Welcome

OARC Global DNS Risks
Technical Meeting

Georgia Tech

February 2, 2009

DNS-OARC

Thanks

- To Georgia Tech for the meeting facilities
- To ICANN for inviting us to organize this meeting
- To our presenters and attendees for coming here on short notice

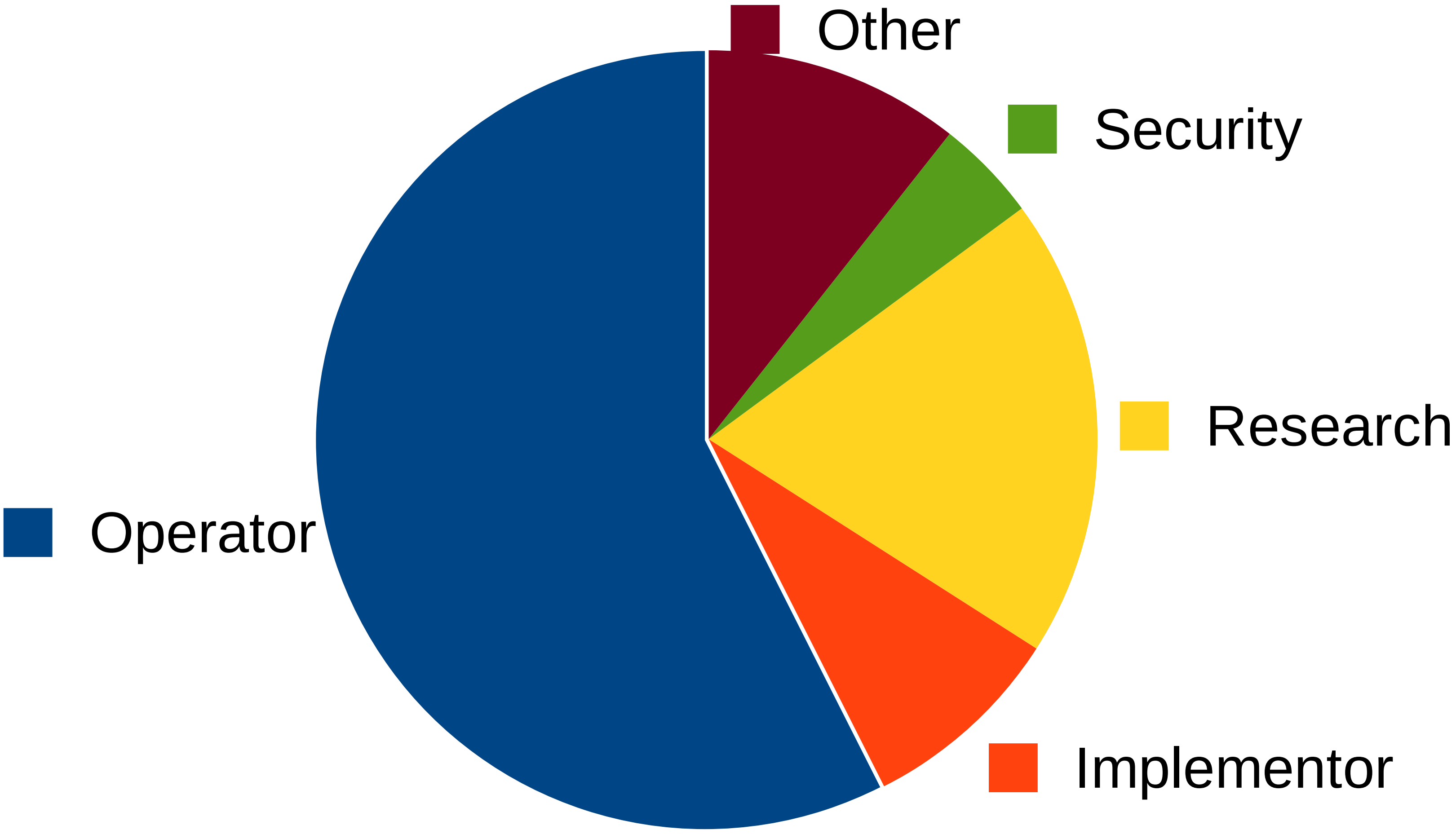
Schedule

- 0900 first session
- 1030 break
- 1100 second session
- 1230 lunch (provided)
- 1400 thrid session
- 1600 wrapup
- 1700 PGP key signing

DNS-OARC

- Created about 5 years ago by Paul Vixie at ISC
- Modelled after “OARCs” in other disciplines
- Seeded with NSF grant money in collaboration with CAIDA
- Spun-off from ISC last year as a stand-alone corporation.

Membership



DNS-OARC

OARC Functions

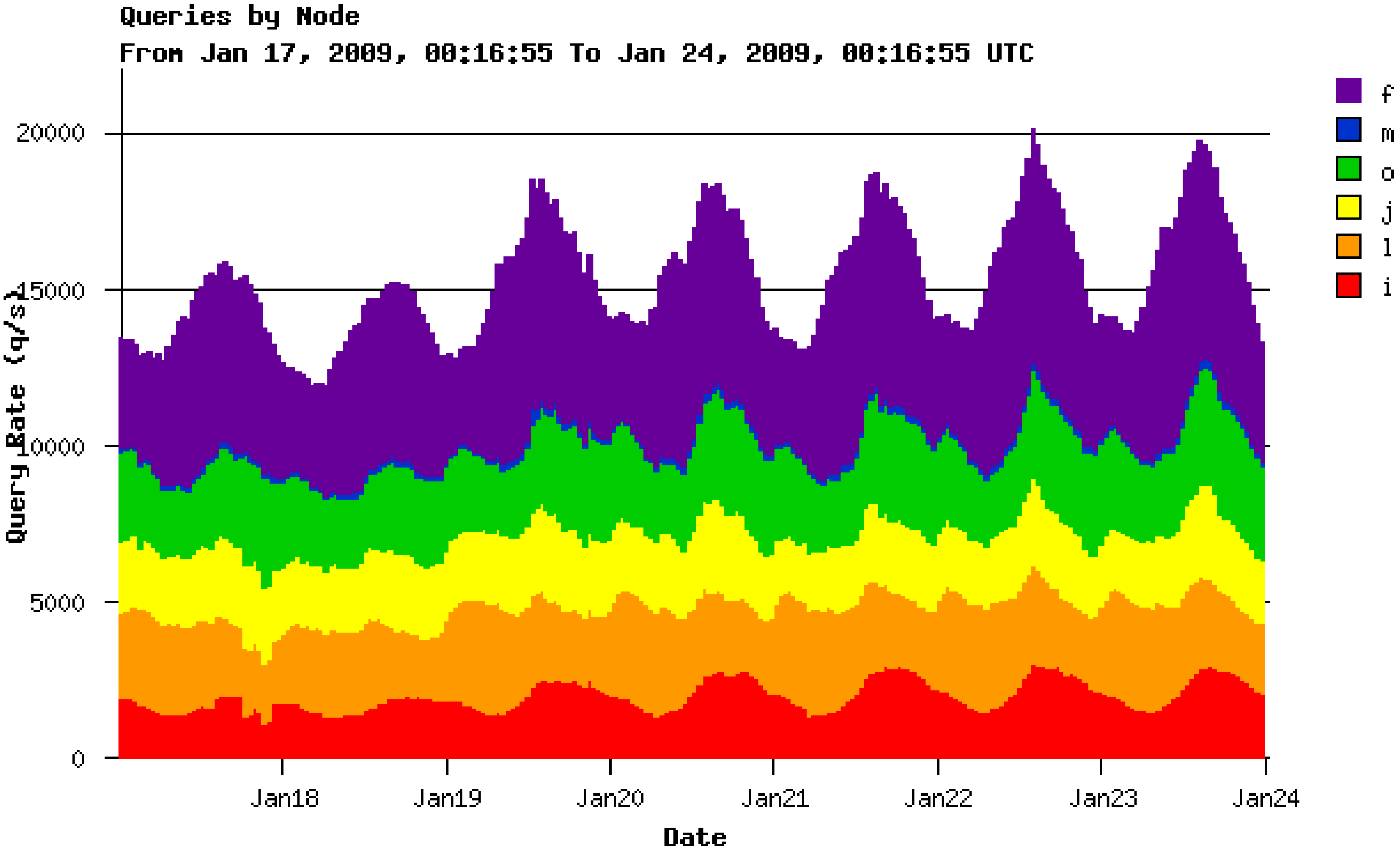
- Incident and outage tracking
  - Attacks, maintenance
- Networking and collaboration
  - Meetings, chat rooms, mailing lists
- Data collection and analysis
  - DITL, attack events
- Education and outreach
  - Tools, workshops, notifications, assistance

OARC Projects

DSC: DNS Statistics Collector

- Collector/presenter architecture
- Transmits summary “datasets” rather than raw packets
- Many members publish their data to OARC
- OARC also makes some DSC data publicly available with a 1-week delay.

DSC: Sample Data



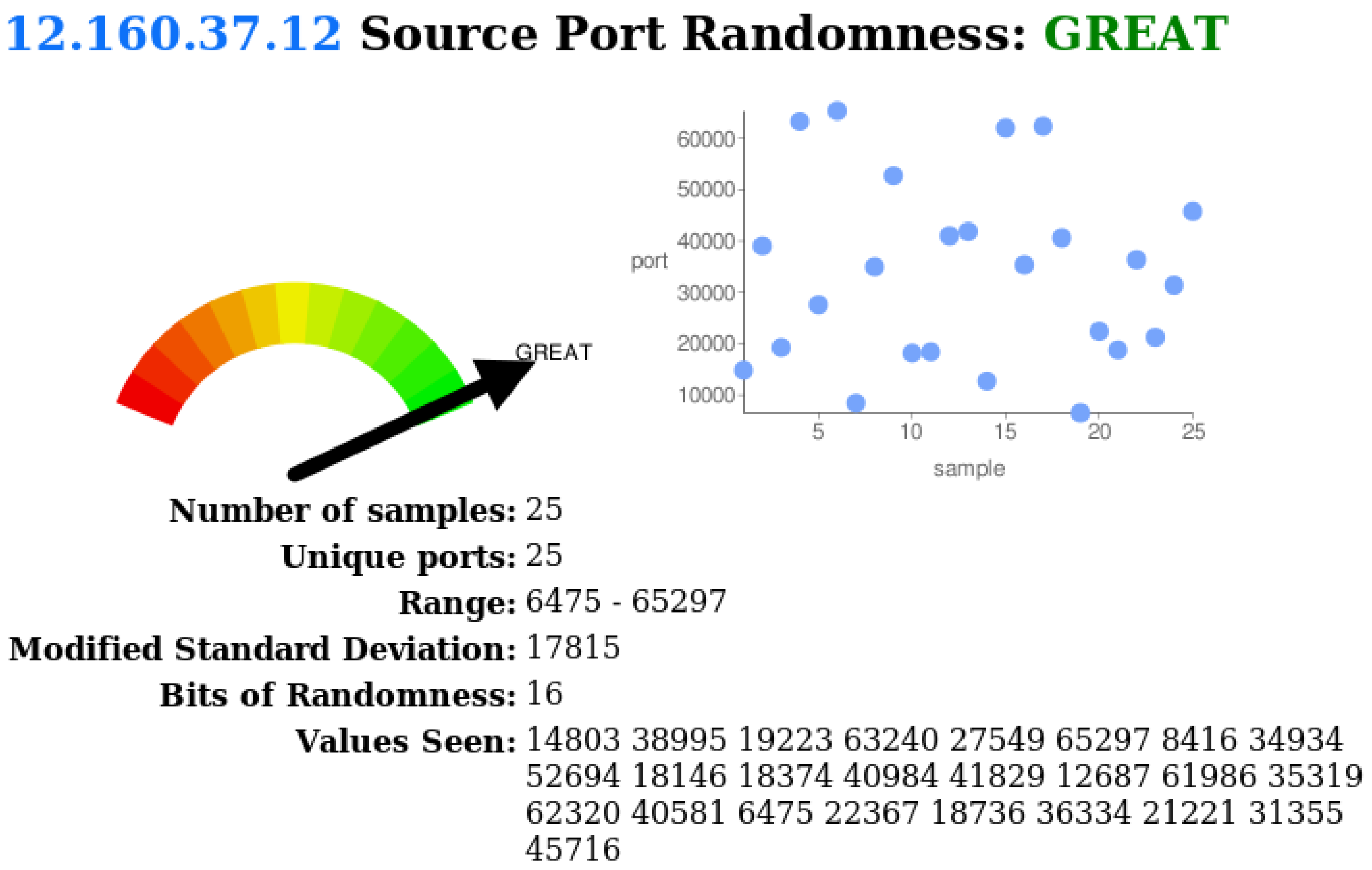
ODVR: Open DNSSEC Validating Resolver

- Currently three DNS resolver processes
  - BIND, Unbound, IANA-testbed
- Allows anyone to experiment with DNSSEC without setting up their own resolver
- Rate-limited and fully logged
- Config files provided
- Data available to OARC members

Porttest: Source Port Measurements

- A tool to help users find out if their resolvers may be vulnerable to Kaminsky attacks
- Both web-based and DNS-based tools
- Attempts to measure entropy, but like Barbie says, “math is hard.”

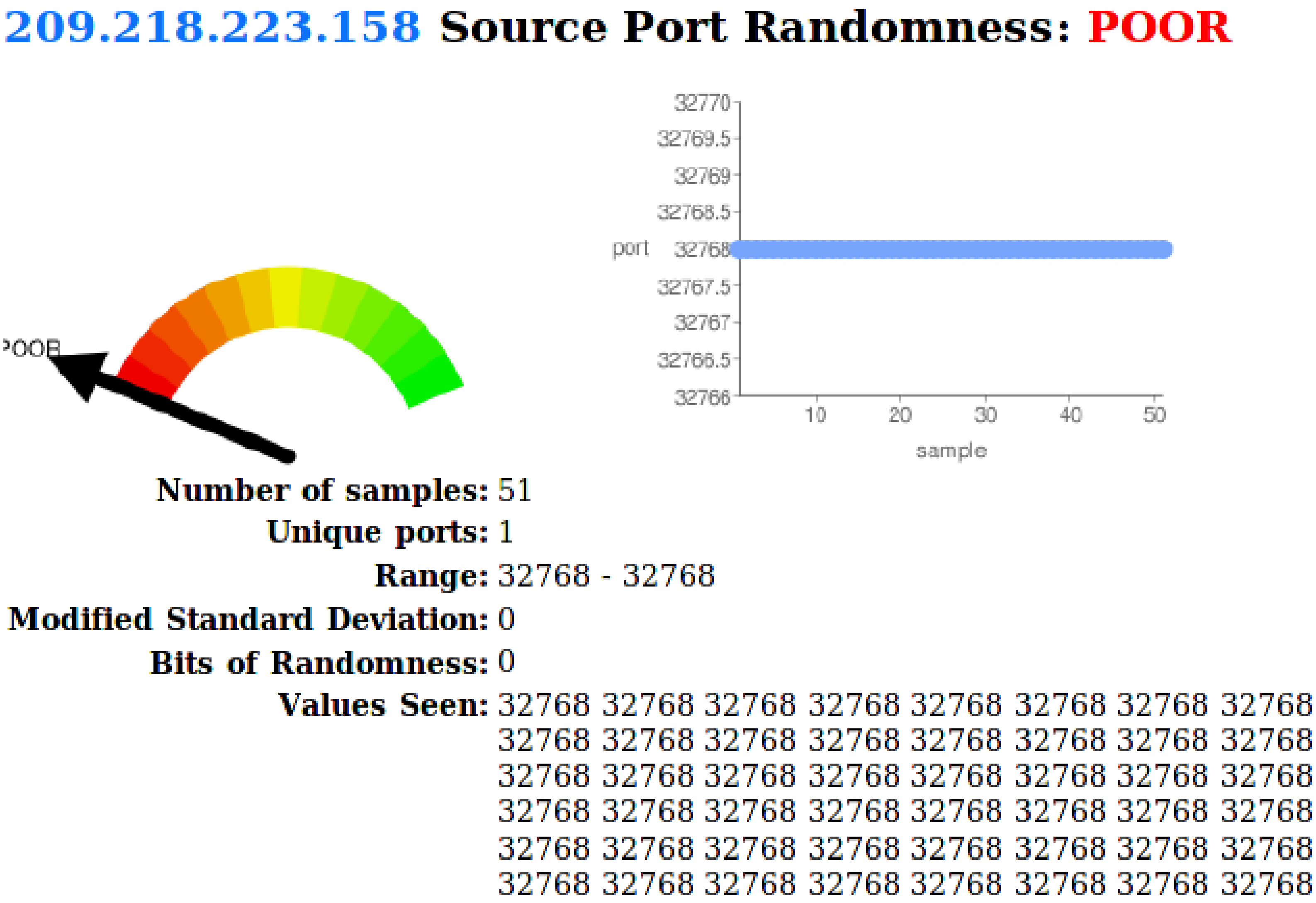
Porttest: Web version



12.160.37.12 Source Port Randomness: GREAT

Number of samples:	25
Unique ports:	25
Range:	6475 - 65297
Modified Standard Deviation:	17815
Bits of Randomness:	16
Values Seen:	14803 38995 19223 63240 27549 65297 8416 34934 52694 18146 18374 40984 41829 12687 61986 35319 62320 40581 6475 22367 18736 36334 21221 31355 45716

Last Night from the Hotel



209.218.223.158 Source Port Randomness: POOR

Number of samples: 51

Unique ports: 1

Range: 32768 - 32768

Modified Standard Deviation: 0

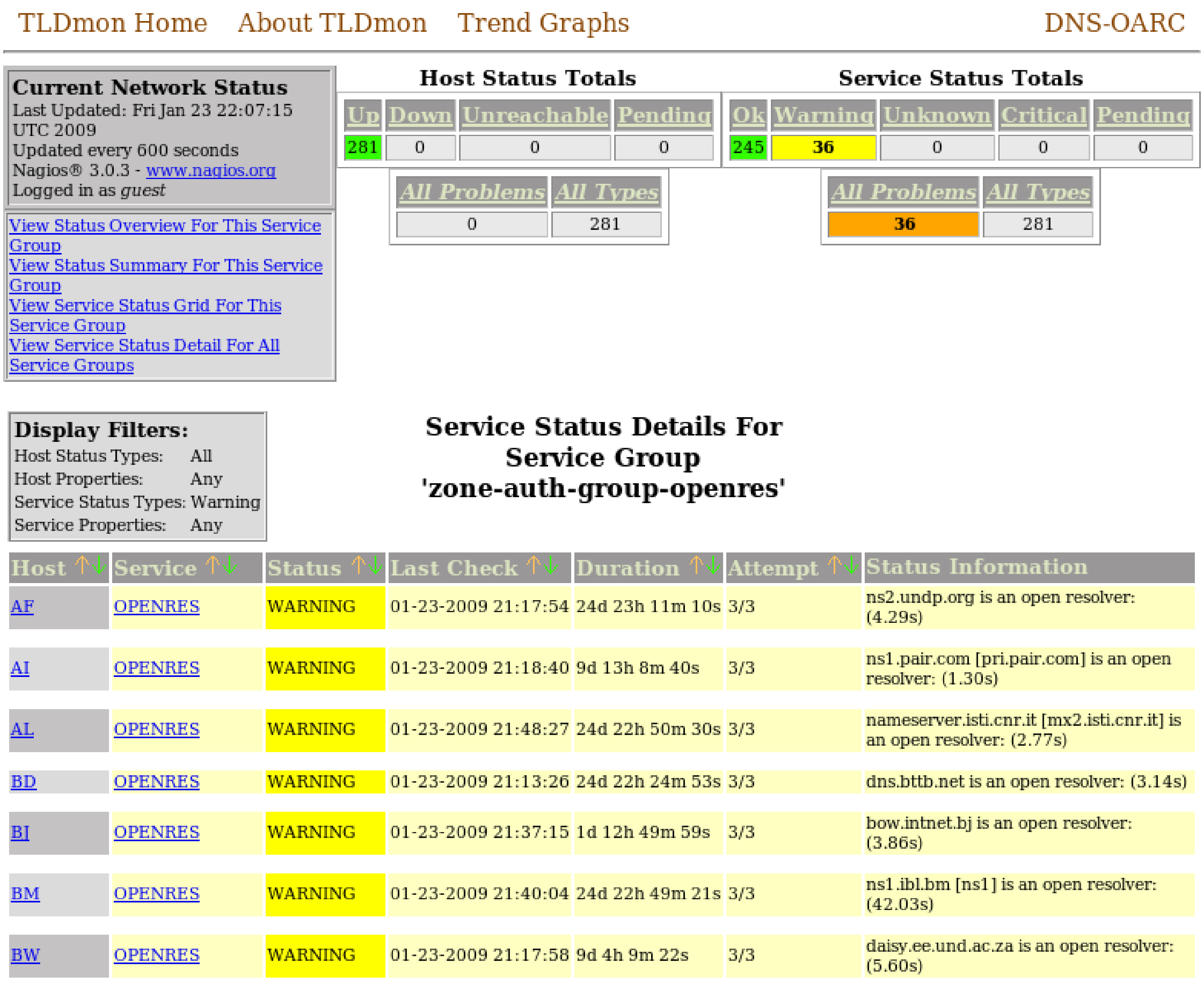
Bits of Randomness: 0

Values Seen: 32768 32768 32768 32768 32768 32768 32768 32768
32768 32768 32768 32768 32768 32768 32768 32768
32768 32768 32768 32768 32768 32768 32768 32768
32768 32768 32768 32768 32768 32768 32768 32768
32768 32768 32768 32768 32768 32768 32768 32768
32768 32768 32768 32768 32768 32768 32768 32768

TLDmon

- Using open-source Nagios tool with custom plugins to monitor TLD zones
- Checks for: authoritative answers, EDNS, IPv6, lameness, NS consistency, open resolvers, matching serial numbers, TCP support, RRSIG expiration
- OARC members may receive problem notifications and request monitoring of additional zones.

TLDmon



TLDmon Home   About TLDmon   Trend Graphs   DNS-OARC

Current Network Status
Last Updated: Fri Jan 23 22:07:15 UTC 2009
Updated every 600 seconds
Nagios® 3.0.3 - www.nagios.org
Logged in as *guest*

View Status Overview For This Service Group
View Status Summary For This Service Group
View Service Status Grid For This Service Group
View Service Status Detail For All Service 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
245	36	0	0	0

All Problems	*All Types*
36	281

Display Filters:

Host Status Types:	All
Host Properties:	Any
Service Status Types:	Warning
Service Properties:	Any

Service Status Details For Service Group 'zone-auth-group-openres'

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
AF	OPENRES	WARNING	01-23-2009 21:17:54	24d 23h 11m 10s	3/3	ns2.undp.org is an open resolver: (4.29s)
AI	OPENRES	WARNING	01-23-2009 21:18:40	9d 13h 8m 40s	3/3	ns1.pair.com [pri.pair.com] is an open resolver: (1.30s)
AL	OPENRES	WARNING	01-23-2009 21:48:27	24d 22h 50m 30s	3/3	nameserver.isti.cnr.it [mx2.isti.cnr.it] is an open resolver: (2.77s)
BD	OPENRES	WARNING	01-23-2009 21:13:26	24d 22h 24m 53s	3/3	dns.bttb.net is an open resolver: (3.14s)
BJ	OPENRES	WARNING	01-23-2009 21:37:15	1d 12h 49m 59s	3/3	bow.intnet.bj is an open resolver: (3.86s)
BM	OPENRES	WARNING	01-23-2009 21:40:04	24d 22h 49m 21s	3/3	ns1.ibl.bm [ns1] is an open resolver: (42.03s)
BW	OPENRES	WARNING	01-23-2009 21:17:58	9d 4h 9m 22s	3/3	daisy.ee.und.ac.za is an open resolver: (5.60s)

DNS-OARC

DITL: Day in the Life of the Internet

- This large-scale data collection effort started in 2006.
- 48-hours full packet capture from DNS roots, TLDs, RIRs, AS112, and more
- Strong focus on DNS, but also includes other types of data
- Tentatively planning for DITL 2009 in April

Simulation Testbed

- A rack of 16 still-somewhat-beefy servers and Ethernet switches
- Can be used to simulate traffic flows seen at busy DNS servers
- Open to all legitimate researchers, with priority given to OARC members

Next Workshop

- May 8-9, 2009
- Amsterdam
- Following RIPE meeting
- Hosted by SIDN (the .nl folks)

Thanks For Listening

Now, on with the show....

DNS-OARC