Managing and Monitoring a Root DNS Service

John Crain
Chief Technical Officer

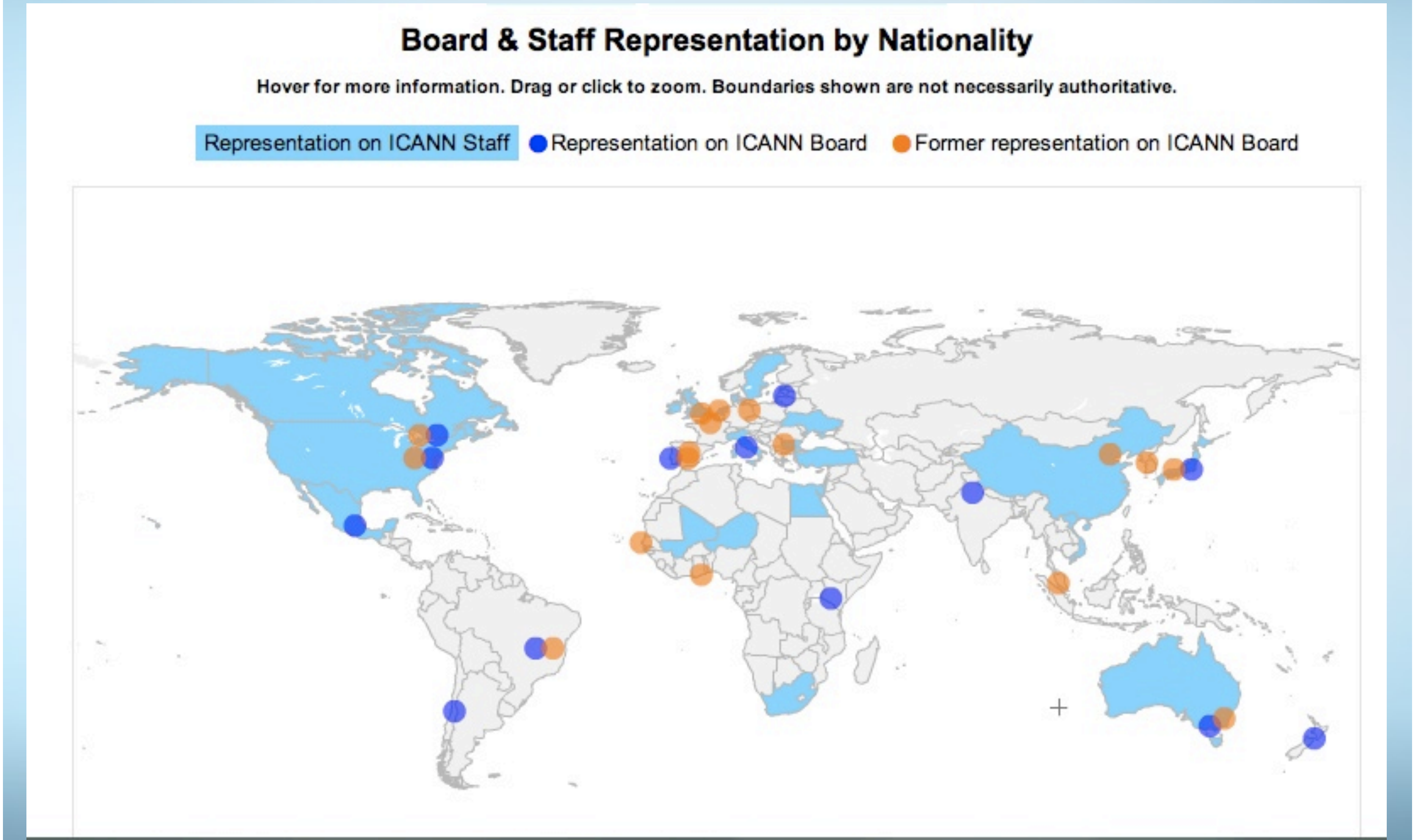
ICANN

Who am I?

- John Crain
  - Chief Technology Officer at ICANN
- Involved with ICANN since early days.
- Prior to ICANN at the RIPE NCC in Amsterdam,
- Prior to that a Design Engineer, designing processes for developing Advanced Thermoplastic Composites.

What is ICANN?

- International, Public Benefit, non-profit organization charged with managing the Internet's identifier systems.
- Ensuring "Security and Stability" of those systems is a core goals
- One of those systems is the Domain Name System. Specifically the content of the "Root Zone".



Board & Staff Representation by Nationality

Hover for more information. Drag or click to zoom. Boundaries shown are not necessarily authoritative.

Representation on ICANN Staff ● Representation on ICANN Board ● Former representation on ICANN Board

Why is the DNS important

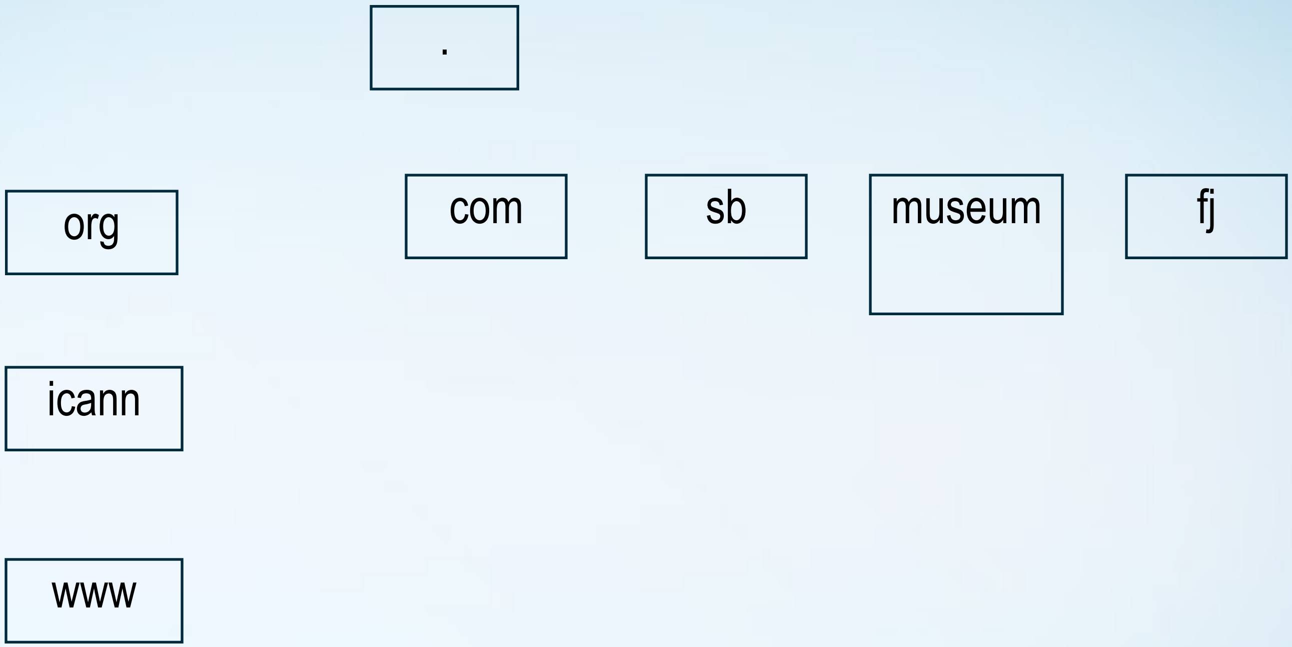
- People use domain names to navigate the Internet
  - Domain names are also used on business cards and advertising
  - **What can you do without your domain name?**

Domain Name System

- Translates the human usable names to machine usable IP addresses
  - www.icann.org to 208.77.188.103

- Hierarchical Database with the entry level, known to all DNS resolvers being the DNS root name servers

The Dot You Forgot!



.

org

com

sb

museum

fj

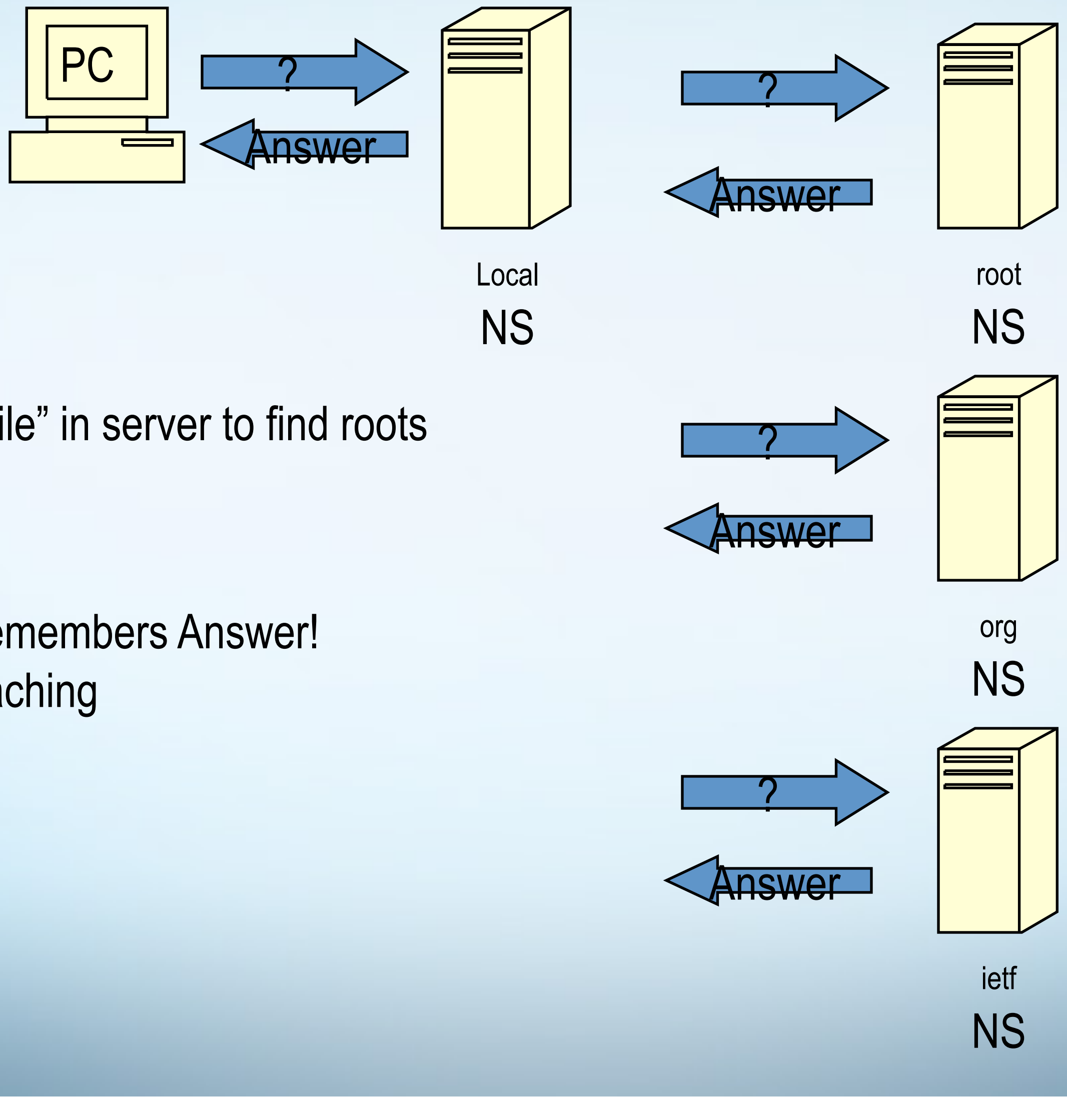
icann

www

http://www.icann.org.

Finding the IP address

(using www.ietf.org as example)



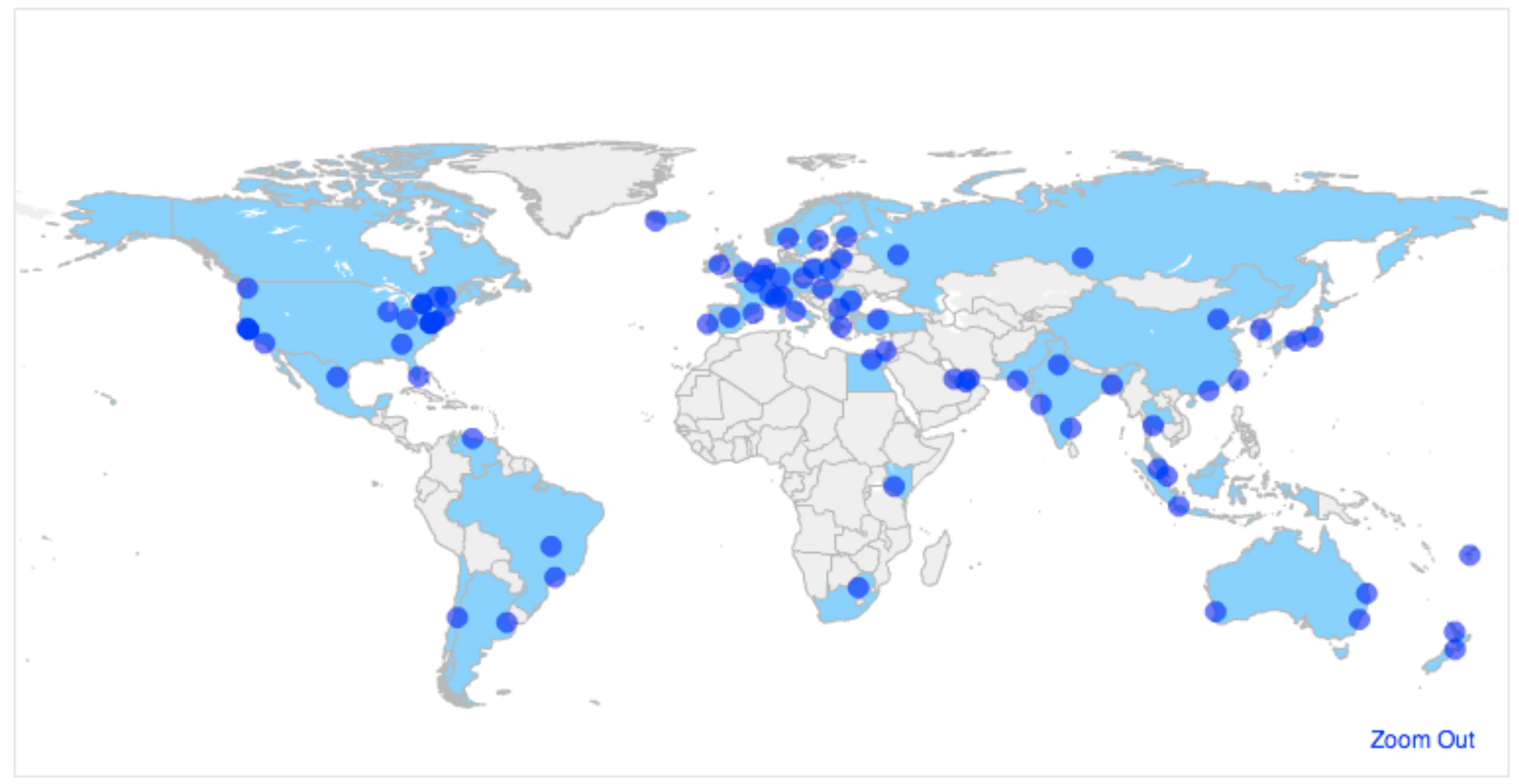
Uses “hints file” in server to find roots

Remembers Answer!
Caching

Root servers are part of the core infrastructure

- 13 Servers systems
  - Named a through m.root-servers.net
  - Through any-cast we have more than 100 locations
- Operated by 12 organizations
  - http://www.root-servers.org
- L.root-servers.net operated by ICANN

http://www.icann.org/maps/root-servers.htm



Monitoring the root takes coordination

- Monitoring can be done externally with standard tools such as DIG, NSLookup, Ping etc. etc.

- Good example is DNSmon

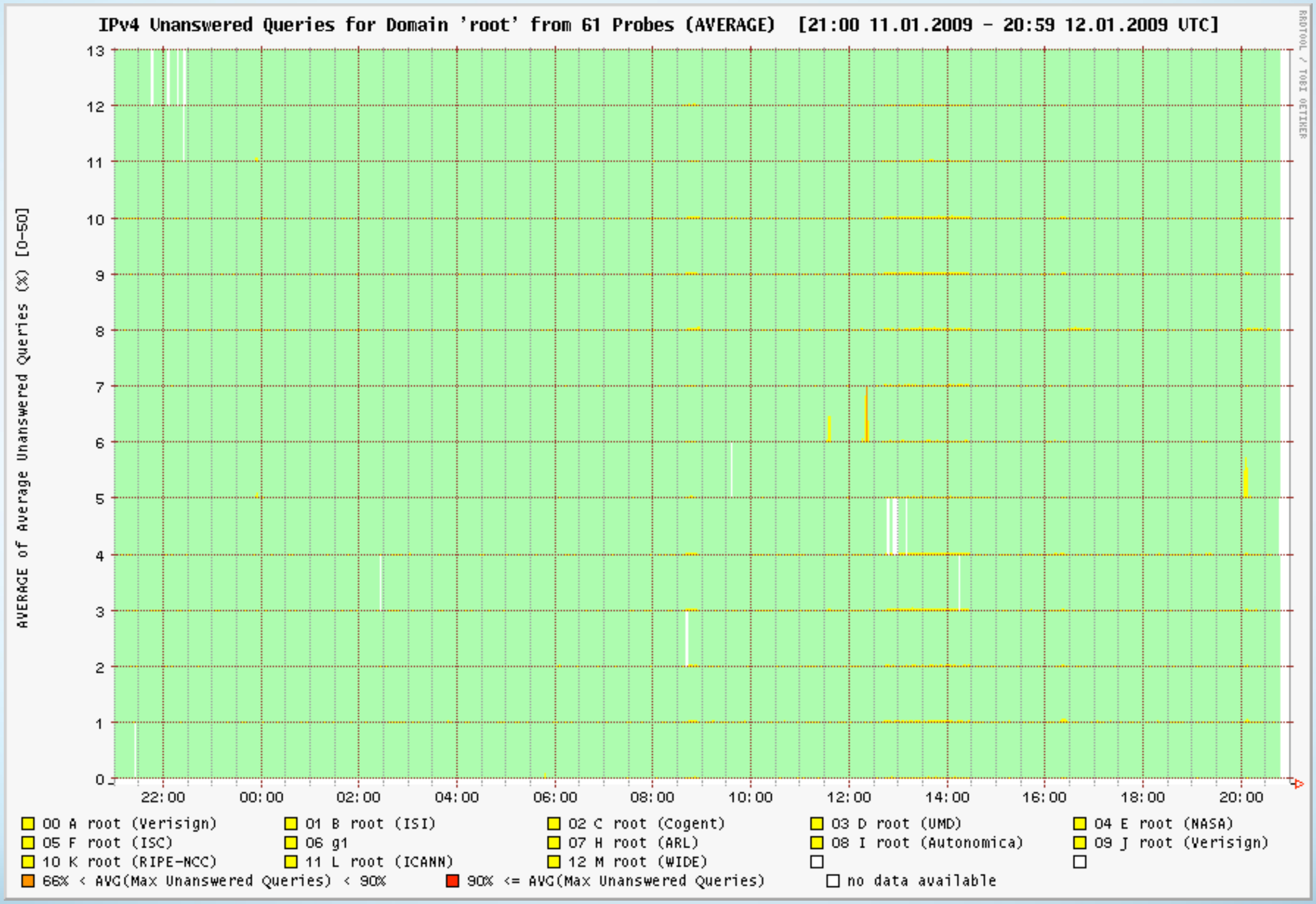
  - http://dnsmon.ripe.net

DNSmon run by RIPE NCC

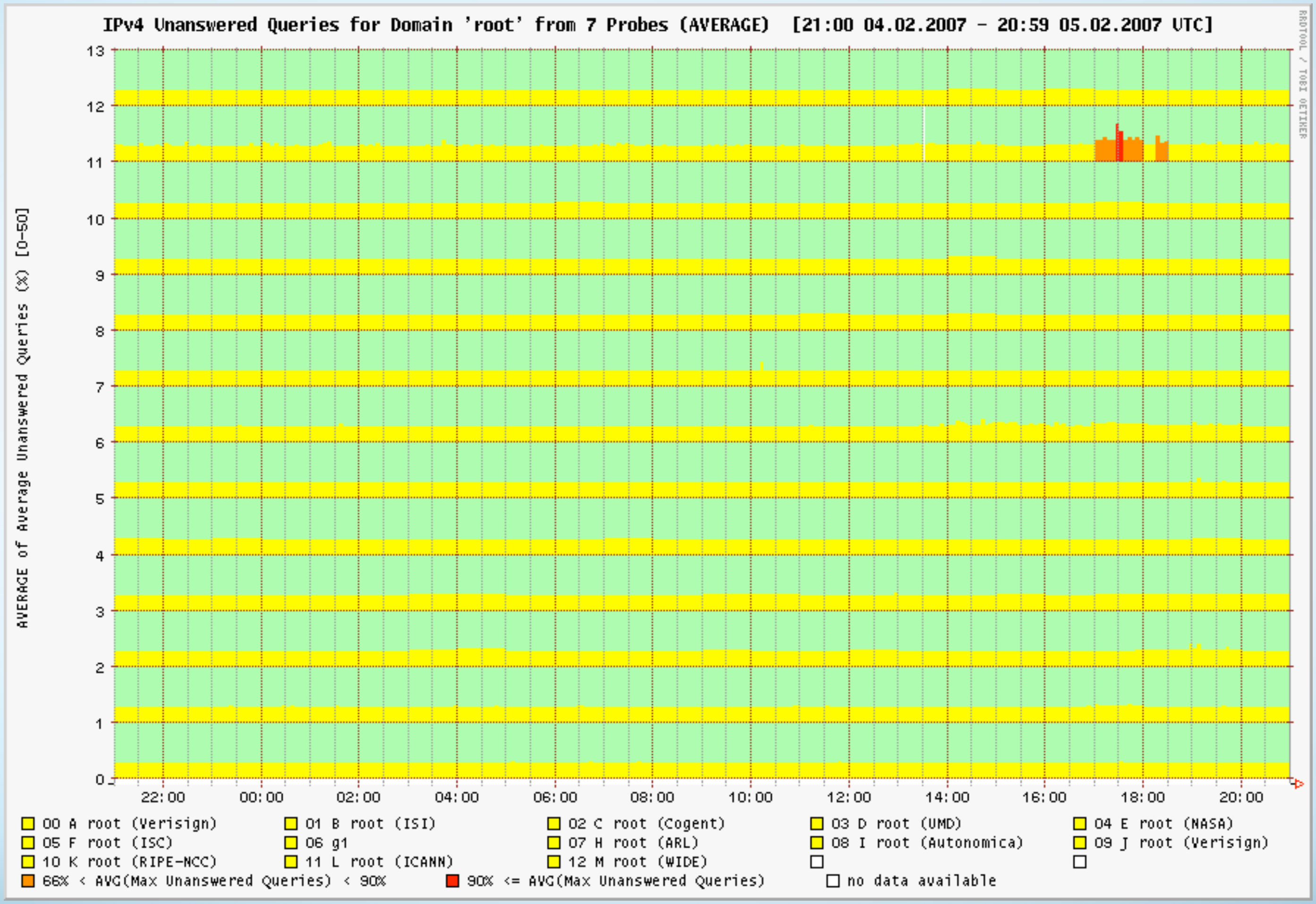
- Sends DNS queries to servers from multiple locations giving a good status of the service as seen from “The Internet”.

- Monitors servers for various zones, including the “root zone”

DNSmon on a good day



DNSmon on a not so good day



Domain Name System Operations, Analysis and Research Center

- http://www.dns-oarc.net

- Formed as a member organization where DNS operators and researches can collaborate on studying the DNS and on operational response when needed.

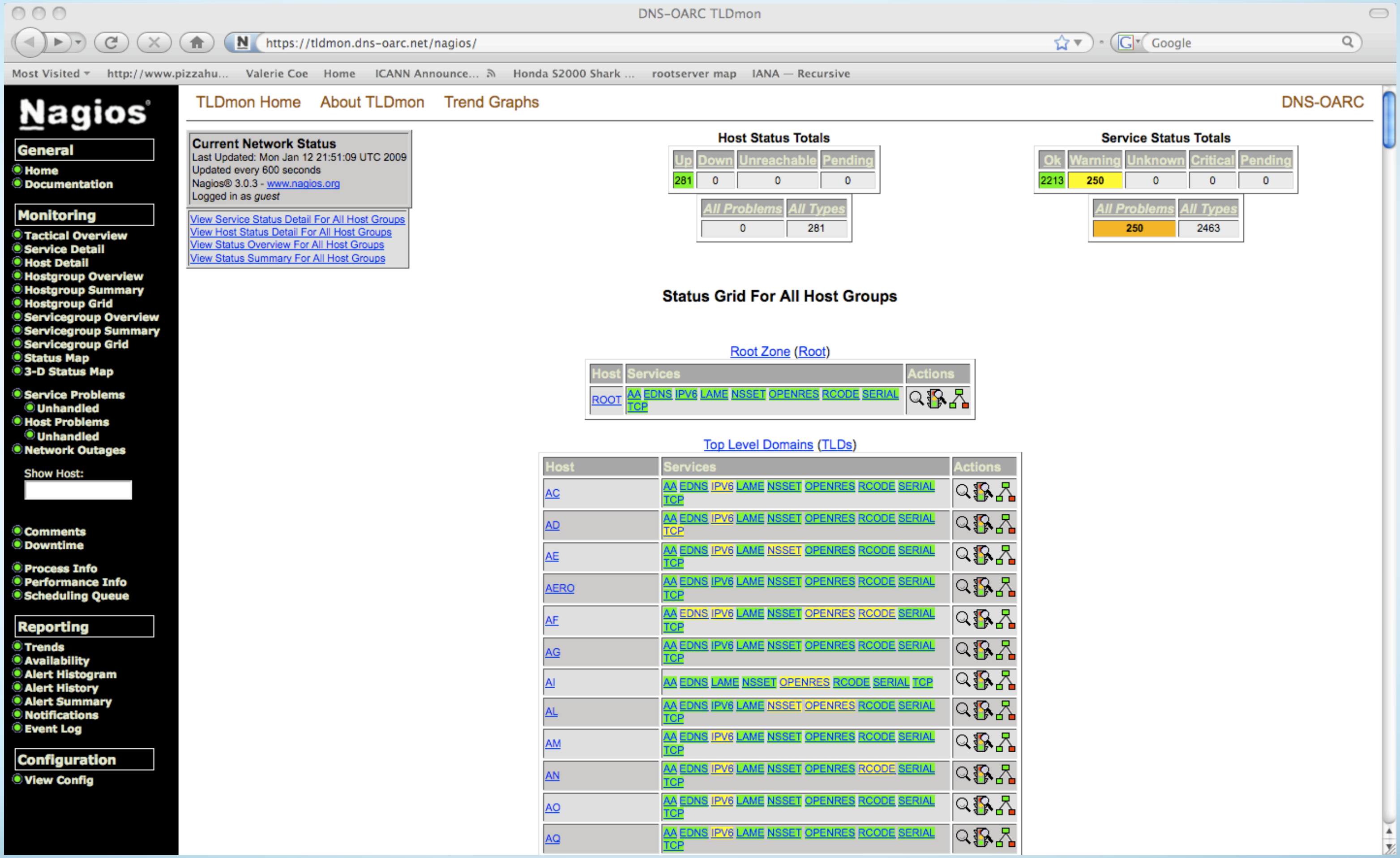
TLD status monitor

- Nagios running scripts written by the measurement factory.

- https://tldmon.dns-oarc.net
- https://tldmon.dns-oarc.net/nagios/

- (We use versions of the same scripts for monitoring L-root)

TLDmon from OARC



Current Network Status
Last Updated: Mon Jan 12 21:51:09 UTC 2009
Updated every 600 seconds
Nagios® 3.0.3 - www.nagios.org
Logged in as *guest*

View Service Status Detail For All Host Groups
View Host Status Detail For All Host Groups
View Status Overview For All Host Groups
View Status Summary For All Host Groups

Host Status Totals

Up	Down	Unreachable	Pending
281	0	0	0

All Problems	*All Types*
0	281

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
2213	250	0	0	0

All Problems	*All Types*
250	2463

Status Grid For All Host Groups

Root Zone (Root)

Host	Services	Actions
ROOT	AA EDNS IPV6 LAME NSSET OPENRES RCODE SERIAL TCP	

Top Level Domains (TLDs)

Host	Services	Actions
AC	AA EDNS IPV6 LAME NSSET OPENRES RCODE SERIAL TCP	
AD	AA EDNS IPV6 LAME NSSET OPENRES RCODE SERIAL TCP	
AE	AA EDNS IPV6 LAME NSSET OPENRES RCODE SERIAL TCP	
AERO	AA EDNS IPV6 LAME NSSET OPENRES RCODE SERIAL TCP	
AF	AA EDNS IPV6 LAME NSSET OPENRES RCODE SERIAL TCP	
AG	AA EDNS IPV6 LAME NSSET OPENRES RCODE SERIAL TCP	
AI	AA EDNS LAME NSSET OPENRES RCODE SERIAL TCP	
AL	AA EDNS IPV6 LAME NSSET OPENRES RCODE SERIAL TCP	
AM	AA EDNS IPV6 LAME NSSET OPENRES RCODE SERIAL TCP	
AN	AA EDNS IPV6 LAME NSSET OPENRES RCODE SERIAL TCP	
AO	AA EDNS IPV6 LAME NSSET OPENRES RCODE SERIAL TCP	
AQ	AA EDNS IPV6 LAME NSSET OPENRES RCODE SERIAL TCP	

Day In The Life of the Internet

- A project from CAIDA with data provided through OARC.
- http://www.caida.org/projects/ditl/
- 48 hr data dump from various authoritative DNS servers (Including 8 of the 13 root-servers)
- Overlapping 24hr data set used.
- 8 billion queries studied in 24hr data set

Lessons learnt from DITL

- Amount of unnecessary queries to the roots is massive > 97%

- Non existent TLDS (22% of total traffic!)
- Repeat queries (servers not caching answer?)
- A for A queries
  - (asking for the IP Address of an IP address)

Operating the L root

- Two large Clusters in Los Angeles and Miami.
- Combined total of more than 80 servers answering DNS.
- Peering directly with more than 50 networks throughout the globe

Local Monitoring

- Until recently no good DNS traffic monitoring software.

- Lots of Nagios/Cacti stats
  - Dig, Ping, Memory/CPU usage etc.

- Domains Statistics Collector
  - Developed by the measurement factory
  - Takes live feed of traffic and places stats into arrays based on predefined parameters.

Gives live view of queries

- Updates XML files to a presenter server every 60s
  - – Shows us many of the trends that we see on DITL
  - – For L root we publish a delayed version
  - – http://stats.l.root-servers.org

Global DNS Risk Symposium

Feb 3-4 2009, Atlanta, Georgia

Goals:

Increase understanding of DNS risk to the user community

Examine strengths and weaknesses of current efforts to share technical practices and operational approaches with a goal of improving collaboration in mitigating risks and filling gaps.

Specific focus areas:

- Understanding large enterprise DNS reliance and enabling effective risk mitigation
- Meeting the challenges to secure and resilient DNS operations in the developing world
- Identifying and improving collaboration in combating malicious activity leveraging the DNS

Questions?

Thank You