

RPKI, what we've learned and what we've been doing

PacNOG 30

elly@apnic.net

Resource Public Key Infrastructure

What is RPKI?

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

<https://youtu.be/rH3CPosGNjY>

Route Origin Authorization

What is contained in 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

eg : “"ISP 4 permits AS 65000 to originate a route for the prefix 192.2.200.0/24"”

RPKI Initiatives

Initial challenge was to get APNIC Members to create ROAs



10 face-to-face and eLearning RPKI training courses delivered

RPKI presentations to NOGs and conferences

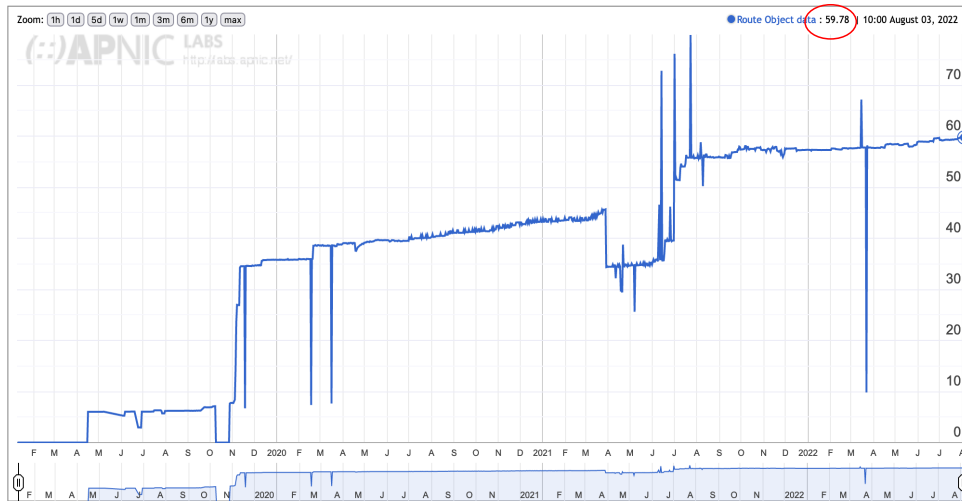
Development of the 'Ready to ROA' campaign – hands on sessions to help Members create ROAs

New shirts, stickers, web content to promote campaign

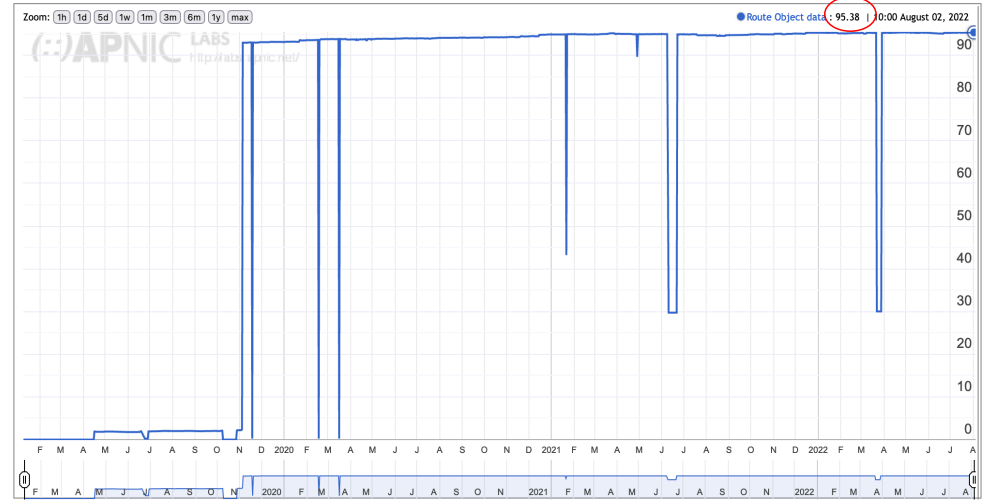
Ready to ROA launched in 2015

ROA coverage – Oceania

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



Display: Addresses (Advertised ROA-Valid Advertised Addresses), IPv6, Percent (of Total)



RPKI invalids



Rise of the invalids

By Tashi Phuntsho on 10 Apr 2020



RPKI invalids are not going away

By Md Abdul Awal on 16 Jul 2021



Solo effort to clean up RPKI invalids across a region

By Peter Peele on 26 Jul 2021

RPKI invalids

- On 27 April 2021, we saw 3526 RPKI invalid routes for IPv4 addresses delegated to APNIC Members

Validation result	IPv4 count	IPv6 count
Invalid AS	556	37
Invalid AS and ML	456	24
Invalid ML	2514	456
Total	3526	517

Table 1 — Validation counts for IPv4 and IPv6 on 27 April 2021, collected from Routeviews collector SG and Routinator 0.8.3.

Cleaning up RPKI invalids



Cleaning up your RPKI invalid routes

By Vivek Nigam on 28 Apr 2021

Fixing your incorrect or outdated ROAs is easy — here's how.

- Email campaign in June 2021 to reach out to Members with RPKI invalid announcements

ROA creation interface

Add new ✕

Prefix


Origin AS

Max length

ROA Enabled (ROAs will be created for this route)

Whois Enabled (Whois route objects will be created for this route)

Options Notify additional contacts



Improved ROA creation interface

Add new ×

Prefix

Origin AS

Max length

ROA Enabled (ROAs will be created for this route)

Are you sure? You have not entered a max length value.

This would mean that the max length is equivalent to the prefix size (/24).

Any more specific announcement may be marked as RPKI invalid.

No, I would like to make changes

OK

Routing status alerts in DASH

The screenshot shows the DASH dashboard with several key components:

- Header:** APNIC logo and a "LOG IN" button.
- Main Title:** "DASH Your Dashboard for Autonomous System Health".
- Introductory Text:** "Rapidly track suspicious traffic seen coming from your network."
- NEW features:**
 - Alert system to detect suspicious traffic
 - Option to receive recurring reports
 - Review and detect your network's BGP, RPKI and IRR misalignments (highlighted with a red box)
- Widgets:**
 - Suspicious traffic:** A line chart showing traffic trends from 17 Jan to 23 Jan, comparing "My network" and "Vietnam".
 - Firing alerts:** "Latest 24 hours" section.
 - Last firing alert:** Details for an "Alert for SSH attacks" triggered on 1 Jun 2021 from 192.168.5.0/24, resulting in 101 hits.
 - Your alerts:** A list of alerts for SSH attacks with columns for Status and Date of last trigger.
 - Offending prefixes:** A table listing prefixes and their associated ports and hit counts.
 - Overview:** Summary statistics for "My network" (55.1% hits), "Vietnam" (16.5% hits, 41.8K hits), and "SE Asia" (16.5% hits, 41.8K hits).

Routing status alerts in DASH

The screenshot displays the APNIC DASH interface. The top navigation bar includes the APNIC logo and the 'DASH' label. A sidebar on the left contains navigation links: Dashboard, Routing status (highlighted), Suspicious traffic, Alerts, What to do, and Latest security news. The main content area is titled 'Routing status' and includes a 'Member Account' dropdown set to 'MEMTEST1-AP' and a 'Showing routes for' dropdown set to 'my prefixes'. The main heading reads: 'Review the routing information of your network to prevent misconfigurations and detect BGP hijacks.' Below this are links for 'About this page' and 'Legend'. The 'Overview of inconsistencies' section shows a 'Total inconsistencies found' of 0. A sub-section titled 'Status of ROAs and route objects as seen in BGP:' contains two metrics: 'ROA mismatches' with a value of 0 and 'Route object mismatches' with a value of 0.

Overview of inconsistencies	
Total inconsistencies found	0
Status of ROAs and route objects as seen in BGP:	
• ROA mismatches	0
• Route object mismatches	0

Routing status alerts in DASH

Overview of inconsistencies

Total inconsistencies found **3**


Status of ROAs and route objects as seen in BGP:

- ROA mismatches **3**
[View prefixes](#) ▾
- Route object mismatches **0**

Routing status for my prefixes

Show ▾

Search by prefix or ASN

Filter by: ROA issues Route object issues 

Prefix ▾	BGP Route ▾	Origin AS ▾	ROA ▾	Route Object ▾
103.21.244.0/22	103.21.244.0/24	AS13335	● Mismatch + info	● Not Published
103.21.244.0/22	103.21.244.14/32	AS11708	● Mismatch + info	● Not Published
103.21.244.0/22	103.21.244.15/32	AS11708	● Mismatch + info	● Not Published

Routing status alerts in DASH

ROA mismatch for 103.21.244.0/24



Reason: The prefix length seen in BGP does not match with the ROA maxlength.

Length in **BGP**: /24 Scope in **ROA** ⓘ : /23 - /23 (103.21.244.0/23 - AS0)

Required actions:

- If you did not expect a route with this length, review your routing configuration to evaluate if there is a misconfiguration or a BGP prefix hijack. [Learn more about BGP hijacking.](#) ▼
- If you did not expect this max length, review the ROAs for this prefix.

Close

Reducing ROA downtime during transfers

- Facilitate resource transfers involving live networks
- Existing ROAs published for 2 weeks after transfers

What we've learned?

Upcoming RPKI improvements

- RPKI invalid alerts
- ROA pre-validation
- Registry API
 - <https://blog.apnic.net/2022/03/22/apnic-registry-api/>
- New ROA guides and Help Centre articles

Thank you!