DS TTL shortening experience in .JP

DNSSEC Workshop @ ICANN48

20 Nov 2013

Yoshiro YONEYA <yoshiro.yoneya@jprs.co.jp>

Background

- One of the biggest concern with registrants and ISPs deploying DNSSEC
  - DNS name resolution will fail if DNSSEC operation was failed
  - Especially, mismatch of DS in parent zone with DNSKEY in child zone requires urgent recovery between parent and child zone administrators (typically, registrant ←→ registrar ←→ registry)
  - Even though urgent recovery has done, the influence will remain until DS cache in validators being expired
  - Registrants and ISPs want to shorten this duration

Possible counter measures

1. Flush failed domain’s cache in validators
   - Ad hoc solution
   - Hard to reach each validators’ operators
   - Almost impossible
2. Shorten DS TTL in parent zone
   - Effective solution
   - Moderate value is not widely shared yet
   - Possible

Measurement in .JP

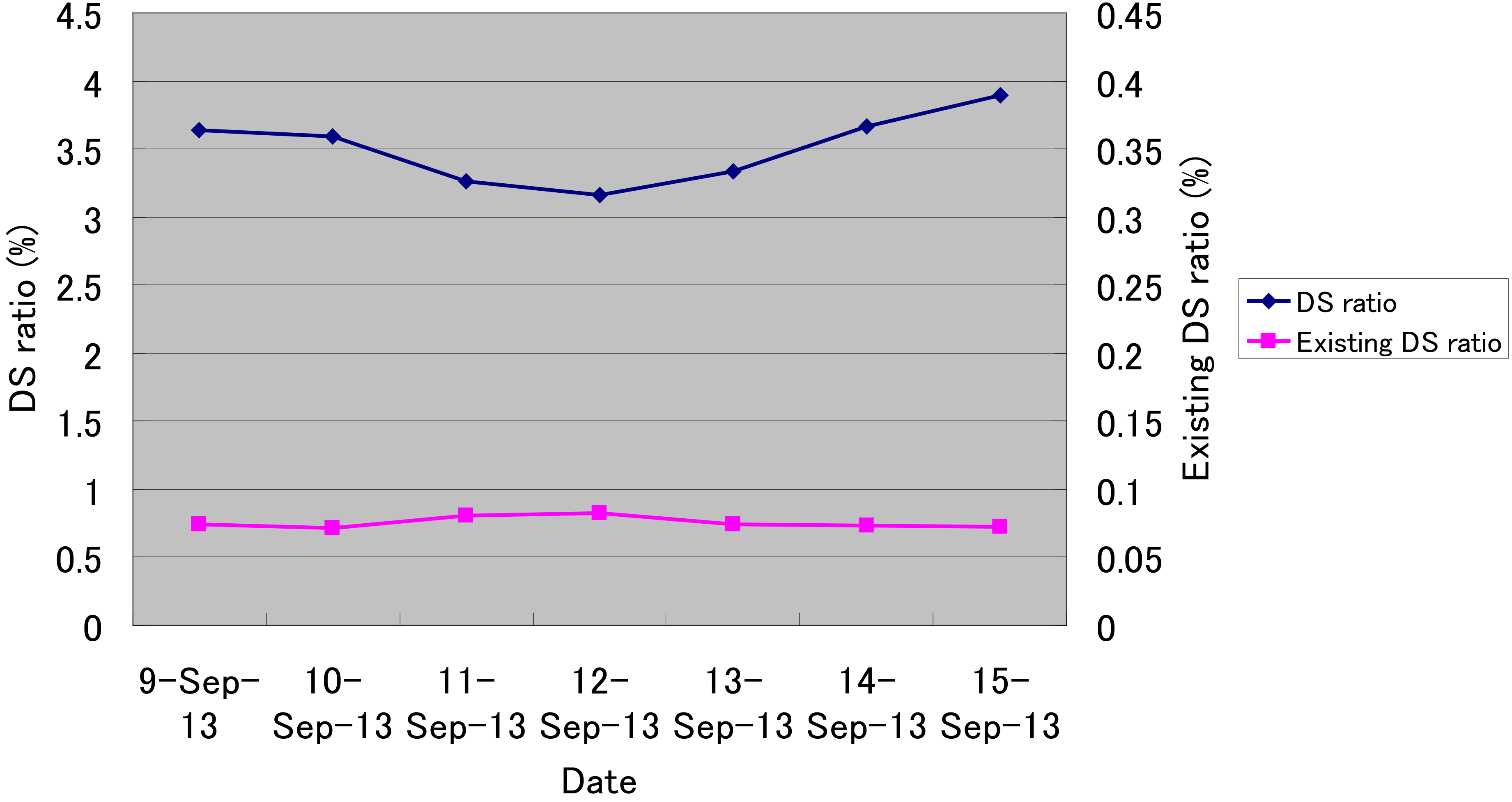
- Dataset and target
  - Query log of 2 out of 7 JP DNS
  - Duration of 9 Sep 2013 – 15 Sep 2013 (typical 1 week)
  - Analyzed DS query ratio
  - DSC graph of 6 out of 7 JP DNS showed the same DS query ratio, so we considered this analysis estimates whole JP DNS
- Analysis results (overview)
  - DS queries / whole DNS queries: about 3.5%

    c.f. Increase of probable DNSSEC Validators and DNSSEC side effect

    <http://www.iepg.org/2013-07-ietf87/4%20-%20IEPG-201307-fujiwara-02.pdf>
  - Existing DS queries / whole DS queries: about 0.08%

    Existing DS queries means DS queries to domain names which have DS records

DS query ratio



Steps to decide moderate DS TTL

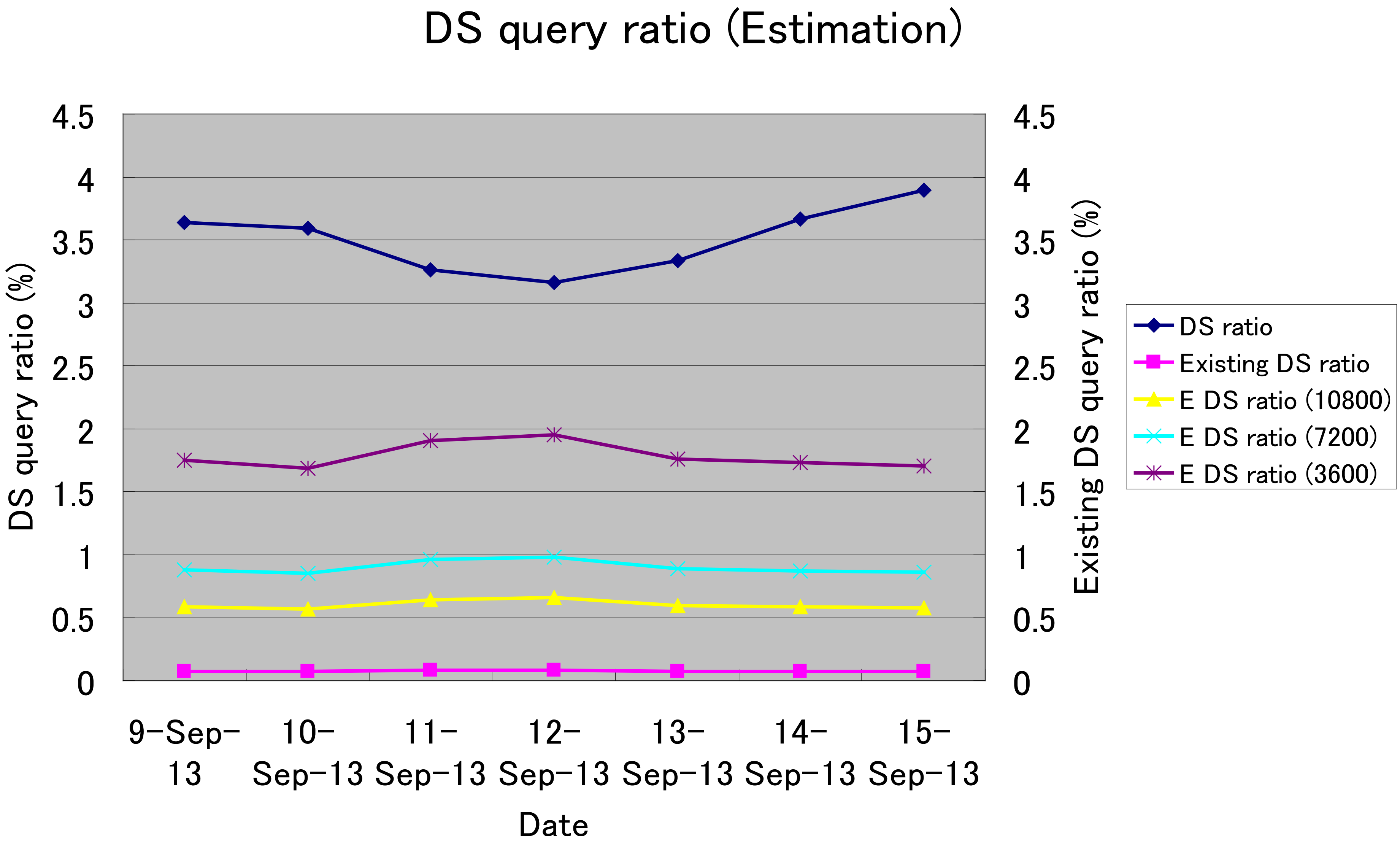
1. Similarity with NCACHE TTL
2. Estimation of influence to current JP DNS
3. Decision

1. Similarity with NCACHE TTL

- DS TTL can be considered as a duration of influence when name resolution failure occurred by DS registration failure
- NCACHE TTL is a duration of status when query name did not exist
- There are similarity between DS and NCACHE regarding name resolution failure
- NCACHE TTL is recommended value is 1 hour (3600) to 3 hours (10800) (RFC 2308)
- DS TTL would also be effective within the range above

2. Estimation of influence to current JP DNS

- TTL=86400 (Current)
  - DS query ratio: 3.5%
  - Existing DS query ratio: 0.08%
- TTL=10800 (1/8)
  - DS query ratio: 3.5% (no increase)
  - Existing DS query ratio: 0.60% (~x8)
- TTL=7200 (1/12)
  - DS query ratio: 3.5% (no increase)
  - Existing DS query ratio: 0.90% (~x12)
- TTL=3600 (1/24)
  - DS query ratio: 3.5% (no increase)
  - Existing DS query ratio: 1.78% (~x24)


DS query ratio (Estimation)
DS query ratio (%)
Existing DS query ratio (%)
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
9-Sep-13
10-Sep-13
11-Sep-13
12-Sep-13
13-Sep-13
14-Sep-13
15-Sep-13
Date
DS ratio
Existing DS ratio
E DS ratio (10800)
E DS ratio (7200)
E DS ratio (3600)

JP’s decision

- Selected the best value for .JP from following conditions

TTL Conditions	10800 (1/8)	7200 (1/12)	3600 (1/24)
Small impact to current JP DNS	Good	Good	Good
Enough scale to shorten DS TTL	Fair	Good	Good
Existing DS queries will not increase drastically when DS and/or validators are increased	Good	Good	Fair

Conclusion

- JPRS decided to shorten DS TTL from 86400 to 7200
  - This value works fine with current JP zone
  - Moderate value will be changed according to increase of validators and DS records
- JPRS shortened DS TTL on 17 Nov 2013
  - DS query ratio was not increased (as estimated)
- Please give your comments based on your similar experiences
  - Would like to have (TLDs') best practice

    <http://datatracker.ietf.org/doc/draft-yoneya-dnssec-kskro-failure-recovery/>