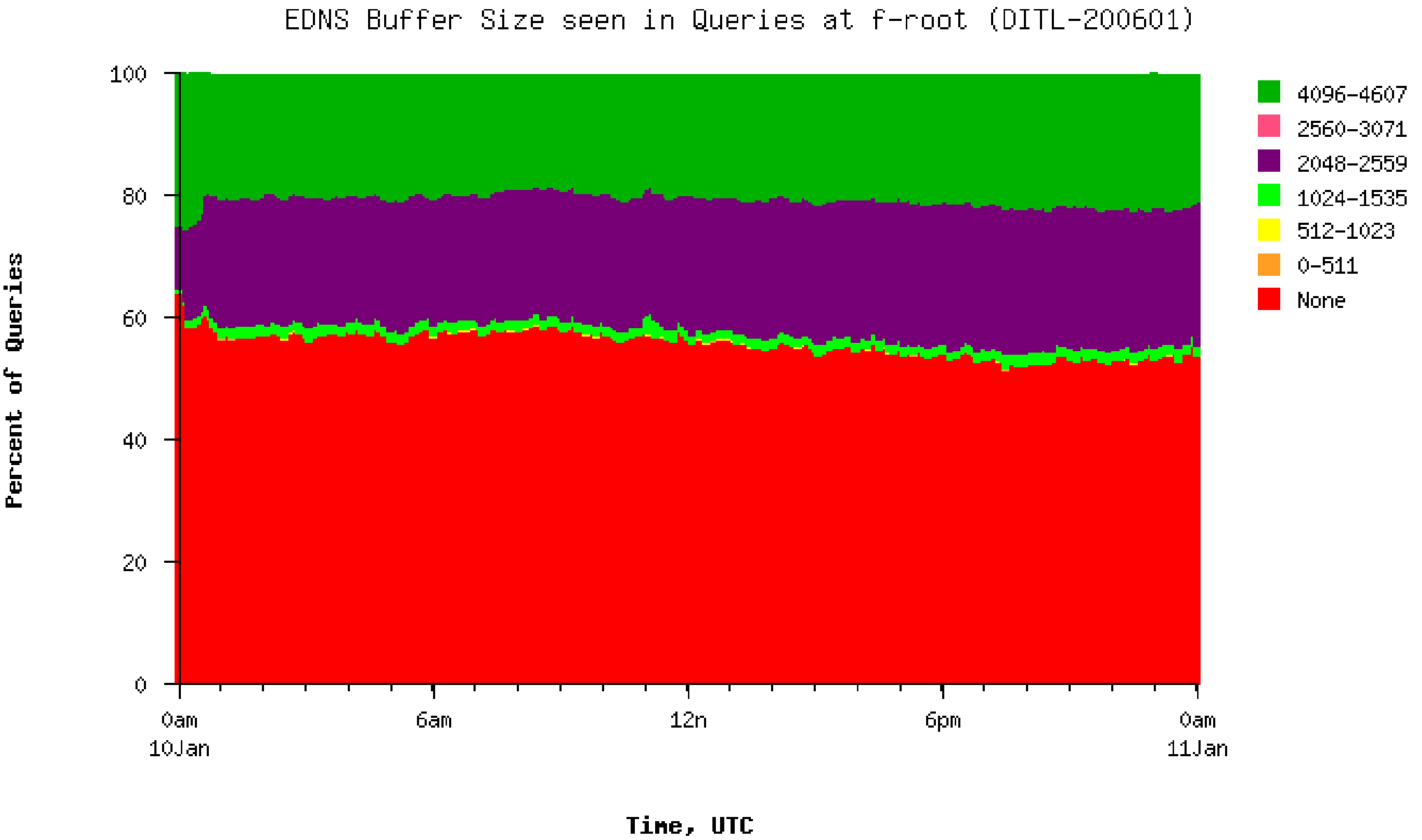
DNSSEC, EDNS, and TCP

NANOG 46
Lightning Talk

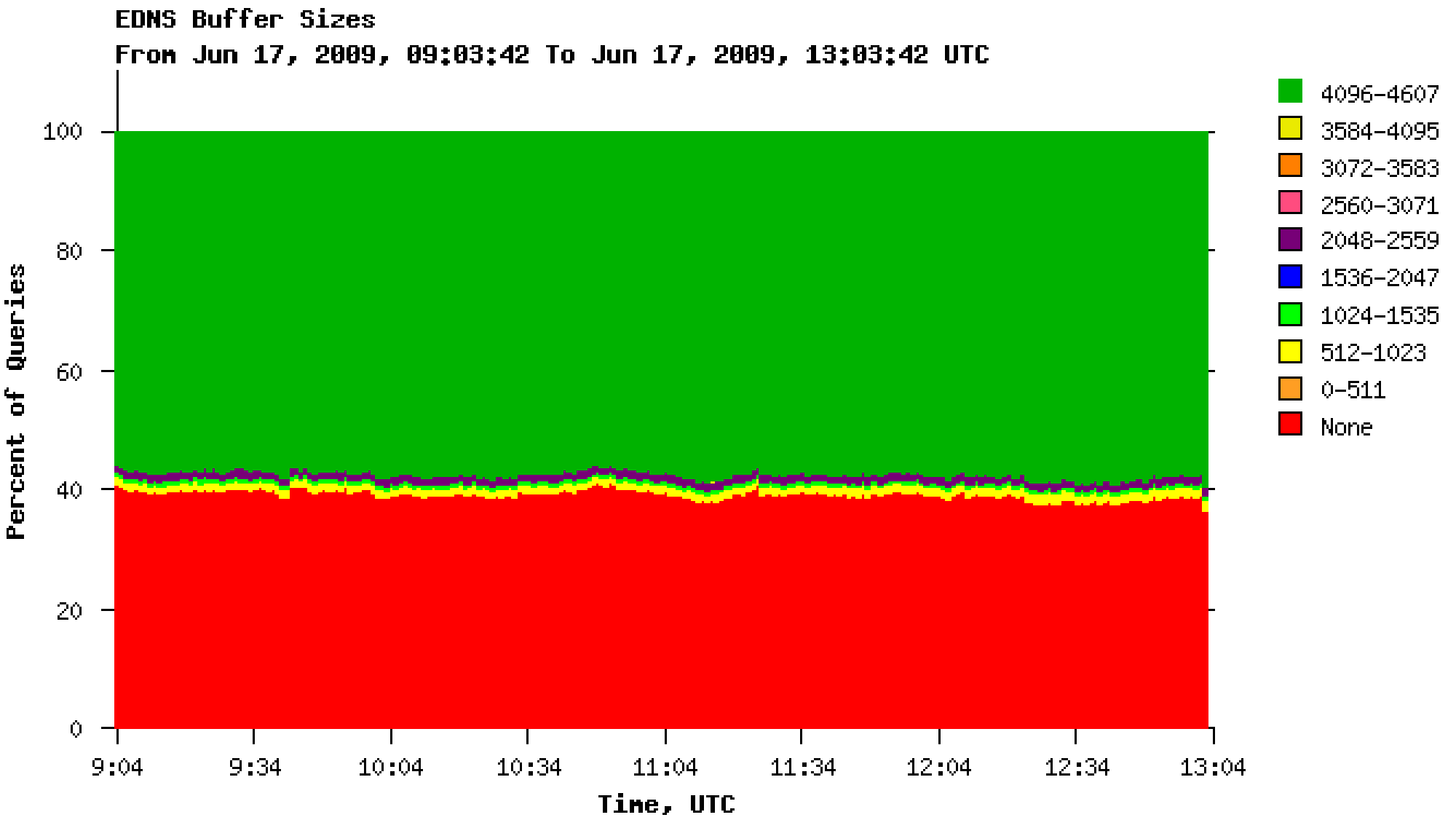
Duane Wessels
and Sebastian Castro

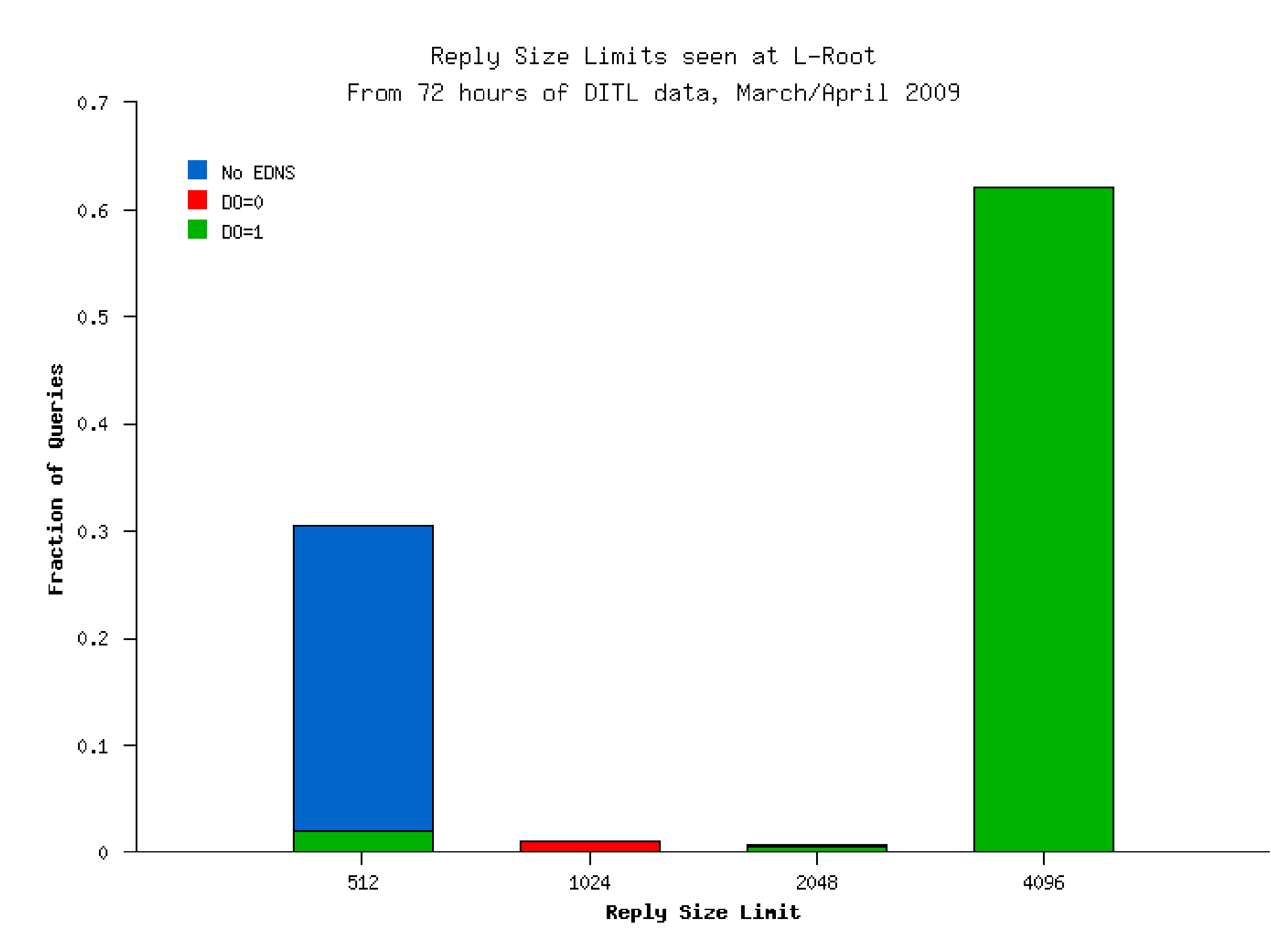
DNS-OARC

f.root-servers.net (2007)



c.root-servers.net (today)




Reply Size Limits seen at L-Root
From 72 hours of DITL data, March/April 2009
No EDNS
DO=0
DO=1
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
Fraction of Queries
512
1024
2048
4096
Reply Size Limit

Date: Tue, 2 Jun 2009 16:21:28 -0400
From: Dave Knight <dknight@ca.afilias.info>
To: dns-operations@dns-oarc.net
Subject: [dns-operations] .ORG is signed

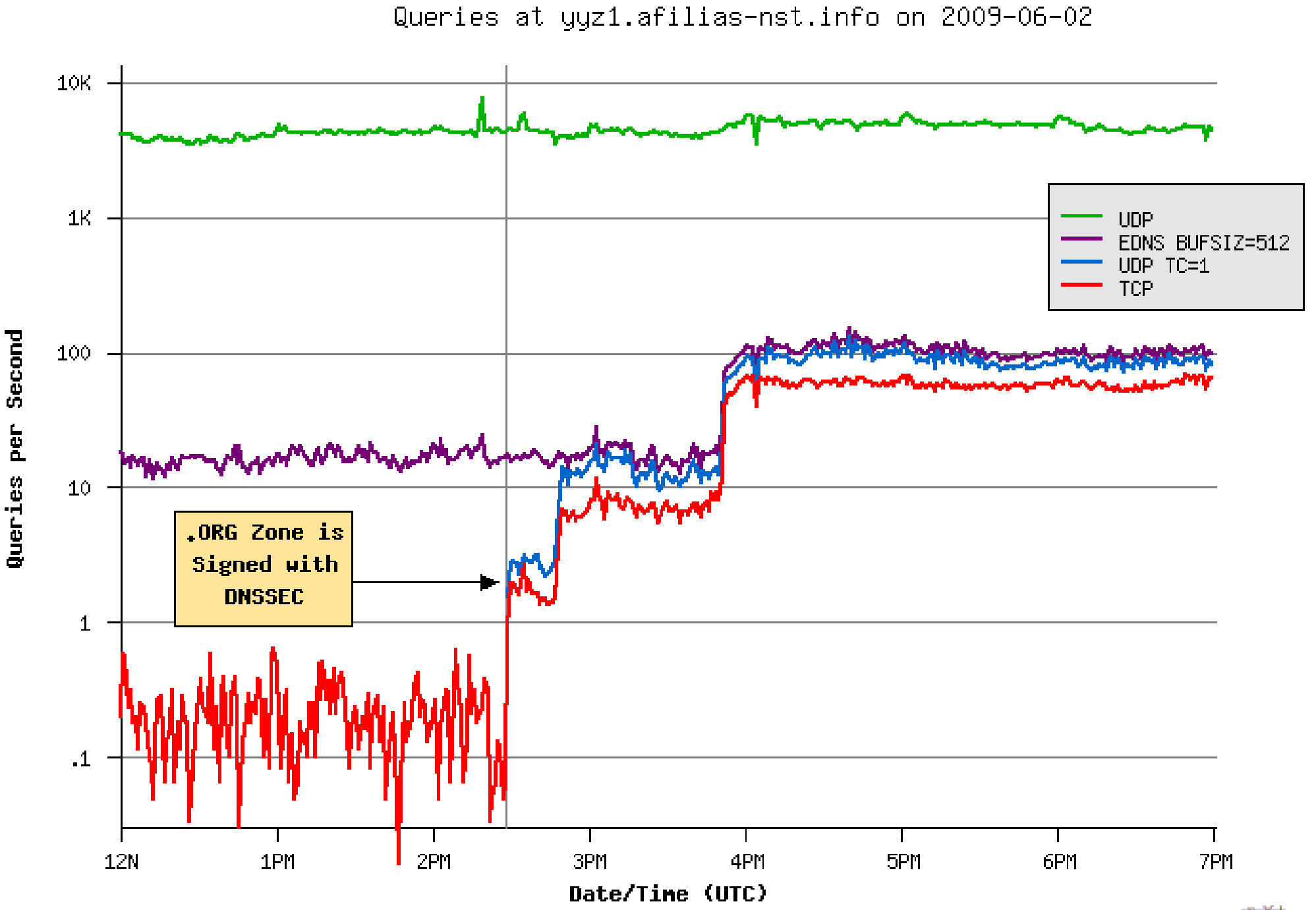
Colleagues,

On behalf of PIR Technical Support I would like to announce that as of today, 2009-06-02, at 16:00 UTC .ORG is DNSSEC signed.

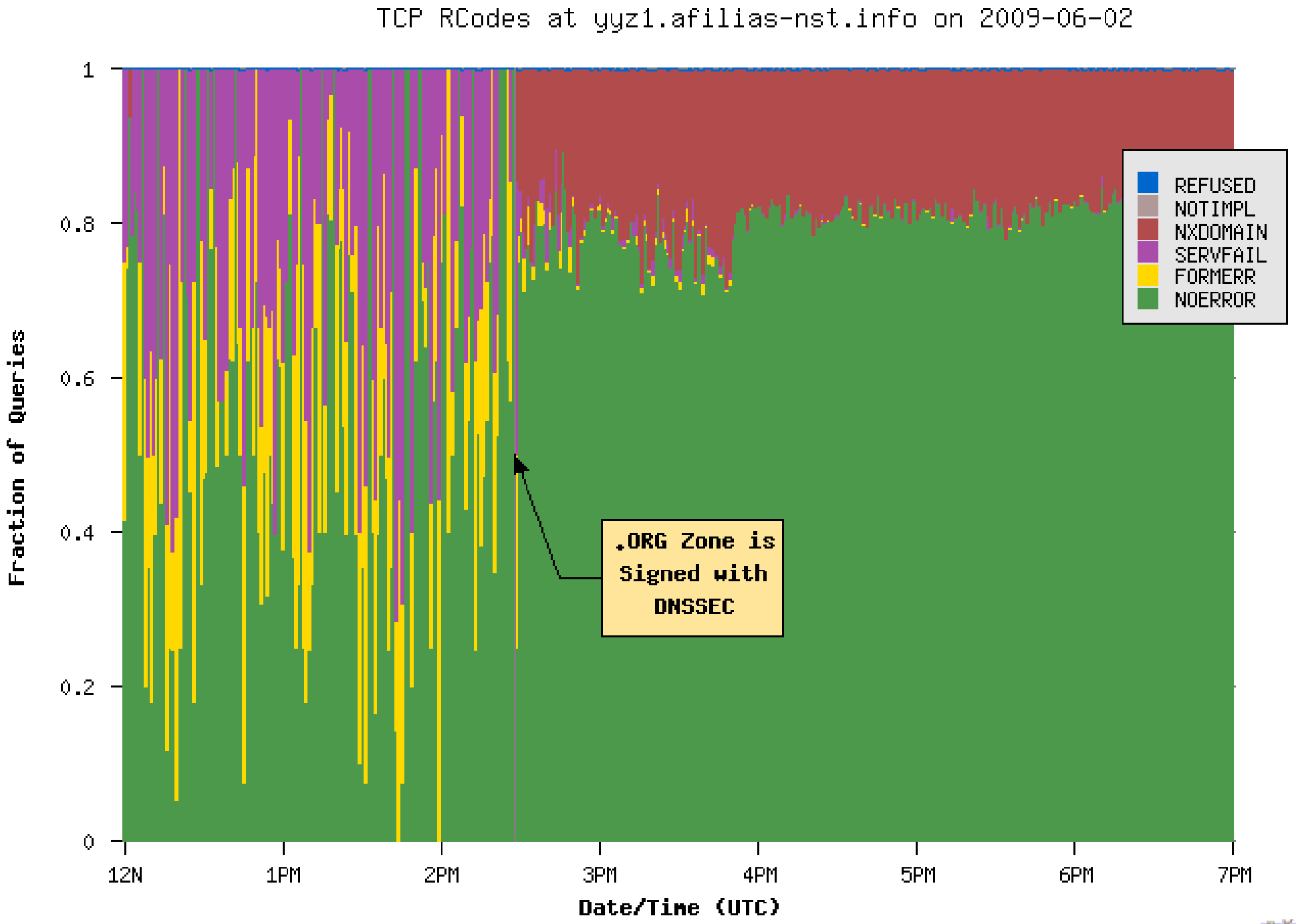
DNS-OARC

was kind enough to share some packet traces with DNS-OARC from this day.

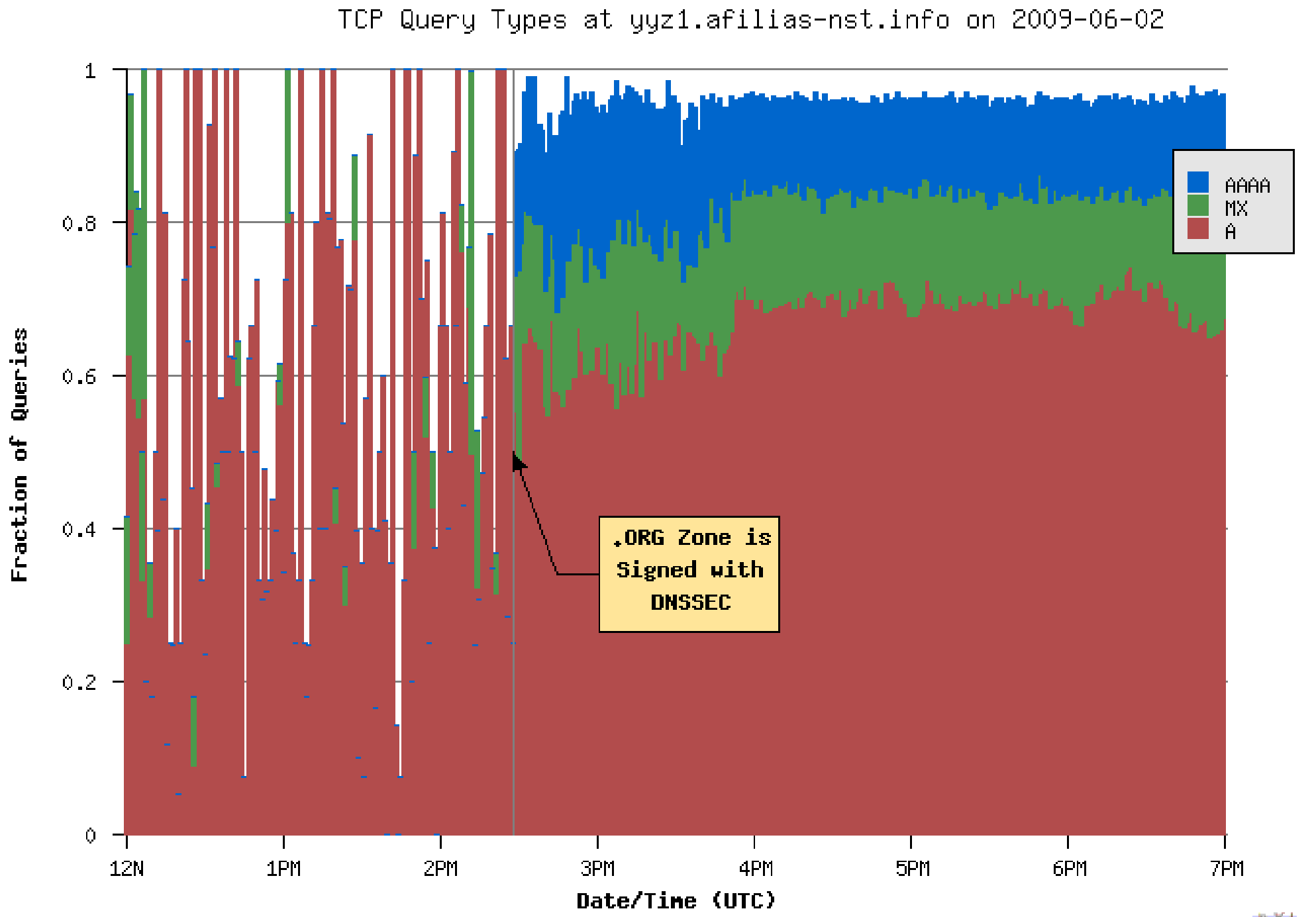
DNS-OARC



DNS-OARC

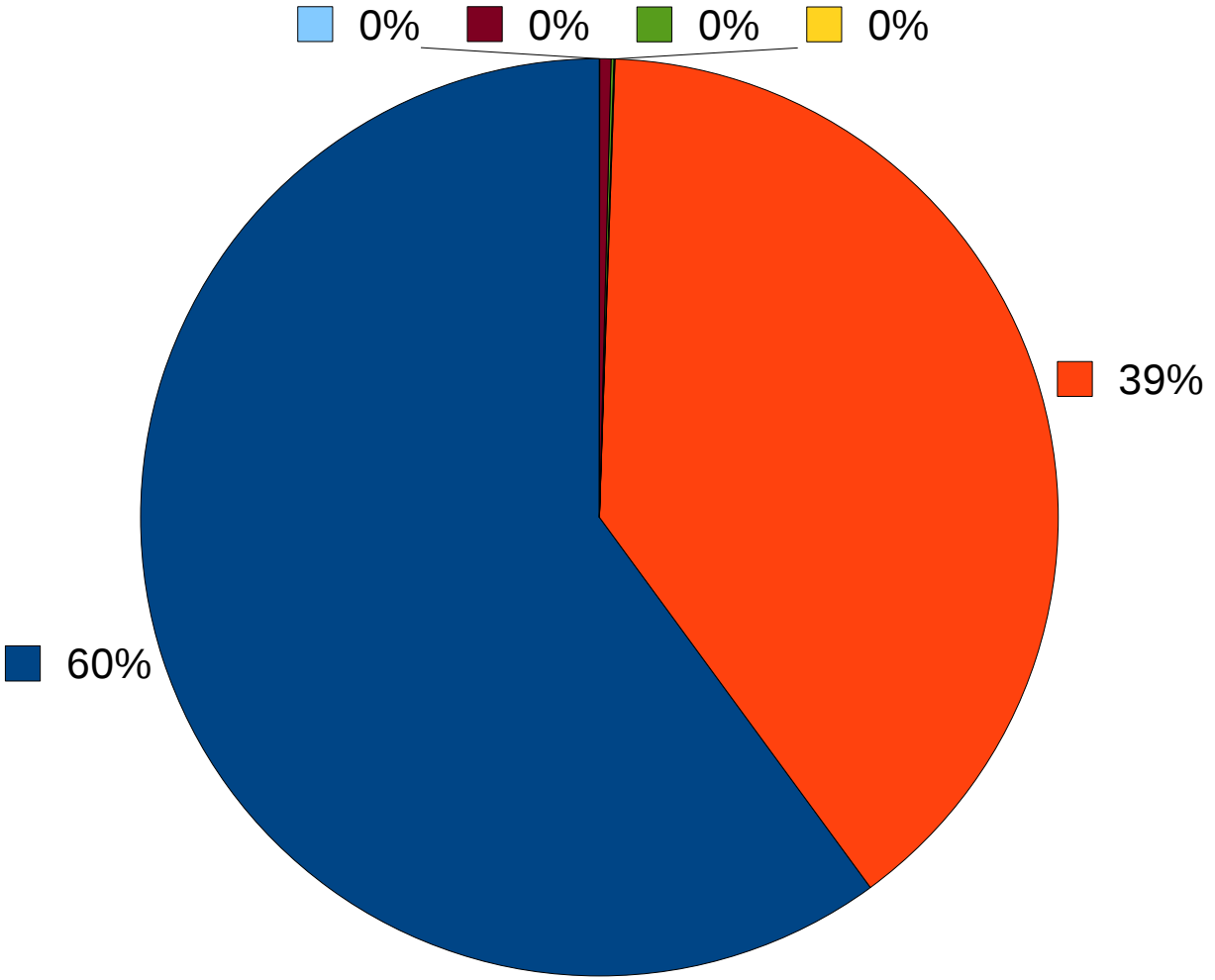


DNS-OARC



DNS-OARC

fpdns Analysis



DNS-OARC

RFC 4035:

A security-aware name server MUST support the EDNS0 ([RFC2671]) message size extension, MUST support a message size of at least **1220** octets, and SHOULD support a message size of 4000 octets.

BIND 9.5.0a1 CHANGES:

1954. [func] Named now falls back to advertising EDNS with a **512** byte receive buffer if the initial EDNS queries fail. [RT #14852]

DNS-OARC