DNS-OARC and Name Collisions: an Introduction

Keith Mitchell
OARC President

WPNC, London
March 2014

DNS-OARC
Domain Name System Operations Analysis and Research Center

DNS-OARC Introduction

DNS-OARC

Domain Name System Operations Analysis and Research Center

What is DNS-OARC ?

The Domain Name System Operations Analysis and Research Center (DNS-OARC) is a non-profit, membership organization that seeks to improve the security, stability, and understanding of the Internet's DNS infrastructure.

DNS-OARC's mission is:

- *to build relationships among its community of members and facilitate an environment where information can be shared confidentially*
- *to enable knowledge transfer by organizing workshops*
- *to promote research with operational relevance through data collection and analysis*
- *to increase awareness of the DNS's significance*
- *to offer useful, publicly available tools and services*

DNS-OARC

Domain Name System Operations Analysis and Research Center

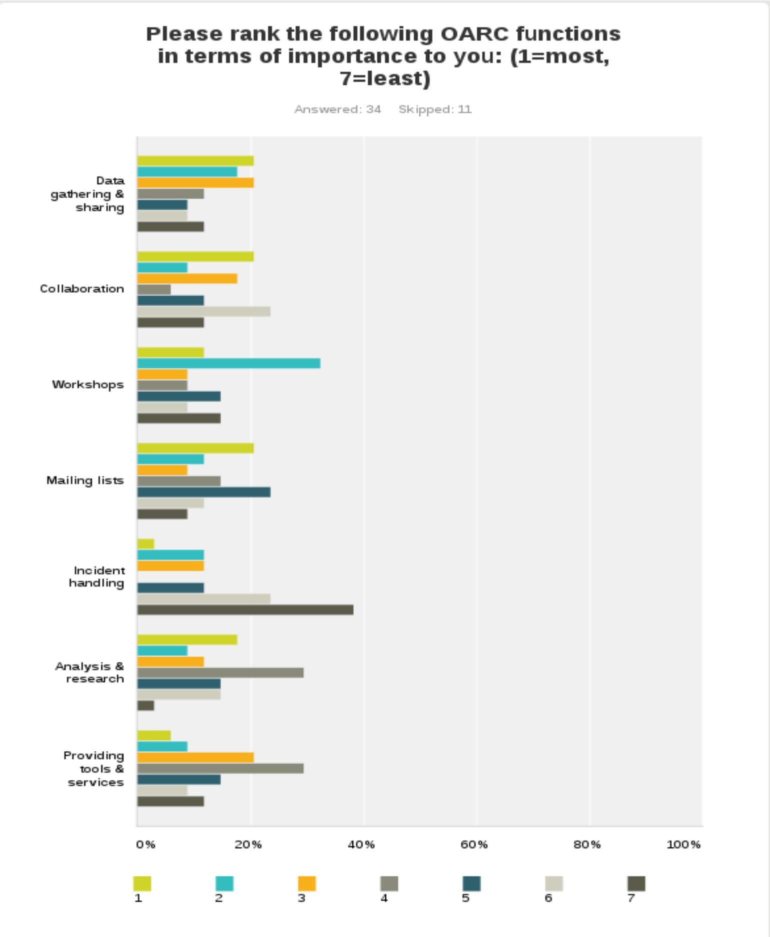
OARC's Functions

- Facilitate co-ordination of DNS operations community
- Ongoing data gathering
- Operate community info-sharing resources
  - Mailing lists, jabber, website, trust vetting
- Maintain/host DNS software tools
- Outreach via external and shared meetings

DNS-OARC

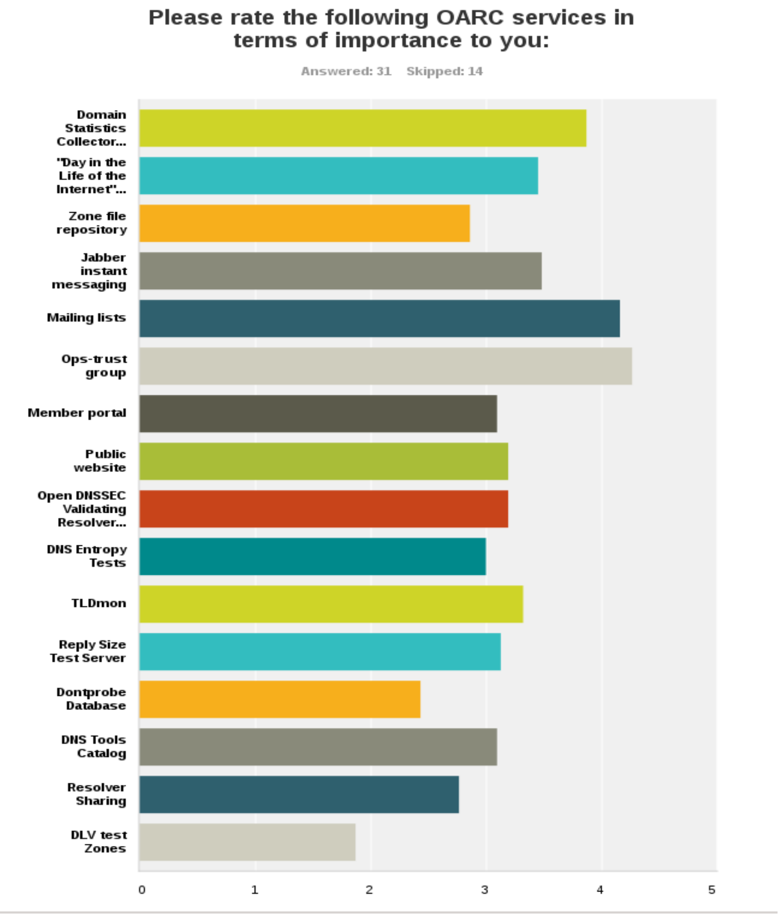
Domain Name System Operations Analysis and Research Center

OARC Functions & Services



Please rank the following OARC functions in terms of importance to you: (1=most, 7=least)

Answered: 34 Skipped: 11



Please rate the following OARC services in terms of importance to you:

Answered: 31 Skipped: 14

DNS-OARC

Domain Name System Operations Analysis and Research Center

OARC Members

Afilias *(.org, .info)*
Dyn
Google
ICANN
Nominet *(.uk)*
RIPE NCC

AFNIC *(.fr)*
APNIC
Akamai
ARIN
Cisco
DENIC *(.de)*
EurID *(.eu)*
Neustar *(.biz)*
SIDN *(.nl)*

.CLUB
.SE
ARI Registry Services
Artemis *(.secure)*
CentralNic
CIRA *(.ca)*
CloudShield
CNNIC *(.cn)*
CORE
CZ.NIC
Demand Media
DK Hostmaster
DNSpod
Donuts
dotBERLIN
IEDR *(.ie)*
Internet Identity

JAS Advisors
JPRS *(.jp)*
KISA/KRNIC
Mark Monitor
Minds+Machines
NIC Chile *(.cl)*
NIC-Mexico *(.mx)*
Nominum
Norid *(.no)*
NZRS
Registro.BR
RTFM
SWITCH *(.ch)*
tcinet.ru
XYZ

Comcast
ISC
Microsoft
Verisign *(.com)*

AFRINIC
CAIDA
Cogent
Dotua
Eesti Internet
LACNIC
Measurement Factory
NASA Ames
Netnod *(.se)*
NLnet Labs
NTT
OTTIX
PowerDNS
Public Interest Registry *(.org)*
Secure64
Team Cymru
University of Maryland
USC/ISI
WIDE

DNS-OARC
Domain Name System Operations Analysis and Research Center

OARC Governance

- Independent legal entity
- Diverse member base
  - direct participation agreements
- Financially self-supporting
- Self-governing, neutral
- Board reflecting member interests
- *501(c)3* non-profit public benefit corporation

DNS-OARC

Domain Name System Operations Analysis and Research Center

OARC Board

- John Crain, ICANN, RSAC Director
- Ondrej Filip, CZ.NIC, Chairman
- Chris Griffiths, Dyn, Director
- Matt Pounsett, Afilias, Treasurer
- Antoin Verschuren, SIDN, Director
- Duane Wessels, Verisign, Director

DNS-OARC Staff Resources

- President, Secretary (Keith Mitchell)
- Systems Engineer (William Sotomayor)
- Events contractor (Denesh Bhabuta)
- Under contract from ISC:
  - Finance/Admin functions
  - Infrastructure services

(not all roles are full-time)

- Hiring 2014:
  - Program Development
  - Administration
  - Website re-Design
  - Software Engineer

DNS-OARC
Domain Name System Operations Analysis and Research Center

2013 Donors – Thank You !

- Verisign
  - $50k one-off donation
  - Keith/William time, Root-Ops jabber servers
- ICANN
  - 1 x Dell r815, 3 x Dell r820 analysis servers
  - Workshop underwriting
- Donuts, Demand Media
  - 2 x Dell r810 analysis servers
- Farsight
  - 4 x Sun X4500 storage servers
- 2014
  - We have a number of offers of other-site hosted server clouds, under discussion..

2013 Achievements

- Created Strategic Development Plan
- Increased staff from 0.6 to ~2FTE
- Governance Rationalization
- Revenue growth from $270k to $470k
- Major infrastructure overhaul
- Significant cash and hardware donations
- Workshop improvements, sponsor program

OARC Development Plan

- Output from Member Survey, Board Retreat, to re-boot DNS-OARC:
  - https://www.dns-oarc.net/files/workshop-201305/Strategy-2013_report.pdf
- Objectives on 3+ year timescale:
  - Governance reforms for more focused operations
  - Grow OARC to a more sustainable and stable “Ideal OARC” level of ~5FTE, $1M revenue
  - Workshop improvements, sponsorship
  - Re-develop systems, infrastructure, processes, websites
  - Solicit funding for new projects and services of value to members

DNS-OARC

Domain Name System Operations Analysis and Research Center

DNS-OARC
Data Sharing

DNS-OARC

Domain Name System Operations Analysis and Research Center

DNS Data Gathering

- Generally involves sensors running on, or adjacent to servers, e.g.
  - Domain Statistics Collector (DSC) - continuous traffic analysis and summary, no payload
  - “Day in the Life of the Internet” (DITL) - full query payload via *dnscap* for 48 hours at least once a year
- Also:
  - Zone File Repository (ZFR) – aggregate archive of TLD zone file contents
  - Capturing data from various user-driven test tools

OARC's Data Sharing Policy

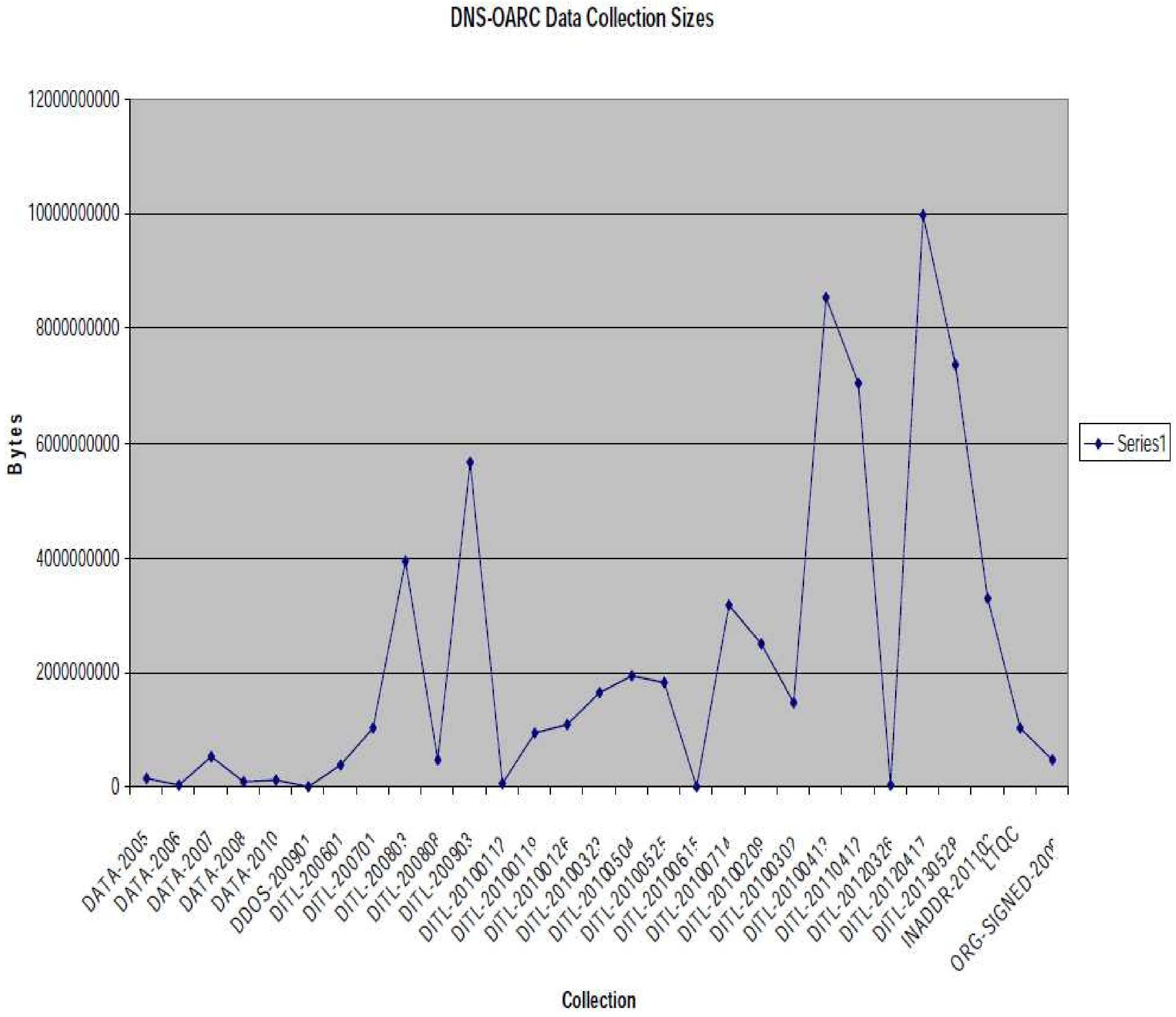
- Governed by Participation Agreement, which applies to all paying Members and non-paying Participants
- Obligations on OARC and participants to preserve privacy of shared data
- OARC-held raw data may not be copied off of OARC's servers
  - Yes, we know this is very “pre-cloud retro” but we are stuck with it
- OARC provides significant storage and compute resources to allow members to analyze data in-situ
- Analysis **results** may be copied off of OARC servers for internal use and/or publication, subject to approval
- Members and researchers encouraged to share and publish their findings

OARC's DITL Dataset

- Since 2006, at least once per year to provide “Internet Science” baseline
- Also during key DNS events such as DNSSEC signing of root, IPv6 enabling, potentially during incidents
- Gathered from most Root, many TLD, and some resolver operators
- Full query traffic to authoritative servers
- ~80Tb Dataset
  - OARC has been doing “big data” for nearly a decade..
  - less challenging with modern hardware than when we first did this !
  - https://www.dns-oarc.net/oarc/data/ditl

DNS-OARC

Domain Name System Operations Analysis and Research Center


DNS-OARC Data Collection Sizes

DNS-OARC

Domain Name System Operations Analysis and Research Center

Dataset Summary

- 76TB used out of 84TB capacity
- Additional interim capacity being brought on-line for DITL 2014 from donated X4500 hardware
- Procuring 80TB *StoragePod* for future requirements

Year	Gb
DITL-200601	372
DITL-200701	989
DITL-200808	452
DITL-20100112	46
DITL-20100119	898
DITL-20100126	1031
DITL-	1562

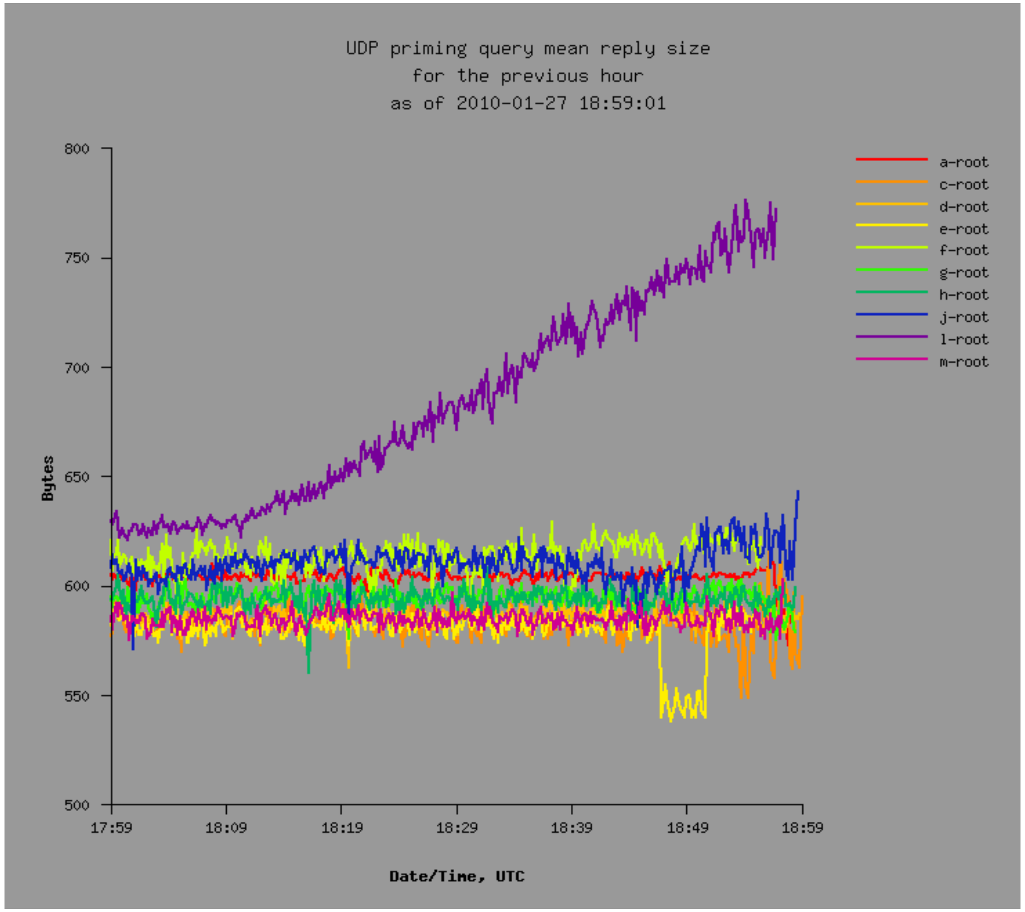
DNS-OARC

Domain Name System Operations Analy

OARC Compute Resources

- Storage:
  - *fs2, fs3, fs4:* IXsystems SATA-based FreeBSD 9.2
- Analysis:
  - *an1, an3*: 64-bit FreeBSD 9.2, using Dell R810 with 144GB of RAM, with 4 X7560 @ 2.27GHz CPUs
  - *an2, an4*: 64-bit Debian Linux 7.1, using Dell R820 with 64GB of RAM, with 2 E5-4603 0 @ 2.00GHz CPUs
- Storage servers export data to analysis servers via NFS
- Member access to analysis servers via ssh

DITL in Action



DNS-OARC

Domain Name System Operations Analysis and Research Center

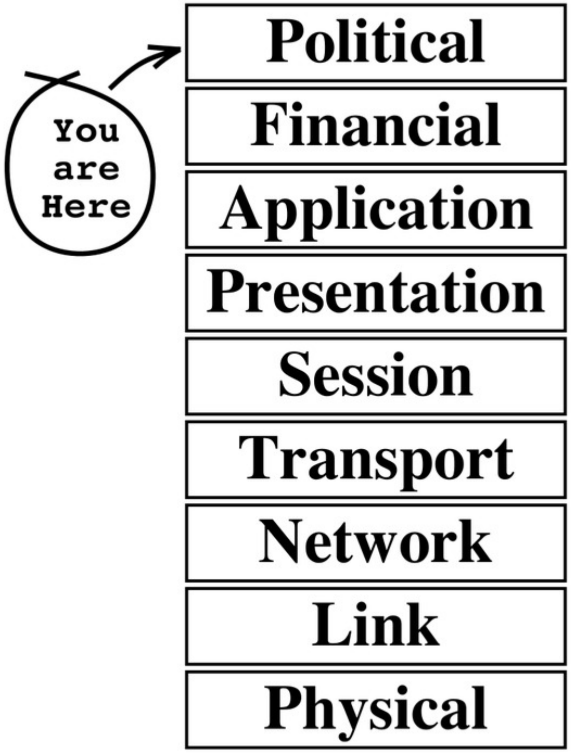
OARC and Name Collisions

DNS-OARC

Domain Name System Operations Analysis and Research Center

Evidence-Informed Policy

- Decisions to make changes at the top level of the DNS are ultimately commercial/political ones
- Many vested high-stakes commercial interests involved..
- ..but cannot be made in an operational vacuum
- Could there be adverse security/stability impacts ?
- How best to inform policy makers with hard evidence ?


You are Here

Political

Financial

Application

Presentation

Session

Transport

Network

Link

Physical

DNS Security *Collides* with Policy

- ICANN approving new TLDs on a competitive bidding process
- Various domains such as “.corp”, “.home” applied for in process
- Unfortunately various entities already make non-standard use of “pseudo TLDs” in their **internal** networks
  - some of these are same as new TLDs being applied for
  - worse, some of these have “internal-use-only” SSL website-security certificates already issued for them !
- Could creating these domains on the wider Internet “collide” with their internal usage ?
- Worse, could it lead to website impersonation and hi-jacking ??

DNS-OARC

Domain Name System Operations Analysis and Research Center

OARC's Data-set to the Rescue

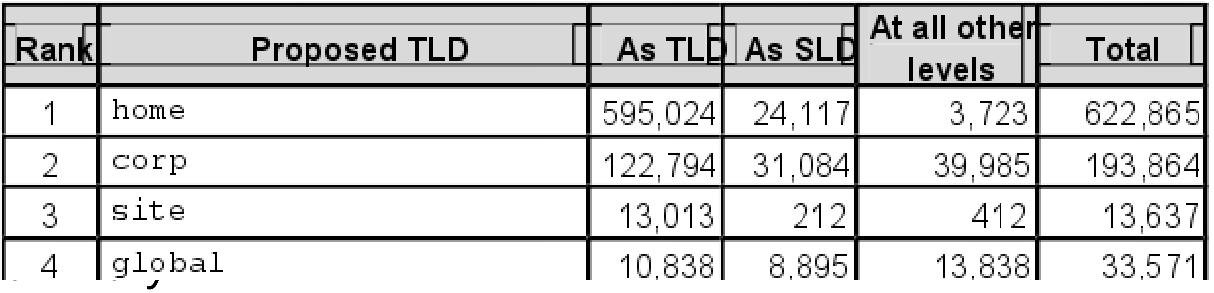
- Rather than debate endlessly, it's been possible to analyze data already gathered to decide the extent of queries for potential new TLDs on the live Internet
- OARC's DITL dataset from 2006-2013 available for this:
  - not the perfect resource for such research,
    but much better than nothing at all
  - triggered donations of some extra CPU-power ☺
- https://www.dns-oarc.net/node/332

DNS-OARC

Domain Name System Operations Analysis and Research Center

ICANN Collisions DITL Query Analysis

- https://www.icann.org/en/about/staff/security/ssr/name-collision-02aug13-en.pdf



Rank	Proposed TLD	As TLD	As SLD	At all other levels	Total
1	home	595,024	24,117	3,723	622,865
2	corp	122,794	31,084	39,985	193,864
3	site	13,013	212	412	13,637
4	global	10,838	8,895	13,838	33,571

- S
  - **Not safe** to delegate “*.corp*” or “*.home*” new TLDs
  - Mostly safe to delegate 80% of rest
  - 20% need further study, safeguards
- http://www.icann.org/en/news/public-comment/name-collision-26feb14-en.htm
  - Other speakers better qualified to say more on this than me...

DNS-OARC

Domain Name System Operations Analysis and Research Center

Some OARC Take-Homes

- There is no substitute for gathering live data from the Internet
- The DNS is pervasive enough its use for data gathering can make it part of the solution,
  not just the problem
- Operators have live data network data, but don't always have the skills/insight/time
  to analyze it
- Researchers can greatly help understand this data, but don't always find it easy to obtain,
  or to interpret operational impact
- Analysis of data is a highly valuable input to informed policy-making and infrastructure protection
- Working together we can answer important protocol, implementation, security and policy questions

DNS-OARC

Domain Name System Operations Analysis and Research Center

Workshops and Meetings

- These are:
  - Twice a year, of 2 days duration
  - Combined with other Internet meetings (RIPE, IETF, NANOG, ICANN)
  - Some member-only content, mostly open to all
  - Sponsor-funded
- May 10-11 2014: Warsaw, PL *(RIPE68)*
- Oct 12-13 2014: Los Angeles, US *(ICANN51)*
- May 16-17 2015: Amsterdam, NL *(RIPE70, SIDN)*
- Oct 03-04 2015: Montreal, CA *(NANOG65)*

DNS-OARC

Domain Name System Operations Analysis and Research Center

Further Information

• Web:	https://www.dns-oarc.net
• Workshops:	https://indico.dns-oarc.net
• E-mail:	admin@dns-oarc.net
• Social:	https://www.linkedin.com/groups/DNSOARC-3193714
• IM:	xmpp:keith@jabber.dns-oarc.net
• Phone:	+1 650 423 1344 (EST)

DNS-OARC

Domain Name System Operations Analysis and Research Center