DNS-OARC's Open DNSSEC Validating Resolver Project

Duane Wessels

APRICOT 2009
Manila, Philippines

February 25, 2009

DNSSEC Landscape

- Spreading outward from the middle.
- Good DNSSEC support in resolver software (BIND, Unbound).
  - But usually not configured
- U.S. Dept of Commerce asked for comments on signing the Root.
  - But we're not there yet...
- IANA has a signed root testbed and an Interim Trust Anchor Repository.
- ~~Six~~ Seven TLDs are signing their zones.
- In other TLDs, domain owners could register signed zones in DLV.

Are End Users Ready?

- DNSSEC means larger responses.
  - Does your NAT/firewall pass DNS messages larger than 512 bytes?
  - And UDP fragments?
  - And allow DNS over TCP?
- Is the channel between applications and resolver secure enough to be trusted? Or should you consider TSIG?
- Will validation failures create chaos and confusion?
- Should applications do their own validation?
- **Now** is the time to tinker with DNSSEC and discover any potential problems.

How To Tinker

- Install or reconfigure a local resolver.
  - Enable DNSSEC features (if necessary)
  - Add trusted keys (e.g., for TLDs, DLV)
  - …and check their signatures?
  - Or use the IANA testbed hints file
  - Or use Paul Wouter's dnssec-conf RPM on Fedora Linux
- Or, for short and simple experimentation, use one of OARC's Open DNSSEC Vadidating Resolvers.
  - https://www.dns-oarc.net/oarc/services/odvr/
  - Currently three flavors
  - Config files provided
  - We collect data for later analysis
- See also www.dnssec.comcast.net

Did you say Open Resolver?

- Myself and others have often pointed out the problems with open resolvers:
  - DDoS attacks
  - Cache poisoning
  - Cache snooping
  - Can trigger bugs
- So why is this open resolver okay?
  - We know its open
  - We rate-limit
  - We log everything

What's Running?

- BIND 9.5 (bind.odvr.dns-oarc.net)
- Unbound 1.1.1 (unbound.odvr.dns-oarc.net)
- IANA testbed (iana-testbed.odvr.dns-oarc.net)
  - ns.iana.org is the Root
  - Also BIND 9.5

bind.odvr.dns-oarc.net

- Trust anchors for TLDs with KSKs:
  - Currently: bg, br, cz, museum, pr, se, gov
  - Plus IANA's experimental IDN TLDs
- DNSSEC Lookaside Validation to dlv.isc.org.
- Master for bogon space.

```
options {
   directory     "/etc/namedb";
   pid-file      "/var/run/named/odvr.pid";
   listen-on     { 149.20.64.20; };
   listen-on-v6 { 2001:4f8:3:2bc:1::64:20; };
   query-source address 149.20.64.20;
   query-source-v6 address 2001:4f8:3:2bc:1::64:20;
   allow-query   { any; };
   recursion       yes;
   dnssec-enable yes;
   dnssec-lookaside . trust-anchor dlv.isc.org;
};

zone "." { type hint; file "named.root"; };

include "trusted-keys.conf";
include "master-bogons.conf";
include "named-rndc.conf";
```

unbound.odvr.dns-oarc.net

- Trust anchors for TLDs with KSKs.
- DNSSEC Lookaside Validation to dlv.isc.org.

```
server:
        num-threads: 1
        Interface: 149.20.64.21
        Interface 2001:4f8:3:2bc:1::64:21
        outgoing-interface: 149.20.64.21
        outgoing-interface: 2001:4f8:3:2bc:1::64:21
        outgoing-range: 32768
        access-control: 0.0.0.0/0 allow
        access-control: ::0/0 allow
        chroot: "/proj/odvr/unbound"
        directory: "/proj/odvr/unbound"
        pidfile: "/var/run/unbound.pid"
        logfile: "/var/log/unbound.log"
        Verbosity: 2

include: "etc/trusted-keys.conf"
include: "etc/dlv-keys.conf"
```

iana-testbed.odvr.dns-oarc.net

- Single trust anchor for ns.iana.org Root zone.
- Master for bogon space.

```
options {
  directory "/etc/namedb";
  pid-file  "/var/run/named/iana-testbed.odvr.pid";
  listen-on     { 149.20.64.22; };
  listen-on-v6  { 2001:4f8:3:2bc:1::64:22; };
  query-source  address 149.20.64.22;
  query-source-v6 address 2001:4f8:3:2bc:1::64:22;
  allow-query   { any; };
  recursion     yes;
  dnssec-enable yes;
};

zone "." { type hint; file "iana-testbed.root"; };

include "trusted-keys.conf";
include "master-bogons.conf";
include "named-rndc.conf";
```

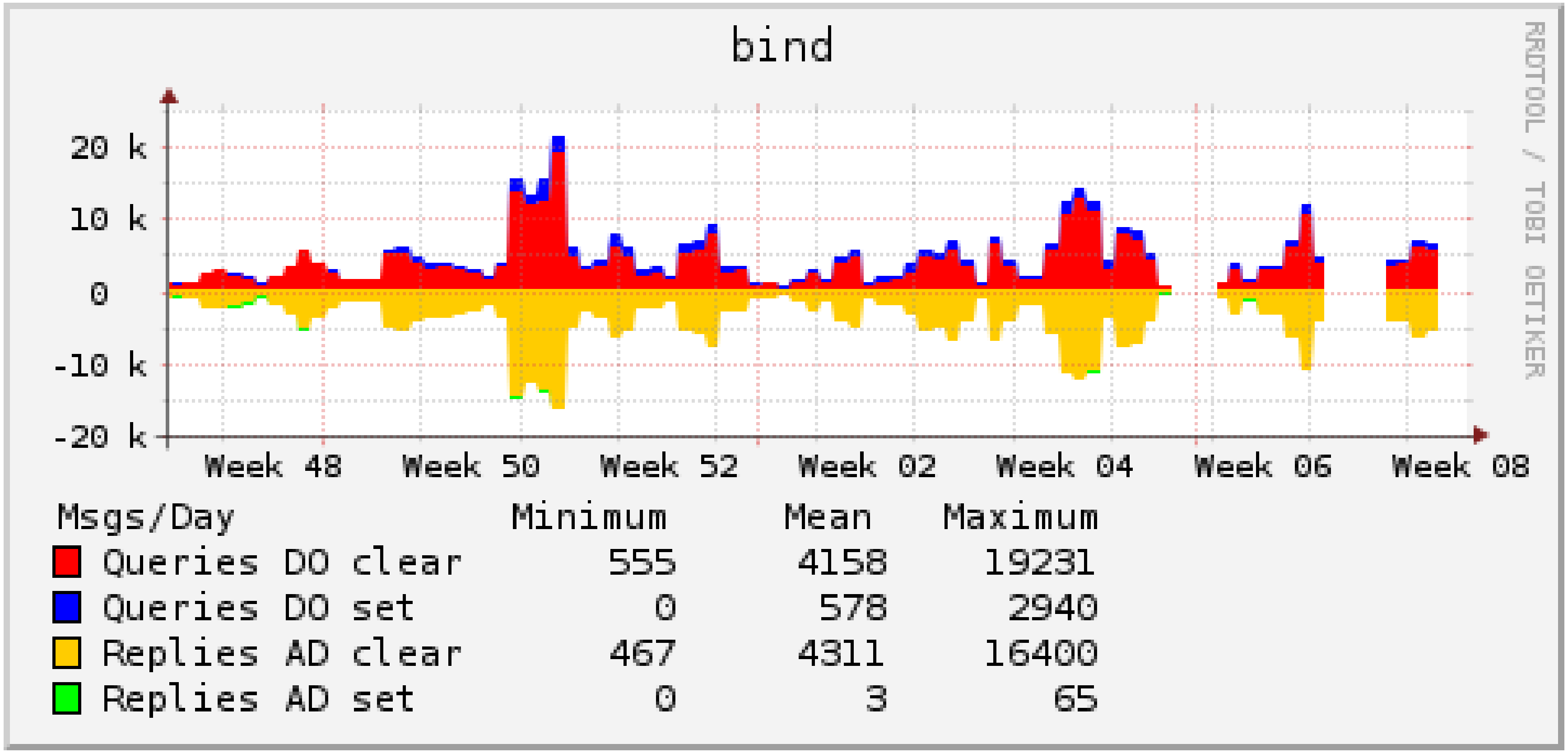
Finding Trust Anchors

- Perl script probes TLDs nightly for KSKs
  - by sending DNS queries
- Handles changes, removals, and additions.
- Keys are stored in SQL database.
- Root zone and dlv.isc.org are handled as special cases.

Validating Published KSKs

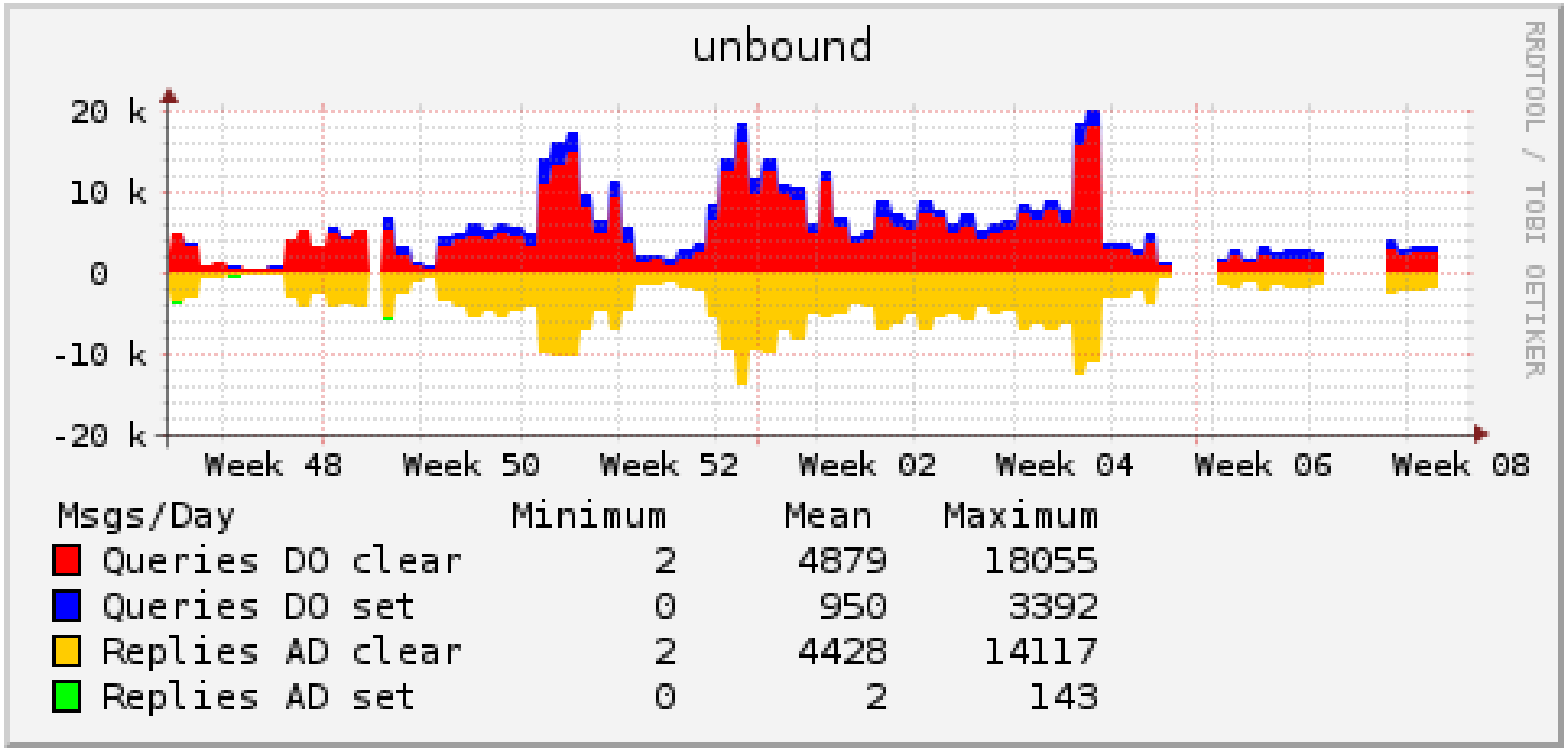
- Administrator receives email notification when KSKs are added or removed.
- Manually track down keys published on registry web pages
    - Google, mailing lists, etc
- Check PGP signature if available
- Set validated bit in SQL database if PGP signature validates.
- Validated bit is “FYI” only. We currently include all trust anchors in our configs, even if they can't be validated.

BIND Traffic



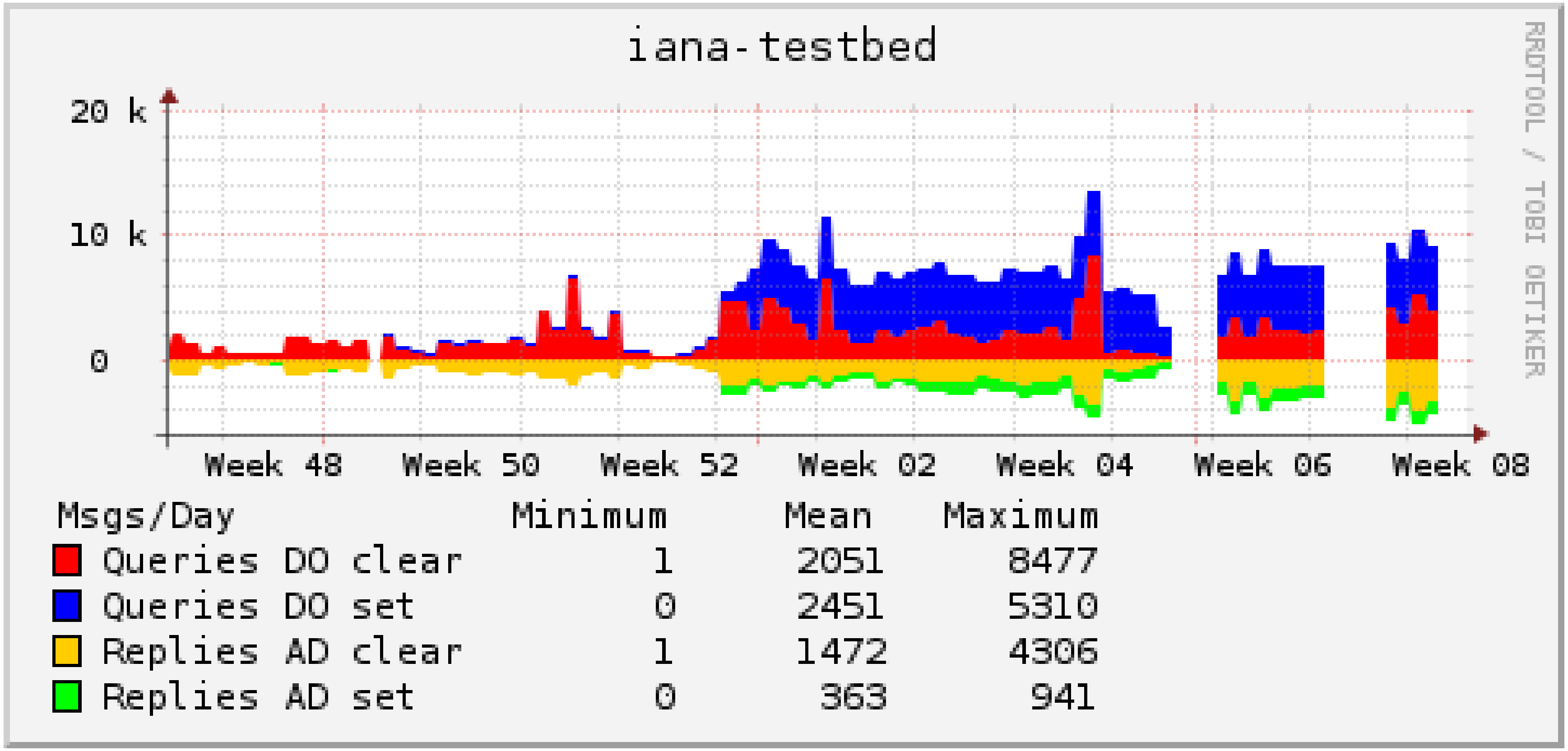
Msgs/Day	Minimum	Mean	Maximum
🟥 Queries DO clear	555	4158	19231
🟦 Queries DO set	0	578	2940
🟨 Replies AD clear	467	4311	16400
🟩 Replies AD set	0	3	65

Unbound Traffic



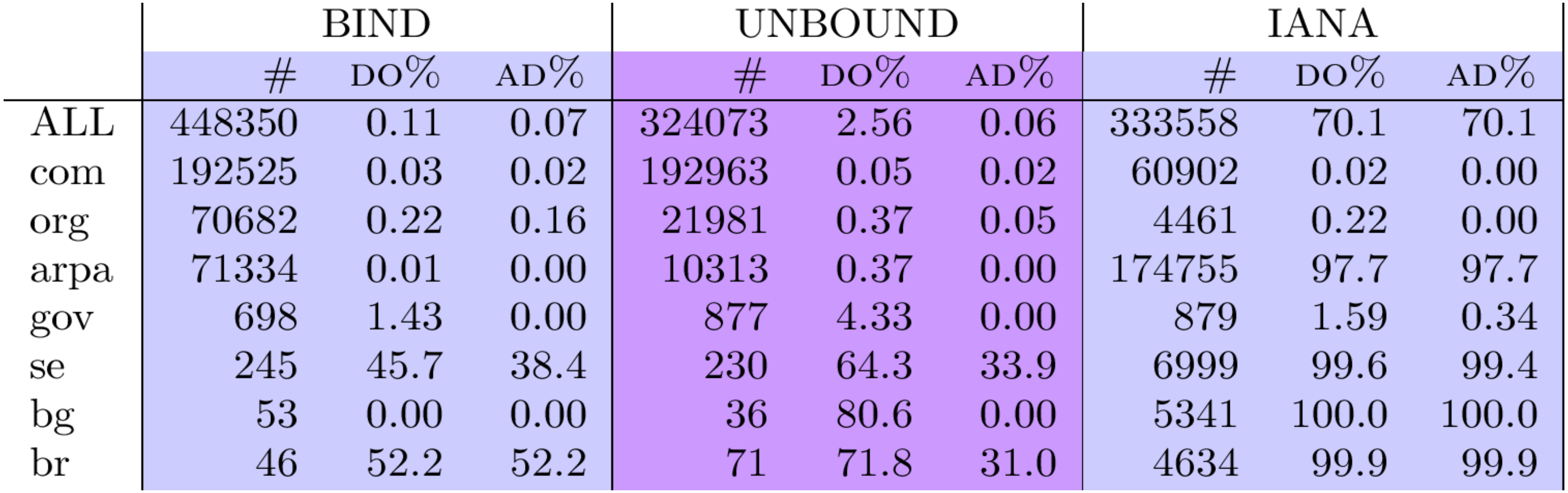
Msgs/Day	Minimum	Mean	Maximum
🟥 Queries DO clear	2	4879	18055
🟦 Queries DO set	0	950	3392
🟨 Replies AD clear	2	4428	14117
🟩 Replies AD set	0	2	143

IANA Testbed Traffic



Msgs/Day	Minimum	Mean	Maximum
🟥 Queries DO clear	1	2051	8477
🟦 Queries DO set	0	2451	5310
🟨 Replies AD clear	1	1472	4306
🟩 Replies AD set	0	363	941

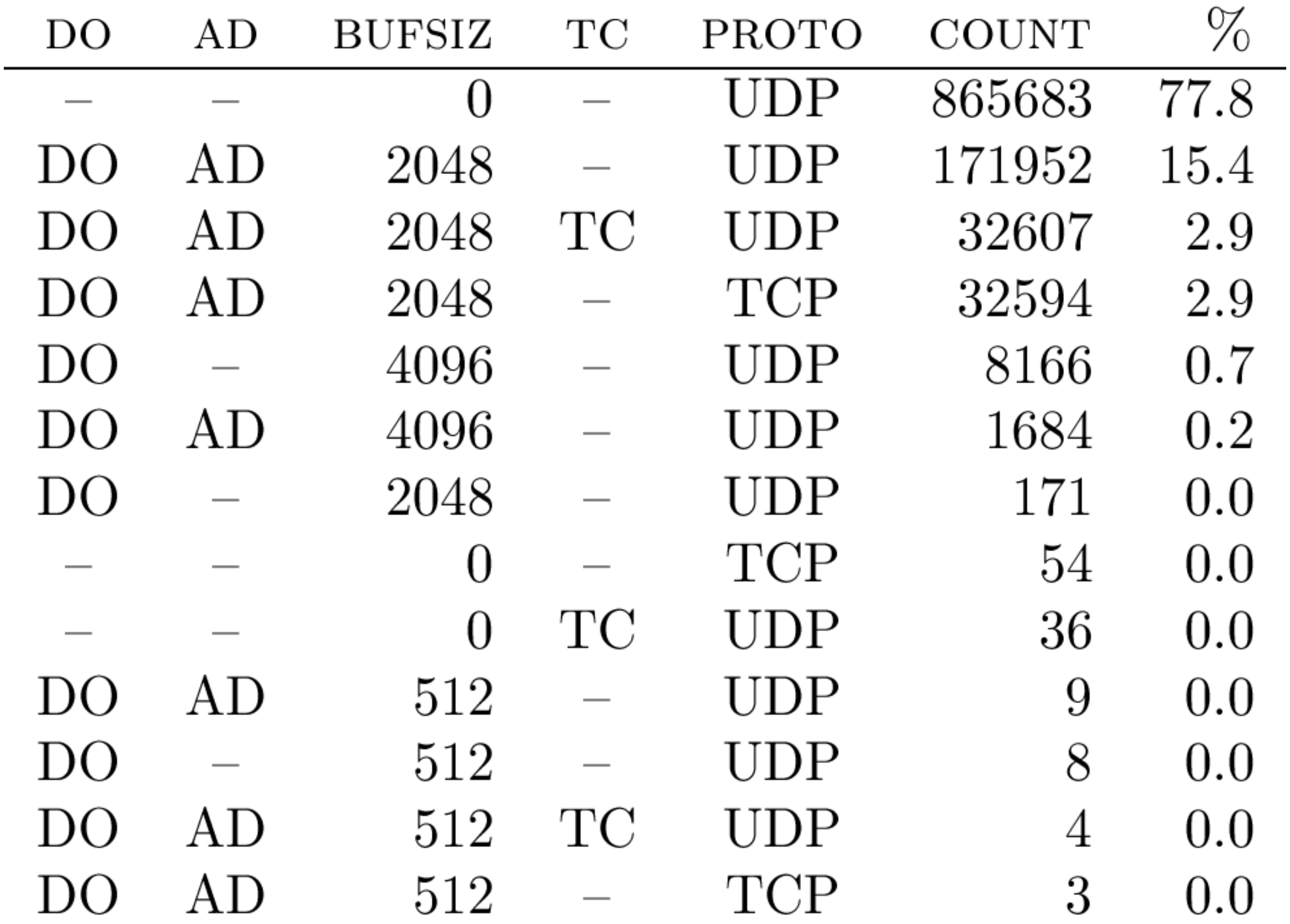
DO and AD bits by TLD



	BIND			UNBOUND			IANA		
	#	DO%	AD%	#	DO%	AD%	#	DO%	AD%
ALL	448350	0.11	0.07	324073	2.56	0.06	333558	70.1	70.1
com	192525	0.03	0.02	192963	0.05	0.02	60902	0.02	0.00
org	70682	0.22	0.16	21981	0.37	0.05	4461	0.22	0.00
arpa	71334	0.01	0.00	10313	0.37	0.00	174755	97.7	97.7
gov	698	1.43	0.00	877	4.33	0.00	879	1.59	0.34
se	245	45.7	38.4	230	64.3	33.9	6999	99.6	99.4
bg	53	0.00	0.00	36	80.6	0.00	5341	100.0	100.0
br	46	52.2	52.2	71	71.8	31.0	4634	99.9	99.9

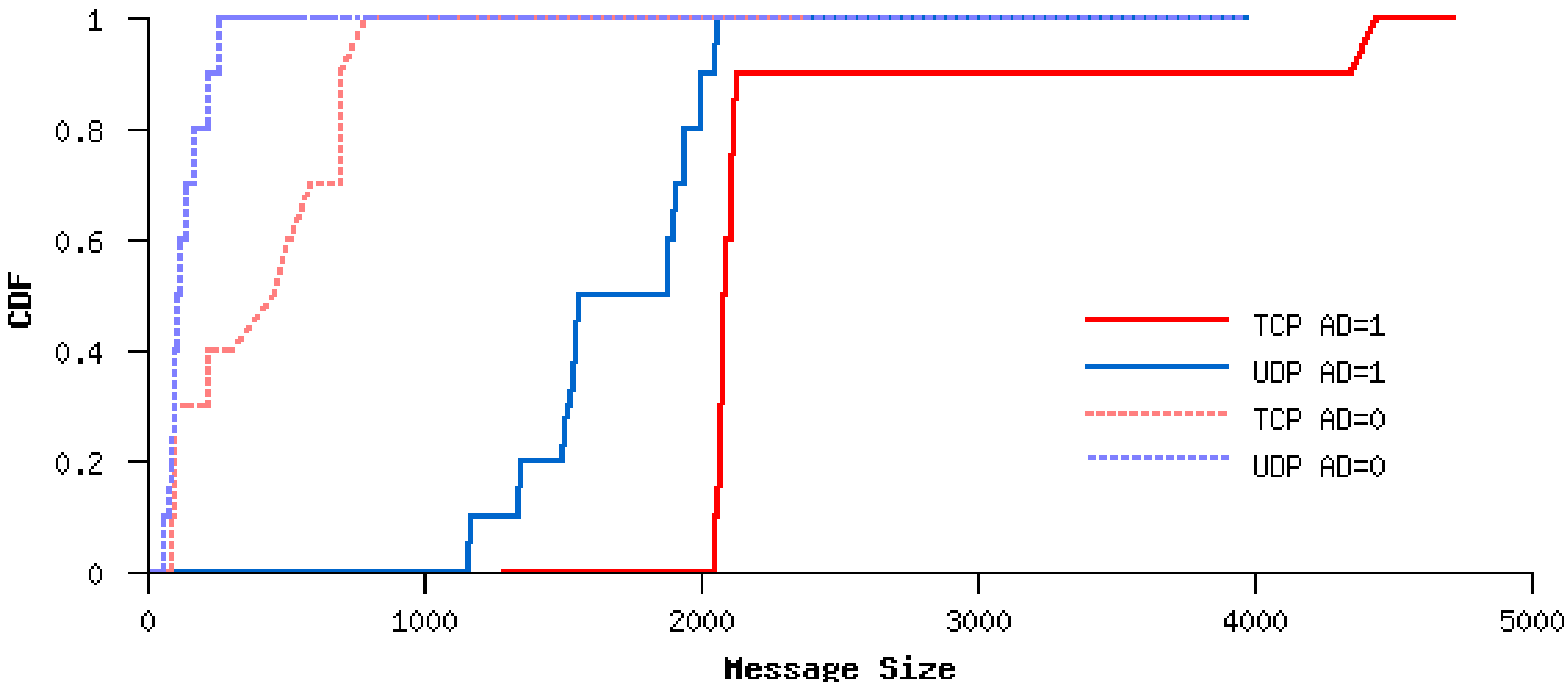
Note: Many queries to the IANA resolver are tests coming from ICANN.

EDNS Buffer Sizes and Truncation



DO	AD	BUFSIZ	TC	PROTO	COUNT	%
–	–	0	–	UDP	865683	77.8
DO	AD	2048	–	UDP	171952	15.4
DO	AD	2048	TC	UDP	32607	2.9
DO	AD	2048	–	TCP	32594	2.9
DO	–	4096	–	UDP	8166	0.7
DO	AD	4096	–	UDP	1684	0.2
DO	–	2048	–	UDP	171	0.0
–	–	0	–	TCP	54	0.0
–	–	0	TC	UDP	36	0.0
DO	AD	512	–	UDP	9	0.0
DO	–	512	–	UDP	8	0.0
DO	AD	512	TC	UDP	4	0.0
DO	AD	512	–	TCP	3	0.0

AD=0 vs AD=1 Response Sizes



Questions?

wessels@dns-oarc.net

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

DNS-OARC