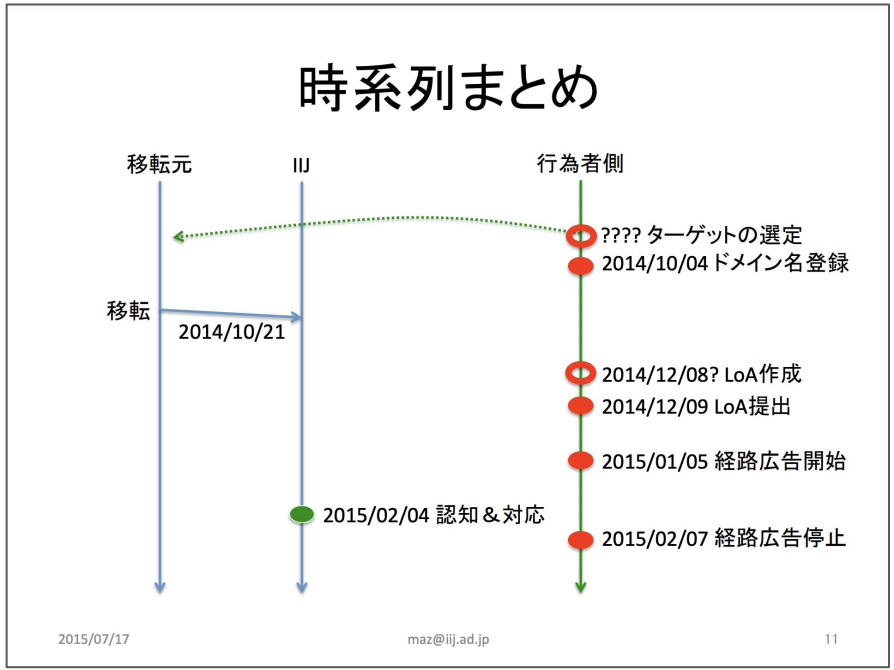
Highlights from the past JANOG meetings

Pickup Programs

Routing Security	A story of BGP route hijacking	JANOG36
	Let's start RPKI with IIJ/AS2497	JANOG47
	Peerlock implementation review working group report	JANOG47
Public NTP	Current status and issues of public NTP service in Fukuoka Univ.	JANOG41,47
Infra in Japan	Did the Internet in Japan really become more robust?	JANOG44
	IPv6 availability on mobile networks	JANOG45
	DOCOMO's Approach toward the Expansion of IPv6 Address Usage in Cellular Networks	JANOG48
	The Introduction to the confederation of KESHIKARAN networks	JANOG47
SDN/NFV Case Studies	Introduced network controller to OCN	JANOG48
	High Functional Cloud NFV System Design and Implementation at LINE Cloud	JANOG48
	The 5 years journey of NFV in KDDI fixed VoIP network	JANOG49
DC Network	What are you doing to operate Clos Network Topology?	JANOG49
Experimental	Measuring Internet Latency with SR-MPLS Egress Peer Engineering	JANOG48
	BGP peering over IX with RFC5549	JANOG49
New Trends	Let's talk about QUIC	JANOG49

A story of BGP route hijacking

JANOG36: 2015 Jul. Speaker: Matsuzaki ‘maz’ Yoshinobu(IIJ)



Background:

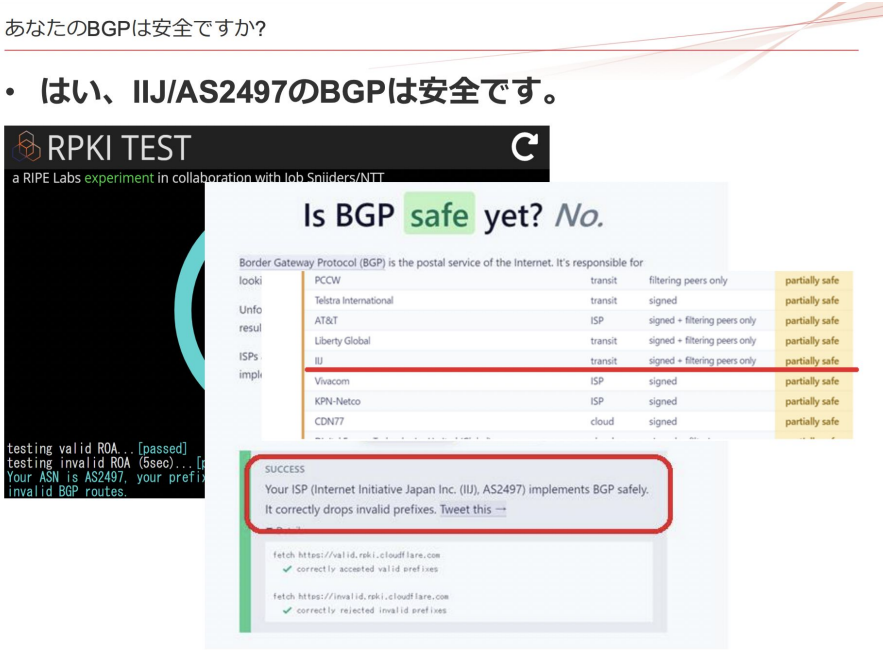
Being a victim of BGP route hijacking is a valuable learning experience. Sharing his real experience in JANOG meeting was a good opportunity to get people thinking.

Summary of the presentation:

- IIJ noticed rogue longer prefixes were announced from an ISP in U.S.
- The root cause was that the perpetrator used fake LoA(Letter of Authority) to get the prefixes announced.
- It was noted that especially in Japan unannounced or provider-independent addresses looks like an easy target.
- Operational countermeasures and possible legal actions were discussed.

Let's start RPKI with IIJ/AS2497

JANOG47: 2021 Jan.　Speaker: Yuichi Yomogita(IIJ), Takafusa Hori(IIJ)



出典: RIPE RPKI Test: https://labs.ripe.net/Members/nathalie_nathalie/rpki-webtest　CloudFlare: https://isbgpsafeyet.com/

Background:

RPKI implementation in Japan is not yet spread widely.
IIJ (AS2497) has been implementing ROA and ROV.
They shared comprehensive views and their experiences.

Summary of the presentation:

- Shared their ROA registration policy
- JPNIC(NIR) is providing JPNIC ROA Web
- They decided to do ROV on their AS border routers, which seems almost the first case of rejecting invalid routes in Japan.
- Shared what they did to remove fears of discarding invalid 3000 prefixes
- Reliability of RPKI related component is important

Peerlock implementation review working group report

JANOG47: 2021 Jan. Speaker: Matsuzaki ‘maz’ Yoshinobu(IIJ)

Background:

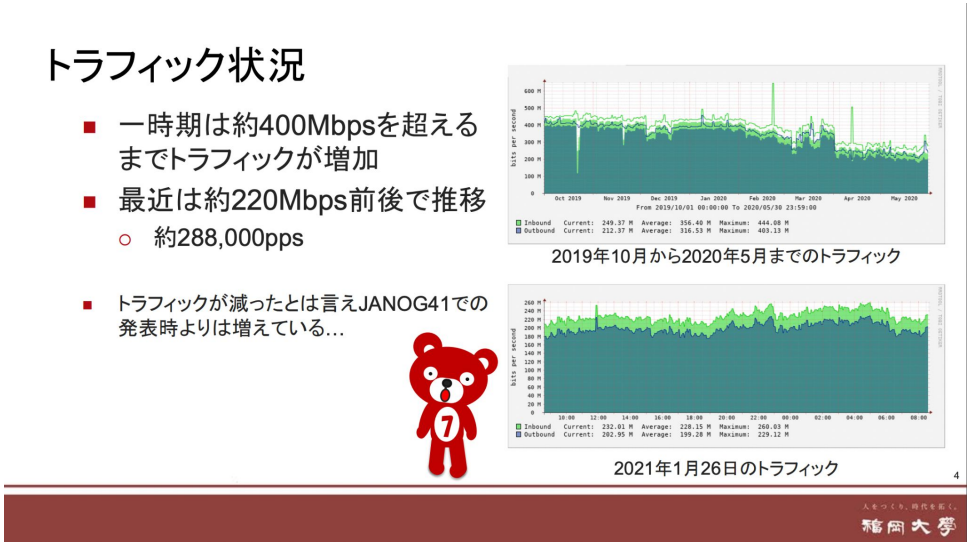
Peerlock is an easy-to-implement route leak blocking mechanism based on as-path filters with trusted adjacent ASes, which is proposed by Job Snijders.
A WG for the introduction of Peerlock at Japanese network operators was launched at JANOG45.

Summary of the presentation:

- The exhaustive study was reported including on what conditions peer lock can easily function
- Useful information was reported to the community such that what should be confirmed between ASes (contact information, operational policy, and estimated time required for configuration changes) for peer lock introduction.

Current status and issues of public NTP service in Fukuoka Univ.

JANOG41: 2018 Jan. and JANOG47 2021 Jan.
Speaker: Sho Fujimura(Fukuoka University), Fuminori ‘Tany’ Tanizaki(NTT West)



Background:

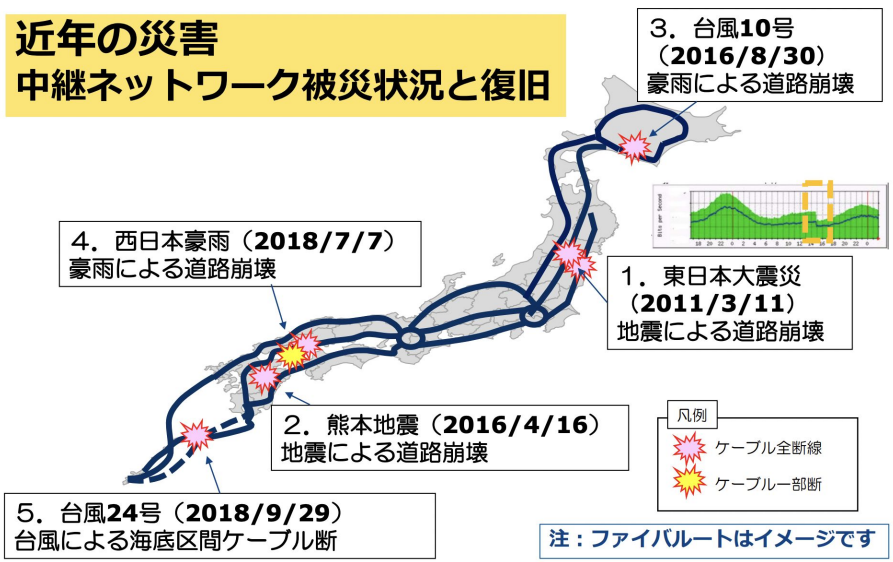
Fukuoka University has been providing public NTP service since 1993, which is being used actively and broadly from all over the world because the IP addresses (133.100.9.2, 133.100.11.8) are embeded in default settings of many gears and softwares.

Summary of the presentation:

- They’re requesting to quit the use of their NTP service
- They’re going to stop the NTP service (not yet)
- Just stopping the NTP service will double the traffic because NTP clients will send retry packets more frequently.
- They logically separated the campus network from the public NTP service in order to do research on the public NTP service.

Did the Internet in Japan really become more robust?

JANOG44: 2019 Jul.　Speaker: Yoshiki Ishida(JPNE), Yoshida Tomoya(NTTCom), Kei Nishida(QTnet)



Background:

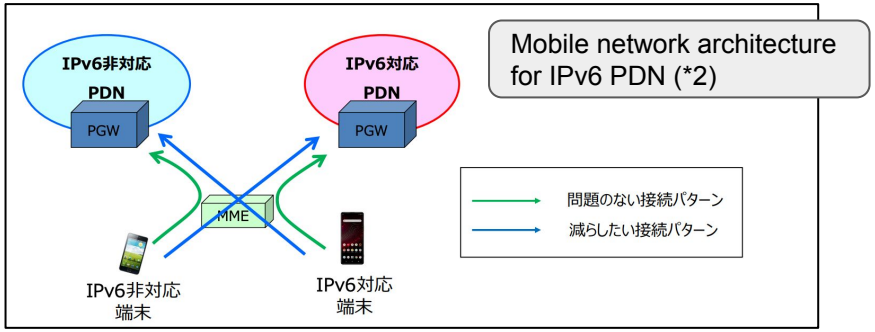
The Great East Japan Earthquake of 2011 has prompted Japanese network operators to strengthen their preparedness for natural disasters.
Eight years later, and having experienced a variety of disasters, they took a look back to see if the issues identified at that time have been resolved.

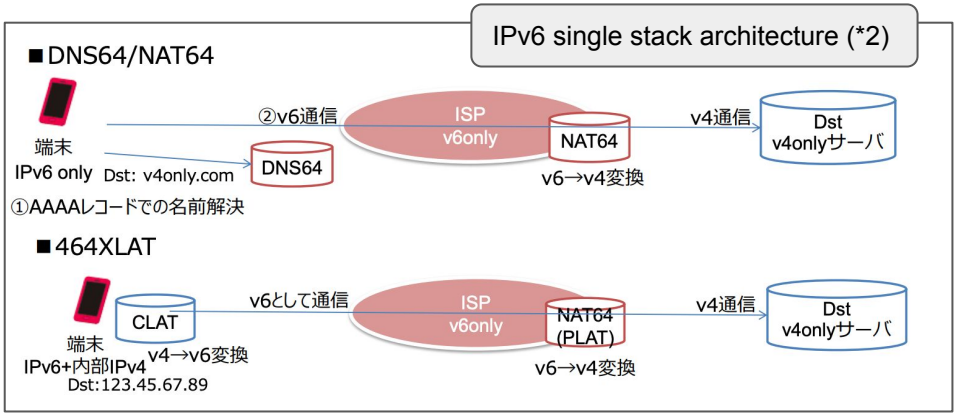
Summary of the presentation:

- Progress has been made in distributing data centers to the east and west in Japan.
- Redundancy (3 routes) of relay cables, access networks, and international oversea cables has progressed.
- Not all the issues resolved yet: Operation under disasters, mutual understanding and coordinated emergency response between NW operators and content providers and so on.

IPv6 availability on mobile networks *1
DOCOMO's Approach toward the Expansion of IPv6 Address Usage in Cellular Networks *2

*1 JANOG45: 2020 Jan. Speaker: Yoshinobu Matuzaki(IIJ)
*2 JANOG48: 2021 Jul. Speaker: Naoya Minakuchi, Koichiro Kunitomo, Masahide Aikawa (NTT DOCOMO)





Background:

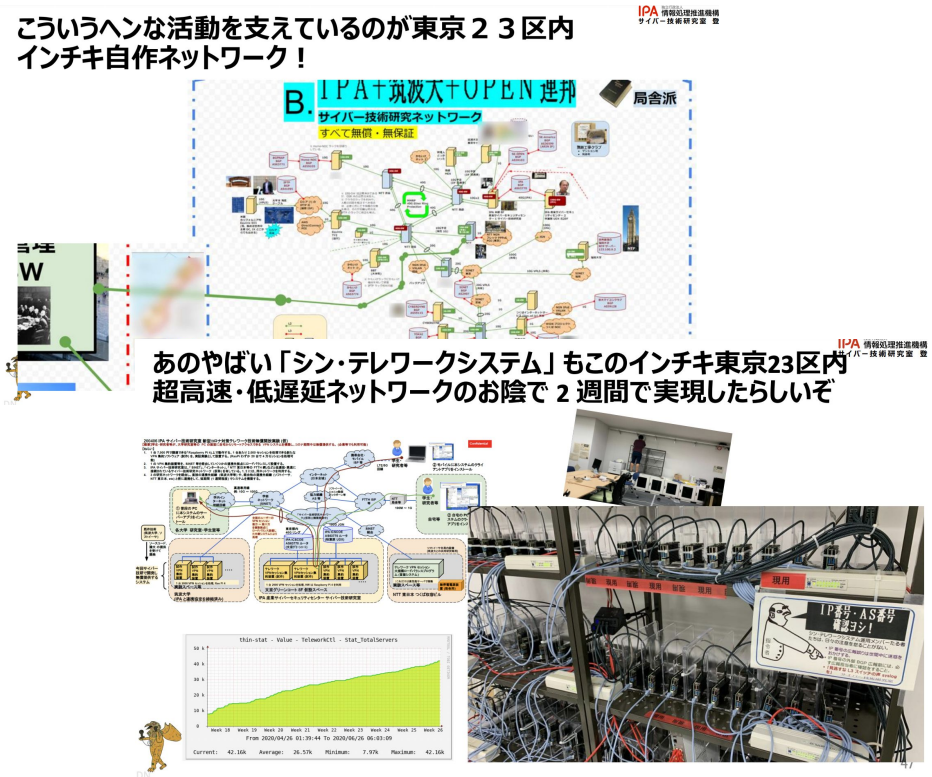
- A survey results of (*1) revealed that IPv6 availability in Japan's mobile networks are quite limited in 2020.

Summary of the presentation:

- Based on the survey results, NTT docomo's efforts to improve IPv6 availability in mobile network were introduced in (*2)
  - How to select IPv6-enabled PDNs in EPC network: MME-based selection and PGW-based selection
  - IPv6 single stack with DNS64/NAT64 and 464XLAT

The Introduction to the confederation of KESHIKARAN networks

JANOG47: 2021 Jan.　Speaker: Dai Nishino(Keshikaran Union Network) and 5 people.



Background:

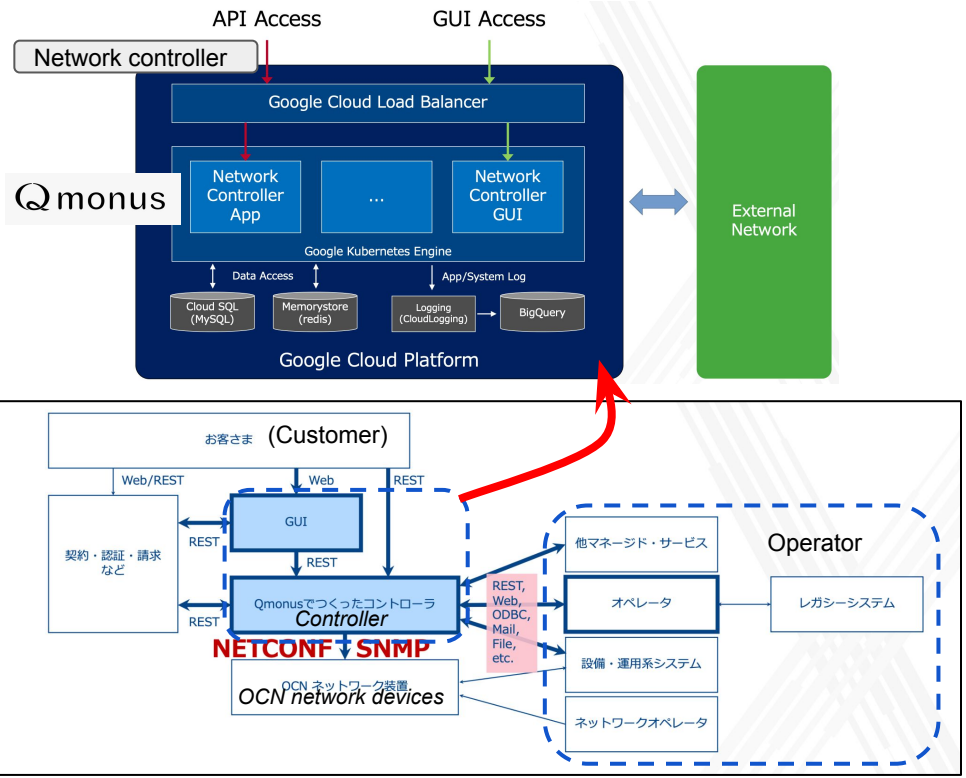
The definition of “Keshikaran Network” is an experimental practical network using dark fibers. KESHIKARAN means “outrageous”.

Summary of the presentation:

- The reason of dark fiber is freedom of choice of gears on both ends
- It’s not usual for non telecom organizations to own dark fibers but they interconnected such an outrageous networks freely in underground of Tokyo
- They talked in an amusing way that once away from the rules of traditional corporate, to play with outrageous network is seeds of innovation

Introduced network controller to OCN

JANOG48: 2021 Jul. Speaker: Ito Yoshiya, Takahashi Haruki (NTT Communications)



Background:

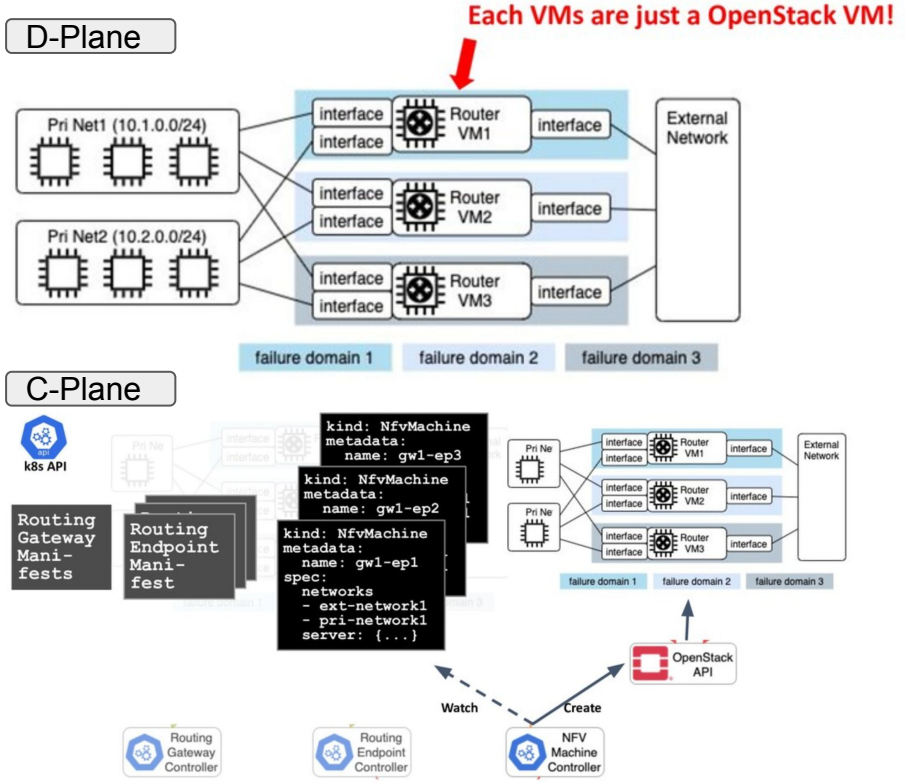
- About 10 days were required from the time customers contract for OCN's Internet service until they were ready to use it.
  - Human operator conducted each required step such as router configuration

Summary of the presentation:

- A fully automated network controller using NTT's in-house orchestrator, *Qmonus*, was introduced.
  - *Qmonus* is a PaaS for development, deployment, and operation of cloud-native application
  - OCN's network devices are monitored and controlled by the network controller using NETCONF and SNMP

High Functional Cloud NFV System Design and Implementation at LINE Cloud

JANOG48: 2021 Jul. Speaker: Hiroki Shirokura(LINE)



Background:

- LINE is developing various Internet services such as messaging and financial, and needed Virtual Private Cloud (VPC) for these services.
  - The VPC requires an isolated private network and NFV services (VPN, ACL…)

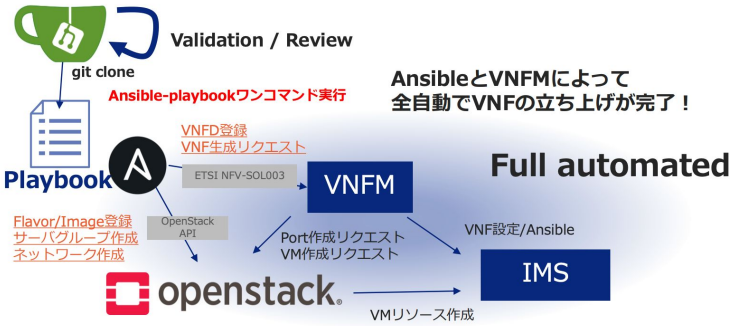
Summary of the presentation:

- LINE's developing VPC SDN architecture including D-Plane and C-Plane were introduced
  - D-Plane with VM-based vRouter operated by OpenStack
  - C-Plane with k8s extension: *KloudNFV*
- Some production experiences and challenges were also introduced

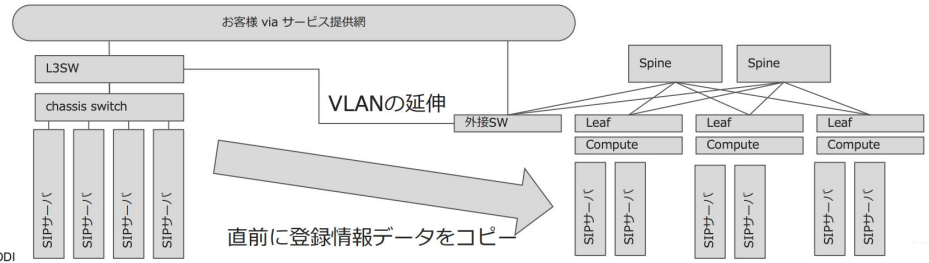
The 5 years journey of NFV in KDDI fixed VoIP network

JANOG49: 2022 Jan. Speaker: Hiroshi Tsuji, Hitomi Koba (KDDI CORPORATION)

Automation on NFV environment



Migration to NFV



Background:

- KDDI had a fixed-line network renewal project from 2016 to 2021
  - aTCA/CGLinux -> NFV

Summary of the presentation:

- KDDI's fixed-line IMS architecture is introduced
  - Multi-vendor was targeted, but resulted in a single-vendor dedicated infrastructure
- Migration from aTCA/Linux to NFV
  - SIP servers needed to be migrated with same IP addresses
    - Extend the VLAN network between old and new network

What are you doing to operate Clos Network Topology?

JANOG48: 2021 Jul.　Speaker: Hiroshi Umehara(Sakura Internet)

Clos Network Topology の理解が無ければ対応が難しい内容について特定のメンバーに依存しスケールできていない。

- プロトコルを理解したトラブルシュート
- Clos に対する詳細なモニタリング
- Clos の拡張(スイッチの新機種検証など)

18

Background:

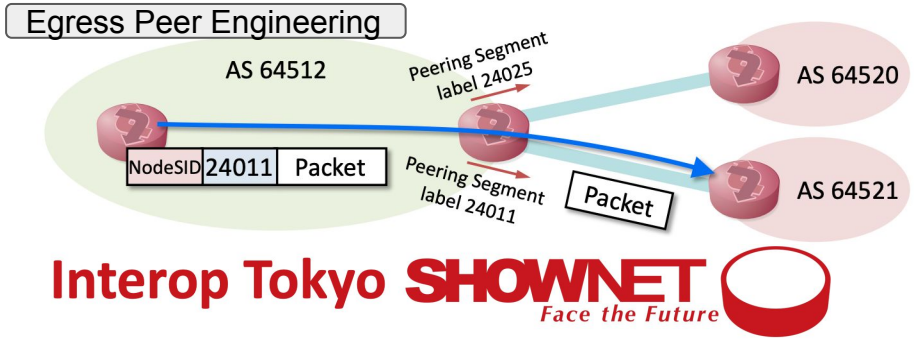
Clos Network Topology is scale-out data center network using BGP, which is being used by several services in Japan.
He made Clos Network Topology implementation with LXC and BIRD to learn by himself.

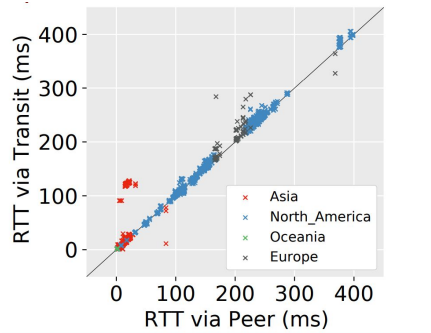
Summary of the presentation:

- Knowledge to operate Clos Network Topology is different from traditional BGP operation
- A lively discussion ensued on how best to educate the team to scale the operational structure and be able to troubleshoot with an understanding of protocols and detailed monitoring of Clos topology.

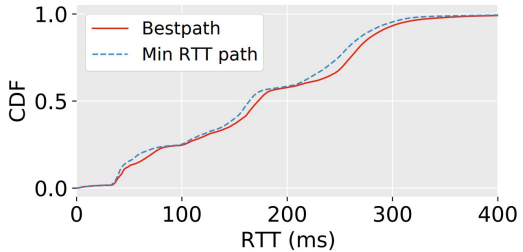
Measuring Internet Latency with SR-MPLS Egress Peer Engineering

JANOG48: 2021 Jul. Speaker: Ryo Nakamura(The University of Tokyo/Interop Tokyo ShowNet NOC Team)





RTT: Peer vs. Transit



Are BGP bestpaths really minimum RTT path?

Background:

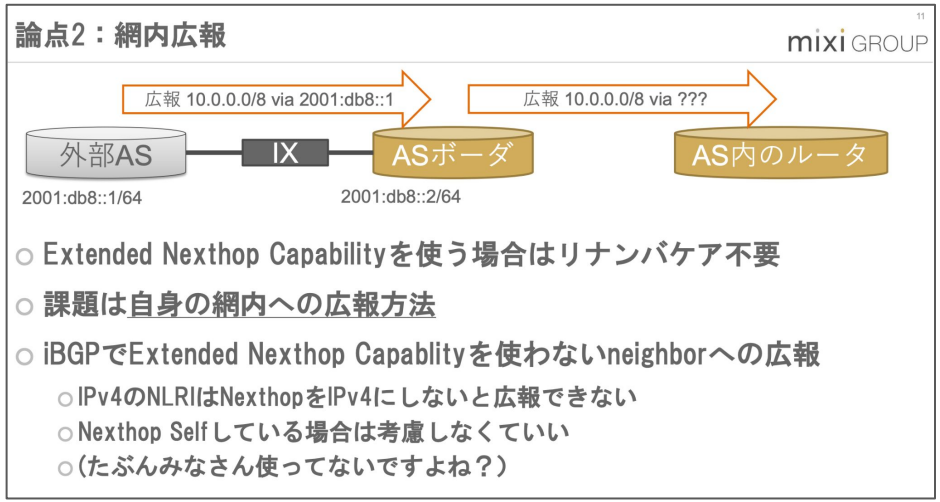
- Segment routing Egress Peer Engineering (EPE) is expected to enable flexible Internet traffic engineering.

Summary of the presentation:

- Presentation on the results of a study on Internet latency using SR-MPLS EPE conducted at Interop Tokyo 2021
  - Latency study: Peer vs. Transit
  - Study on whether BGP best path is really the minimal RTT path.
  - As an overall result, it was confirmed that Internet latency can be shortened by using EPE.

BGP peering over IX with RFC5549

JANOG49: 2022 Jan.　Speaker: Junpei Yoshino(mixi,Inc)



Background

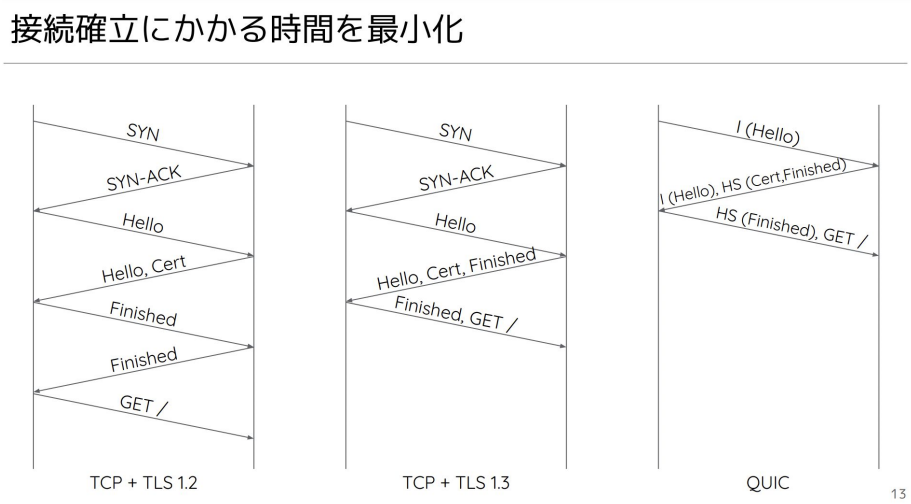
- IX IPv4 renumber is a bother
- “RFC5549 Advertising IPv4 NLRI with an IPv6 Next Hop” in NANOG56

Summary

- Share testing results and config samples
- difference with next-hop-self and without

Let's talk about QUIC

JANOG49: 2022 Jan.　Speaker: Yuya Kawakami(SoftBank Corp.), Kazuho Oku(Fastly K.K.)



Background:

QUIC is a new encrypted UDP-based transport layer protocol.
Due to support by web browsers and contents, use of QUIC is spreading.

Summary of the presentation:

- They explained from QUIC’s design philosophy and implementation to its impact on network operation deeply.
- Use of QUIC may cause problems with existing network infrastructure. In particular, the CGNAT NAT table overflow issue was analyzed and discussed.