Changes to JP DNS traffic by DNSSEC

-- from DSC of a.dns.jp --

Masato Minda <minmin@jprs.co.jp>

Japan Registry Services Co., Ltd. (JPRS)

RIPE 62 dns-wg @ Amsterdam

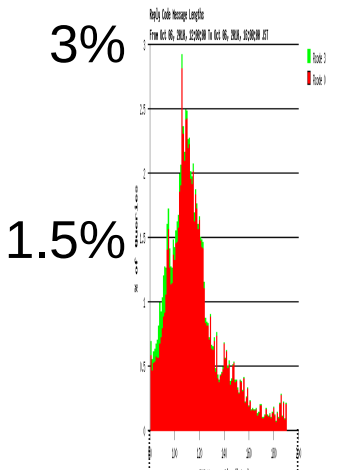
DNSSEC in JP

- JP started the DNSSEC service at 2011-01-16.
  - Registrants can use the DNSSEC now.
- Event dates before service start
  - **2010-10-17** Start signing of JP zone with NSEC3 Opt-out
  - **2010-10-29** First ZSK for roll over was pre-published
  - 2010-11-03 JP did first ZSK roll over
  - 2010-12-10 DS was registered in Root zone

  ⇒ About implementation of DNSSEC in JP was talked at 24th CENTR Technical workshop. https://www.centr.org/main/meetings/6093-CTR.html

DNS response size distribution

Before DNSSEC



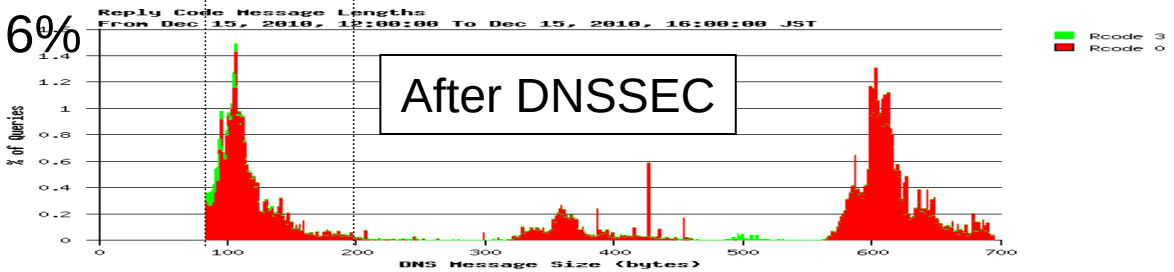
3%

1.5%

80 200

- Before DNSSEC sign
  - 2010-10-06 12:00-16:00 at a.dns.jp
  - Traffic peak is around 110 octets
- After DNSSEC sign
  - 2010-12-15 12:00-16:00 at a.dns.jp
  - Three traffic peaks around 110, 360 and 610 octets

1.6%

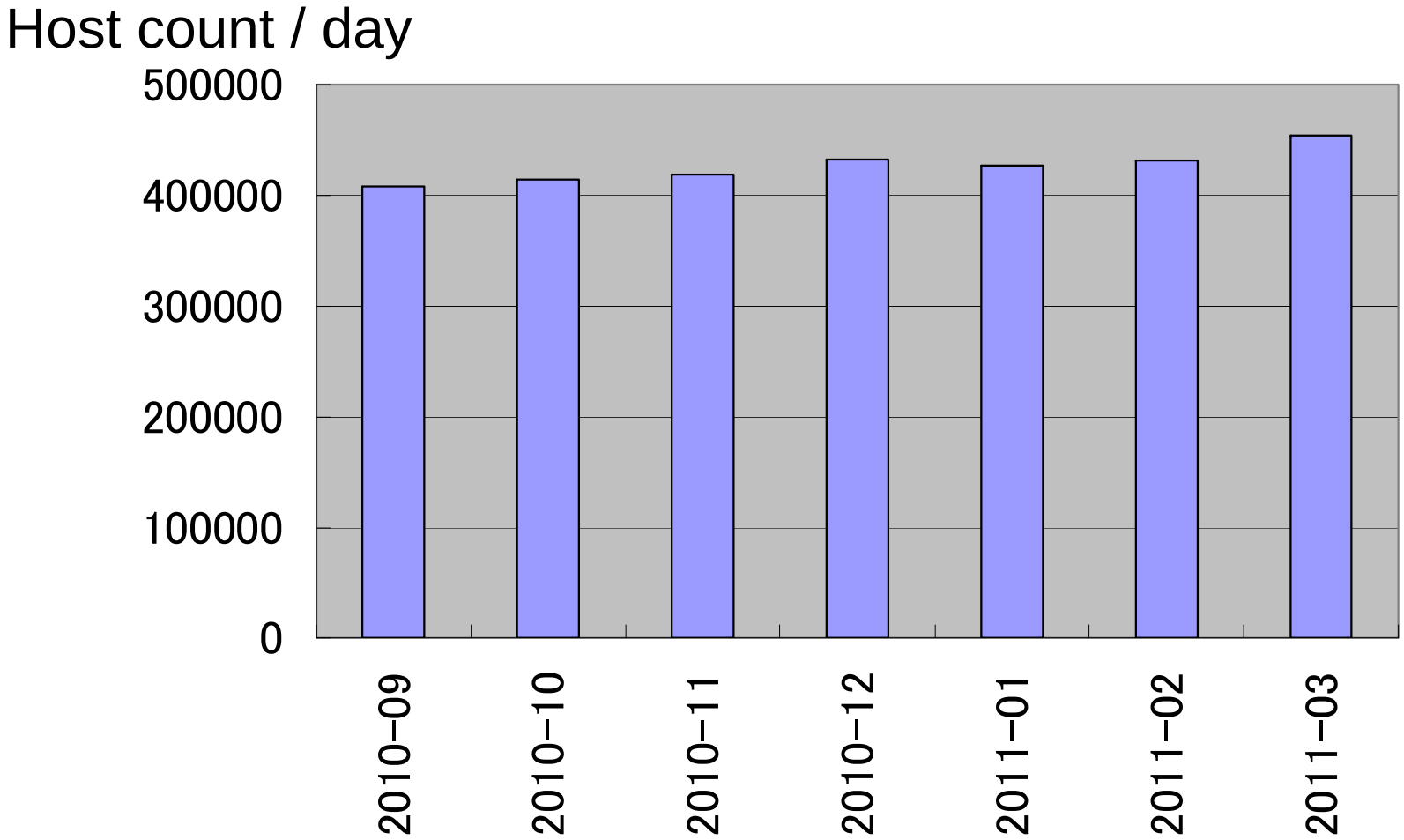


0 200 400 600

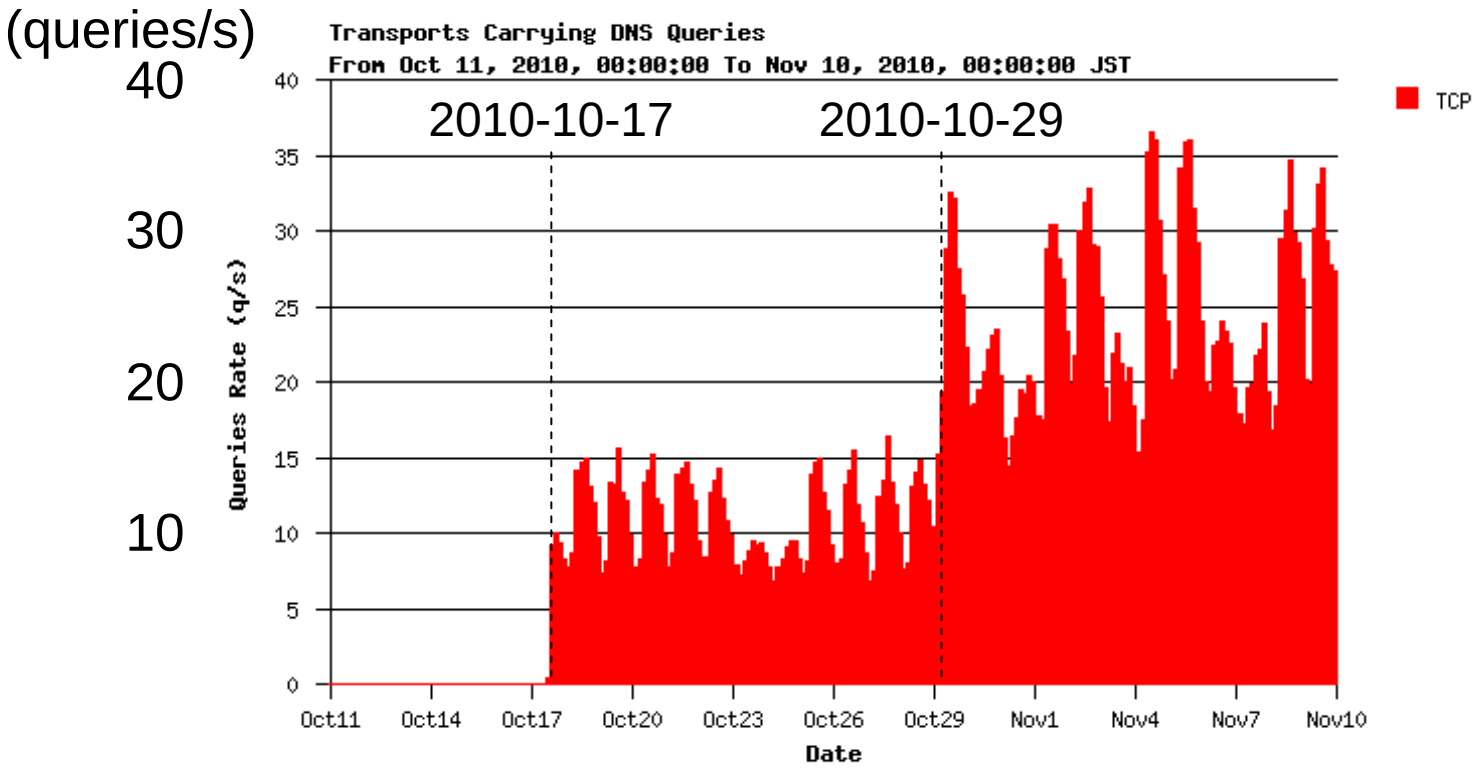
Considerations around the peaks

- The peak around 110 octets
  - These are answers to query without the DO-bit. Its implementation is old resolver (before BIND 9.3) or Nominum CNS.
- The peaks around 360 or 610
  - These are answers to query with DO-bit. Its implementation has DNSSEC capability.
  - The peak around 360 has 1 NSEC3 RR.
  - The peak around 610 has 2 NSEC3 RRs.

Number of DNSSEC Ready Resolvers (unique host count with DO-bit. at a.dns.jp)



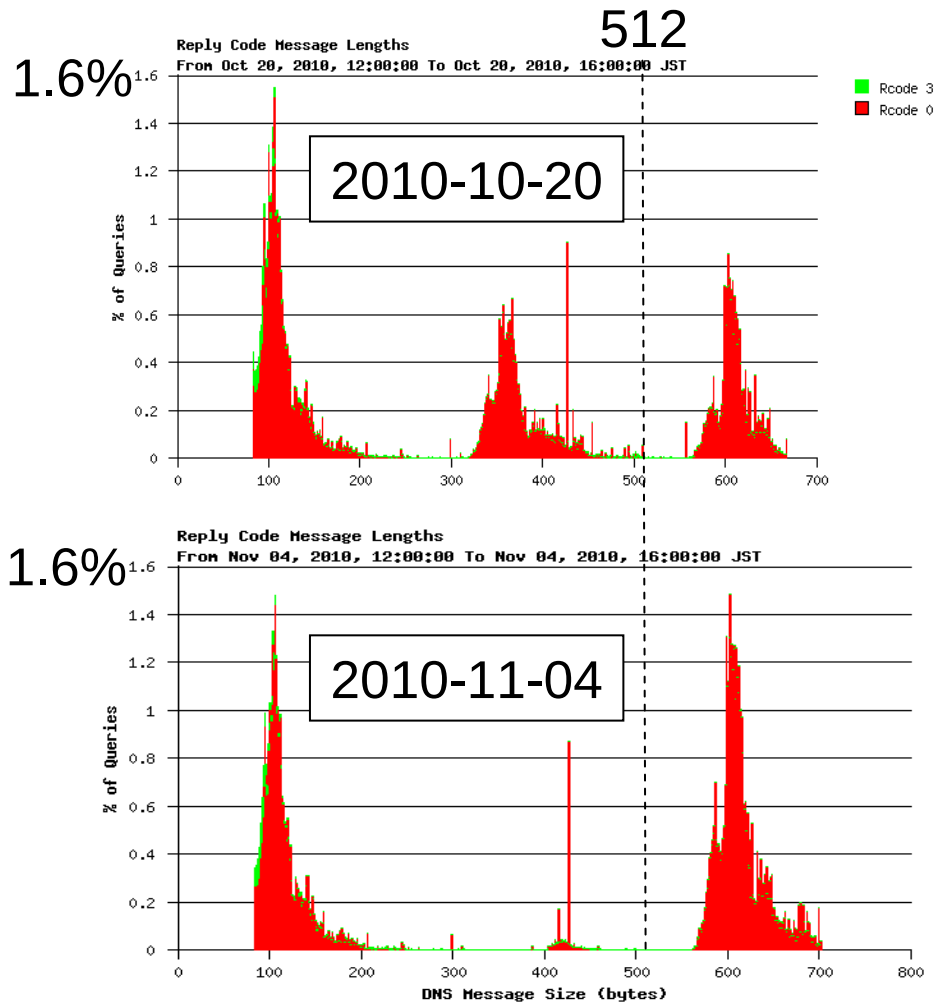
Number of TCP queries



- From 2010-10-11 to 11-10 at a.dns.jp
- TCP queries increased by JP zone signing at 2010-10-17, and then, increased by ZSK pre-publishing at 2010-10-29

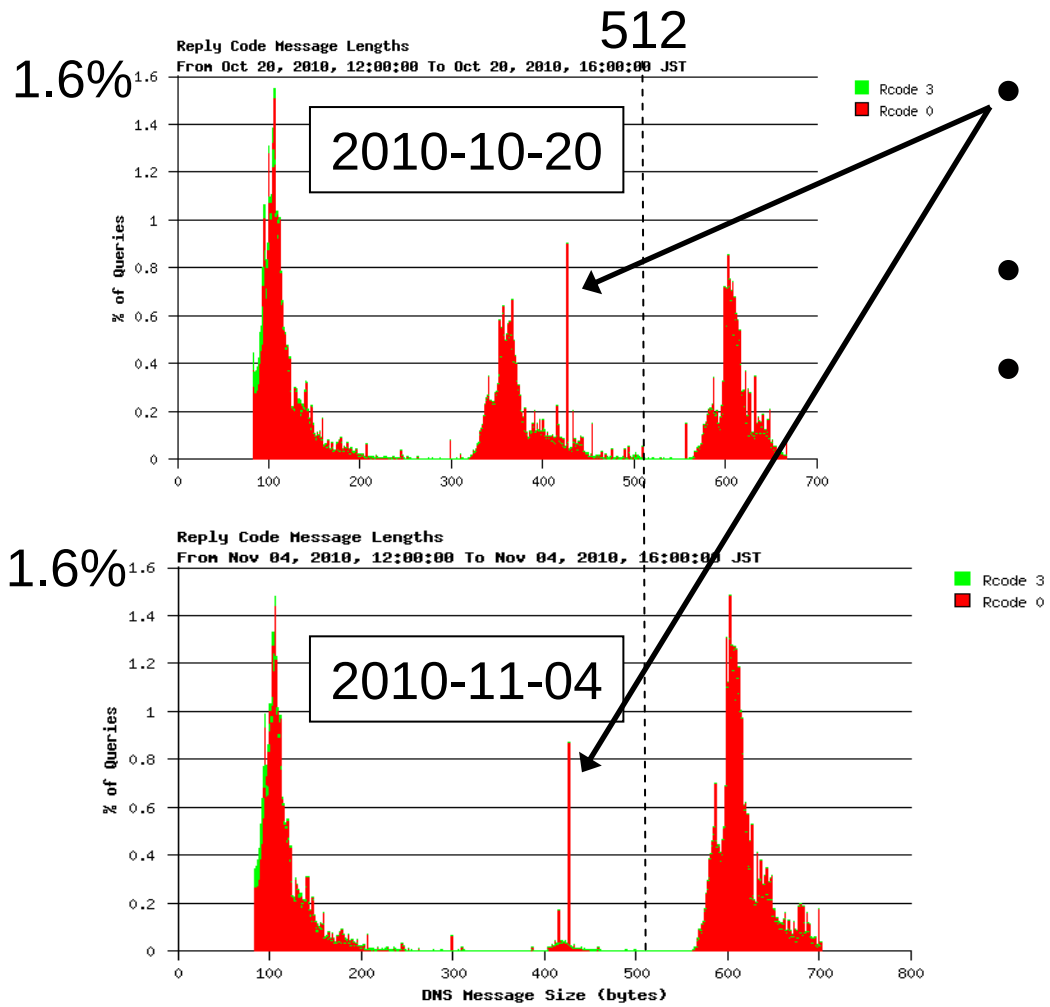
Number of TCP queries

Differences of around 2010-10-29



- After 2010-10-29;
  A peak around 360 octets decreased significantly .
  - This is caused by the changes of NSEC3's parameter.
- TCP queries are increasing according to widen of packet size distribution.
  - There are not a few environments which have the 512 octets limitation in UDP with DNS.

What is this spike?



- There is the spike at about 430 octets.
- Its real value is 427.
- It is an answer to query with EDNS0 of the IP address of JP's NS.

ex.)

```
$ dig +dnssec +norec @a.dns.jp a.dns.jp a
```

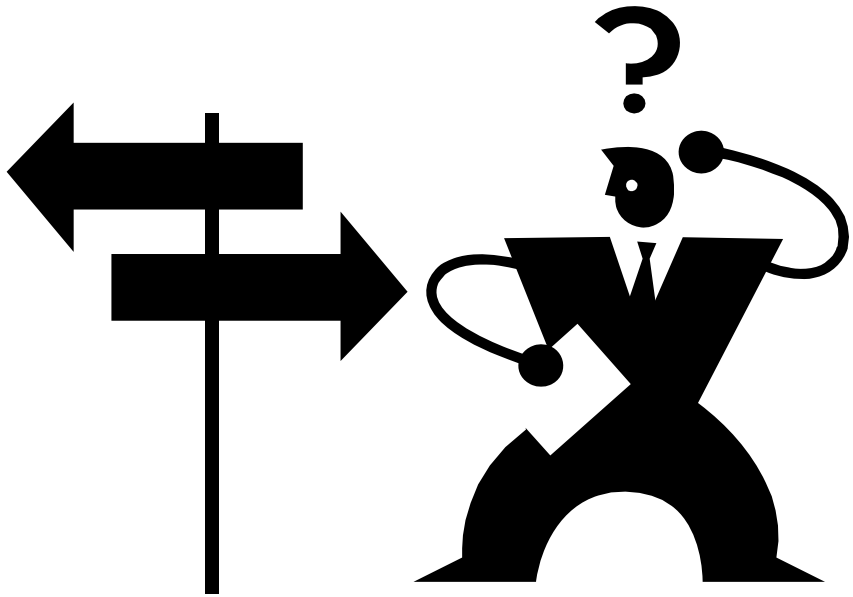
Response Size of DNSKEY

- Present response size of DNSKEY at .JP

```
$ dig +dnssec jp dnskey | grep SIZE
;; MSG SIZE  rcvd: 1203
```

  - DNSKEY has 3 ZSKs, 1 KSK, 1 RRSIG by ZSK, and 1 RRSIG by KSK.
  - JP will use the double signing KSK roll over. But in this setting, the DNS response size will be 1769 octets.
  - 1769 is too big for traditional MTU.
- JP will decrease the response size of DNSKEY.
  - Target date is end of 2011-06.
  - Remove the RRSIG by ZSK for DNSKEY
  - Decrease the ZSK of DNSKEY

Q and A



E-mail: <*techplan-contact* at *jprs* dot *co* dot *jp*>