PACNOG 37

RPKI uptake in the region

What's new?

vivek@apnic.net
Regional Manager
Member and Registry Services

Resource Public Key Infrastructure

What is RPKI?

A robust security framework for verifying the association between **resource holders** and their **Internet number resources**.

route and route6 objects

Represents a single IPv4/IPv6 route injected into the Internet routing mesh

```
route6:          2001:df2:ee01::/48
descr:           Prefix for APNICTRAINING LAB DC
origin:          AS45192
mnt-by:          MAINT-AU-APNICTRAINING
last-modified:   2016-06-23T14:32:38Z
source:          APNIC
```

```
route:           202.125.97.0/24
descr:           Prefix for APNICTRAINING LAB DC
origin:          AS45192
mnt-by:          MAINT-AU-APNICTRAINING
country:         AU
last-modified:   2016-06-16T23:23:17Z
source:          APNIC
```

Out-of-date route objects?

```
whois -h whois.radb.net 203.76.192.0/24
```

```
route:          203.76.192.0/24
descr:          Proxy-registered
origin:         AS55821
source:         NTTCOM
```

```
route:          203.76.192.0/24
descr:          Proxy-registered
origin:         AS17970
source:         RADB
```

```
route:          203.76.192.0/24
descr:          REACH (Customer Route)
origin:         AS23944
source:         REACH
```

Route Origin Authorization (ROA)

What is contained in a ROA?

- The AS number you have authorized
- The prefix that is being originated from it
- The most specific prefix (maximum length) that the AS may announce

For example: “ISP 4 permits AS65551 to originate a route for the prefix 198.51.100.0/24"

Route Origin Validation (ROV)

- Valid
  - The prefix, prefix length, and origin AS match an entry in the database
- Invalid
  - Prefix is found, but origin-AS is wrong, OR
  - The prefix length is longer than the maximum length
- Not Found
  - No applicable ROA exists for the prefix

Deploying RPKI

- Step 1. Create your ROA
  - The AS number you have authorized
  - The prefix that is being originated from it
  - The most specific prefix (maximum length) that the AS may announce

- Step 2. Deploy ROV
  - Full routing table
    - Set up a validator and drop RPKI-invalid routes
  - Default/Partial feed
    - Encourage upstreams to drop RPKI-invalid routes

Real-world route hijacks

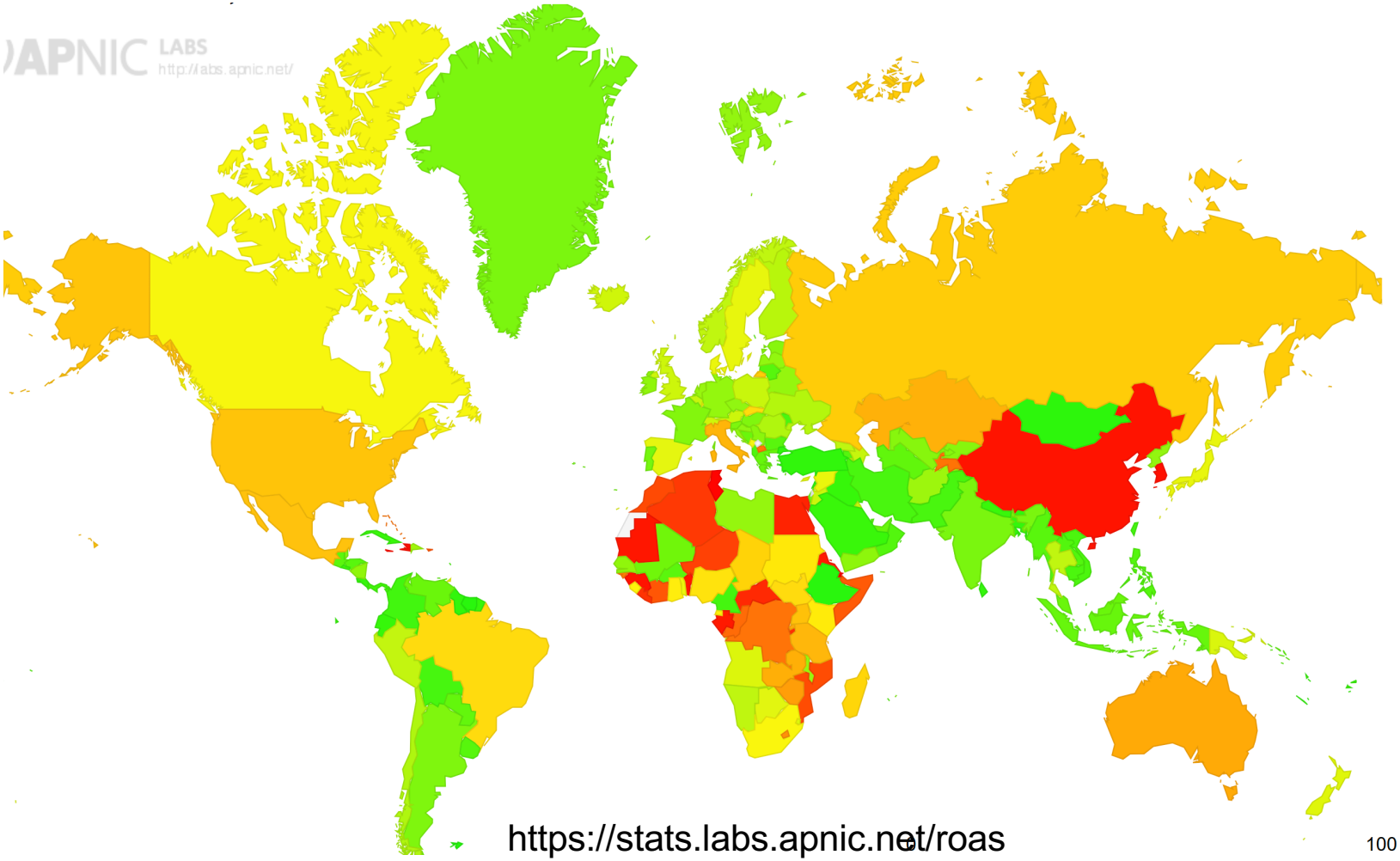
Background:
Route hijacking, a form of BGP attack, occurs when a malicious or misconfigured network announces IP prefixes it does not own. This misleads other networks into directing traffic through unintended paths, potentially leading to data interception, service disruption, or denial of service.

	Sample Case - Impacted	Sample Case - Not Impacted
When	5 Feb 2021	2 Apr 2022
What	Campana hijacked Twitter route and advertise to internet	SPT Vietnam hijack route Akamai in TM network.
How it happened and mitigation work	TM saw the best route to Twitter is via Campana. TM sent traffic user to Campana and being blackhole. Manually rejected routes at peering sites with Campana.	Akamai had registered ROA, mentioning the prefix only valid to be advertised by Akamai and TM. Telstra, which already have validator, saw the IP as invalid route, because at that time Akamai already register ROA. Hence, no effect to TM user accessing Akamai in MY.

Problem Statement: Route Hijacking in TM's Network Infrastructure Before RPKI Deployment

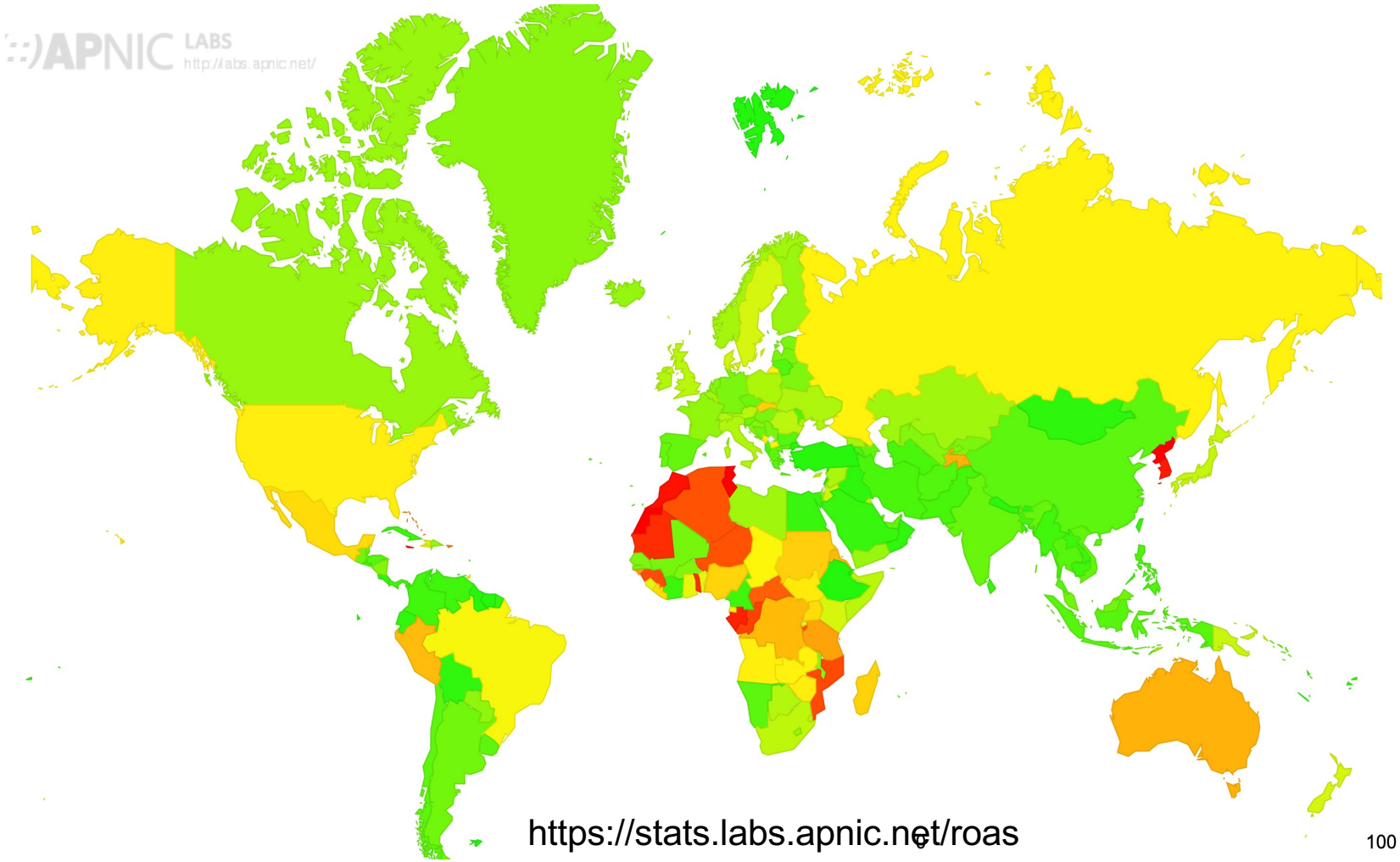
https://www.mynog.org/wp-content/uploads/2025/presso/TB%20-%202.00%20PM%20Telekom%20Malaysia.pdf

ROA – Global Snapshot (PacNOG 36)



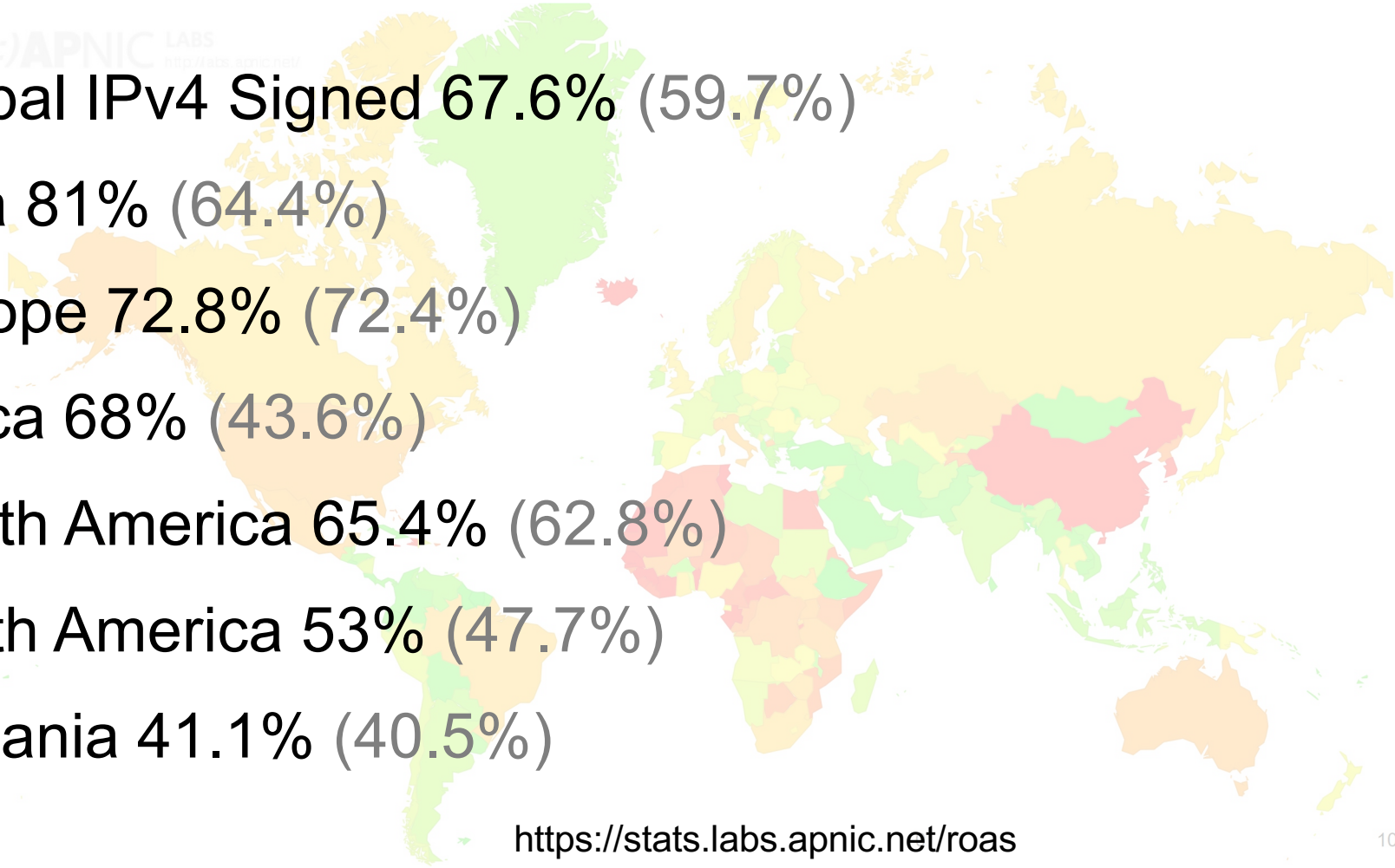
https://stats.labs.apnic.net/roas

ROA – Global Snapshot (PacNOG 37)



https://stats.labs.apnic.net/roas

ROA – Global Snapshot by Region

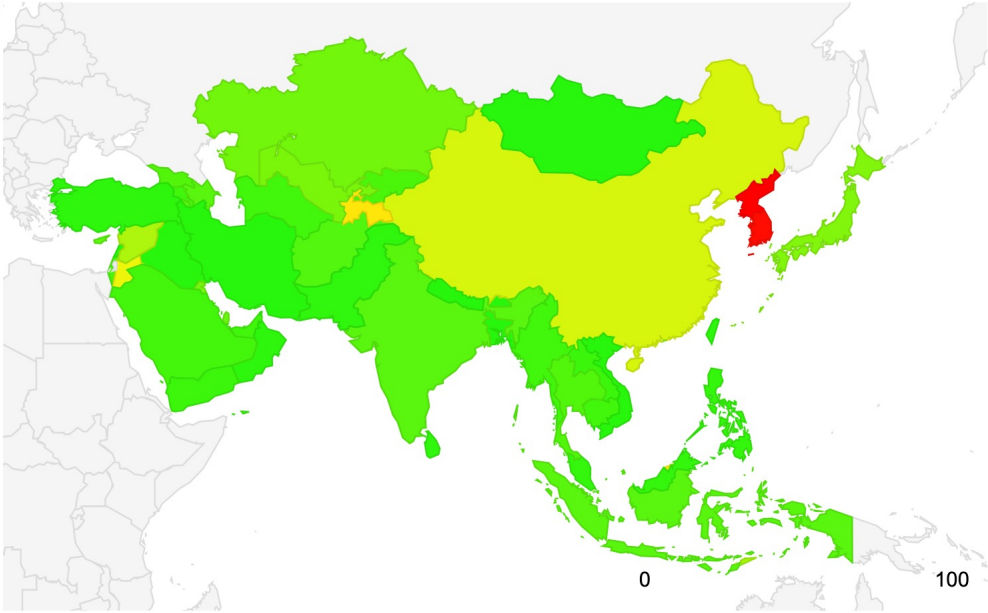


- Global IPv4 Signed 67.6% (59.7%)
- Asia 81% (64.4%)
- Europe 72.8% (72.4%)
- Africa 68% (43.6%)
- South America 65.4% (62.8%)
- North America 53% (47.7%)
- Oceania 41.1% (40.5%)

https://stats.labs.apnic.net/roas

RPKI ROA – Asia

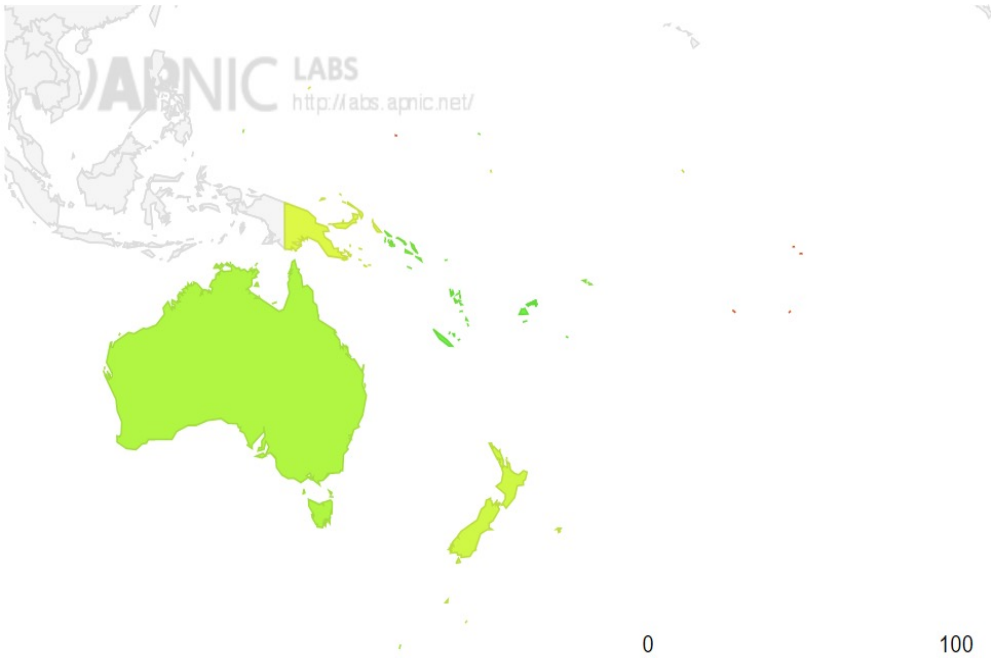
- 3 Sub-regions
  - 92.7% (90.6%) South-East Asia
    - MY,VN,TH,SG,PH,ID,MM,LA,BN,KH,TL
  - 91.1% (89.1%) South Asia
    - IN,LK,NP,BT,PK,BD,AF,MV
  - 57.6% (30.8%) East Asia
    - TW,JP,MN,CN,MO,KR,HK,KP



https://stats.labs.apnic.net/roa/XD

RPKI ROA – Oceania

- 4 Sub-regions
  - Melanesia 92.8% (89.8%)
    - FJ,NC,PG,SB,VU
  - Micronesia – 87.8% (54.6%)
    - FM,GU,KI,MH,MP,NR,PW
  - AU and NZ – 75% (73.4%)
    - AU,NZ,NF
  - Polynesia – 38.8% (32.8%)
    - AS,CK,NU,PF,PN,TK,TO,TV,WF,WS



https://stats.labs.apnic.net/roa/XF

RPKI ROA – Polynesia

Code	Region	V4 Valid	PacNOG36	PacNOG37
NU	Niue	512	100.00%	100%
PN	Pitcairn	256	100.00%	100%
TO	Tonga	9,728	97.40%	97.6%
WS	Samoa	18,432	88.9%	88.9%
TK	Tokelau	2,048	66.7%	71.4%
TV	Tuvalu	4,096	48.5%	51.4%
AS	American Samoa	5,376	25.0%	19.5%
PF	French Polynesia	9,472	12.4%	13%
WF	Wallis and Futuna Islands	256	6.70%	17.6%
CK	Cook Islands	256	2.90%	94.4%

https://stats.labs.apnic.net/roa/QS

RPKI ROA – Melanesia

Code	Region	PacNOG37
NC	New Caledonia	100%
FJ	Fiji	99.3%
VU	Vanuatu	96.5%
SB	Solomon Islands	86.2%
PG	Papua New Guinea	67.9%

https://stats.labs.apnic.net/roa/QQ

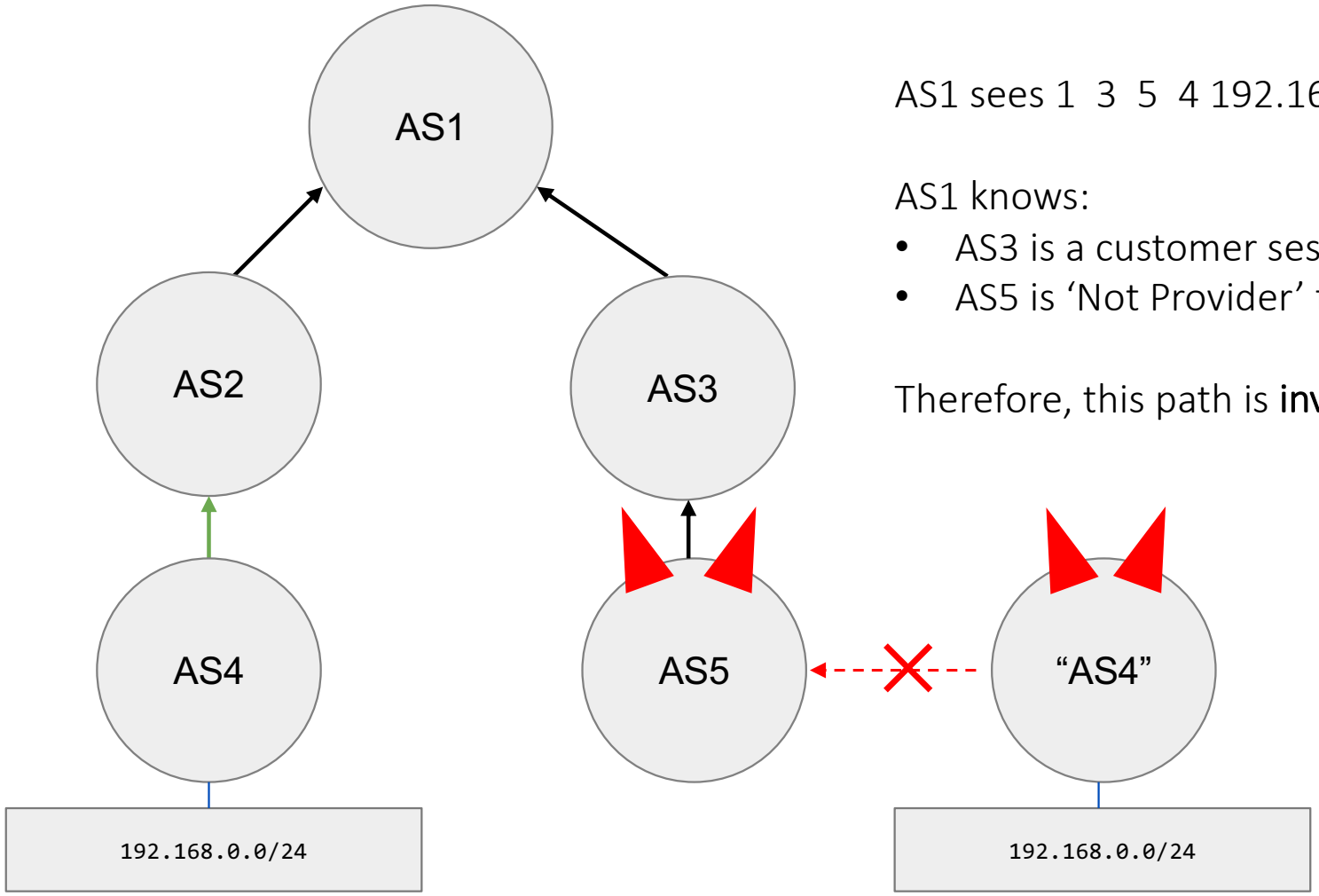
Limitation of ROV

- Route Origin Validation (ROV) only validates the origin of a route. It confirms whether the origin AS is authorised to announce a prefix based on published ROAs, but it does not validate the AS path that the route travelled through

AS Provider Authorization (ASPA)

- Signed by the holder of the ASN (Customer AS)
- Authorizing their transit provider ASNs (Provider AS)
  - The holder of the Customer AS Number declares which AS Numbers may appear as their Providers in BGP paths
- ASPA helps mitigate:
  - Forged-origin and forged-path attacks
  - Route leaks

Forged-origin attacks



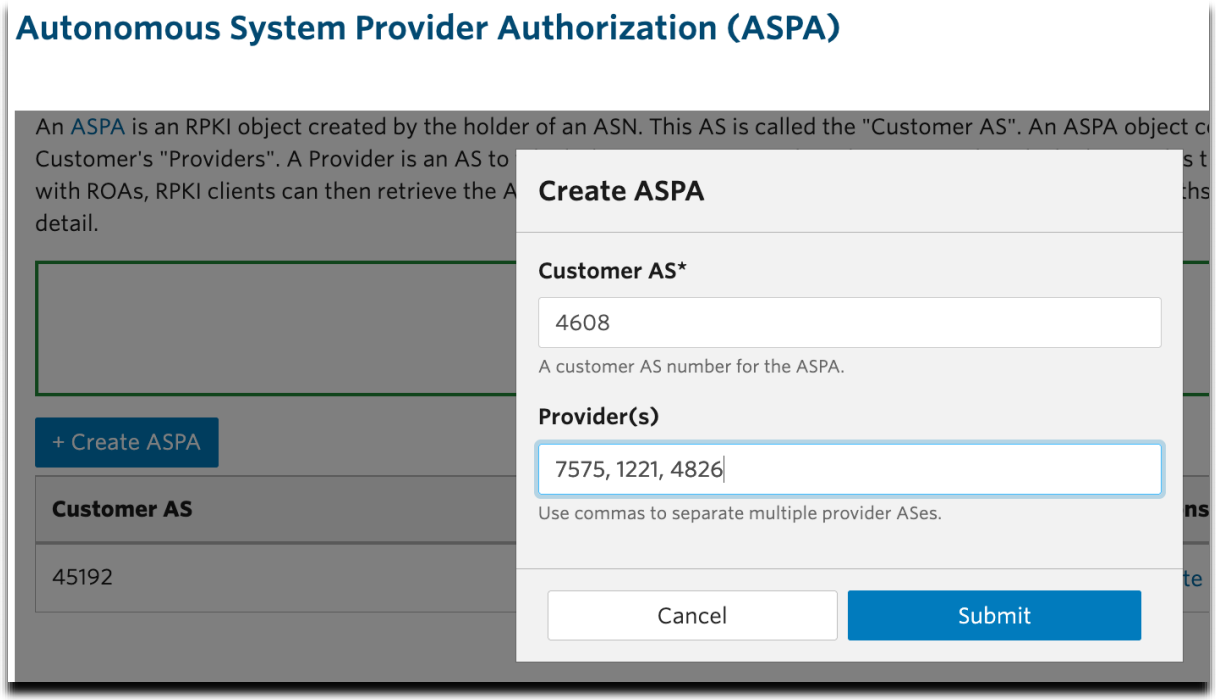
AS1 sees 1 3 5 4 192.168.0.0/24

AS1 knows:

- AS3 is a customer session
- AS5 is ‘Not Provider’ for AS4

Therefore, this path is **invalid**

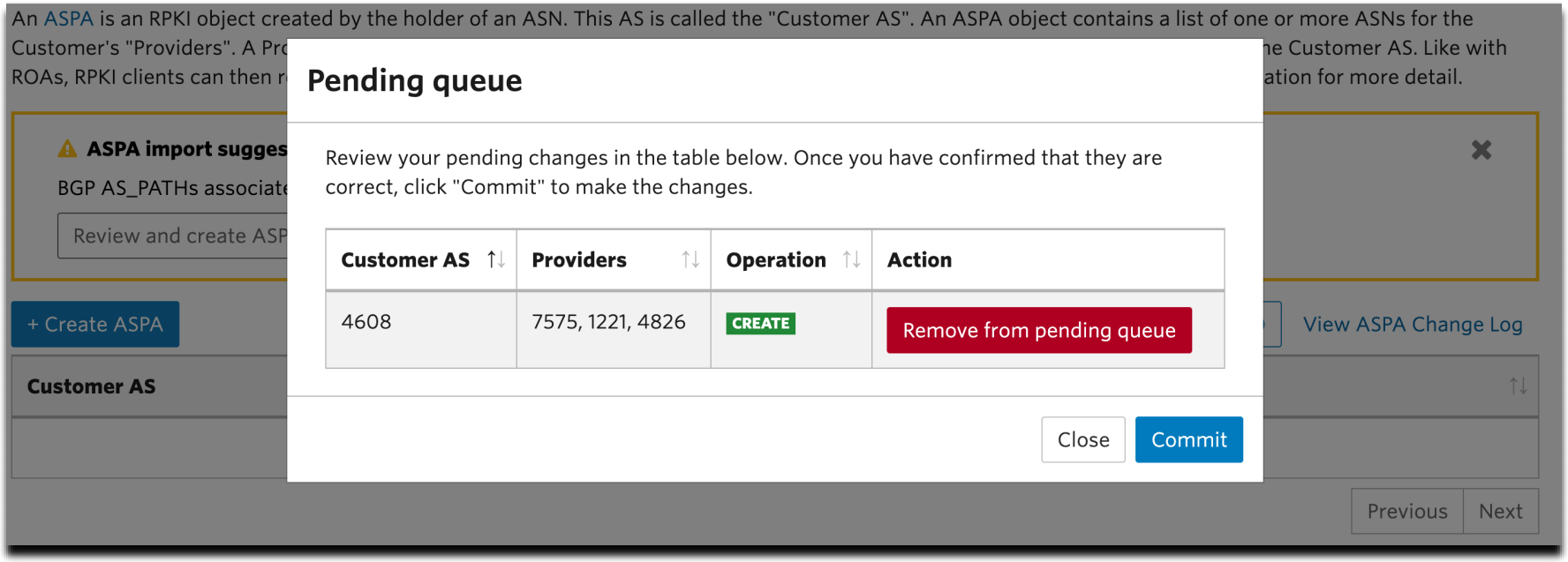
Creating ASPA objects in MyAPNIC (Step 1 of 2)



- Log in to MyAPNIC
- Navigate to Route Management
- Click on **Create ASPA**
- Enter your ASPA details and click **Submit**

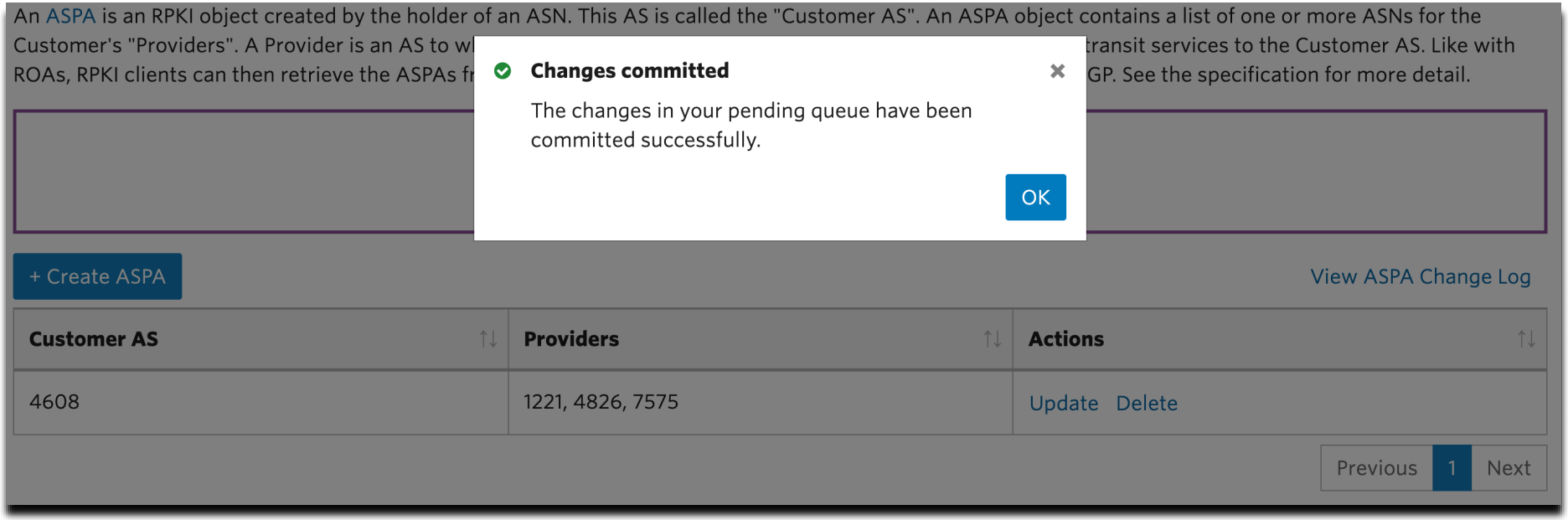
Creating ASPA objects in MyAPNIC (Step 2 of 2)

- Review your pending changes and click on **Commit** once confirmed.

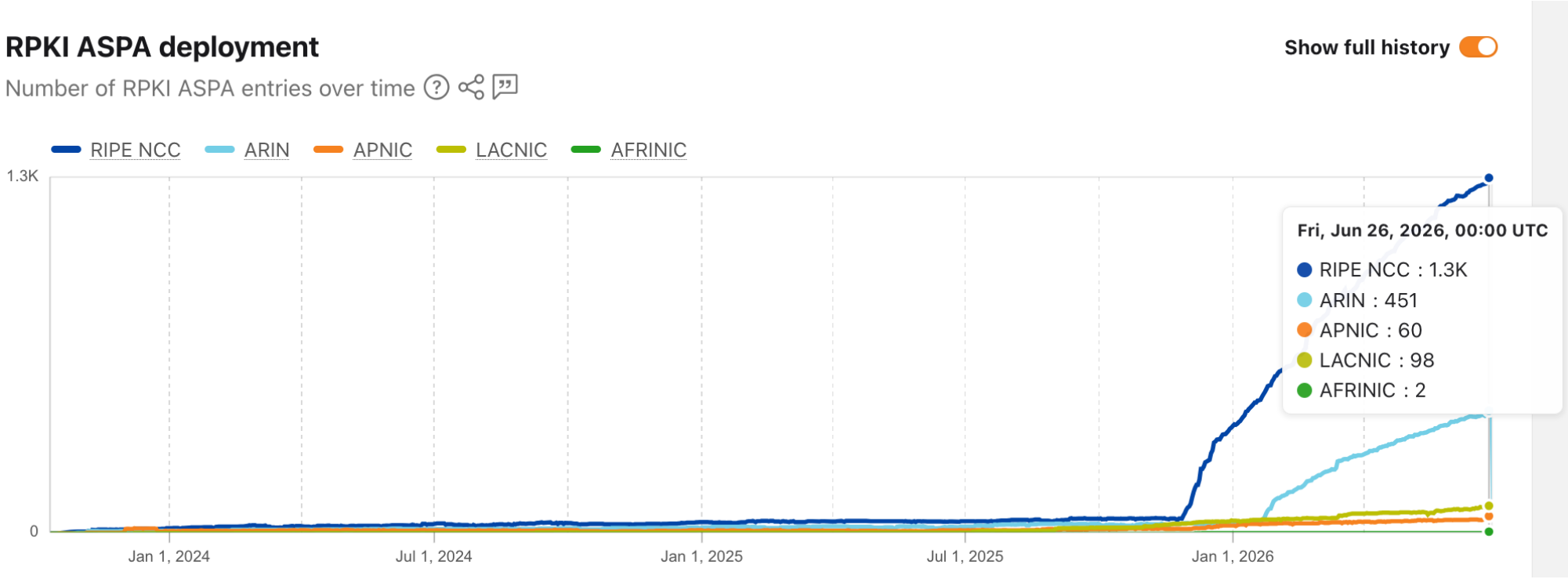


Creating ASPA objects in MyAPNIC

- Your ASPA object is now published



ASPA uptake in the region



https://radar.cloudflare.com/routing/rpki

What should operators do next?

1. Check your ROA coverage
2. Check your ROAs are up to date (https://dash.apnic.net/)
3. Deploy ROV or encourage your upstream to do so
4. Create ASPA objects for your AS provider relationships
5. Improve routing security for the wider Internet

Thank you