

# RPKI Status Updates

Presented by: Makito Lay

Phnom Penh, Cambodia | 22 October 2023

**KHNOG**  
*Cambodia Network Operators Group*

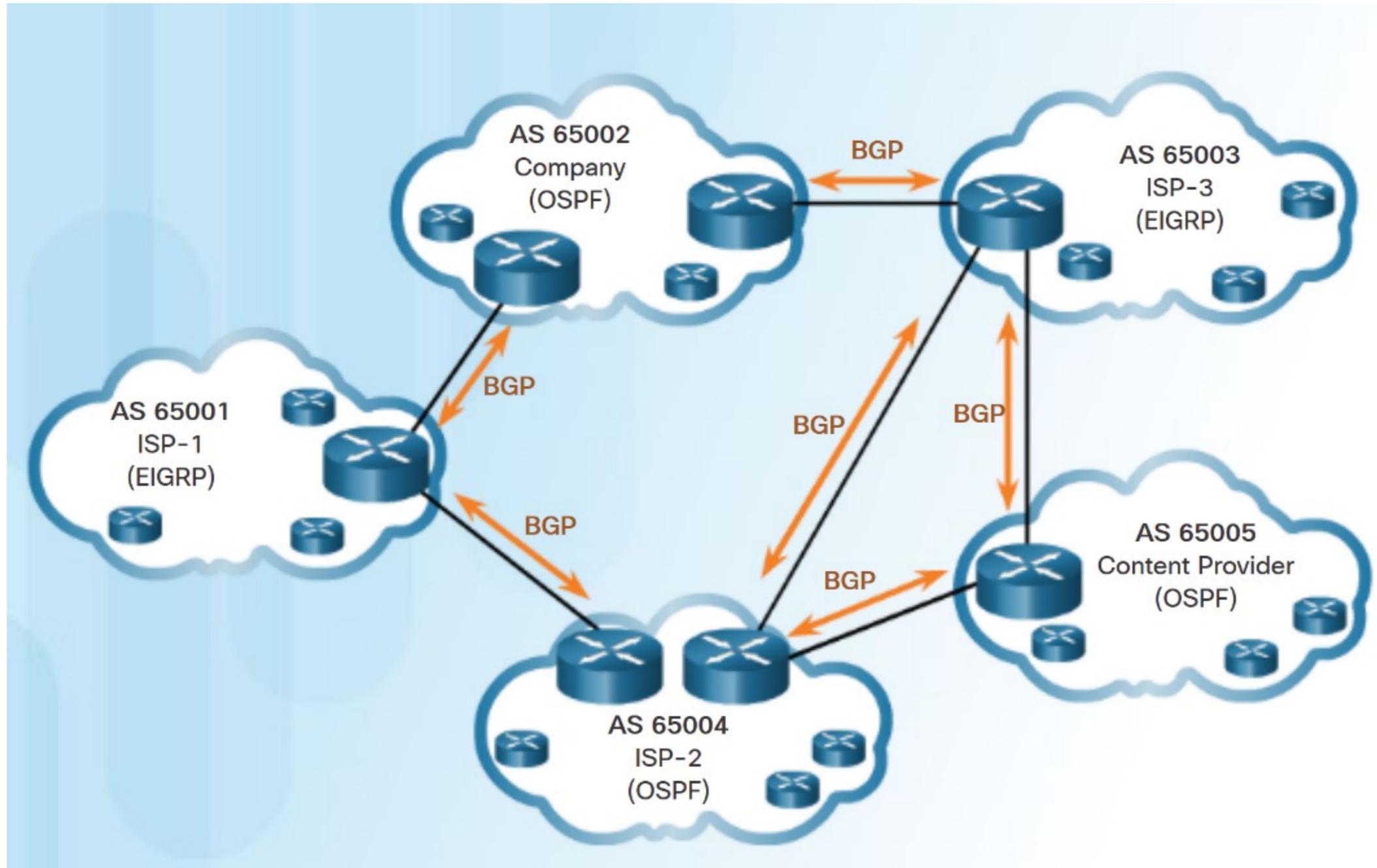
KHNOG 5 Conference

# Agenda



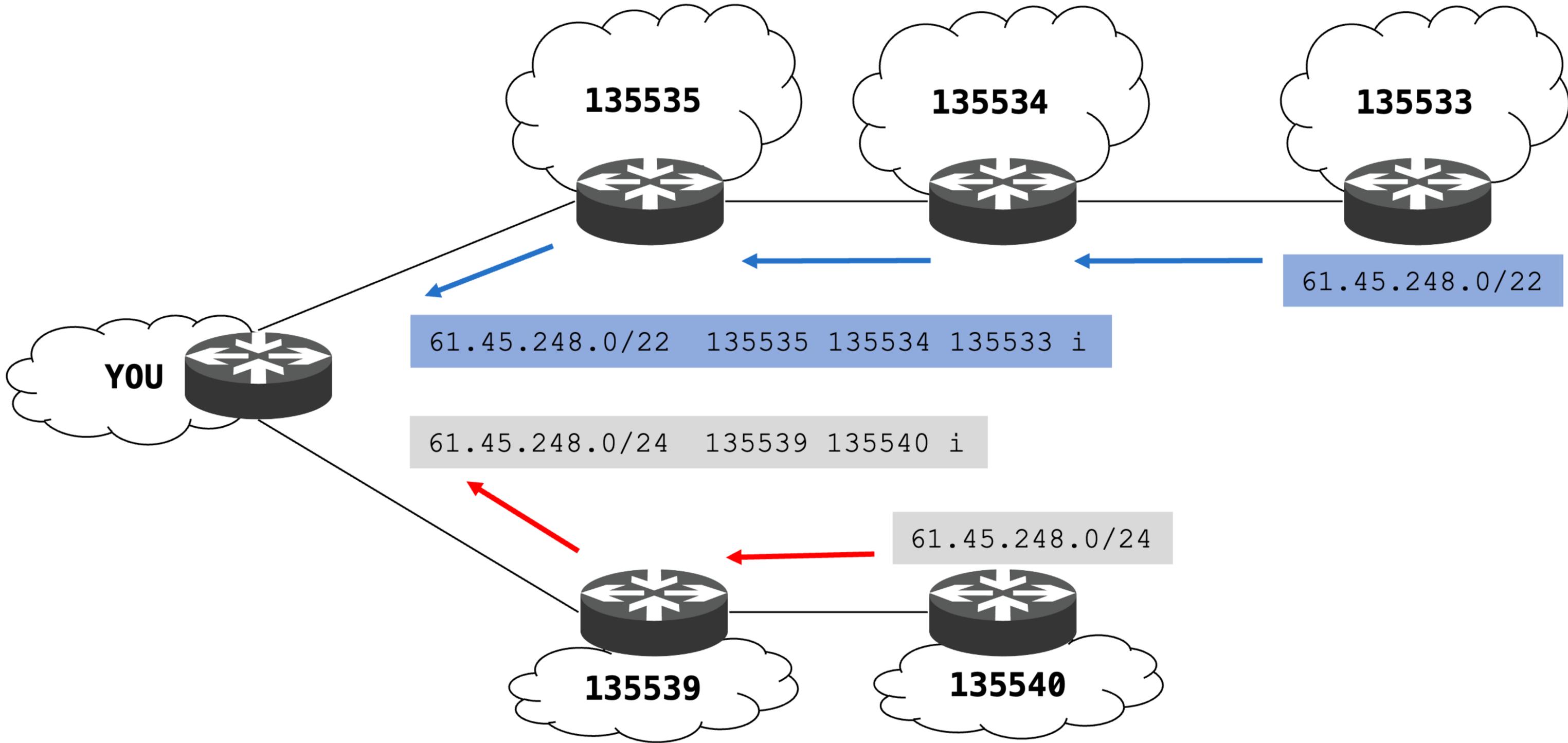
- Internet Routing and BGP Hijack
- What is RPKI?
- ROA Coverage in Asia / South-Eastern Asia / Cambodia
- Common Issues after ROA Creation
- ROV Adoption in Cambodia
- Recommendations

# Internet Routing

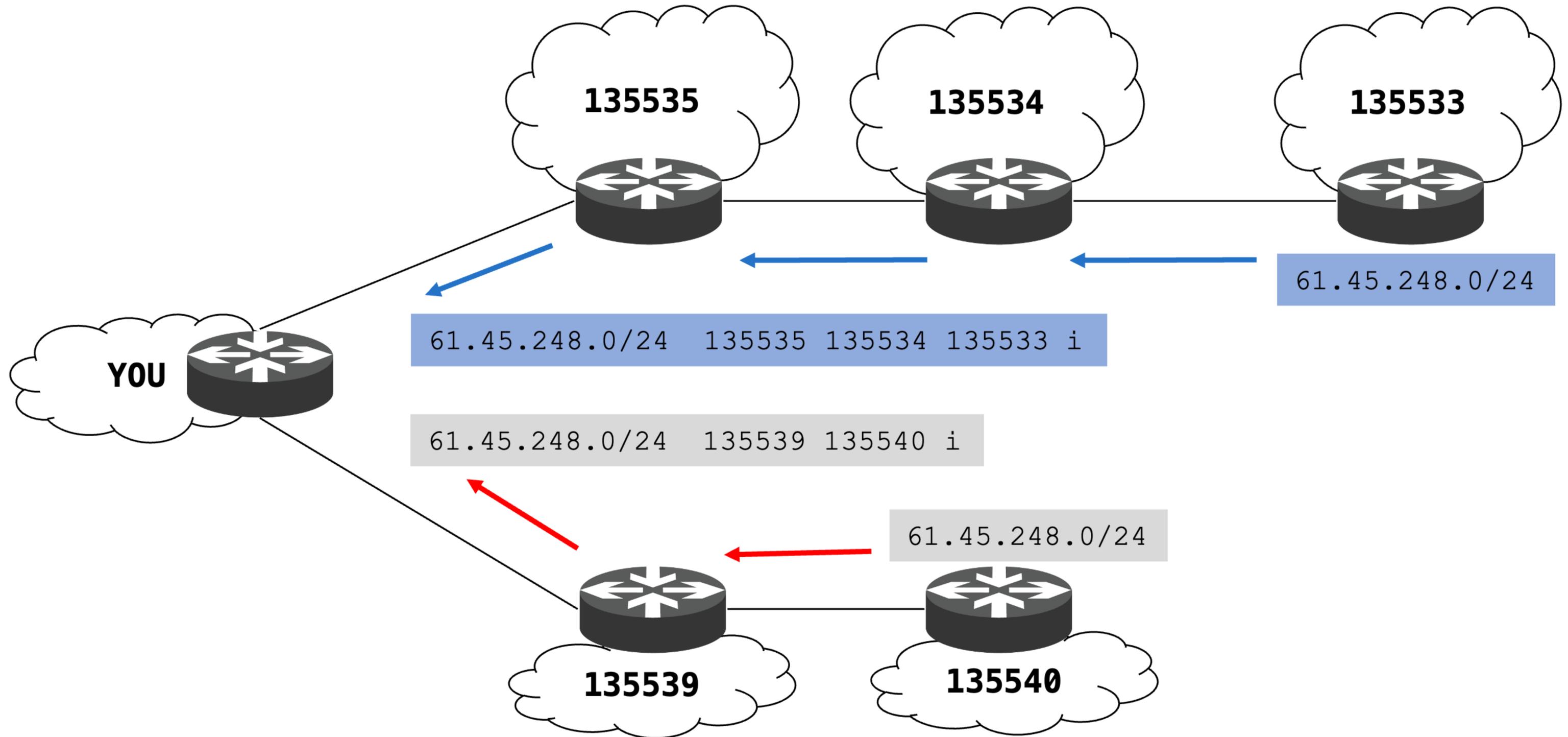


Source: Screenshot taken from “3.5.3.4 Packet Tracer - Configure and Verify eBGP.pka” example from Connecting Networks Cisco Networking Academy course

# Internet Routing



# Internet Routing



# BGP Hijack



- Announcing a more specific path.
- Announcing an address space that is owned by someone else.



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](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 AS to originate their prefixes

## Route Origin Validation (ROV)

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

- For mitigating BGP route leaks and hijacks.
- 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)

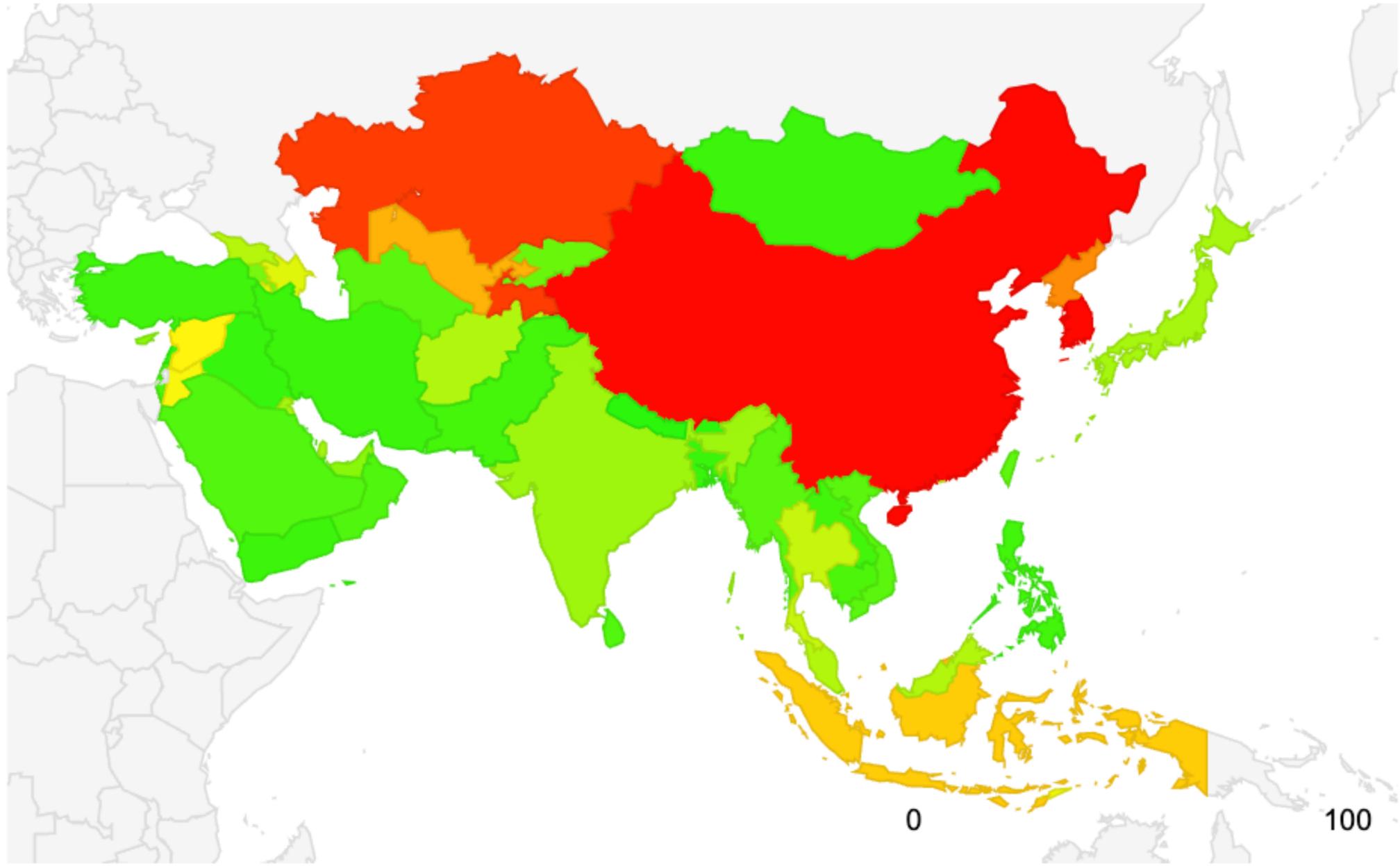


- To be done by resource holder:
  - Creating ROA for prefixes belong to own address space
    - Prefix
    - Origin AS
    - Max. Length
      - Also known as “Most Specific Announcement (MSA)”
  - APNIC members can create ROA in MyAPNIC portal
    - APNIC Help Centre: ROA objects
      - <https://help.apnic.net/s/article/roa-objects>
    - 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



Region Map for Asia (142)



Source: <https://stats.labs.apnic.net/roa/XD> (11 Oct 2023)

# ROA Coverage in Asia



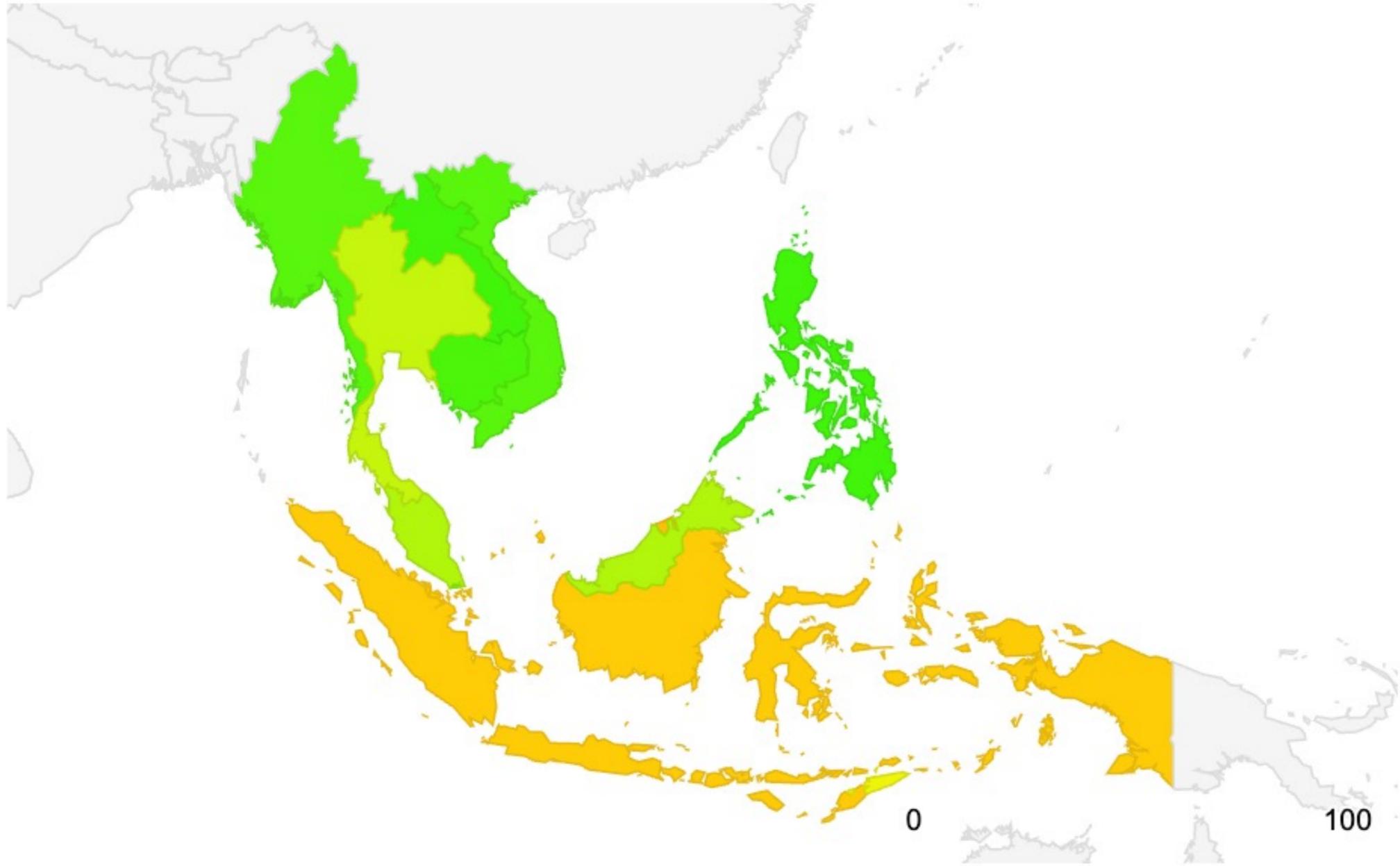
Code	Region	IPv4 Valid		IPv4 Invalid		IPv4 Unknown		IPv4 Total
BT	Bhutan, Southern Asia	36,864	98.60%	0	0.00%	512	1.40%	37,376
NP	Nepal, Southern Asia	568,064	98.50%	0	0.00%	8,448	1.50%	576,512
LB	Lebanon, Western Asia	522,496	96.80%	256	0.00%	17,152	3.20%	539,904
IQ	Iraq, Western Asia	700,160	95.60%	2,816	0.40%	29,440	4.00%	732,416
BD	Bangladesh, Southern Asia	1,690,553	95.50%	11,596	0.70%	67,840	3.80%	1,769,989
...								
KP	Democratic People's Republic of Korea, Eastern Asia	512	28.60%	0	0.00%	1,280	71.40%	1,792
KZ	Kazakhstan, Central Asia	400,639	12.40%	1	0.00%	2,823,936	87.60%	3,224,576
TJ	Tajikistan, Central Asia	10,240	12.40%	256	0.30%	72,192	87.30%	82,688
CN	China, Eastern Asia	6,642,723	2.20%	441,821	0.10%	293,069,122	97.60%	300,153,666
KR	Republic of Korea, Eastern Asia	1,869,346	1.70%	1,246	0.00%	106,616,870	98.30%	108,487,462
<b>XD</b>	<b>Asia</b>	<b>317,547,608</b>	<b>38.40%</b>	<b>3,244,556</b>	<b>0.40%</b>	<b>507,154,555</b>	<b>61.30%</b>	<b>827,946,719</b>

Source: <https://stats.labs.apnic.net/roa/XD> (11 Oct 2023)

# ROA Coverage in South-Eastern Asia



Region Map for South-Eastern Asia (035)



Source: <https://stats.labs.apnic.net/roa/XU?o=v4tadpl1> (11 Oct 2023)

# ROA Coverage in South-Eastern Asia



Code	Region	IPv4 Valid		IPv4 Invalid		IPv4 Unknown		IPv4 Total
LA	Lao People's Democratic Republic	76,032	93.40%	512	0.60%	4,864	6.00%	81,408
PH	Philippines	5,746,856	93.40%	37,204	0.60%	369,668	6.00%	6,153,728
KH	Cambodia	393,211	90.70%	2,565	0.60%	37,632	8.70%	433,408
VN	Vietnam	14,055,297	87.70%	86,143	0.50%	1,879,040	11.70%	16,020,480
MM	Myanmar	175,872	87.60%	3,072	1.50%	21,760	10.80%	200,704
SG	Singapore	9,214,823	76.10%	124,856	1.00%	2,761,407	22.80%	12,101,086
MY	Malaysia	4,200,082	67.40%	20,339	0.30%	2,011,393	32.30%	6,231,814
TH	Thailand	5,679,029	63.10%	95,307	1.10%	3,232,512	35.90%	9,006,848
TL	Timor-Leste	9,216	53.70%	256	1.50%	7,680	44.80%	17,152
ID	Indonesia	7,509,802	41.50%	95,702	0.50%	10,487,552	58.00%	18,093,056
BN	Brunei Darussalam	57,088	38.90%	0	0.00%	89,856	61.10%	146,944
<b>XU</b>	<b>South-Eastern Asia</b>	<b>47,117,308</b>	<b>68.80%</b>	<b>465,956</b>	<b>0.70%</b>	<b>20,903,364</b>	<b>30.50%</b>	<b>68,486,628</b>

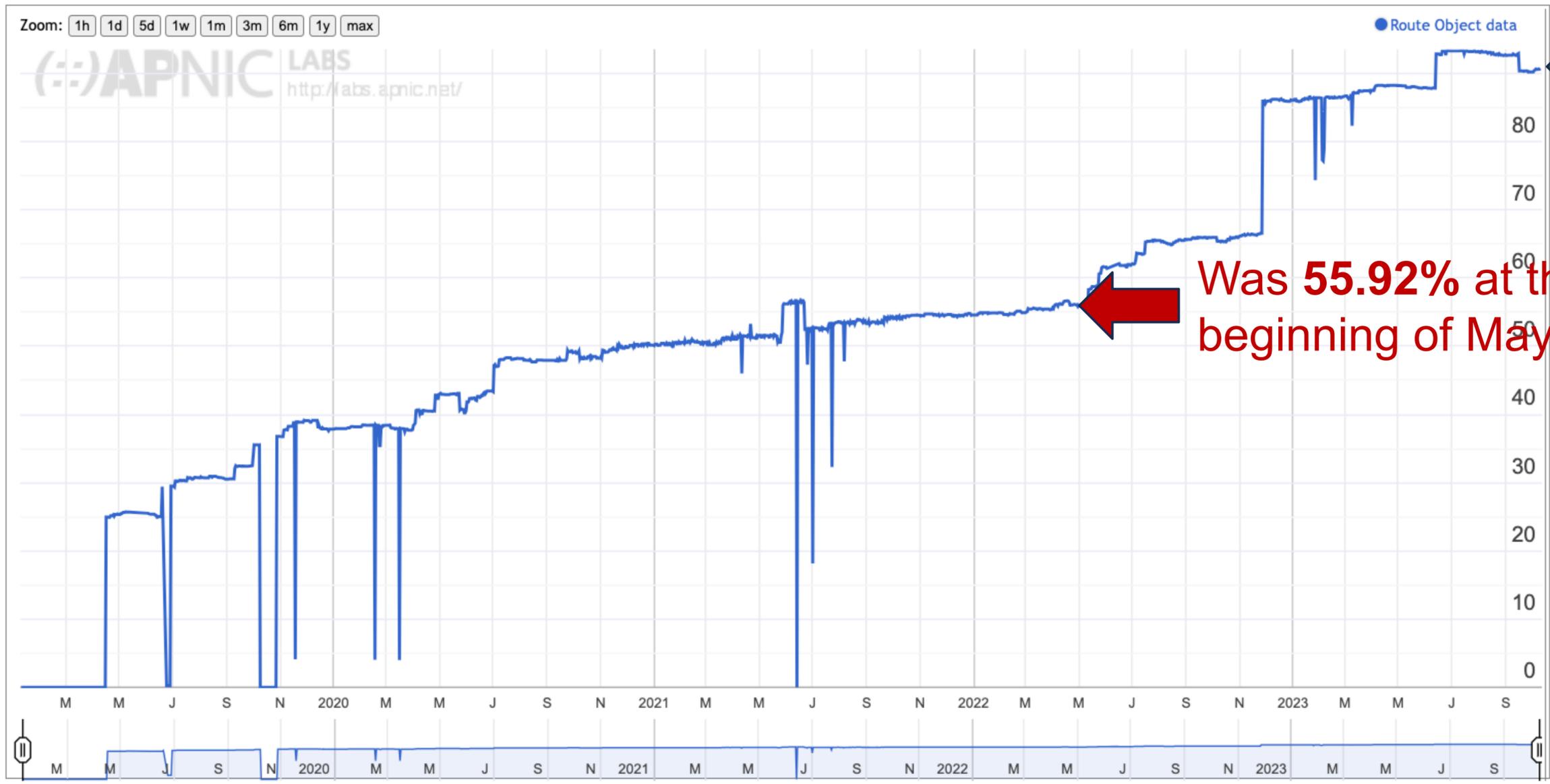
Source: <https://stats.labs.apnic.net/roa/XU?o=v4tadpl1> (11 Oct 2023)

# ROA Coverage in Cambodia



## Use of Route Object Validation for Cambodia (KH)

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

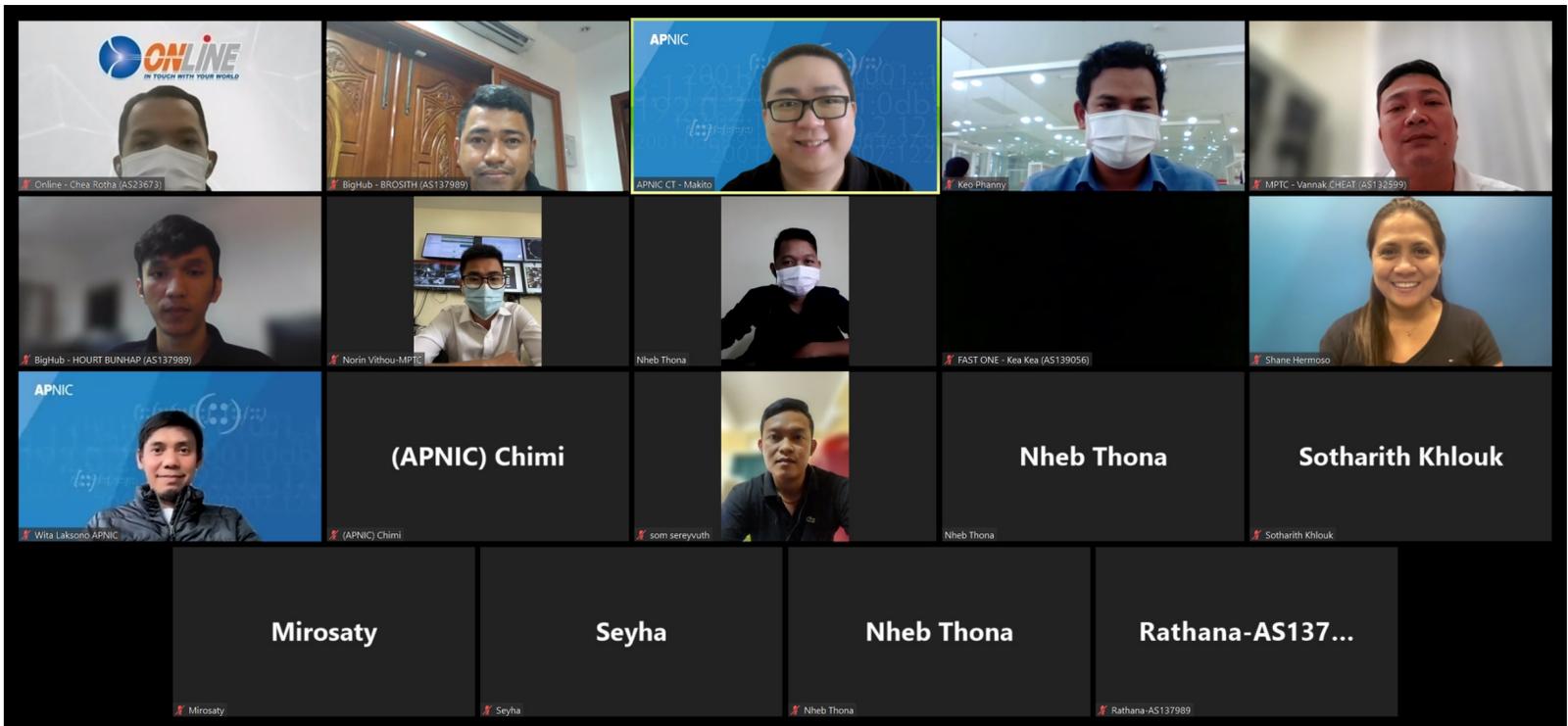


Currently (Oct 2023) 90.70% of Cambodia's IPv4 addresses have VALID ROA.

Was 55.92% at the beginning of May 2022.

Source: <https://stats.labs.apnic.net/roa/KH> (11 Oct 2023)

# Online RPKI Sessions & Technical Assistance



- APNIC delivered monthly online RPKI sessions to targeted networks from June 2022 to January 2023.
- One-to-one technical assistance provided by APNIC's Retained Community Trainer in Khmer.

# Face-to-face RPKI Session



- In November 2022, ROA coverage significantly improved following APNIC's face-to-face RPKI session in Phnom Penh.
- Thanks to local community for your cooperation and support!

# 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.

# Route Origin Validation (ROV)



- Should be done by all networks on the Internet:
  - Setting up RPKI Validators
  - Configuring Border Routers to validate received prefixes
    - **VALID**
      - ROA exists, both prefix length and origin AS match with the record
    - **INVALID**
      - ROA exists, but prefix length or/and origin AS 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 Cambodia



ASN	AS Name	RPKI Validates	Samples
55636	TPLC-KH TPLC Holding Ltd.	98.88%	179
17726	CAMNET-AS Telecom Cambodia	1.65%	121
138606	SUGAPTELTD-AS-AP Suga Pte. Ltd	0.78%	129
9902	NEOCOMISP-KH-AP NEOCOMISP LIMITED, IPTX Transit and Network Service Provider in Cambodia.	0.75%	536
131207	SINET-KH SINET, Cambodias specialist Internet and Telecom Service Provider.	0.71%	1,545
45498	SMART-AXIATA-KH SMART AXIATA Co., Ltd.	0.68%	19,127
17976	CAMGSM-CELLCARD-AS-AP CAMGSM Company Ltd	0.59%	6,480
58424	XINWEITELECOM-KH # 3BEo, Sangkat Beoun Prolit, Khan 7Makara, Phnom Penh.	0.55%	182
38235	MEKONGNET-ADC-AS-AP ANGKOR DATA COMMUNICATION	0.40%	2,725
38209	CAMINTEL-AS CAMINTEL, National Telecommunication Provider, Phnom Penh, Cambodia	0.39%	259
38901	EZECOM-AS-AP EZECOM limited	0.20%	1,961
131178	EZECOM-AS-AP EZECOM limited	0.20%	4,055
23673	ONLINE-AS Cogetel Online, Cambodia, ISP	0.17%	1,171
38623	VIETTELCAMBODIA-AS-AP ISPIXP IN CAMBODIA WITH THE BEST VERVICE IN THERE.	0.17%	35,404
24492	IIT-WICAM-AS-AP WiCAM Corporation Ltd.	0.10%	1,002
...			

Source: <https://stats.labs.apnic.net/rpki/KH> (11 Oct 2023)

# ROV Adoption in Cambodia



- Cambodia Network eXchange (CNX) is dropping INVALID prefixes and hosting public RPKI Validators.

The screenshot shows the Alice RPKI Validator interface. On the left, a sidebar lists route servers: rs01.cnx.net.kh (IPv4), rs01.cnx.net.kh (IPv6), rs02.cnx.net.kh (IPv4), rs02.cnx.net.kh (IPv6), rs03.cnx.net.kh (IPv4), and rs03.cnx.net.kh (IPv6). The main panel displays the configuration for rs01.cnx.net.kh (IPv4) via Telcotech, with the next hop IP 103.7.144.57. A search bar is present with the text 'Filter by Network or Next Hop'. Below the search bar, there are tabs for 'Filtered' (selected) and 'Accepted'. The 'ROUTES FILTERED' section shows 8 routes, with 2 displayed. Both routes are marked as 'INVALID' with a red minus icon. The first route is 103.141.164.0/23 and the second is 103.141.164.0/24. Both have a next hop of 103.7.144.57, origin of IGP, local preference of 100, MED of 0, and AS path of 55329 131178. The error message for both is 'RPKI: Invalid. Generic code: the route must be treated as rejected. RPKI INVALID route'.

Status	Network	Next Hop	Origin	Local Pref	MED	AS Path
⊖	103.141.164.0/23 RPKI: Invalid Generic code: the route must be treated as rejected RPKI INVALID route	103.7.144.57	IGP	100	0	55329 131178
⊖	103.141.164.0/24 RPKI: Invalid Generic code: the route must be treated as rejected RPKI INVALID route	103.7.144.57	IGP	100	0	55329 131178

Source: [https://lg.sabay.com/routeservers/rs01/protocols/AS55329\\_1/routes](https://lg.sabay.com/routeservers/rs01/protocols/AS55329_1/routes) (11 Oct 2023)

# Major Networks Dropping INVALID



ASN	Name	Source
1221	Telstra	<a href="https://lists.ausnog.net/pipermail/ausnog/2020-July/044367.html">https://lists.ausnog.net/pipermail/ausnog/2020-July/044367.html</a>
4637		<a href="https://www.zdnet.com/article/telstra-to-roll-out-rpki-routing-security-from-june-2020/">https://www.zdnet.com/article/telstra-to-roll-out-rpki-routing-security-from-june-2020/</a>
1239	Sprint / T-Mobile	<a href="https://www.sprint.net/policies/bgp-aggregation-and-filtering">https://www.sprint.net/policies/bgp-aggregation-and-filtering</a>
1299	Telia	<a href="https://www.teliacarrier.com/Our-Network/BGP-Routing/Routing-Security.html">https://www.teliacarrier.com/Our-Network/BGP-Routing/Routing-Security.html</a>
2497	IJ	<a href="https://www.ij.ad.jp/en/dev/iir/pdf/iir">https://www.ij.ad.jp/en/dev/iir/pdf/iir</a>
2914	NTT	<a href="https://www.gin.ntt.net/support/policy/rr.cfm#RPKI">https://www.gin.ntt.net/support/policy/rr.cfm#RPKI</a>
3356	Level3	<a href="https://twitter.com/lumentechco/status/1374035675742412800">https://twitter.com/lumentechco/status/1374035675742412800</a>
4826	Vocus	<a href="https://blog.apnic.net/2021/05/13/vocus-rpki-implementation/">https://blog.apnic.net/2021/05/13/vocus-rpki-implementation/</a>
6939	Hurricane Electric	<a href="https://mailman.nanog.org/pipermail/nanog/2020-June/108277.html">https://mailman.nanog.org/pipermail/nanog/2020-June/108277.html</a>
7018	AT&T	<a href="https://mailman.nanog.org/pipermail/nanog/2019-February/099501.html">https://mailman.nanog.org/pipermail/nanog/2019-February/099501.html</a>
7922	Comcast	<a href="https://corporate.comcast.com/stories/improved-bgp-routing-security-adds-another-layer-of-protection-to-network">https://corporate.comcast.com/stories/improved-bgp-routing-security-adds-another-layer-of-protection-to-network</a>
9002	RETN	<a href="https://twitter.com/RETNnet/status/1333735456408793089">https://twitter.com/RETNnet/status/1333735456408793089</a>
16509	Amazon	<a href="https://aws.amazon.com/blogs/networking-and-content-delivery/how-aws-is-helping-to-secure-internet-routing/">https://aws.amazon.com/blogs/networking-and-content-delivery/how-aws-is-helping-to-secure-internet-routing/</a>
37100	Seacom	<a href="https://www.ripe.net/participate/mail/forum/routing-wg/PDZIMzAzMzhhlWVhOTAtnZlxOC1IMziOLTBJzjMyOGI1Y2NkM0BzZWVjb20ubXU+">https://www.ripe.net/participate/mail/forum/routing-wg/PDZIMzAzMzhhlWVhOTAtnZlxOC1IMziOLTBJzjMyOGI1Y2NkM0BzZWVjb20ubXU+</a>
...		

Source: <https://taejoong.github.io/pubs/publications/li-2023-rov.pdf> (11 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.
  - 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

# 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 Status Updates

# Questions & Answers