RPKI: Actions Required by HK Networks

Che-Hoo Cheng

APNIC

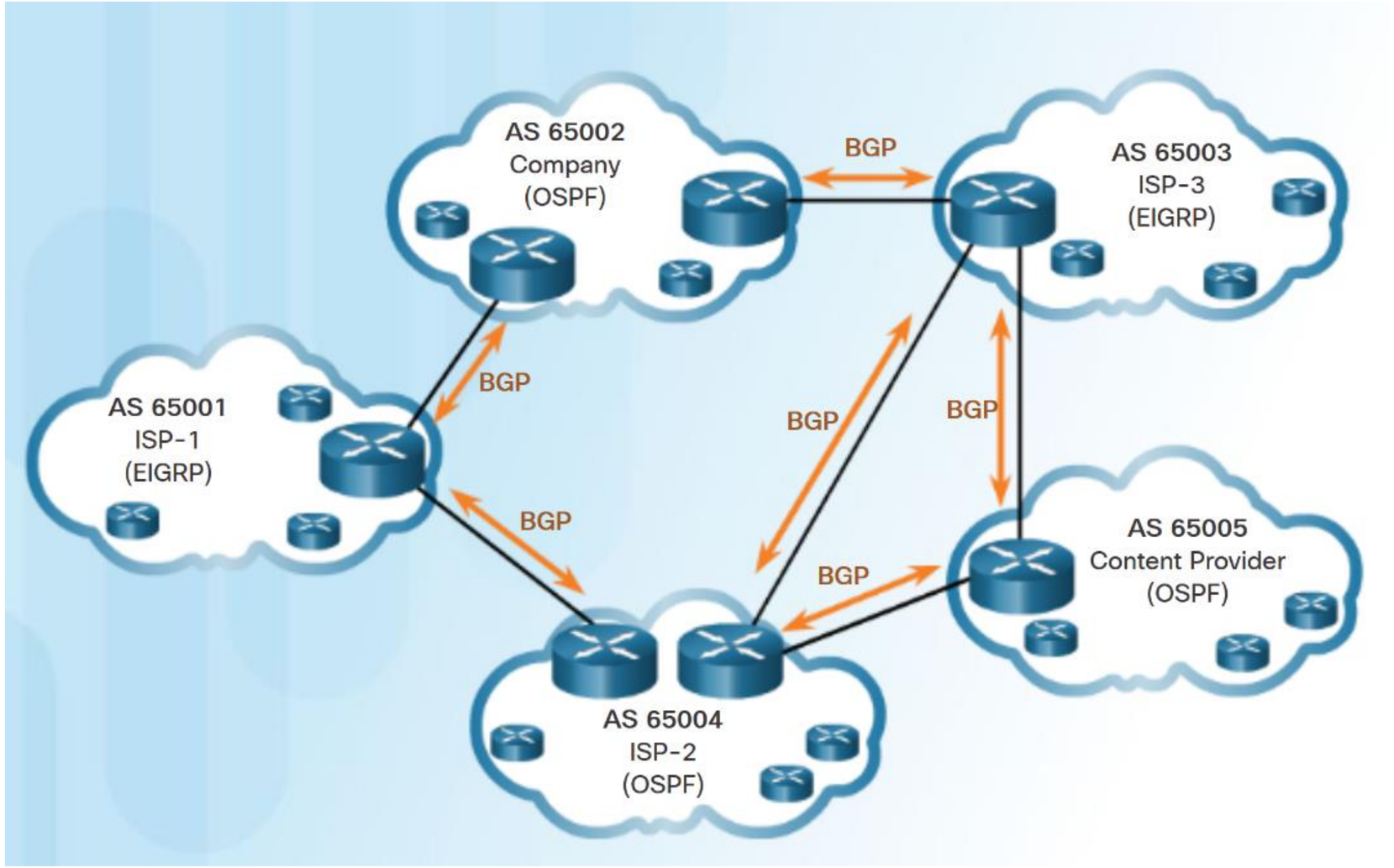
2023-10-30

@HKNOG 12.0

Agenda

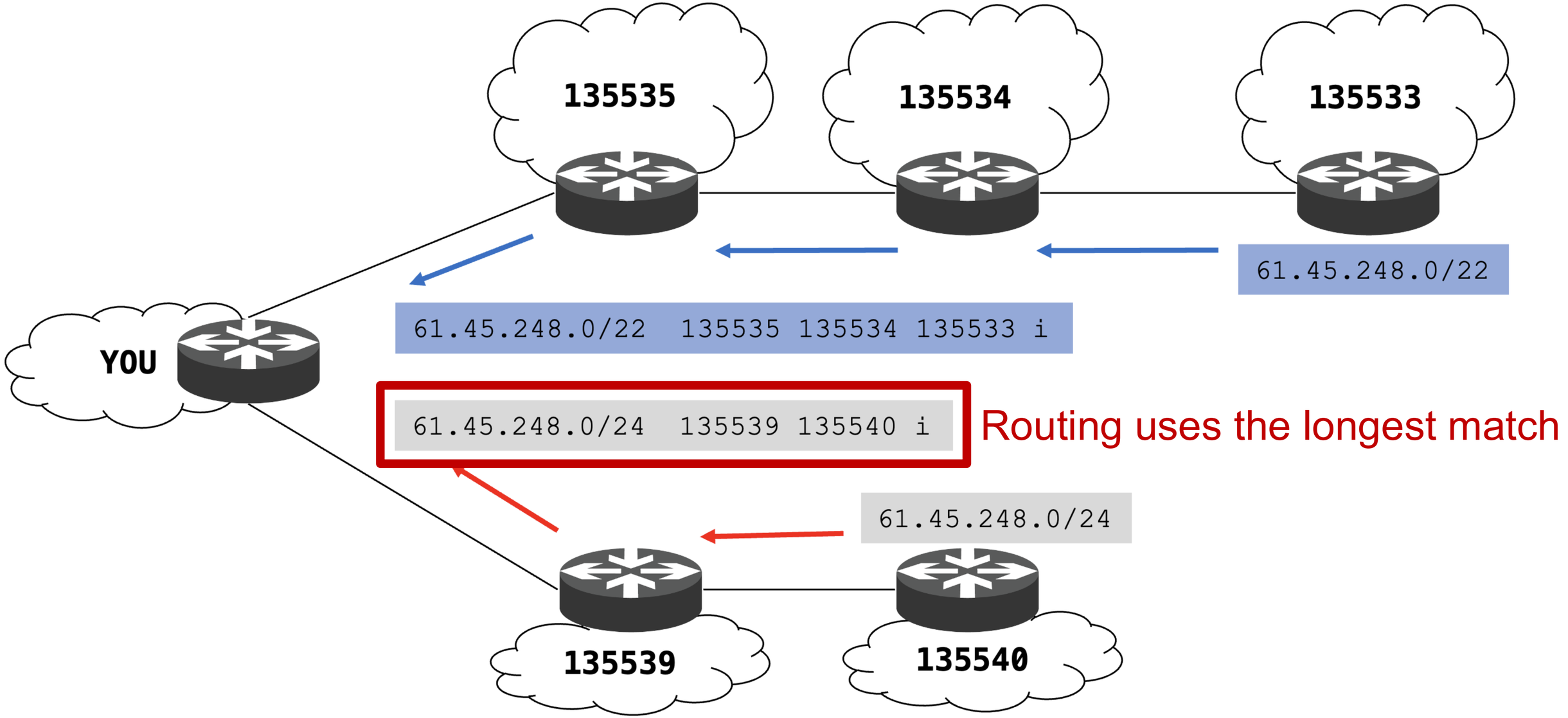
- Internet Routing and BGP Hijack
- What is RPKI?
- ROA Coverage in Asia / Eastern Asia / Hong Kong
- Common Issues after ROA Creation
- ROV Adoption in Hong Kong
- Recommendations

Internet Routing

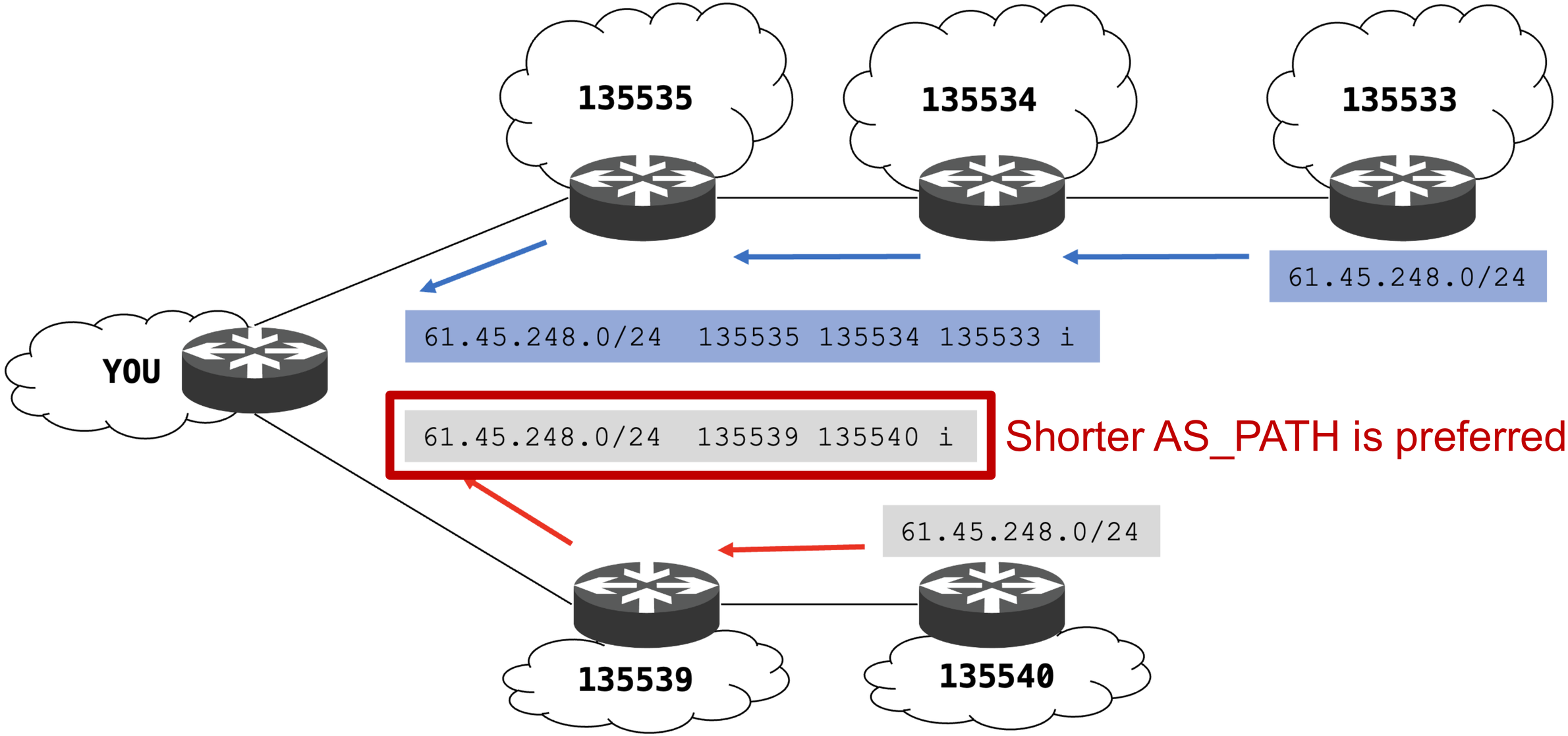


Source: Screenshot taken from “3.5.3.4 Packet Tracer - Configure and Verify eBGP.pka” example from Connecting Networks Cisco Networking Academy course

Internet Routing



Internet Routing



BGP Hijack

- Definition:
  - Announcing a more specific path
  - Announcing an address space that is owned by someone else
- Impacts:
  - Rerouting traffic to a malicious network
  - Enabling interception and alteration of sensitive data
  - Causing network unavailability

Source: Williams, R. (2015). street signs being stolen [Image]. https://media.apnarm.net.au/media/images/2015/02/06/IQT_06-02-2015_NEWS_05_STOLENSIGNS1_t1880.jpg

What is RPKI?

- Resource Public Key Infrastructure.

Route Origin Authorisation (ROA)

Resource holders permit specific ASes to originate their prefixes

Route Origin Validation (ROV)

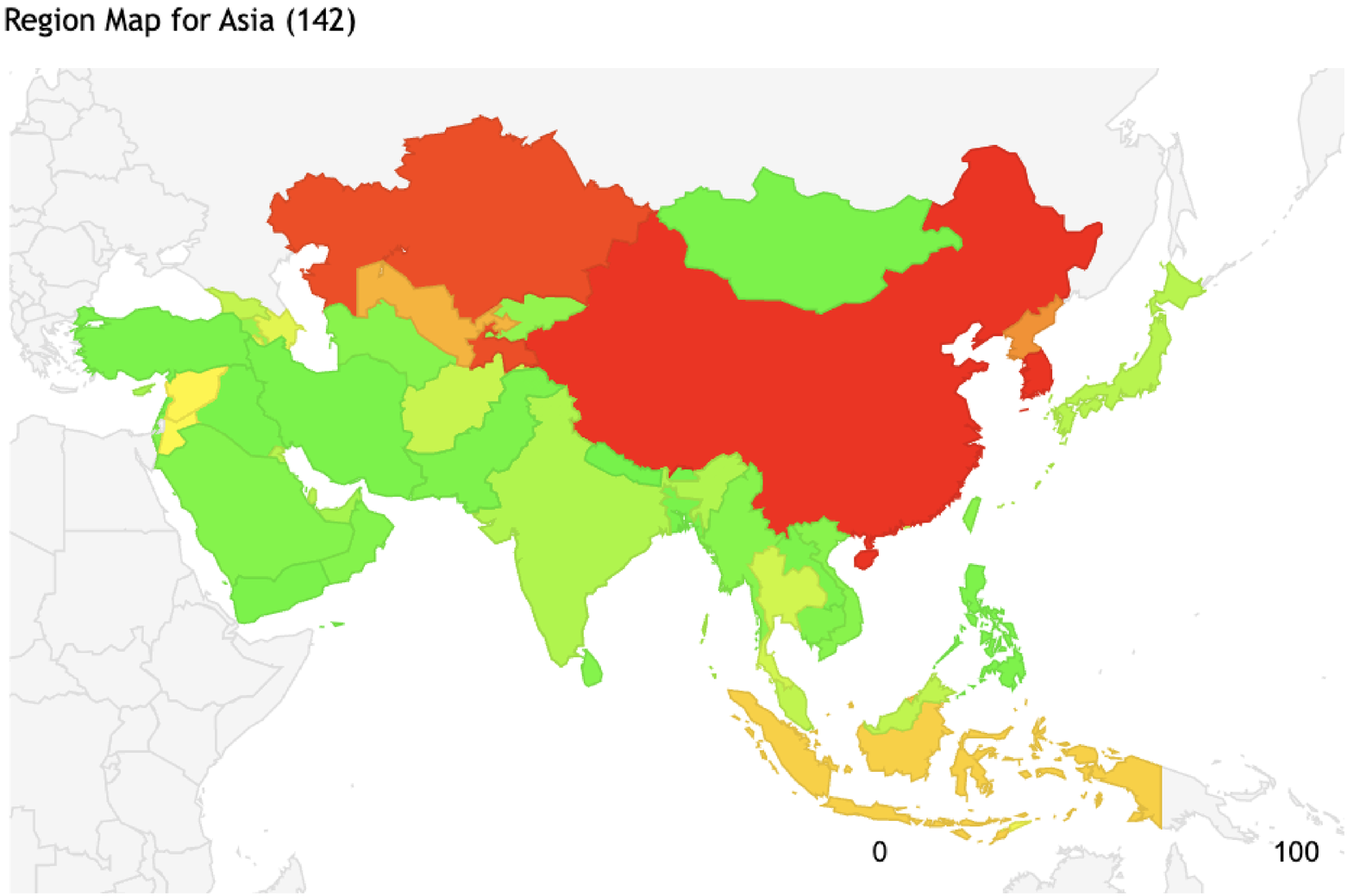
Other networks check whether the received prefixes are originated by the permitted ASes

- For mitigating BGP certain kinds of route hijacks and leaks.
- Applicable to both IPv4 and IPv6.
- ROA and ROV are done cryptographically.
  - Resource holders use private key to sign authorisations
  - Other networks use public key to validate the signatures

Route Origin Authorisation (ROA)

- To be done by resource holder:
  - Creating ROA for prefixes belong to own IPv4/IPv6 address space
    - Prefix
    - Origin AS
    - Max. Length
      - Also known as “Most Specific Announcement (MSA)”
  - APNIC members can create ROA in MyAPNIC portal
    - APNIC Help Centre: ROA objects
      - https://help.apnic.net/s/article/roa-objects
    - Route Management – Guide to manage your routes and (RPKI) ROA
      - https://www.apnic.net/wp-content/uploads/2017/01/route-roa-management-guide.pdf
    - How to Create ROAs in MyAPNIC
      - https://www.youtube.com/watch?v=NLG2siznuu4

ROA Coverage in Asia



Source: https://stats.labs.apnic.net/roa/XD (13 Oct 2023)

ROA Coverage in Asia

Code	Region	IPv4 Valid		IPv4 Invalid		IPv4 Unknown		IPv4 Total
BT	Bhutan, Southern Asia	36,864	98.60%	0	0.00%	512	1.40%	37,376
NP	Nepal, Southern Asia	567,552	98.40%	0	0.00%	9,472	1.60%	577,024
LB	Lebanon, Western Asia	525,056	97.30%	256	0.00%	14,336	2.70%	539,648
BD	Bangladesh, Southern Asia	1,684,916	95.90%	11,089	0.60%	60,672	3.50%	1,756,677
IQ	Iraq, Western Asia	699,904	95.60%	2,816	0.40%	29,440	4.00%	732,160
…								
KP	Democratic People's Republic of Korea, Eastern Asia	512	28.60%	0	0.00%	1,280	71.40%	1,792
TJ	Tajikistan, Central Asia	10,496	12.70%	256	0.30%	71,936	87.00%	82,688
KZ	Kazakhstan, Central Asia	400,895	12.40%	1	0.00%	2,822,400	87.60%	3,223,296
CN	China, Eastern Asia	6,680,094	2.20%	441,826	0.10%	293,030,722	97.60%	300,152,642
KR	Republic of Korea, Eastern Asia	1,885,985	1.70%	1,247	0.00%	106,613,542	98.30%	108,500,774
XD	**Asia**	**318,136,632**	**38.40%**	**3,108,393**	**0.40%**	**507,084,926**	**61.20%**	**828,329,951**

Source: https://stats.labs.apnic.net/roa/XD (13 Oct 2023)

ROA Coverage in Eastern Asia

Source: https://stats.labs.apnic.net/roa/XS (13 Oct 2023)

ROA Coverage in Eastern Asia

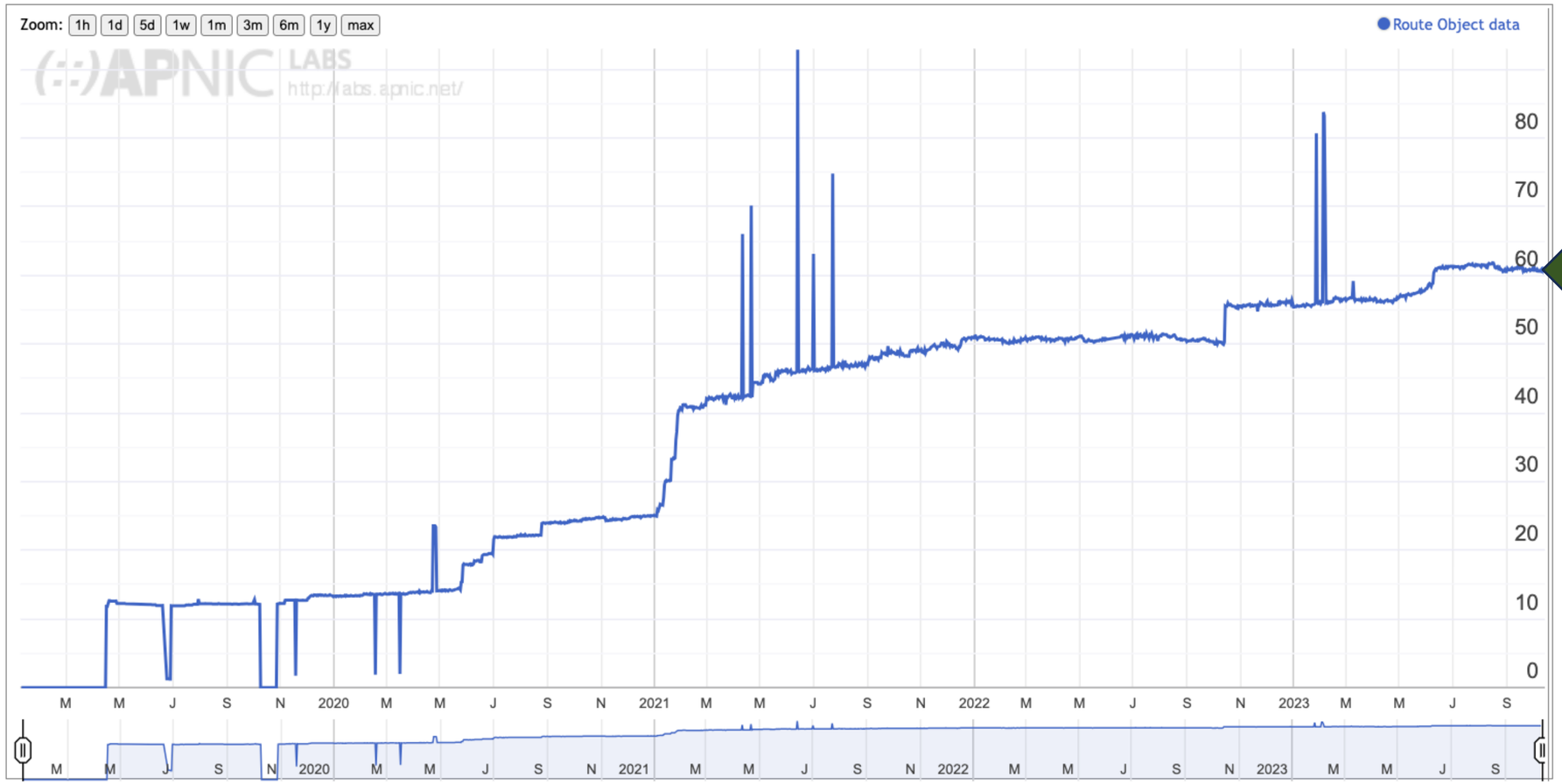
Code	Region	IPv4 Valid		IPv4 Invalid		IPv4 Unknown		IPv4 Total
MN	Mongolia	181,727	94.60%	289	0.20%	9,984	5.20%	192,000
MO	Macao Special Administrative Region of China	336,896	86.40%	256	0.10%	52,992	13.60%	390,144
TW	Taiwan	29,463,342	86.20%	1,082,546	3.20%	3,650,338	10.70%	34,196,226
JP	Japan	123,748,089	70.20%	371,080	0.20%	52,246,976	29.60%	176,366,145
HK	Hong Kong Special Administrative Region of China	12,251,612	61.30%	55,863	0.30%	7,687,852	38.40%	19,995,327
KP	Democratic People's Republic of Korea	512	28.60%	0	0.00%	1,280	71.40%	1,792
CN	China	6,680,094	2.20%	441,826	0.10%	293,030,722	97.60%	300,152,642
KR	Republic of Korea	1,885,985	1.70%	1,247	0.00%	106,613,542	98.30%	108,500,774
XS	**Eastern Asia**	**174,548,257**	**27.30%**	**1,953,107**	**0.30%**	**463,293,686**	**72.40%**	**639,795,050**

Source: https://stats.labs.apnic.net/roa/XS (13 Oct 2023)

ROA Coverage in Hong Kong

Use of Route Object Validation for Hong Kong Special Administrative Region of China (HK)

Display: **Addresses** (Advertised ROA-Valid Advertised Addresses), **IPv4**, **Percent** (of Total)



Currently (Oct 2023) **61.30%** of Hong Kong's IPv4 addresses have VALID ROA.

Address Span | Valid
IPv4 | Percent

Hide country ASN List
Hide Regional Use
Redraw

JSON Data Set

CSV Data Set

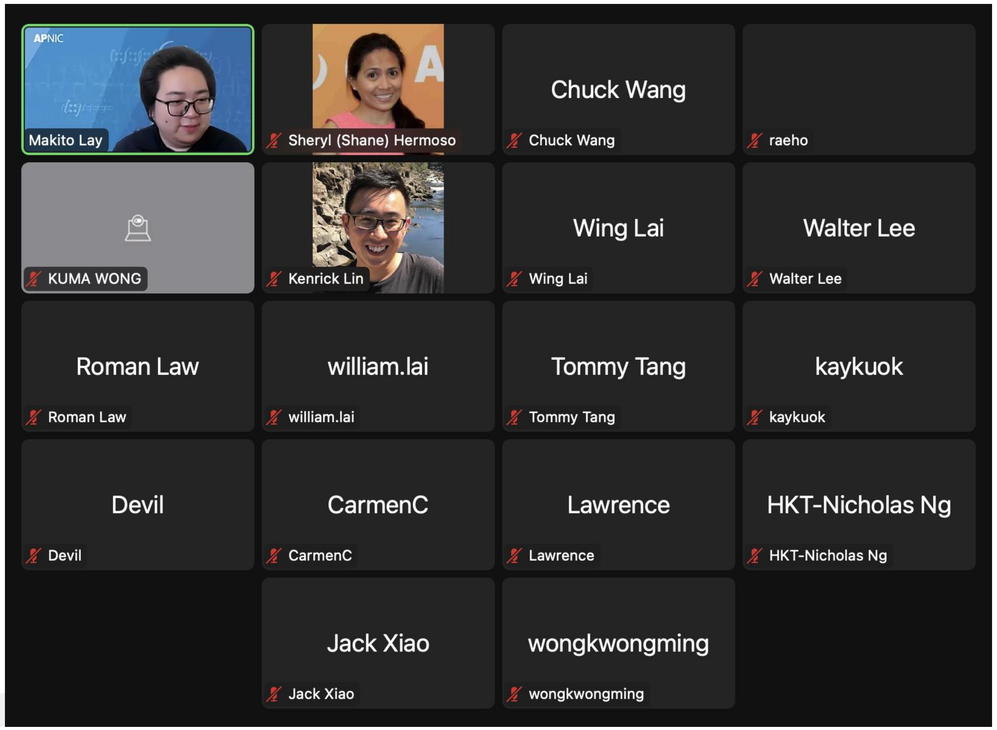
Source: https://stats.labs.apnic.net/roa/HK (13 Oct 2023)

ROA Coverage in Hong Kong

ASN	AS Name	IPv4 Valid		IPv4 Invalid		IPv4 Unknown		IPv4 Total
9304	HUTCHISON-AS-AP HGC Global Communications Limited	23,282	1.60%	268	0.00%	1,465,093	98.40%	1,488,643
4515	ERX-STAR HKT Limited	94,208	15.00%	4	0.00%	535,042	85.00%	629,254
134548	DXTL-HK DXTL Tseung Kwan O Service	0	0.00%	0	0.00%	286,464	100.00%	286,464
132203	TENCENT-NET-AP-CN Tencent Building, Kejizhongyi Avenue	226,804	45.20%	12	0.00%	274,688	54.80%	501,504
4058	CITICTEL-CPC-AS4058 CITIC Telecom International CPC Limited	768	0.30%	0	0.00%	248,321	99.70%	249,089
134175	SH2206-AP UNIT A17,9F SILVERCORP INTL TOWER 707-713 NATHAN RD	0	0.00%	0	0.00%	231,424	100.00%	231,424
135097	MYCLOUD-AS-AP LUOGELANG FRANCE LIMITED	89,600	28.00%	0	0.00%	230,400	72.00%	320,000
136800	MOACKCOLTD-AS-AP MOACK.Co.LTD	1,024	0.50%	0	0.00%	223,230	99.50%	224,254
9293	HKNET-VIPNET NTT Com Asia Limited	0	0.00%	0	0.00%	207,872	100.00%	207,872
62325	HD	0	0.00%	0	0.00%	186,112	100.00%	186,112
35916	MULTA-ASN1	512	0.30%	0	0.00%	158,715	99.70%	159,227
328608	Africa-on-Cloud-AS	32,768	17.50%	5,888	3.20%	148,220	79.30%	186,876
16625	AKAMAI-AS	0	0.00%	0	0.00%	146,944	100.00%	146,944
…								

Source: https://stats.labs.apnic.net/roa/HK (13 Oct 2023)

Online RPKI Sessions & Technical Assistance



- In August, APNIC delivered online RPKI session to HK and MO members in Cantonese for the first time (more to come).
- One-to-one technical assistance in Cantonese is available.

Common Issues after ROA Creation

- Invalid Origin AS
  - Multiple origin ASes in Anycast scenario
    - Solution: Create ROA for each and every origin AS
  - Prefixes are originated by a different AS
    - Solution: Create ROA with the actual origin AS
- Invalid Prefix Length
  - Announcing /24s, but ROA covers only up to /23
    - Solution: Set Max. Length of the ROA to “/24”

What's Next after Having ROA?

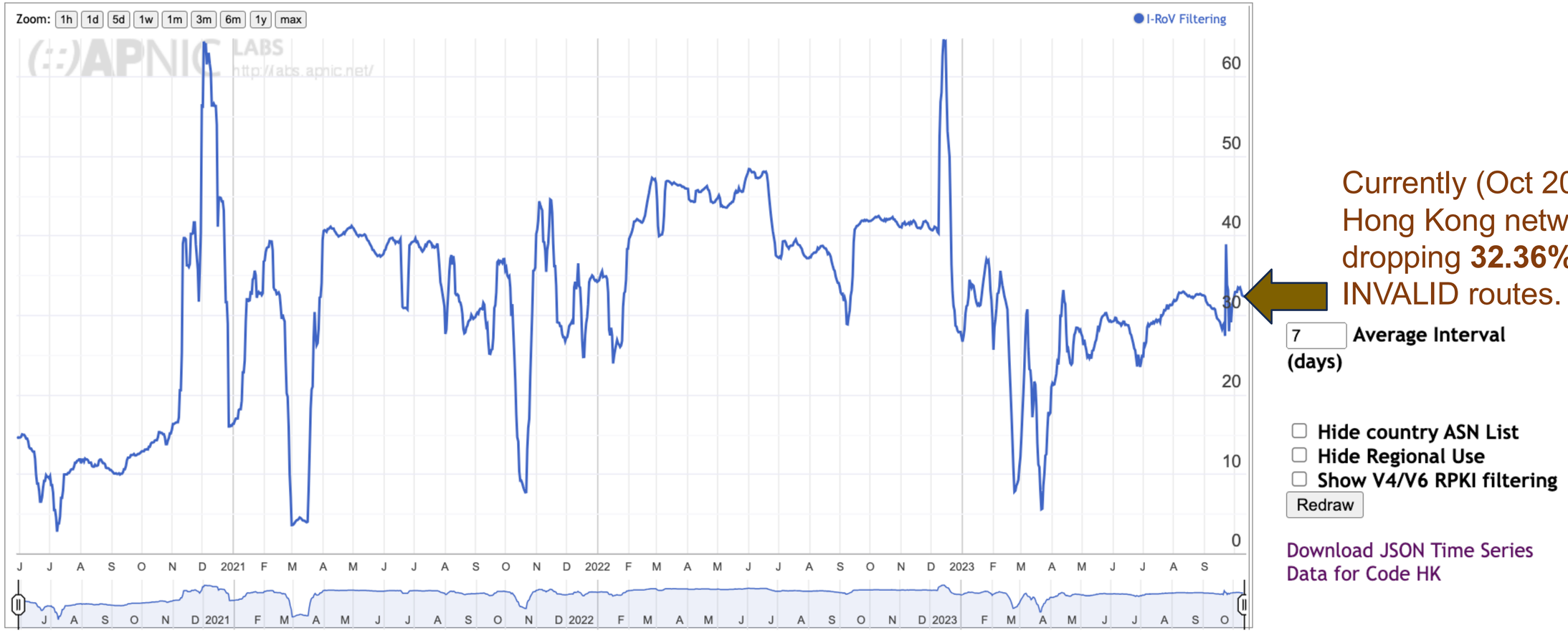
- ROA is an authorisation that permits a specific AS to originate a specific prefix.
- ROAs are created for other networks to perform ROV.
- The authorisation is meaningless if no one validates it.
- All networks should eventually implement ROV.
- ROV for IPv6 is as important as IPv4.

Route Origin Validation (ROV)

- Should be done by all networks on the Internet:
  - Setting up RPKI Validators
  - Configuring Border Routers to validate received IPv4/IPv6 prefixes
    - VALID
      - ROA exists, both origin AS and prefix length match with the record
    - INVALID
      - ROA exists, but origin AS or/and prefix length mismatch with the record
    - UNKNOWN / NOT FOUND
      - ROA does not exist
  - Implementing routing policies based on validation state
    - Prefer VALID over UNKNOWN over INVALID; or
    - Drop INVALID

ROV Adoption in Hong Kong

Use of RPKI Validation for Hong Kong Special Administrative Region of China (HK)



Currently (Oct 2023) Hong Kong networks are dropping **32.36%** of INVALID routes.

7 **Average Interval (days)**

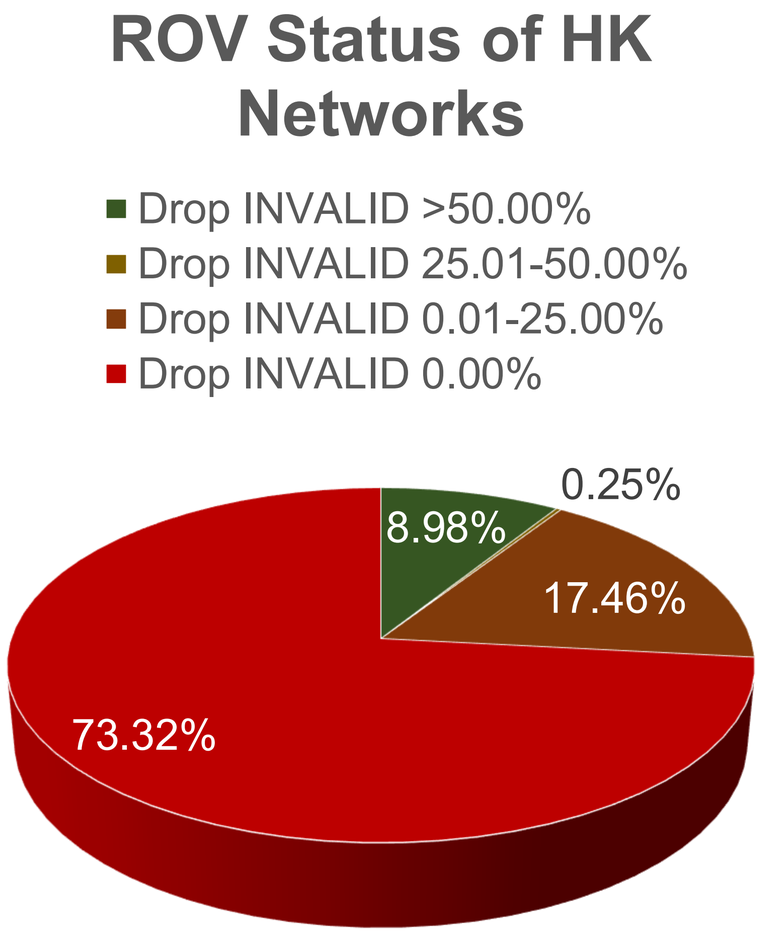
- ☐ **Hide country ASN List**
- ☐ **Hide Regional Use**
- ☐ **Show V4/V6 RPKI filtering**

Redraw

Download JSON Time Series Data for Code HK

Source: https://stats.labs.apnic.net/rpki/HK (13 Oct 2023)

ROV Adoption in Hong Kong



- Among 401 sample networks:
  - 36 networks (8.98%) are dropping more than 50.00% of INVALID routes
  - 1 network (0.25%) is dropping 25.01% to 50.00% of INVALID routes
  - 70 networks (17.46%) are dropping 0.01% to 25.00% of INVALID routes
  - 294 networks (73.32%) do not appear to be dropping INVALID route at all
- More actions need to be taken.

Source: https://stats.labs.apnic.net/rpki/HK (13 Oct 2023)

Major Networks Dropping INVALID

ASN	Network Name	Source
1221	Telstra	https://lists.ausnog.net/pipermail/ausnog/2020-July/044367.html
4637		https://www.zdnet.com/article/telstra-to-roll-out-rpki-routing-security-from-june-2020/
1239	Sprint / T-Mobile	https://www.sprint.net/policies/bgp-aggregation-and-filtering
1299	Telia	https://www.teliacarrier.com/Our-Network/BGP-Routing/Routing-Security.html
2497	IIJ	https://www.iij.ad.jp/en/dev/iir/pdf/iir_vol50_focus1_EN.pdf
2914	NTT	https://www.gin.ntt.net/support/policy/rr.cfm#RPKI
3356	Level3	https://twitter.com/lumentechco/status/1374035675742412800
4826	Vocus	https://blog.apnic.net/2021/05/13/vocus-rpki-implementation/
6939	Hurricane Electric	https://mailman.nanog.org/pipermail/nanog/2020-June/108277.html
7018	AT&T	https://mailman.nanog.org/pipermail/nanog/2019-February/099501.html
7922	Comcast	https://corporate.comcast.com/stories/improved-bgp-routing-security-adds-another-layer-of-protection-to-network
9002	RETN	https://twitter.com/RETNnet/status/1333735456408793089
16509	Amazon	https://aws.amazon.com/blogs/networking-and-content-delivery/how-aws-is-helping-to-secure-internet-routing/
37100	Seacom	https://www.ripe.net/participate/mail/forum/routing-wg/PDZlMzAzMzhhLWVhOTAtNzIxOC1lMzI0LTBjZjMyOGI1Y2NkM0BzZWFjb20ubXU+
…		

Source: https://taejoong.github.io/pubs/publications/li-2023-rov.pdf (13 Oct 2023)

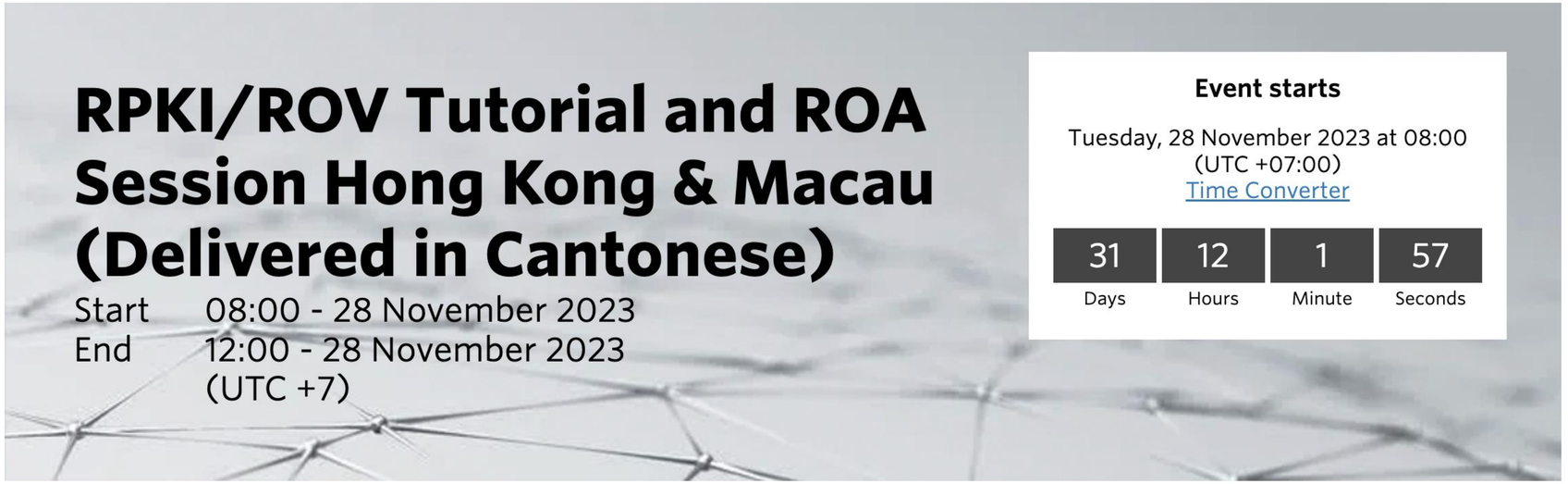
Recommendations

- Create ROAs for all your prefixes.
  - Origin AS and Max. Length must match actual BGP announcements
    - Ensure ROAs are up-to-date upon sub-assignments
  - Multiple ROAs with different Origin ASes for Anycast prefixes
  - For networks using leased IPv4 address space, request your lease provider to create relevant ROAs
    - Regardless whether the address space is in APNIC region
- Advise your customers and peers to sign their prefixes.
  - Unlike Internet Routing Registry (IRR), ROA cannot be proxy-registered
- Monitor whether your network is announcing INVALID.

Recommendations

- Implement ROV in your network.
  - Especially if you do a lot of peering
  - Employ at least two RPKI Validators for redundancy purpose
    - Ensure consistency across all RPKI Validators
  - Establish and secure RPKI-to-Router (RTR) sessions
  - Update routing policies to support ROV
    - Set LOCAL_PREF based on validation state, or drop INVALID (preferred)
    - Use BGP Communities to propagate validation state (optional)
  - For Internet Transit, receive full routing table and drop default route

Upcoming RPKI Training



YOUR TRAINERS

Makito Lay
Network Analyst / Technical Trainer

Makito has 18 years experience in ISP and Telecom industry, focusing on building technology solutions for service provider IP core, broadband access and datacenter networks. His expertise includes Routing & Switching technologies, IPv6, MPLS and ISP services. Makito is a founding member of Cambodia Network Operators Group

TU

START
Tue, 28 November 2023
08:00 (UTC +7)

END
Tue, 28 November 2023
12:00 (UTC +7)

Register

Switch Timezone: ON Showing browser local time (Asia/Phnom_Penh)

Course Overview | Course Materials

Target Audience

Anyone interested to understand the RPKI framework and how it helps secure Internet Routing.

Synopsis

- Why do we keep seeing news headlines about major networks not being reachable because traffic got rerouted to somewhere else? BGP mishaps are very common and frighteningly very

Need Help?

ROA Creation & General Enquiries

APNIC Help Centre
https://help.apnic.net/s

ROV Implementation & Technical Discussions

APNIC Technical Assistance Platform
https://academy.apnic.net/technical-assistance

Training Resources

APNIC Academy
https://academy.apnic.net

Online Courses:

- ❑ RPKI Deployment
- ❑ RPKI Deployment Status: 2022 in Review
- ❑ Historical Resource Management and the Benefits of RPKI
- ❑ Hosted vs. Delegated RPKI
- ❑ Demystifying AS0
- ❑ How to set up Router/OS 7 and ROV

Virtual Labs:

- ❑ RPKI Lab with Routinator
- ❑ RPKI Lab with FORT
- ❑ RPKI Lab with RPKI-Prover
- ❑ RPKI Lab (Sandbox)

RPKI: Actions Required by HK Networks

Questions & Answers