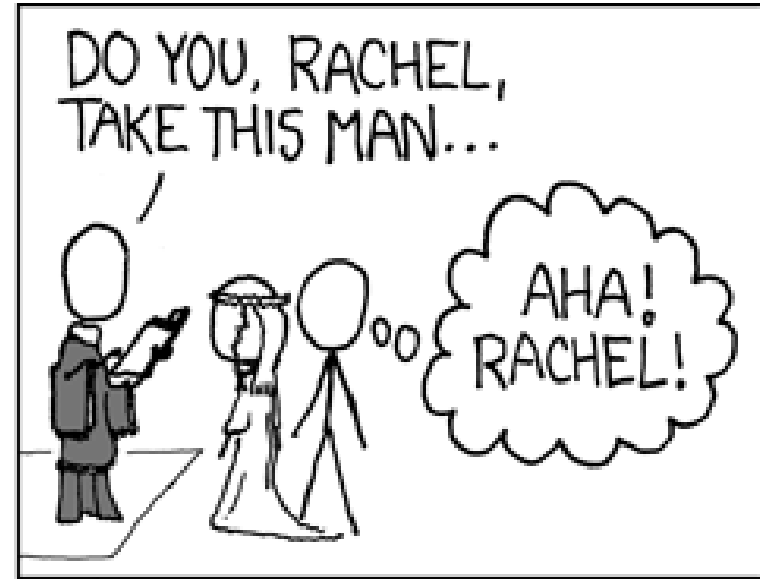


Domain Name System (DNS)



<http://xkcd.com/302/>

Computer Networking: A Top Down Approach

6th edition

Jim Kurose, Keith Ross

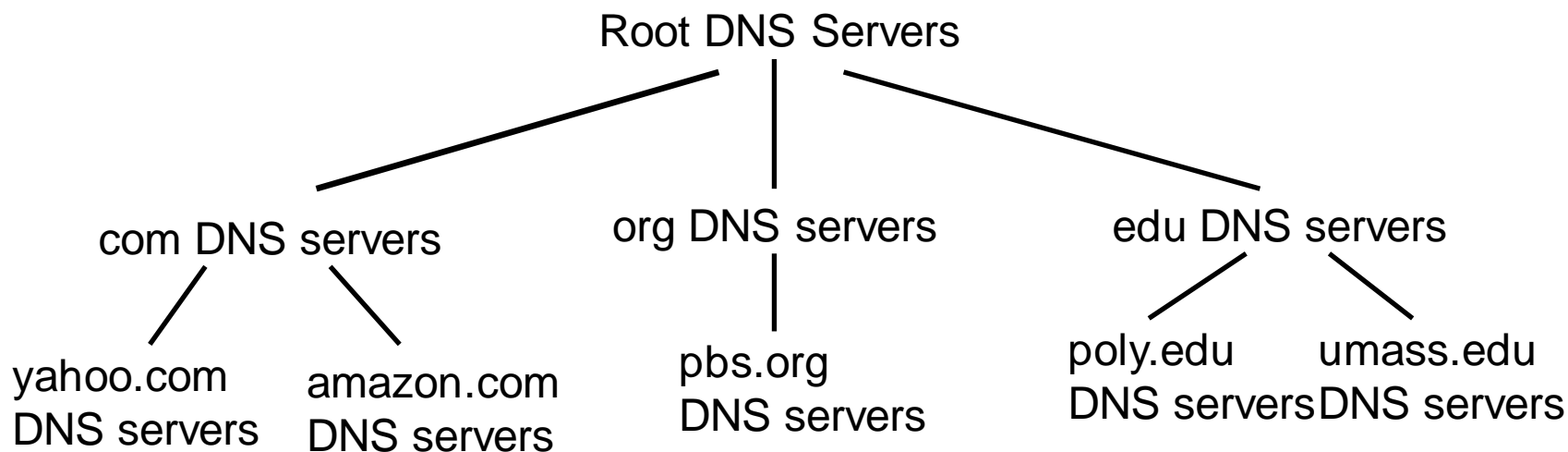
Addison-Wesley

Some materials copyright 1996-2012
J.F Kurose and K.W. Ross, All Rights Reserved



Overview

- Domain Name System (DNS)
 - Hierarchical name space
 - Maps friendly names to IP address
 - Large distributed database of records



Names and IP addresses

- Why use names instead of IP address?
 - Names are easier for humans to remember
 - www.bbc.co.uk versus 64.91.253.46
 - IP address could change if changing ISPs
 - Single name could map to multiple IP address
 - Load balance over several servers
 - Send user to nearest server to reduce latency
 - Allow multiple names to go to same place

Hierarchical network names

- **Host name:** `www.cs.princeton.edu`
 - **Domain:** registrar for each top-level domain
 - **Host name:** local admin assigns to each host
- **IP addresses:** `128.112.7.156`
 - **Prefixes:** ICANN, regional Internet registries, and ISPs
 - **Hosts:** static configuration, or dynamic using DHCP
- **MAC addresses:** `00-15-C5-49-04-A9`
 - **Blocks:** assigned to vendors by the IEEE
 - **Adapters:** assigned by the vendor from its block

Domain Name System

- Domain Name System (DNS)
 - Maps host name to IP address
 - DNS resolver, sends query
 - DNS server, provides response
- How does the server know the answer?

Option 1: Local file

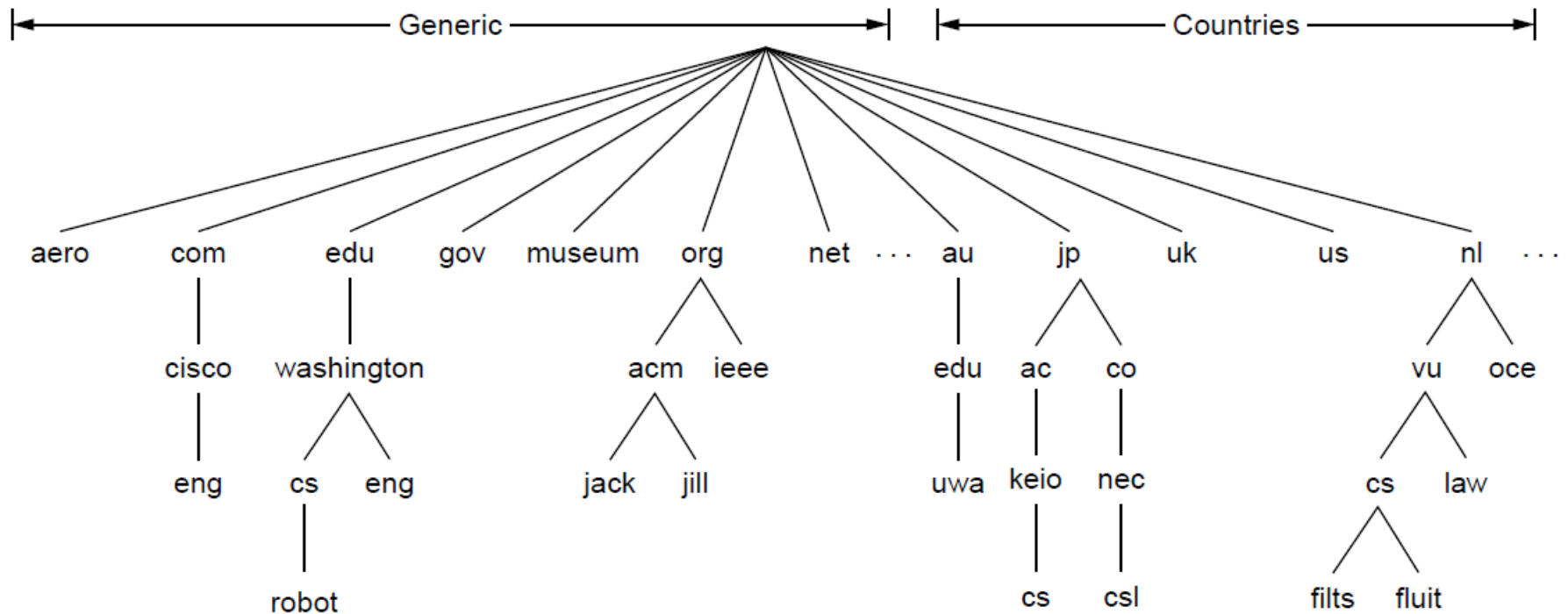
- Store name to address mapping in local file
 - ARPANET prior to 1983, hosts.txt
 - Flat namespace
 - SRI updated hosts.txt, others downloaded it
 - Worked in a world of a small number of large computers
 - Doesn't scale as more and more computers were placed on the network

Option 2: Central server

- Central server
 - All name to address mapping stored in one place
 - All queries go to central server
- Problems:
 - Single point of failure
 - Server may experience high volume of traffic
 - Server may be distant from a host wanting a lookup
 - Single point of update
 - Does not scale

Domain Name System (DNS)

- Distributed, hierarchical collection of servers
 - Name space is hierarchical



Generic Top Level Domains (TLDs)

Domain	Intended use	Start date	Restricted?
com	Commercial	1985	No
edu	Educational institutions	1985	Yes
gov	Government	1985	Yes
int	International organizations	1988	Yes
mil	Military	1985	Yes
net	Network providers	1985	No
org	Non-profit organizations	1985	No
aero	Air transport	2001	Yes
biz	Businesses	2001	No
coop	Cooperatives	2001	Yes
info	Informational	2002	No
museum	Museums	2002	Yes
name	People	2002	No
pro	Professionals	2002	Yes
cat	Catalan	2005	Yes
jobs	Employment	2005	Yes
mobi	Mobile devices	2005	Yes
tel	Contact details	2005	Yes
travel	Travel industry	2005	Yes
xxx	Sex industry	2010	No

Top level domains

- **Top-level domains (TLD)**
 - Around 22 generic TLDs, e.g. com, net, org, edu
 - Most popular with US organizations
 - Around 250 country specific TLDs
 - Two letter ISO code, e.g. au, ch, se
 - Some violations, e.g. uk instead of gb
 - TLDs run by registrars appointed by Internet Corporation for Assigned Names and Numbers (ICANN)
 - Money in names
 - Cybersquatting
 - Country of Tavalu sold lease to .tv for 50 million

Top level domains

- Set to expand, you can buy your own TLD!
 - June 2011
 - ICANN approves creation of TLDs for brands and organizations
 - \$185,000 initial application, \$25,000 annual fee
 - Is an easy-to-remember domain name relevant anymore?
 - Google the name instead
 - What name should you type to get to General Motors?

Second-level domains

- Second-level domains

- Getting name-of-company.com is easy

- Buy from a registrar for the desired TLD, small annual fee



superwidget.com is already taken. [\(Get info\)](#) [Use Domain Buy to get this name](#)

View alternative results below or search again:

.com

[Important information about Private Registration.](#) [Why register multiple domains?](#)

[Select All](#) [More Domain Options](#)

<input type="checkbox"/>	superwidget.co	✓	\$17.99 SALE!	Save \$12.00
<input type="checkbox"/>	superwidget.info	✓	\$1.99*	BEST VALUE!
<input type="checkbox"/>	superwidget.net	✓	\$9.99* SAVE!	Save \$5.00
<input type="checkbox"/>	superwidget.org	✓	\$6.99* SALE!	Save \$8.00
<input type="checkbox"/>	superwidget.us	✓	\$3.99 SALE!	SPECIAL!
<input type="checkbox"/>	superwidget.ca	✓	\$12.99/yr	
<input type="checkbox"/>	superwidget.biz	✓	\$5.99* SALE!	Save \$9.00
<input type="checkbox"/>	superwidget.mobi	✓	\$6.99*	Save \$11.00
<input type="checkbox"/>	superwidget.me	✓	\$8.99 SALE!	Save \$11.00
<input type="checkbox"/>	superwidget.tv	✓	\$39.99/yr	

View: [Available](#) | [Backorder](#)

We also recommend...

Additional Premium International

[Select All](#) Show: [All](#)

- [bestsuperwidget.com](#)
- [superwidgetnow.com](#)
- [freesuperwidget.com](#)
- [superwidgettoday.com](#)
- [superwidgetshop.com](#)
- [superwidgetblog.com](#)
- [mysuperwidget.com](#)
- [superwidgetsite.com](#)
- [thesuperwidnet.com](#)

Subdomains

- Further hierarchy under a second-level domain
 - e.g. mail.company.com, www.company.com, inf.phy.cam.ac.uk
 - Each domain controls the subdomains under it
- Domain resource records
 - Each domain has a set of data about its server(s)
 - At a minimum, the IP address for a name

Domain resource record

Type	Meaning	Value
SOA	Start of authority	Parameters for this zone
A	IPv4 address of a host	32-Bit integer
AAAA	IPv6 address of a host	128-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
SPF	Sender policy framework	Text encoding of mail sending policy
SRV	Service	Host that provides it
TXT	Text	Descriptive ASCII text

- **A** - most important, maps hostnames to IPv4 addresses
- **MX** - username@company.com go to this server name
- **NS** - server that stores the record
- Fields have a TTL - time-to-live, for caching

Setting DNS resource record

Set Nameservers

* Required

If you are hosting your Web site with us (you have a hosting account with us associated with this domain) or you want to Park or Forward your domain, we will automatically set your nameservers for you.

- I want to **park** my domains.
- I want to **forward** my domains.
- I have a **hosting account** with these domains.
- I have **specific nameservers** for my domains.

Did You Know?

Domains using our nameservers benefit from our worldwide DNS presence through Anycast DNS.

[Learn More](#)

Nameserver 1: *

NS1.LINODE.COM

Nameserver 2: *

NS2.LINODE.COM

Nameserver 3:

NS3.LINODE.COM

Nameserver 4:

NS4.LINODE.COM

[Add more](#) | [Manage DS Records](#)

SOA Record						
Primary DNS	Email	Default TTL	Refresh Rate	Retry Rate	Expire Time	Options
ns1.linode.com	a@b.com	Default	Default	Default	Default	Settings

NS Records				
Name Server	Subdomain	TTL	Options	
ns1.linode.com	keithv.com	Default	Edit Remove	
ns2.linode.com	keithv.com	Default	Edit Remove	
ns3.linode.com	keithv.com	Default	Edit Remove	
ns4.linode.com	keithv.com	Default	Edit Remove	
ns5.linode.com	keithv.com	Default	Edit Remove	

[Add a new NS record](#)

MX Records				
Mail Server	Preference	Subdomain	TTL	Options
mx1.emailsvr.com	10		Default	Edit Remove
mx2.emailsvr.com	20		Default	Edit Remove

[Add a new MX record](#)

A/AAAA Records			
Hostname	IP Address	TTL	Options
	69.164.194.211	Default	Edit Remove
mail	69.164.194.211	Default	Edit Remove
www	69.164.194.211	Default	Edit Remove

[Add a new A record](#)

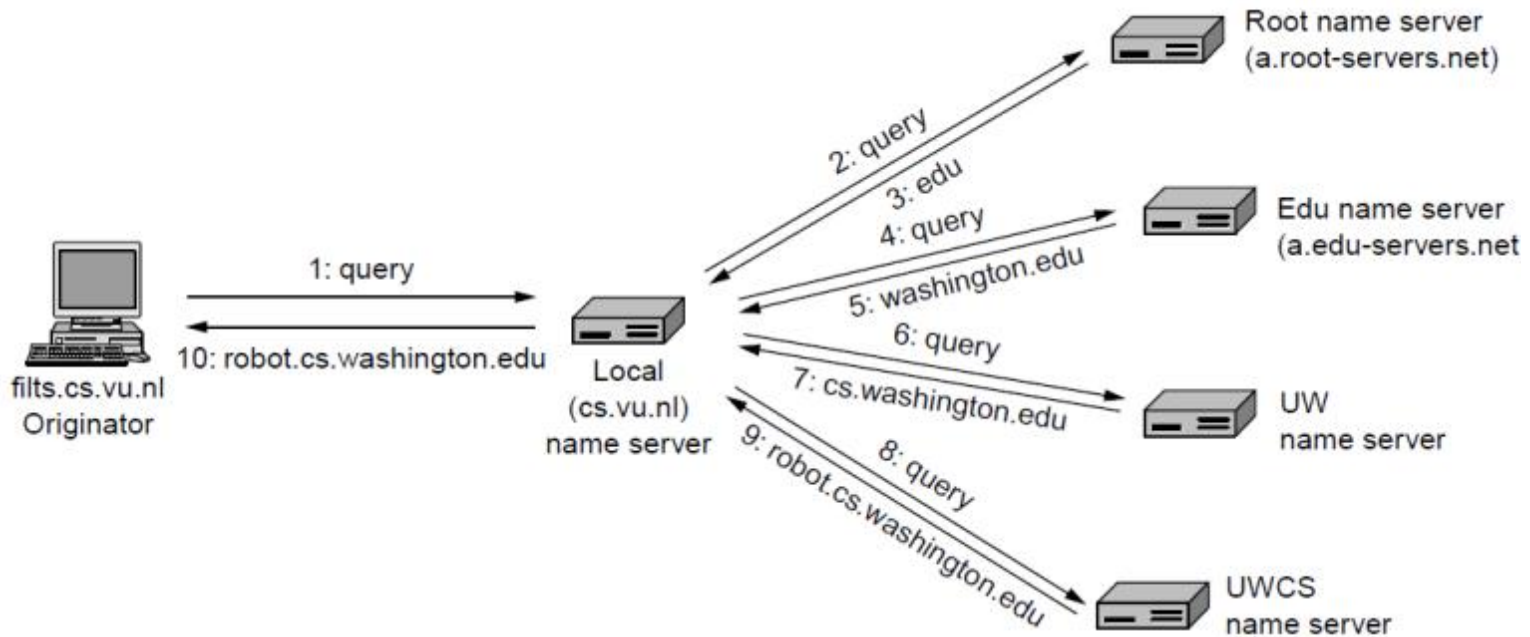
CNAME Records			
Hostname	Aliases to	TTL	Options

[Add a new CNAME record](#)

TXT Records			
Name	Value	TTL	Options

[Add a new TXT record](#)

Name resolution



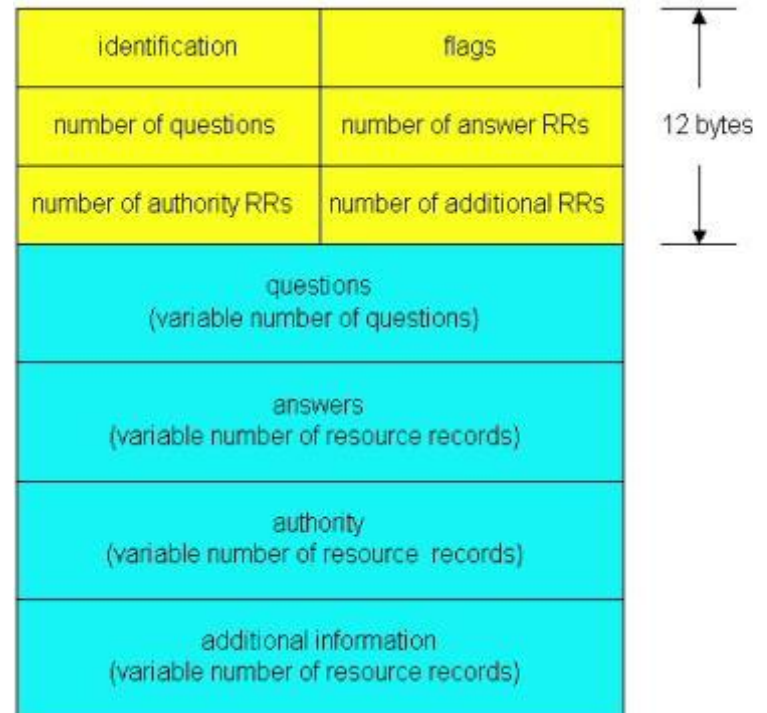
- Step 1: Host contacts its local DNS server
 - Host configured with local server
 - Manually configured (e.g. /etc/resolve.conf) or via DHCP
 - A "recursive query", originator waits for complete answer from local DNS server

DNS query

- Name lookup via DNS query
 - Transported over UDP
 - Retry same server with exponential backoff
 - Can switch to trying other DNS servers

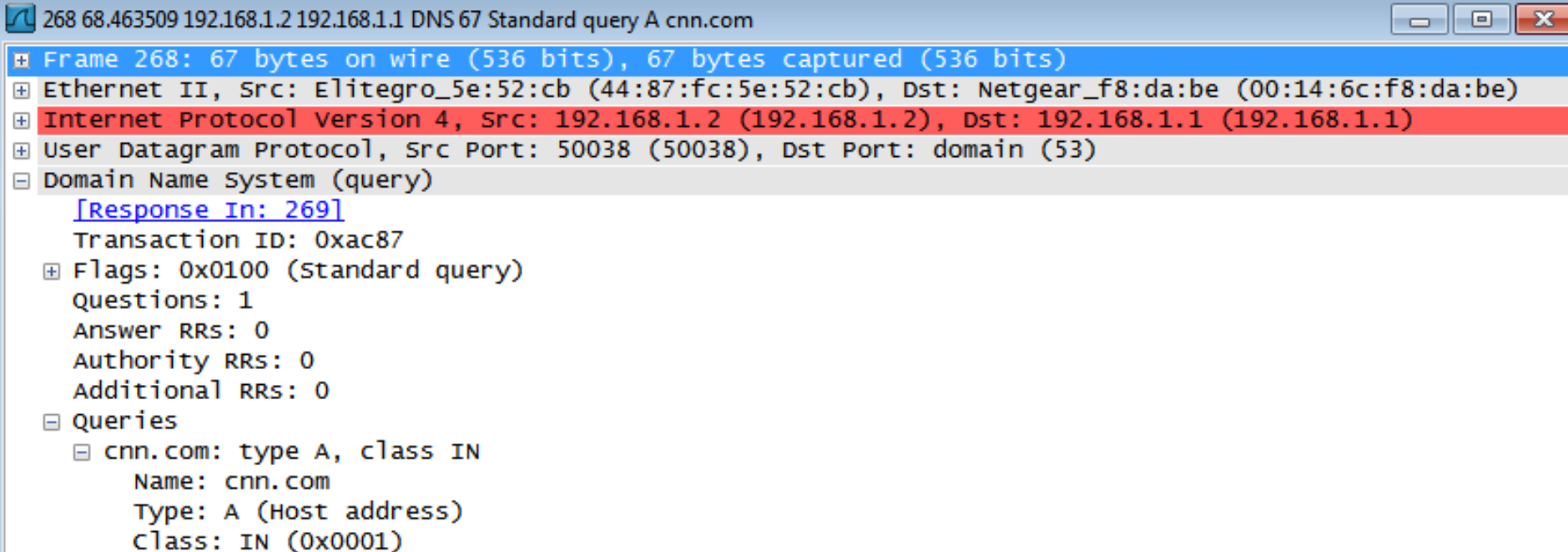
- Identification:
 - 16 bit # for query, reply uses same #

- Flags:
 - Query or reply
 - Recursion desired
 - Recursion available
 - Reply is authoritative



Example DNS query

```
status = getaddrinfo("cnn.com", "80", &hints, &res);
```



268 68.463509 192.168.1.2 192.168.1.1 DNS 67 Standard query A cnn.com

- Frame 268: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)
- Ethernet II, Src: Elitegro_5e:52:cb (44:87:fc:5e:52:cb), Dst: Netgear_f8:da:be (00:14:6c:f8:da:be)
- Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.1.1 (192.168.1.1)
- User Datagram Protocol, Src Port: 50038 (50038), Dst Port: domain (53)
- Domain Name System (query)
 - [\[Response In: 269\]](#)
 - Transaction ID: 0xac87
 - Flags: 0x0100 (standard query)
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - cnn.com: type A, class IN
 - Name: cnn.com
 - Type: A (Host address)
 - Class: IN (0x0001)

Example DNS response

```
269 68.491794 192.168.1.1 192.168.1.2 DNS 247 Standard query response A 157.166.226.25 A 157.166.226.26 A 157.166.255.18 A 157.16...
+ Frame 269: 247 bytes on wire (1976 bits), 247 bytes captured (1976 bits)
+ Ethernet II, Src: Netgear_f8:da:be (00:14:6c:f8:da:be), Dst: Elitegro_5e:52:cb (44:87:fc:5e:52:cb)
+ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.2 (192.168.1.2)
+ User Datagram Protocol, Src Port: domain (53), Dst Port: 50038 (50038)
- Domain Name System (response)
  [Request In: 268]
  [Time: 0.028285000 seconds]
  Transaction ID: 0xac87
+ Flags: 0x8180 (standard query response, No error)
  Questions: 1
  Answer RRs: 4
  Authority RRs: 3
  Additional RRs: 3
- Queries
  - cnn.com: type A, class IN
    Name: cnn.com
    Type: A (Host address)
    Class: IN (0x0001)
- Answers
+ cnn.com: type A, class IN, addr 157.166.226.25
+ cnn.com: type A, class IN, addr 157.166.226.26
+ cnn.com: type A, class IN, addr 157.166.255.18
+ cnn.com: type A, class IN, addr 157.166.255.19
- Authoritative nameservers
+ cnn.com: type NS, class IN, ns ns5.timewarner.net
+ cnn.com: type NS, class IN, ns ns1.timewarner.net
+ cnn.com: type NS, class IN, ns ns3.timewarner.net
+ Additional records
```

DNS query to nowhere?

- Request lookup of a bogus domain name

```
status = getaddrinfo("fewavbawe34332.com", "80", &hints, &res);
```

The image shows a network packet capture window on the left and a web browser window on the right. The packet capture window displays a DNS query response for the domain 'fewavbawe34332.com'. The response is a Standard query response A, indicating that the domain exists but has no IP address assigned (a 'DNS query to nowhere'). The browser window shows a search for 'fewavbawe34332.com' on the Bresnan website, which returns several search results, including 'Stock Alert: *VELA*', 'Dove® For Women', 'GCLL Hot Stock of 2011!', 'Mortgage Rates Hit 2.50%', and 'Mutual Funds- Scottrade'.

Packet Capture Details:

- Frame 33: 112 bytes on wire (896 bits)
- Ethernet II, Src: Netgear_f8:da:be (08:00:27:08:00:27:f8:da:be)
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
- User Datagram Protocol, Src Port: 54472, Dst Port: 112
- Domain Name System (response)
 - [Request In: 32]
 - [Time: 0.121800000 seconds]
 - Transaction ID: 0xfc33
 - Flags: 0x8180 (Standard query response)
 - Questions: 1
 - Answer RRs: 1
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - fewavbawe34332.com: type A, class IN
 - Name: fewavbawe34332.com
 - Type: A (Host address)
 - Class: IN (0x0001)
 - Answers
 - fewavbawe34332.com: type A, class IN
 - Name: fewavbawe34332.com
 - Type: A (Host address)
 - Class: IN (0x0001)
 - Time to live: 10 seconds
 - Data length: 4
 - Addr: 184.106.31.174 (184.106.31.174)

Browser Search Results:

Search: fewavbawe34332.com

Web Results:

- [Stock Alert: *VELA*](#)
"The World's Most Undervalued 4G Company." - Tobin Smith, Fox Business
Sponsored by [www.telecominvesting.com/VELA](#)
- [Dove® For Women](#)
Beauty Is Skin Deep - Explore Our Range of Products Today!
Sponsored by [www.Dove.us](#)
- [GCLL Hot Stock of 2011!](#)
Read Why GCLL Could Explode! Don't Miss The Opportunity of a Lifetime!
Sponsored by [www.GoGreenInvesting.com](#)
- [Mortgage Rates Hit 2.50%](#)
If you owe under \$729k you may qualify for 3.01% APR Govt Refi Plans.
Sponsored by [www.MortgageRatesExperts.com](#)
- [Mutual Funds- Scottrade](#)
Scottrade Offers One of the Largest Selections of Mutual Funds.
Sponsored by [Scottrade.com](#)

Related Searches:

- [The Few](#)
- [Maths Worksheets](#)
- [Math Homework Help](#)
- [Multiplication Math](#)
- [Math Help](#)
- [Printable Math Worksheets](#)
- [Saxon Math](#)
- [Help Algebra](#)
- [My Algebra](#)
- [Math Problem](#)

Sponsored Results:

- [Stock Alert: *VELA*](#)
"The World's Most Undervalued 4G Company." - Tobin Smith, Fox Business
[www.telecominvesting.com/VELA](#)
- [Dove® For Women](#)
Beauty Is Skin Deep - Explore Our Range of Products Today!
[www.Dove.us](#)
- [GCLL Hot Stock of 2011!](#)
Read Why GCLL Could Explode! Don't Miss The Opportunity of a Lifetime!
[www.GoGreenInvesting.com](#)

Explore with **YAHOO! SEARCH**

article: wiki_A.de | Progressive Music & Classic Rock portal

... AVAVG 8|6380 - AVA AG 8|6381 - AVA Studios 8|6382 - AVB ... Holding AG 8|6557 - AWDarena 8|6558 - AWE 8|6559 - AWE ... to Kings 9|7149 - A Feast for Crows 9|7150 - A Few Good ...
[portal.progressiverocks.com/na/p/artic-de/wiki_A](#)

pzb 42000 pdf pto

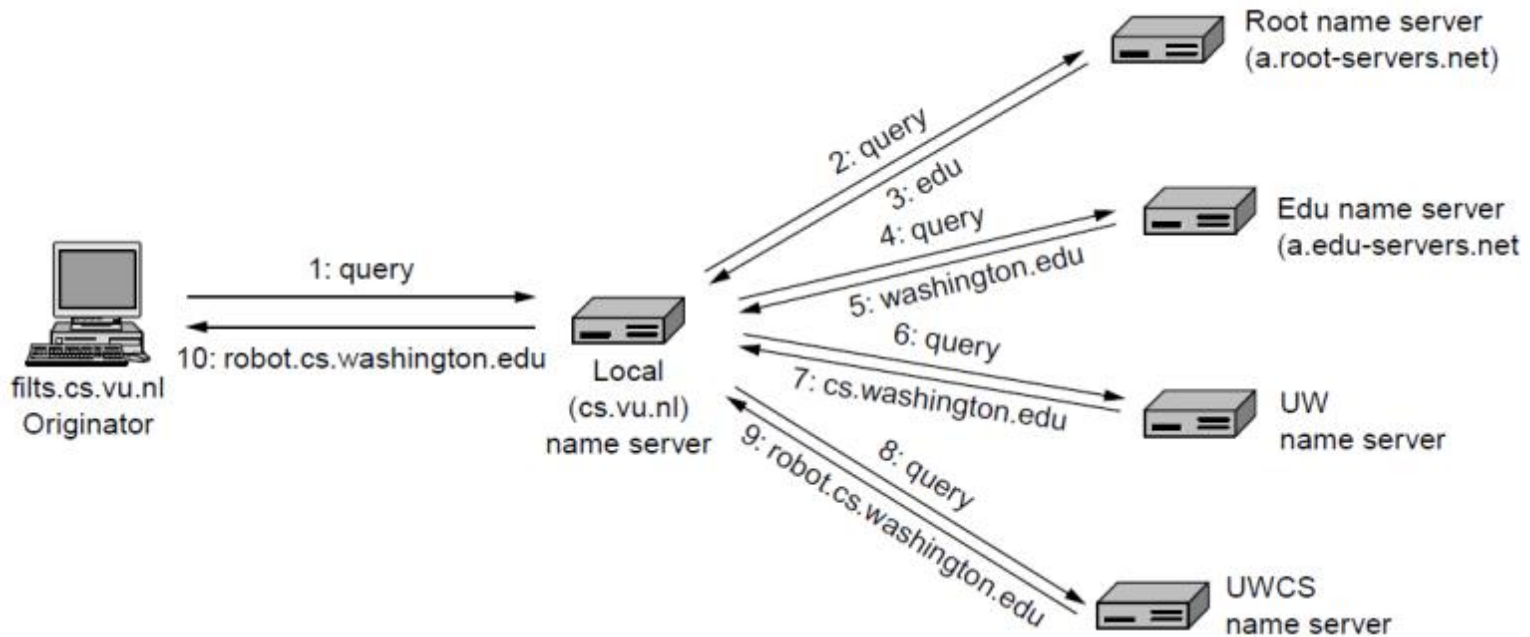
Enter your Docstoc comment email and we'll send we your login information.
[www.binushacker.net/tips/pzb-42000-pdf-pt.html](#)

Domain Name Servers

- Distributed, hierarchical collection of servers
 - Root servers, named: letter.root-servers.net, A-M
 - a.root-servers.net, actually a geographically distributed set of servers reached via anycast routing

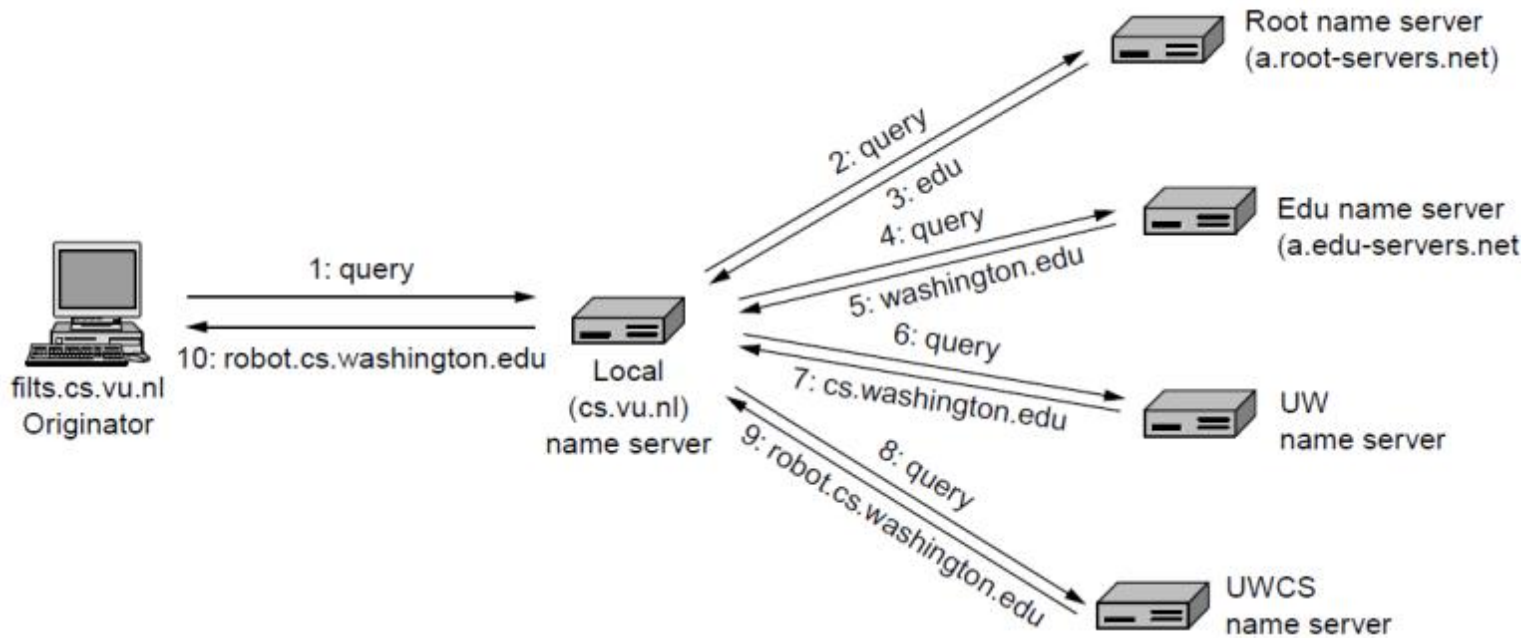


Name resolution



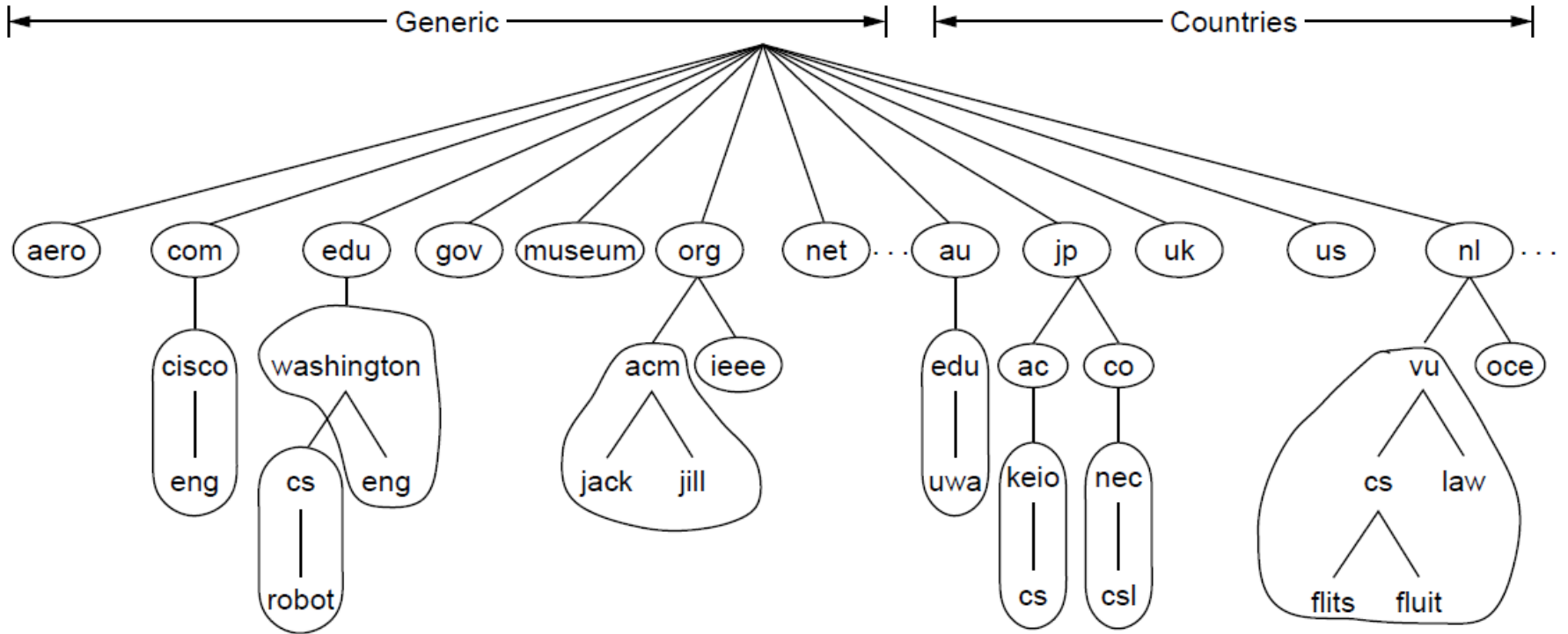
- Step 2/3: Root NS responds with NS handling `.edu`
 - An "iterative query"
 - Local NS has ongoing conversation with multiple servers to find answer for originator

Name resolution

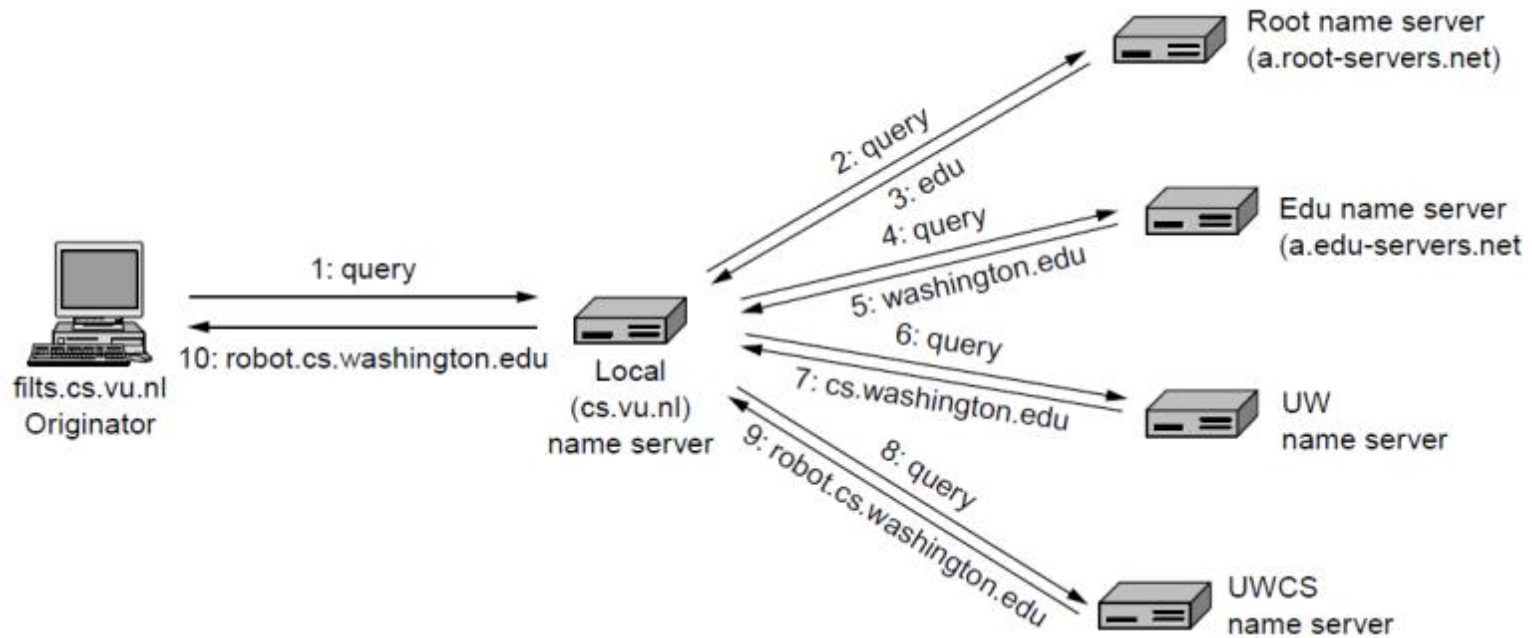


- Step 4/5: edu NS responds with NS for UW
 - Name space divided into non-overlapping zones
 - Zone has a primary name server, 1+ secondary
 - Zone boundaries controlled by domain owner

Name space zones



Name resolution



- Step 6/7: UW NS responds with NS for UWCS
 - UW CS department runs their own DNS server
- Step 8/9: UWCS NS responds with address of robot
 - UWCS NS is the authoritative server
 - The actual DNS record is stored here

Caching

- Recursive queries sufficient to find mapping
 - But expensive, loads root servers
 - Time consuming, incur many RTTs
 - Cache records for certain amount of time (TTL)
- Different levels of caching
 - In the resolver's operating system
 - Local DNS server
 - Can remember steps in the recursive query
 - Go directly to authoritative server for a new hostname at a previous found domain name

Negative caching

- Negative caching
 - Normally DNS cache stores only successful name resolutions
 - But common misspellings can be expensive to lookup
 - Talk to root server and then TLD server before discovering it is a bogus domain name
 - DNS servers can store negative entries and quickly return that name can't be resolved

Cache poisoning

- DNS cache poisoning

- Fool DNS server into entering a non-authoritative entry

- Users get sent to wrong IP address

- Controller of spoofed domain name can:

- Spread malicious software

- Steal information

- e.g. <http://www.wellsfargo.com> now goes a web server running a site very similar to real site... User sees the correct URL in their browser.

- <http://www.youtube.com/watch?v=1d1tUefYn4U>



Example Windows DNS cache

```
Administrator: cmd
c:\source\c\Socket\Release>ipconfig /displaydns

Windows IP Configuration

    adx.g.doubleclick.net
    -----
    Record Name . . . . . : adx.g.doubleclick.net
    Record Type . . . . . : 5
    Time To Live . . . . . : 31
    Data Length . . . . . : 8
    Section . . . . . : Answer
    CNAME Record . . . . . : pagead.l.doubleclick.net

    widgets.amung.us
    -----
    Record Name . . . . . : widgets.amung.us
    Record Type . . . . . : 1
    Time To Live . . . . . : 76
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 173.192.225.170

    www.keithv.com
    -----
    Record Name . . . . . : www.keithv.com
    Record Type . . . . . : 1
    Time To Live . . . . . : 44062
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 69.164.194.211

    Record Name . . . . . : ns2.linode.com
    Record Type . . . . . : 1
    Time To Live . . . . . : 44062
    Data Length . . . . . : 4
    Section . . . . . : Additional
    A (Host) Record . . . : 65.19.178.10
```

Exploring DNS with dig

```
vertanen@katie:~$  
vertanen@katie:~$ dig keithv.com  
  
; <<>> DiG 9.7.3 <<>> keithv.com  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59257  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0  
  
;; QUESTION SECTION:  
;keithv.com.                IN      A  
  
;; ANSWER SECTION:  
keithv.com.                86398  IN      A      69.164.194.211  
  
;; Query time: 2058 msec  
;; SERVER: 10.34.34.2#53<10.34.34.2>  
;; WHEN: Tue Nov 15 12:28:51 2011  
;; MSG SIZE rcvd: 44  
  
vertanen@katie:~$ dig keithv.com  
  
; <<>> DiG 9.7.3 <<>> keithv.com  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39546  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0  
  
;; QUESTION SECTION:  
;keithv.com.                IN      A  
  
;; ANSWER SECTION:  
keithv.com.                86278  IN      A      69.164.194.211  
  
;; Query time: 1 msec  
;; SERVER: 10.34.34.2#53<10.34.34.2>  
;; WHEN: Tue Nov 15 12:30:51 2011  
;; MSG SIZE rcvd: 44  
  
vertanen@katie:~$
```

Summary

- Domain Name System (DNS)
 - Global distributed database
 - Maps human friendly names to IP addresses
 - Critical for the functioning of the Internet
 - DNS resolution multistep process involving:
 - Root servers, top-level domain servers, authoritative servers
 - Caching to improve performance