Internet Naming & Addressing

Objectives: How do we name and address machines in the Internet? What are mnemonic names vs. IP addresses? How do we translate between the two? Understand DNS as a distributed naming infrastructure: design principles, hierarchy & scalability, iterative vs. recursive queries, caching, types of DNS records. Introduction of network tools: nslookup(1) and dig(1).

NS4: April 4, 2016
Textbook (K&R): Sections 2.1, 2.5

Two tales of Internet names

- How did you name your traceroute/ping targets?
  - www.csail.mit.edu, www.cs.purdue.edu (mnemonic; some hierarchy encoded)
- But, machines like binary, bits & bytes
  - IPv4: 32 bits specifically
  - 128.30.2.155 (dotted notation: a.b.c.d; letter = unsigned byte/octet)
  - Also hierarchical – will see later
- Need translation (via DNS)

DNS: domain name system

people: many identifiers:
- SSN, name, passport #

Internet hosts, routers:
- IP address (32 bit) - used for addressing datagrams
- "name", e.g., www.yahoo.com - used by humans

Q: how to map between IP address and name, and vice versa ?

Domain Name System:

- *distributed database* implemented in hierarchy of many *name servers*
- *application-layer protocol:* hosts, name servers communicate to *resolve* names (address/name translation)
  - note: core Internet function, implemented as application-layer protocol
  - complexity at network's "edge"

DNS: services, structure

DNS services

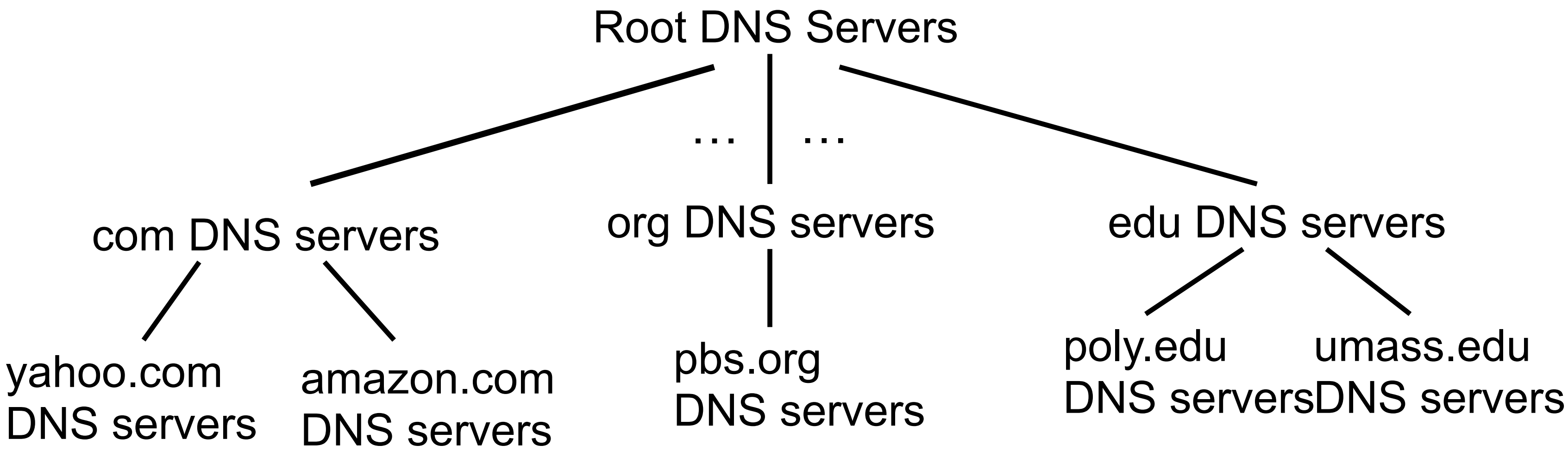
- hostname to IP address translation
- host aliasing
  - canonical, alias names
- mail server aliasing
- load distribution
  - replicated Web servers: many IP addresses correspond to one name

why not centralize DNS?

- single point of failure
- traffic volume
- distant centralized database
- maintenance

A: doesn't scale!

DNS: a distributed, hierarchical database

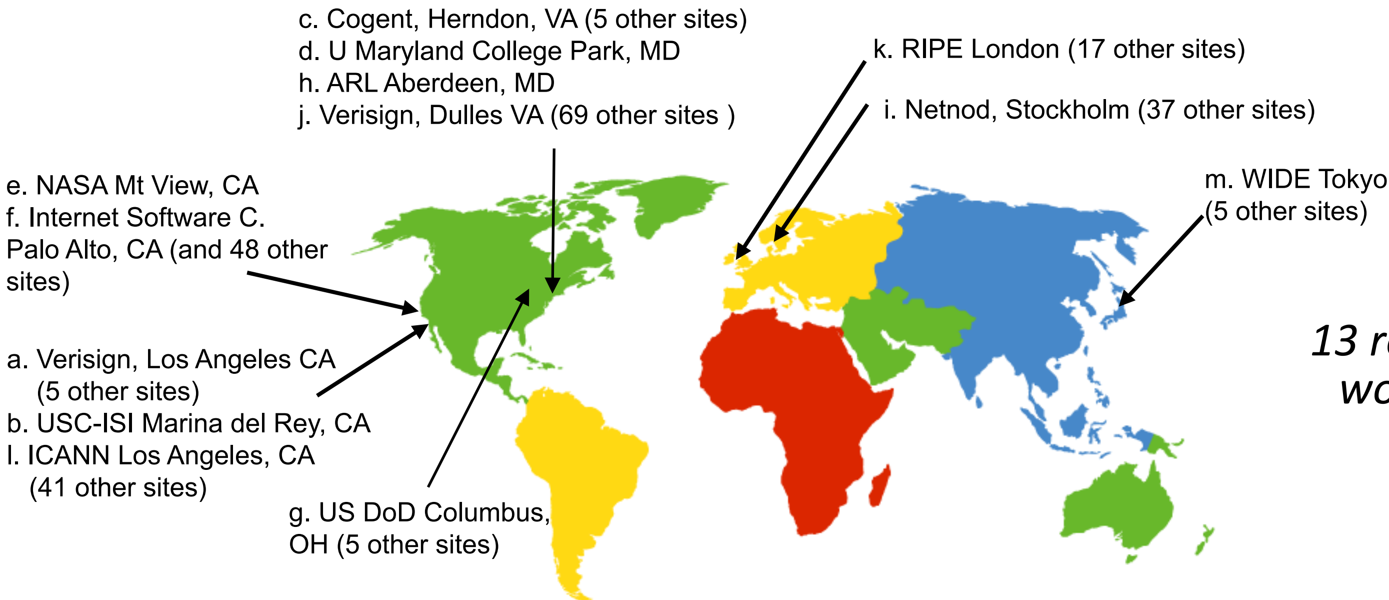


client wants IP for www.amazon.com; 1st approx:

- client queries root server to find com DNS server
- client queries .com DNS server to get amazon.com DNS server
- client queries amazon.com DNS server to get IP address for www.amazon.com

DNS: root name servers

- contacted by local name server that can not resolve name
- root name server:
  - contacts authoritative name server if name mapping not known
  - gets mapping
  - returns mapping to local name server



13 root name "servers" worldwide

TLD, authoritative servers

top-level domain (TLD) servers:

- responsible for com, org, net, edu, aero, jobs, museums, and all top-level country domains, e.g.: uk, fr, ca, jp, sg
- Network Solutions maintains servers for .com TLD
- Educause for .edu TLD

authoritative DNS servers:

- organization's own DNS server(s), providing authoritative hostname to IP mappings for organization's named hosts
- can be maintained by organization or service provider

Local DNS name server

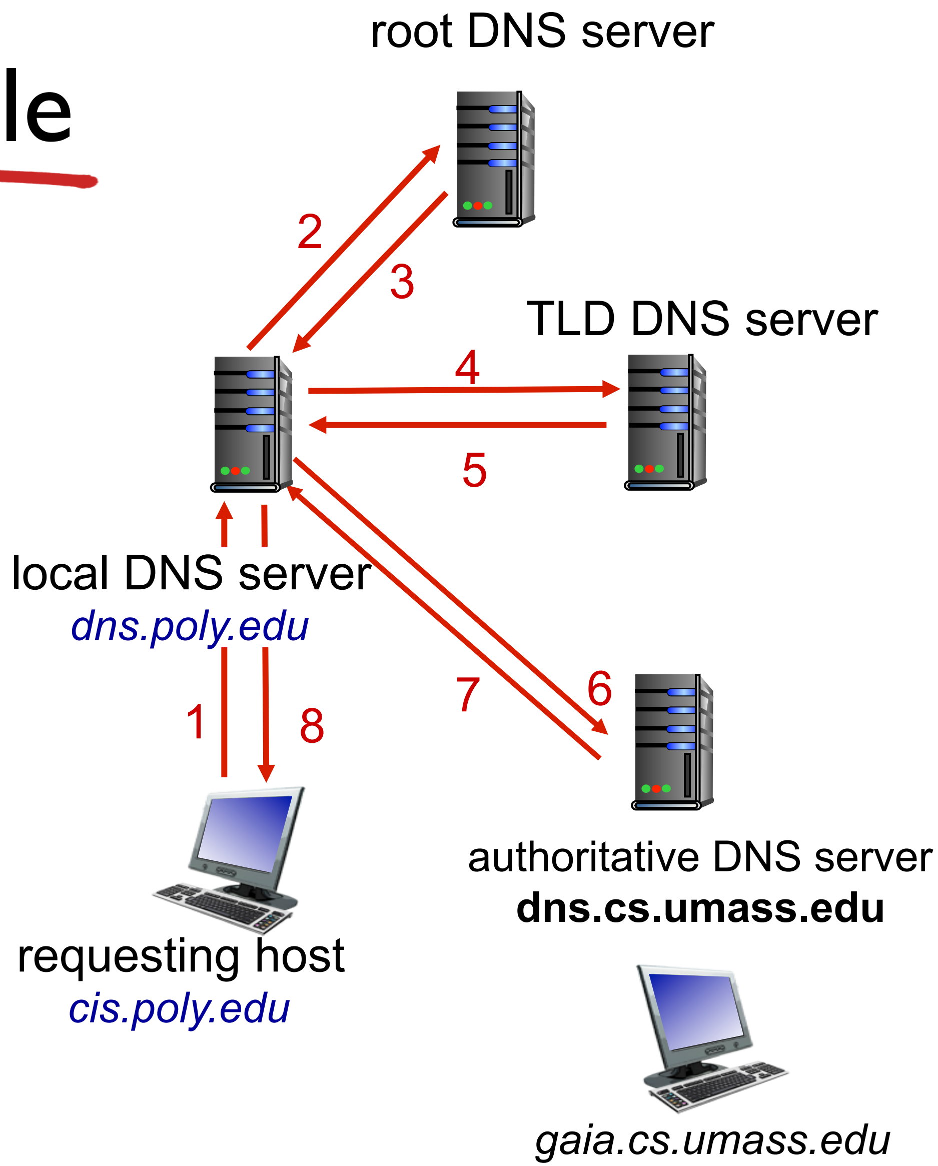
- does not strictly belong to hierarchy
- each ISP (residential ISP, company, university) has one
  - also called “default name server”
- when host makes DNS query, query is sent to its local DNS server
  - has local cache of recent name-to-address translation pairs (but may be out of date!)
  - acts as proxy, forwards query into hierarchy

DNS name resolution example

- host at cis.poly.edu wants IP address for gaia.cs.umass.edu

iterated query:

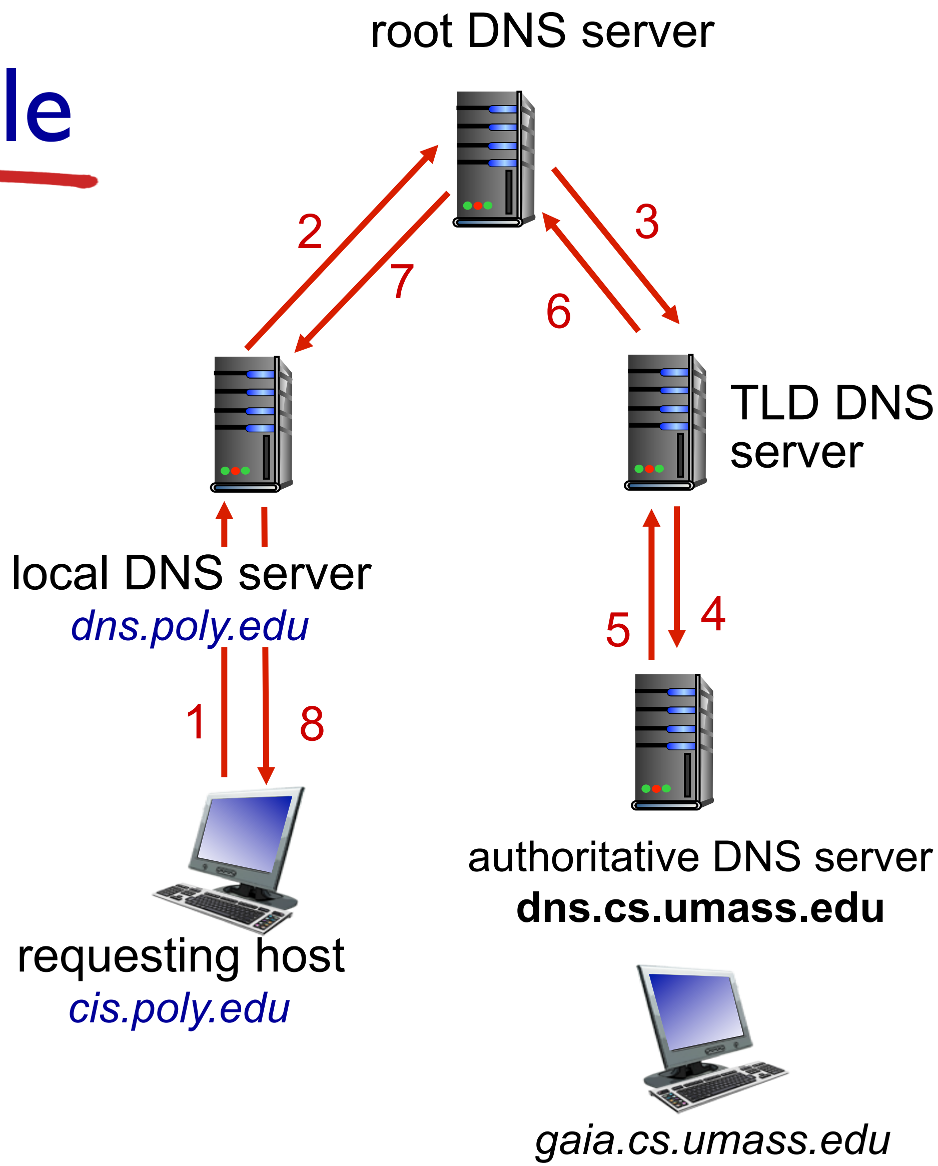
- ❖ contacted server replies with name of server to contact
- ❖ "I don't know this name, but ask this server"



DNS name resolution example

recursive query:

- puts burden of name resolution on contacted name server
- heavy load at upper levels of hierarchy?



DNS: caching, updating records

- once (any) name server learns mapping, it *caches* mapping
  - cache entries timeout (disappear) after some time (TTL)
  - TLD servers typically cached in local name servers
    - thus root name servers not often visited
- cached entries may be *out-of-date* (best effort name-to-address translation!)
  - if name host changes IP address, may not be known Internet-wide until all TTLs expire
- update/notify mechanisms proposed IETF standard
  - RFC 2136

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 `servereast.backup2.ibm.com`
- `value` is canonical name

type=MX

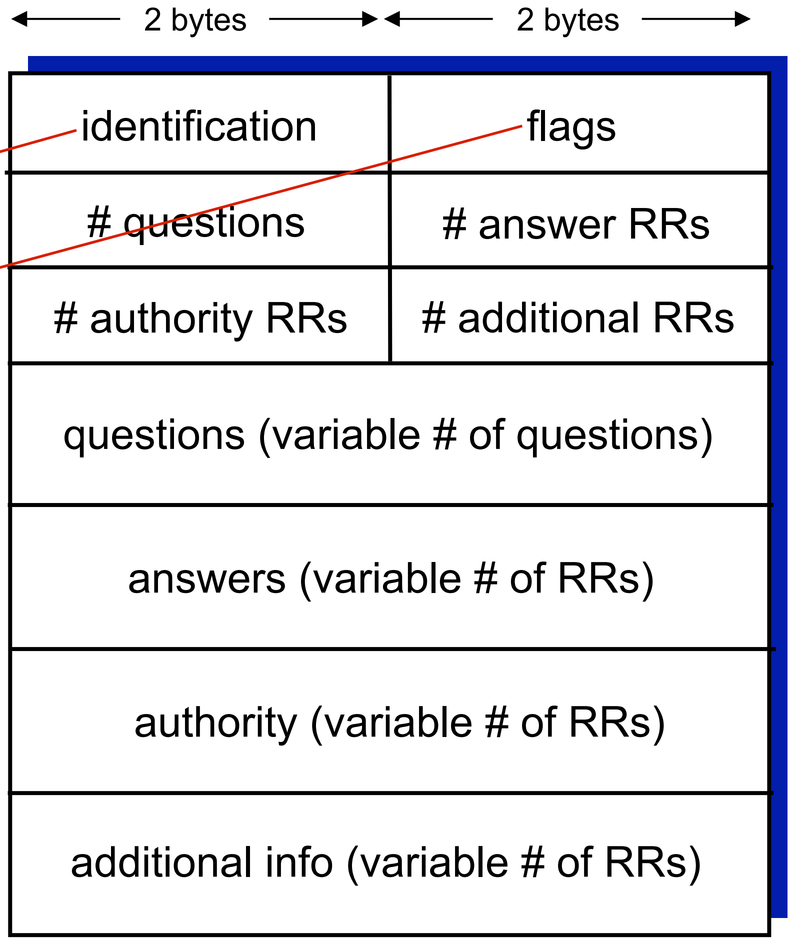
- `value` is name of mailserver associated with `name`

DNS protocol, messages

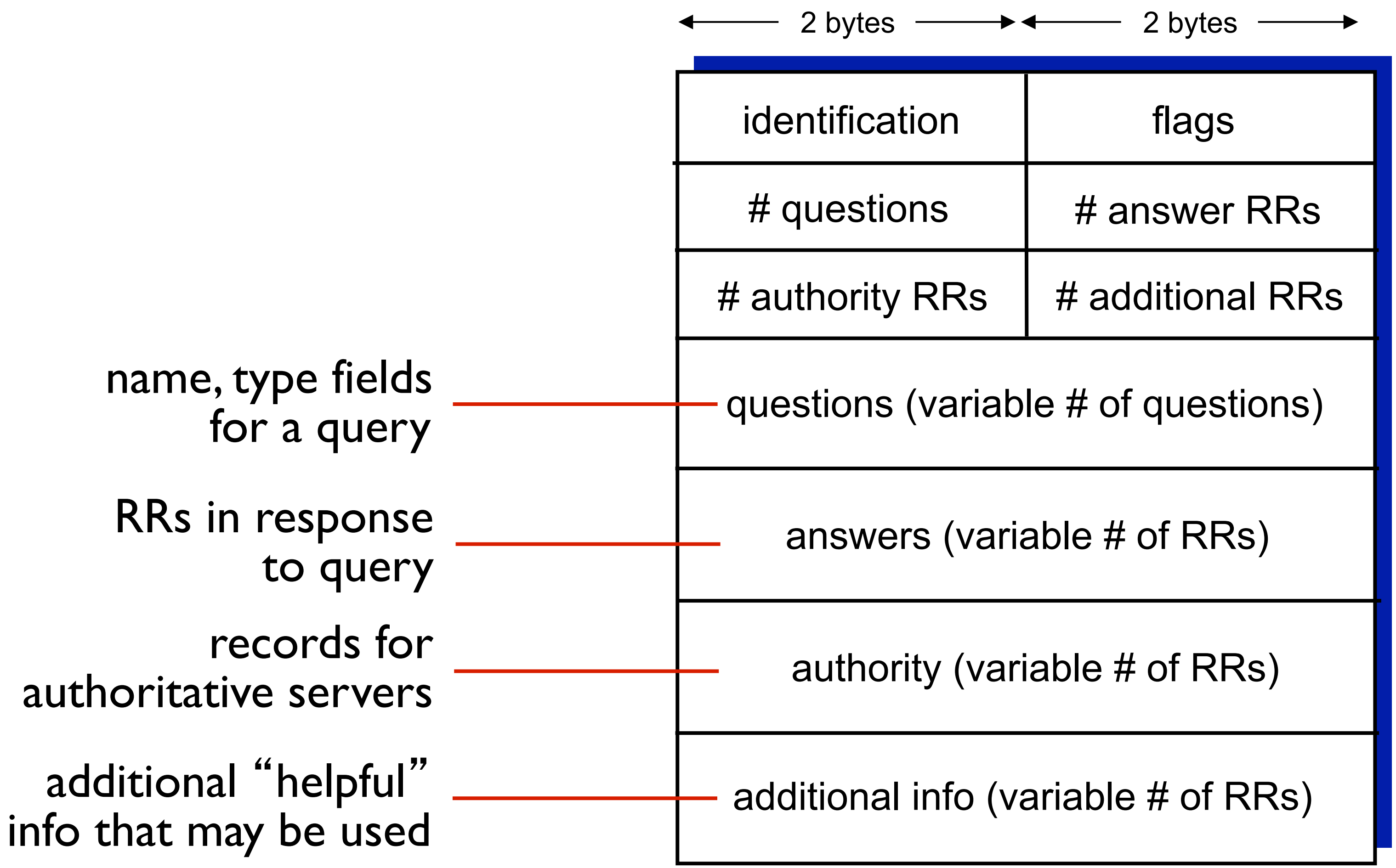
- *query* and *reply* messages, both with same *message format*

msg header

- identification: 16 bit # for query, reply to query uses same #
- flags:
  - query or reply
  - recursion desired
  - recursion available
  - reply is authoritative



DNS protocol, messages



Inserting records into DNS

- 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:
    `(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

Attacking DNS

DDoS attacks

- Bombard root servers with traffic
  - Not successful to date
  - Traffic Filtering
  - Local DNS servers cache IPs of TLD servers, allowing root server bypass
- Bombard TLD servers
  - Potentially more dangerous

Redirect attacks

- Man-in-middle
  - Intercept queries
- DNS poisoning
  - Send bogus replies to DNS server, which caches

Exploit DNS for DDoS

- Send queries with spoofed source address: target IP
- Requires amplification

SECURITY

DNS poisoning slams web traffic from millions in China into the wrong hole

ISP blames unspecified attack for morning outage

By John Leyden, 21 Jan 2014 Follow 2,451 followers

8

A widespread DNS outage hit China on Tuesday, leaving millions of surfers adrift.

DNS issues in China between 7am and 9am GMT left millions of domains inaccessible. Two-thirds of China's DNS (Domain Name System) infrastructure was blighted by the incident, which stemmed from a cache poisoning attack.

Chinese netizens were left unable to visit websites or use social media and instant messaging services as a result of the screw-up, the Hong Kong-based *South China Morning Post* reports.

The snafu, which affected China's root servers, meant all queries resolve to the IP address 65.49.2.178. A fix was implemented around two hours after the snag first surfaced.

All China's generic top-level domain names were affected. Services provided by local internet giants such as search engine Baidu and social-media portal Sina.com were rendered unavailable to locals unless they accessed them through virtual private network (VPN) technology.

DNS servers provide a lookup function that converts domain names, such "www.baidu.com," into a numerical IP address understood by routers and servers.

The cause of the problem, which might take up to 12 hours to be fully resolved, was not immediately clear, with an attack by hackers being at least one of the possible reasons.

DNSPod, a DNS provider that describes itself as the largest in the country, handling three million domains, put out an update on Twitter blaming an attack without going into details.

More coverage of the incident can be found in a story by the *Wall Street Journal* here. ®

RELATED STORIES

Three-yaargh! Major UK mobile network's data goes down

Exclusive Revealed: How Microsoft DNS went titsup globally on Xbox One launch day

BIND 9 patched against remote crash vuln

Vixie warns: DNS Changer 'blackouts' inevitable

MORE READING

MOST READ MOST COMMENTED

MH370 airliner MYSTERY: The *El Reg* Pub/Dinner-party Guide

GRAV WAVE TSUNAMI boffinry BONANZA – the aftershock of the universe's Big Bang

It's all in the wrist: Google crams cloud brains into tiny Android Wear WATCH-PUTERS

Google hit by Monday morning blues: Talk, Hangouts, Sheets crash

Malaysia Airlines mystery: Click here for the TRUTH

SPOTLIGHT

Soon-to-be Facebook intern wins UK Cyber Security Challenge

272

MH370 airliner MYSTERY: The *El Reg* Pub/Dinner-party Guide

42

Spam, a lot of it: Bubble tea is the Seoul of wit

41

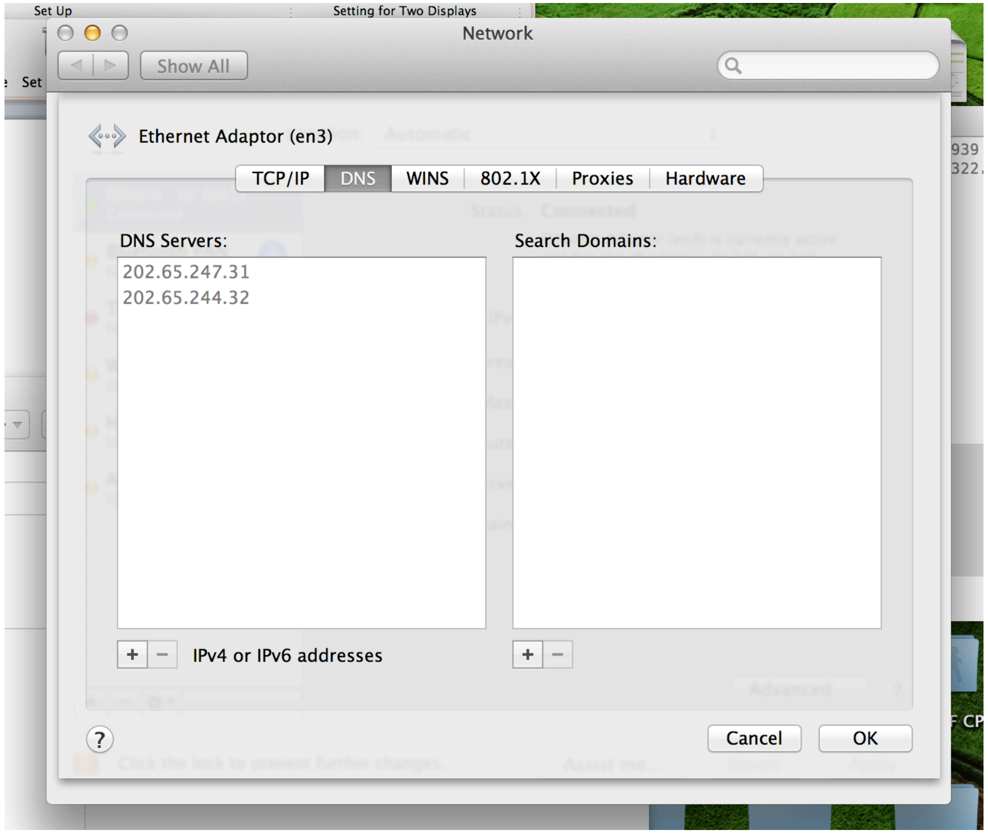
Anti-snoop Blackphone hits shelves in June: NOW we'll see how much you value privacy

MORE

Activity 4.1: DNS via nslookup

Davids-MacBook-Pro-2:~ david_yau$ nslookup www.csail.mit.edu
Server: 202.65.247.31
Address: 202.65.247.31#53

Non-authoritative answer:
Name: www.csail.mit.edu
Address: 128.30.2.155



What's IP addr of www.csail.mit.edu?

Who provided the answer?

What is 202.65.247.31?

Why is the answer non-authoritative?

Activity 4.2: DNS via dig

1. Familiarize yourself with the dig tool

    % man –s 1 dig

2. You'd like to email leighton@mit.edu. Find the email server you should use.

3. How many answers did you get? Why might it be useful to have more than one answer?

4. Now find the IP address of the first server.

5. Use whois to verify the organization that owns the IP address in Q4.
You can use either the command line, or http://who.domaintools.com

Activity #3: dig from M1 can see more!

```
236:~ david_yau$ dig mit.edu MX
. . .
;; ANSWER SECTION:
mit.edu. 120 IN MX 100 dmz-mailsec-scanner-4.mit.edu.
mit.edu. 120 IN MX 100 dmz-mailsec-scanner-5.mit.edu.
mit.edu. 120 IN MX 100 dmz-mailsec-scanner-6.mit.edu.
mit.edu. 120 IN MX 100 dmz-mailsec-scanner-7.mit.edu.
mit.edu. 120 IN MX 100 dmz-mailsec-scanner-8.mit.edu.
mit.edu. 120 IN MX 100 dmz-mailsec-scanner-1.mit.edu.
mit.edu. 120 IN MX 100 dmz-mailsec-scanner-2.mit.edu.
mit.edu. 120 IN MX 100 dmz-mailsec-scanner-3.mit.edu.

;; AUTHORITY SECTION:
mit.edu. 10073 IN NS ns1-37.akam.net.
mit.edu. 10073 IN NS use2.akam.net.
mit.edu. 10073 IN NS asia2.akam.net.
mit.edu. 10073 IN NS ns1-173.akam.net.
mit.edu. 10073 IN NS asia1.akam.net.
mit.edu. 10073 IN NS use5.akam.net.
mit.edu. 10073 IN NS eur5.akam.net.
mit.edu. 10073 IN NS usw2.akam.net.

;; ADDITIONAL SECTION:
dmz-mailsec-scanner-1.mit.edu. 1800 IN A 18.9.25.12
```

1. What new answers do you get?
2. What is the DNS type of the “extra” records returned? What does the type mean?
3. Ask your local DNS server to find the IP addr. of dmz-mailsec-scanner-3.mit.edu.
4. Now use the authoritative name server asia2.akam.net to do the resolution in Q3. Do the two answers agree?
5. What’s the IP addr. of asia2.akam.net?
6. Use whois to find out who owns the IP addr. in Q5.
7. Do a web search for the company in Q6, and briefly describe the company’s business.

Reflections on DNS

- Protection domains to the next level (cf. OS processes)
  - Different *physical machines*: strong modularity, strong fault isolation
- Distributed (hierarchical) servers: scalability
- *Indirection* (name-IP addr) some virtues
  - Late binding: runtime — Server can move
  - Many-to-one mappings — Aliasing
  - One-to-many mappings — Load balancing
- Cost of indirection?
  - Delay, security (poisoned/intercepted mappings)