Testbed: DNSSEC für DE

- Bericht zum Advent -

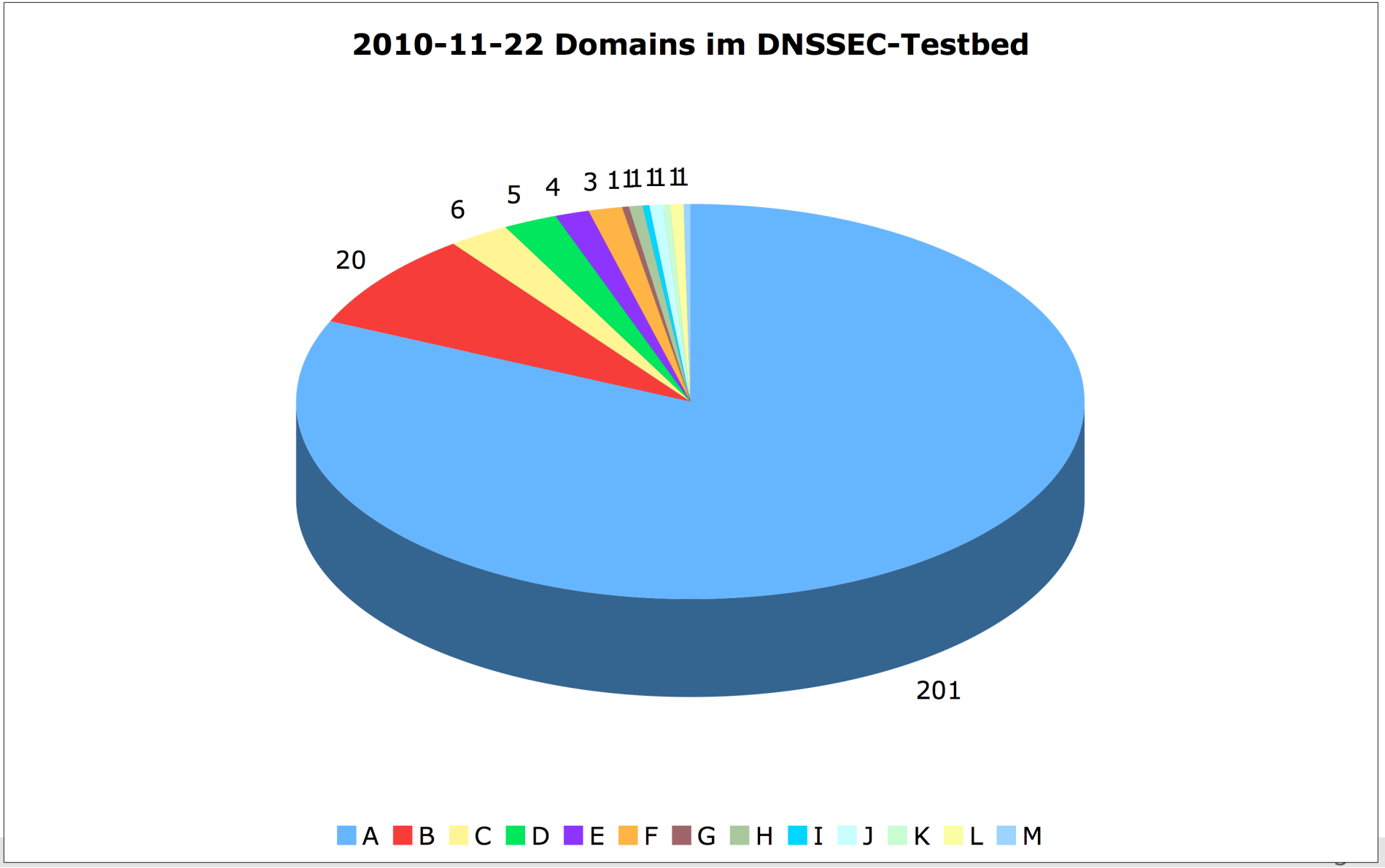
Peter Koch <koch@denic.de>
Marcos Sanz <sanz@denic.de>

Frankfurt/Main, 24. November 2010

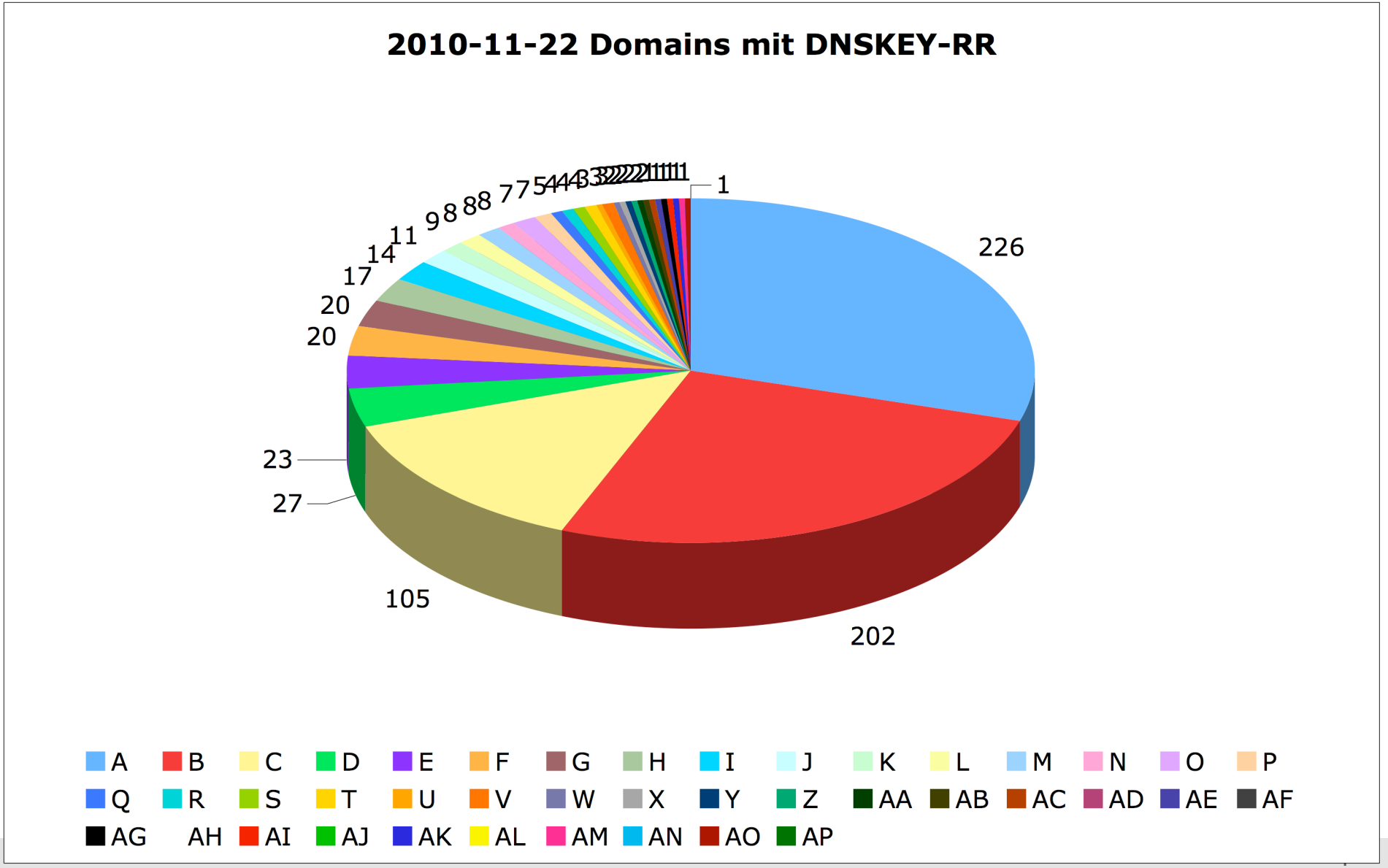
Testbed-Status

- 246 Domains im Testbed
  - 13 RegAccs
  - aktuell 6% mit Validierungsfehlern
- ca. 120 q/s im Tagesmittel
  - davon 20-30% via IPv6
- 225 Abonnenten auf der Testbedliste
- Zonenaktualisierung dreimal täglich
  - YYYYMMDD{29,61,93}, ca. 08:30, 16:30, 00:30

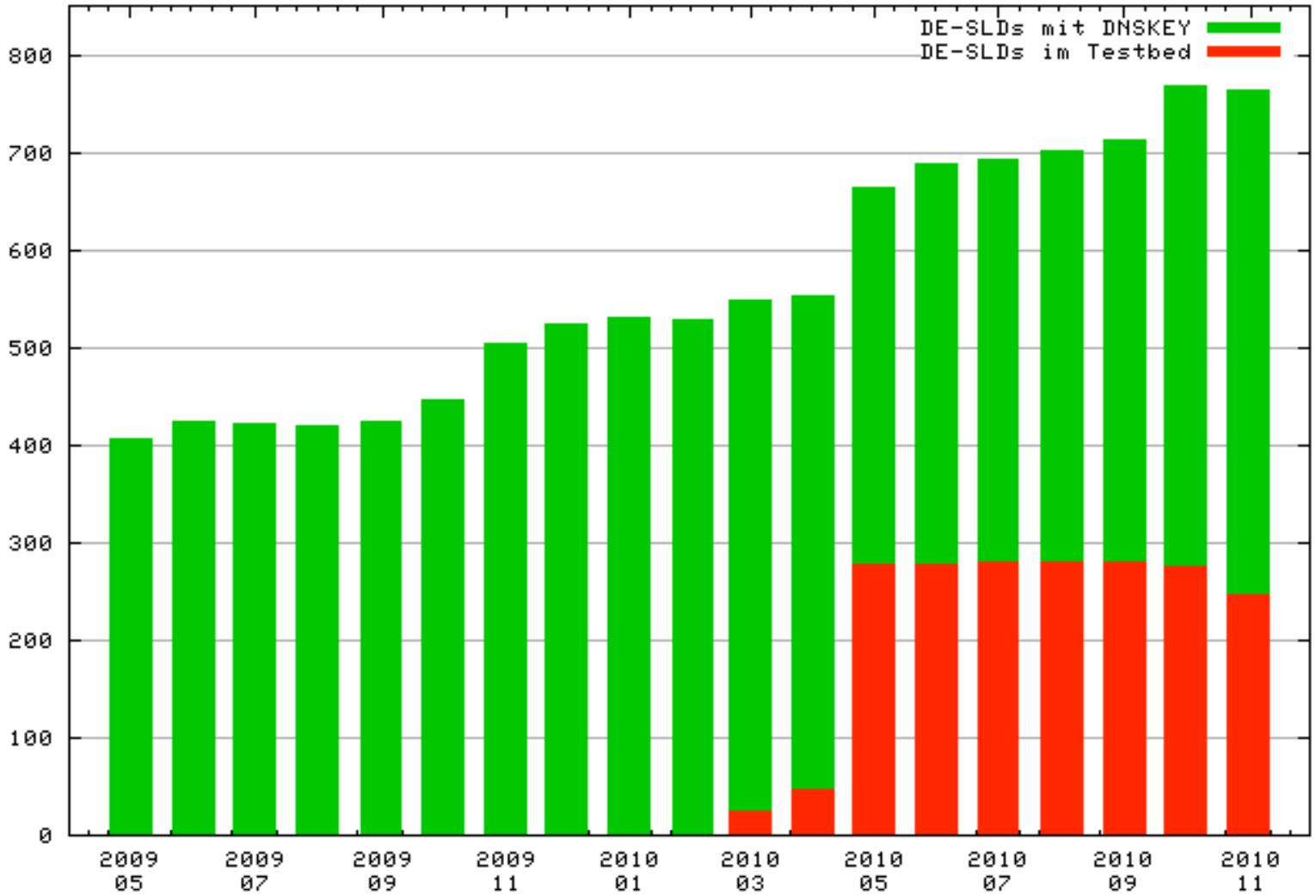
RegAccs mit DNSSEC-Kunden im Testbed



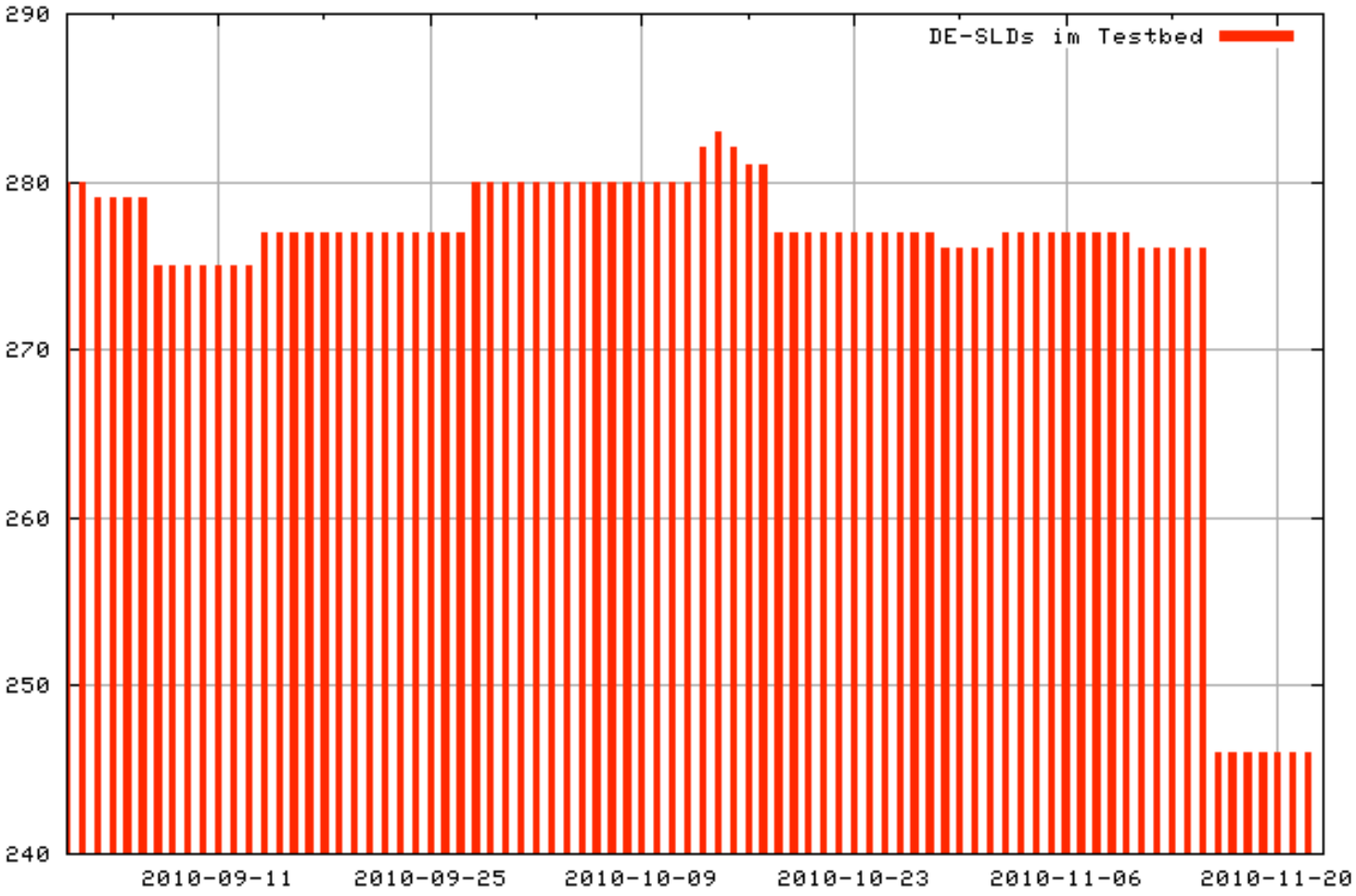
RegAccs mit DNSSEC-Interessenten aktuell



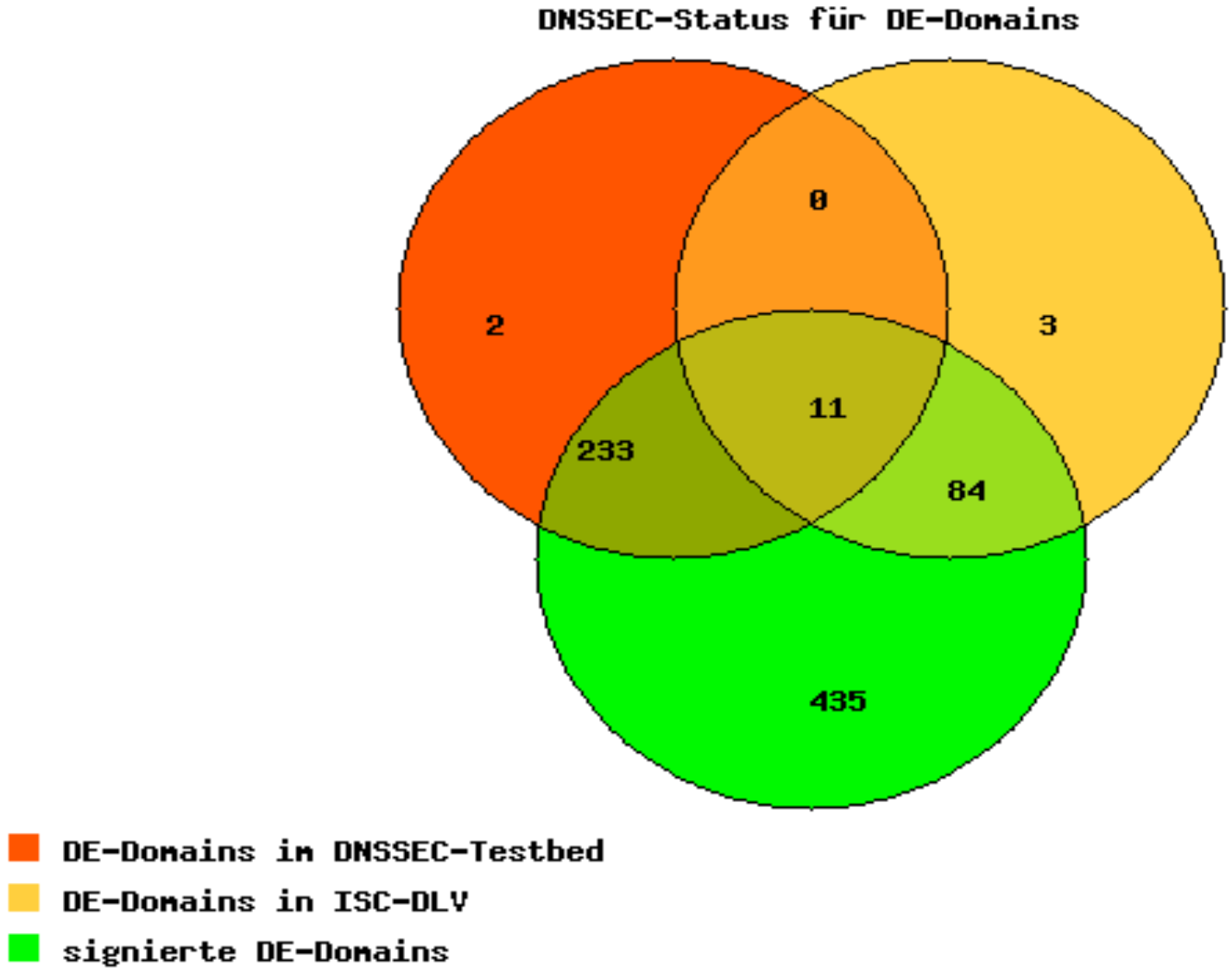
Entwicklung DNSKEY unter DE (11/2010)



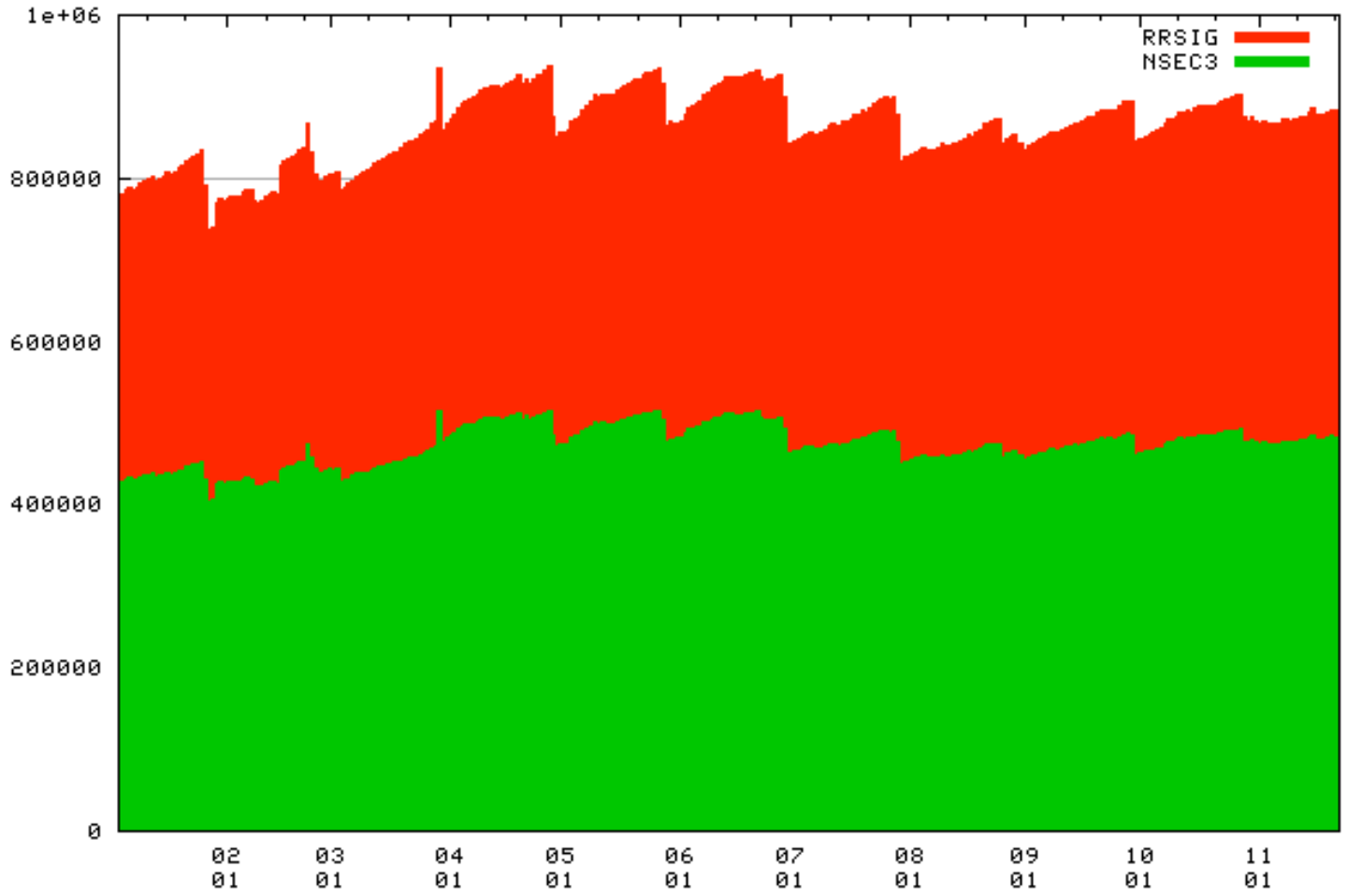
Entwicklung DNSKEY im Testbed (09-11/2010)



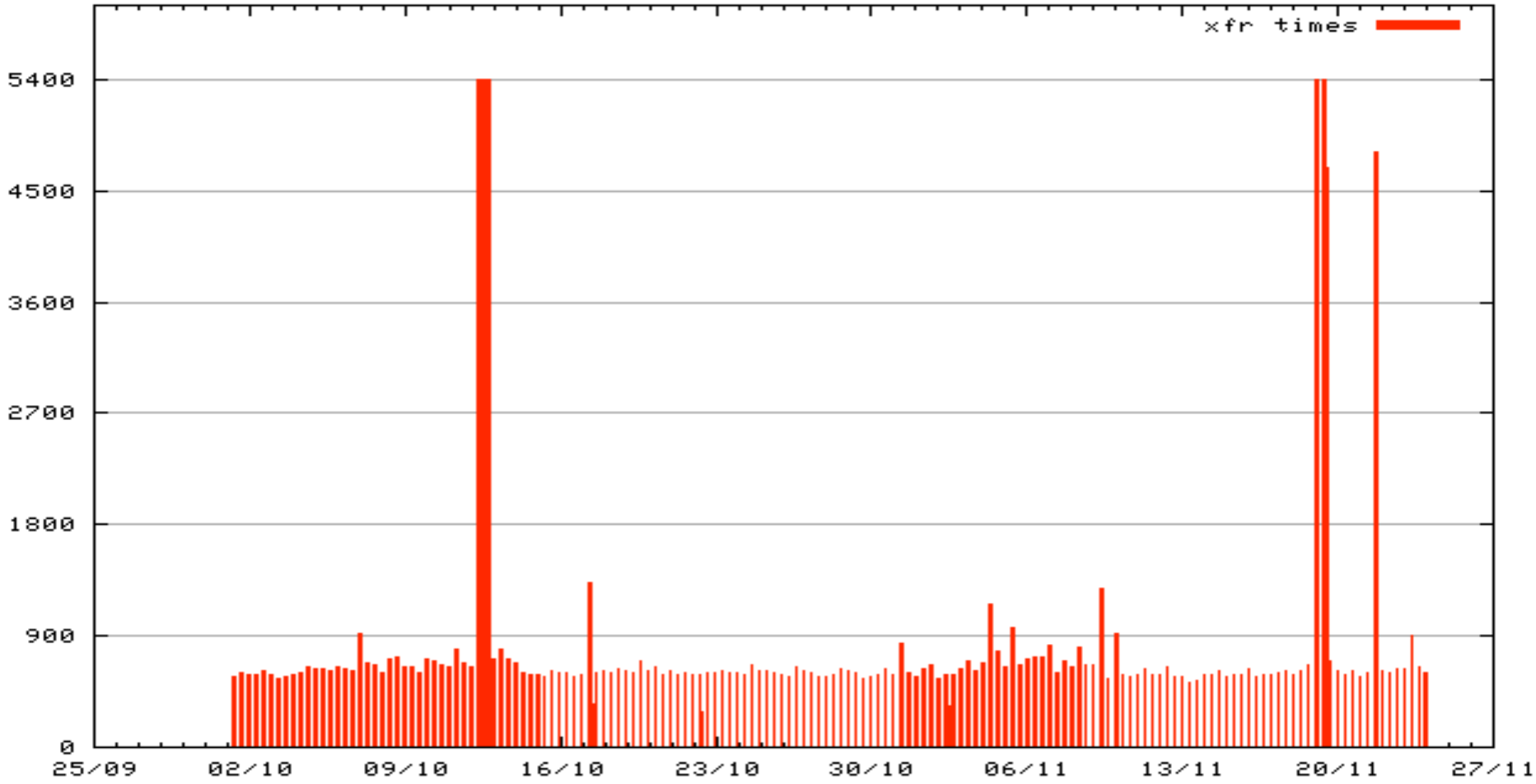
Signiert vs. Testbed vs. ISC-DLV (2010-11-22)



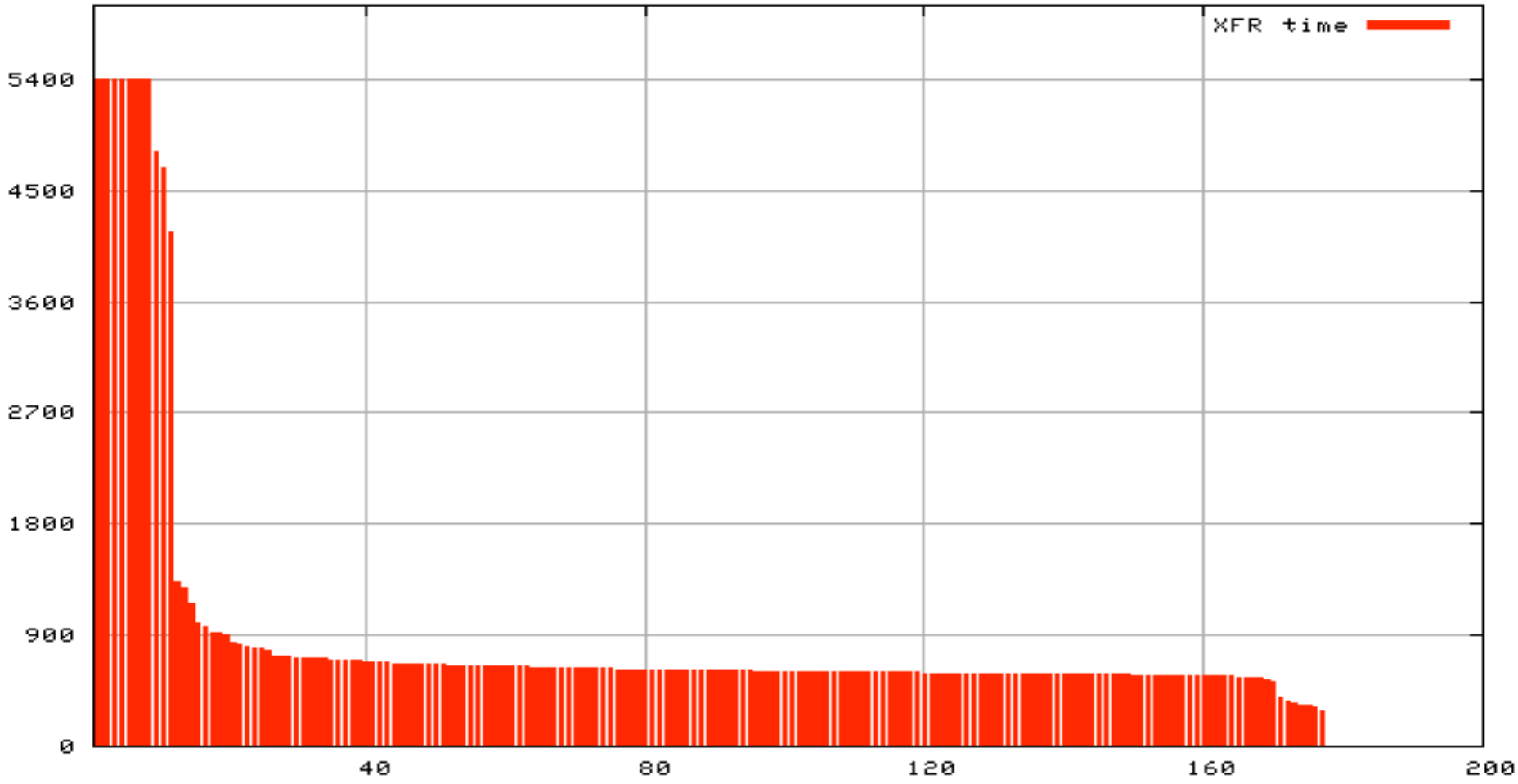
Anzahl NSEC3/RRSIG-RRs (2010-11-22)



Verteilung der XFR-Zeiten nach HK



Verteilung der XFR-Zeiten nach HK (ii)



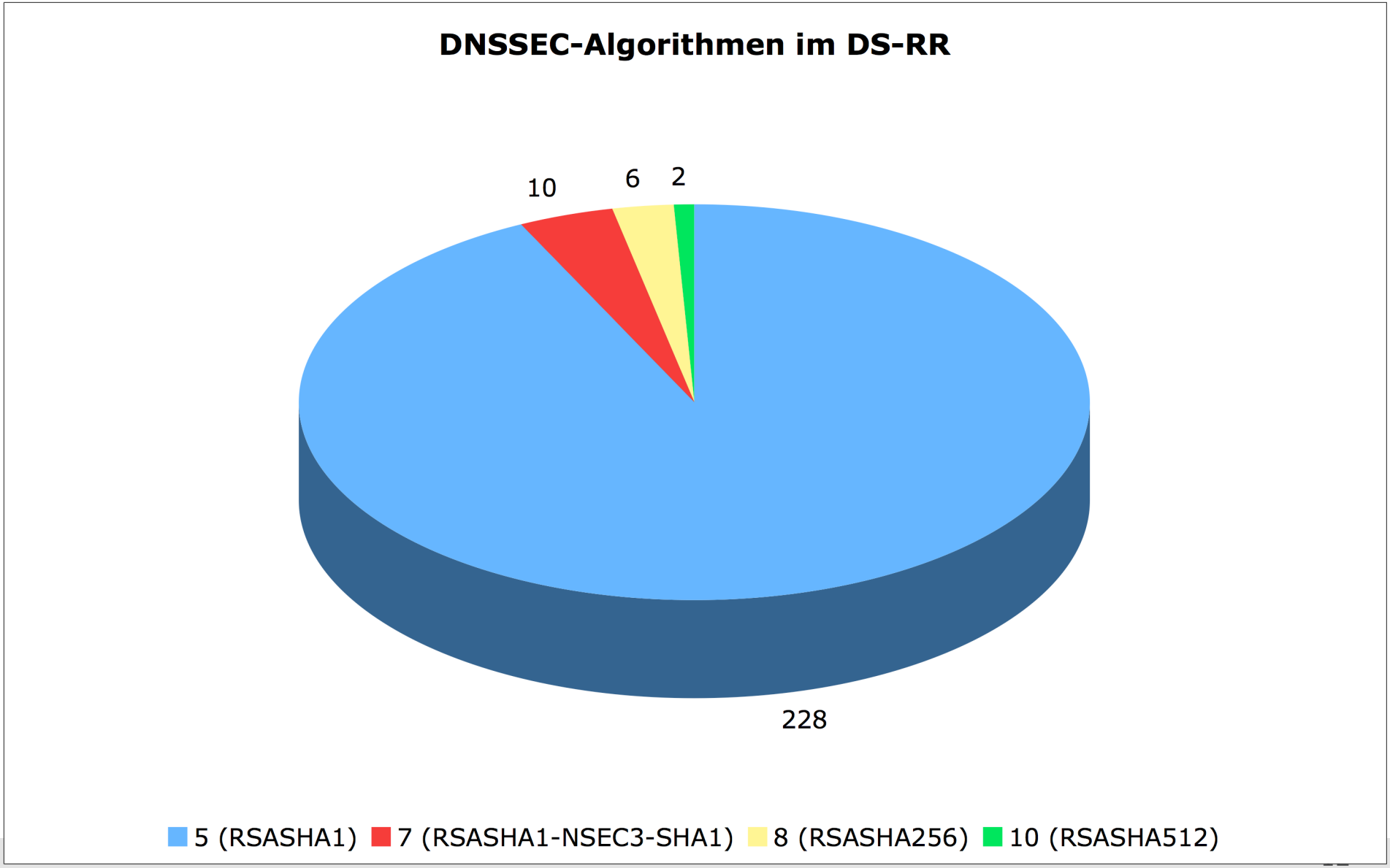
NAST-Webclient http://nast.denic.de

Nameserver Predelegation Check Webinterface

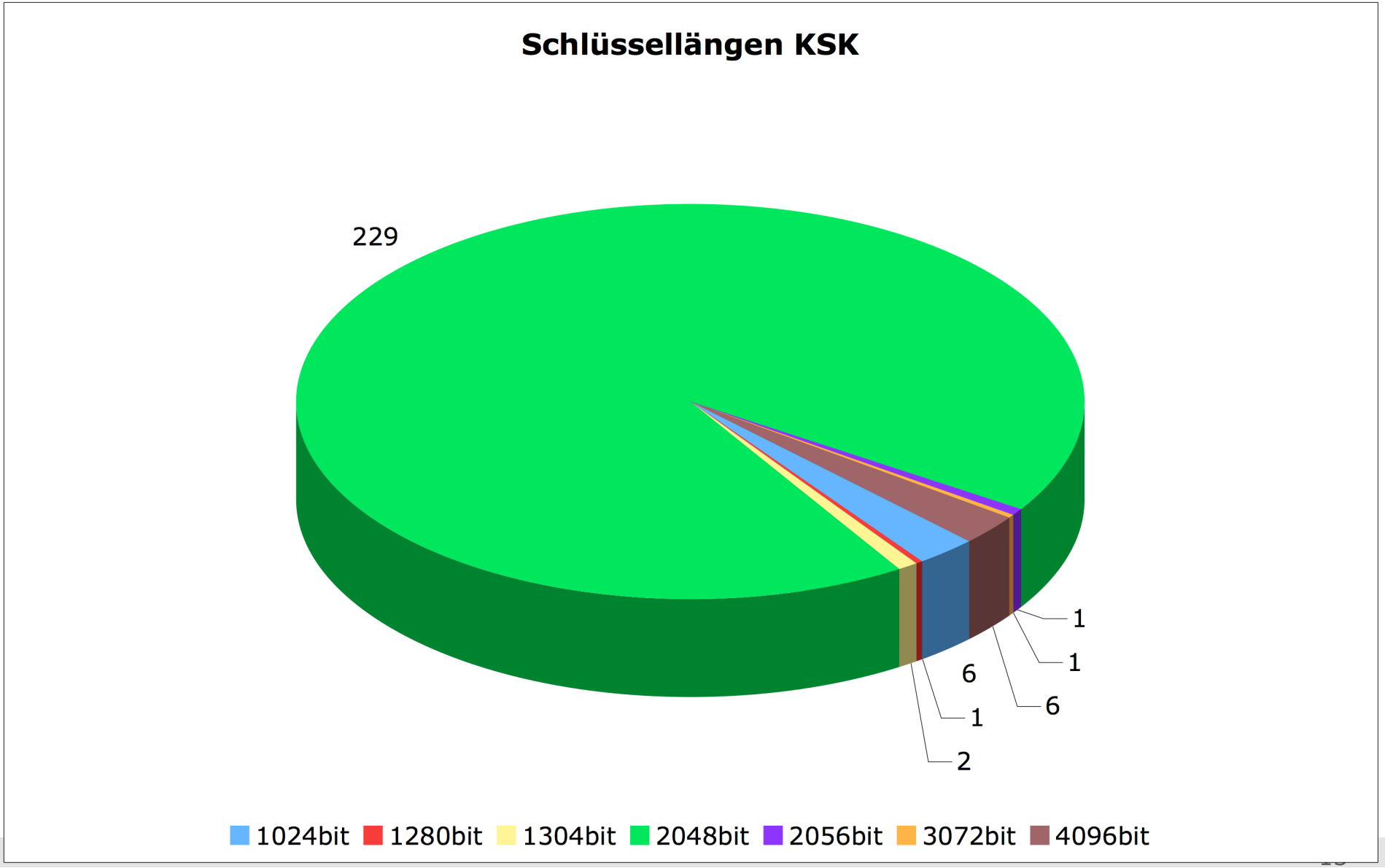
Mit dem NAST Webinterface können Sie einen Nameserver Predelegation Check durchführen. Die Nameserver Ihrer Zone (Domain) werden dabei verschiedenen Tests unterzogen, um sicherzustellen, dass sie korrekt konfiguriert sind und die Domain sicher und einfach delegiert werden kann. Damit wird ein hoher Grad an Qualität für die Domain erzielt.

Bitte tragen Sie im Formular Ihre Domain ein. Die Angabe der Nameserver ist optional. Sind die Nameserver nicht angegeben, so werden diese automatisch aus dem DNS ermittelt. Dies ist natürlich nur bei bereits registrierten Domains möglich.

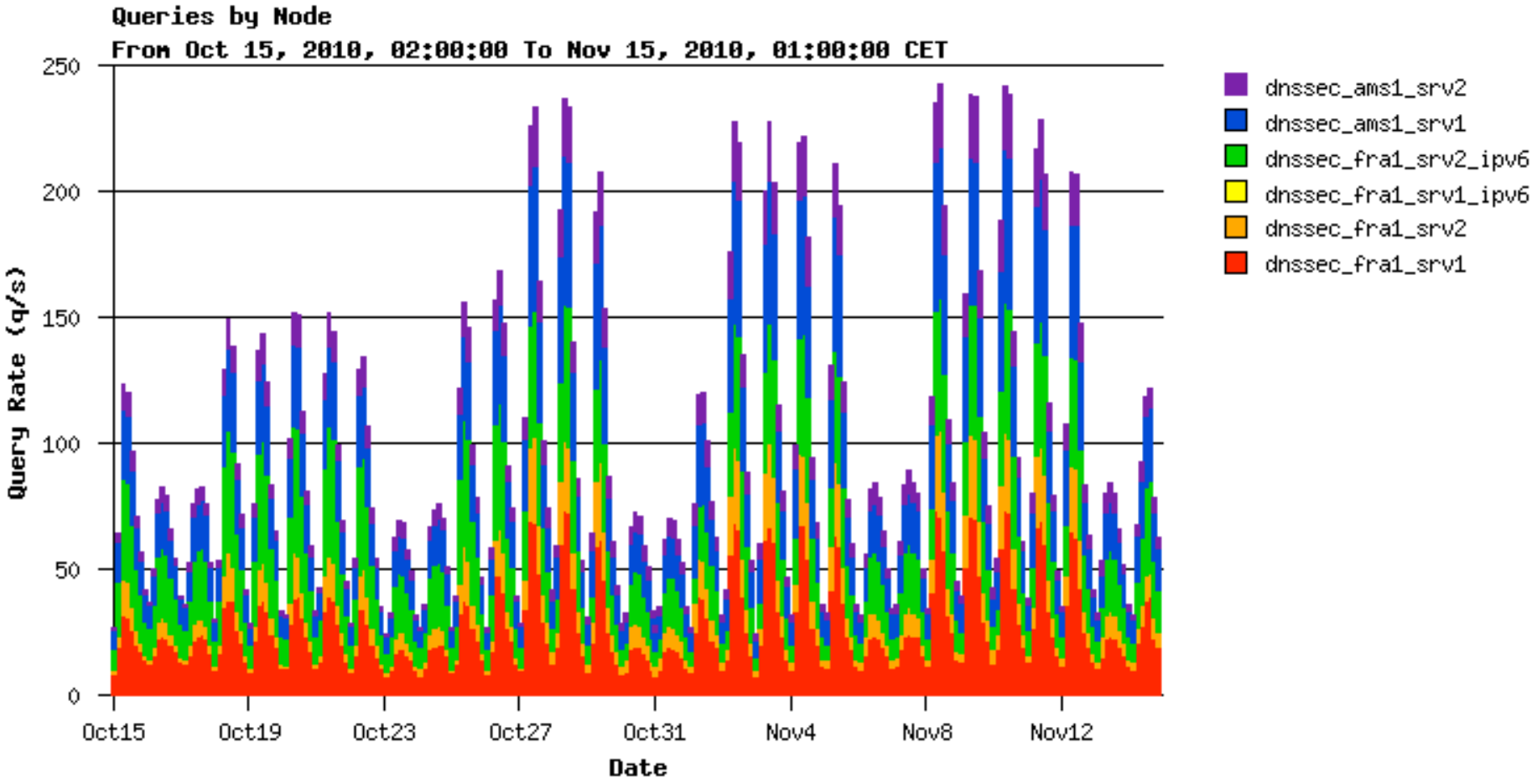
DNSSEC-Algorithmen im Testbed (2010-11-22)



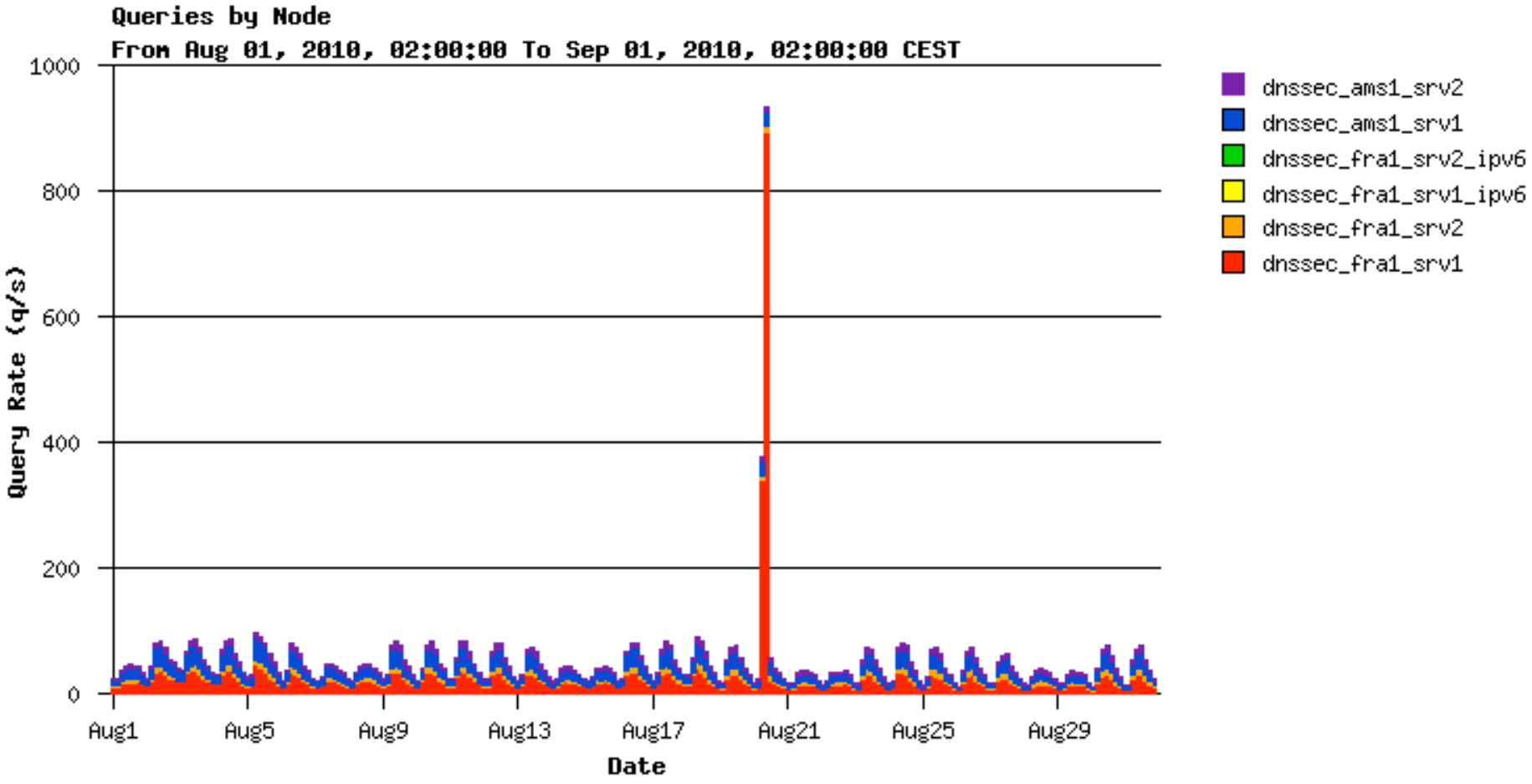
Schlüssellängen KSK im Testbed (2010-11-22)



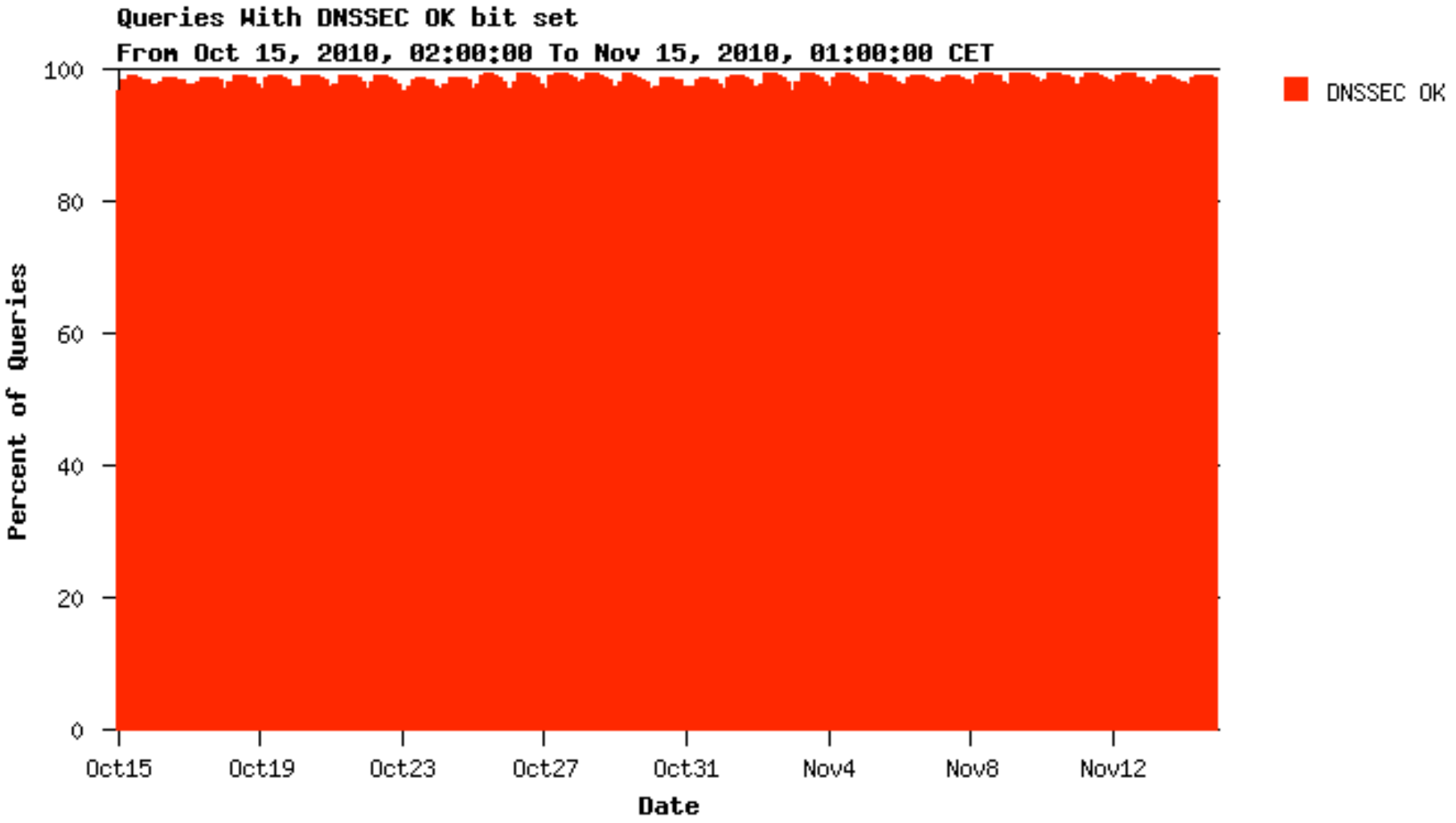
Testbed-Querys Oktober/November 2010



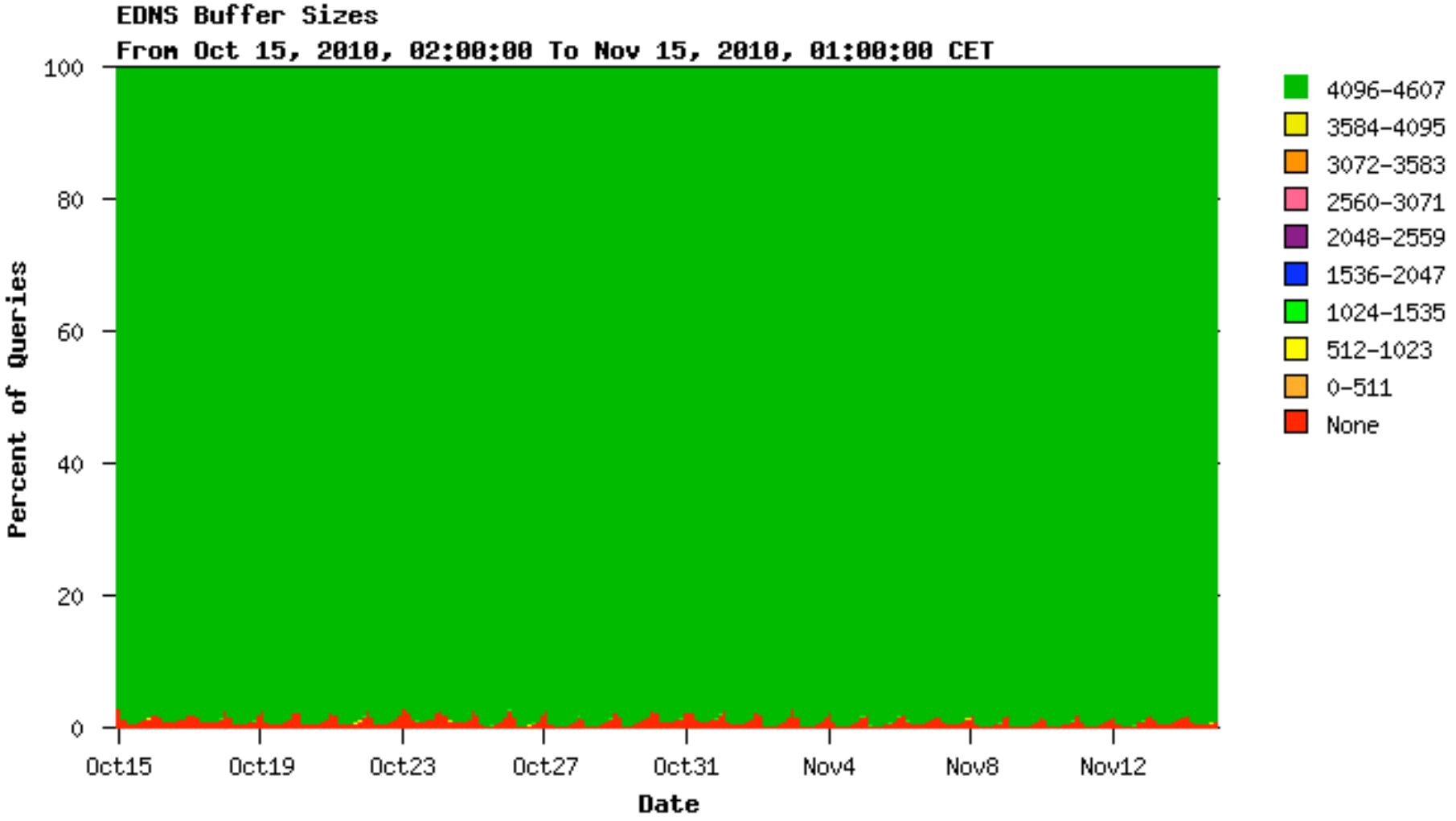
Testbed-Querys August 2010



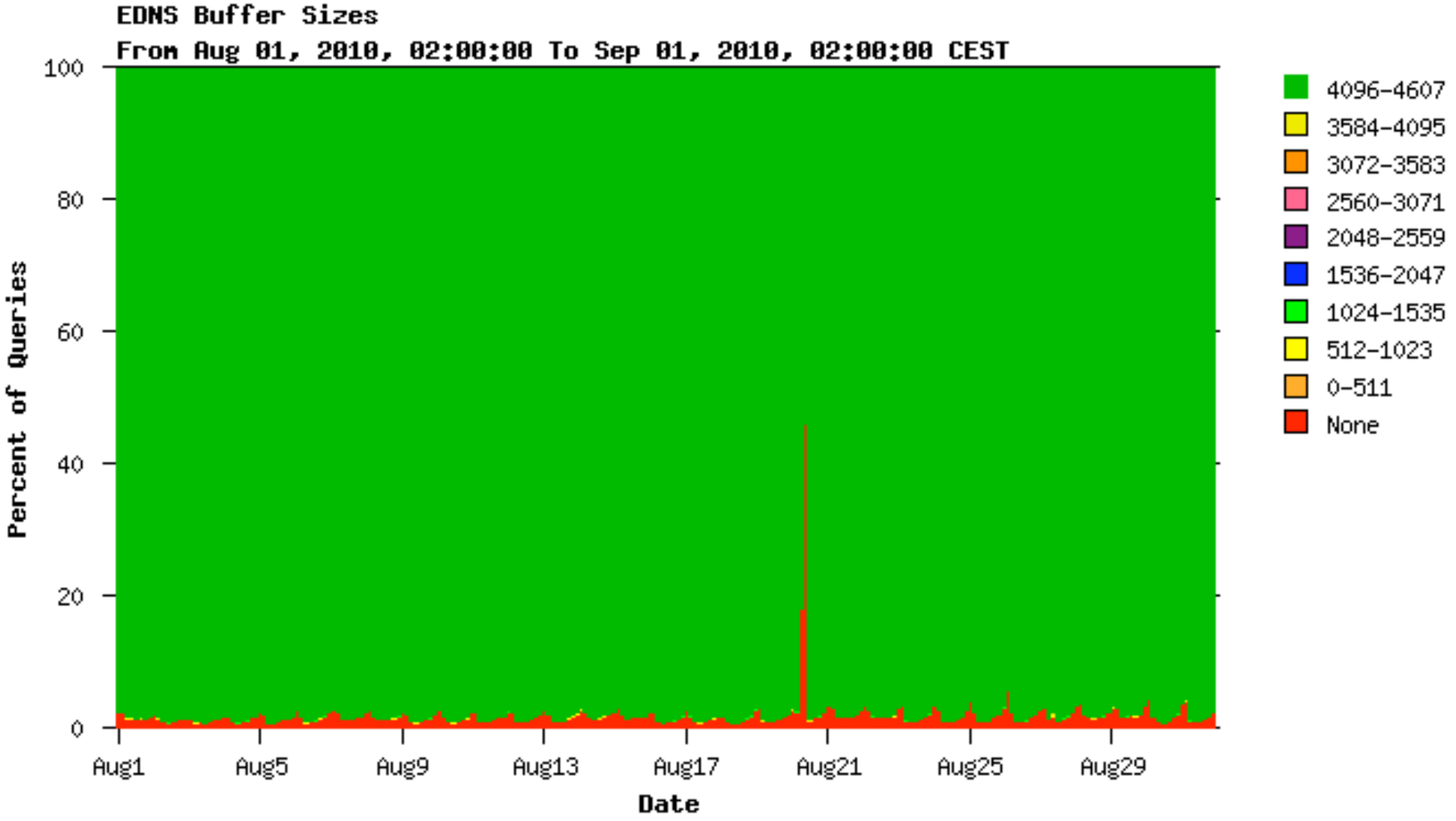
DNSSEC OK Oktober/November 2010



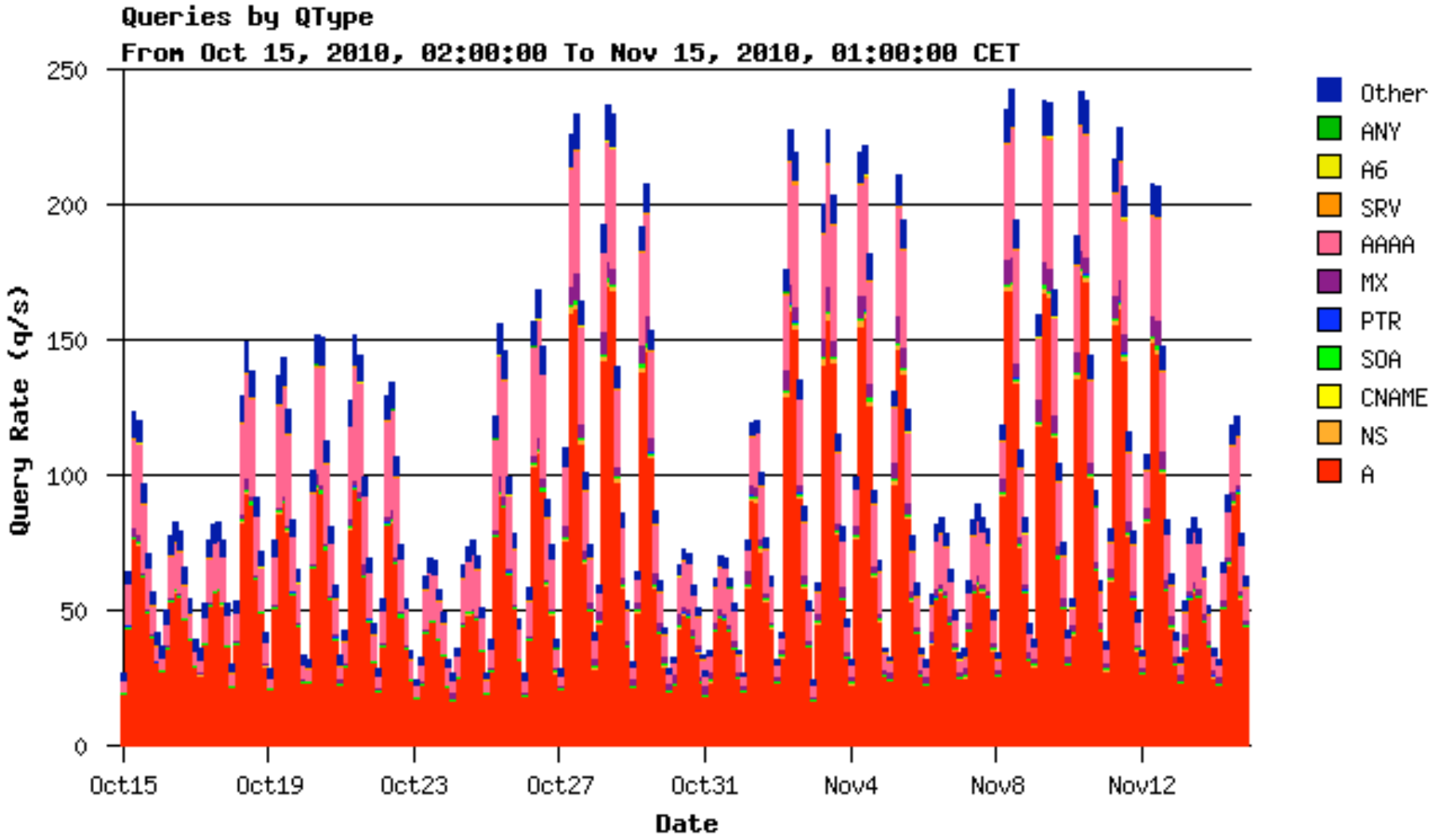
EDNS Buffer Size Oktober/November 2010



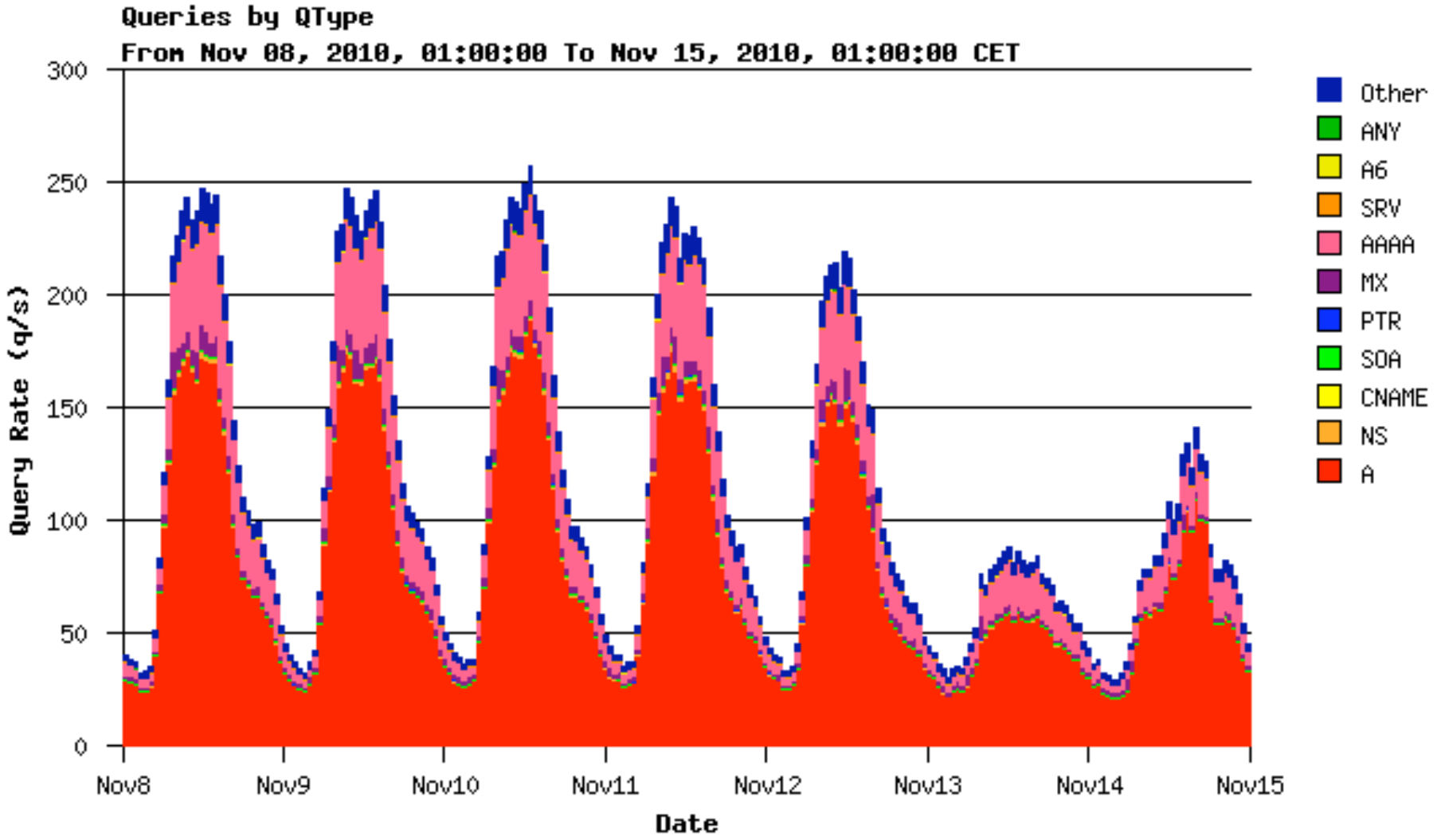
EDNS Buffer Size August 2010



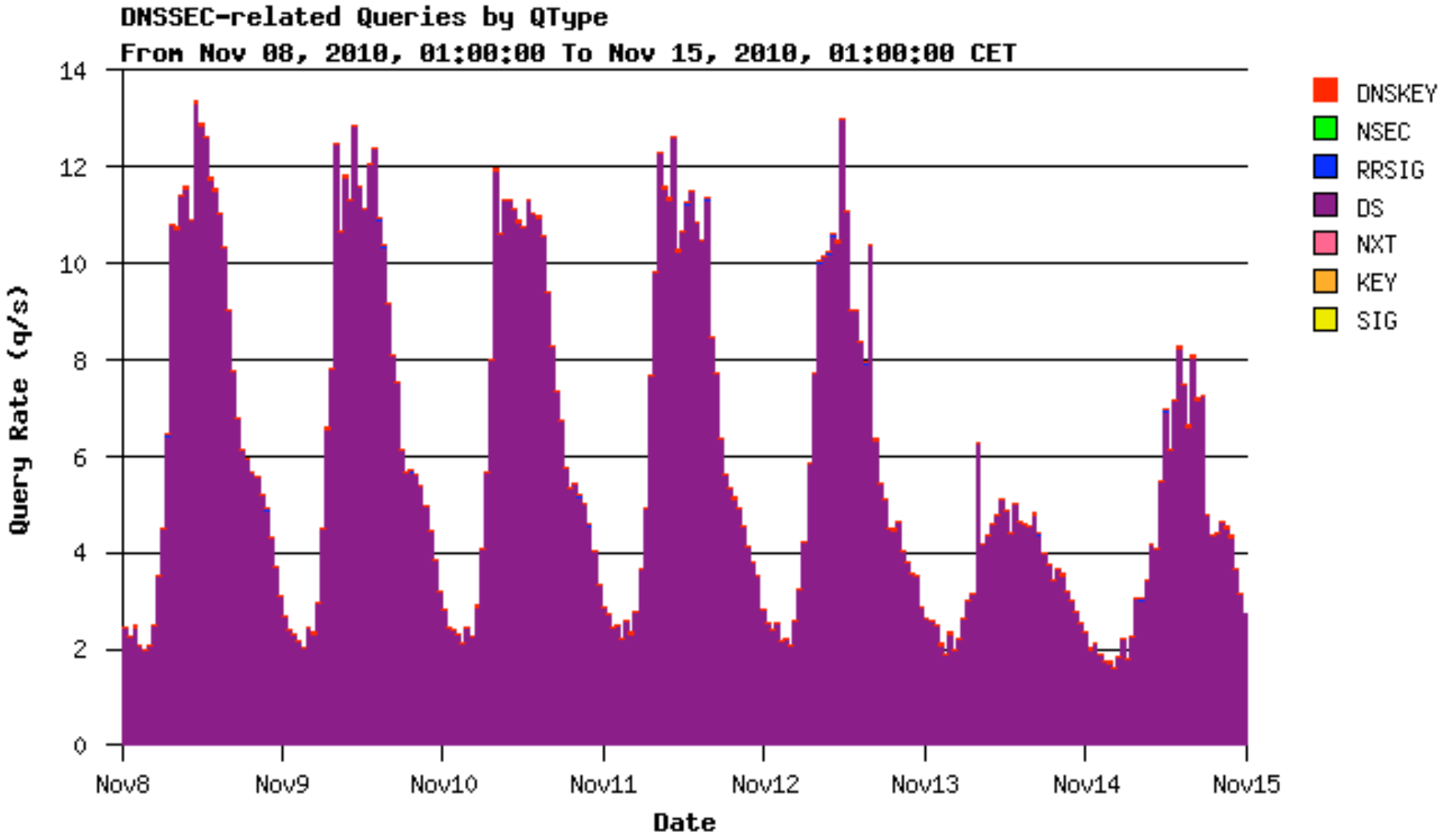
Testbed QTYPEs Oktober/November 2010



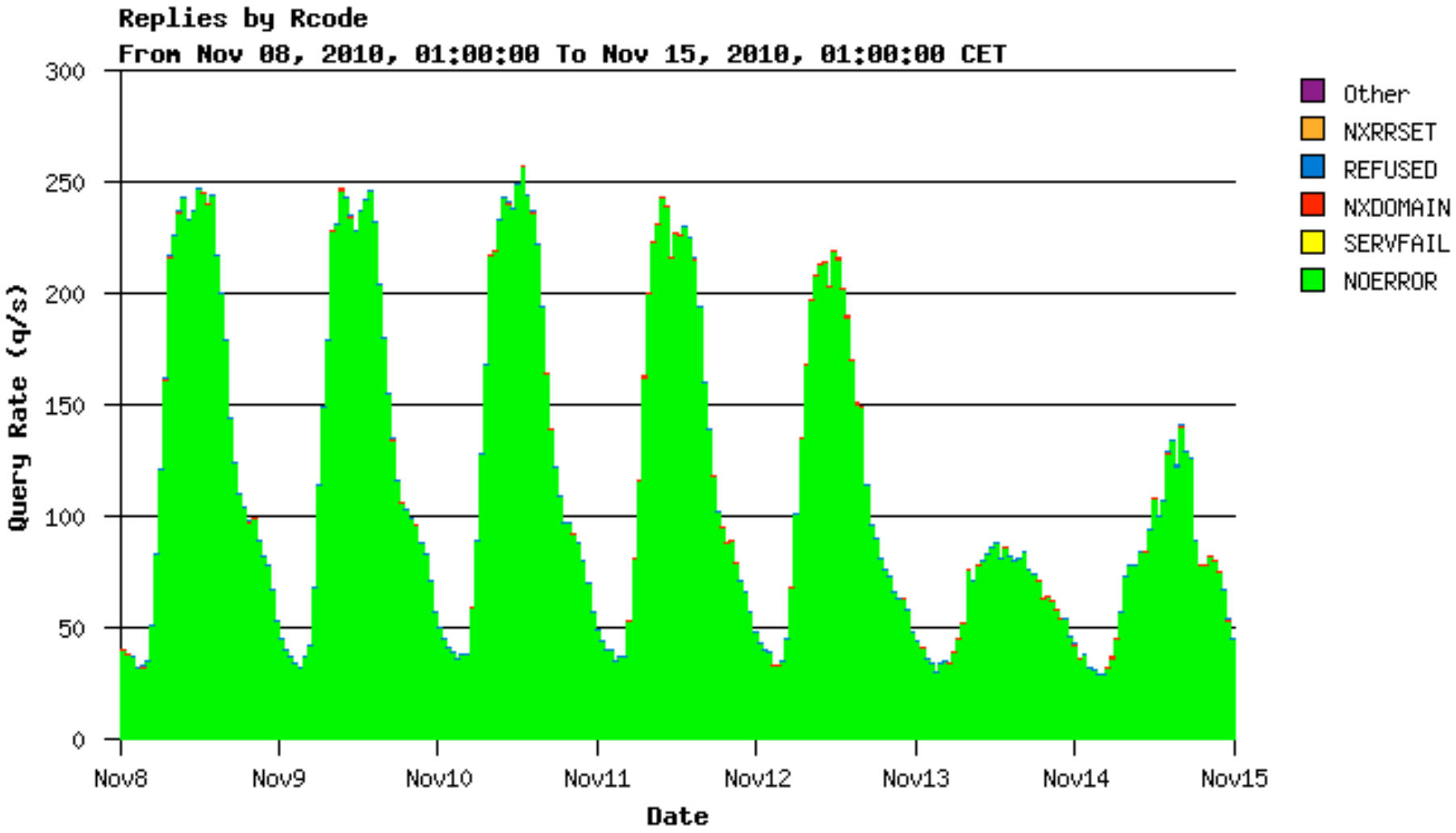
Testbed QTYPEs November 2010



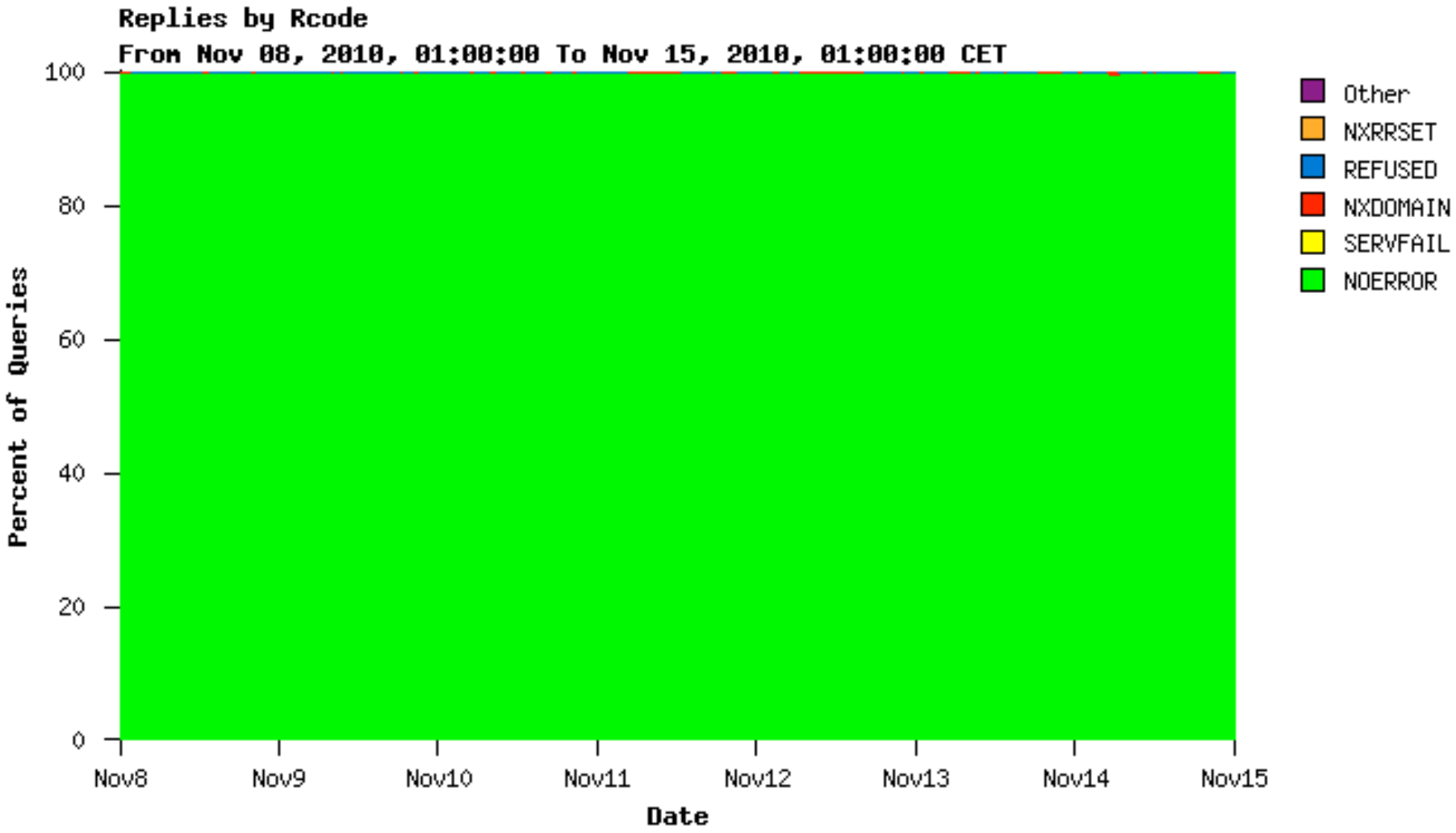
Testbed DNSSEC-QTYPEs November 2010



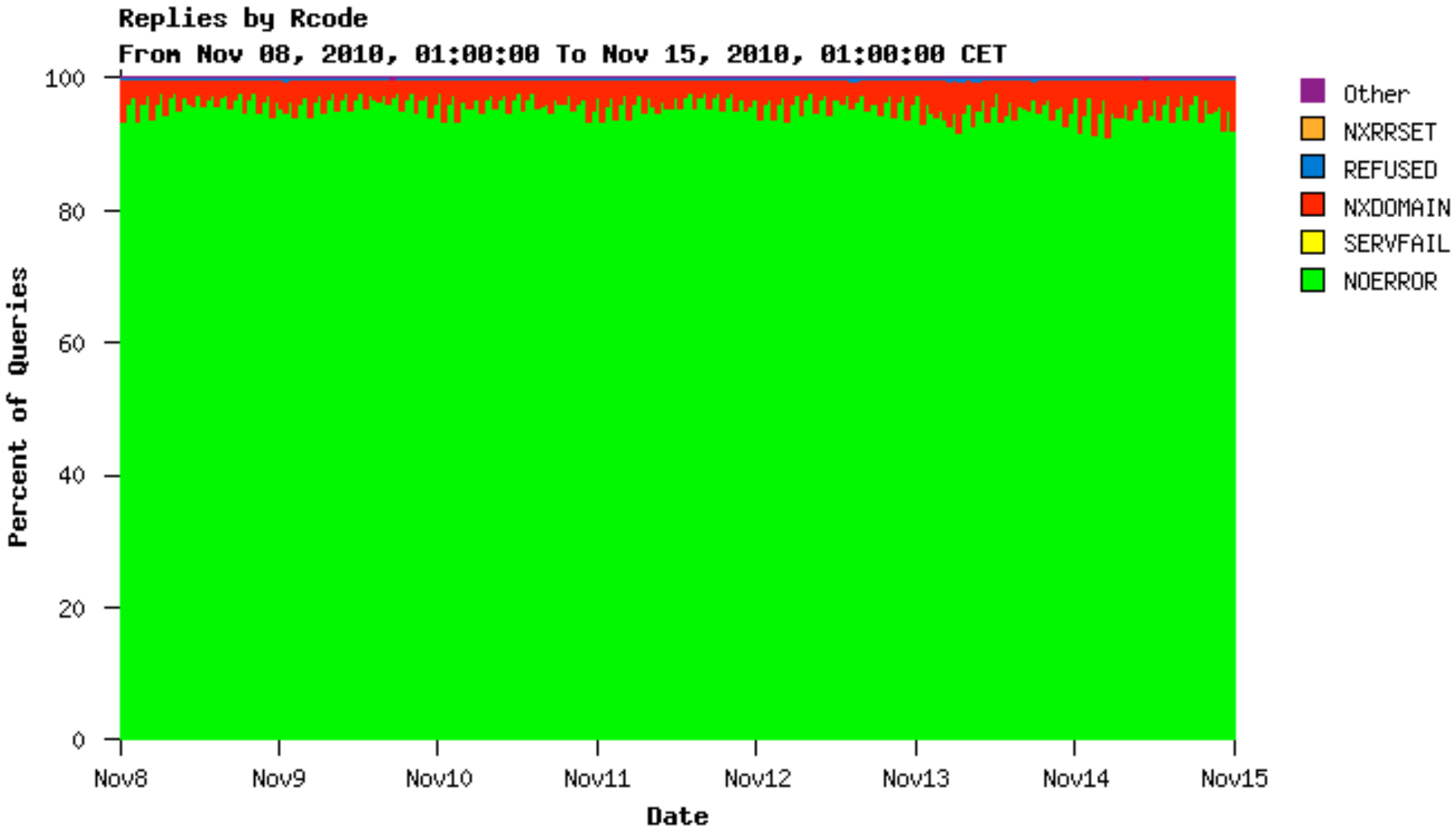
Testbed RCODEs November 2010



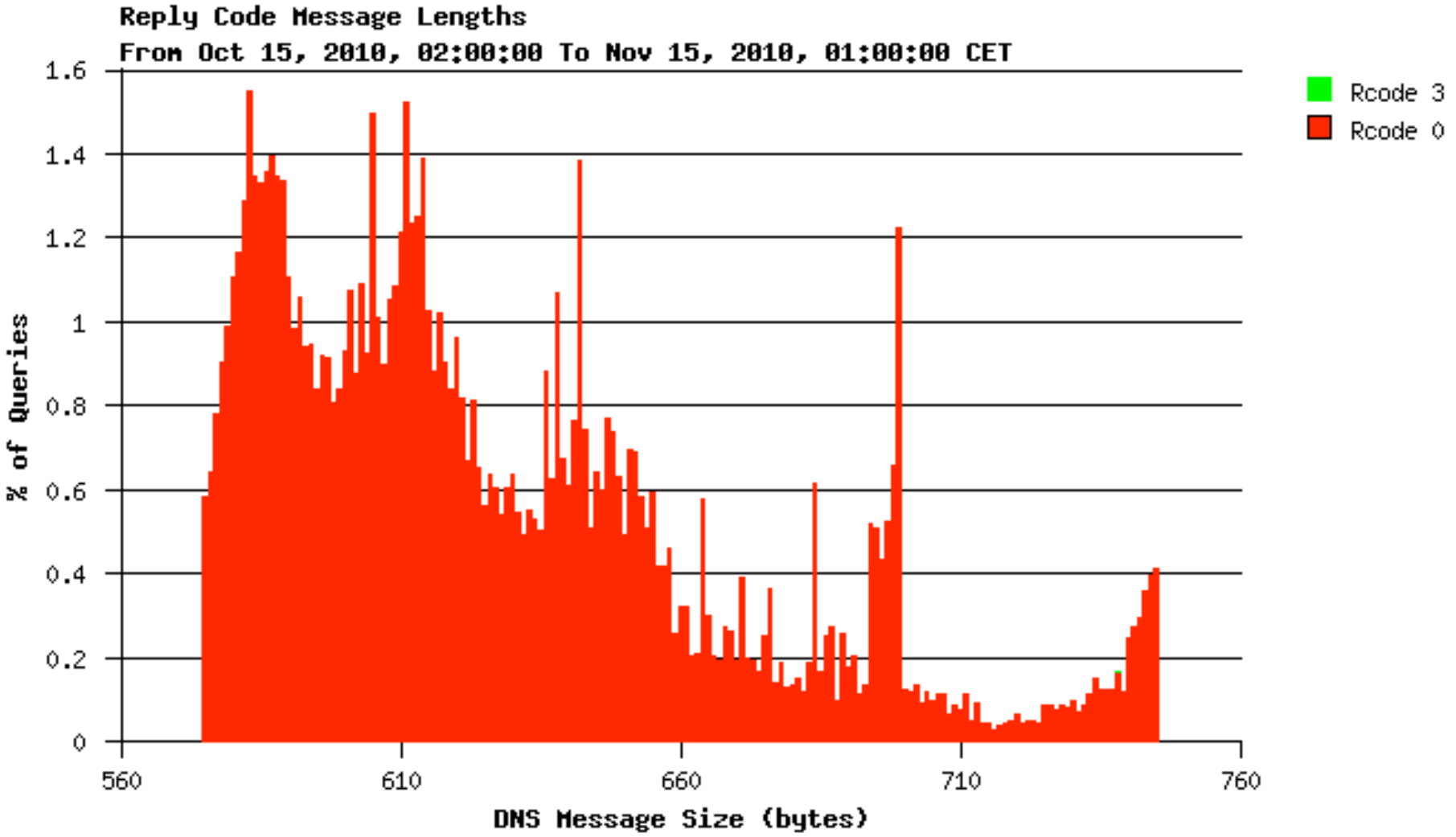
Testbed RCODEs in % November 2010



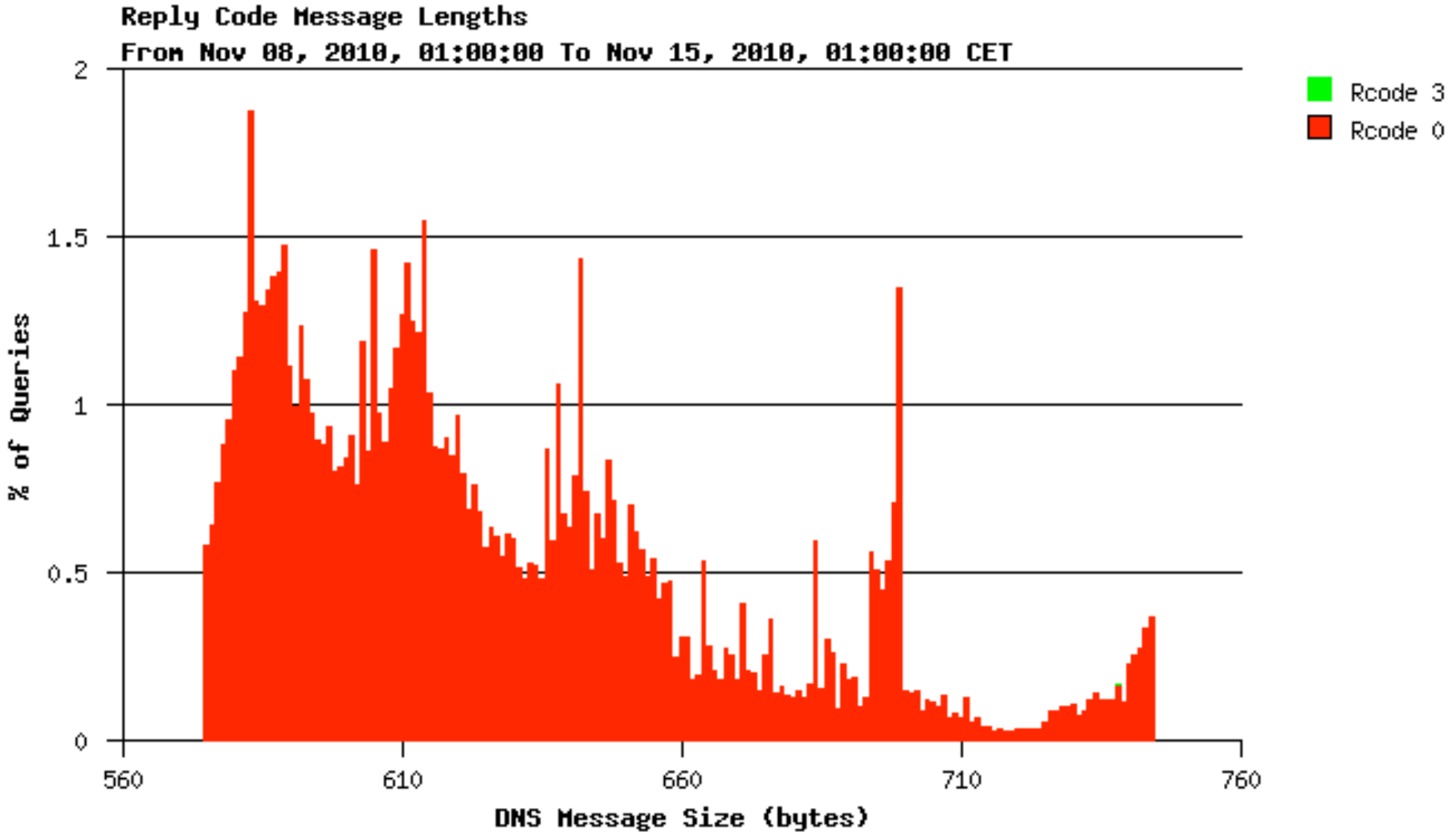
DE RCODEs in % November 2010



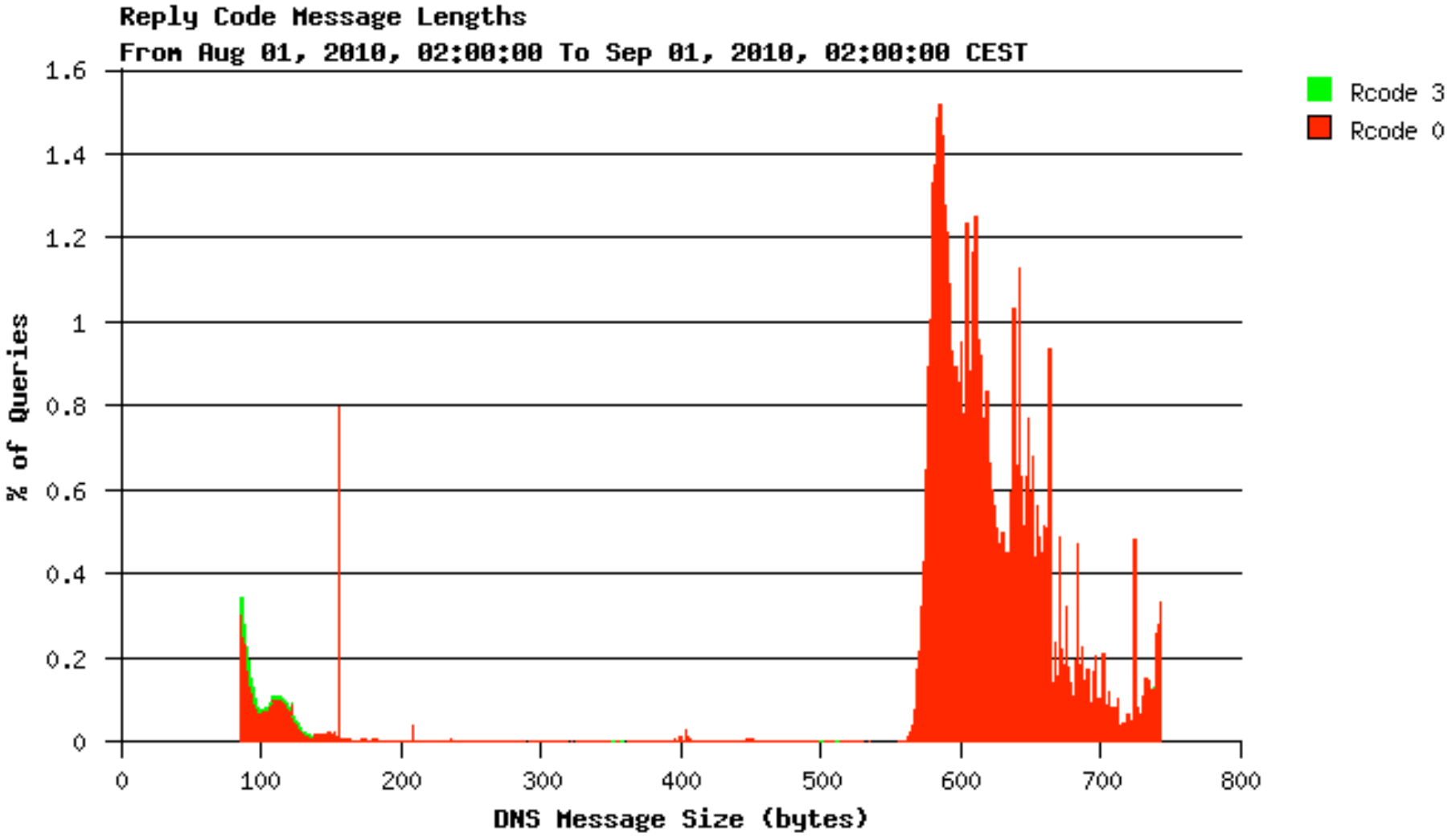
Antwortlängen Testbed Oktober/November 2010



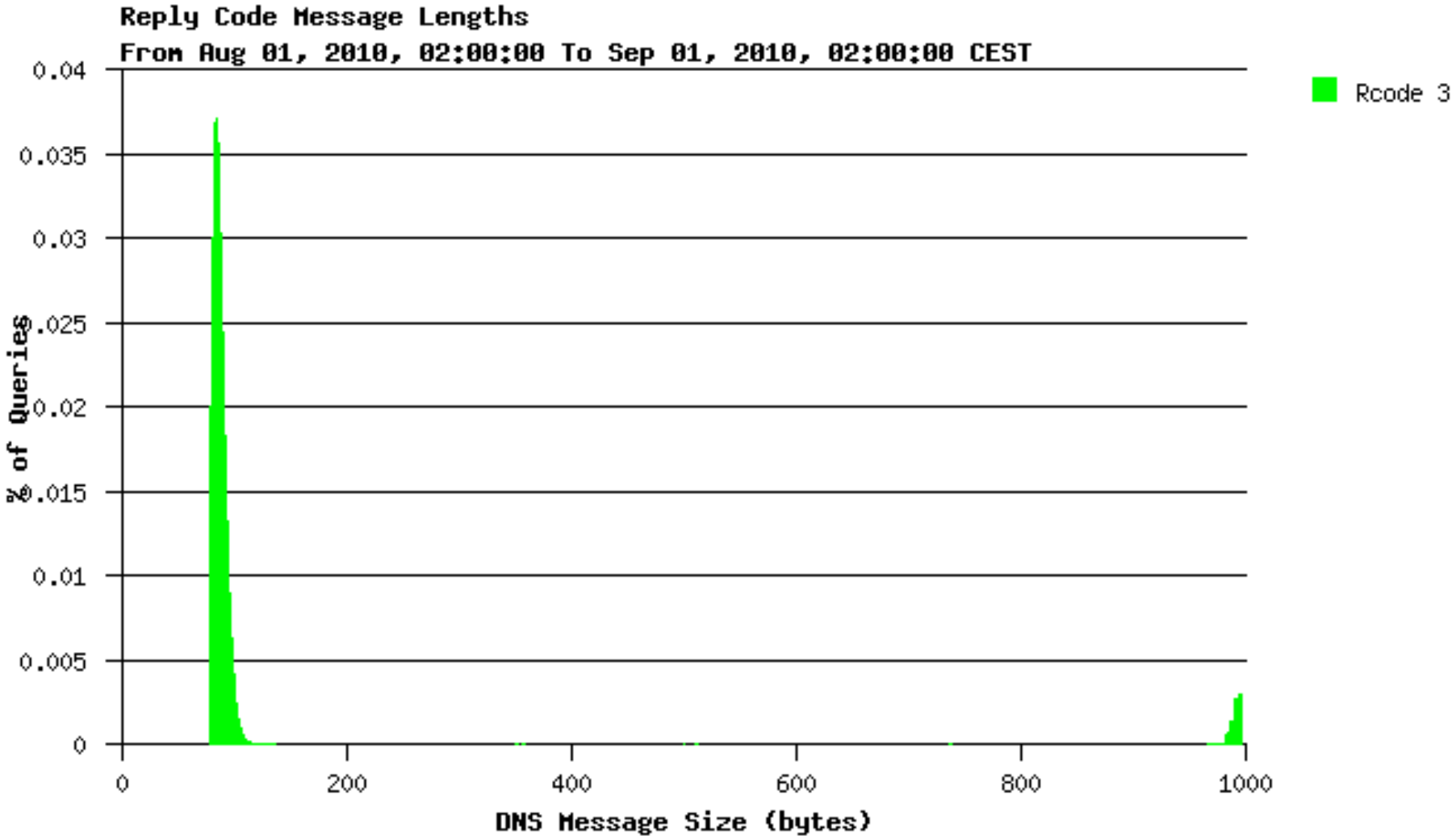
Antwortlängen Testbed November 2010



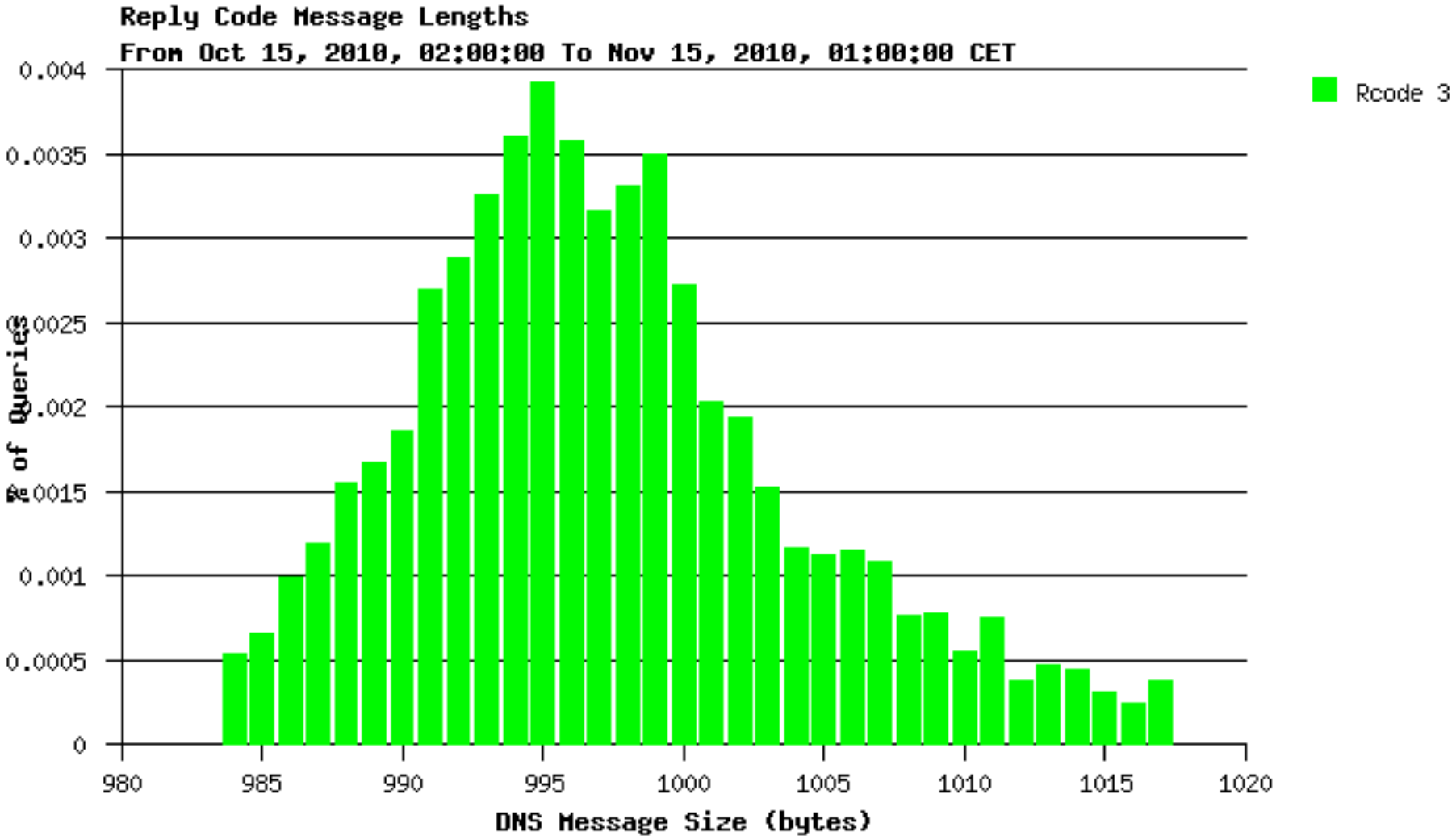
Antwortlängen Testbed August 2010



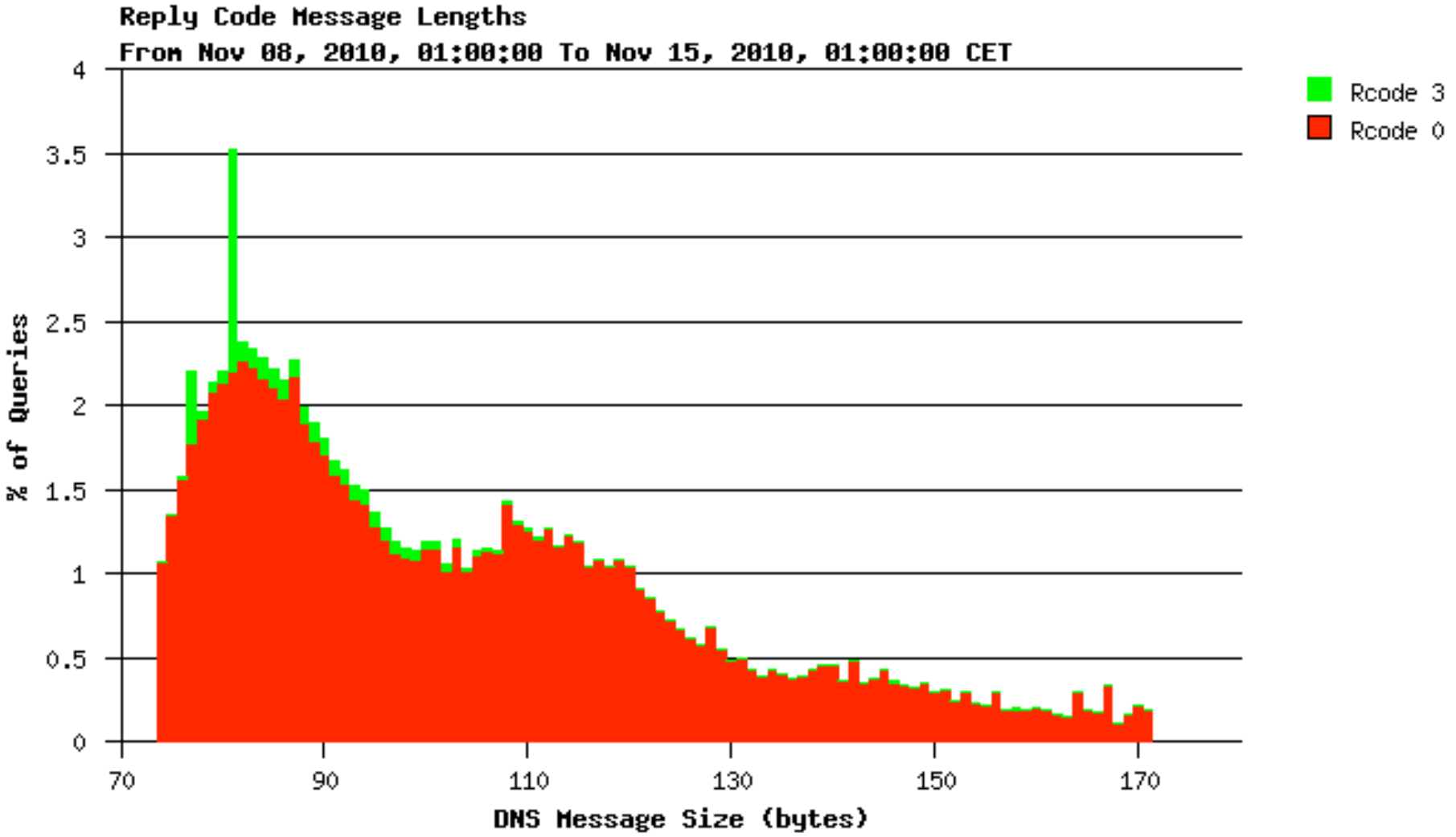
Antwortlängen NXDOMAIN Testbed August 2010



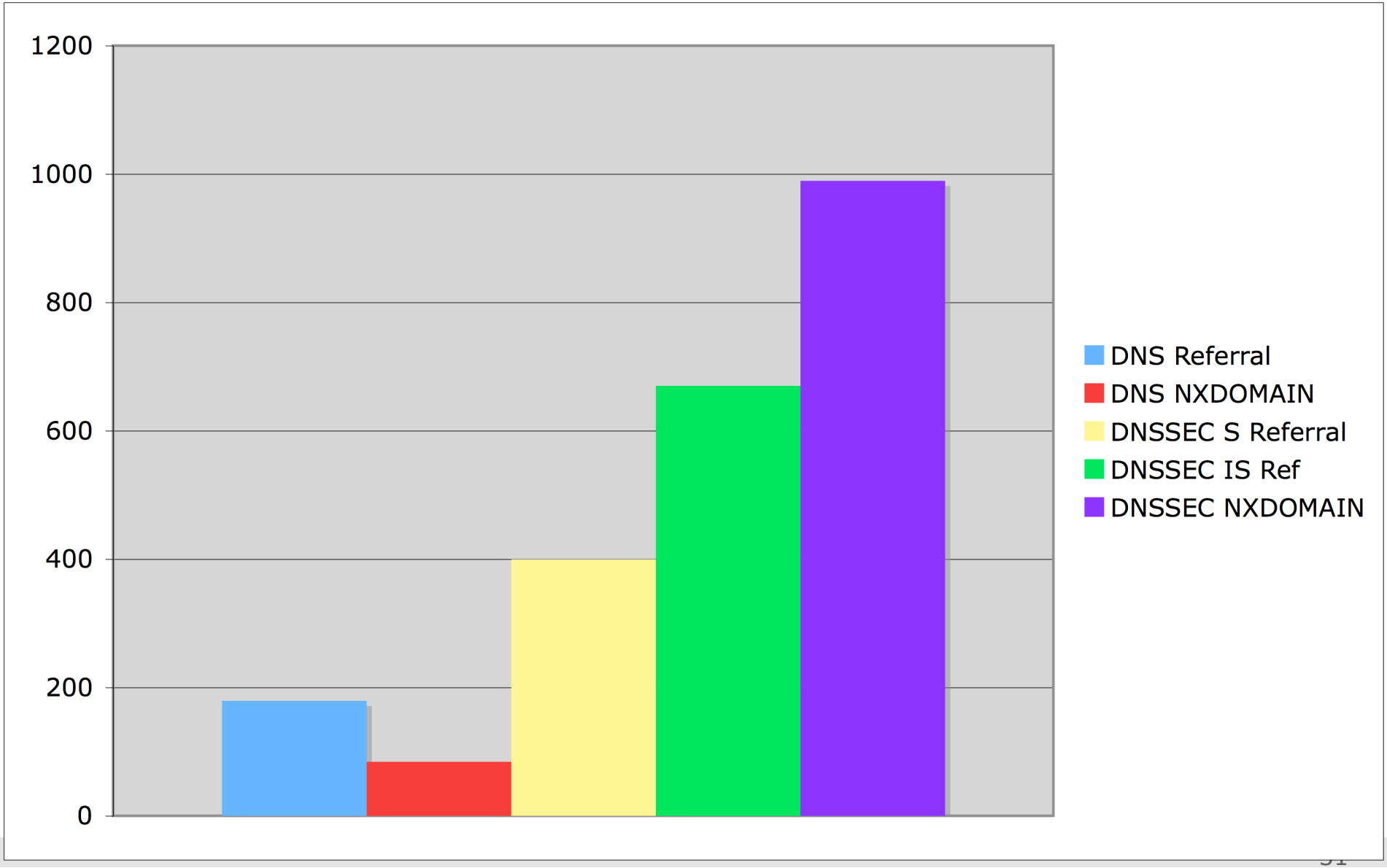
Antwortlängen NXDOMAIN Testbed Okt/Nov 2010



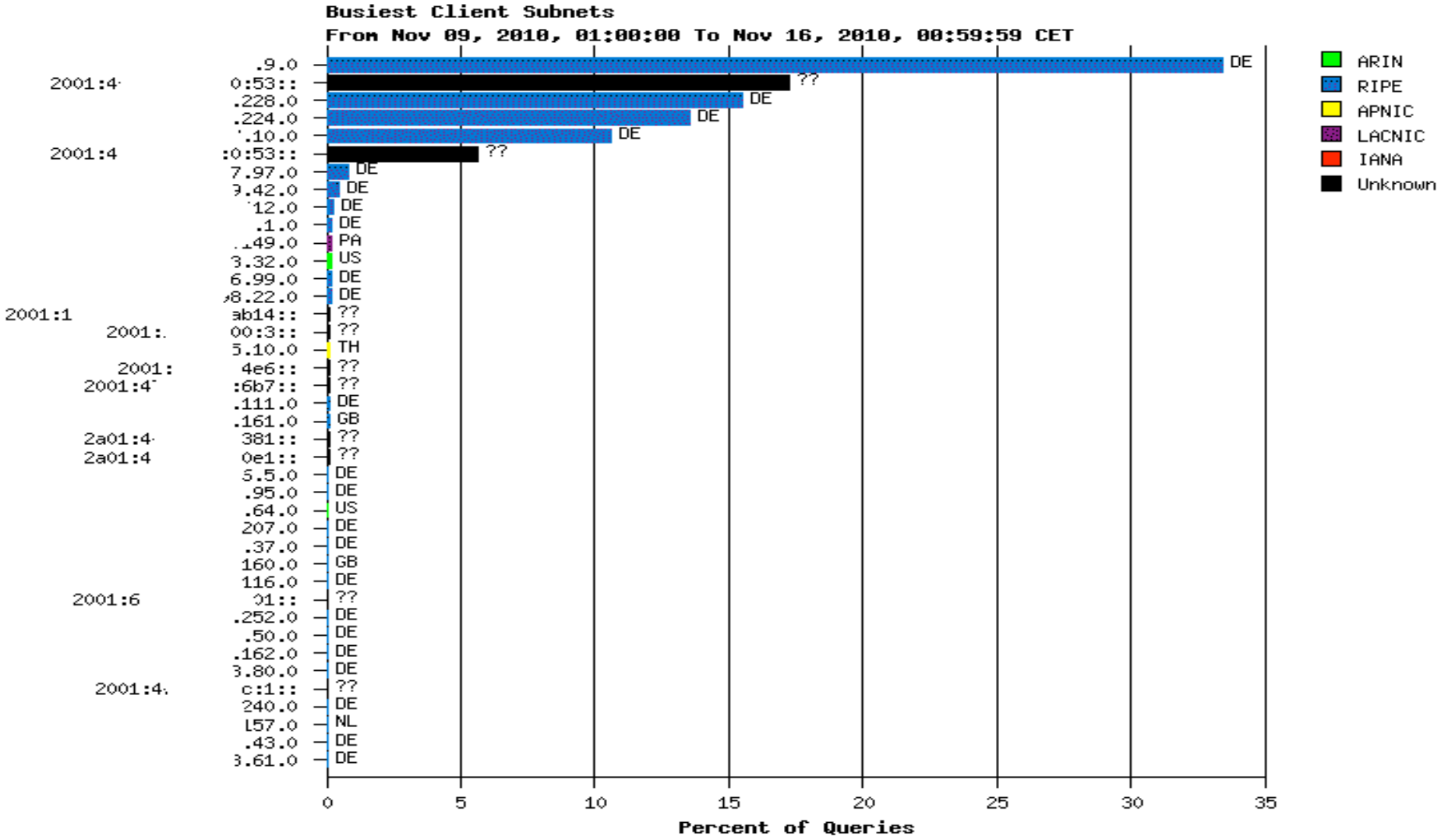
Antwortlängen DE November 2010



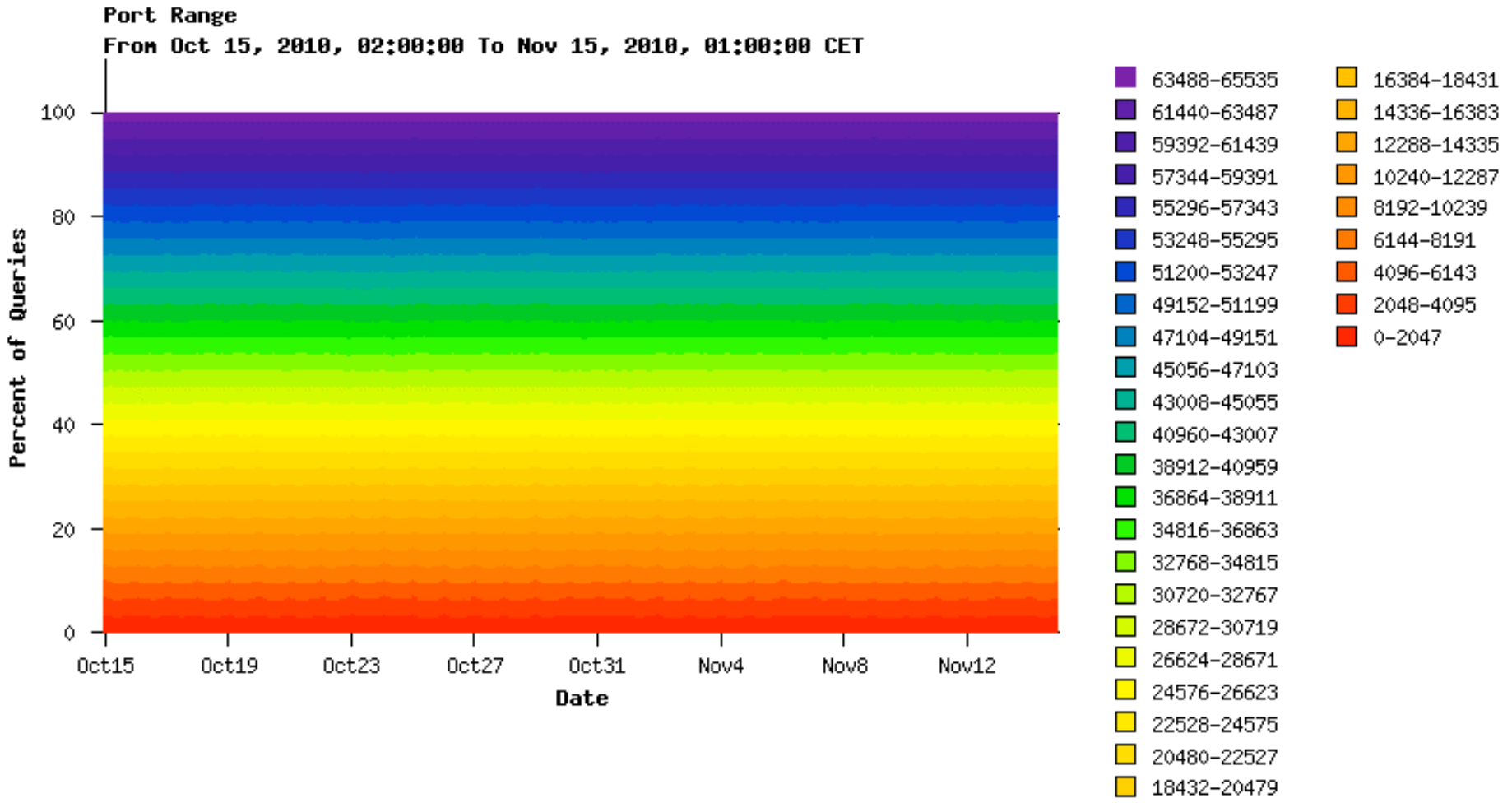
DNS-Antwortlängen



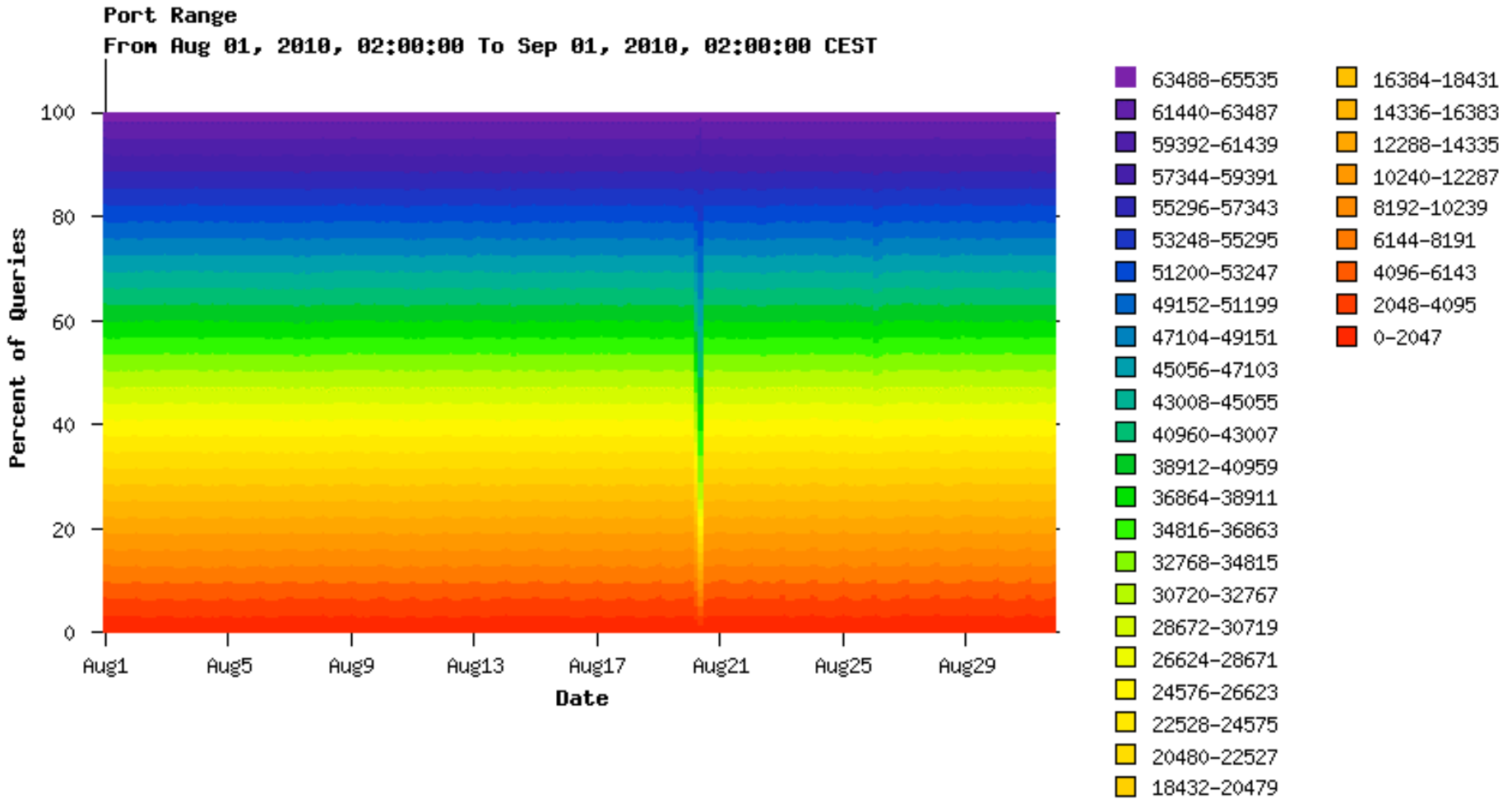
Quellen Testbed November 2010



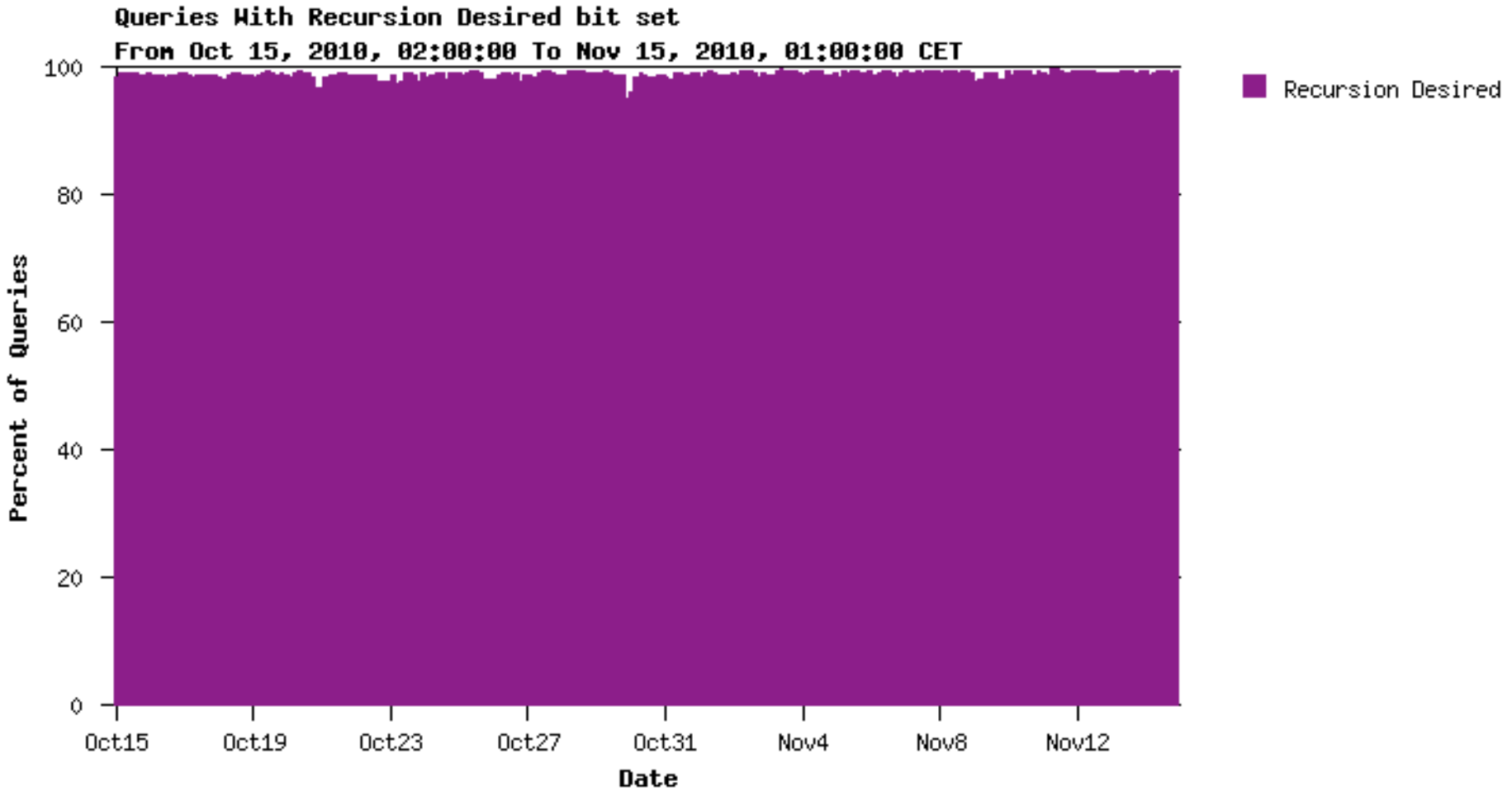
Query-Source-Ports Oktober/November 2010



Query-Source-Ports Ende August 2010



Rekursive Querys Testbed Oktober/November



BIND-Konfiguration: vorher

- Umlenkung
- aber „rekursiv“
- und unübersichtlich
- sowie wartungsintensiv
- Lösung: neues BIND-Feature

```
zone "de" {
        type forward;
        // Die Reihenfolge der beiden Adressen kann beliebig gewaehlt
        // werden
        forwarders {
                81.91.161.228;  // auth-fra.dnssec.denic.de
                87.233.175.25;  // auth-ams.dnssec.denic.de
                // IPv6 nur bei geeigneter Konnektivität aktivieren
                // 2A02:568:0:1::53;    // auth-fra.dnssec.denic.de
        };
        forward first;
};

// WICHTIG: Diese Liste muss regelmaessig gepflegt werden und
//          darf nur im Zusammenhang mit der Testbed-Infrastruktur
//          eingesetzt werden!
//          Die Markierung als "bogus" verhindert, dass die offiziellen
//          Nameserver gefragt werden.
server 194.0.0.53       { bogus yes; }; // a.nic.de
server 81.91.164.5      { bogus yes; }; // f.nic.de
server 77.67.63.105     { bogus yes; }; // l.de.net
server 195.243.137.26   { bogus yes; }; // s.de.net
server 194.246.96.1     { bogus yes; }; // z.nic.de

server 2001:678:2::53   { bogus yes; }; // a.nic.de
server 2001:608:6:6::10 { bogus yes; }; // f.nic.de
server 2001:668:1f:11::105      { bogus yes; }; // l.de.net
```

BIND-Konfiguration: neu, mit Patch

```
zone de {
        type static-stub;
        server-addresses { 87.233.175.25; 81.91.161.228; };
        // server-names {};
};
```

- Neuer Zonentyp `static-stub`
- Fragen nicht mehr „rekursiv“
- **Feature verfügbar als Patch gegen BIND 9.7.1-P2**
- **Integration in BIND 9 angestrebt**
- Auch für „split DNS“-Konfigurationen interessant

Nächste Schritte

- Härtung der Prozesse (Redundanz, Key-Backup)
- Abarbeitung Testplan
- weitere Verbesserung der Zonenaktualität
- Auswertung der Daten für eine GoLive-Planung

Nächste Schritte: Testplan (Auszug)

- Provider-/Operatorwechsel unter DNSSEC
- Betrieb eines validierenden Resolovers
- NSEC3-Salt-Wechsel
- DE-SLD-KSK-Rollover
  - Massen-Rollover, Timing, Nachricht Zonenverteilung
- DNSSEC-Health

Vielen Dank!

<http://www.denic.de/dnssec>