

# DNS (A War Story)

Chris Dawe  
Wheelwrights, LLC

[www.wheelwrights-llc.com](http://www.wheelwrights-llc.com)

@ctdawe

# What I'm Doing Today

- Exploring DNS by focusing on specific real-world examples of DNS failure and troubleshooting
- Deliberately skirting a lot of abstract detail

# What is DNS?

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

# Why DNS?

Instead of plugging an IP address into Safari,

75.101.132.77

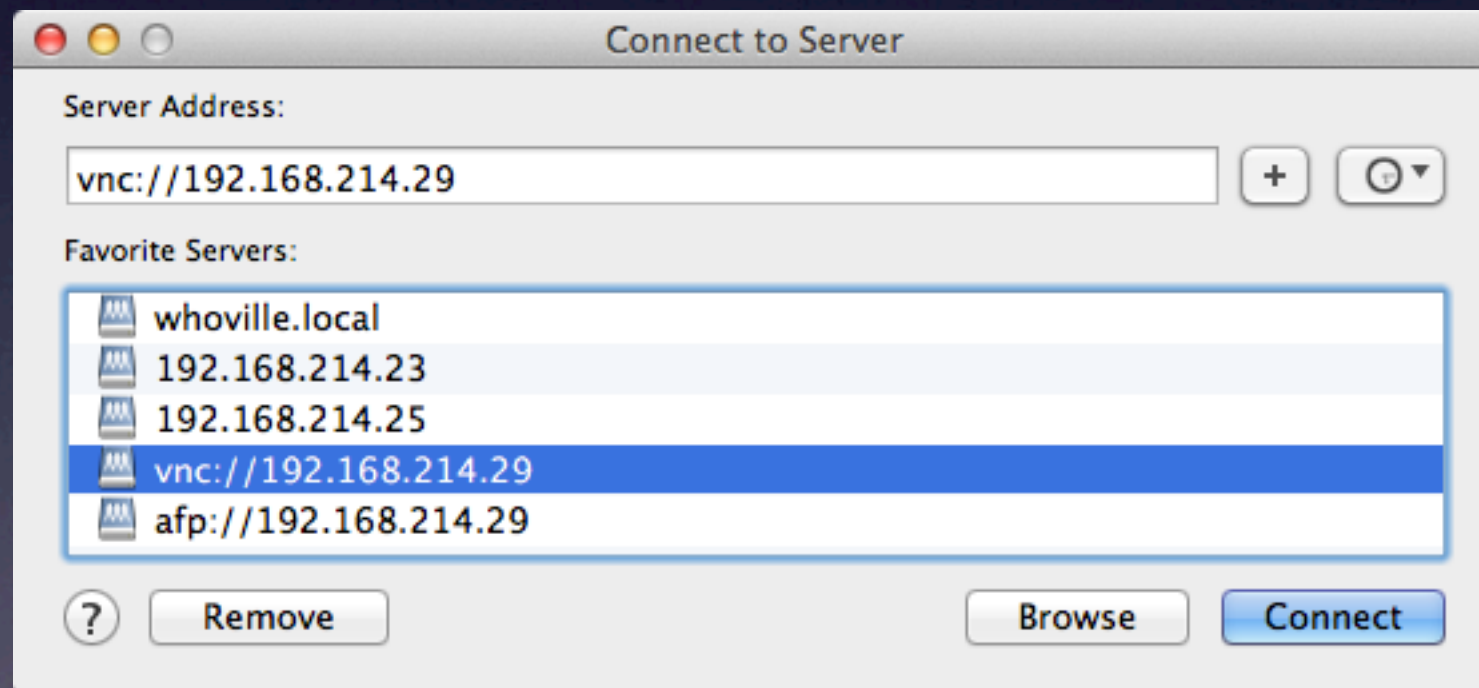
We get to use a name.

www.mactech.com



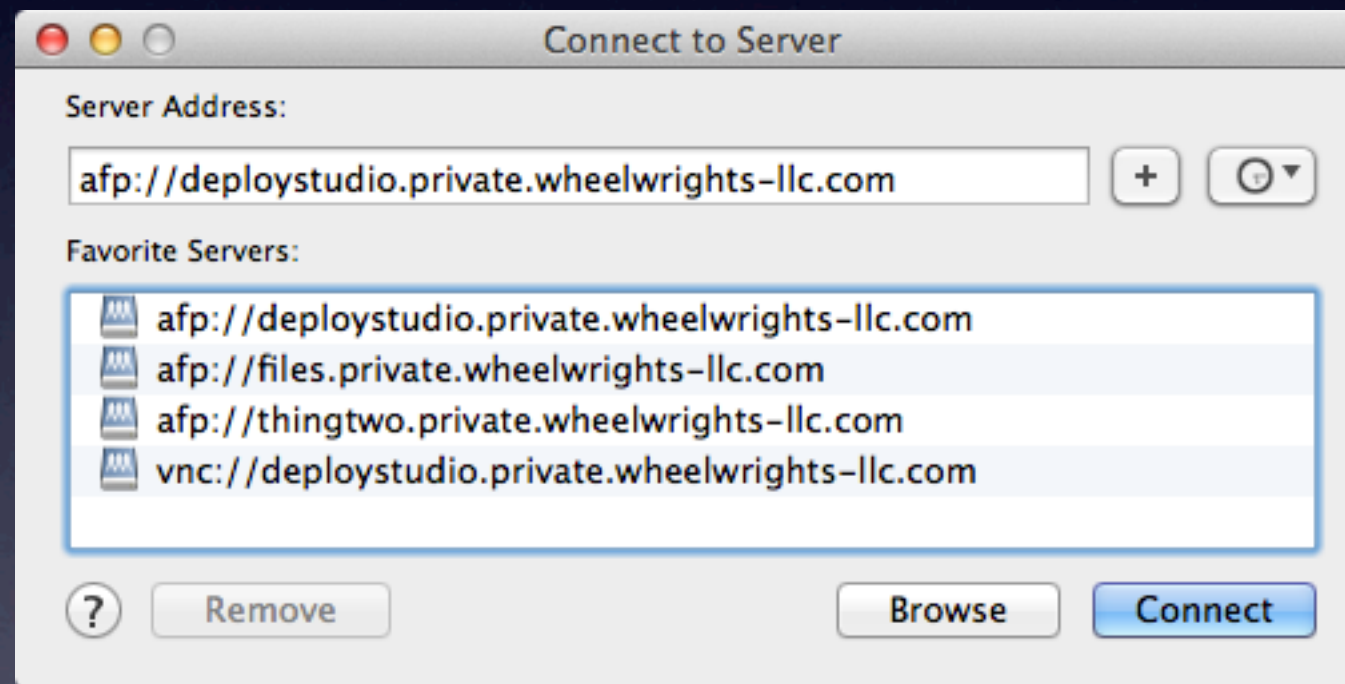
# Why DNS?

Transform the “Connect to Server” dialog from a bunch of ugly numbers:

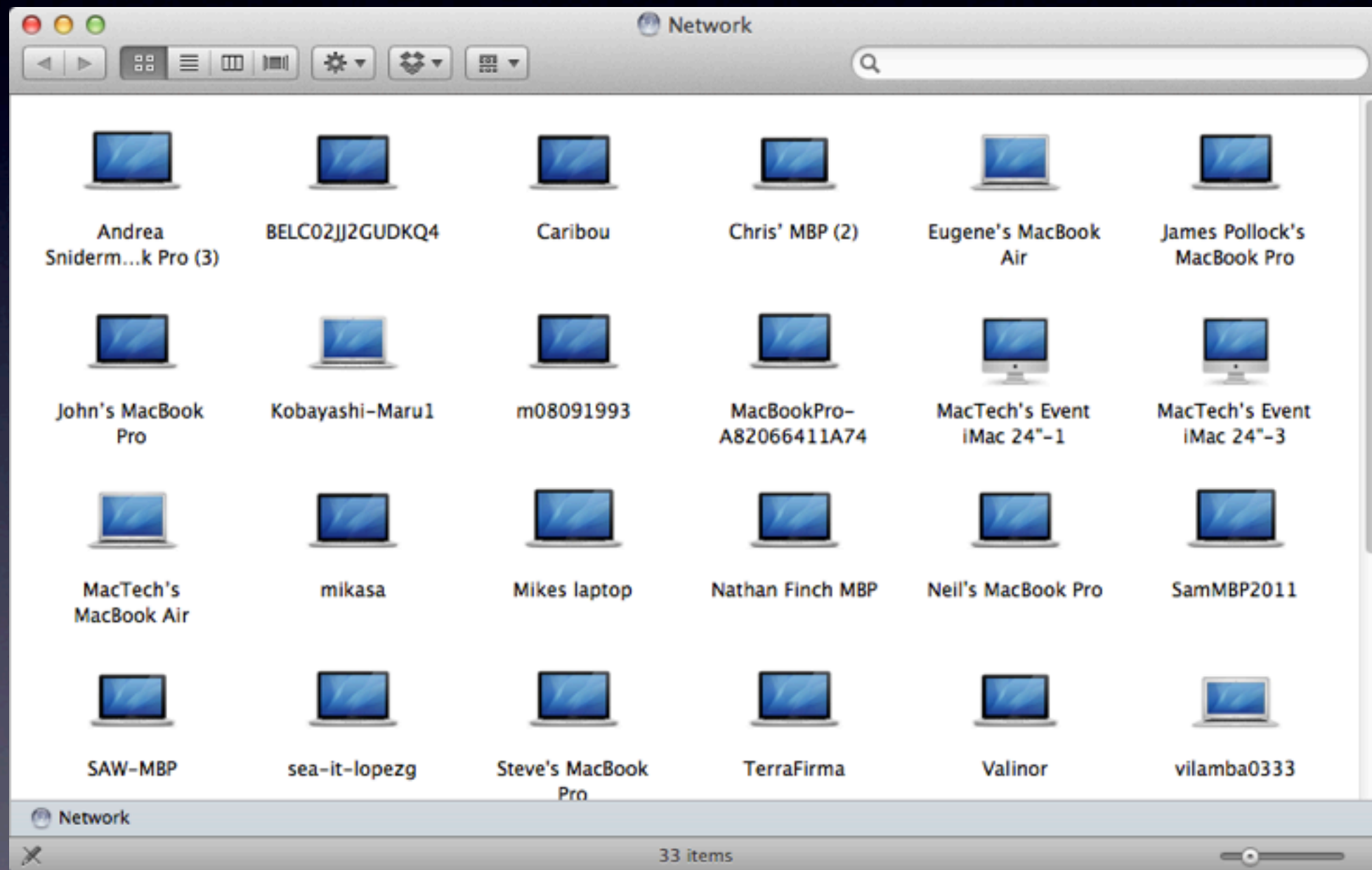


# Why DNS?

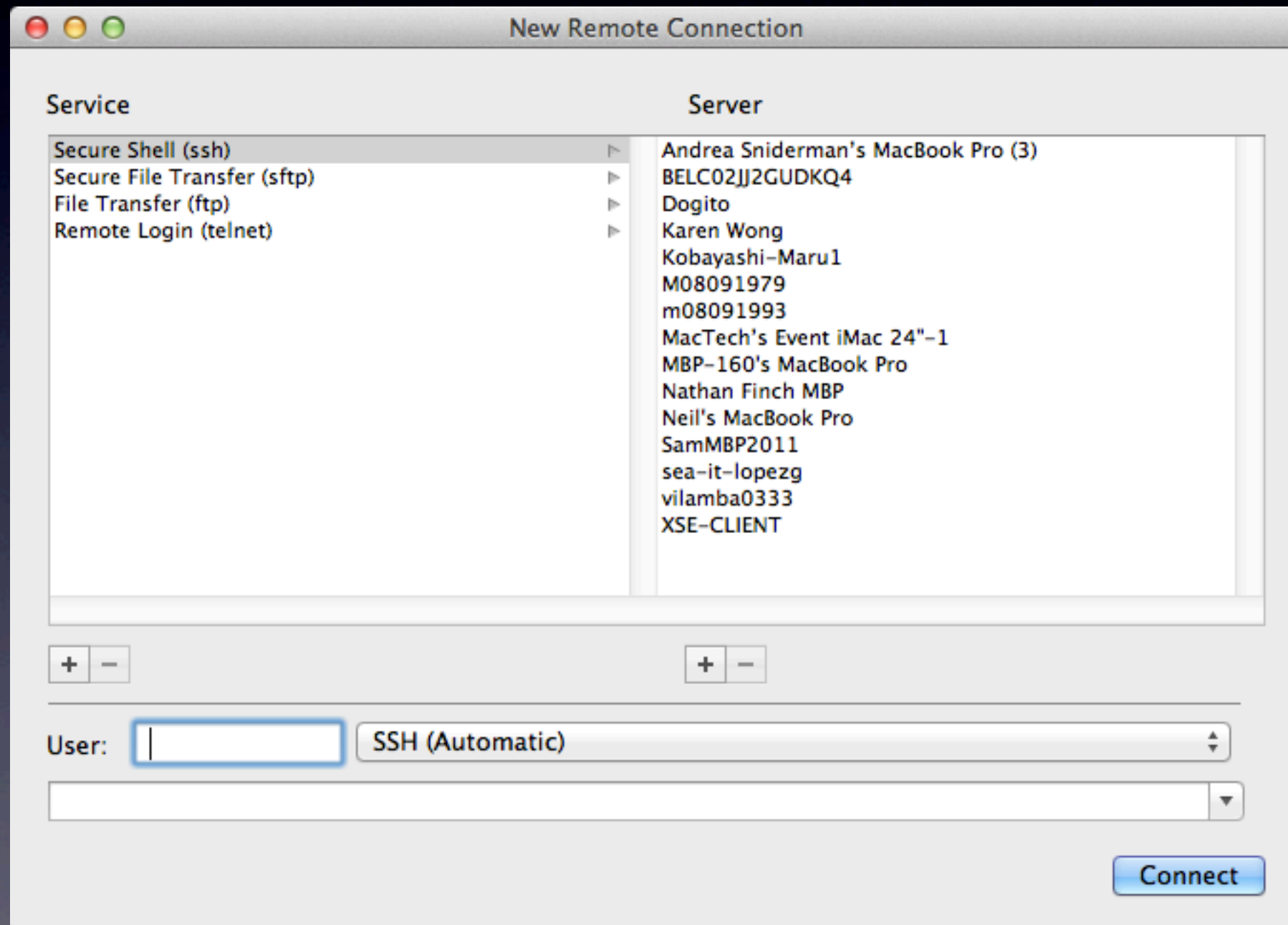
Into something more readable, like this:



# Don't We Have Bonjour?



# Don't We Have Bonjour?





# Things Bonjour Doesn't Work With

- Email
- Web Sites
- Apple Push Notifications (Dark Sky Weather Warnings)
- AD Binding
- Generally, any services that live on a non-local network

# What's the Point?

- Domain Name Service makes the Internet more human-friendly
- It does so by converting human-friendly words to computer-friendly IP addresses, and vice versa
- People find names easy to remember, and numbers hard

# It's Not Magic

```
private.wheelwrights-llc.com. IN SOA thingone.private.wheelwrights-llc
```

```
.com admin.private.wheelwrights-llc.com. (
```

```
    2013030402      ;Serial
```

```
    86400           ;Refresh
```

```
    3600            ;Retry
```

```
    604800          ;Expire
```

```
    345600          ;Negative caching TTL
```

```
)
```

```
lorax      IN      A      192.168.214.29
```

```
brother-mfc IN     A      192.168.214.61
```

```
thingtwo IN     A      192.168.214.25
```

```
office-5250 IN  A      192.168.214.62
```

```
whoville IN     A      192.168.214.27
```

```
smartups-a  IN   A      192.168.214.51
```

```
thingone IN     A      192.168.214.23
```

```
munki       IN     CNAME   lorax.private.wheelwrights-llc.com.
```

```
deploystudio IN  CNAME   lorax.private.wheelwrights-llc.com.
```

```
files       IN     CNAME   thingone.private.wheelwrights-llc.com.
```



# It's Not Magic



“Patient, true, and unafraid of toil.”



# Engineered Simplicity

- Humans engineer simplicity all the time
- I go to Caffé Vita in Fremont, not 4301 Fremont Ave. N., Seattle, WA 98103
- Call Shelley Watson, not (555) 555-1212

# Engineered Simplicity

```
private.wheelwrights-llc.com. IN SOA thingone.private.wheelwrights-llc
.com admin.private.wheelwrights-llc.com. (
    2013030402      ;Serial
    86400           ;Refresh
    3600            ;Retry
    604800          ;Expire
    345600          ;Negative caching TTL
)
```

```
lorax      IN  A      192.168.214.29
brother-mfc IN  A      192.168.214.61
thingtwo   IN  A      192.168.214.25
office-5250 IN A      192.168.214.62
whoville   IN  A      192.168.214.27
smartups-a IN  A      192.168.214.51
thingone   IN  A      192.168.214.23
munki      IN  CNAME   lorax.private.wheelwrights-llc.com.
deploystudio IN CNAME   lorax.private.wheelwrights-llc.com.
files      IN  CNAME   thingone.private.wheelwrights-llc.com.
```

# Essential DNS

- Client/Server System
- “Zones” organize data in delegated, hierarchical fashion
- Zones contain records that describe hosts in the zone
- Question (Query) and answer (Response)



# Four Critical Questions

1. Who is the client asking?
2. What is the client asking?
3. What is the answer?
4. Who cares? (Why is the response important?)



# A Real World Scenario In Two Chapters

- This Actually Happened™
- Names, domains, and IP addresses have been changed to protect the non-technical

# I Receive Email

“No one at our office has received any email today. Is something wrong? Help!”

# Background

- Customer runs their own email server, which is located on the office network
- Mail server known to be mail.ctdawe.com
- Server known to be 75.151.122.149
- I know this because of record-keeping
- I could probably find some of it in client application settings



# What I Want to See in Terminal

Connect to the server using telnet

```
dawe$ telnet mail.ctdawe.com 25
```

```
Trying 75.151.122.149...
```

```
Connected to mail.ctdawe.com.
```

```
Escape character is '^['.
```



# What I Actually See

## The Symptom, Pt. I

Connect to the server using telnet

```
dawe$ telnet mail.ctdawe.com 25
```

```
mail.ctdawe.com: nodename nor servname  
provided, or not known
```

# What I Actually See

## The Symptom, Pt. 2

Connect to the server using telnet

```
dawe$ telnet 75.151.122.149 25
```

```
Trying 75.151.122.149...
```

```
Connected to mail.ctdawe.com.
```

```
Escape character is '^['.
```

# Oh Bother

- Connecting by DNS name  
(mail.ctdawe.com) fails
- Connecting by IP address succeeds
- Because sending email depends on DNS records for delivery, mail delivery fails
- Whiskey Tango Foxtrot? THIS WAS WORKING YESTERDAY!!!



# Open the Toolbox

- Because connection by name fails but by IP address works, it's time to investigate DNS

dawe\$ man dig

- Domain Internet Groper (yeah, really)
- Flexible command line tool allows us to specify excruciatingly granular queries



# dig Usage

## Format

`dig @dns_server address rcrd_type +options`

## Example

`dig @8.8.8.8 www.mactech.com a +short`

# Domain Name Registrar

- Manages the reservation of Internet domain names
- Common examples include Network Solutions, GoDaddy, Namecheap
- Registration of a domain typically enables a DNS domain in the registrar's servers, or allows you to define DNS servers manually.

# DNS Zones

- A portion of the DNS name space for which administrative responsibility has been delegated

`ctdawe.com.`

- Contains resource records associated with the zone, e.g. `mail.ctdawe.com.`
- Traditionally, there's only one version of the zone, with only one set of records



# Back to Theory

- Address (A) Record
- Mail Exchanger (MX) Record
- Pointer (PTR) Record
- Start of Authority (SOA) Record



# Start of Authority (SOA)

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

```
dawe$ dig ctdawe.com soa +short  
dns1.registrar-servers.com.
```

# Address Record (A)

- Maps a name to an IP address
- Expected

mail.ctdawe.com.      IN      A      75.151.122.149

# Address Record (A)

Let's confirm the A record we have on paper

```
dawe$ dig @dns1.registrarservers.com mail.ctdawe.com a
```

```
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN
```

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1,  
ADDITIONAL: 0
```



# Mail Exchanger Record (MX)

- Defines host(s) that accept mail for a domain
- Expected

```
ctdawe.com.    IN      MX  10    mail.ctdawe.com.
```

# Mail Exchanger Record (MX)

What does the customer MX look like?

```
dawe$ dig @dns1.registrarservers.com ctdawe.com mx
```

```
ctdawe.com.      1800    IN  MX  20 eforward5.registrar-  
servers.com.
```

```
ctdawe.com.      1800    IN  MX  10 eforward1.registrar-  
servers.com.
```

# Pointer, aka Reverse Record (PTR)

- The pointer (PTR, or reverse lookup) record returns a name when querying an IP address.
- Your circuit provider typically hosts it
- Expected

```
149.122.151.75.in-addr.arpa. 1457    IN  
PTR    mail.ctdawe.com.
```



# PTR Record

```
dawe$ dig @dns1.registrarservers.com -x  
75.151.122.149
```

```
149.122.151.75.in-addr.arpa. 1457    IN  
PTR    mail.ctdawe.com.
```

# What Do We Know?

- DNS Authority `dns1.registrar-servers.com`
- The authoritative DNS resolves the MX record  
an unfamiliar set of servers
- Documented hostname name for MX has no A  
record in DNS
- But a PTR record exists resolving the expected  
IP address to `mail.ctdawe.com`

# Clean Up the Mess

1. Access the authoritative DNS host
2. Configure a proper Address (A) record
3. Correct the Mail Exchange (MX) record
4. Remember that DNS changes take time to propagate



# Why Did This Happen?

- The human factor is a factor
  - “Our web designer called and asked if they could have our ‘Network Solutions’ information to move the web site.”
- The designer moved DNS authority to a new host and didn’t migrate all the records.

# Conclusions

- Customer gave up critical management information without understanding intentions or implications.
- The web consultant “set up a new web site” and nuked the remainder of the domain in the process.

# This Is Not Uncommon

**Zack Williams** @zdw May 31  
Note to other tech people - please ask before you change DNS settings at the registrar and inadvertently blackhole a domain's email.  
[Expand](#) [Reply](#) [Retweet](#) [Favorite](#) [More](#)

**Chris Dawe** @ctdawe May 31  
[@zdw](#) But we've got to make the new website available! The owner is asking!  
[Expand](#)

**Zack Williams** @zdw May 31  
[@ctdawe](#) You sir are a mind reader - that's exactly what happened. Also, password at the registrar was 3 characters long. High security!  
[Hide conversation](#) [Reply](#) [Retweet](#) [Favorite](#) [More](#)  
1:30 PM - May 31, 2012 · [Details](#)



# Fixed Now?

Sort of...but wait...



“No one at our office has received any email today. Is something wrong? Help!”



# Split Horizon DNS

- Network Address Translation (NAT) broke globally-routable Internet
- Some information shouldn't be available on the Internet
- Reliability suffers from keeping DNS only in house, particularly for small businesses (One Mac mini and a DSL line? Really?)



# Split-Horizon DNS

## The Fundamental Idea

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

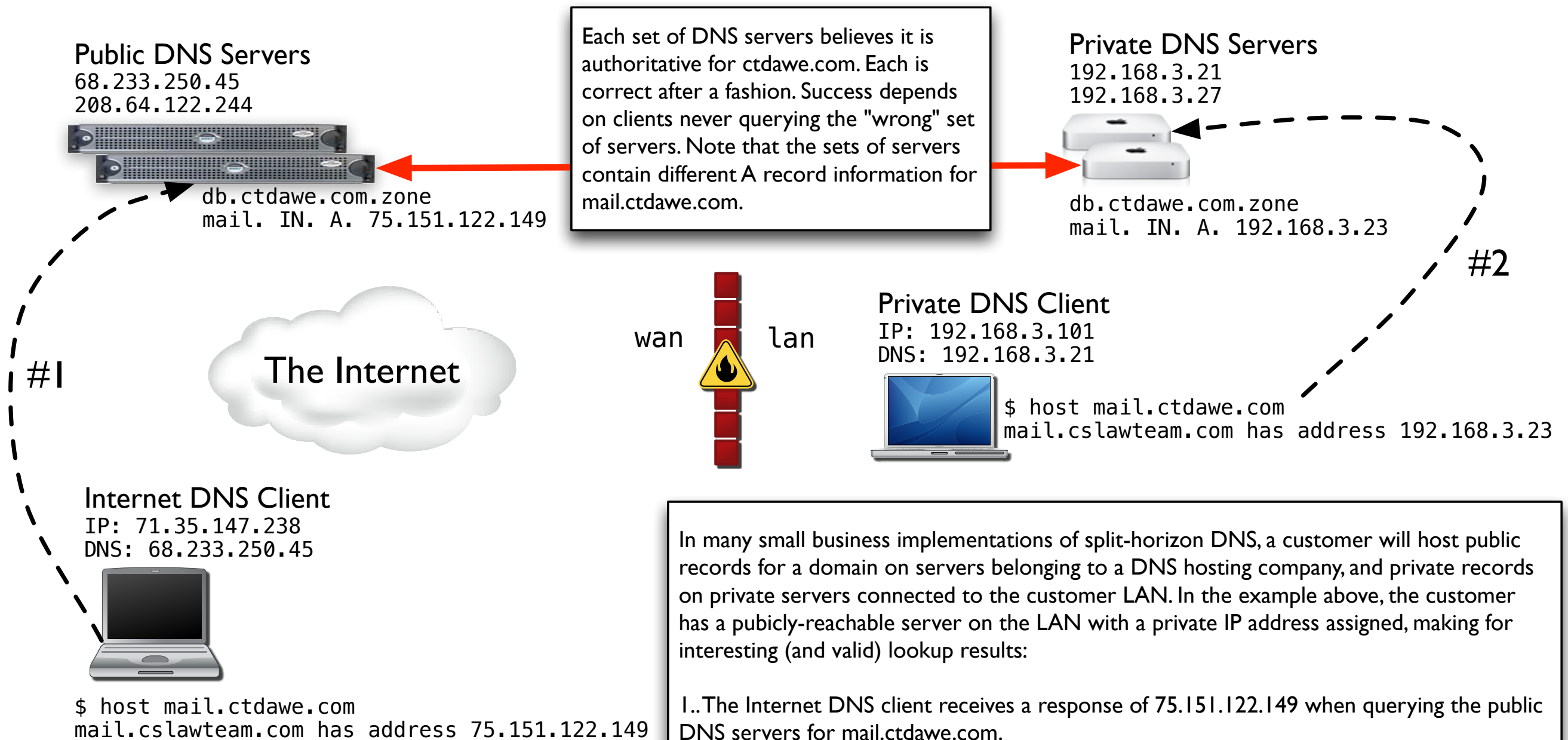
# Split-Horizon DNS

## Two Common Methods

1. Configure one set of DNS server with two sets of records and offer different answers depending on address of requesting client
2. Configure two different sets of DNS servers with different zone contents, each offering data to different sets of clients

# One Example of Split Horizon DNS

(simplified)



In many small business implementations of split-horizon DNS, a customer will host public records for a domain on servers belonging to a DNS hosting company, and private records on private servers connected to the customer LAN. In the example above, the customer has a publicly-reachable server on the LAN with a private IP address assigned, making for interesting (and valid) lookup results:

- 1..The Internet DNS client receives a response of 75.151.122.149 when querying the public DNS servers for mail.ctdawe.com.
- 2..The private DNS client receives a response of 192.168.3.23 when querying the private DNS servers for mail.ctdawe.com.

In order for this setup to function, the private client must not query the public server, and the public client must not query the private server (and in this example can not query the private server), as each would likely receive a response that would likely not be reachable.



# Addressing the Elephant

The private DNS server thinks

`mail.ctdawe.com. IN A 192.168.3.23`

Clients talking to the private DNS server never lost contact with `mail.ctdawe.com` so users on the office network never saw an explicit error

# Is That All?

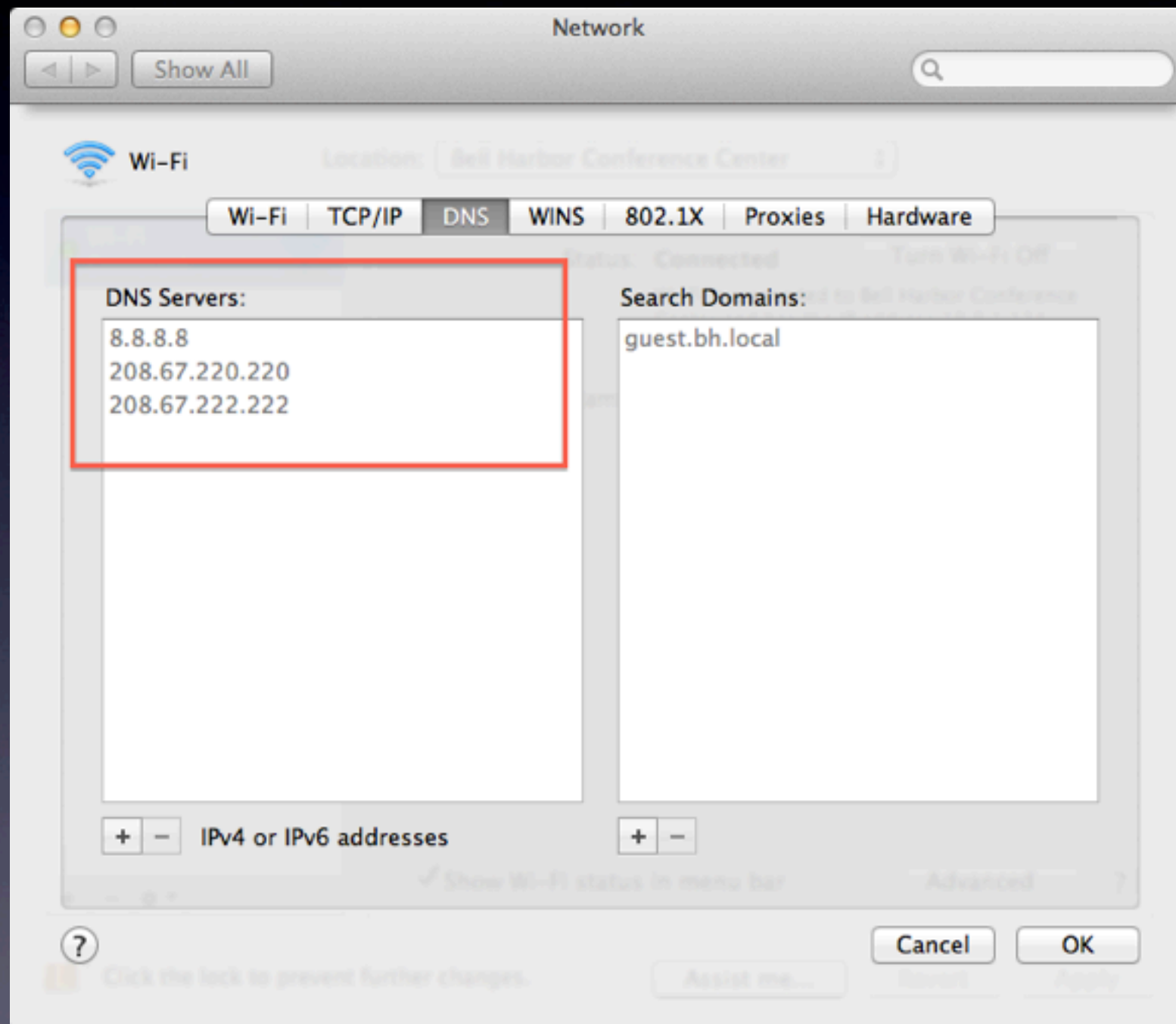
Almost.

# I Receive Email

“No one at our office can see the new web site. Did we break something again? Help!”



# Break Out the Tools



# Break Out the Tools

- scutil

```
dawe$ scutil --dns
```

```
DNS configuration (for scoped queries)
```

```
resolver #1
```

```
  search domain[0] : ctdawe.com
```

```
  nameserver[0] : 192.168.3.21
```

```
  nameserver[1] : 192.168.3.27
```

# Break Out the Tools

## Query the Public Server

```
dig @dns1.registrar-servers.com www.ctdawe.com a  
+short
```

```
70.32.106.38
```

## Query the Private Server

```
dig @192.168.3.21 www.ctdawe.com a +short
```

```
75.101.132.77
```



# Simple Fix

On the private DNS server, update A record for the web server to match the record on the public DNS server

```
www.ctdawe.com.    IN    A    70.32.106.38
```

# Are We Fixed?



Finally, yes.

# Tools to Explore

- BIND
- dig
- host
- scutil
- mDNSResponder
- Network Utility (If you must)



# Additional Record Types

- CNAME (Canonical Name) aka Alias
- SRV (Service)
- AAAA (IPv6 Address)
- TXT (Text)

# DNS (A War Story)

Chris Dawe  
Wheelwrights, LLC

[www.wheelwrights-llc.com](http://www.wheelwrights-llc.com)

@ctdawe