Data-Gathering for Recent DNS Events

Keith Mitchell
OARC Programme Manager
Internet Systems Consortium

UKNOF7

3rd Apr 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

Presentation Overview

- OARC Background & introduction
- OARC Data-gathering infrastructure
- “Day in the Life of the Internet”
- Root server attack 6th March 2007

OARC Background and Introduction

OARC Mission

- Provide trusted channels for Internet incident reporting and handling
- Facilitate confidential sharing of DNS operations data
- Interface with research community for analysis and publication
- Outreach to vendors, end-users and law enforcement

OARC Motivation

- DNS infrastructure makes everything work as expected
- DNS outage of any network service provider or large content provider affects everyone using the Internet
- Growing resource demand for Internet:
  - abuse prevention
  - infrastructure protection
  - operational co-ordination

OARC Motivation

- Increasing incidence of attacks against the DNS, e.g.
  - Microsoft outage in 2001
  - DDoS attack on Root Servers 2002
  - Open recursive resolvers Q1 2006
  - DDoS attack on Root Servers Feb 2007
- DNS increasingly implicated in and compromised by Botnet activity

OARC Members

- Current total 44, includes:
  - 6 root server operators
  - 2 gTLD operators
  - 12 ccTLD operators
  - 11 DNS implementers
  - researchers at 5+ institutions
  - RIRs, DNS registrars, operators
- 10+ potential new members in pipeline

OARC Members

- Afilias
- AFNIC
- APNIC
- Autonomica
- BFK
- Cambridge Univ
- ChangeIP.com
- CIRA
- Cisco
- Cogent
- CZ.NIC
- Damballa
- DENIC
- eNom

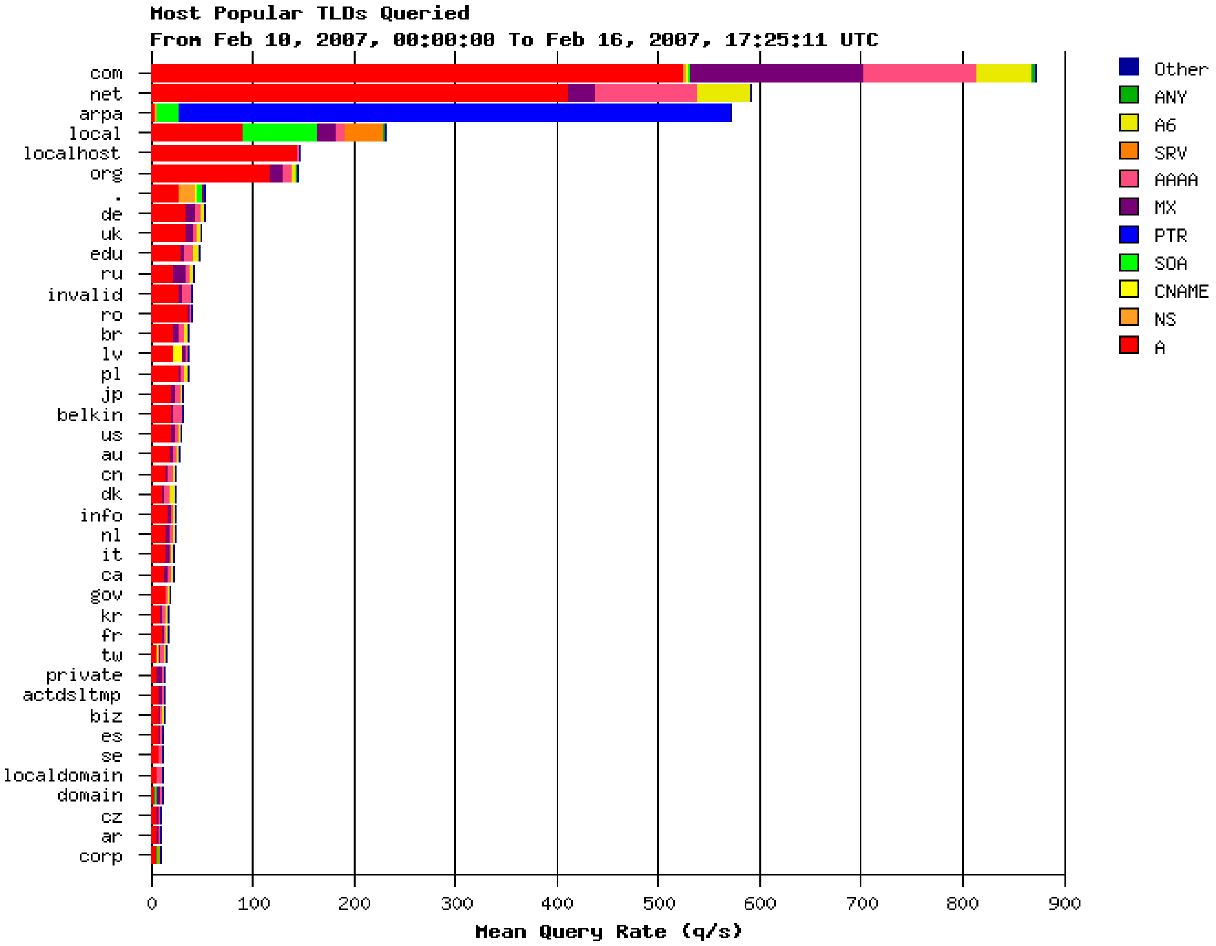
- EP.net
- F-root
- Georgia Tech
- Google
- II-F
- Internet Perils
- ISC
- ISoc-IL
- Microsoft
- NASA Ames
- NASK
- *NIC.CL*
- NIDA
- NInet Labs

- Nominet UK
- NTT
- *OpenDNS*
- PIR
- Registro.BR
- RIPE NCC
- Shinkuro
- SIDN
- Team Cymru
- UMR.edu
- NeuStar/uDNS
- UMD.edu
- WIDE

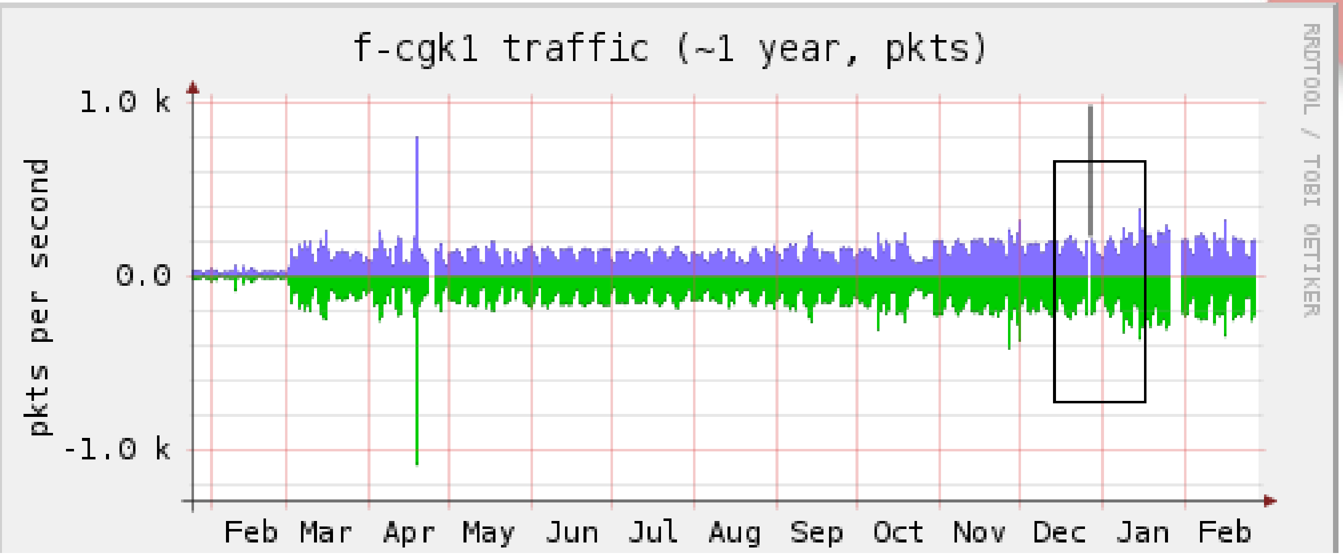
OARC Member Services

- DSC Data Gathering
  - From c, e, f-root, various TLD, and other live servers using DSC toolset
  - Graphing and display of statistics
- Analysis
  - Tools and server resources to allow members (and researchers) to conduct analysis
  - Policies and practices to ensure confidentiality and anonymity of data preserved

DSC Data Gathering


Most Popular TLDs Queried
From Feb 10, 2007, 00:00:00 To Feb 16, 2007, 17:25:11 UTC

Taiwan earthquake



OARC Member Services

- Member-only mailing list
- Encrypted jabber.oarc.isc.org server
  - including private groupchat
- https://oarc.isc.org portal
  - secure member-only “bulletin board”
  - filtered Channel from ISC and between members
  - member-determined bi- and multi-lateral controls on access to all of above
- Annual member meeting

OARC Public Services

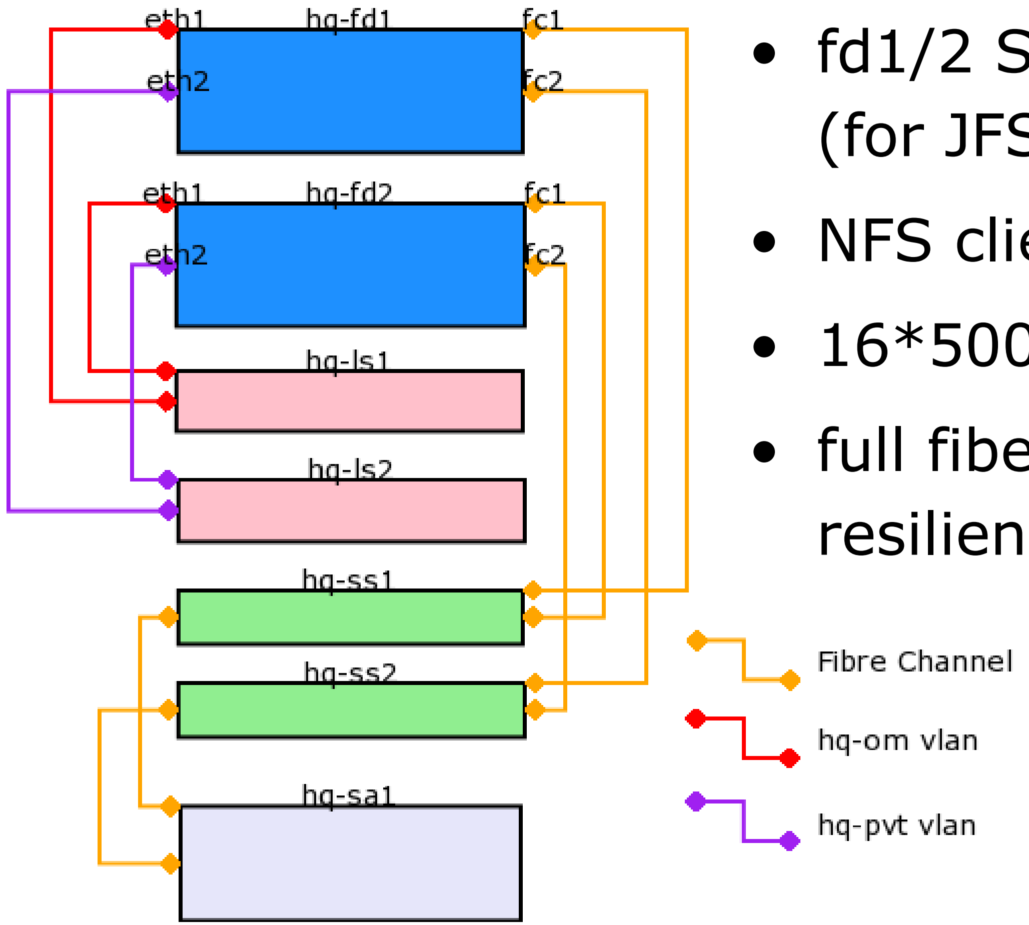
- Twice-yearly open meetings for DNS researchers and operators
- <dns-operations@lists.oarci.net> mailing list
- Two other closed DNS mailing lists
- http://public.oarci.net
  - Drupal-based content repository and forums
- Home for:
  - “Orphan Projects”
  - “Flood Victims”

OARC Data-Gathering Infrastructure

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
- To Do:
  - Deploy full resilience for RAID servers
  - Need to add significant storage capacity in medium term (“SATAbeast”)

A “Day in the Life of the Internet” (DITL) 8-10th Jan 2007

“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

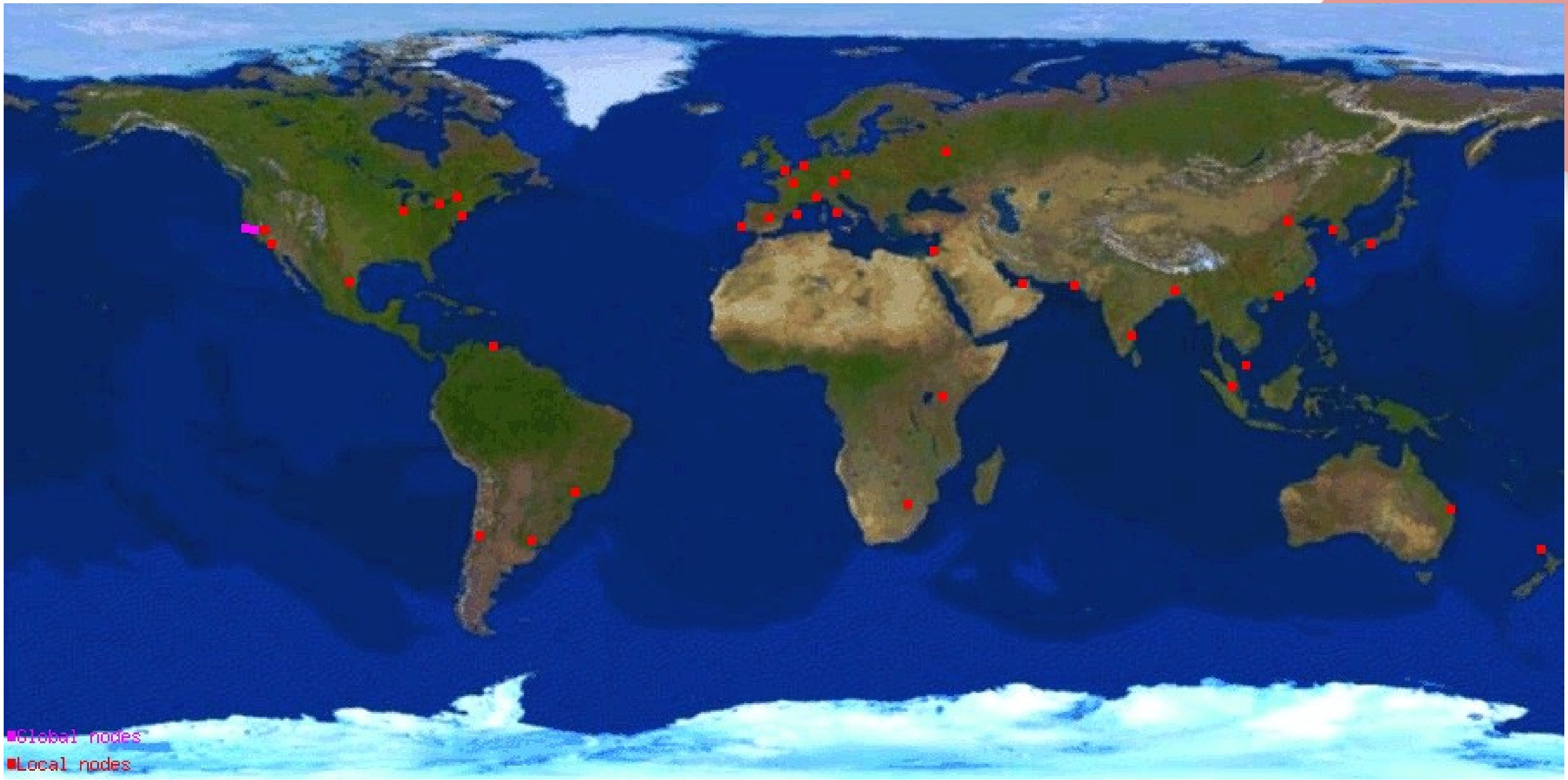
- Do pending upgrades and estimate of data volumes **before** you start !
- Simple legalities = enlarged participation☺
- Data uploading was harder than gathering
  - dry-runs helpful
- Disable auto-rotation
- Generate, preserve, share and validate data MD5 checksums
- Upgraded hardware performed well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

DITL Results

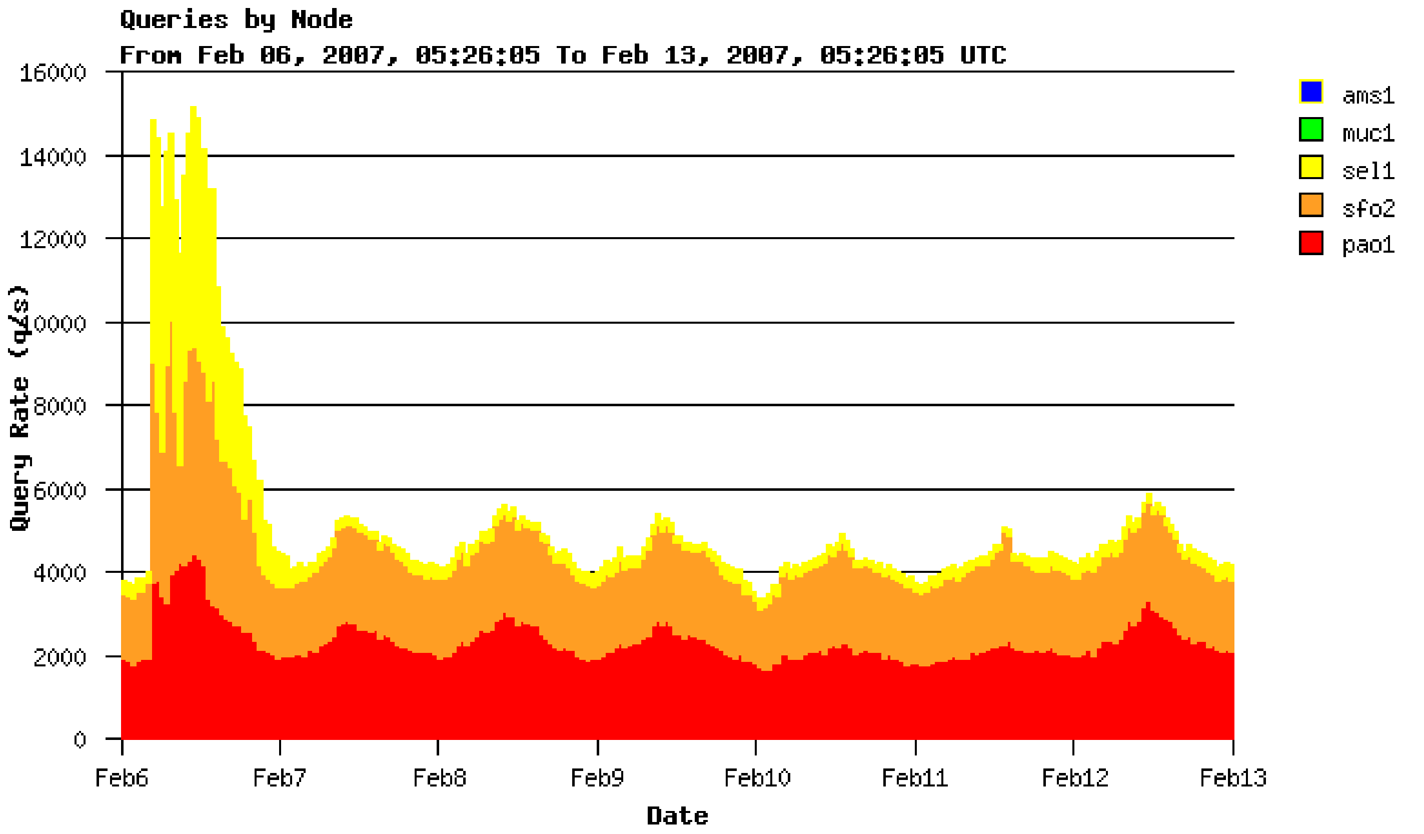
- OARC RAID now holds over 2TB of data
    - available for research analysis
    - space for at least as much again
- Report summarising outcomes available to participants and OARC members
- More roots interested for next time
- Left us in great shape to do it again without notice 4 weeks later...

Root Server DDoS Attack
6th Feb 2007

F-root Anycast Instances



Root DDoS Attack



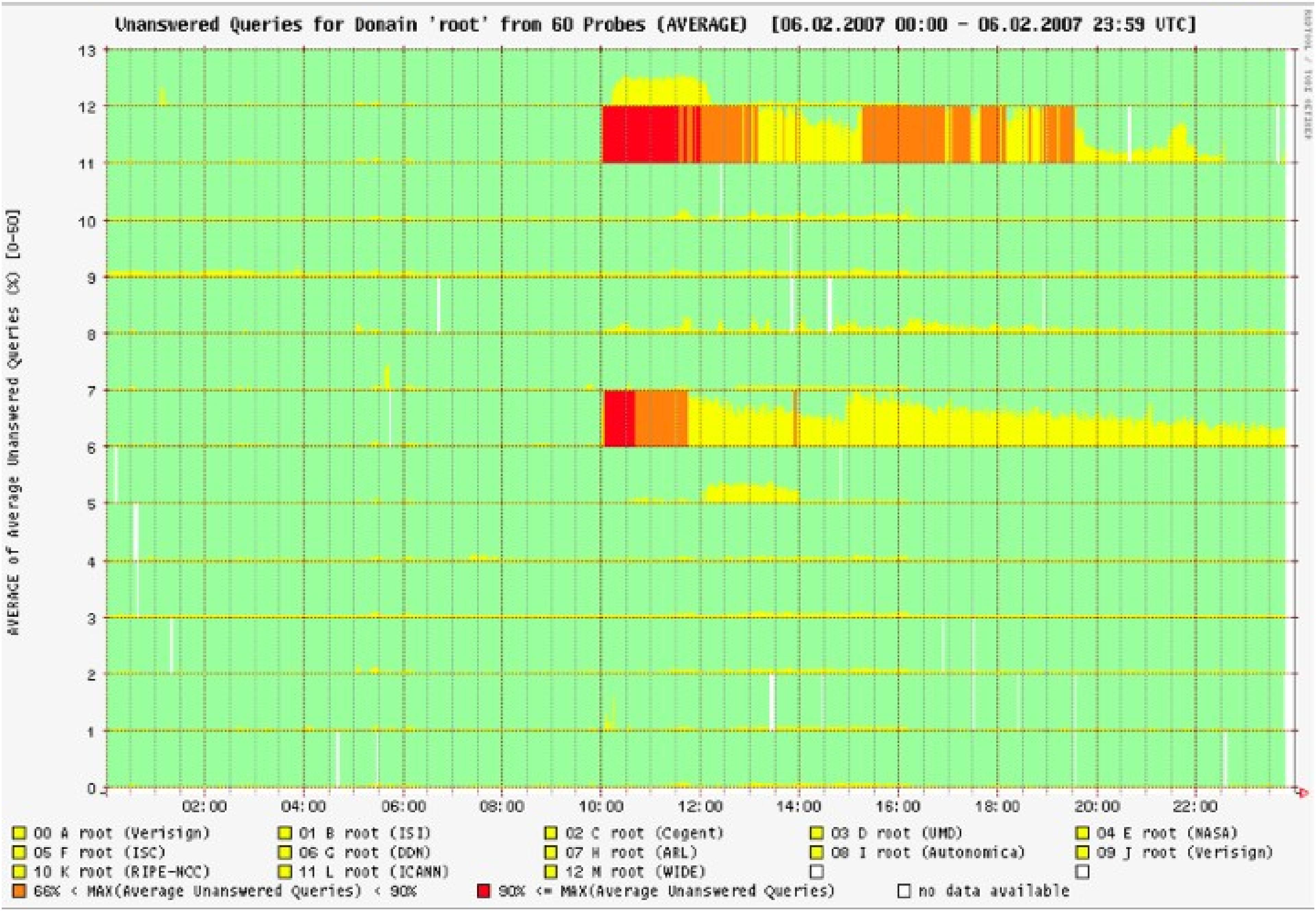
Attack overview

- 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. While this attack didn't have an impact on the service to end-users it was measured
- Here are some preliminary observations made at F-root including the type, quantity and distribution of attack traffic and how it coped
- See also ICANN report:
  - http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf

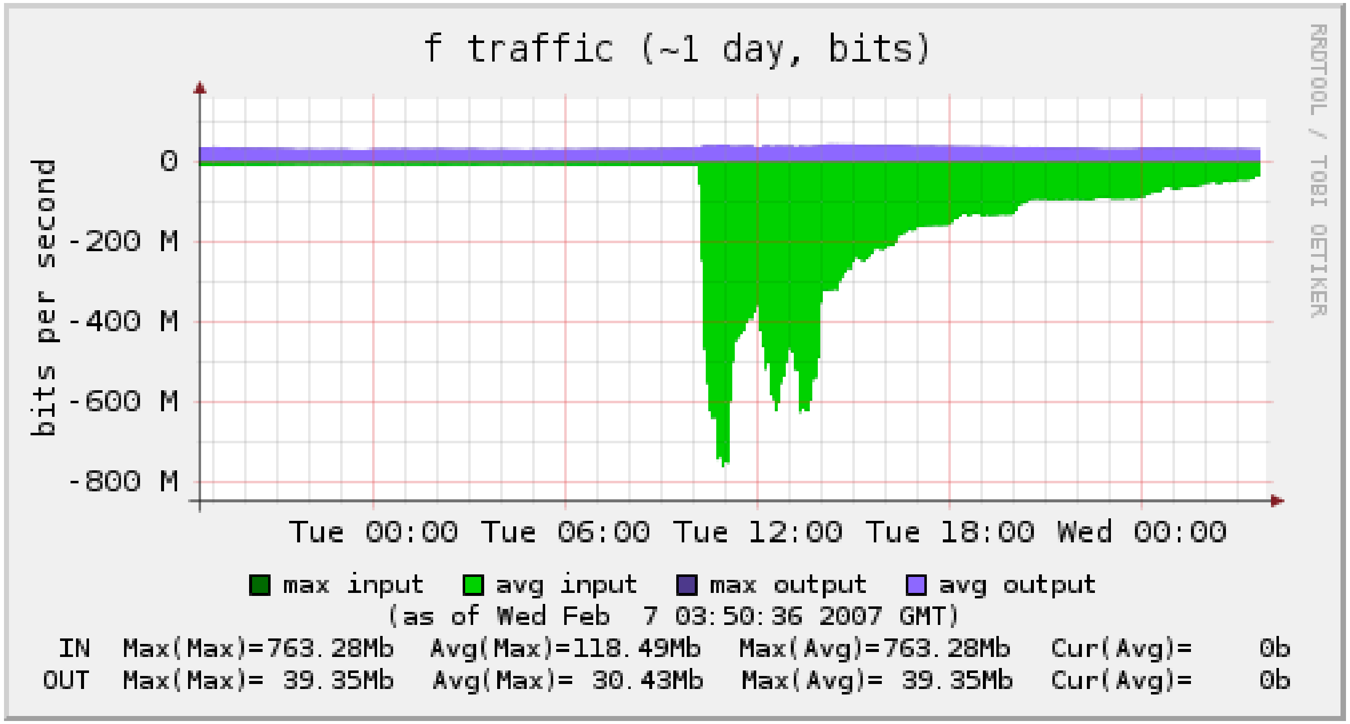
Attack points of interest

- 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

http://dnsmon.ripe.net

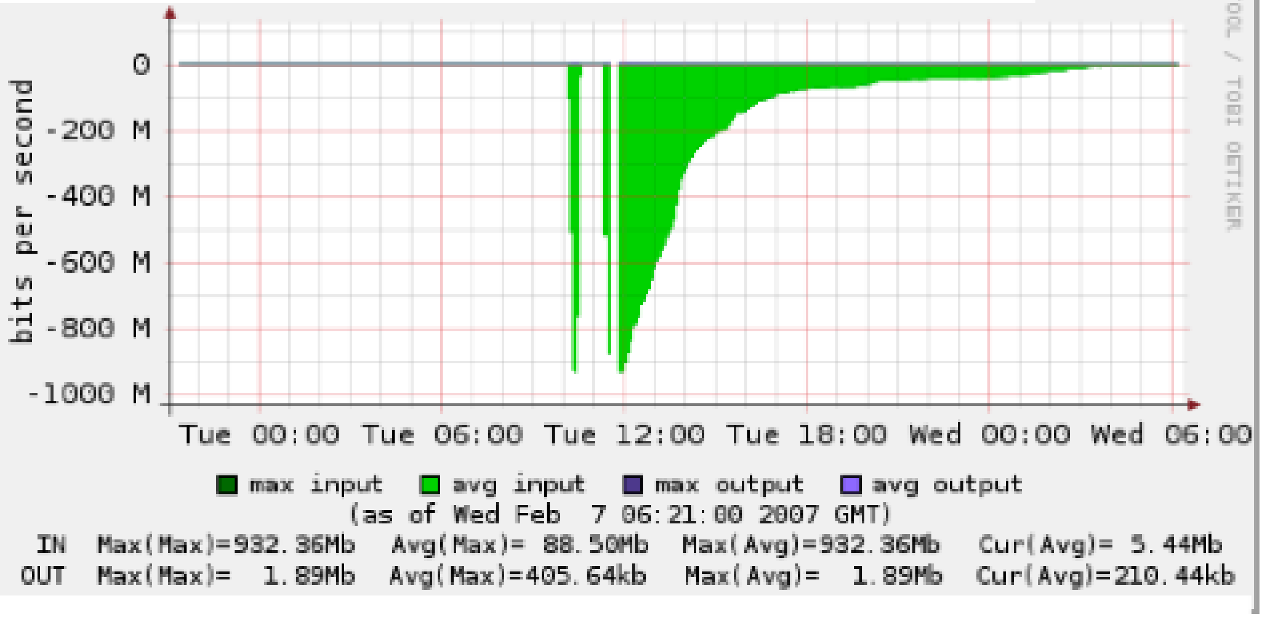


Aggregated traffic on F root



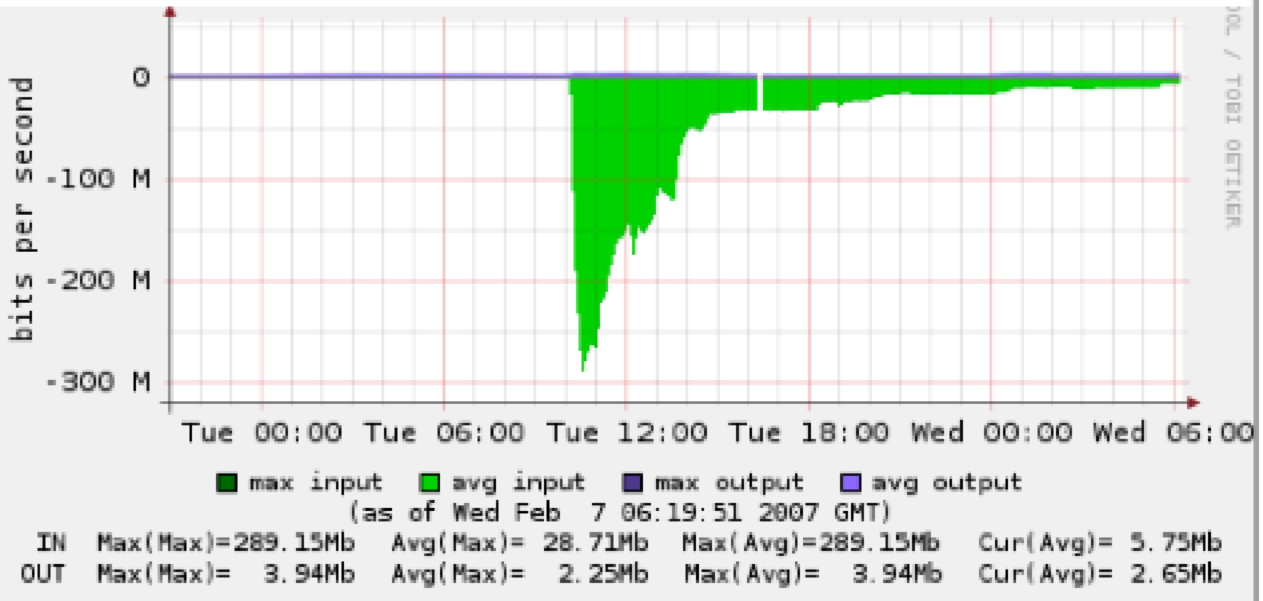
```
                    (as of Wed Feb  7 03:50:36 2007 GMT)
  IN   Max(Max)=763.28Mb   Avg(Max)=118.49Mb   Max(Avg)=763.28Mb   Cur(Avg)=     0b
 OUT   Max(Max)= 39.35Mb   Avg(Max)= 30.43Mb   Max(Avg)= 39.35Mb   Cur(Avg)=     0b
```

Seoul - capped at 1Gb/s



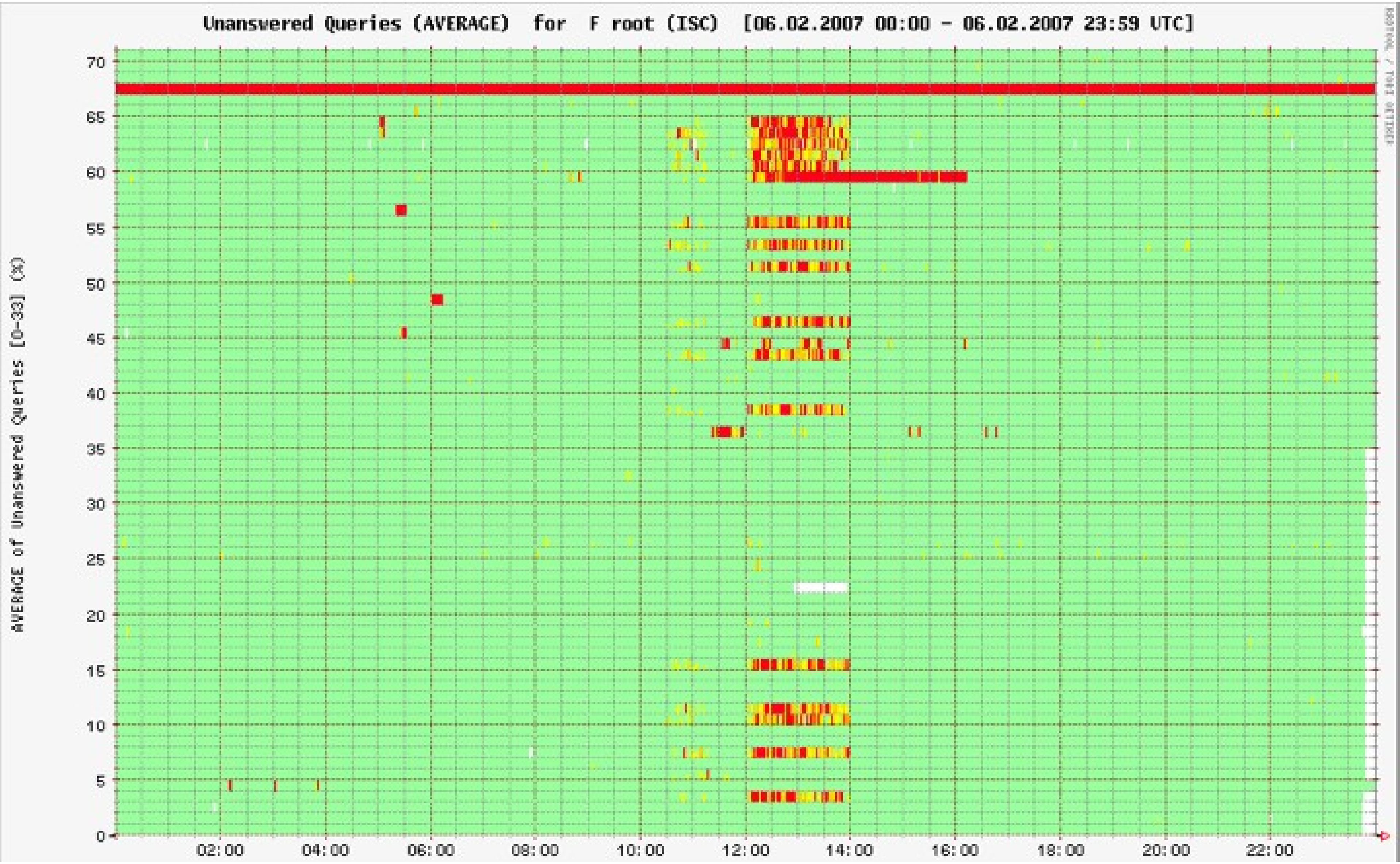
```
(as of Wed Feb  7 06:21:00 2007 GMT)
 IN  Max(Max)=932.36Mb  Avg(Max)= 88.50Mb  Max(Avg)=932.36Mb  Cur(Avg)= 5.44Mb
OUT  Max(Max)=  1.89Mb  Avg(Max)=405.64kb  Max(Avg)=  1.89Mb  Cur(Avg)=210.44kb
```

Beijing - peaked at 300Mb/s

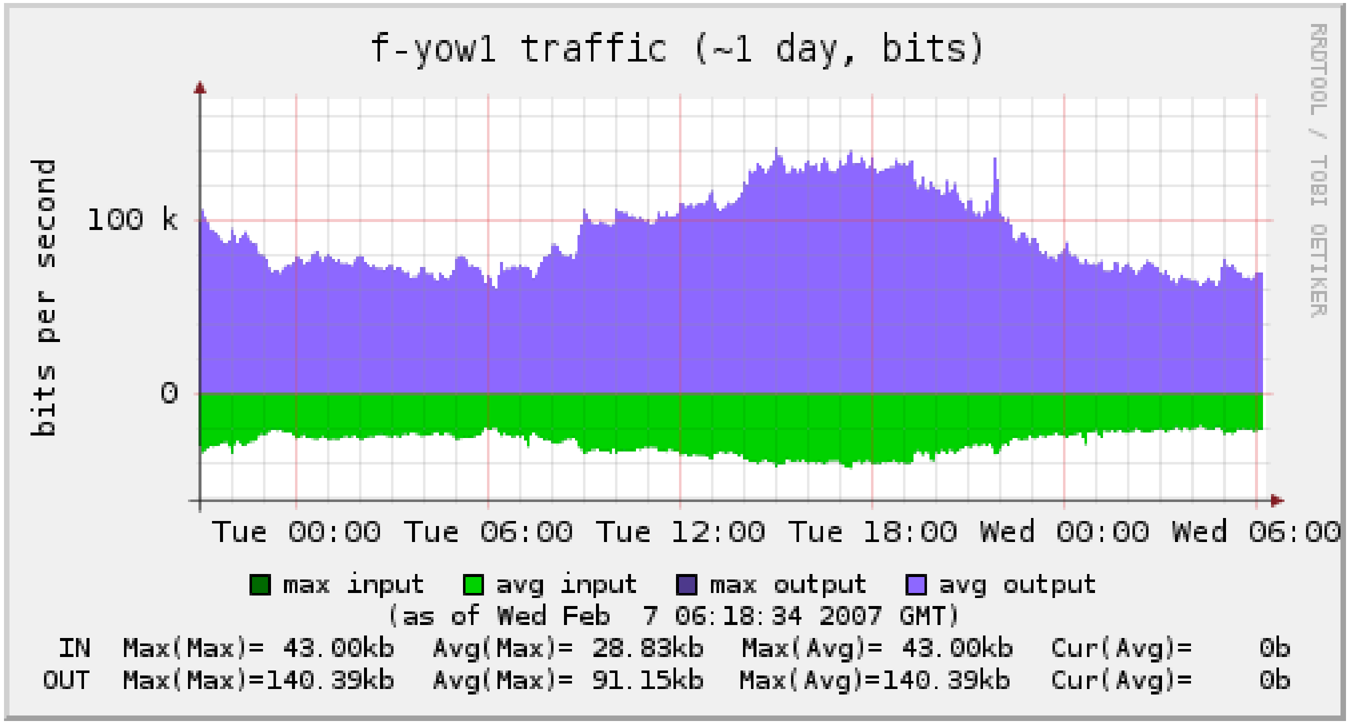


```
(as of Wed Feb  7 06:19:51 2007 GMT)
 IN  Max(Max)=289.15Mb  Avg(Max)= 28.71Mb  Max(Avg)=289.15Mb  Cur(Avg)= 5.75Mb
OUT  Max(Max)=  3.94Mb  Avg(Max)=  2.25Mb  Max(Avg)=  3.94Mb  Cur(Avg)= 2.65Mb
```

Service impact

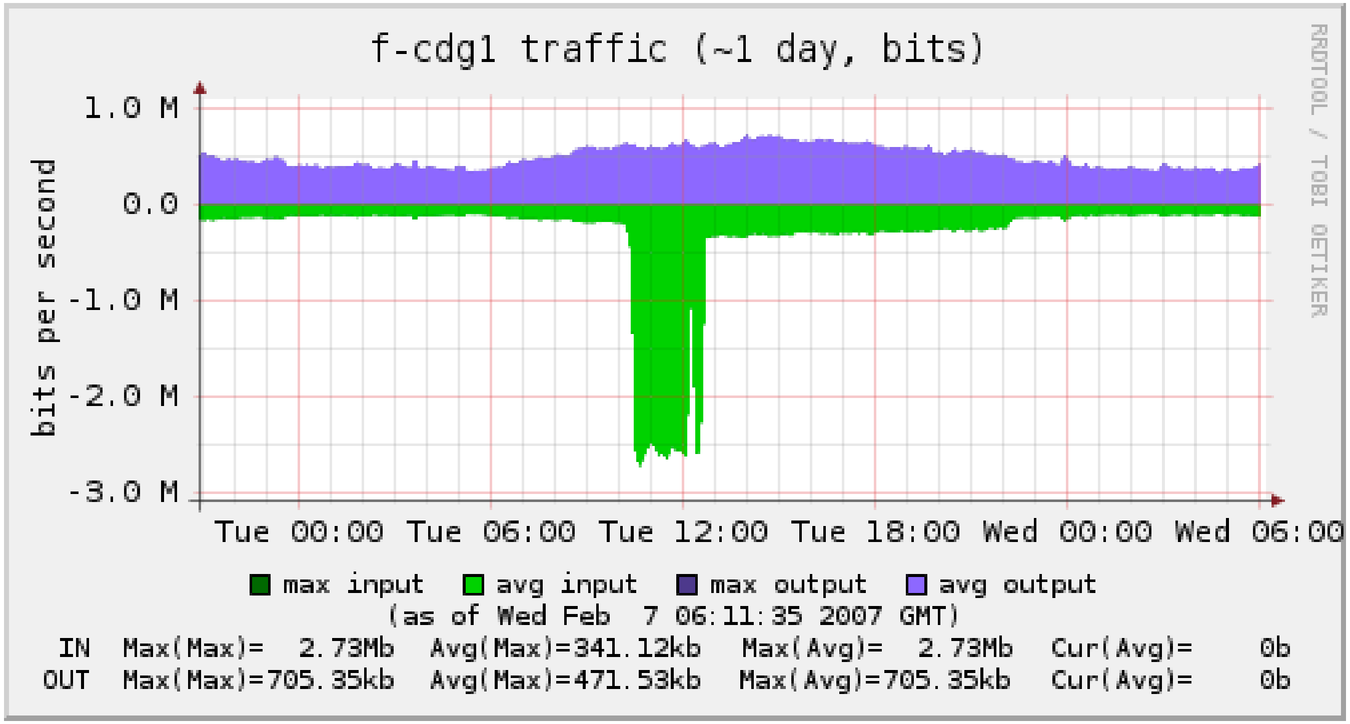


Some nodes got nothing



```
                   (as of Wed Feb  7 06:18:34 2007 GMT)
 IN  Max(Max)= 43.00kb  Avg(Max)= 28.83kb  Max(Avg)= 43.00kb  Cur(Avg)=    0b
OUT  Max(Max)=140.39kb  Avg(Max)= 91.15kb  Max(Avg)=140.39kb  Cur(Avg)=    0b
```

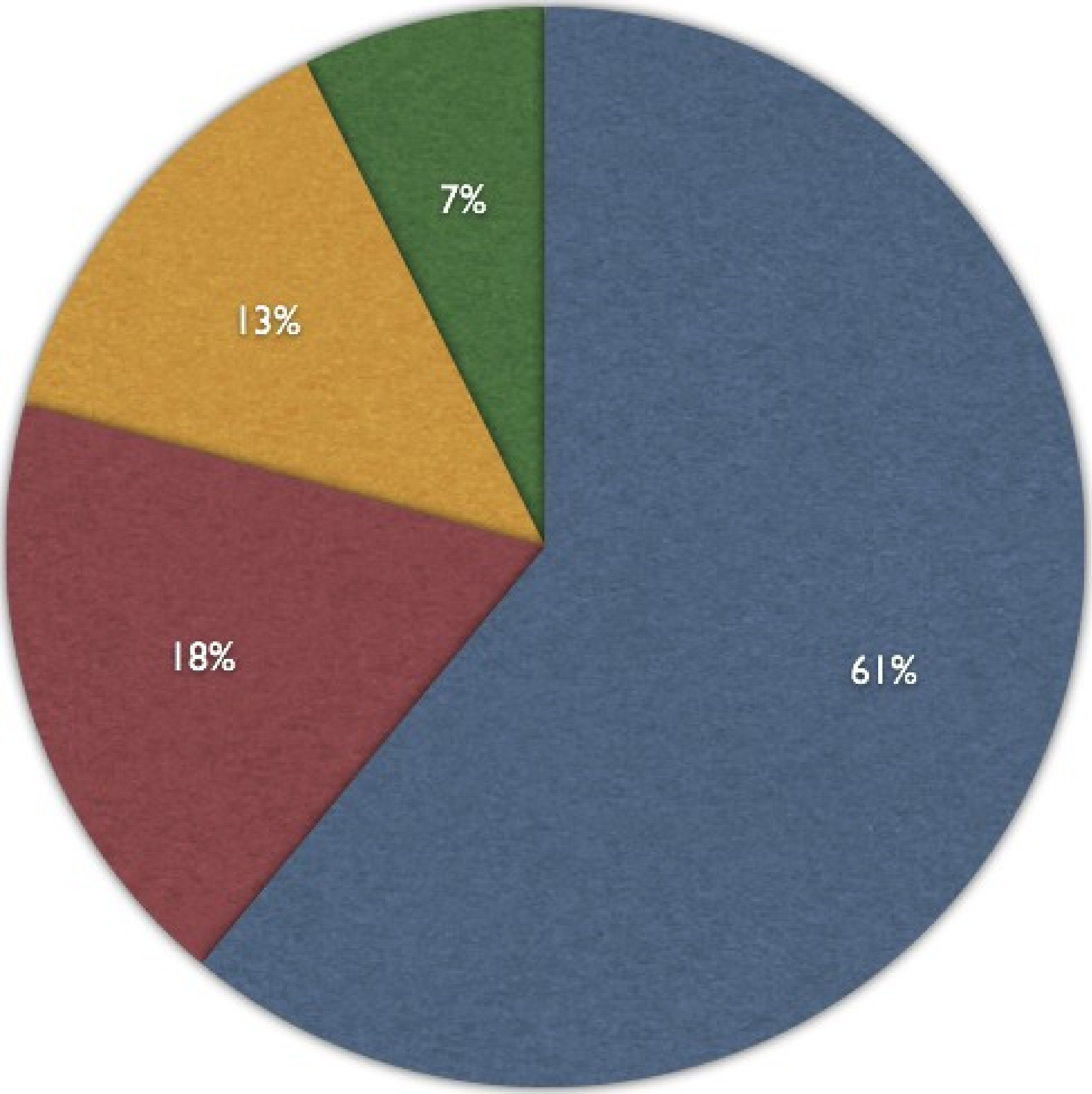
Others saw peculiar patterns



```
                    (as of Wed Feb  7 06:11:35 2007 GMT)
 IN  Max(Max)=   2.73Mb  Avg(Max)=341.12kb  Max(Avg)=   2.73Mb  Cur(Avg)=     0b
OUT  Max(Max)=705.35kb  Avg(Max)=471.53kb  Max(Avg)=705.35kb  Cur(Avg)=     0b
```

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



Other equates to 35 F-root anycast nodes

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

Acknowledgments

- Dave Knight, ISC
  - http://www.nanog.org/mtg-0702/real/ddos.ram
  - http://www.nanog.org/mtg-0702/presentations/knight.pdf
- Joao Damas, ISC
- John Kristoff, UltraDNS
- ICANN L-root team
- All DITL contributors

Supporting ISC

- Providing my time to do UKNOF is only one of ISC's many Internet public benefit activities
- Please consider supporting ISC where it contributes value to your business, e.g.
  - joining BIND, DHCP, OARC, NTP forums
  - training courses
  - hosting/peering for f-root instances (UK f-root instance is at LoNAP)

OARC Contact Info

- Web: https://oarc.isc.org
- Paper: http://public.oarci.net/files/oarc-briefing.pdf
- E-mail: keith_mitchell@isc.org
- Jabber: keith@jabber.oarc.isc.org
- Phone: +1 650 423 1348 (EST)
  +44 778 534 6152

Questions ?