<36th APNIC Meeting, XIAN CHINA>

KISA(KRNIC) UPDATE

YOUNGSUN LA

(rays@kisa.or.kr)

Korea Internet & Security Agency

Contents

- IPv6 Verified NSDs R&D
- WHOIS User Analysis & Statistics
- RPKI Testbed

IPv6 Verified NSDs R&D
- Efforts to mitigate IPv6 obstacles

- Background : NSDs aren’t fully support IPv6, performance not verified, this make customers hesitate to deploy IPv6 at their organizations.
- KISA is going to
  - Survey NSD vendors readiness and awareness
  - Research IPv6 security vulnerabilities
  - Coordinate IPv6 NSD developer WG
  - Develop performance measurement methodology
  - Measure some of NSDs(FW, WAF, IPS, VPN, MDM)
  - Develop guidelines for both of vendors and customers
  - Facilitate IPv6 verified NSDs release in the market

IPv6 Verified NSDs R&D - Survey

- The surveyed(recipient) : 160 org.
- Respondents : 18 org.
- Summary of aggregate responses
  - Q1) IPv6 awareness : high(8), medium(7), low(3)
  - Q2) IPv6 readiness : none(8), a little(6), almost ready(4), done(0)
  - Q3) Reasons why IPv6 difficult(multiple answers possible)
    - Cost a lot to R&D (6)
    - Low need from market(9)
    - Lack of experts and IPv6 tech.(11)
    - No IPv6 succeed cases(best practice) (5)
    - Difficult to construct R&D&Test environment(13)

IPv6 Verified NSDs R&D - Survey(contd)

- Summary of aggregate responses(contd)
  - Q4) When will it be ready :
    - Internal(self) plan (5) : *no response(3), 1Y(1), 10Y(1)
    - Immediately if there is need from market or government's plan(decision)(13)
  - Q5) What do you want from government(multiple answers possible):
    - Policy & plan, determine when the introduction(13)
    - Technical support(14)
    - IPv6 products development support(9)
    - Information feed(9)
    - Other comments(funding(1))

IPv6 Verified NSDs R&D - Survey(contd)

- Summary of aggregate responses(contd)
  - Q6) Do you think certificate is need :
    - no(8)
    - yes(10) *(new(2)/current(8))
  - Q7) When is suitalbe for certificate introduction :
    - 2014(1), 2015(6), 2016(3), 2017~(7), no response(1)
  - [FYI] Products that survey respondent have :
    - MDM(2), FW(6), UTM(4), VPN(4), IDS(1), IPS(5), DLP(1), DDoS(4), PC firewall(1), Scanner(1), Log analysis tool(1), Document security system(1), Source code scanner(1), WAF(3), Server access auditor(2), DB access control(1), zombie PC detector(1), VOIP(1), Security managent server(1), Wireless firewall(1), Vnti-Virus(1), patch management system(1)

IPv6 Verified NSDs R&D
- IPv6 NSD developers WG

- 9 Participants
  - KISA, KSEL(CC certificate Authority), Ahnlab(UTM, FW, IPS, VPN), FutureSystems(UTM, FW, IPS, VPN), XNsystems(UTM, FW, IPS, VPN), NexG(UTM, FW, IPS, VPN), MONITORAPP(WAF), ExTrus(MDM), NetMan(NAC)

IPv6 Verified NSDs R&D
- IPv6 security vulnerability research

- Known IPv6 vulnerability in CVE
  - 150 Vulnerabilities
- References
  - Guidelines for the Secure Deployment of IPv6(NIST)
  - http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=ipv6#top
  - A Profile for IPv6 in the U.S Government-Version1.0(NIST)
- Information wanted!
- (if necessary) Joint research to regist and share IPv6 security vulnerabilities

IPv6 Verified NSDs R&D
- What's the next

- Performance measurement(BMT)
- Guideline document development
- Gradually expand the target NSD
  - 2013 : IPS, VPN, FW, MDM, WAF
  - 28 NSD categories exist in KR (Source : IT Security Certification Center)
  - CC certificate is mandatory for government, public organizations

  * The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security.
- (Ultimately) to promote IPv6 verified NSDs launch in the market

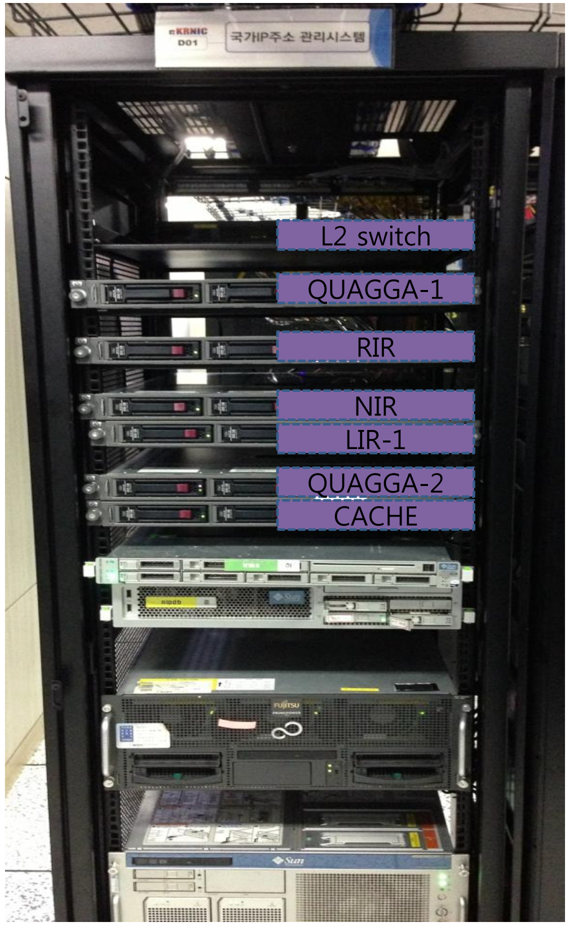
WHOIS User Analysis & Statistics

- 0.8Milion queries per day
- Without analysis there is no improvement
- Items : Utilization, query source classification, time, query target classification, top user(ranking), etc.
- Changes in utilization before(after) hacking incident
  - Scanning detected(coincidence? Or symptom?)
- Future directions
  - (systematic)Monitoring, control to see if there is the presence of repeating patterns
  - Abnormal traffic purification

WHOIS User Analysis & Statistics
- Statistics Summary

- Avg. query per day : 812,133
- Query via :
  - "Command(64.58%)", "OPEN API(30.2%)", "HTTP(5.22%)"
  - (mainly) IT experts use WHOIS service
- Target : IP(62.51%), domain(34.36%)
  - 9 target domain among domain top 20 are abnormal (i.e. IA9-KR, IM9-KR, IM12-KR, …)
  - a significant level of abnormal traffic
- User classification :
  - private(97.99%), education(1.4%), public(0.56%), financial(0.06%)

RPKI Testbed
- System configuration



No.	HOST	IP	role
1	L2 SWITCH	-	test BGP (private configuration)
2	QUAGGA-1	eth0: 172.16.0.10	S/W ROUTER (For RPKI Verification)
3	RIR	eth0: 202.30.OOO.XXX	Root CA server
4	NIR	eth0: 202.30.OOO.xxx	KISA CA server
5	LIR-1	eth0: 202.30.OOO.xxx	ISP CA server
6	QUAGGA-2	eth0: 172.16.0.20	S/W ROUTER (For RPKI Verification)
7	CACHE	eth0: 202.30.OOO.xxx eth1: 172.16. 0.50	RPKI Validator (Local Cache server)

- Linux server 6ea, L2 switch 1ea
- QUAGGA-1, QUAGGA-2, (for the safety) private network(L2 switch)
- CACHE configured with both of public and private network to communicate S/W router and CA server

RPKI Testbed
- SW configuration

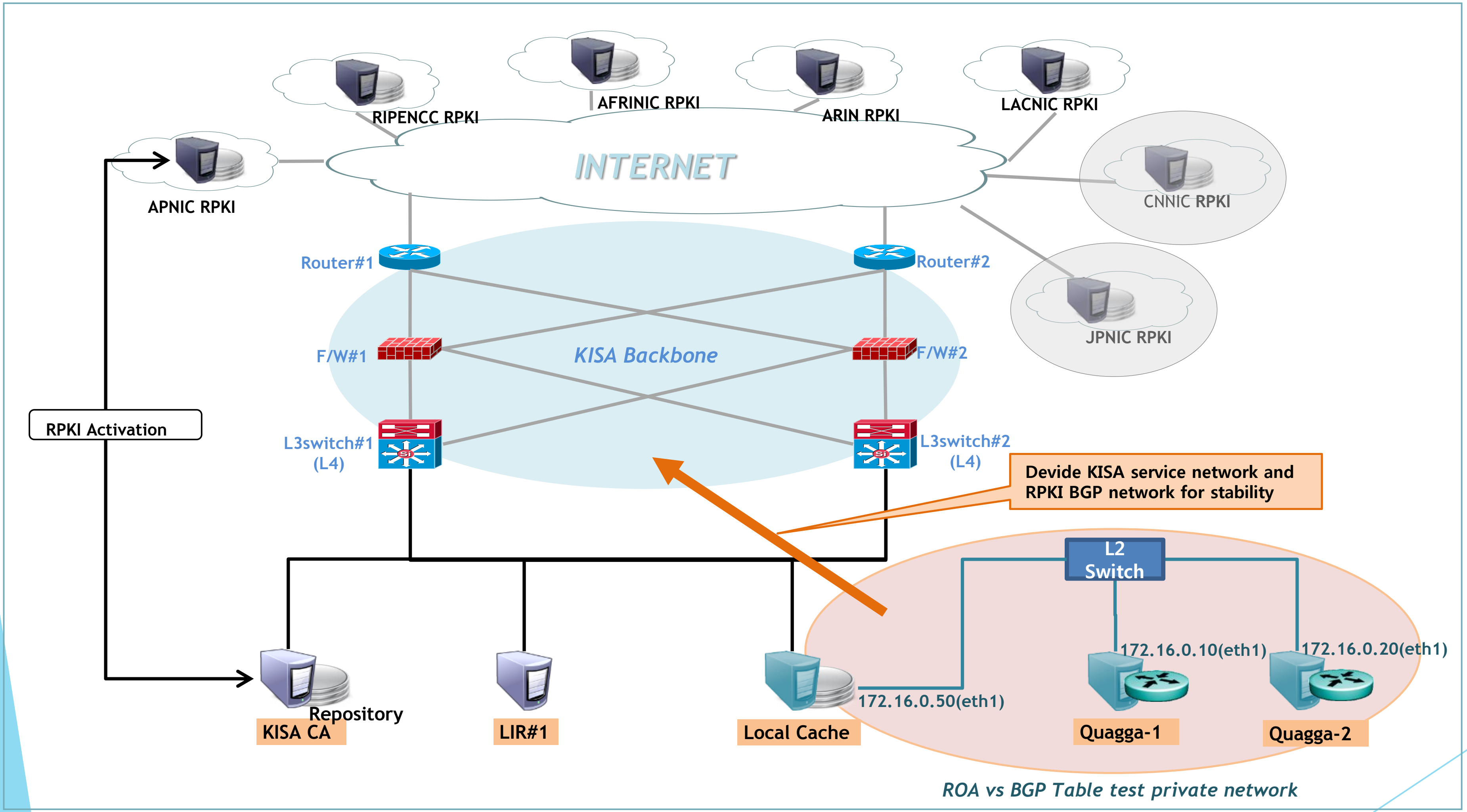
- CA server : RPKI.NET RPKI CA engine(http://download.rpki.net)
- RPKI Validator(cache server) : RIPE NCC RPKI Validator
  - http://www.ripe.net/lir-services/resource-management/certification/tools-and-resources
- RPKI enabled BGP router : Quagga-SRX
  - http://www-x.antd.nist.gov/bgpsrx

RPKI Testbed

- What have we done
  - Configured Trust Anchor between CA(Grandparenting Operation)
  - Three level CA(RIR-NIR-LIR/ISP) structure
  - Assigned Reousorces and issued ROA
  - Synchronize Repository to Local Cache server
  - Verified ROAs
  - Checked telecommunication between Local Cache and BGP router

- What's the next
  - Test with global entities
  - We should choose RPKI service Activation method
    - 1) Use APNIC's RPKI Activation service(RPKI Portal or Create Own RPKI Engine)
    - 2) KISA could be Root Certification Authority(itself)
      (it requires Trust Anqor Locator distribution)

RPKI Testbed
- RPKI Global linkage test first draft



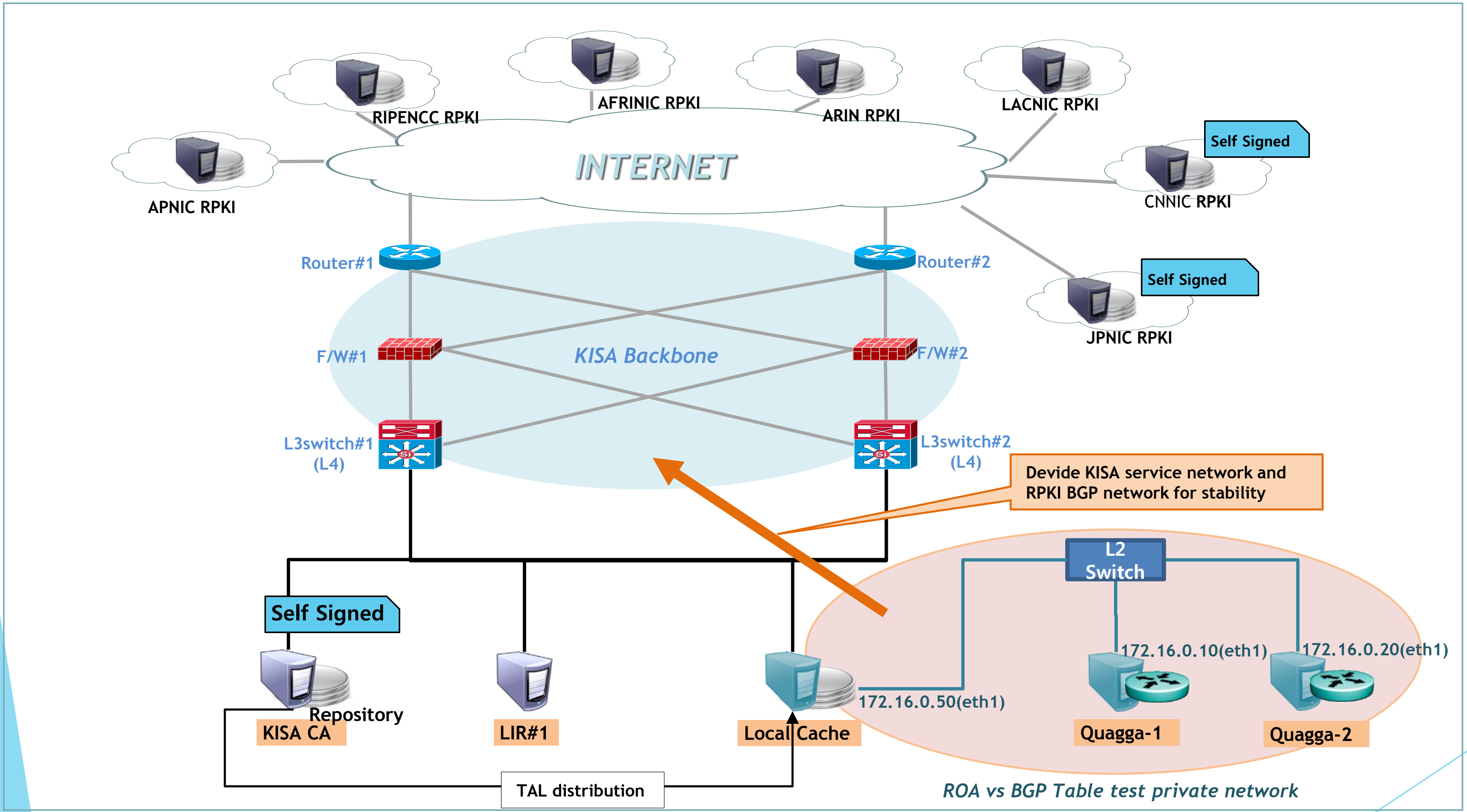
Devide KISA service network and RPKI BGP network for stability

ROA vs BGP Table test private network

□ need ASN & IP Prefix from APNIC

□ need ISP's cooperation : ISP that have global routing table for test

RPKI Testbed in KR
- RPKI Global linkage test second draft



□ need ASN & IP Prefix from APNIC

□ TAL Publication between countries for Repository & ROA data shareness(self Signed environment)

THANK YOU