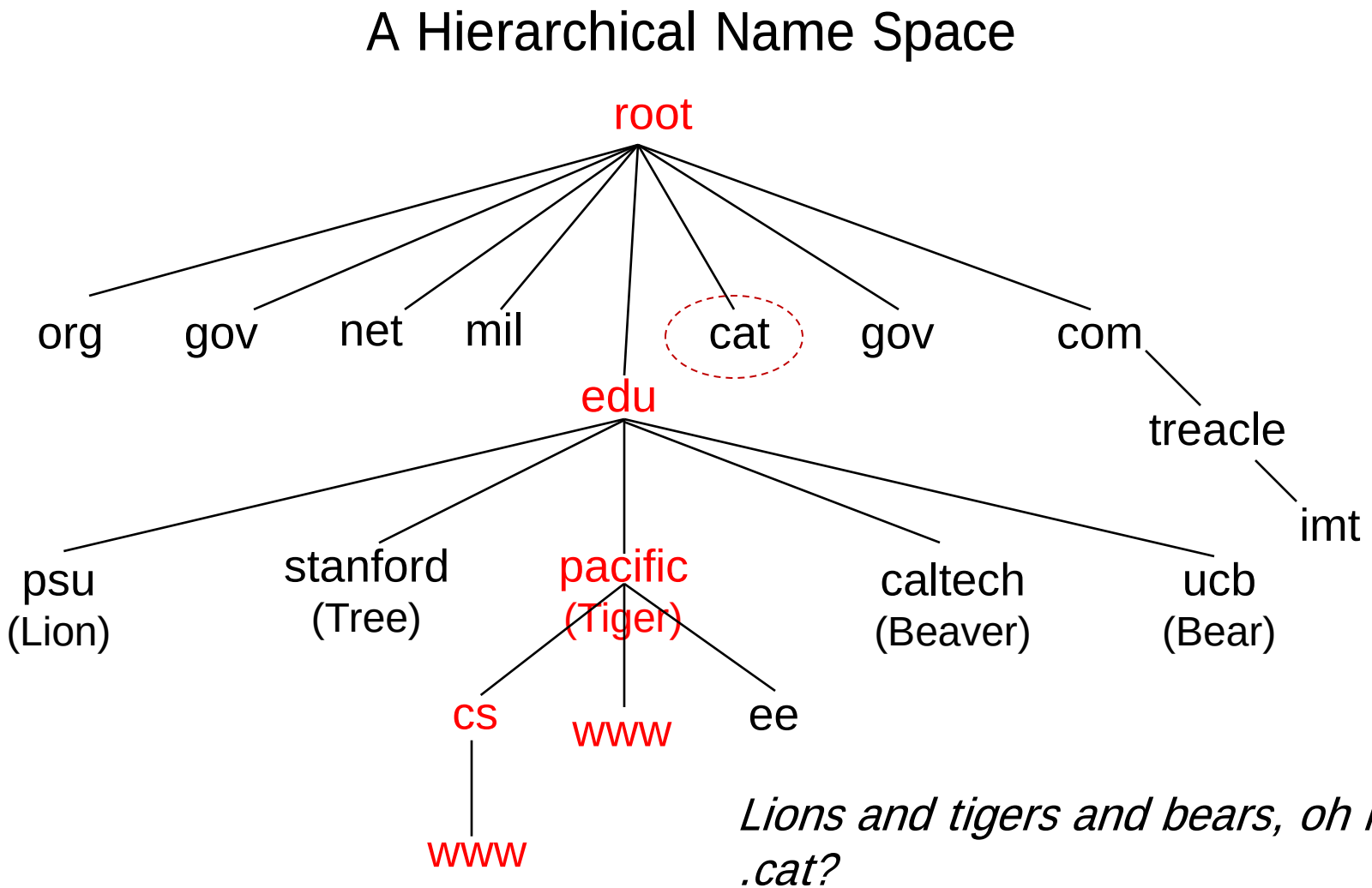
- Each domain has at least one authoritative DNS server that publishes information about that domain and the name servers of any domains subordinate to it (delegated)
- The top of the hierarchy is served by the root name servers
  - The servers to query when looking up (resolving) a TLD
  - 13 root name servers
  - Distributed across 255 hosts  (10/2011)
  - Distributed across 1,510 hosts  (02/2022)

# Root Name Servers

# Root Zone Servers

| # | Svr | Sites | Operator |
|---|---|---|---|
| 1. | A | 6 | VeriSign |
| 2. | B | 1 | USC-Information Sciences Institute |
| 3. | C | 6 | Cogent |
| 4. | D | 1 | University of Maryland |
| 5. | E | 1 | Nasa Ames |
| 6. | F | 49 | Internet Systems Consortium |
| 7. | G | 6 | US DOD |
| 8. | H | 2 | US Army Research Lab |
| 9. | I | 38 | Netnod |
| 10. | J | 70 | VeriSign |
| 11. | K | 18 | RIPE |
| 12. | L | 51 | ICANN |
| 13. | M | 6 | WIDE Project |

# DNS Domain Name System



# .cat TLD

- .cat (Catalan pronunciation: [ˈpun ˈkat]) (point cat) is a sponsored top-level domain intended to be used to highlight the Catalan language and culture.
- Its policy has been developed by ICANN and Fundació puntCAT.
- It was approved in September 2005
- Domain hacks
  - kitty.cat
  - meow.cat

# TLD's

| | |
|---|---|
| .aero | air-transport industry |
| .asia | Asia-Pacific region companies |
| .biz | business |
| .coop | cooperatives |
| .gov | limited to US government entities |
| .info | informational |
| .int | international organizations |
| .jobs | job advertisements |
| .mil | US military |
| .museum | museums |
| .name | individuals |
| .mobi | mobile devices |
| .pro | professions |
| .travel | tourism and travel |
| .xxx | sexually explicit |

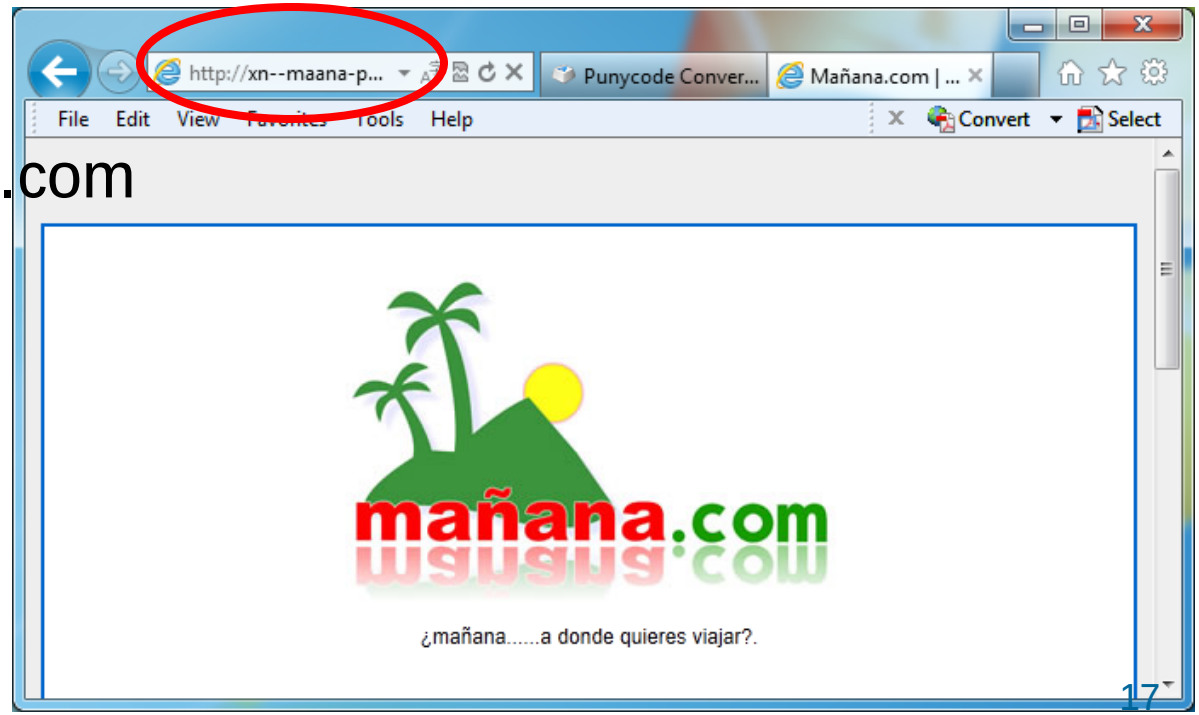
# Country Codes (Partial)

| | |
|---|---|
| .ac | Ascension Island |
| .am | Armenia |
| .bf | Burkina Faso |
| .bj | Benin |
| .bm | Bermuda |
| .bo | Bolivia |
| .bs | Bahamas |
| .dj | Djibouti |
| .gf | French Guiana |
| .im | Isle of Man |
| .io | British Indian Ocean Territory |
| .iq | Iraq |
| .jo | Jordan |
| .ky | Cayman Islands |
| .lv | Latvia |
| .me | Montenegro |
| .no | Norway |
| .sm | San Marino |
| .to | Tonga |
| .tv | Tuvalu |
| .wf | Wallis and Futuna |

| | |
|---|---|
| .中国 | China |
| .ভারত | India |
| .امارات | Jordan |

# Internationalized Domain Name

- IDN - Internationalized Domain Name
  - Chinese, Russian, Arabic, etc.
- Encoded in multi-byte Unicode
- Stored in DNS as ASCII strings using Punycode
- RFC 3492
- Example:
  - mañana.com
  - xn--maana-pta.com



# DNS

- Start local
  - localhost
- Think global
- Think future
  - IPv6 2620:0:2d0:200::10

# hosts

- hosts file still is used today
- Unix - /etc/hosts
- Windows - \windows\system32\drivers\etc\hosts
- OS X - /etc/hosts (sym link to /private/etc/hosts)

```
# For loopback
127.0.0.1          localhost
10.0.0.8           cheshire
127.0.0.1          adsite.com
```

???

# Local Name Server

- Does not strictly belong to hierarchy
- Each ISP (residential ISP, company, university) has one or more
- Also called “default name server”
- When host makes DNS query, query is sent to its local DNS server
- Acts as proxy, forwards query into hierarchy
- You will likely be running local name servers

# Hierarchical Database

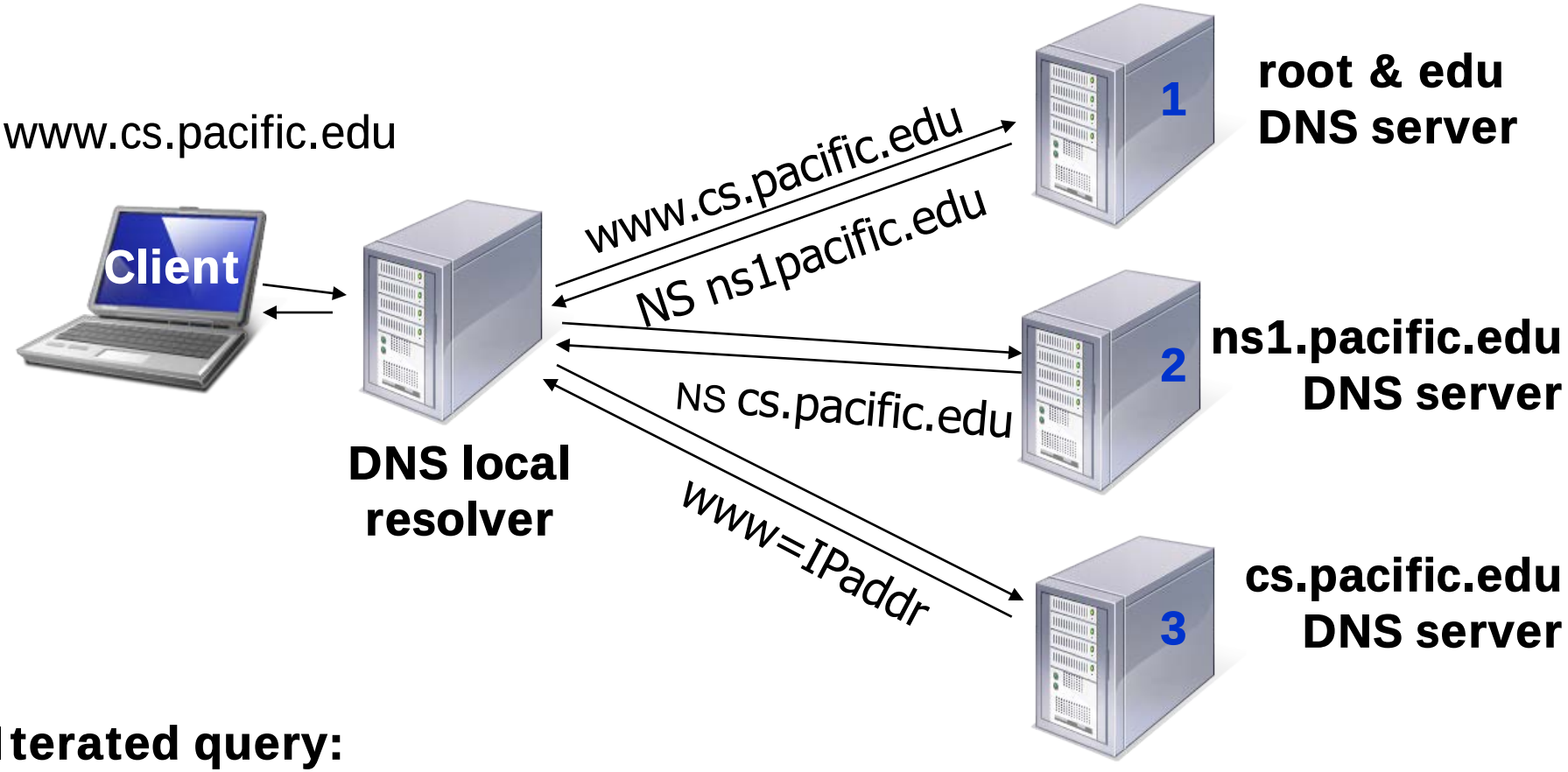
Client wants IP for www.cs.pacific.edu

- Client queries Network DNS server
- Network DNS server

1. queries a root server to find edu DNS server
2. queries edu DNS server to get pacific.edu DNS server
3. queries pacific.edu DNS server to get cs.pacific.edu DNS server
4. queries cs.pacific.edu DNS server to get IP address for www.cs.pacific.edu

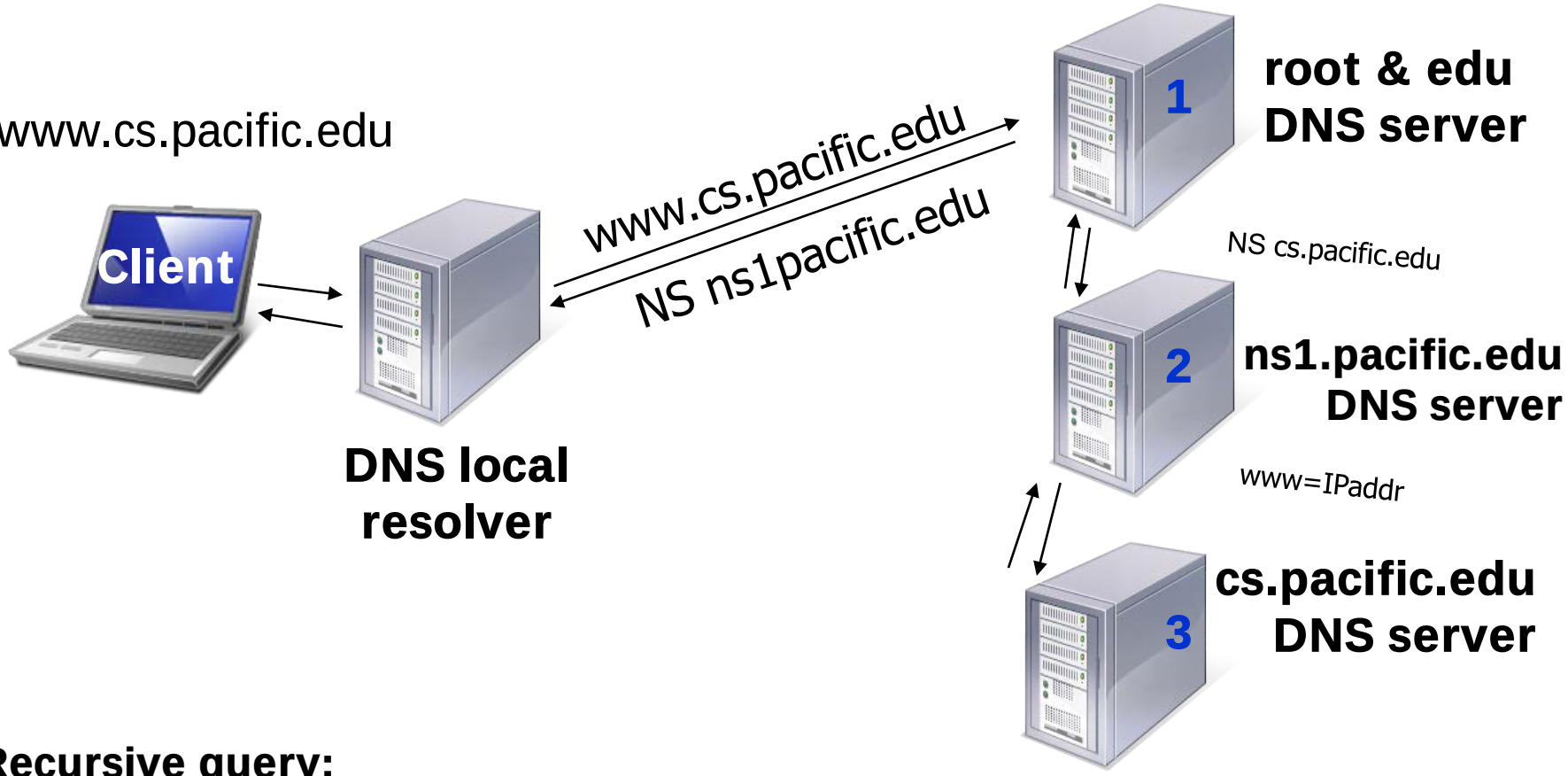
- Network DNS server provides answer to Client

# DNS Lookup Example



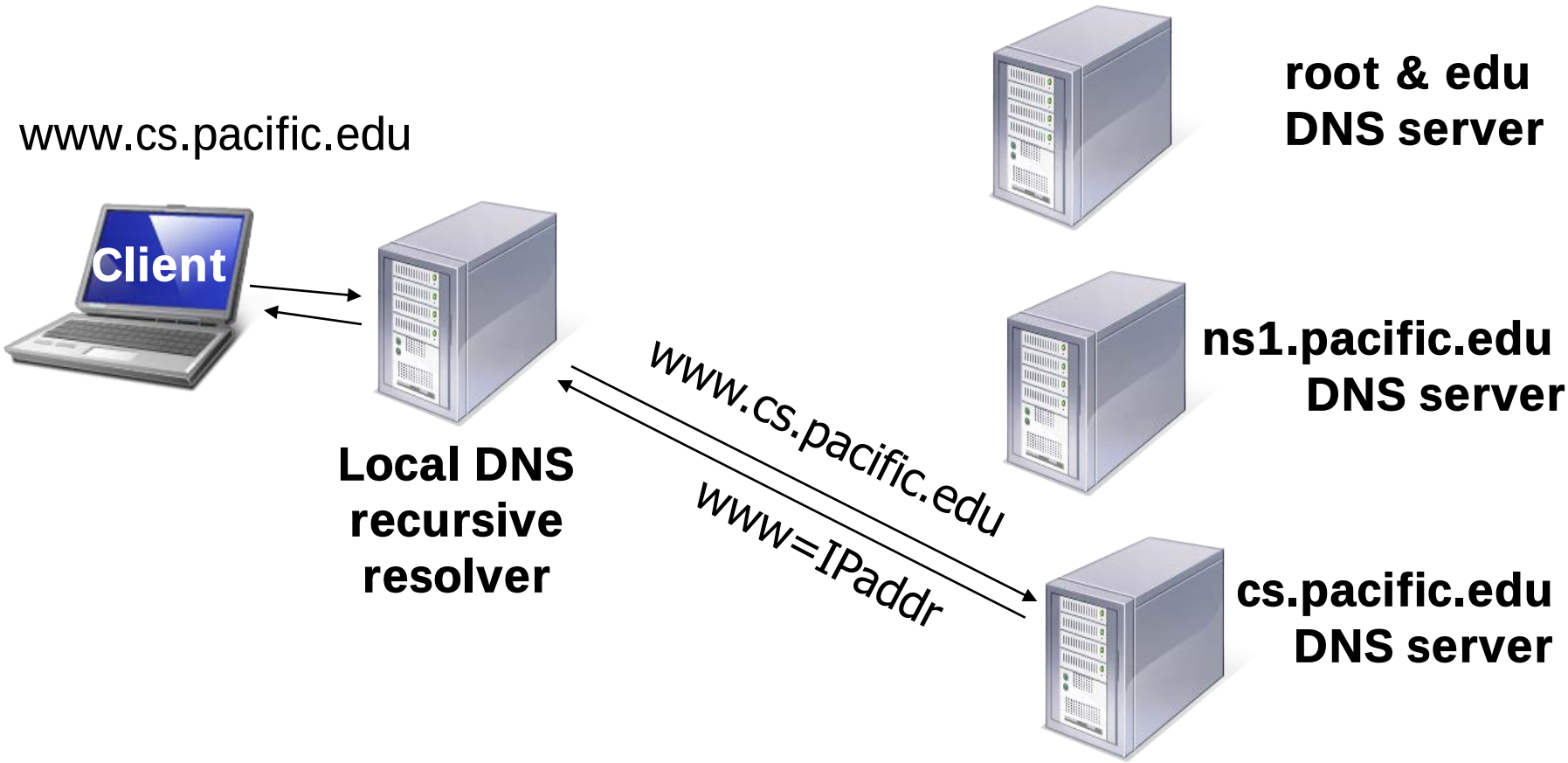

**Iterated query:**
Contacted server replies with name of server to contact
"I don't know this name, but ask this server"

# DNS Lookup Example




**Recursive query:**
Contacted server replies with resolved answer
"I know this name, here is answer. I'm not authoritative though".

# Lookup using cached DNS server




Caching servers improve efficiency, reduce DNS traffic, and reduce latency by storing query results for a period of time (TTL).

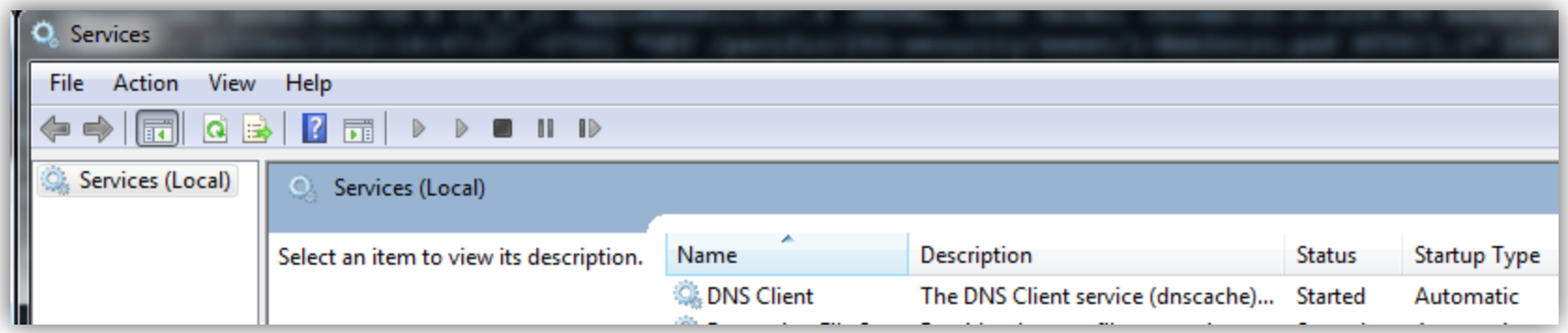
# OS - Caching DNS Service

www.cs.pacific.edu


Windows: ipconfig /displaydns
ipconfig /flushdns

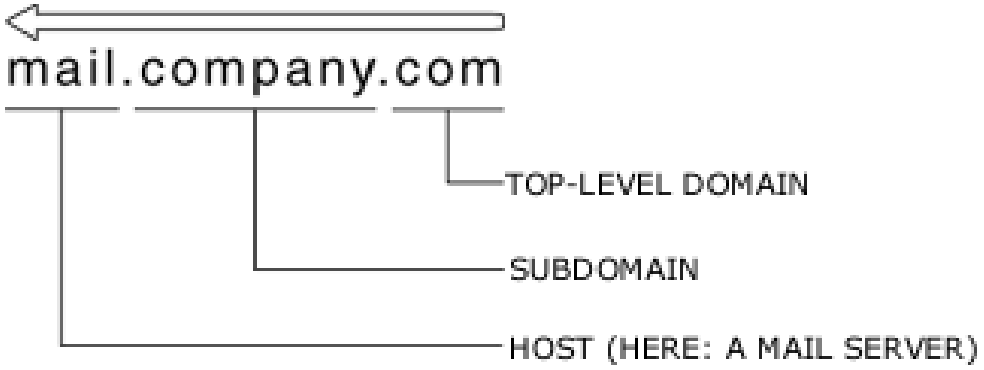
Ubuntu: resolvectl utility
$ resolvectl

**Local DNS Caching Service**



# DNS - Hierarchical service

- Root name servers for top-level domains
- Authoritative name servers for delegated subdomains
- Local resolvers contact authoritative servers when they don’t know a name



# DNS Caching

- Once (any) name server learns mapping, it caches mapping (including Windows)
- Cache entries timeout (disappear) after TTL
- TLD servers typically cached in local name servers
  - Thus root name servers not often visited
  - Avoids a huge bottleneck
    - If DNS is correctly configured
    - *Hello! This means you*

# Caching

- DNS responses are cached
  - Quick response for repeated translations
  - Useful for finding servers as well as addresses
    - such as NS records for domains
- Negative results are also cached
  - Response: **NXDOMAIN** (Non-Existent Domain)
  - Saves time for nonexistent sites, e.g. misspelling
- Cached data periodically times out (TTL)

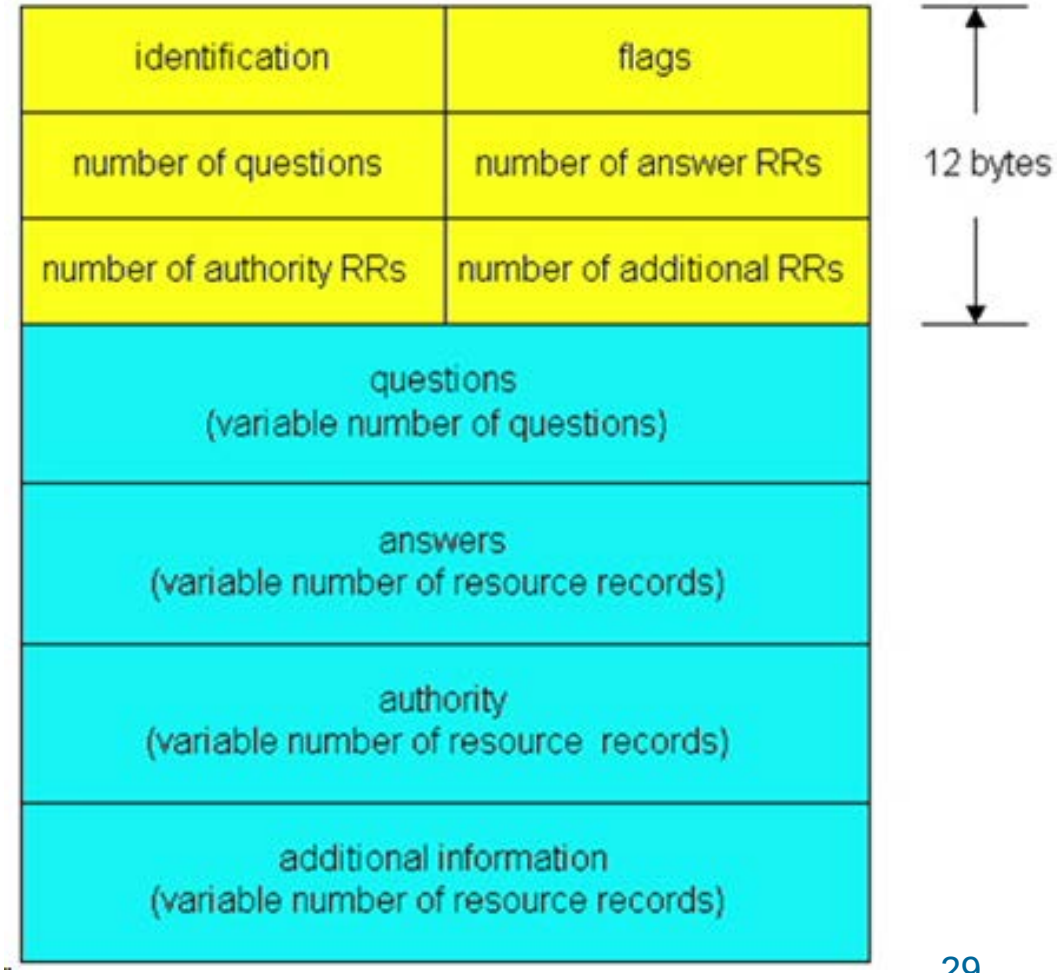
```
dig results for www.pacific.edu & wombat.pacific.edu (NX)

www.pacific.edu.    43458    IN      A          138.9.110.12
pacific.edu.        10800    IN      SOA     ns1.pacific.edu
```

Remaining TTL (from 1 day?) vs Absolute 180 min

FQDN (Technically correct)

# DNS Protocol Message

- DNS protocol : query and reply messages
  - Both with same message format
- msg header
  - identification: 16 bit # for query, reply to query uses same #
- flags:
  - query or reply
  - recursion desired
  - recursion available
  - reply authoritative



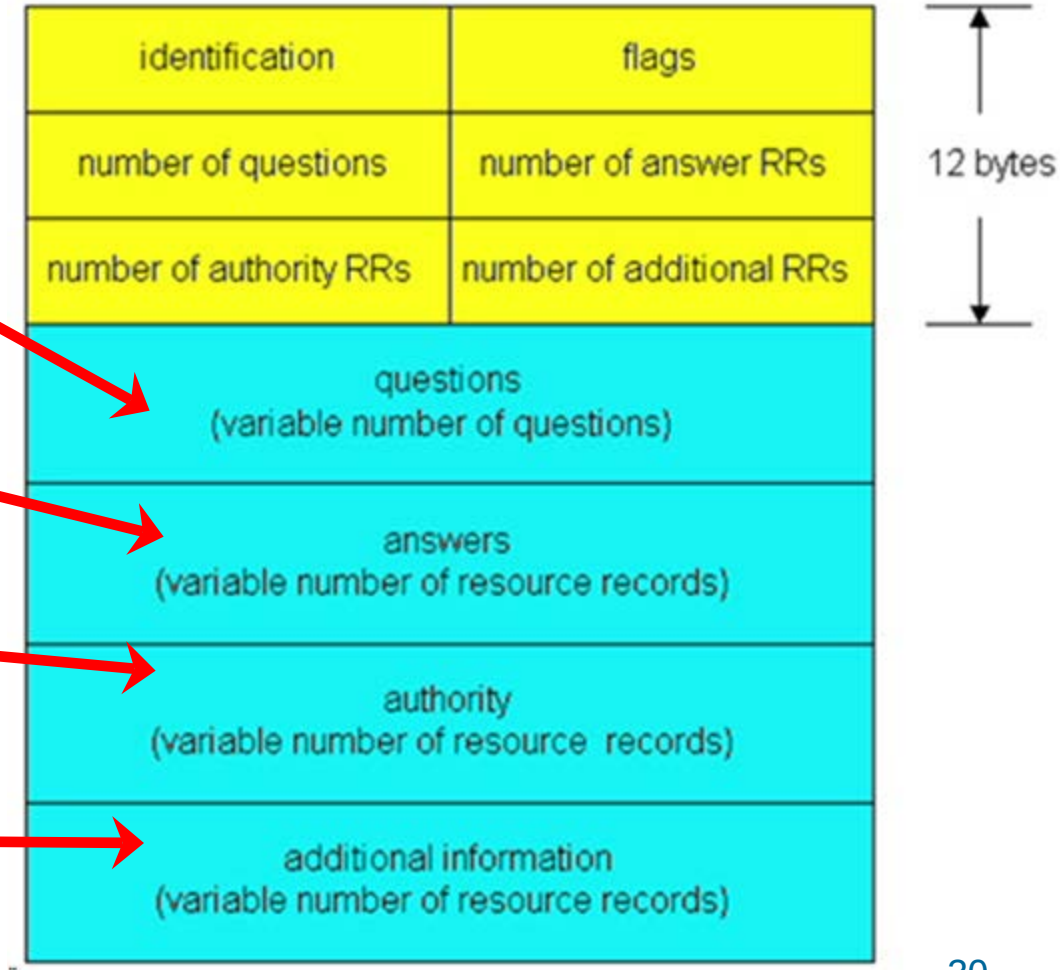
# DNS Protocol Message

Name, type fields for a query

RRs in response to query

records for authoritative servers

additional “helpful” info that may be used



# DNS Records

Is the size and complexity starting to become visible?

# DNS Records

Reading a FQDN from the right...

- TLD's (ex: com gov edu)
- Second-level domains (ex: google pacific)
- Third-level domains - subdomains & CNAMEs
  - (ex: dot.ca.gov cliodhna.cop.uop.edu)
  - (ex: ftp.pacific.edu www.pacific.edu)

  - CNAME?
  - canonical - authorized, recognized, accepted

# DNS records

DNS: distributed db storing resource records (RR)

RR format: **(name, value, type, ttl)**

- Type=A
  - name is hostname
  - value is IP address
- Type=NS
  - name is domain
  - (e.g. foo.com)
  - value is hostname of authoritative name server for this domain
- Type=CNAME
  - name is alias name for some “canonical” (the real) name
  - www.ibm.com is really: seast.backup2.ibm.com
  - value is canonical name
- There are ~35 record types

# DNS Records

- Type=MX
  - name is Mail eXchange record
  - value is hostname of the Mail Transfer Agent for the domain
- Type=AAAA
  - IPv6 address record
  - value is 128-bit IPv6 address
- Type=PTR
  - Pointer Record
  - value is pointer to a canonical name
- Type=SOA
  - start of authority record
  - value is the primary name server, email contact, domain serial number, and several zone TTL timers

# DNS Records

- Tools to query DNS
  - dig - domain information groper
  - nslookup (cmd)
  - whois (cmd)
  - http://www.dnsgoodies.com/
  - http://www.mydnstools.info

# dig treacle.com

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;treacle.com.                   IN      A

;; ANSWER SECTION:
treacle.com.            10800   IN      A       107.138.2.17

;; AUTHORITY SECTION:
treacle.com.            10800   IN      NS      ns.treacle.com.
treacle.com.            10800   IN      NS      ns1.treacle.com.

;; ADDITIONAL SECTION:
ns.treacle.com.         10800   IN      A       107.138.2.17
ns1.treacle.com.        10800   IN      A       107.138.2.17

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Aug 10 12:10:56 PDT 2022
;; MSG SIZE  rcvd: 123
```

# dig any pacific.edu (then)

```
; <<>> DiG 9.5.1b1 <<>> pacific.edu any
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29714
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 2, ADDITIONAL: 0
;; QUESTION SECTION:
;pacific.edu.                   IN      ANY

;; ANSWER SECTION:
pacific.edu.            10186   IN      NS      ns2.pacific.edu.
pacific.edu.            10186   IN      NS      ns1.pacific.edu.
pacific.edu.            18585   IN      A       138.9.110.12

;; AUTHORITY SECTION:
pacific.edu.            10186   IN      NS      ns1.pacific.edu.
pacific.edu.            10186   IN      NS      ns2.pacific.edu.
;; Query time: 48 msec
;; MSG SIZE  rcvd: 109
```

# dig pacific.edu (Now)

```
; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> pacific.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26950
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 13, ADDITIONAL: 26

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;pacific.edu.                   IN      A

;; ANSWER SECTION:
pacific.edu.            60      IN      A       52.35.243.230
pacific.edu.            60      IN      A       54.191.120.137
pacific.edu.            60      IN      A       35.160.234.155

;; AUTHORITY SECTION:
.                       185472  IN      NS      e.root-servers.net.
.                       185472  IN      NS      m.root-servers.net.
.                       185472  IN      NS      c.root-servers.net.
.                       185472  IN      NS      l.root-servers.net.
.                       185472  IN      NS      b.root-servers.net.
```

# dig pacific.edu any

```
mmaxwell@Jammy:~$ dig pacific.edu any

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> pacific.edu any
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19757
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;pacific.edu.                   IN      ANY

;; ANSWER SECTION:
pacific.edu.            602     IN      NS      ns-705.awsdns-24.net.
pacific.edu.            602     IN      NS      ns-2044.awsdns-63.co.uk.
pacific.edu.            602     IN      NS      ns-110.awsdns-13.com.
pacific.edu.            602     IN      NS      ns-1289.awsdns-33.org.

;; Query time: 31 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (TCP)
;; WHEN: Wed Aug 10 12:18:49 PDT 2022
;; MSG SIZE  rcvd: 180
```

# dig ns pacific.edu

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31454
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 2
;; QUESTION SECTION:
;pacific.edu.                   IN      NS
;; ANSWER SECTION:
pacific.edu.            7858    IN      NS      ns2.pacific.edu.
pacific.edu.            7858    IN      NS      ns1.pacific.edu.
;; ADDITIONAL SECTION:
ns1.pacific.edu.        13465   IN      A       138.9.1.21
ns2.pacific.edu.        64051   IN      A       138.9.1.22
;; Query time: 2 msec
;; SERVER: 10.0.0.2#53(10.0.0.2)
;; WHEN: Wed Oct 24 22:36:45 2012
;; MSG SIZE  rcvd: 97
```

# dig mx pacific.edu

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17615
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 2, ADDITIONAL: 2
;; ANSWER SECTION:
pacific.edu.          3547    IN      MX      10 mx30.pacific.edu.
pacific.edu.          3547    IN      MX      10 mx10.pacific.edu.
pacific.edu.          3547    IN      MX      10 mx20.pacific.edu.
;; AUTHORITY SECTION:
pacific.edu.          8101    IN      NS      ns1.pacific.edu.
pacific.edu.          8101    IN      NS      ns2.pacific.edu.
;; ADDITIONAL SECTION:
ns1.pacific.edu.      13708   IN      A       138.9.1.21
ns2.pacific.edu.      64294   IN      A       138.9.1.22
;; Query time: 3 msec
;; SERVER: 10.0.0.2#53(10.0.0.2)
;; WHEN: Wed Oct 24 22:32:42 2012
;; MSG SIZE  rcvd: 160
```

# dix mx pacific.edu (now)

```
mmaxwell@Jammy:~$ dig mx pacific.edu

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> mx pacific.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42735
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;pacific.edu.                   IN      MX

;; ANSWER SECTION:
pacific.edu.            60      IN      MX      0 pacific-edu.mail.protection.outlook.com.

;; AUTHORITY SECTION:
pacific.edu.            453     IN      NS      ns-110.awsdns-13.com.
pacific.edu.            453     IN      NS      ns-2044.awsdns-63.co.uk.
pacific.edu.            453     IN      NS      ns-1289.awsdns-33.org.
pacific.edu.            453     IN      NS      ns-705.awsdns-24.net.

;; ADDITIONAL SECTION:
ns-110.awsdns-13.com.   24514   IN      A       205.251.192.110
ns-110.awsdns-13.com.   139792  IN      AAAA    2600:9000:5300:6e00::1
ns-705.awsdns-24.net.   129353  IN      A       205.251.194.193
ns-705.awsdns-24.net.   139741  IN      AAAA    2600:9000:5302:c100::1
ns-1289.awsdns-33.org.  134158  IN      A       205.251.197.9
ns-2044.awsdns-63.co.uk. 139754 IN      A       205.251.199.252

;; Query time: 39 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Aug 10 12:21:17 PDT 2022
;; MSG SIZE  rcvd: 352
```

# dig

- Trace dig's path

  dig pacific.edu +trace

- SOA Information

  dig pacific.edu +nssearch

  SOA ns1.pacific.edu. hostmaster.pacific.edu.
  2012100803 1200 3600 604800 86400
  from server ns1.pacific.edu in 69 ms.

We will come back to this set of numbers later

# whois pacific.edu

Domain Name: PACIFIC.EDU

Registrant:

University of the Pacific
3601 Pacific Avenue
Stockton, CA 95211
UNITED STATES

Administrative Contact:

Server Group - Office of Information Technology
University of the Pacific
3601 Pacific Avenue
Stockton, CA 95211
UNITED STATES
(209) 946-2251
dnsadmin@pacific.edu

Technical Contact:

Server Group - Office of Information Technology
University of the Pacific
3601 Pacific Avenue
Stockton, CA 95211
UNITED STATES
(209) 946-2251
dnsadmin@pacific.edu

Name Servers:

NS1.PACIFIC.EDU 138.9.1.21
NS2.PACIFIC.EDU 138.9.1.22

Domain record activated: 23-Jul-1992
Domain record last updated: 12-Jul-2006
Domain expires: 31-Jul-2013

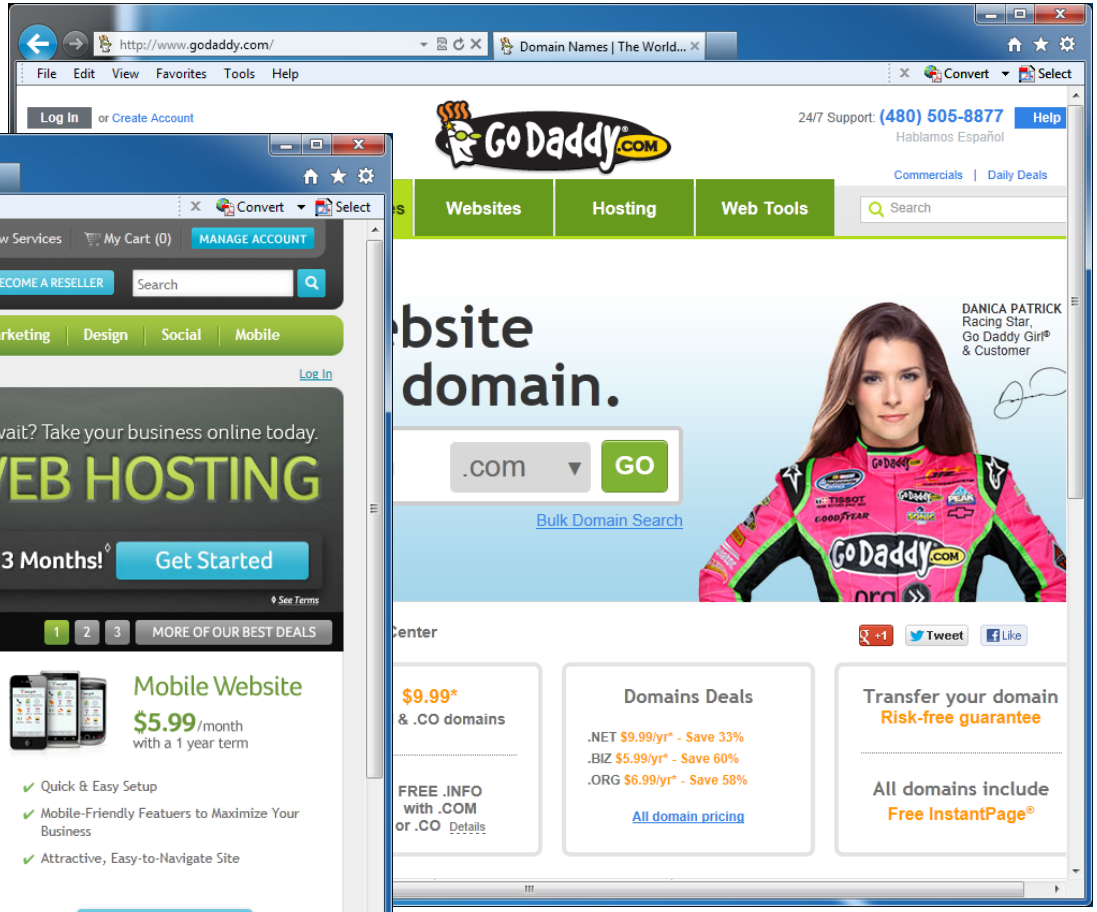
# whois pacific.edu

```
Domain Name: PACIFIC.EDU

Registrant:
        University of the Pacific
        3601 Pacific Avenue
        Stockton, CA 95211
        USA

Administrative Contact:
        Domain Admin
        University of the Pacific
        3601 Pacific Avenue
        Stockton, CA 95211
        USA
        +1.2099462251
        dnsadmin@pacific.edu
```

```
Technical Contact:

        University of the Pacific
        3601 Pacific Avenue
        Stockton, CA 95211
        USA
        +1.2099462251
        dnsadmin@pacific.edu

Name Servers:
        NS-110.AWSDNS-13.COM
        NS-1289.AWSDNS-33.ORG
        NS-2044.AWSDNS-63.CO.UK
        NS-705.AWSDNS-24.NET

Domain record activated:    23-Jul-1992
Domain record last updated: 22-Jun-2022
Domain expires:             31-Jul-2023
```

# DNS Configuration

- It starts with a domain

# Inserting Records

- Example: new startup “Network Utopia”
- Register name networkuptopia.com at DNS registrar (e.g., Network Solutions)
  - Provide names, IP addresses of authoritative name server (primary and secondary)
  - Registrar inserts two RRs into com TLD server: (one shown)

```
(networkutopia.com, dns1.networkutopia.com, NS)
(dns1.networkutopia.com, 212.212.212.1, A)
```

- Create authoritative server Type A record for www.networkuptopia.com; Type MX record for networkutopia.com

# DNS Configuration

- named daemon is used for ISC BIND
- A DNS Server may be caching/master/slave server
  - root.server file has data for all Root Servers.
  - Forward Zone file for every domain.
  - Reverse Zone file for every domain.
  - Configuration file:

    /etc/named.conf

# DNS Configuration

```
// A nameserver config for bind 9
//
acl "bogon" {
    // Filter out the bogon networks  - RFC1918 Caution
    0.0.0.0/8;
    1.0.0.0/8;                    Addresses in CIDR notation
    10.0.0.0/8;
    169.254.0.0/16;
    172.16.0.0/12;
    192.168.0.0/16;
    223.0.0.0/8;
    224.0.0.0/3;
}
```

# DNS Configuration

```
options {
        directory "/var/named";
        version "None of your business";
        query-source address * port 53;
        statistics-file "/var/named/named.stats";
        blackhole {
                // Deny anything from the bogon networks ACL
               bogon;
               };
        zone-statistics yes;
        forwarders {
                206.13.31.12;          The ISP's DNS servers
                206.13.28.12;
                };
         };
```

# DNS Configuration

```
view "internal" {
        match-clients { 10.0.0.0/8; };
        recursion yes;
        zone "." {
                type hint;
                file "root.servers";
                };
        zone "localhost" {
                type master;
                file "pri.localhost";
                };
        zone "0.0.127.in-addr.arpa" {
                type master;
                file "localhost.rev";
                };
        zone "treacle.com" {
                type master;
                file "treacle.hosts.internal";
                forwarders { };
                };
```

# DNS Configuration

```
zone "2-7.191.206.63.in-addr.arpa" {
        type master;
        file "treacle.rev.internal";
        forwarders { };
        };
 zone "0.0.10.in-addr.arpa" {
        type master;
        file "private.rev.internal";
        forwarders { };
        };
 };
```

# DNS Configuration

```
view "external" {
        match-clients { any; };
        recursion no;
        zone "." {
                type hint;
                file "root.servers";
                };
        zone "treacle.com" {
                type master;
                file "treacle.hosts";
                };
        zone "2-7.191.206.63.in-addr.arpa" {
                type master;
                file "treacle.rev";
                };
        };
```

# DNS Configuration

```
logging {
        // based on nic
        channel named.log {
                file "/var/log/dns_default.log" versions 2 size 5m;
                severity info;
                print-category yes;
                print-severity yes;
                print-time yes;
                };
            channel dns_queries.log {
                file "/var/log/dns_queries.log" versions 2 size 1m;
                severity info;
                print-time yes;
                };
```

# DNS Configuration

```
  category default {
        named.log;
        };
    category queries {
        dns_queries.log;
        };
};
```

# DNS Configuration

**Sample domain.hosts file**

```
$TTL   3h
treacle.com.    IN      SOA     tea.treacle.com. postmaster.treacle.com. (
                                2012053101      ;serial
                                3h              ;refresh
                                1h              ;retry
                                1w              ;expire
                                1d )            ;negative caching TTL

                IN      NS                      ns.treacle.com.
                IN      MX      10              mail.treacle.com.

                IN      TXT                     "Looking Glass Research"
                IN      HINFO                   "CHRYSALIS" "PRIMOS"

treacle.com.            IN      A       63.206.191.202
www.treacle.com.        IN      A       63.206.191.202
```

# domain.reverse

```
$TTL   3h
@          IN      SOA     tea.treacle.com. postmaster.treacle.com. (
           2011121001      ;serial
           3h              ;refresh
           1h              ;retry
           1w              ;expire
           1h )            ;TTL

            IN      NS      ns.treacle.com.
            IN      NS      ns1.treacle.com.

202         IN      PTR     tea.treacle.com.
```

# rootservers

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers "cache  .  <file>"
;       This file is made available by InterNIC  FTP.INTERNIC.NET
; formerly NS.INTERNIC.NET
.                       3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.     3600000      AAAA  2001:503:BA3E::2:30
;
; FORMERLY NS1.ISI.EDU
.                       3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000      A     192.228.79.201
```

Through G


# 23 October 2013

## First New Generic Top-Level Domains Delegated

# News

- First New Generic Top-Level Domains Delegated
- The Internet Corporation for Assigned Names and Numbers (ICANN) today announced that the first new generic Top-Level Domains (gTLDs) from its New gTLD Program were delegated. This means they were introduced into the Internet's Root Zone, the central authoritative database for the Internet's Domain Name System...

# New gTLDs

- شبكة (xn--ngbc5azd) – Arabic for "web/network"
  - Registry: International Domain Registry Pty. Ltd.
- онлайн (xn--80asehdb) – Cyrillic for "online"
  - Registry: CORE Association
- сайт (xn--80aswg) – Cyrillic for "site"
  - Registry: CORE Association
- 游戏(xn--unup4y) – Chinese for "game(s)"
  - Registry: Spring Fields, LLC

# gTLDs

- aero – air transport
- asia – Asia Pacific
- biz – Business
- cat – Catalan culture
- com – commercial
- coop – cooperatives
- edu – post secondary
- gov – US government
- info – informational
- int – International orgs
- jobs – employment
- mil – US military
- mobi – mobile
- museum – museums
- name – families
- net – network
- org – Organizations
- post – postal
- pro – professional
- tel – telephone
- travel – travel related
- xxx - pornography

# Zone Transfers

- Cone Zone Xfer

# Zone Transfer

- A primary (aka master) server loads the DNS information from the configuration files
- The secondary (aka slave) server(s) load all their information from the primary server
- When the secondary downloads information from the primary, it is called a zone transfer
- The portion of database replicated is a 'zone'
- Uses TCP on port 53
- Information logged via syslog

# Zone Transfer

- Primary server sends NOTIFY when data changes

  and/or

- Secondary server requests based on TTLs
  - Refresh, Retry, Expire fields

◇◇◇◇◇◇

- Secondary server requests a zone transfer from the primary server
  - Compares serial numbers (datestamp)
- Secondary server makes a backup copy of the zone data on disk
- Secondary server uses the new data only after the transfer is completed *atomicity*

# Client DNS Cache

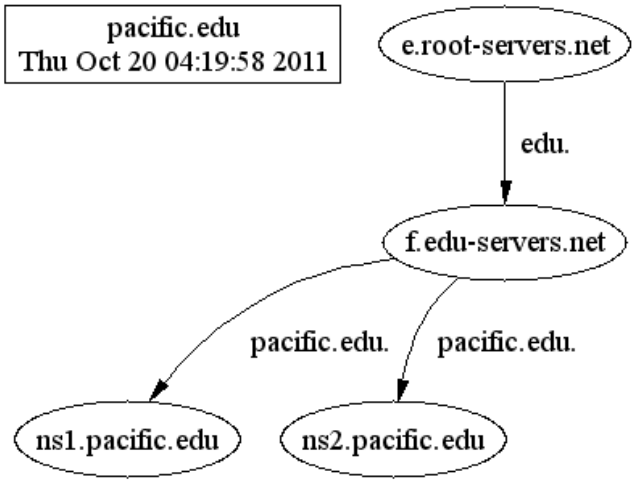
- Microsoft Windows maintains a local cache via the DNS service
- Make sure that service is running
- To see cache: `ipconfig /displaydns`
- To flush cache: `ipconfig /flushdns`

```
entropy.dns-oarc.net
----------------------------------------
Record Name . . . . . : entropy.dns-oarc.net
Record Type . . . . . : 1
Time To Live  . . . . : 942
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 149.20.59.26
```

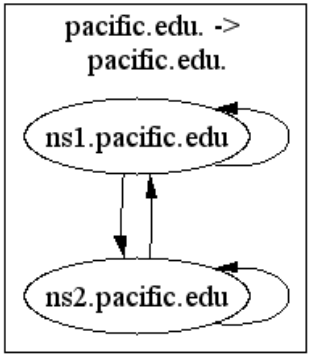
# DNS Configuration

Source of Authority SOA values (seconds)

```
2011101900      ; serial number YYMMDDnn
1200            ; refresh          20 min
3600            ; update retry     1 hour
604800          ; expire           168 hour
86400           ; minimum TTL      24 hour
```




Refresh how often secondary/slave nameservers check with the master for updates.
Retry how long secondary/slave nameservers will wait to contact the master nameserver again if the last attempt failed.




```
Thu Oct 20 04:20:02 UTC 2011
pacific.edu             NS          ns1.pacific.edu
ns1.pacific.edu         hostmaster.pacific.edu (2011101900 1200 3600 604800 86400)
 !!! pacific.edu SOA retry exceeds refresh
pacific.edu             NS          ns2.pacific.edu
ns1.pacific.edu         hostmaster.pacific.edu (2011101900 1200 3600 604800 86400)
```

*A failing refresh would be retried after it is time for the next refresh.*

# DNS Security


# DNS Vulnerabilities

- Implementation Vulnerabilities
  - BIND/Microsoft DNS – buffer overflow
  - CHARGEN stream causes crash
- Inherent Vulnerabilities
  - Protocol weaknesses
  - Host-address mapping provided by DNS is trusted
- Obvious problems
  - Interception of requests
    - Incorrect or malicious responses
  - 0wn3d DNS servers
    - Incorrect or malicious responses
- Mitigation - authenticated requests/responses

# DNS Hijacking / Redirection

## Redirecting via DNS resolution

- By DNS service providers to block access to selected domains as a form of censorship/safety
- By self-serving ISPs to direct users' HTTP traffic to the ISP's own webservers where advertisements are served (pay-per-view), statistics collected, marketing done
  - Example: 404 responses (next slide)
  - Example: Parked domains (next slide)
- For malicious purposes such as phishing

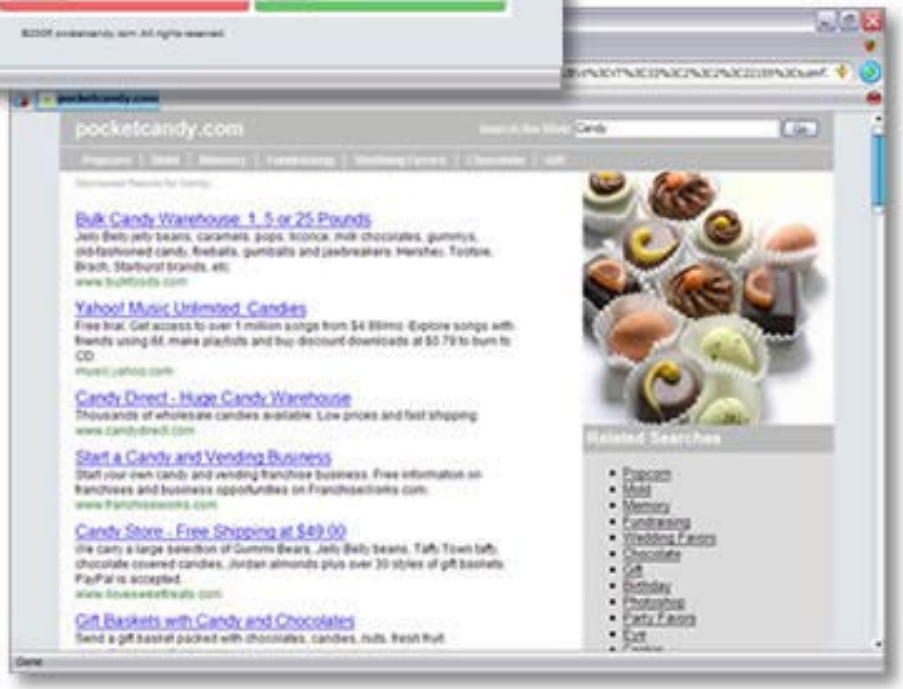
# DNS Hijacking / Redirection

- Typosquatting
  - goggle.com - spyware infector (next slide)
  - whitehouse.com - pr0n
- Gripe/Hate sites
  - www.martinlutherking.org (KKK)
- Expired domains - parked domain monetization
- Type-in traffic from search strings entered in the browser address bar (significant volume)
- Redirecting 404s

# DNS Hijacking/Redirection

- In August 2010, Google filed a complaint with the National Arbitration Forum to obtain the domain names:
  - goggle.com **(don’t visit these)**
  - goggle.net
  - goggle.org
- On October 12, 2011, the organization dismissed Google's complaint
- Current business/legal framework is not up to the challenges/problems of the Internet

# Parked Domains

# Pharming

- Changing IP addresses to redirect URLs to fraudulent sites
  - By exploiting a DNS server vulnerability
  - DNS settings on unsecured wireless routers
  - By altering the hosts file on victim's computer
    - Redirect AV, search, patch, etc. URL's
- Potentially more dangerous than phishing attacks
- No email solicitation is required (phishing)

# DNS Security

Notable Pharming attacks:

- January 2008 – Drive-by javascript attack targeting a Mexican bank
- January 2005 - domain name for large New York ISP Panix was hijacked to a site in Australia.
- November 2004 - Google and Amazon users were sent to Med Network Inc. online pharmacy
- March 2003 - group called "Freedom Cyber Force Militia" hijacked visitors to Al-Jazeera Web site and presented them with the message "God Bless Our Troops"

# DNS Cache Poisoning

- When a DNS server has received and cached false (poisoned) DNS data used to redirect users to malicious websites
- Multiple techniques used to load malicious IP-address information into legitimate DNS servers
- Removes the need to trick a user into visiting a malicious website since the malicious IP-address is provided by a legitimate DNS server
- Countermeasures
  - Update older resolvers
  - DNSsec

# DNS Cache Poisoning

- DNS resource records (see RFC 1034)
  - An “A” record supplies a host IP address
  - A “NS” record supplies name server for domain
- Example
  - www.evil.org NS ns.yahoo.com /delegate to yahoo
  - ns.yahoo.com A 1.2.3.4 / address for yahoo
- Result
  - If resolver looks up www.evil.org, then evil name server will give resolver address 1.2.3.4 for yahoo
  - Lookup yahoo through cache goes to 1.2.3.4

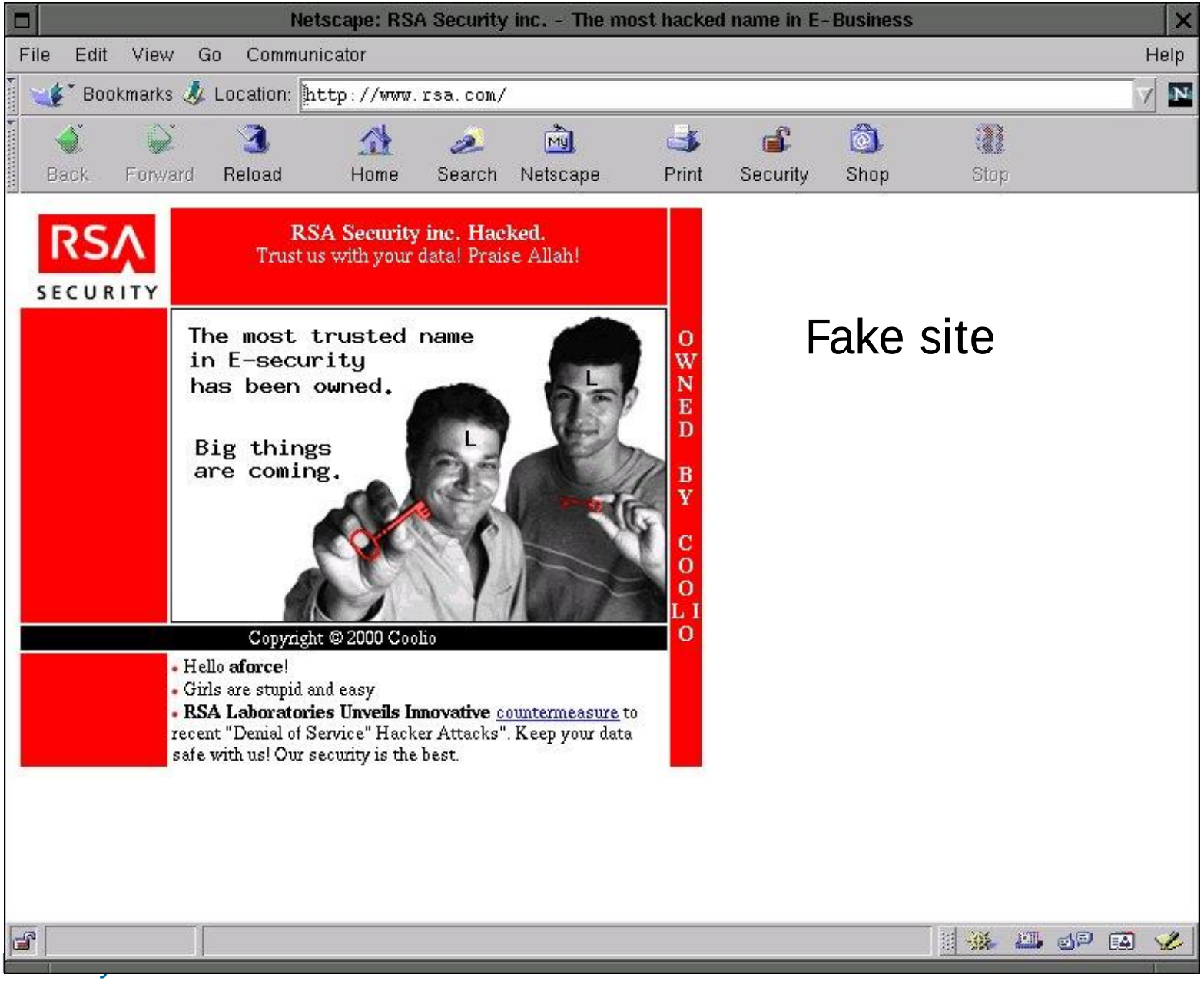
# Dec. 2009 - DNS Attack

Twitter's DNS records were altered by someone using valid twitter login credentials.


# DNS "Defacement"

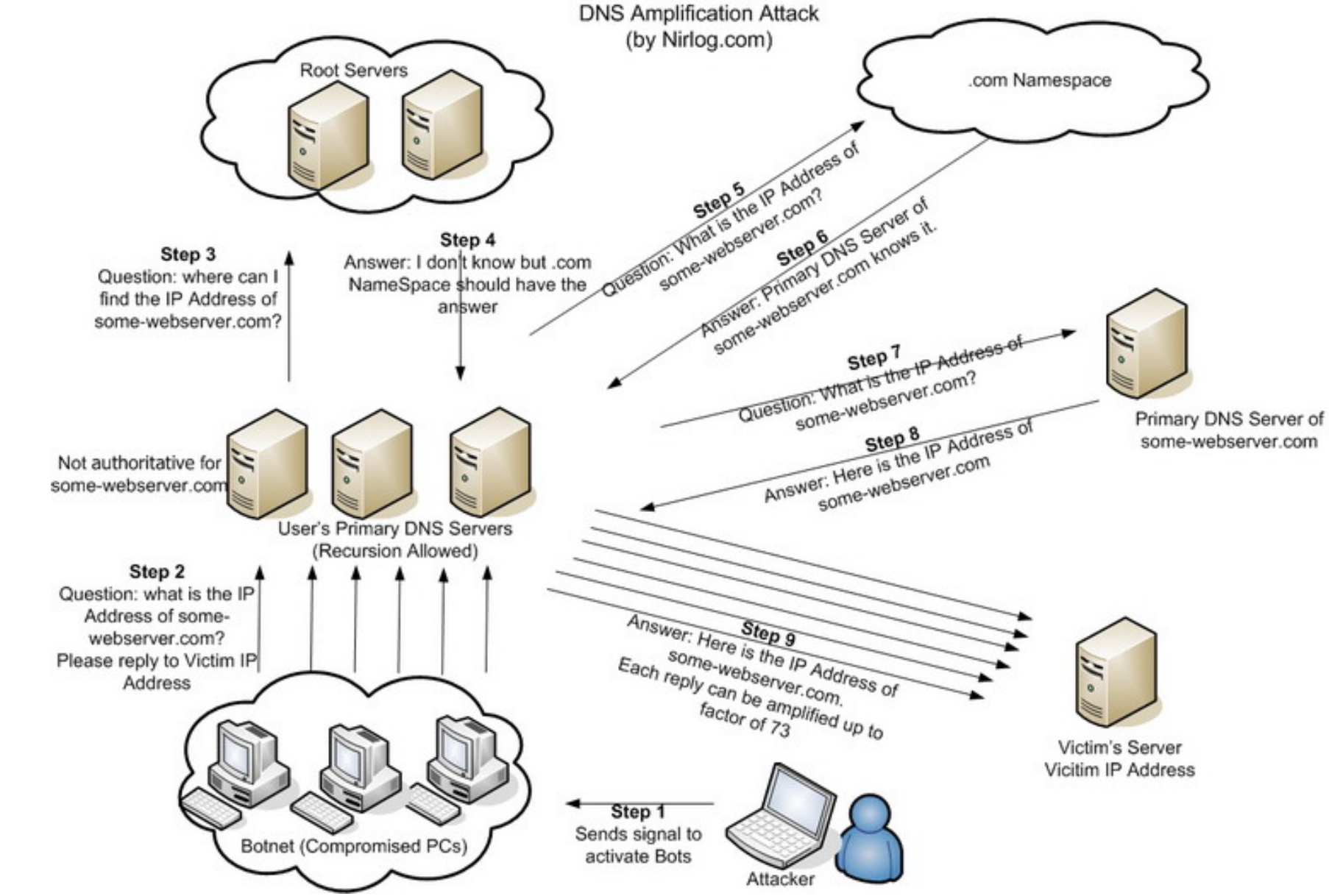
Real site

# DNS "Defacement"




Fake site

# DNS Amplification Attack



# DDoS Attempt

14-Oct-2011 14:38:33.654 security: info: client 24.8.5.151#53: view external: query (cache) './ANY/IN' denied

c-24-8-5-151.hsd1.co.comcast.net.

14-Oct-2011 17:05:31.094 security: info: client 69.73.170.241#53: view external: query (cache) './ANY/IN' denied

static-241-170-73-69.nocdirect.com. Fulshear, Texas

;; MSG SIZE rcvd: **359** (**~60** byte query)

abstechs.com, delgadolawoffices.com, ranchopower.com, revealip.com, utvdubs.com, **voogru.com**, xtremeracingcats.com

online gameing community – team fortress, half life, etc.

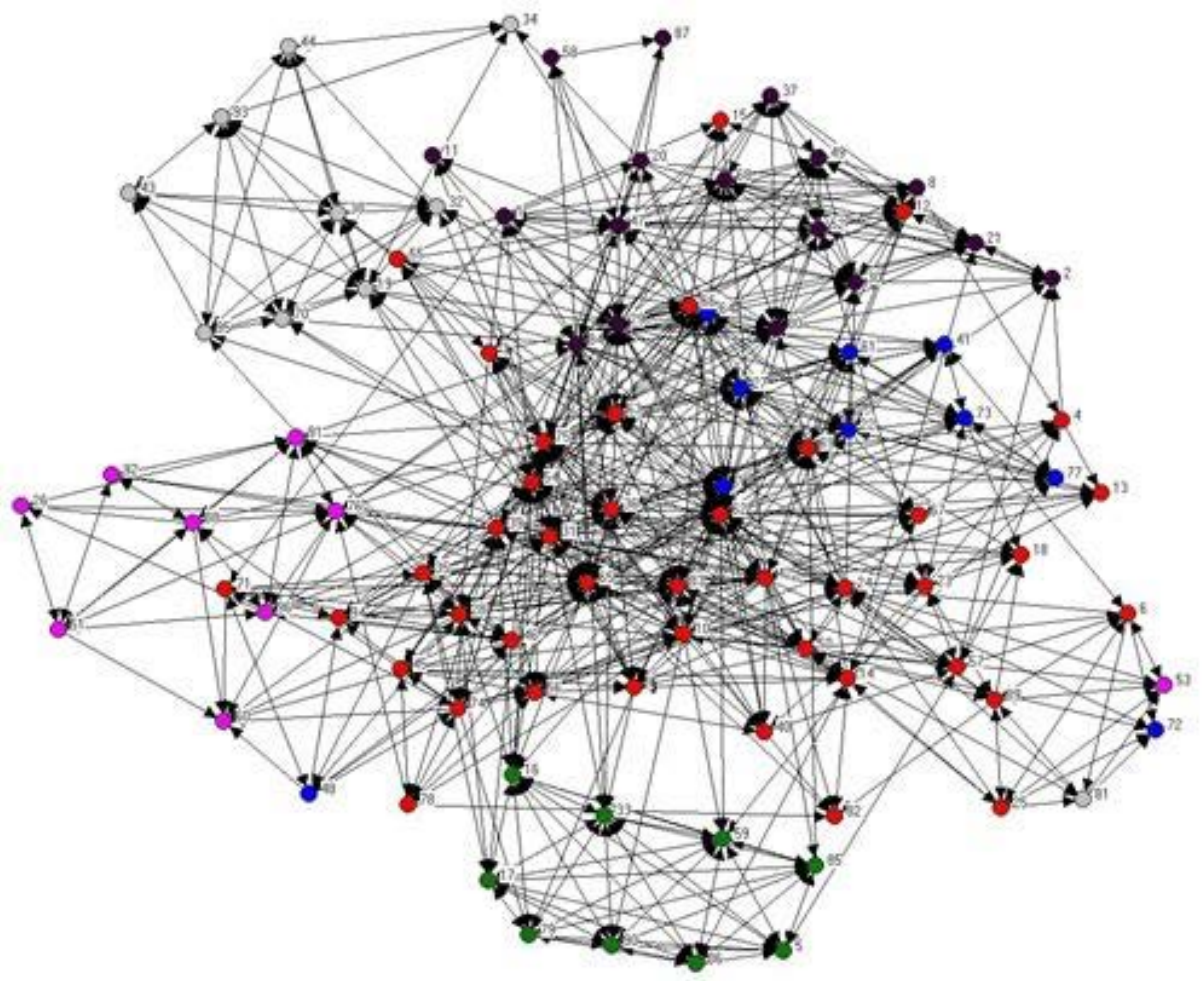
Actual source address is spoofed – the client is the intended target


# Pacific Traceroute DNS Wart

Authoritative?!

# Anomaly

## Network Analysis Time

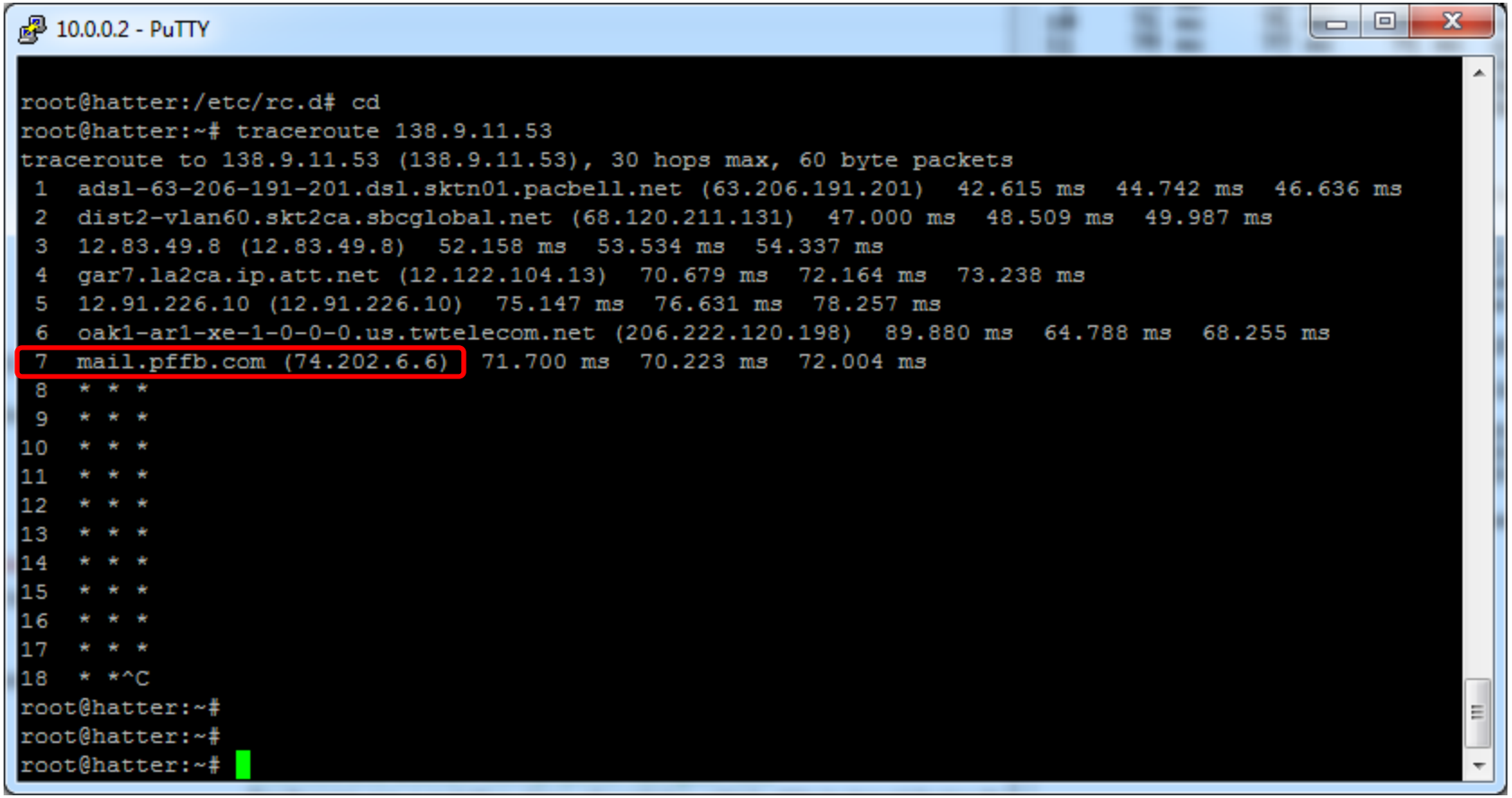


Anomaly

**DEVIATION OR DEPARTURE FROM THE NORMAL OR COMMON ORDER, FORM, OR RULE.**

**SYN: ABNORMALITY, DEVIATION, ECCENTRICITY, EXCEPTION, IRREGULARITY, RARITY.**

# Route To Pacific




Traceroute on a Linux host

74.202.6.6 presumed to be last hop prior to Pacific's network
TimeWarner Telecom routes Pacific's traffic to mail.pffb.com
mail.pffb.com then routes the traffic to Pacific?

# Route To Pacific

```
C:\tachyon>tracert 138.9.11.53

Tracing route to uop-11-53.pacific.edu [138.9.11.53]
over a maximum of 30 hops:

  1     1 ms     <1 ms     <1 ms  hatter.treacle.com [10.0.0.2]
  2    47 ms     43 ms     44 ms  adsl-63-206-191-201.dsl.sktn01.pacbell.net [63.206.191.201]
  3    42 ms     42 ms     43 ms  dist2-vlan60.skt2ca.sbcglobal.net [68.120.211.131]
  4    42 ms     42 ms     43 ms  12.83.49.8
  5    57 ms     58 ms     57 ms  gar7.la2ca.ip.att.net [12.122.104.13]
  6    56 ms     67 ms     58 ms  12.91.226.10
  7    66 ms     66 ms     66 ms  oak1-ar1-xe-1-0-0-0.as.twtelecom.net [206.222.120.198]
  8    71 ms     70 ms     69 ms  mail.pffb.com [74.202.6.6]
  9    73 ms     72 ms     71 ms  uop-11-53.pacific.edu [138.9.11.53]
 10    71 ms     75 ms     75 ms  uop-11-53.pacific.edu [138.9.11.53]
 11    79 ms     77 ms     71 ms  uop-11-53.pacific.edu [138.9.11.53]
 12     *         *         *     Request timed out.
 13     *         *         *     Request timed out.
 14     *         *         *     Request timed out.
 15   ^C
```

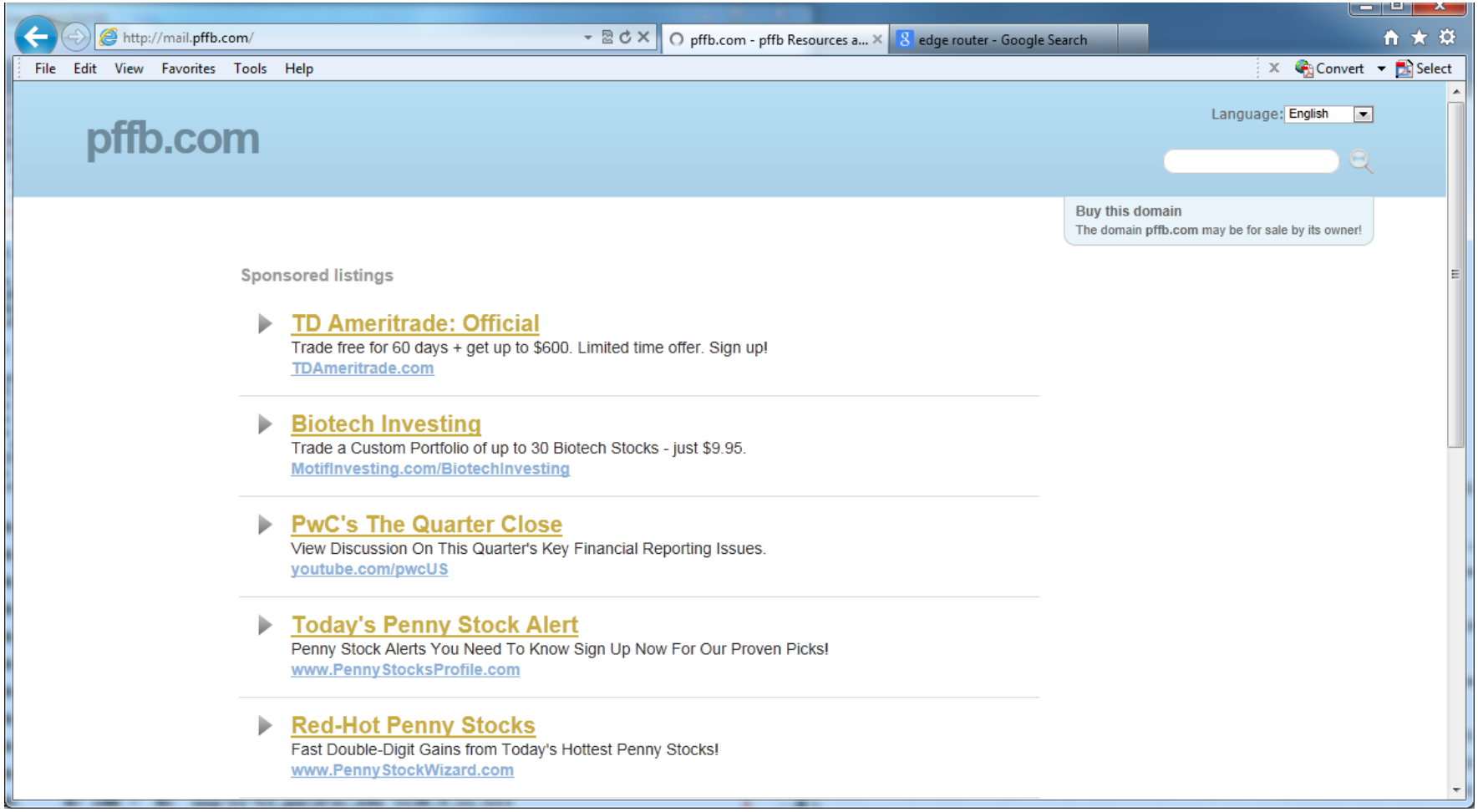
Tracert on a Windows 7 host

# Route To Pacific

```
C:\tachyon>pathping 138.9.11.53

Tracing route to uop-11-53.pacific.edu [138.9.11.53]
over a maximum of 30 hops:
  0  MarchHare.treacle.com [10.0.0.5]
  1  hatter.treacle.com [10.0.0.2]
  2  adsl-63-206-191-201.dsl.sktn01.pacbell.net [63.206.191.201]
  3  dist2-vlan60.skt2ca.sbcglobal.net [68.120.211.131]
  4  12.83.49.8
  5  gar7.la2ca.ip.att.net [12.122.104.13]
  6  12.91.226.10
  7  oak1-ar1-xe-1-0-0-0.us.twtelecom.net [206.222.120.198]
  8  mail.pffb.com [74.202.6.6]
  9  uop-11-53.pacific.edu [138.9.11.53]
 10  uop-11-53.pacific.edu [138.9.11.53]
 11  uop-11-53.pacific.edu [138.9.11.53]
 12     *        *        *
Computing statistics for 275 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           MarchHare.treacle.com [10.0.0.5]
                                     0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%      0/ 100 =  0%  hatter.treacle.com [10.0.0.2]
                                     0/ 100 =  0%   |
  2   44ms     0/ 100 =  0%      0/ 100 =  0%  adsl-63-206-191-201.dsl.sktn01.pacbell.net [63.206.191.201]
                                     0/ 100 =  0%   |
  3   ---    100/ 100 =100%    100/ 100 =100%  dist2-vlan60.skt2ca.sbcglobal.net [68.120.211.131]
                                     0/ 100 =  0%   |
  4   ---    100/ 100 =100%    100/ 100 =100%  12.83.49.8
                                     0/ 100 =  0%   |
  5   ---    100/ 100 =100%    100/ 100 =100%  gar7.la2ca.ip.att.net [12.122.104.13]
                                     0/ 100 =  0%   |
  6   59ms     0/ 100 =  0%      0/ 100 =  0%  12.91.226.10
                                     0/ 100 =  0%   |
  7   71ms     0/ 100 =  0%      0/ 100 =  0%  oak1-ar1-xe-1-0-0-0.us.twtelecom.net [206.222.120.198]
                                     0/ 100 =  0%   |
  8   69ms     0/ 100 =  0%      0/ 100 =  0%  mail.pffb.com [74.202.6.6]
                                     0/ 100 =  0%   |
  9   74ms     0/ 100 =  0%      0/ 100 =  0%  uop-11-53.pacific.edu [138.9.11.53]
                                     0/ 100 =  0%   |
 10   75ms     0/ 100 =  0%      0/ 100 =  0%  uop-11-53.pacific.edu [138.9.11.53]
                                     0/ 100 =  0%   |
 11   74ms     0/ 100 =  0%      0/ 100 =  0%  uop-11-53.pacific.edu [138.9.11.53]

Trace complete.
```

pathping on a Windows 7 host

# http:///mail.pffb.com




Generally – going there is not a good practice. Use a text browser like Lynx. It's a 'Parked Domain'

# Parked Domain? Wot?

- In this example – An expired domain that resolves to a page of ad links predicted to be similar to what the viewer was looking for.

- Pakistan Foundation Fighting Blindness  is .org
- pffb may have been a financial company.
- PFF Bancorp, Inc.  Pomona CA.
  - Class action lawsuit for Securities Fraud
  - (Reuters) - Creditors of failed savings and loan PFF Bancorp Inc (PFFBQ.PK) ..... **dated 2008**

# dig command

10.0.0.2 - PuTTY

```
root@hatter:~# dig -x 74.202.6.6

; <<>> DiG 9.7.3 <<>> -x 74.202.6.6
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47359
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 6, ADDITIONAL: 0

;; QUESTION SECTION:
;6.6.202.74.in-addr.arpa.       IN      PTR

;; ANSWER SECTION:
6.6.202.74.in-addr.arpa. 6796   IN      PTR     mail.pffb.com.

;; AUTHORITY SECTION:
in-addr.arpa.           135941  IN      NS      c.in-addr-servers.arpa.
in-addr.arpa.           135941  IN      NS      d.in-addr-servers.arpa.
in-addr.arpa.           135941  IN      NS      a.in-addr-servers.arpa.
in-addr.arpa.           135941  IN      NS      b.in-addr-servers.arpa.
in-addr.arpa.           135941  IN      NS      f.in-addr-servers.arpa.
in-addr.arpa.           135941  IN      NS      e.in-addr-servers.arpa.

;; Query time: 2 msec
;; SERVER: 10.0.0.2#53(10.0.0.2)
;; WHEN: Tue Oct 16 21:01:16 2012
;; MSG SIZE  rcvd: 180

root@hatter:~#
```

The DNS Response is authoritive – according to six of the root servers.

# dig we must

A dig from Level3 in Dallas for mail.pffb.com:

IP address: 82.98.86.178

Host name: mail.pffb.com

Alias: mail.pffb.com

82.98.86.178 also resolved to sedoparking.com

82.98.86.178 is in Germany(DE) near Frankfurt

# whois at network-tools.com

Whois from network-tools.com

Domain Name: PFFB.COM
Registrar: GODADDY.COM, LLC
Whois Server: whois.godaddy.com
Referral URL: http://registrar.godaddy.com
Name Server: NS1.SEDOPARKING.COM
Name Server: NS2.SEDOPARKING.COM
Status: clientDeleteProhibited
Status: clientRenewProhibited
Status: clientTransferProhibited
Status: clientUpdateProhibited
Updated Date: 12-aug-2011
Creation Date: 03-feb-1998
Expiration Date: 02-feb-2013

>>> Last update of whois database: Tue, 16 Oct 2012 06:40:27 UTC <<<

# whois at arin.net

Whois query for 74.202.6.6... Results returned from whois.arin.net:
NetRange: 74.202.0.0 - 74.203.255.255
CIDR: 74.202.0.0/15
OriginAS:
NetName: TWTC-NETBLK-9
NetHandle: NET-74-202-0-0-1
RegDate: 2006-11-14
Updated: 2012-02-24
Ref: http://whois.arin.net/rest/net/NET-74-202-0-0-1

OrgName: tw telecom holdings, inc.
OrgId: TWTC
RegDate: 1999-03-17
Updated: 2008-10-04
Ref: http://whois.arin.net/rest/org/TWTC

ReferralServer: rwhois://rwhois.twtelecom.net:4321

# Bad Data

- Bad DNS records for a device that is the routing hop adjacent to the University?
- Been there for a while
- It's a twtelecom problem
  - However - if exploited – Pacific gets the pain
  - Remember 'fate sharing' – slide 6

- This is not a best practice
  - Understatement
  - Exploiting could divert traffic to...

# SOMEWHERE ELSE?

# Objectives Met

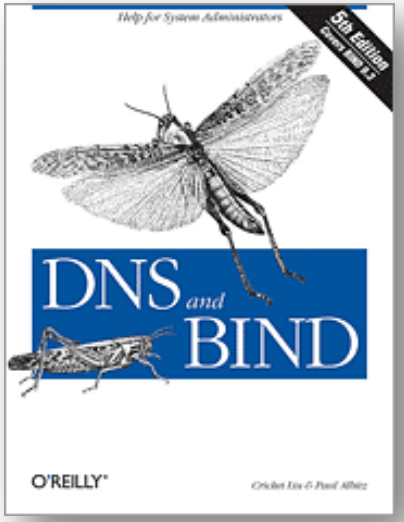
- Understanding of the Domain Name Service
- History and Evolution
- How DNS Functions
- DNS Configuration
- Importance of Accuracy
- Security Issues

# Not Covered

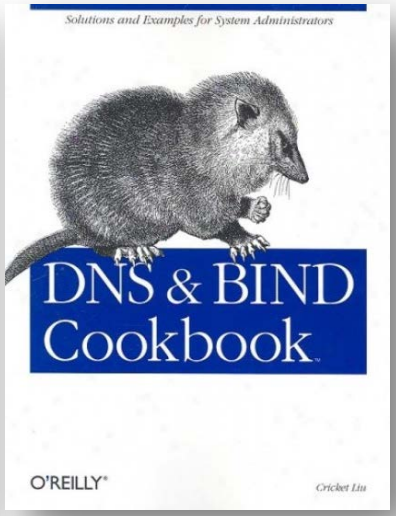
- Active Directory
  - Microsoft directory service
  - Dynamic DNS (DDNS) an integral part of AD

# References

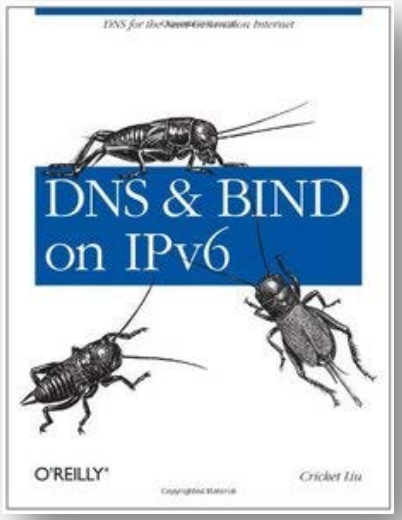
- DNS and BIND 5th Edition
  by Cricket Liu and Paul Albitz




- DNS & BIND Cookbook
  by Cricket Liu




- DNS and BIND on IPv6
  by Cricket Liu



# Additional References

- Punycode Translator

  https://www.charset.org/punycode.php
- Geolocate IP Addresses

  https://www.geolocation.com/
- DNS reading

  https://dnsinstitute.com/documentation/dns-essentials-book/

# Remember (1)

- DNS: Domain Name Service
- A (1)hierarchical (2)distributed naming system for computers, services, or any resource connected to the Internet or a private network
- DNS provides the translation function between the two Internet namespaces:
  - The domain name hierarchy
  - The Internet Protocol (IP) address space
  - It *Resolves* domain names to IP addresses
- DNS replaced a central hosts.txt file
  - Local hosts.txt file still used today
  - windows/system32/drivers/etc/hosts.txt
- Default UDP port 53
- FQDN – Fully.Qualified.Domain.Name. vs. dotted-quad xxx.xxx.xxx.xxx
- Right-most label is the Top Level Domain (TLD)

# Remember (2)

- Internet Corporation for Assigned Names and Numbers ICANN (Policy)
- Internet Assigned Numbers Authority IANA (Technical)
- Regional Internet Registries
  - AfriNIC.net African Internet Address Registry
  - APNIC.net Asian Pacific Internet Address Registry
  - ARIN.net American Registry for Internet Numbers
  - LACNIC.net Latin American and Caribbean Internet Address Registry
  - RIPE.net Réseaux IP Européens

If it is highlighted – know it.