It's Always DNS®

Pam Lefkowitz
Core Computing Technologies, Inc.
pam@corecomputing.com
@alwaysdns

What is DNS?

(the boring definition)

- Domain Name Service
- Hierarchical distributed naming system for computers, services, and resources connected to the Internet

What is DNS?

(the practical definition)

- I go to the the Signature Room at 95th, not 875 N. Michigan Ave, Chicago, IL 60611
- I call Ben Greiner, not (555) 555-1212
- I go to www.corecomputing.com, not 198.187.29.21

Bonjour Won't Work With...

- Email
- Web Sites
- Apple Push Notifications
- AD Binding
- Anything not on the local subnet

How DNS Works

http://www.apple.com

Magic

What's My DNS?

DNS registrars have a whois form

pam$ whois example.com

Registration information
Contact information
Name Servers
Creation and expiration dates

Who's Who and What's What

- NS - Declares name servers for a given domain.
- A - the IP address for an FQDN (www.apple.com).
- CNAME - Points to an A record.
- MX - A record where mail should be delivered.
- TXT - Facts about the domain.
- SRV - Advanced way to define services

Start of Authority (SOA)

Defines the DNS server or servers that are authoritative for the domain

```
pam$ dig rocketsciencesimplified.com soa +short
```

```
rocketsciencesimplified.com
```

```
dig @8.8.8.8 rocketsciencesimplified.com soa +short
```

```
ns13.zoneedit.com
```

CD's...er, Records...

- NS
  - `10800 IN **NS** ns13.zoneedit.com.`
  - `10800 IN **NS** ns15.zoneedit.com.`

```
example.com.        10800 IN SOA    example.com. pam.corecomputing.com. (
                            2012010105 ; serial
                            20864      ; refresh (5 hours 47 minutes 44 seconds)
                            3600       ; retry (1 hour)
                            14976      ; expire (4 hours 9 minutes 36 seconds)
                            10800      ; minimum (3 hours)
                            )
                    10800 IN NS         ns13.zoneedit.com.
                    10800 IN NS         ns15.zoneedit.com.
```

CD's...er, Records...

- A Record
  - `files.example.com.  IN  A  1.2.3.4`
  - `mdm.example.com.  IN  A  5.6.7.8`
- AAAA Record
  - `mdm.example.com. IN AAAA fe80::202:b3ff:fe1e:8329`

```
example.com.        10800 IN SOA    example.com. pam.corecomputing.com. (
                                    2012010105 ; serial
                                    20864      ; refresh (5 hours 47 minutes 44 seconds)
                                    3600       ; retry (1 hour)
                                    14976      ; expire (4 hours 9 minutes 36 seconds)
                                    10800      ; minimum (3 hours)
                                    )
                                        10800 IN NS     ns13.zoneedit.com.
                                        10800 IN NS     ns15.zoneedit.com.
files.example.com.                      10800 IN A      1.2.3.4
mdm.example.com.                        10800 IN A      5.6.7.8
mdm.example.com.                        10800 IN AAAA   fe80::202:b3ff:fe1e:8329
```

CD's...er, Records...

- PTR
  - `4.3.2.1.in-addr.arpa.PTR IN 100000 files.example.com.`
  - `8.7.6.5.in-addr.arpa.PTR IN 100000 mdm.example.com.`

```
59.168.192.in-addr.arpa.        10800 IN SOA    3.2.1.in-addr.arpa. pam.3.2.1.in-addr.arpa. (
                                                2012010105 ; serial
                                                86400      ; refresh (1 day)
                                                3600       ; retry (1 hour)
                                                604800     ; expire (1 week)
                                                345600     ; minimum (4 days)
                                                )
                                        10800 IN NS         ns13.zoneedit.com.
4.3.2.1.in-addr.arpa.                   10800 IN PTR        files.example.com.
8.7.6.5.in-addr.arpa.                   10800 IN PTR        mdm.example.com.
```

CD's...er, Records...

- CNAME
  - `www.example.com.  IN  CNAME  files.example.com.`
  - `ftp  IN  CNAME  mdm`

```
example.com.        10800 IN SOA    example.com. pam.corecomputing.com. (
                                    2012010105 ; serial
                                    20864      ; refresh (5 hours 47 minutes 44 seconds)
                                    3600       ; retry (1 hour)
                                    14976      ; expire (4 hours 9 minutes 36 seconds)
                                    10800      ; minimum (3 hours)
                                    )
                                        10800 IN NS          ns13.zoneedit.com.
                                        10800 IN NS          ns15.zoneedit.com.
files.example.com.                      10800 IN A           1.2.3.4
mdm.example.com.                        10800 IN A           5.6.7.8
mdm.example.com.                        10800 IN AAAA        fe80::202:b3ff:fe1e:8329
www.example.com.                        10800 IN CNAME       files.example.com.
ftp                                     10800 IN CNAME       mdm
```

CD's...er, Records...

- MX
  - `example.com. MX 10 files.example.com.`
  - `example.com. MX 30 mdm.example.com.`
- Resource: `http://domainmx.net/mxsetup.shtml`

CD's...er, Records...

```
example.com.        10800 IN SOA    example.com. pam.corecomputing.com. (
                                    2012010105 ; serial
                                    20864      ; refresh (5 hours 47 minutes 44 seconds)
                                    3600       ; retry (1 hour)
                                    14976      ; expire (4 hours 9 minutes 36 seconds)
                                    10800      ; minimum (3 hours)
                                    )
                                        10800 IN NS         ns13.zoneedit.com.
                                        10800 IN NS         ns15.zoneedit.com.
files.example.com.                      10800 IN A          1.2.3.4
mdm.example.com.                        10800 IN A          5.6.7.8
mdm.example.com.                        10800 IN AAAA       fe80::202:b3ff:fe1e:8329
www.example.com.                        10800 IN CNAME      files.example.com.
ftp                                     10800 IN CNAME      mdm

example.com.                IN MX 10    mail.example.com.
example.com.                IN MX 30    mdm.example.camp.
```

CD's...er, Records...

- TXT
  - `example.com. IN  TXT "v-spf1 +mx a:mail.example.com -all"`

```
example.com.          10800 IN SOA    example.com. pam.corecomputing.com. (
                                      2012010105 ; serial
                                      20864      ; refresh (5 hours 47 minutes 44 seconds)
                                      3600       ; retry (1 hour)
                                      14976      ; expire (4 hours 9 minutes 36 seconds)
                                      10800      ; minimum (3 hours)
                                      )
                                        10800 IN      NS          ns13.zoneedit.com.
                                        10800 IN      NS          ns15.zoneedit.com.
files.example.com.                      10800 IN       A          1.2.3.4
mdm.example.com.                        10800 IN       A          5.6.7.8
mdm.example.com.                        10800 IN     AAAA         fe80::202:b3ff:fe1e:8329
www.example.com.                        10800 IN     CNAME        files.example.com.
ftp                                     10800 IN     CNAME        mdm

example.com.          IN MX 10          mail.example.com.
example.com.          IN MX 30          mdm.example.camp.

example.com.          IN TXT            "v-spf1 +mx a:mail.example.com -all"
```

CD's...er, Records...

- SRV
  - Needed for iCal, AddressBook, iChat Service
    - CLI
      - /var/named/db.example.com
  - `_caldav._tcp 86400 IN SRV 0 0 8008 files.example.com.`
  - `_carddavs._tcp 86400 IN SRV 0 1 8443 files.example.com.`
  - `_xmpp-server._tcp 86400 IN SRV 0 1 5269 files.example.com.`
  - `_xmpp-client._tcp 86400 IN SRV 0 1 5222 files.example.com.`
- Resource
  - http://docs.info.apple.com/article.html?path=ServerAdmin/10.6/en/cs4d72c0a5.html

What If My IP Changes

- Public IP Changes
- LAN IP Changes
  - host
  - hostname
  - changeip
  - scutil

March 6, 2013

- Names, domains, and IP addresses have been changed to protect the non-technical

While driving in that mess, my phone rings…

Client: “Pam, we can’t send email.”

Me: “Hmm. Anything else?”

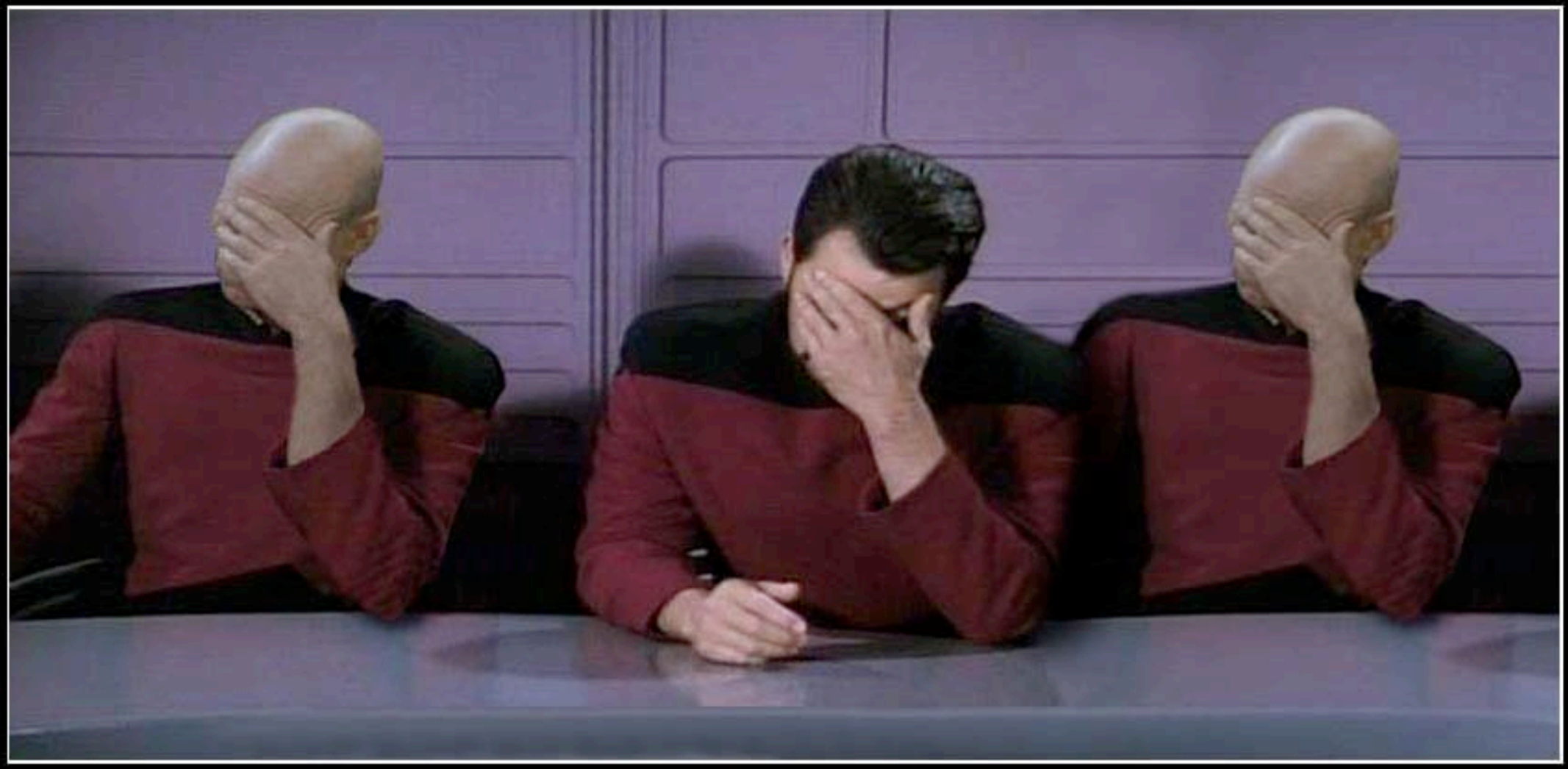
Client: “I have no users.”

Me: “Hmm. What changed?”

Client: “Nothing. Our friend who’s a consultant was fixing a problem with the network.”

Me: “What did he do?”

Client: “He said you had the wrong IP in system preferences so he changed it.”



TRIPLE FACEPALM

When the Fail is so strong, reality starts acting up…

What They Did

- Users are tied to the LDAP domain
- LDAP domain is tied to DNS
- DNS is tied to the IP

What I know

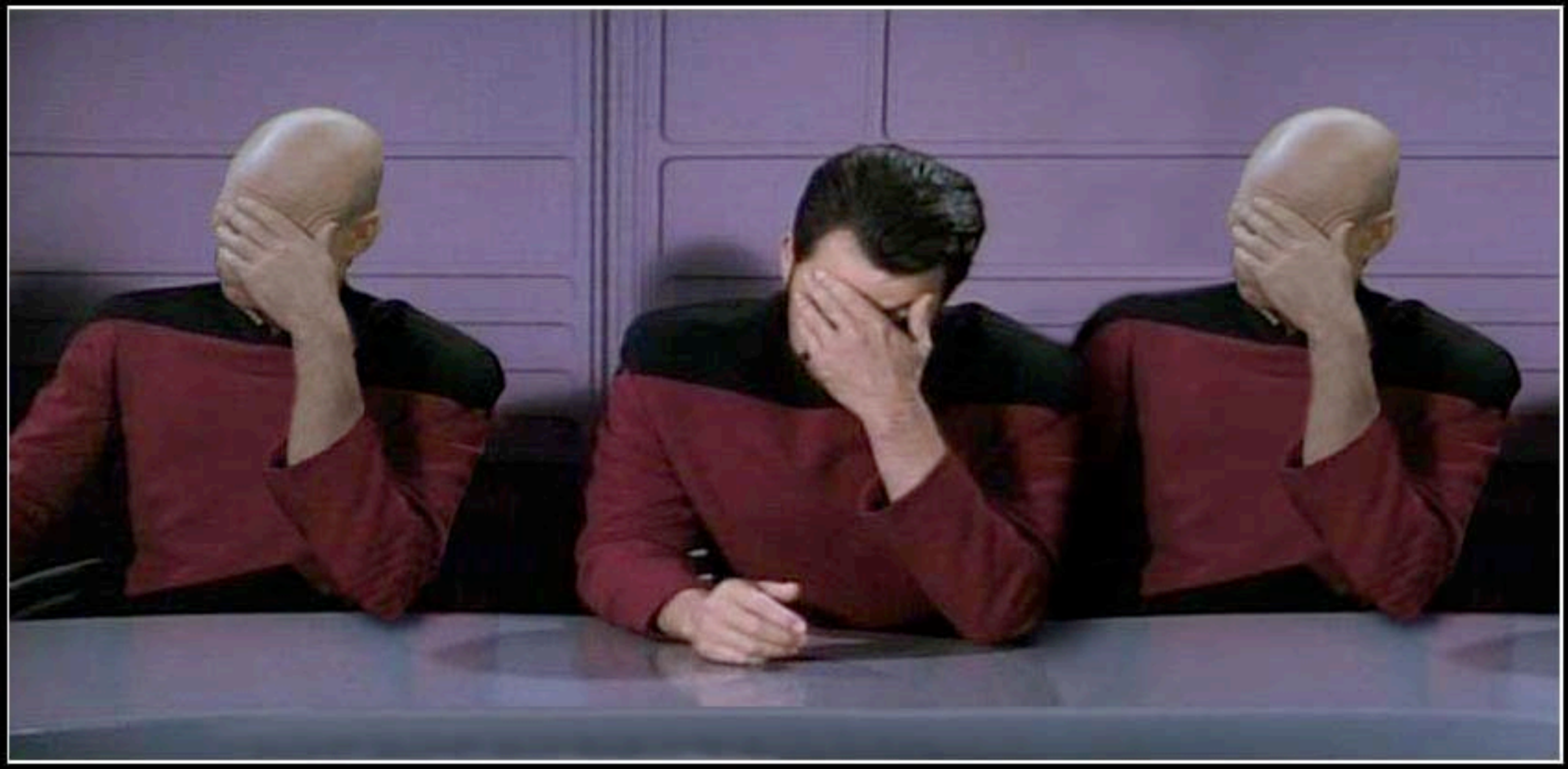
(remember, I'm in the car on a snow-packed road in a blizzard)

- In-house server runs filesharing, email, and VPN services
- Mail server known to be `mail.clientname.com`
- Server behind NAT at some internal IP
- Server has some public IP

Shoot the Trouble

(not the client)

- Can you connect to the internet?
- Is the switch on? Are the cables plugged in?
- Can you connect to the server from inside?
- What's the IP of the server?



TRIPLE FACEPALM

When the Fail is so strong, reality starts acting up…

How I fixed it

From a client computer, use Network Utility

mail.clientname.com

Open Go > Connect to Server

192.168.55.10

Open Network Preference Pane

DNS server = 192.168.55.10

Why Did This Happen?

- The human factor is a factor

  "You were too expensive and he was just going to set up a website. He couldn't VPN. He said you set up the network wrong. He said the server should have a public IP."

Conclusions

- Customer gave up critical management information without understanding intentions or implications.
- The other consultant change critical information without knowing what services were active or the implication of the changes.
- You get what you pay for.

Split-Horizon DNS

- Offer different query results depending on the client that's asking
- Differentiate clients by IP address

Diggin' It

- pam$ dig rocketsciencesimplified.com any

```
rocketsciencesimplified.com.        10800 IN SOA      rocketsciencesimplified.com. pam.corecomputing.com. (
                                    2013041631 ; serial
                                    20864      ; refresh (5 hours 47 minutes 44 seconds)
                                    3600       ; retry (1 hour)
                                    14976      ; expire (4 hours 9 minutes 36 seconds)
                                    10800      ; minimum (3 hours)
                                    )
rocketsciencesimplified.com.        10800      IN        A         192.168.6.100
giles.rocketsciencesimplified.com   10800      IN        A         192.168.6.100
rocketsciencesimplified.com.        10800      IN        SOA       rocketsciencesimplified.com.
rocketsciencesimplified.com.         7200      IN        NS        giles.rocketsciencesimplified.com.
```

Diggin' It

- pam$ dig @8.8.8.8 rocketsciencesimplified.com any

```
rocketsciencesimplified.com.        10800 IN SOA    ns13.zoneedit.com       soacontact.zoneedit.com. (
                                    2013154583 ; serial
                                    300       ; refresh (5 minutes)
                                    300       ; retry (5 minutes)
                                    300       ; expire (5 minutes)
                                    300       ; minimum (5 minutes)
                                    )
rocketsciencesimplified.com. 300    IN      A       76.29.10.221
giles                        300    IN      A       76.29.10.221
rocketsciencesimplified.com. 7200   IN      SOA     ns13.zoneedit.com. soacontact.zoneedit.com. 2013154583 300 300 300 300
rocketsciencesimplified.com. 7200   IN      NS      ns15.zoneedit.com.
rocketsciencesimplified.com. 7200   IN      NS      ns13.zoneedit.com.
rocketsciencesimplified.com. 7200   IN      MX      5 mail.rocketsciencesimplified.com.
```

Which Way Did He Go?

- Built-in tools
  - nslookup
  - dig
  - mDNSResponder
  - Network Utility
  - host/hostname
  - changeip
  - scutil

Public Static IP

- Not Necessary!
- Dynamic DNS Services
  - Providers - Free and Paid
  - Update Clients
  - Other services they provide

Stories From The Front

Pam Lefkowitz
Core Computing Technologies, Inc.
pam@corecomputing.com
@alwaysdns