KR DNS Monitoring & DNSSEC Deployment Status

Young-Sun LA
NIDA/KRNIC
rays@nida.or.kr

Contents

- Introduction
- KR DNS Distributional map
- QPS(2008.3~2009.3)
- Query National TOP15
- Cache statistics
- Conficker Domain Query
- DNSSEC Adopting status
- DNSSEC Architecture in .KR
- Plan
- DNSSEC Roadmap

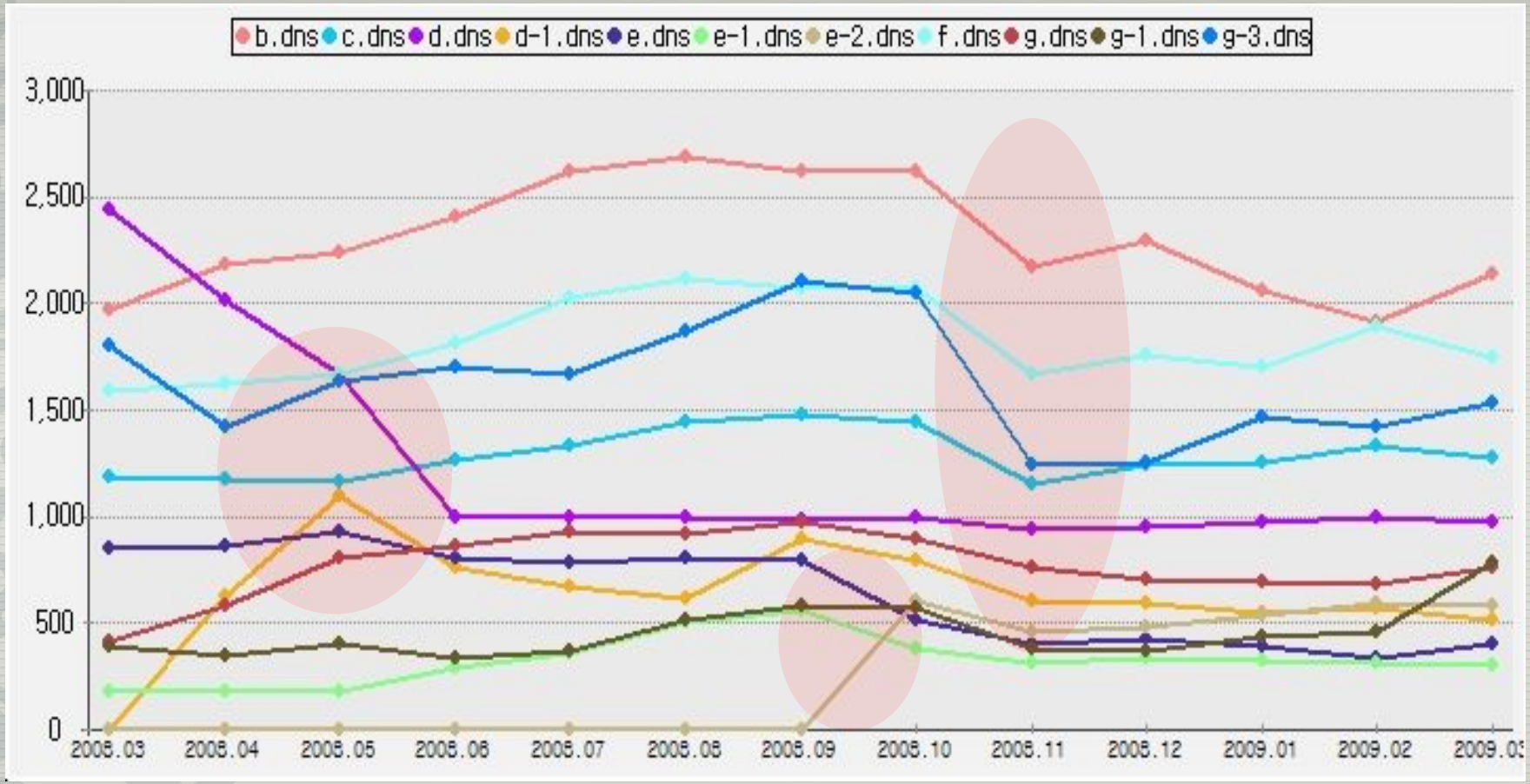
Introduction

- NIDA/KRNIC
  - .KR Registry
    - KR Domain exceeded a Million on 13th Dec. 2008
    - 29 Registrars for KR Domains
  - .KR DNS Deployment
    - 11 sites at home and abroad
    - Cf.) 3 root mirror(f/NIDA, j/KT, m/KINX)
  - Organization Integration
    - NIDA(KRNIC) is going to be KISA(KRNIC) in July.

      * KISA : Korea Internet & Security Agency

KR DNS Distributional Map

QPS (2008.3~2009.3)

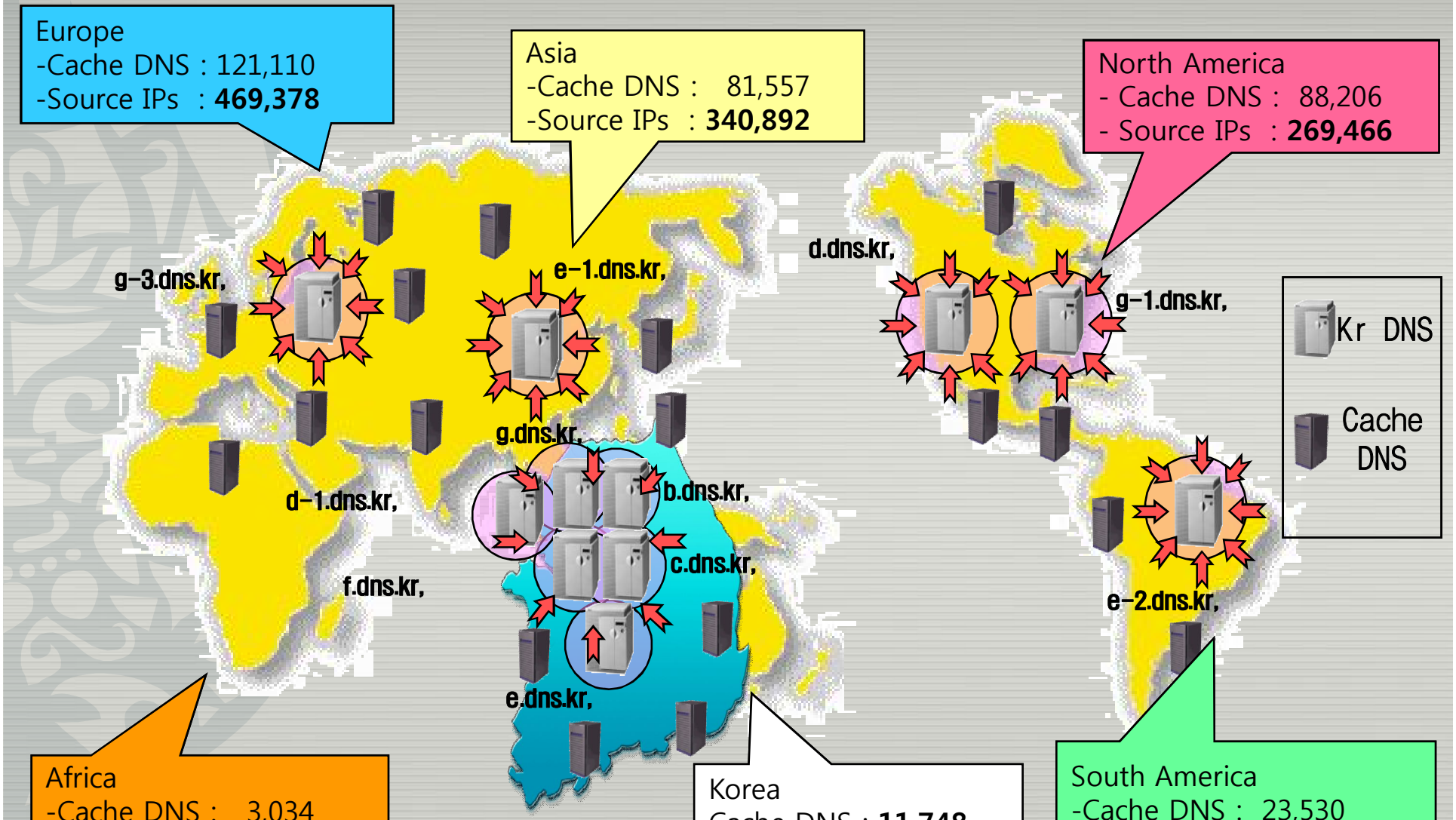


- APR. 2008 : (new) D1 up, D down, Anycast, Load Balance
- SEP. 2008 : (new) E2 up, E&E1 down, Anycast, Load Balance
- DEC. 2008 : Total Traffic 20% drop, PTR(particularly abroad)

Query National TOP15('09.3.26)

Rank.	Nation	Contineltal	Query(per Day)	
1	Korea	Asia	279,847,990	KR DNS(B ~G)
2	U.S.A	North America	188,444,149	KR DNS(G, D Mirror)
3	Russia	Europe	41,014,349	
4	German	Europe	33,879,033	KR DNS(G Mirror)
5	China	Asia	28,628,569	KR DNS(E Mirror)
6	England	Europe	24,352,011	
7	Japan	Asia	23,308,707	
8	France	Europe	17,900,393	
9	Canada	North America	15,147,497	
10	Italy	Europe	11,607,953	
11	Spain	Europe	10,995,300	
12	Nederland	Europe	9,722,634	
13	Taiwan	Asia	8,408,915	
14	Australia	Pacific	7,725,771	
15	Brazil	South America	6,677,017	KR DNS(E Mirror)

Cache Statistics(2009.3)

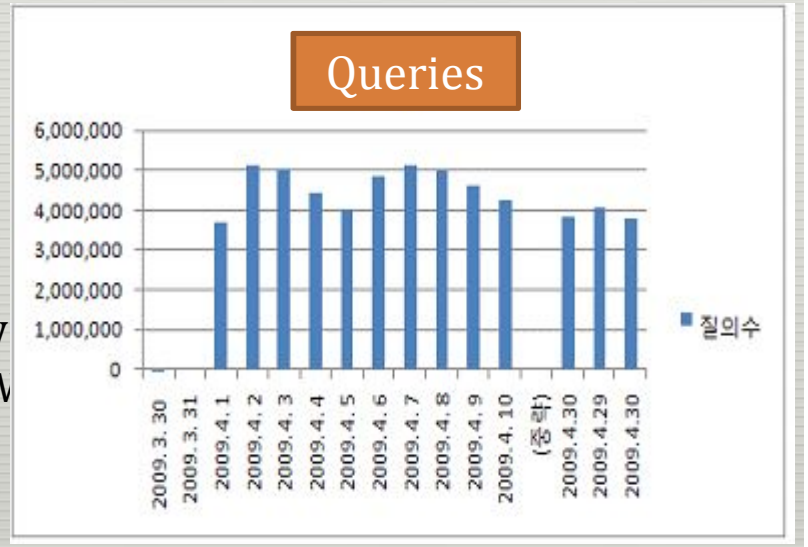


Cache Statistics(2009.3)

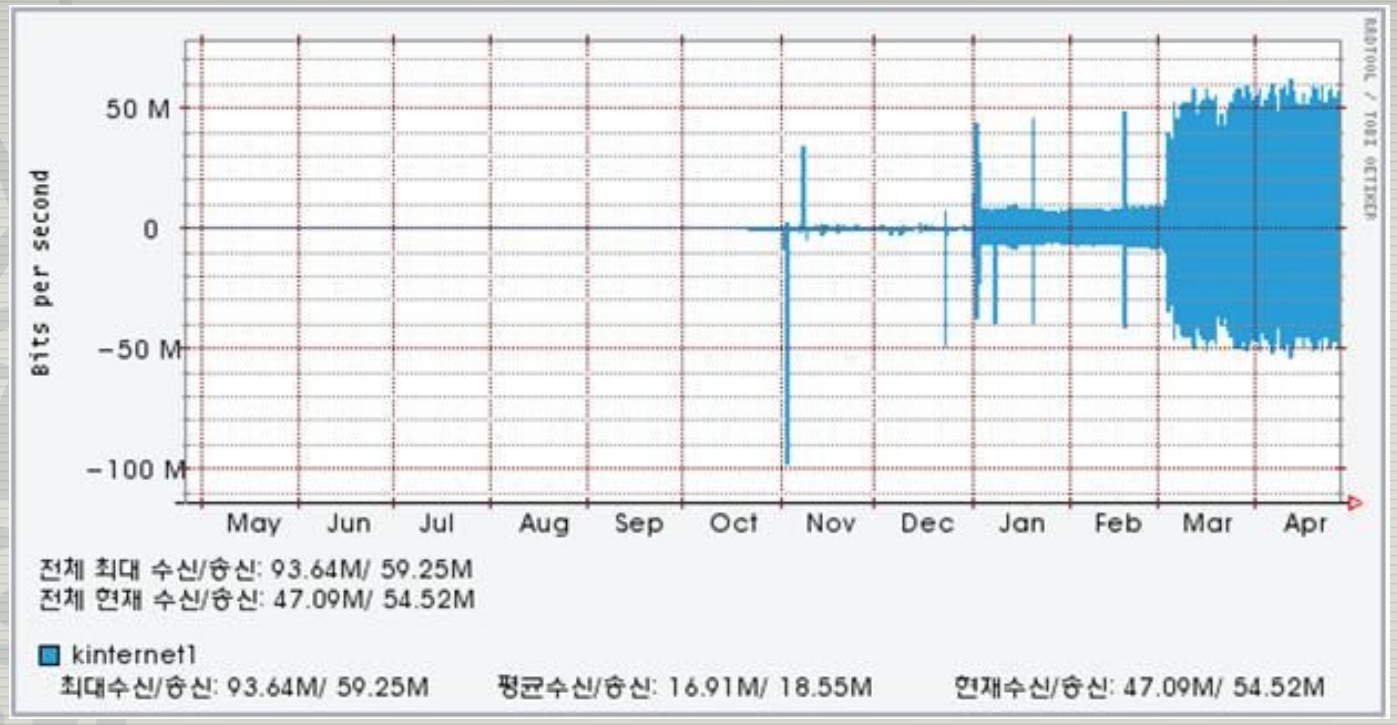
- IP Gathering Period : 30/03/2009 ~ 31/03/2009
- Total Source IP : 1,269,778
- Cache checking : 1,094,635(86.2% done)
  - Cache/non-Cache : 318,213(29%)/776,596(71%)
  - Cf.) Total number of source IP in April : 10,830,000

Conficker Domain Query

- KR Domain names affected by Conficker : about 40,000 domains(438 registered domains)
  (* provided by ICANN)
- Monitoring results
  - Queries to Conficker(suspected) KR domains
    - 3/30 : 13,054 queries
    - 3/31 : 81,830
    - 4/1 : 3,718,426
    - 4/2 : 5,125,077
  - National TOP10
    - 3/31 : KR-US-VN-FR-RU-CN-DE-CA-JP-TW
    - 4/1 : CN-RU-VN-KR-IN-ID-UA-TH-PH-TW
    - 4/2 : CN-RU-VN-KR-US-UA-IN-ID-TH-PH

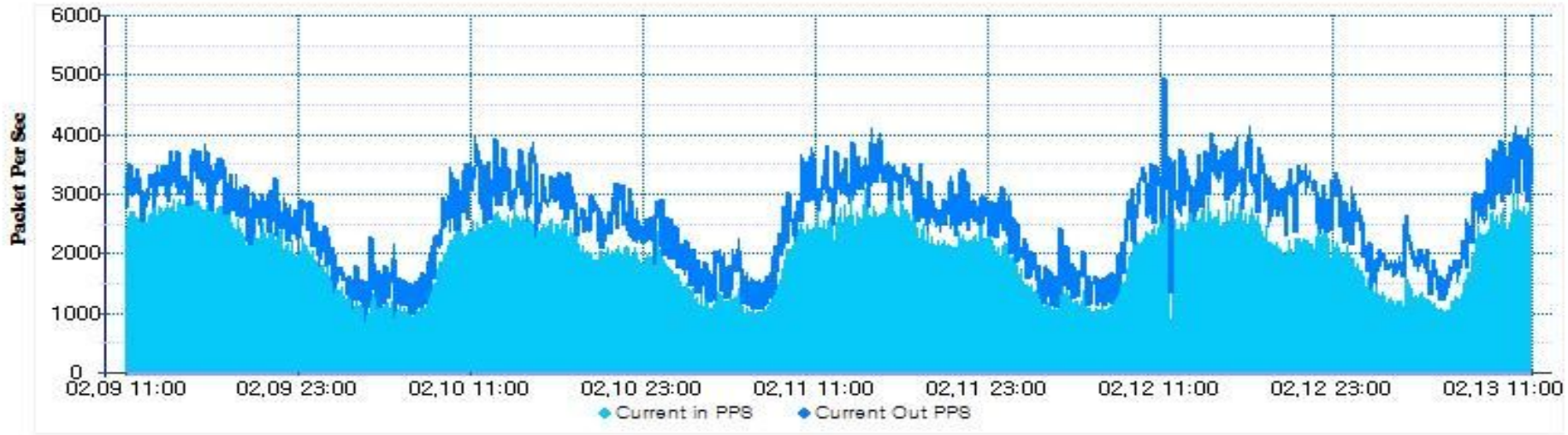


Monitoring(Puny code converter)



- UTF-8 -> Puny code
- Traffic Increased
- Need to get rid of wild card in the zone setting

Monitoring(incident)



in Bound				out Bound			
MIN	MAX	AVG	CUR	MIN	MAX	AVG	CUR
905	3,712	2,048	2,689	954	4,947	2,566	3,778

- Normal : IN >= OUT
- Abnormal : IN < OUT (2009. 2)
- Malformed packet detected

Monitoring(incident)

- 09:15:38.178845 IP **169.***.**.**.47996 > **61.74.75.1**.domain: 22426 **update+**% [b2&3=0x2d36] [12288q] Type0 (Class 0)? . Type0 (Class 0)? . Type0 (Class 0)? . Type0 (Class 0)? . Type0 (Class 0)? . Type0 (Class 0)? . Type0 (Class 0)? **.[|domain]**

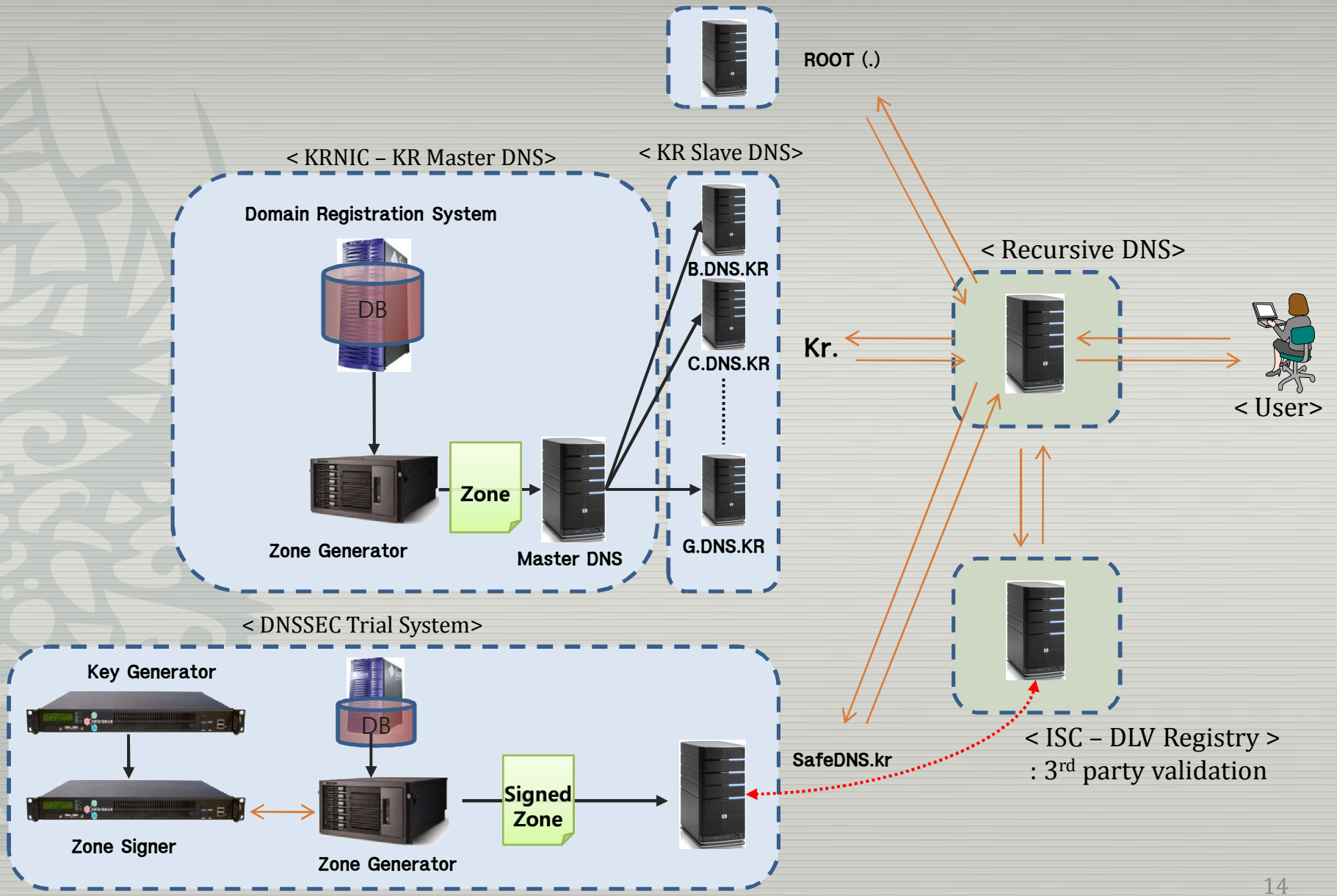
- (2009.2.10) packet sampling , a number of Malformed packet(above) were detected

- Source IP : 169.***.**.**(a university in U.S.A own the IP)
- Destination IP : 61.74.75.1(B.DNS.KR's IP)
- It's returned to normal after days

DNSSEC Adopting Status

- Trial system(NSEC) with safedns.kr in 2007
- Key administration research in 2008
- Basic Policy Established : 2009. 1
- BIND 9.6.0-P1 Patch : 2009.2
- DLV(safedns.kr) setting : 2009.3
- Roadmap Establishment : 2009.4
- Trial system alteration to support NSEC3 : now

Architecture with DLV



DLV Configration

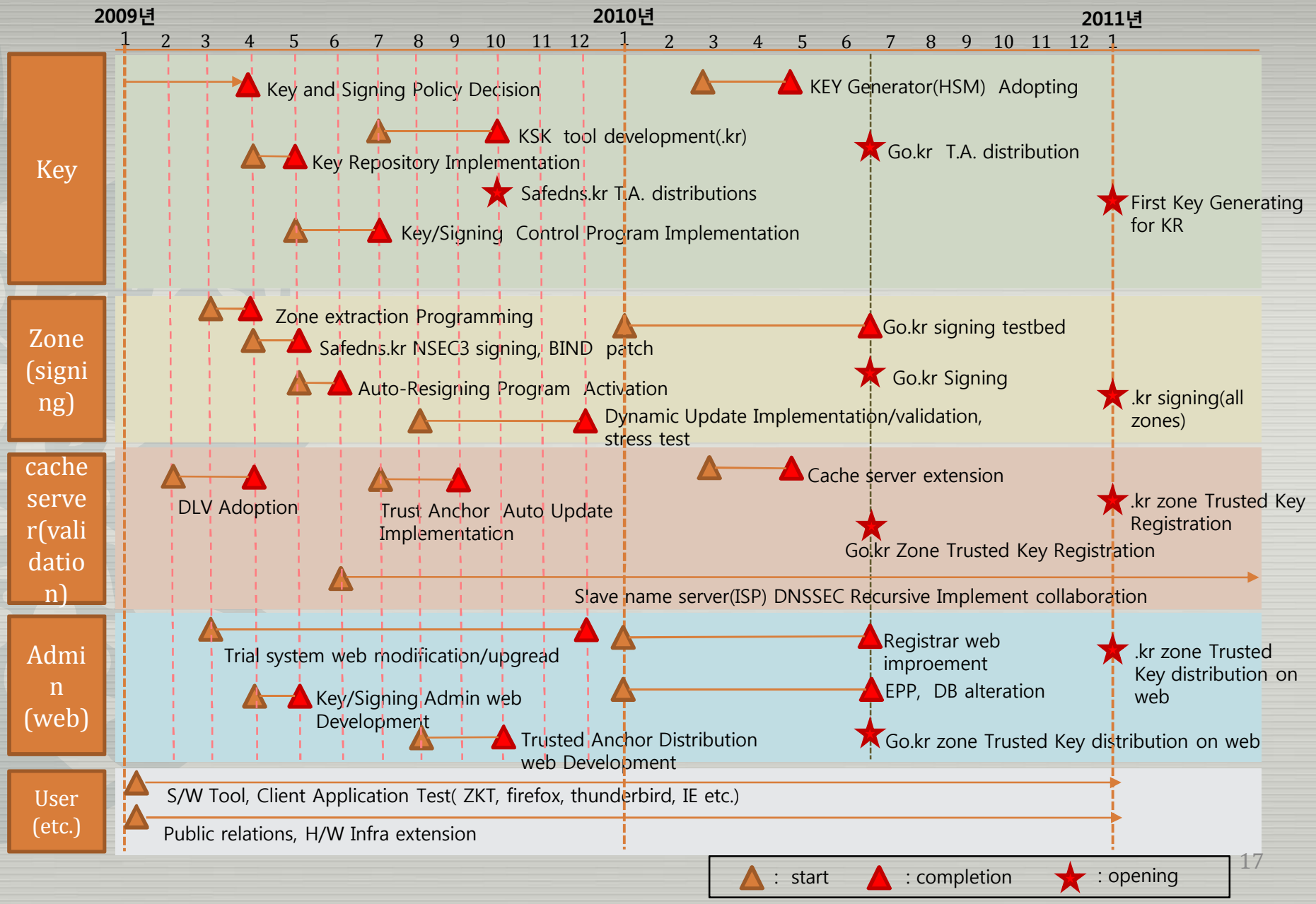

```
options {
        version "unknown";
        directory "/var/named";
        dump-file "/var/named-log/cache_dump.db";
        statistics-file "/var/named-log/named_stats.txt";
        edns-udp-size 1460;
        allow-query { any; };
        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside "." trust-anchor dlv.isc.org.;
        listen-on-v6 { any; };

};
```

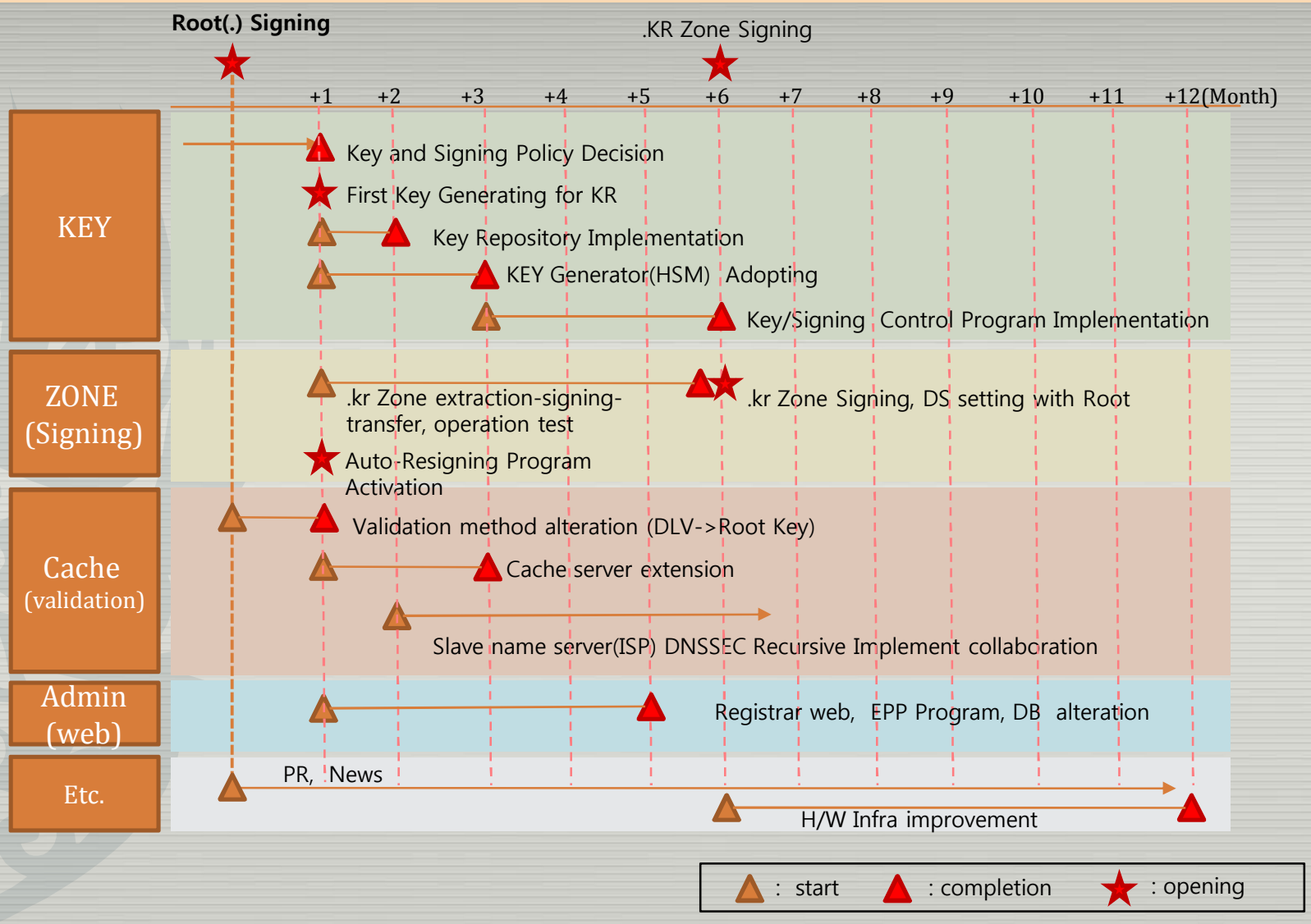
Plan

- Step by step
  - Safedns.kr -> go.kr -> kr
- Trial system improvement
  - NSEC->NSEC3
  - cf.) DLV with NSEC3
- Publicity campaign
  - Education
- Management S/W Development
- Versional Roadmap

Kr DNS DNSSEC Deployment Roadmap I
(Root Signing After 2011)



Kr DNS DNSSEC Deployment Roadmap II
(Root Signing before 2011)



THANK YOU

RAYS@NIDA.OR.KR