

New Milestones in RPKI ROV Adoption

Jovana Palibrk



The network observability company

**This is a presentation
originally from:**

Doug Madory



Measuring RPKI deployment progress

- Two steps needed to identify and reject RPKI-Invalid BGP routes.

1

Create ROAs to define correct origins for address space

2

ASes reject RPKI-invalid routes that don't match ROAs

NetFlow + RPKI

- Offered as a capability to evaluate impact of rejecting RPKI-Invalids on traffic levels
- Kentik was challenged, heeded the challenge!
- The rest of this talk focuses on what Kentik learned so far from its aggregate data

Analysing traffic in context of rejecting RPKI invalids using pmacct

Job Snijders [job at ntt.net](#)

Tue Feb 12 18:15:54 UTC 2019

- Previous message (by thread): [Clueful Contact at IPVolume.net ?](#)
- Next message (by thread): [Route Filtering Update](#)
- Messages sorted by: [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#)

Dear all,

Whether to deploy RPKI Origin Validation with an "invalid == reject" policy really is a business decision. One has to weigh the pros and cons: what are the direct and indirect costs of accepting misconfigurations or hijacks for my company? what is the cost of deploying RPKI? What is the cost of honoring misconfigured RPKI ROAs? There are a few thousand misconfigured ROAs, what does this mean for me?

To answer these questions, Paolo Lucente and myself worked to extend pmacct traffic analysis engine (<http://pmacct.net/>) in such a way that it can do perform the RFC 6811 Origin Validation procedure and present the outcome as a property in the flow aggregation process.

Kind regards,

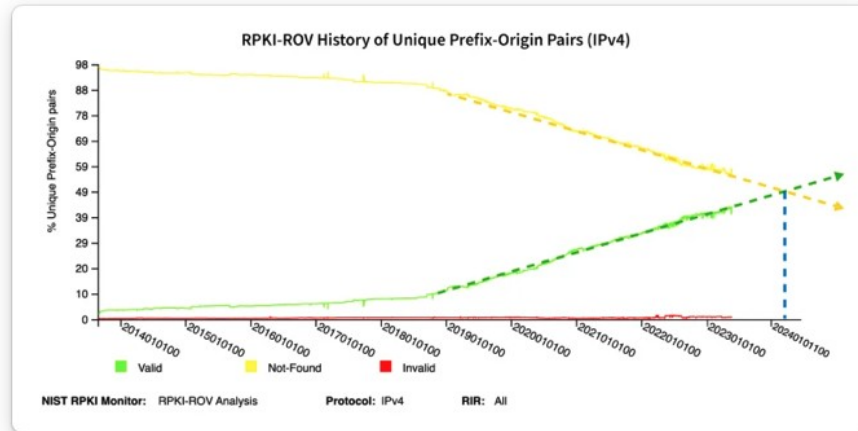
Job

ps. Dear Kentik & Deepfield, please copy+paste this feature! We'll happily share development notes with you, you can even look at pmacct's source code for inspiration. :-)

ROA Creation Predictions


- Last year, we made this bold prediction in our post:

If we are to assume steady growth of the share of BGP routes with ROAs, it should become the majority case in about a year from now (May 2024). Mark your calendars!



ROA Creation Predictions

● But y'all were doubters!


 **Doug Madory** ✓
@DougMadory

Ok BGP/RPKI nerds... what's your prediction on when these (very faint!) lines will cross and the majority of globally routed IPv4 routes have ROAs? (IPv6 is already there)
rpk-monitor.antd.nist.gov

Jan-Feb 2024	9.8%
Mar-Apr 2024	19.6%
May-Jun 2024	17.6%
Jul-Aug 2024	52.9%

51 votes · Final results
12:04 PM · Dec 15, 2023 · **1,907** Views

2 3 1 1

 **Doug Madory** · You
Director of Internet Analysis at Kentik
4mo · 🌐

Ok BGP/RPKI nerds... what's your prediction on when the majority of globally routed IPv4 routes will have ROAs?

IPv6 is already there according to <https://lnkd.in/efkMeP83> (cc: [Doug Montgomery](#))

Twitter/X version of this poll is here: <https://lnkd.in/eX9VqubD>

When will the majority of IPv4 BGP routes have ROAs? (we're currently at 47.15% according to NIST)
You can see how people vote. [Learn more](#)

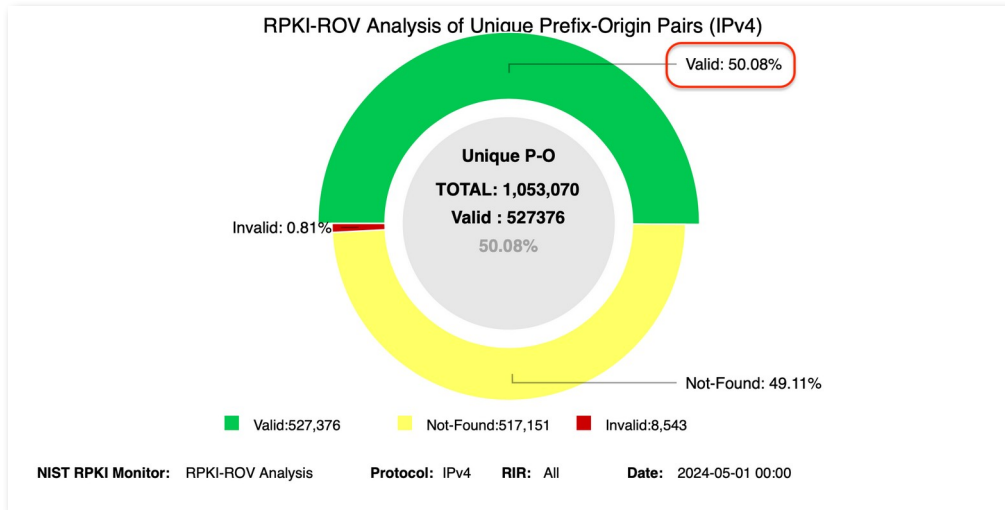
Jan-Feb 2024 ✓	0%
Mar-Apr 2024 ✓	9%
May-Jun 2024 ✓	18%
Jul 2024 or later ✓	73%

55 votes · Poll closed

8 1 comment · 1 repost

Measuring RPKI deployment progress

- We recently passed a milestone (May 1):
 - >50% of IPv4 routes in global routing table have ROAs (NIST RPKI monitor)

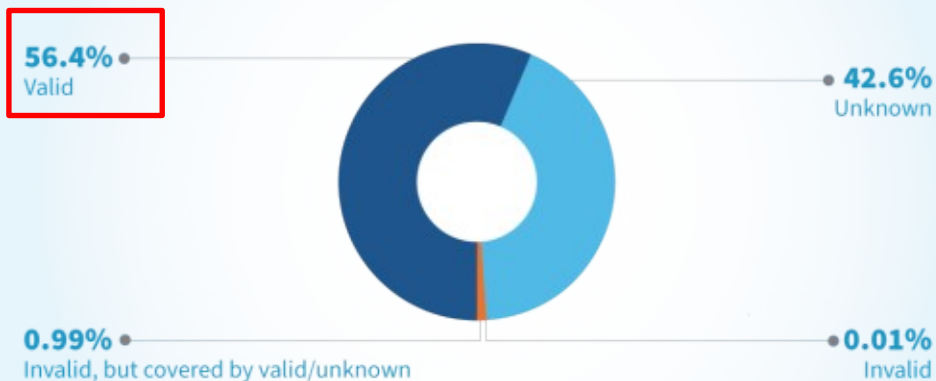


IPv6 achieved this late last year

Measuring RPKI deployment progress

- But RPKI ROV is ultimately about protecting traffic, so ...
- At NANOG 84 in Austin, TX, we explored ROA creation (1.) using Kentik's aggregate NetFlow
 - 1/3 of BGP routes had ROAs. just >1/2 of traffic (bps) went to routes with ROAs

Internet traffic volume by RPKI evaluation

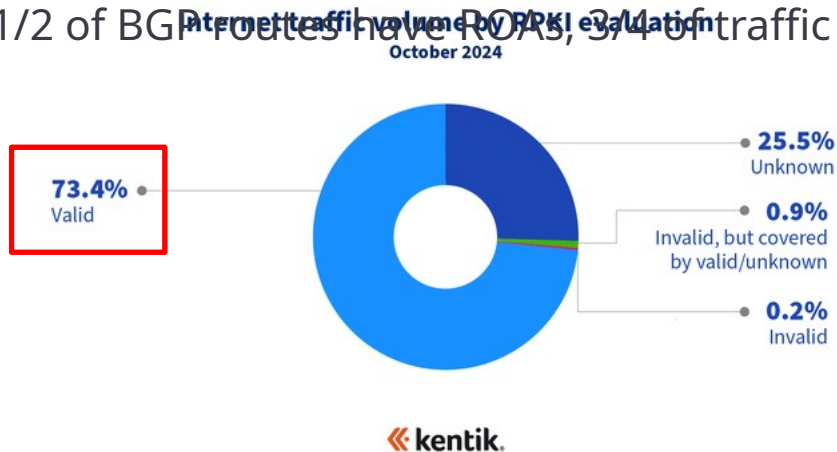


Stats from Feb 2022:

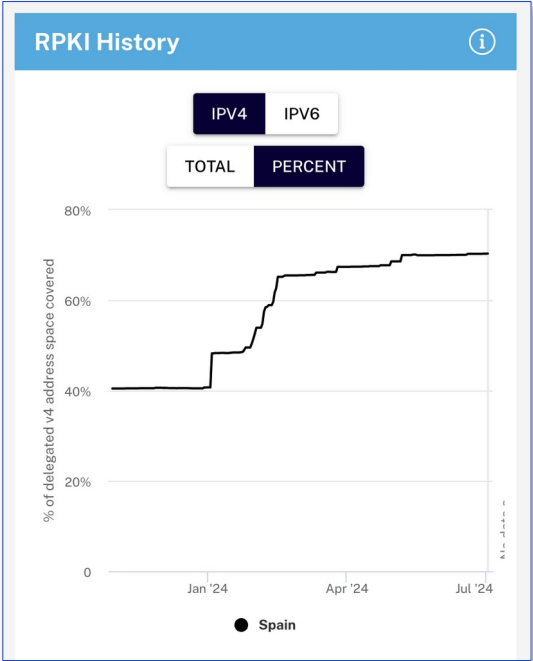
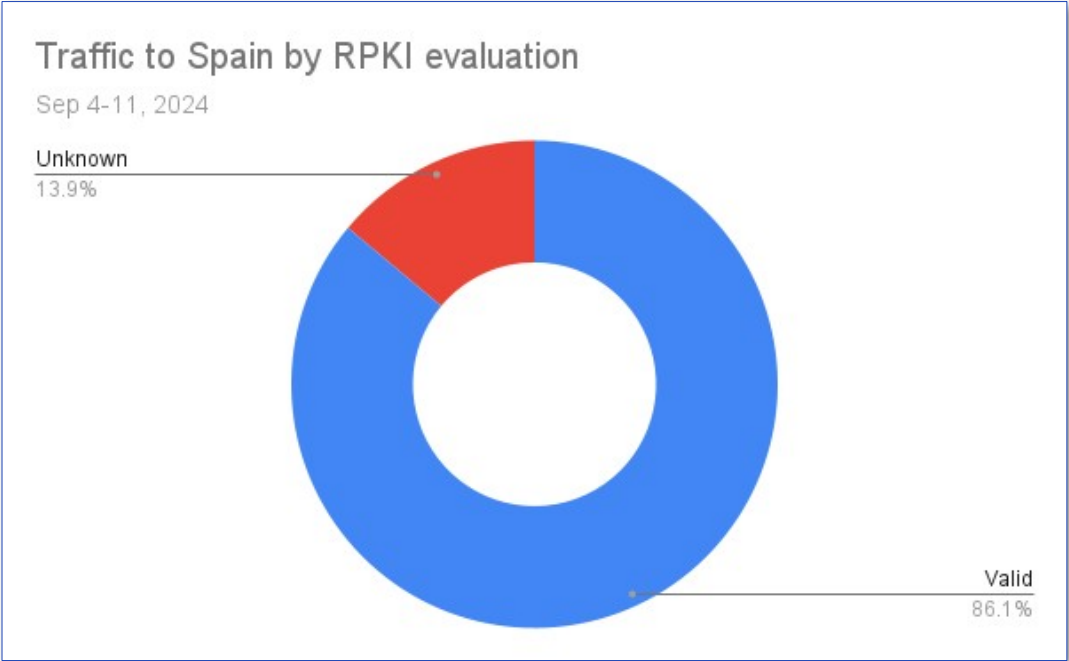
How has this changed since?

Measuring RPKI deployment progress

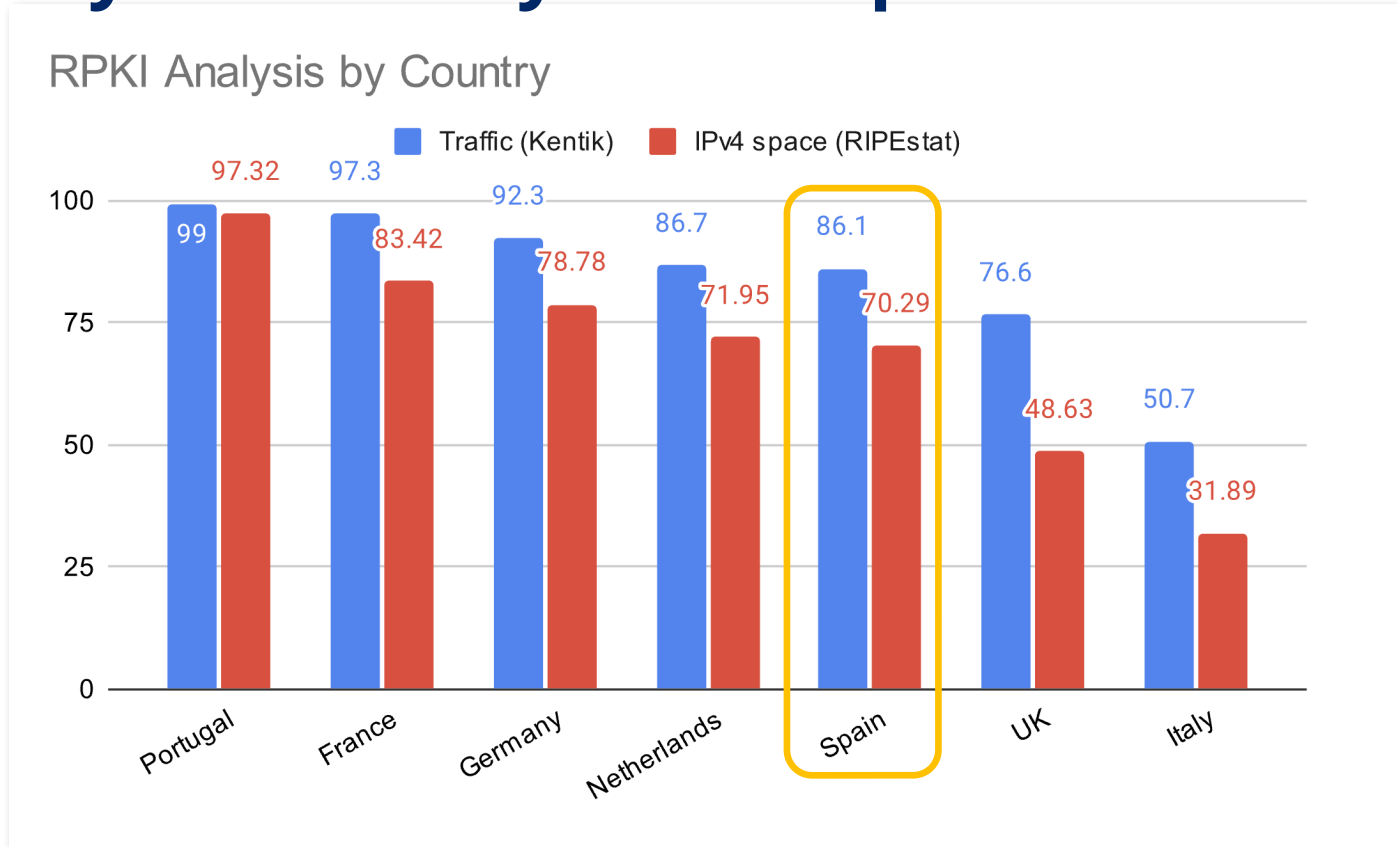
- But RPKI ROV is ultimately about protecting traffic, so ...
- At NANOG 84 in Austin, TX, I explored ROA creation (1.) using Kentik's aggregate NetFlow
 - Feb 2022: 1/3 of BGP routes had ROAs, >1/2 of traffic (bps) went to routes with ROAs
 - Oct 2024: >1/2 of BGP routes have ROAs, 3/4 of traffic (bps) went to routes with ROAs



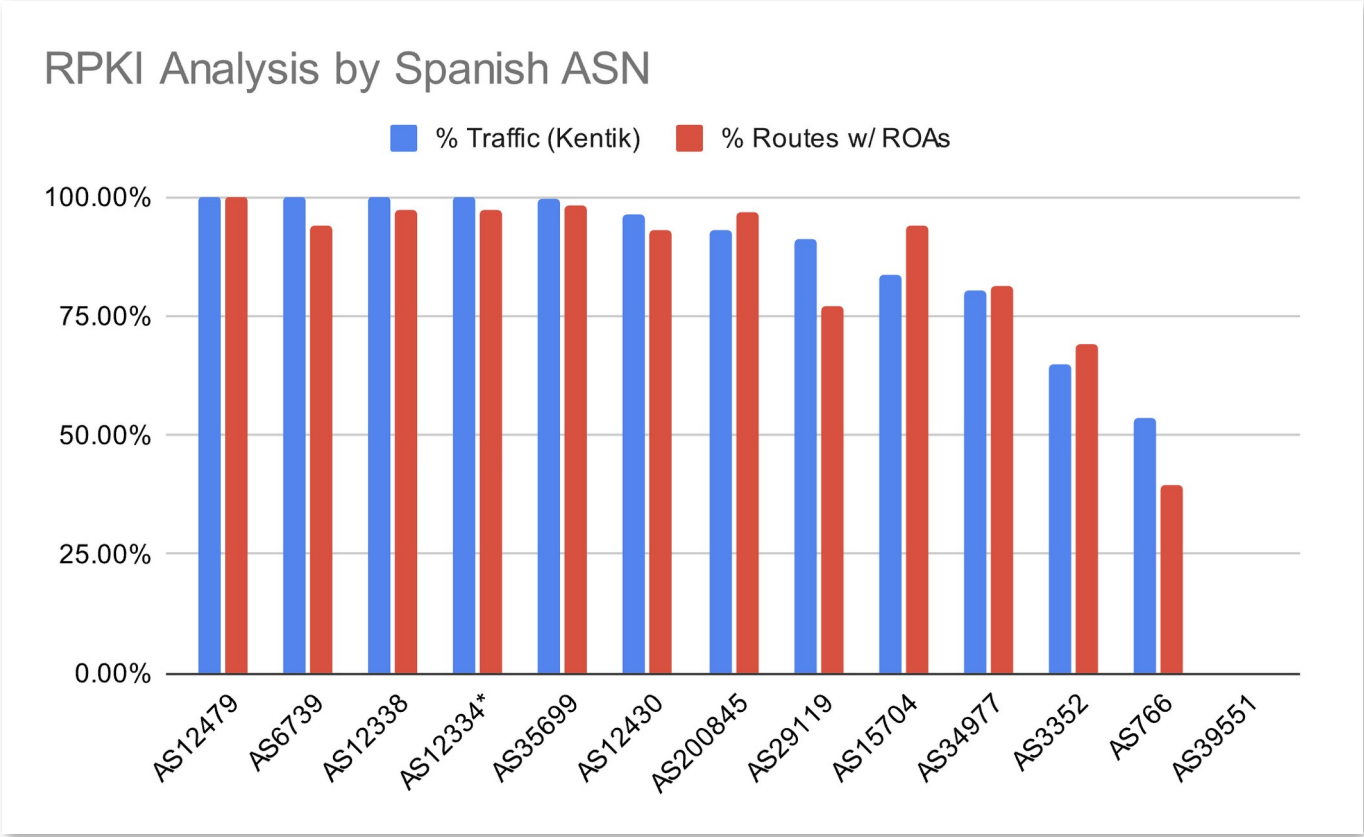
Country-level Analysis: España



Country-level Analysis: España



Country-level Analysis: España

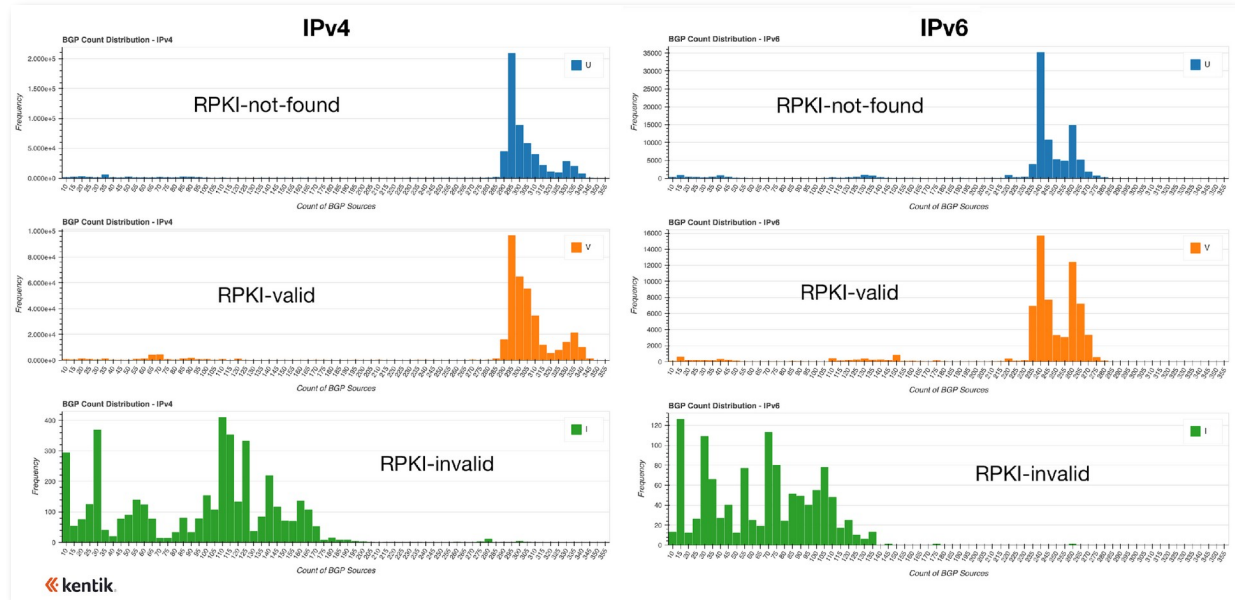


Propagation Reduction of RPKI-Invalids

- ROAs alone are useless if only a few networks are rejecting invalid routes.
- 2022 analysis showed propagation of RPKI-invalid routes is half or less than other types.

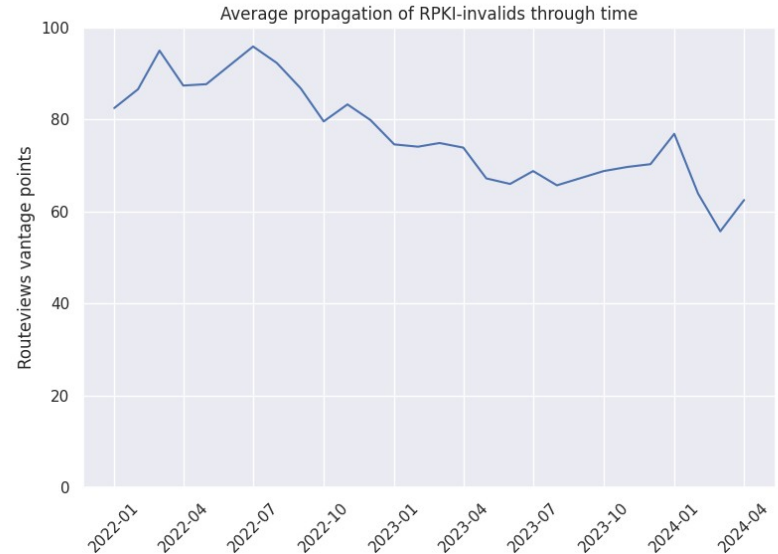
Stats from Aug 2022

How has this changed since?



RPKI-Invalid Propagation Declining

- 24% decline in the propagation of RPKI-invalids
- Analyzing propagation of RPKI-invalid routes over time faces challenges:
 - Set of persistently RPKI-invalid routes not guaranteed to stay constant.
 - Propagation is heavily influenced by which providers are transiting a route.
- Does the trend hold for RPKI-invalid beacons?



RPKI-Invalid Propagation Declining

- RIPE NCC and Job Snijders (AS15562) announce RPKI-invalid (and RPKI valid) routes for measurement of RPKI ROV deployment.
- Invalid routes from each of these beacons all experienced an overall decline in propagation while the control routes saw increased propagation.



Invalid Propagation Different for ARIN and RIPE

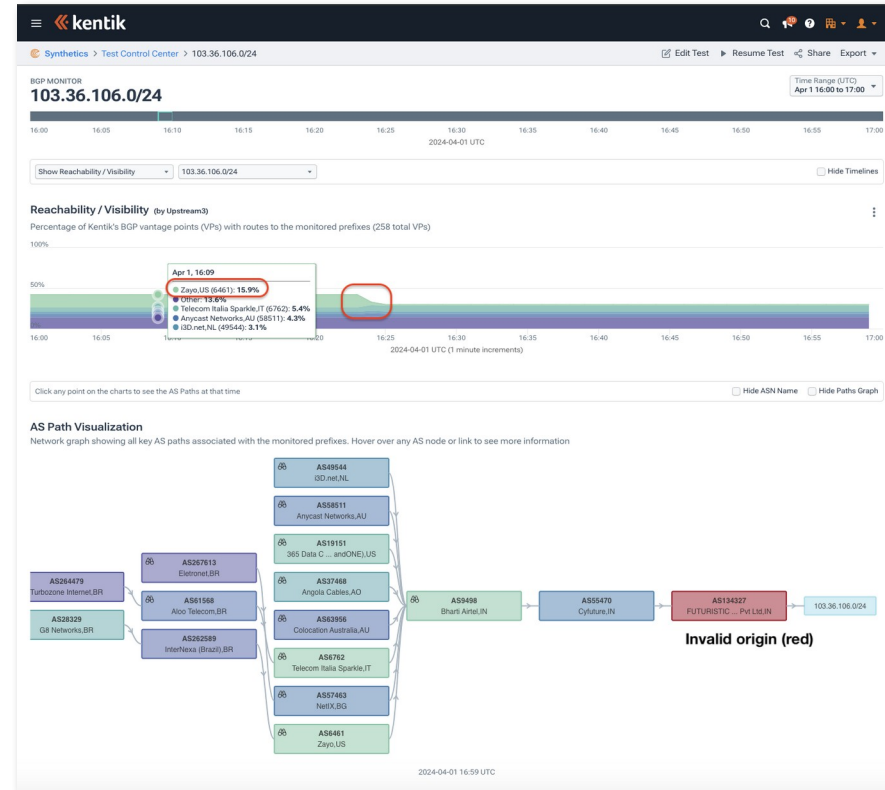
Final observation:

- Two RPKI-invalid routes in “Job’s Beacons” experience slightly different propagation.
- ROAs published in different RIR TALs:
 - 209.24.0.0/24 (green) is in the ARIN TAL
 - 194.32.71.0/24 (orange) is in the RIPE TAL
- Accepting the ARIN TAL requires a lengthy Relying Party Agreement that some providers refuse to accept.
- Result:
 - ROAs published by ARIN are seen by fewer networks.
 - Slightly reducing the efficacy of RPKI ROV for ARIN managed IP space.



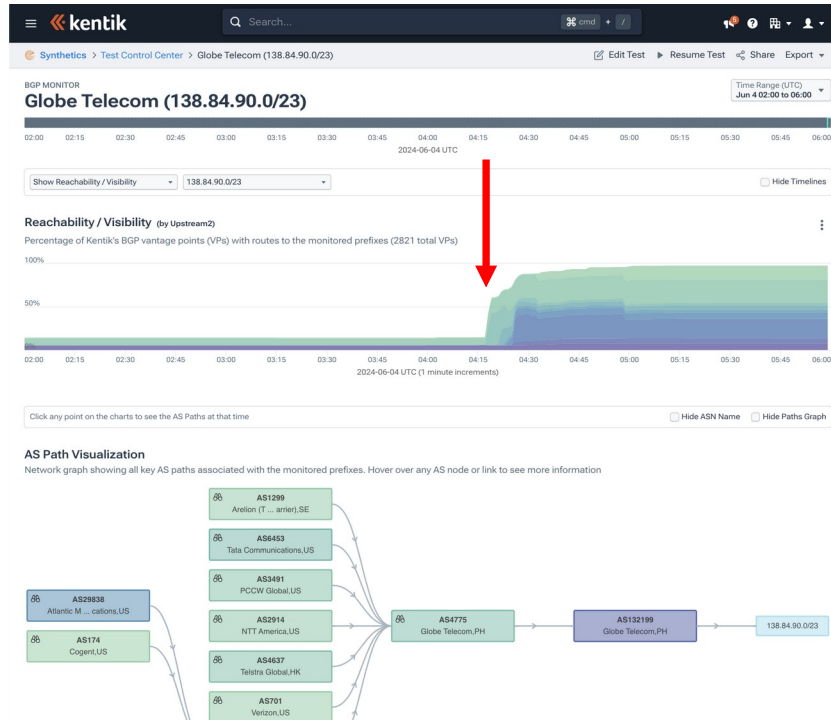
Another Tier-1 AS Rejecting RPKI-Invalids

- Much of the reduction of propagation of RPKI-invalid routes is due to the rejection of invalids by Tier-1 (DFZ) ASes.
- Another RPKI milestone in April:
 - An additional Tier-1 AS began rejecting RPKI-invalid routes from customer networks.
 - On April 1 at 16:24 UTC, we saw Zayo (AS6461) begin rejecting RPKI-invalid routes.

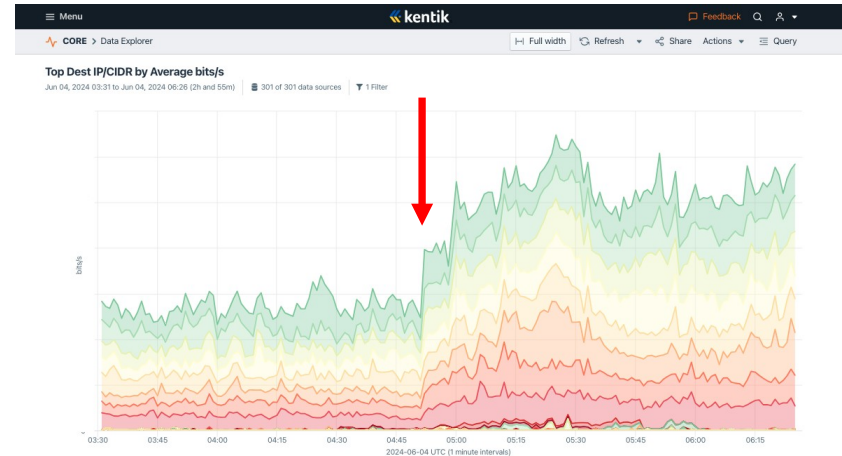


Fixing ROA misconfigurations

- Globe Telecom (PH) recently fixed several ROAs causing routes to be RPKI-invalid.



Traffic volume to previously RPKI-invalid routes increased.



A Call To Action

1. Reject RPKI-invalids.

- Given that the majority of BGP routes have ROAs (including a super majority of traffic), networks should reject RPKI-invalid routes to avoid mistakenly egressing traffic based on the acceptance of mis-originated routes.

2. Create ROAs.

- And given the scale to which RPKI-invalid routes are suppressed, it would benefit resource holders to create ROAs for their address ranges to enable networks around the world to automatically reject mis-originated routes.

Conclusion

- Progress due to the dedicated efforts of hundreds of engineers at dozens of companies.
 - >1/2 of BGP routes have ROAs, 3/4 of traffic (bps) went to routes with ROAs
 - Propagation of RPKI-invalids continues to decline, Zayo now rejecting invalids
- RPKI ROV doesn't solve all the issues surrounding Internet routing security.
 - Only an opening salvo towards addressing the various "determined adversary" scenarios best characterized by the recent attacks against cryptocurrency services.
- Need to build off the progress made by RPKI ROV to address more difficult scenarios.



Thank you!

Jovana Palibrk
Solutions Engineer
jovana@kentik.com

