

Recent DNS Events and OARC Activities

Keith Mitchell

**OARC Programme Manager
Internet Systems Consortium**

CENTR/RIPE54

Tallinn, Estonia

May 2007



What is OARC ?

- Operations, Analysis and Research Center for the Internet
- Co-ordination centre to protect Global DNS infrastructure
- Trusted, neutral environment for operators and researchers to:
 - gather and share data
 - co-ordinate response to attacks
- Secretariat run and managed by ISC
 - Keith's day job

OARC Members

- Afilias
- AFNIC
- APNIC
- Autonomica
- BFK
- Cambridge Univ
- ChangeIP.com
- CIRA
- Cisco
- Cogent
- CZ.NIC
- Damballa
- DENIC
- eNom
- EP.net
- F-root
- Georgia Tech
- Google
- II-F
- Internet Perils
- ISC
- ISoc-IL
- Microsoft
- NASA Ames
- NASK
- *NIC.CL*
- NIDA
- Nlnet Labs
- Nominet UK
- NTT
- *OpenDNS*
- PIR
- Registro.BR
- RIPE NCC
- Shinkuro
- SIDN
- Team Cymru
- UMR.edu
- NeuStar/uDNS
- UMD.edu
- WIDE

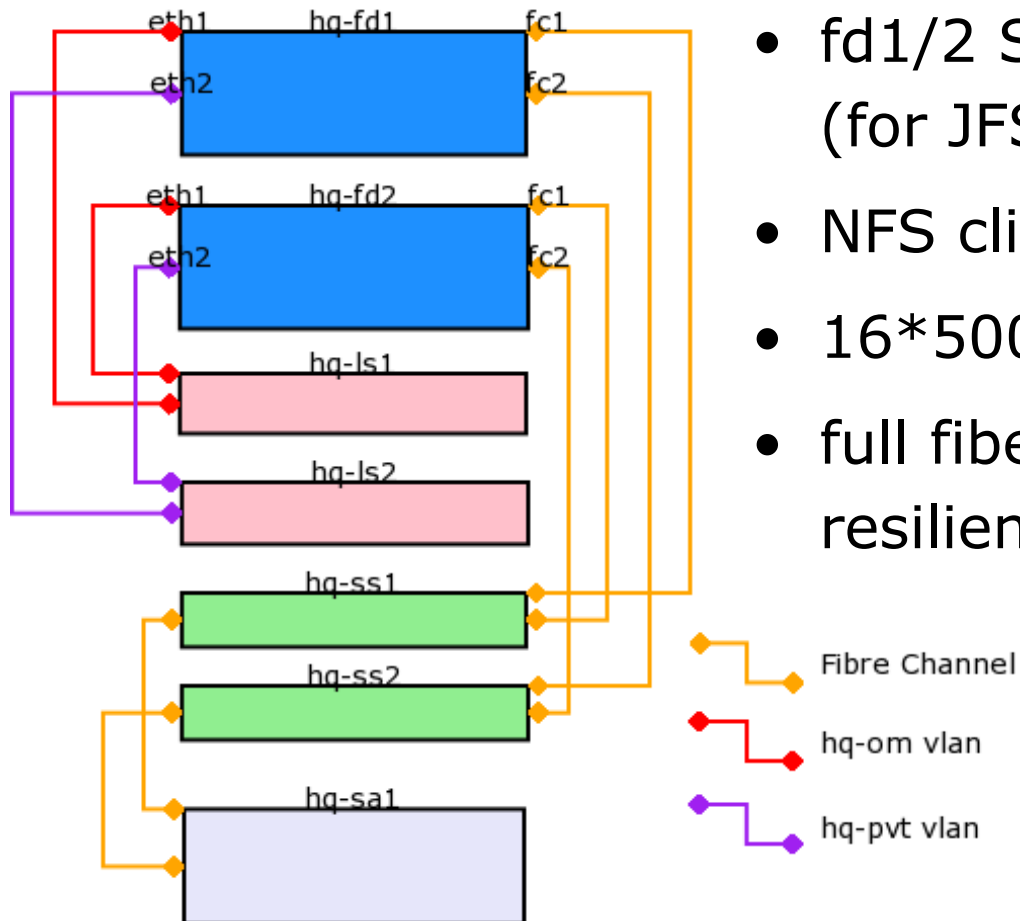


OARC Systems

- Main server resources are FreeBSD Celestica Opteron-based boxes located in ISC rack at PAIX
- in1 and in2.oarc.isc.org provide main world/member-facing services
 - websites, e-mail, jabber
- an1 and an2 for DSC data analysis
- fd1 and fd2 fiberchannel-attached dual storage servers for hosting data
- gs1 and gs2 guest access for other projects
- also console server, switch etc



OARC RAID Architecture



- fd1/2 SuSE-10.1 Linux-based (for JFS support)
- NFS clients FreeBSD-based
- 16*500Gb SATA in RAID6
- full fiberchannel multipath resilience planned

Systems Upgrades

- Recently Completed:
 - in1 FreeBSD 5.4 → in2 FreeBSD 6.2 migration
 - Jabber server supports full s2s SSL
 - CVS repository available for shared tool development: DSC, DNSCAP, oarsh
- To Do:
 - Deploy full resilience for RAID servers
 - Need to add significant storage capacity in medium term ("SATAbeast")
 - Evaluate FreeBSD/ZFS as alternative to Linux/JFS



New Tool: DNSCAP

- Network capture utility designed specifically for DNS traffic
- Similar to tcpdump, but better recognition of DNS transactions and protocol options
- Produces binary data in pcap format
- <http://public.oarci.net/tools/dnscap/>

“Day in the Life of the Internet”

- Wide-ranging collaborative research project to improve “network science” by building up baseline of regular Internet measurement data over 48-hour periods
- See <http://www.caida.org/projects/ditl/>
- DNS data gathered via OARC is one part of this

DITL 8-10th Jan 2007

- OARC has supported this annually since 2004
- DNS query data gathered close to participating root and TLD servers using tcpdump into "PCAP" files
- Uploaded via ssh script to central OARC RAID system
- Available to OARC members for analysis

DITL Jan 2007 Participants

- **c.root-servers.net** Cogent
- **e.root-servers.net** NASA
- **f.root-servers.net** ISC
- **k.root-servers.net** RIPE NCC
- **m.root-servers.net** WIDE
- **as112.namex.it** NaMEX
- **b.orsn-servers.net** FunkFeur
- **m.orsn-servers.net** Brave GmbH

DITL Challenges

- Too much data
 - problem of success !
 - ran out of disk space 2 hours before end
 - “in-flight” upgrade to fix this...
- Limited space on collecting servers
- Bandwidth loss due to Taiwan quake
- Too close to seasonal holiday
- Bleeding-edge platforms

DITL Lessons Learned

- Do pending upgrades and estimate of data volumes **before** you start !
- Simple legalities = enlarged participation 😊
- Data uploading was harder than gathering
 - dry-runs helpful
- Disable auto-rotation
- Generate, preserve, share and validate data
MD5 checksums
- Upgraded hardware performed well overall

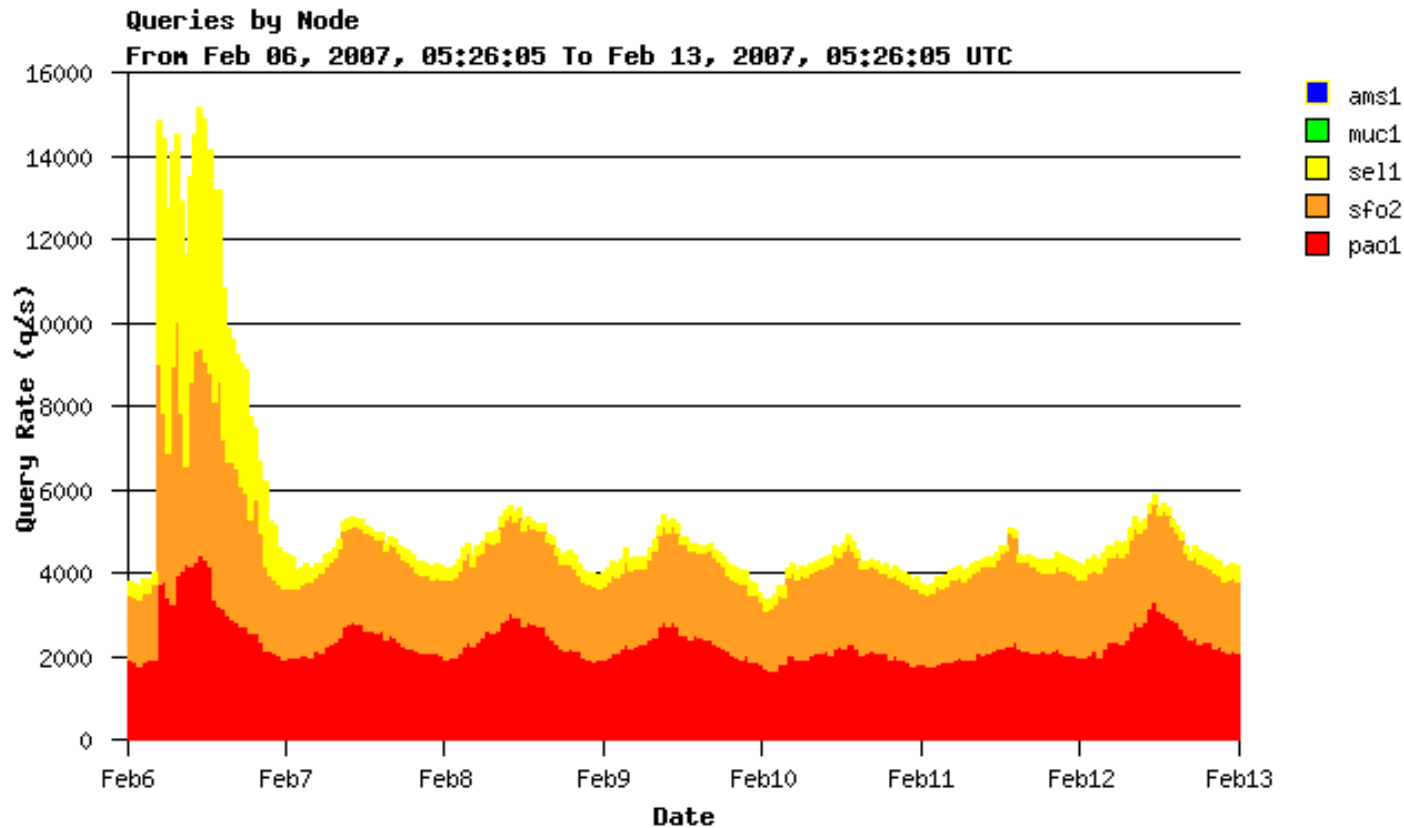


DITL Results

- OARC RAID now holds over 2TB of data
 - available for research analysis
 - space for at least as much again
- Report summarising outcomes available to participants and OARC members
- More roots interested for next time
- Left us in great shape to do it again without notice 4 weeks later...

Root DDoS Attack

6th Feb 2007



Attack overview

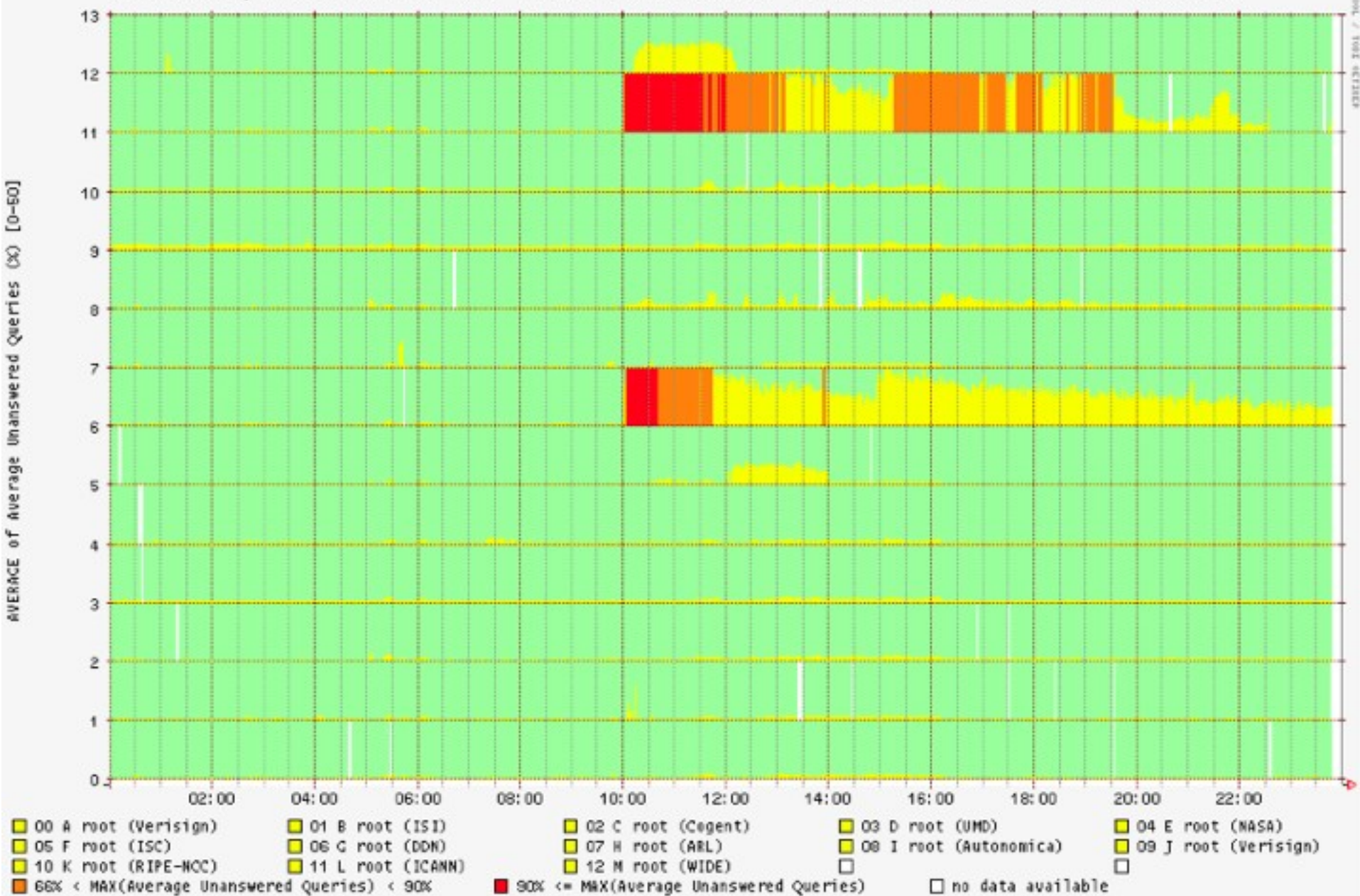
- Commenced at 10:00 UTC on Tue 6th Jan for 24 hours
- At least 6 Internet root and 1 TLD name servers sustained a DDoS attack
- Attack did not impact on end-user service, but was measured
- Preliminary observations made at F-root include:
 - type, quantity and distribution of attack traffic
 - how it coped
- See also ICANN report:
 - <http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf>



Attack points of interest

- Happened **exactly** 4 weeks after 2007 DITL
 - may allow baseline comparison
- Happened during NANOG meeting
 - usual suspects on-hand...
- Did not use any exotic amplification techniques
- Mostly did not spoof source addresses

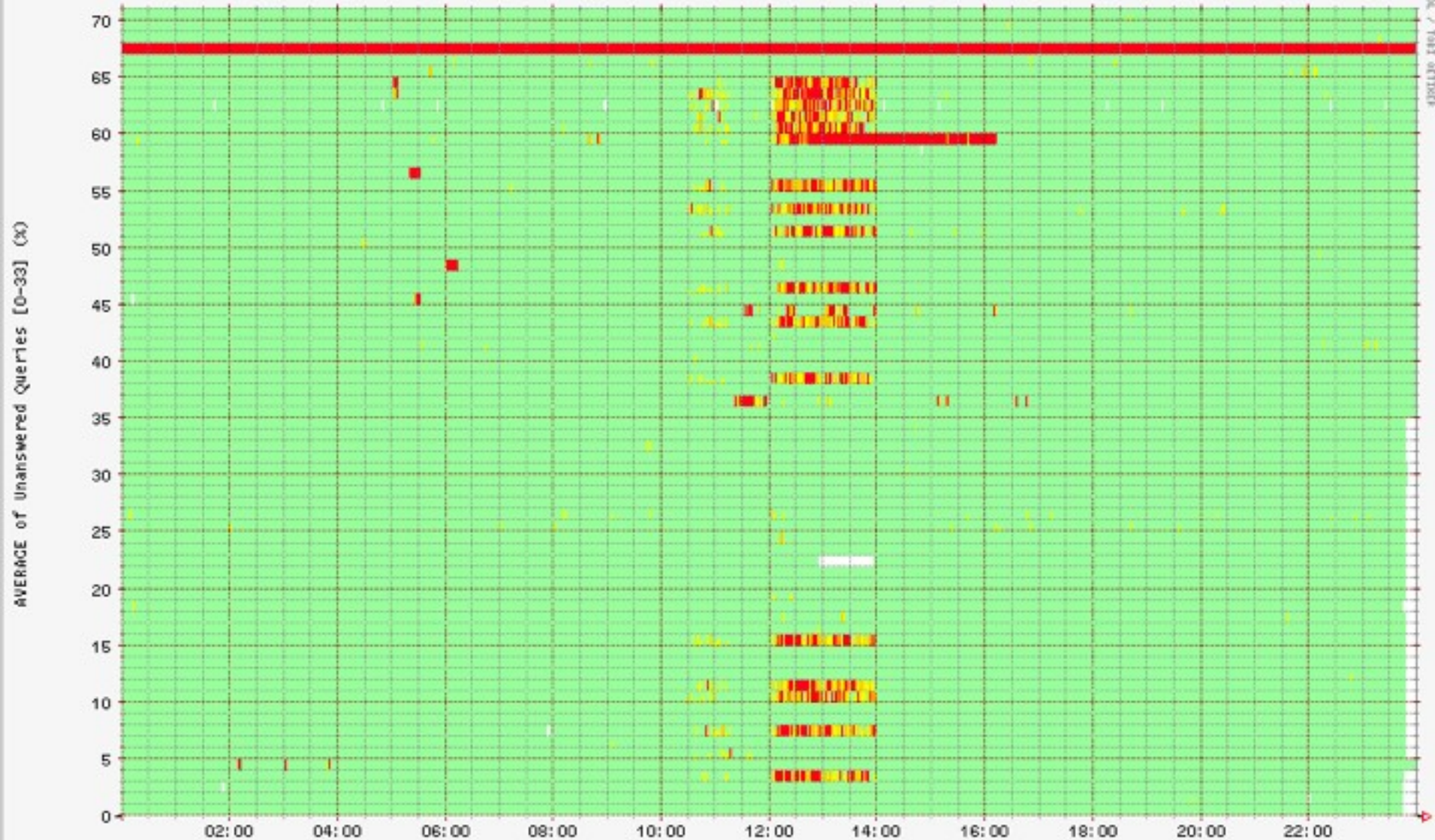
Unanswered Queries for Domain 'root' from 60 Probes (AVERAGE) [06.02.2007 00:00 - 06.02.2007 23:59 UTC]



Service impact



Unanswered Queries (AVERAGE) for F root (ISC) [06.02.2007 00:00 - 06.02.2007 23:59 UTC]



Packet analysis

- All port 53 DNS queries, containing random data
- Average size was bigger than normal traffic
 - Size random up to 1024 bytes
 - Most were more than 350 bytes
- Some were malformed DNS messages
- Contained random QTYPEs
 - updates, unknown, etc

Attack Observations

- Anycast works !
 - end-users not really impacted
 - some f-root nodes impacted, but service overall maintained
 - non-anycast nodes (G, L) hit hardest
- Filtering packets >512 bytes only partially effective
- Main sources S Korea and BellSouth, but .kr caused most of the pain
- More analysis required, will be presented at upcoming NANOG and OARC meetings



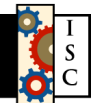
Acknowledgments

- Dave Knight, ISC/Afilias
- Joao Damas, ISC
- John Kristoff, UltraDNS
- ICANN L-root team
- All DITL contributors

OARC Contact Info

- Meeting: At Chicago IETF, 2?/? July
- Web: <https://oarc.isc.org>
- E-mail: keith_mitchell@isc.org
- Jabber: [keith@jabber.oarc.isc.org](jabber:keith@jabber.oarc.isc.org)
- Phone: +1 650 423 1348 (EST)
+44 778 534 6152
- Paper: <http://public.oarci.net/files/oarc-briefing.pdf>

<http://public.oarci.net/files/OARC-Tallinn.pdf>



Questions ?

