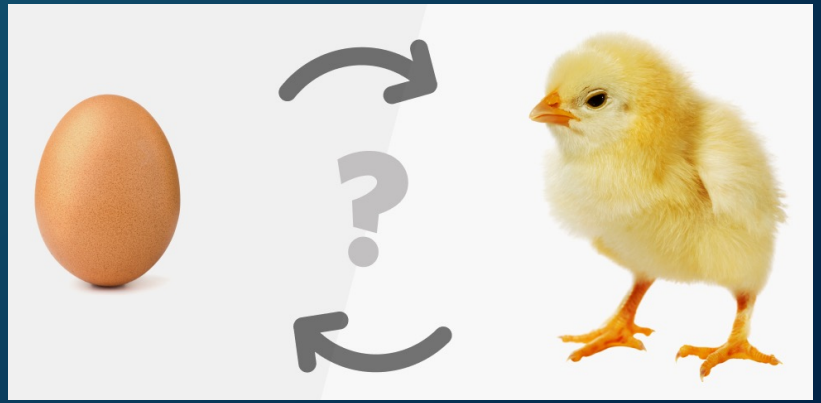
Are we turning a corner on BGP security?

Doug Madory, dmadory@kentik.com, Kentik

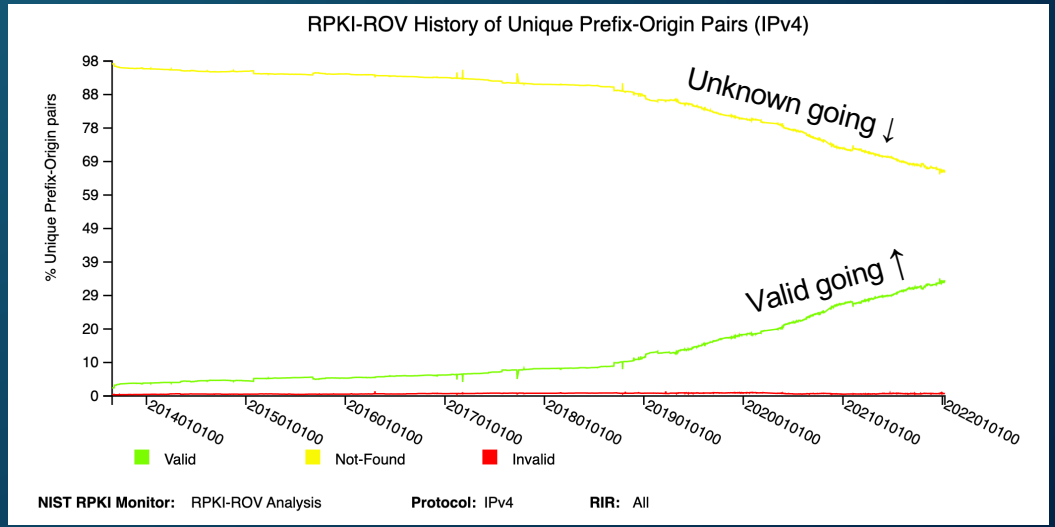
Where are we with RPKI ROV adoption?

- Presently stands as the Internet's best defense against BGP hijacks due to typos or other BGP mishaps.
- Core challenge: broad deployment requires many individual actions.
  - *Why reject RPKI-invalids if no one is creating ROAs?*
  - *Why create ROAs if no one is rejecting RPKI-invalids?*



Where are we with RPKI ROV adoption?

- Enormous progress in recent years as Tier-1 NSPs agreed to reject RPKI-Invalids.
  - NTT, GTT, Arelion (Telia), Cogent, Telstra, PCCW, Lumen, and more!
- According to NIST RPKI Monitor, the trend line is going in the right direction!

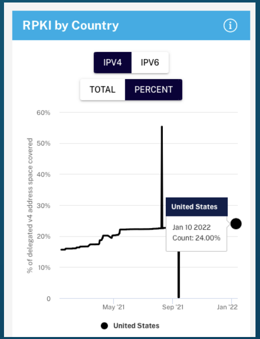


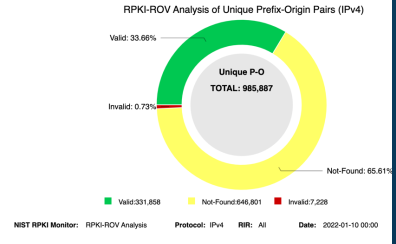
https://rpki-monitor.antd.nist.gov

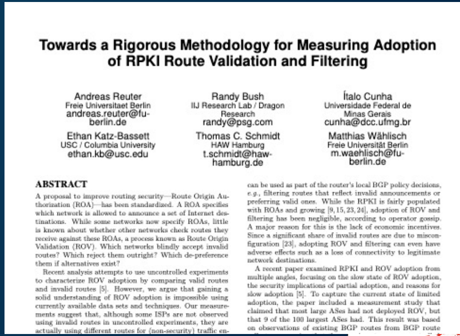
Measuring RPKI deployment progress

- It takes two steps to reject an RPKI-Invalid BGP route.

	1 ROAs created to assert valid origin and prefix length.	2 Networks reject RPKI-invalids
How to evaluate progress?	*Multiple resources (ex: NIST, RIPE)*	*Active area of research*







Towards a Rigorous Methodology for Measuring Adoption of RPKI Route Validation and Filtering

Andreas Reuter, Freie Universitaet Berlin, andreas.reuter@fu-berlin.de
Randy Bush, IIJ Research Lab / Dragon Research, randy@psg.com
Ítalo Cunha, Universidade Federal de Minas Gerais, cunha@dcc.ufmg.br
Ethan Katz-Bassett, USC / Columbia University, ethan.kb@usc.edu
Thomas C. Schmidt, HAW Hamburg, t.schmidt@haw-hamburg.de
Matthias Wählisch, Freie Universität Berlin, m.waehlisch@fu-berlin.de

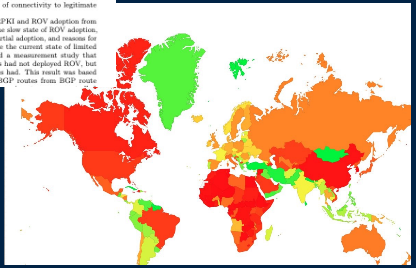
ABSTRACT

A proposal to improve routing security—Route Origin Authorization (ROA)—has been standardized. A ROA specifies which network is allowed to announce a set of Internet destinations. While some networks now specify ROAs, little is known about whether other networks check routes they receive against these ROAs, a process known as Route Origin Validation (ROV). Which networks blindly accept invalid routes? Which reject them outright? Which de-preference them if alternatives exist?

Recent analysis attempts to use uncontrolled experiments to characterize ROV adoption by comparing valid routes and invalid routes [5]. However, we argue that gaining a solid understanding of ROV adoption is impossible using currently available data sets and techniques. Our measurements suggest that, although some ISPs are not observed using invalid routes in uncontrolled experiments, they are actually using different routes for (non-security) traffic en-

can be used as part of the router's local BGP policy decisions, *e.g.*, filtering routes that reflect invalid announcements or preferring valid ones. While the RPKI is fairly populated with ROAs and growing [9, 15, 23, 24], adoption of ROV and filtering has been negligible, according to operator gossip. A major reason for this is the lack of economic incentives. Since a significant share of invalid routes are due to misconfiguration [23], adopting ROV and filtering can even have adverse effects such as a loss of connectivity to legitimate network destinations.

A recent paper examined RPKI and ROV adoption from multiple angles, focusing on the slow state of ROV adoption, the security implications of partial adoption, and reasons for slow adoption [5]. To capture the current state of limited adoption, the paper included a measurement study that claimed that most large ASes had not deployed ROV, but that 9 of the 100 largest ASes had. This result was based on observations of existing BGP routes from BGP route

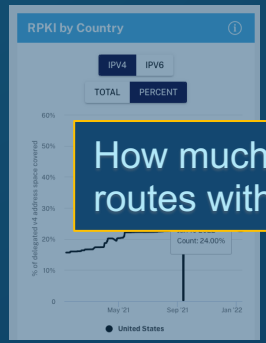


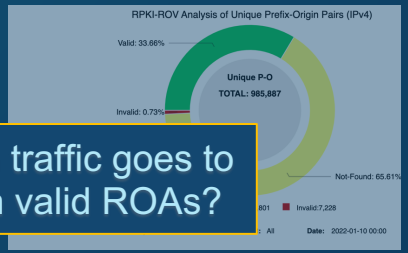
https://stats.labs.apnic.net/roas

Measuring RPKI deployment progress

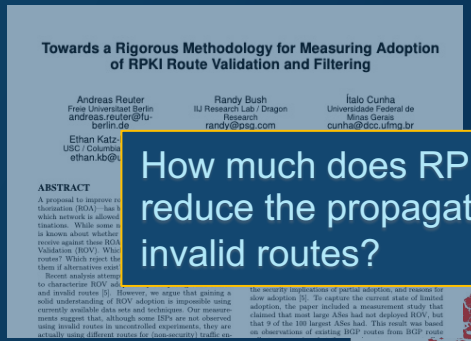
- We have two questions we want to answer.

How to evaluate progress?	1 ROAs created to assert valid origin and prefix length.	2 Networks reject RPKI-invalids
	Multiple resources (ex: NIST, RIPE)	*Active area of research*

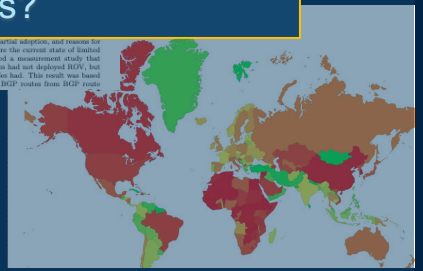




How much traffic goes to routes with valid ROAs?



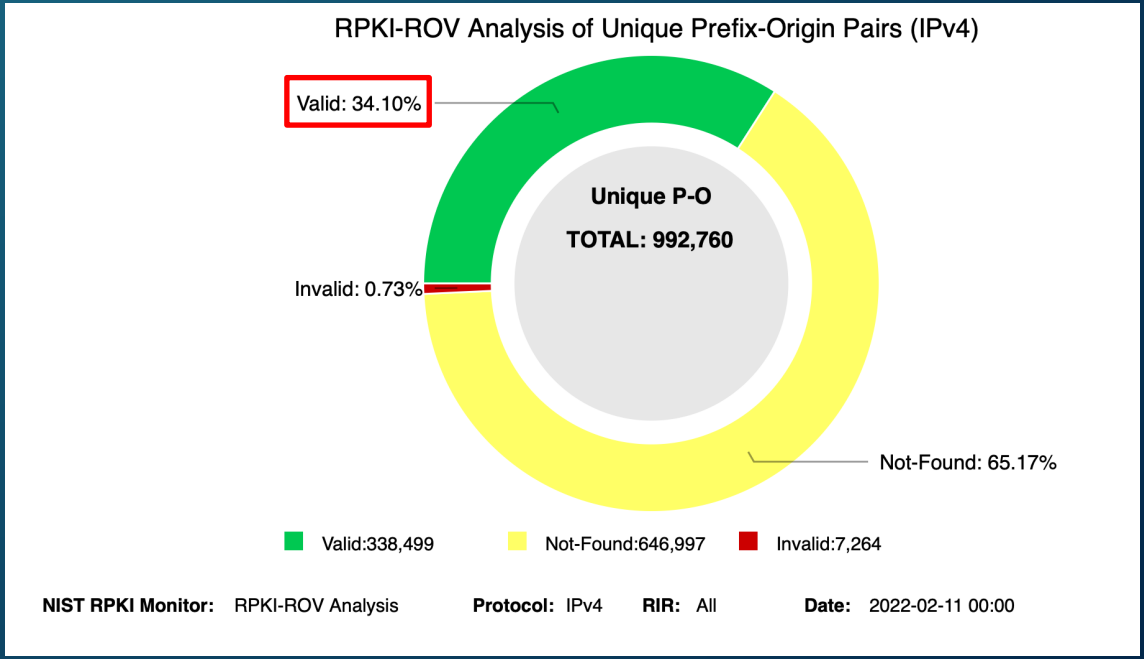
How much does RPKI ROV reduce the propagation of invalid routes?



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

Where are we with ROA creation?

- NIST RPKI Monitor reports that *only 34.1% of IPv4 BGP routes* are presently signed. *



Two RPKI unknown routes for each RPKI valid one.

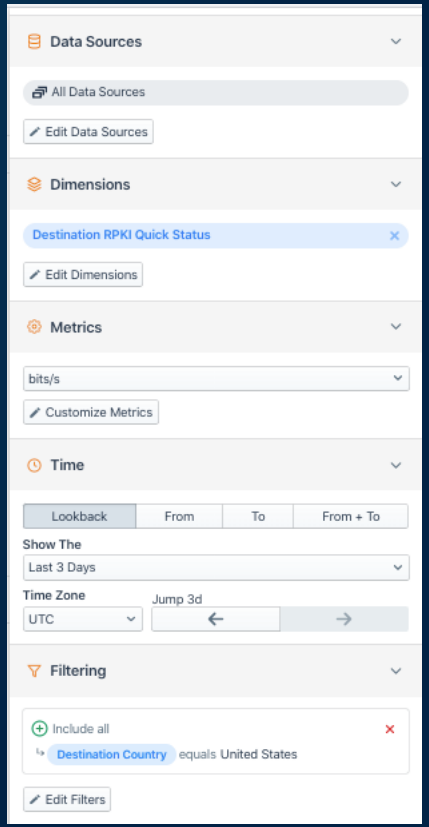
Question:
What proportion of overall traffic is safeguarded by that 34.1%?

*32.6% of IPv6 routes are RPKI-Valid

Kentik’s perspective can deepen understanding of RPKI

- Kentik has over 300 customers and almost half have opted-in to the use of their data as part of aggregate analysis.
  - Note: analysis is subject to biases of the customer set which includes (NSPs, CDNs and enterprises) and is skewed toward the US.

- Kentik’s NetFlow analytics platform annotates flow records with an RPKI evaluation of route of destination IP upon intake.
  - Originally built to understand how much traffic would be lost by dropping invalids.
  - Can also be used to understand RPKI from a traffic-volume perspective.

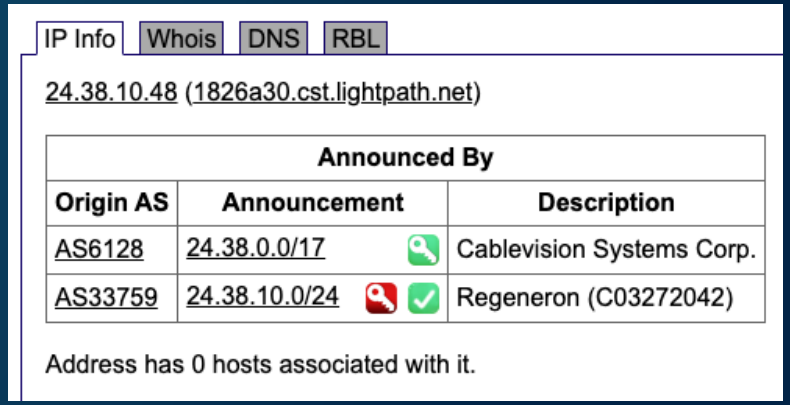


What proportion of traffic goes to signed routes?

- Kentik tracks four cases of RPKI outcome.
  1. Valid
  2. Unknown
  3. Invalid
  4. Invalid – but covered by valid/unknown

Note #4 only exists in the analysis-plane and is not part of IETF/BGP/Routing!

Example of #4:

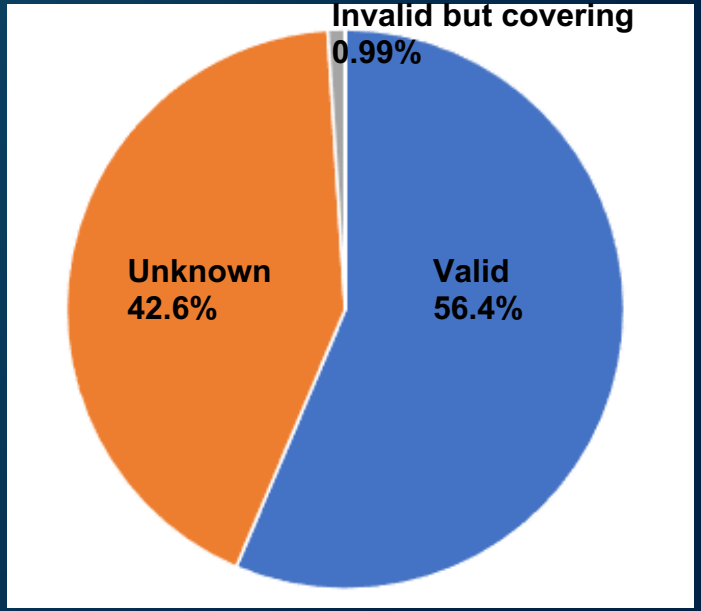


Only ~1/3 of BGP routes have ROAs - but how much traffic?

Period of analysis: 22 Arp 2022 00:00 UTC to 29 Apr 2022 00:00 UTC (7 days)

Main Observations*

- 0.1% of traffic volume is ‘Invalid but covering’
- 41.0% is Unknown
- 58.0% is Valid
- 0. 1% is Invalid



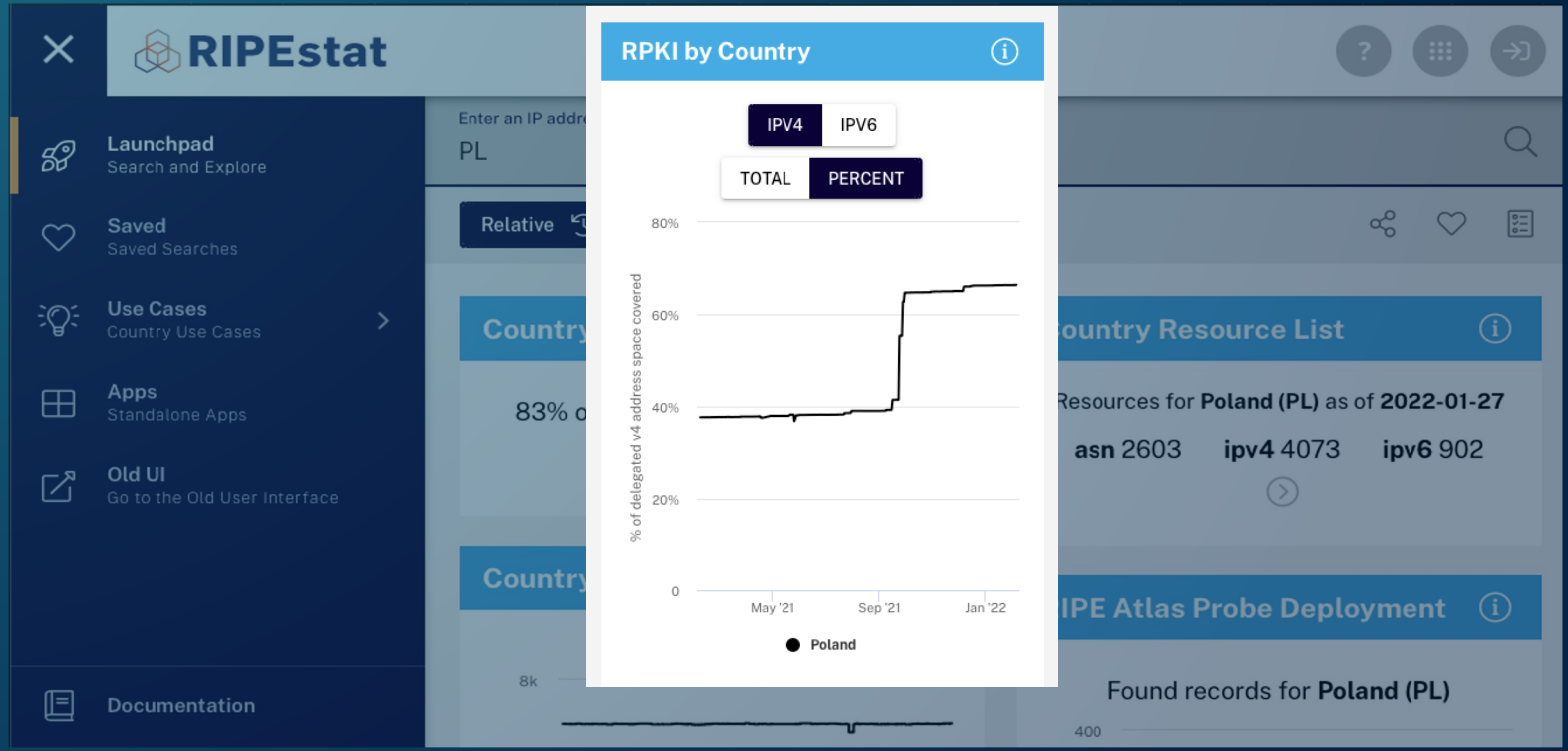
Traffic to invalid routes is infinitesimal.

- Not a reason to not drop invalids.

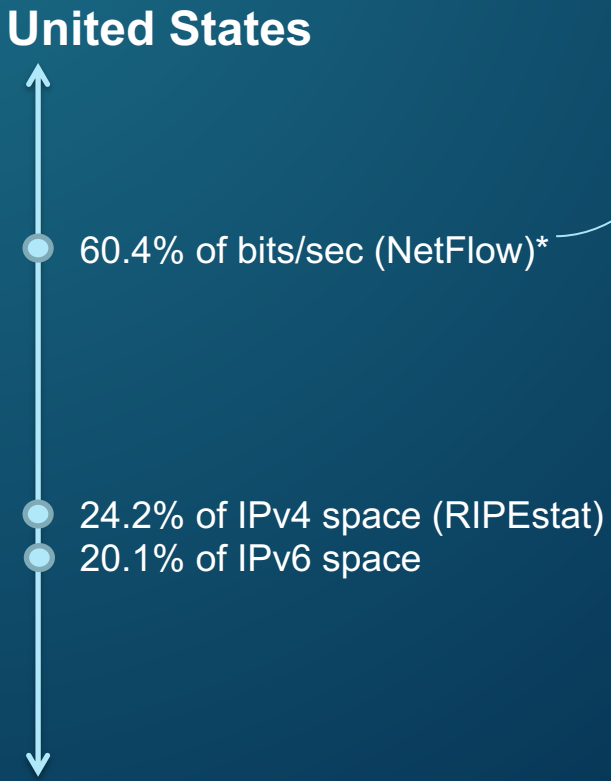
*Combined IPv4 + IPv6

Comparing metrics for ROA creation by country

- RIPEstat reports % of IP address space https://stat.ripe.net/app/launchpad/



For example, how is the US doing with ROA creation?



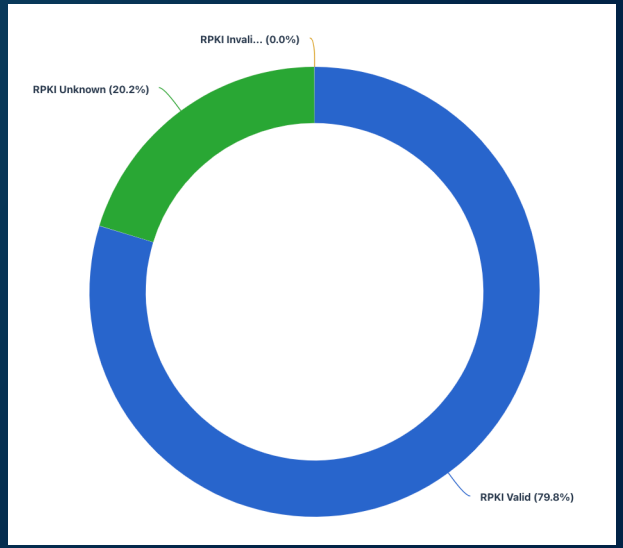
Why?

Major RPKI deployments	Valid %*
• Eyeball networks	
• Comcast (AS7922)	99.7%
• Spectrum (AS20115)	99.9%
• Content providers	
• Amazon (AS16509)	100%
• Google (AS15169)	100%
• Cloudflare (AS13335)	93.3%

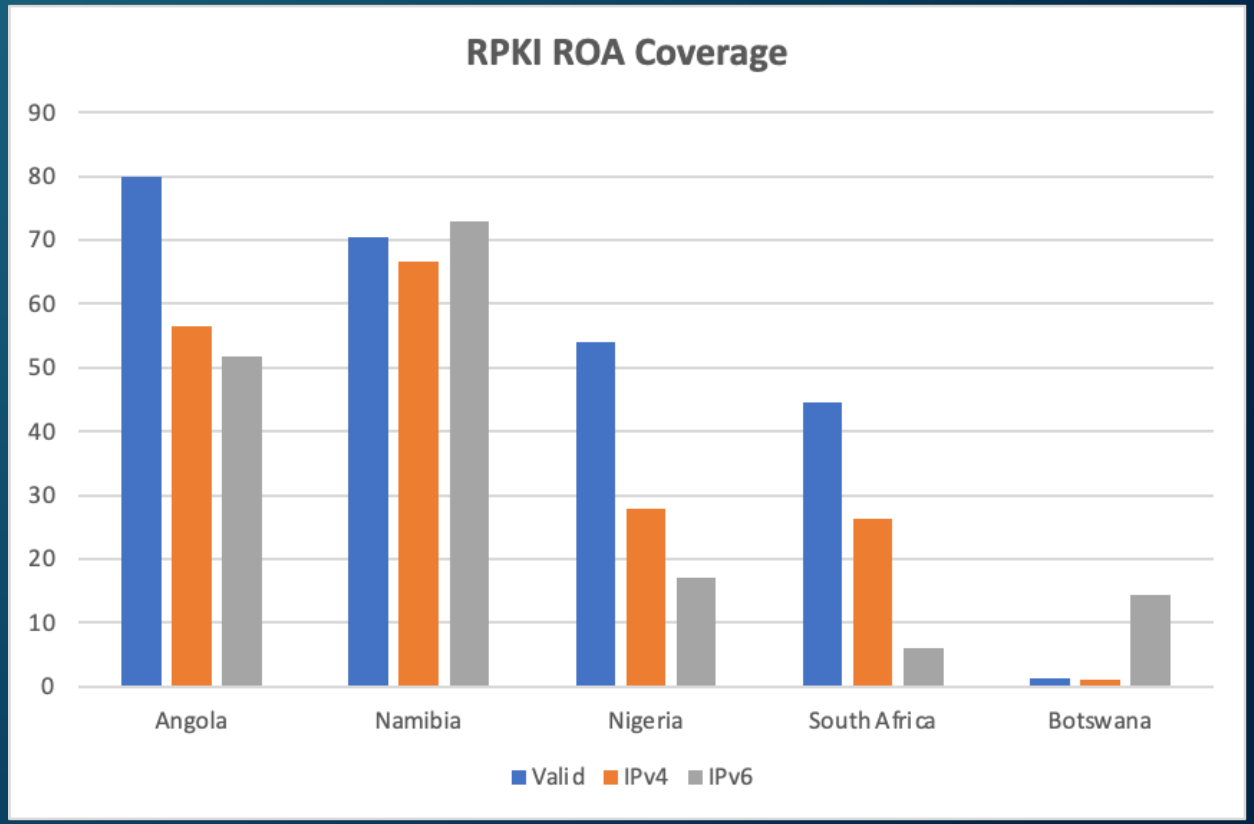
Maybe not a majority of BGP routes, but these companies account for a lot of US traffic!

Many countries are doing better than earlier stats suggest

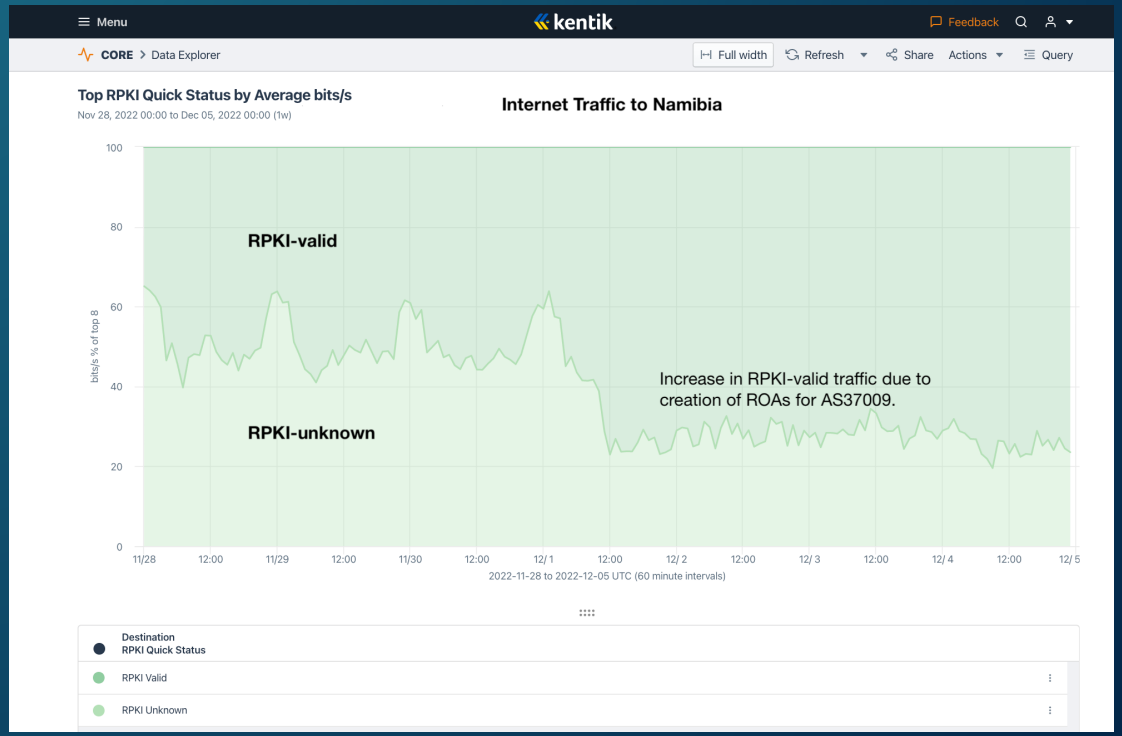
- Angola doing very well with RPKI ROA deployment!
- 79.8% traffic is RPKI-valid according to Kentik's aggregate NetFlow data.
- Biggest valid destinations
  1. AS37645 (ZAP)
  2. AS36907 (TVCabo)
  3. AS37119 (Unitel)
- Great job Angola!

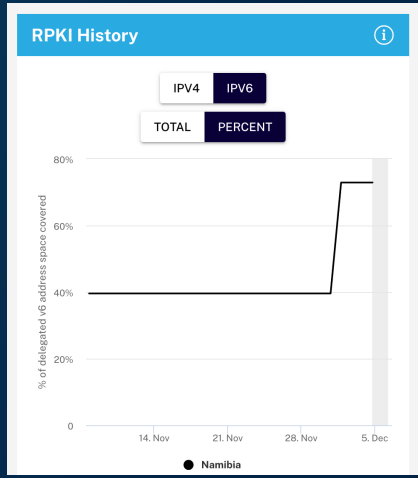


Countries in the region



Namibia’s RPKI ROA gains are very recent





https://stat.ripe.net/app/launchpad/S1_NA_C32C23C5C26C8_TMR672

Question: How much traffic goes to routes with valid ROAs?

Answer: Most of it!

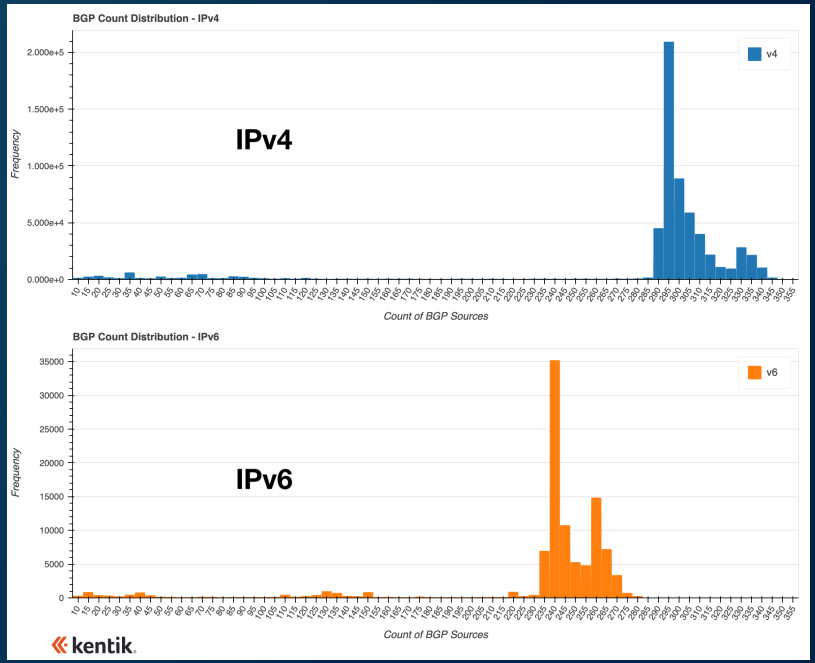
Question: How much does RPKI reduce propagation of invalids?

Answer: *Let's find out…*

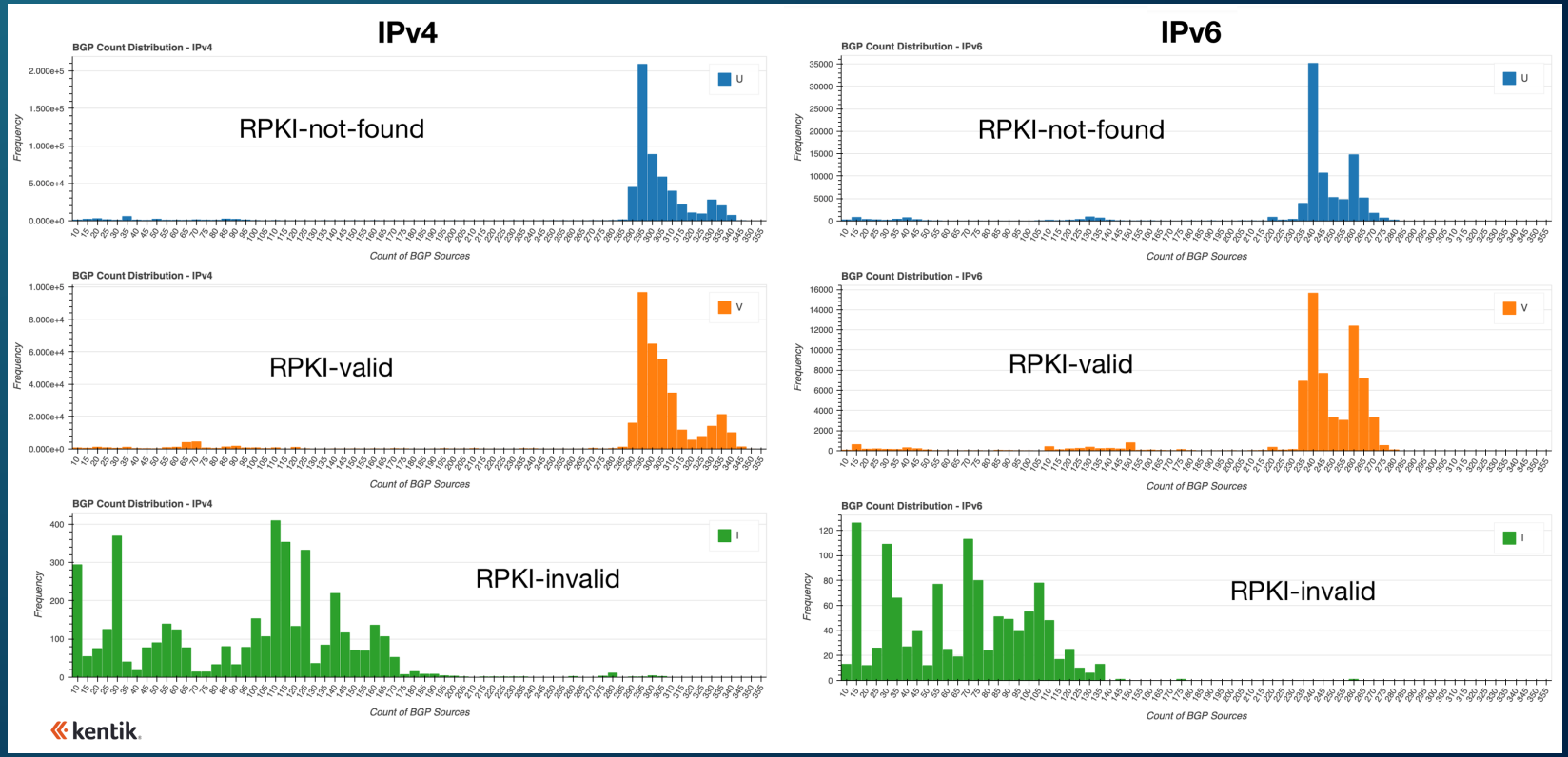
RPKI ROV & propagation of invalids

- On the right is a histogram of the number of IPv4 and IPv6 prefixes seen by count of vantage points.
- The count of vantage points can serve as a measure of route's propagation — the more vantage points, the more propagation.
- Peaks of globally routed prefixes (those seen by nearly all vantage points)
  - 295 for IPv4
  - 240 for IPv6*

* the lower number reflects the smaller number of IPv6 vantage points in the Routeviews dataset.

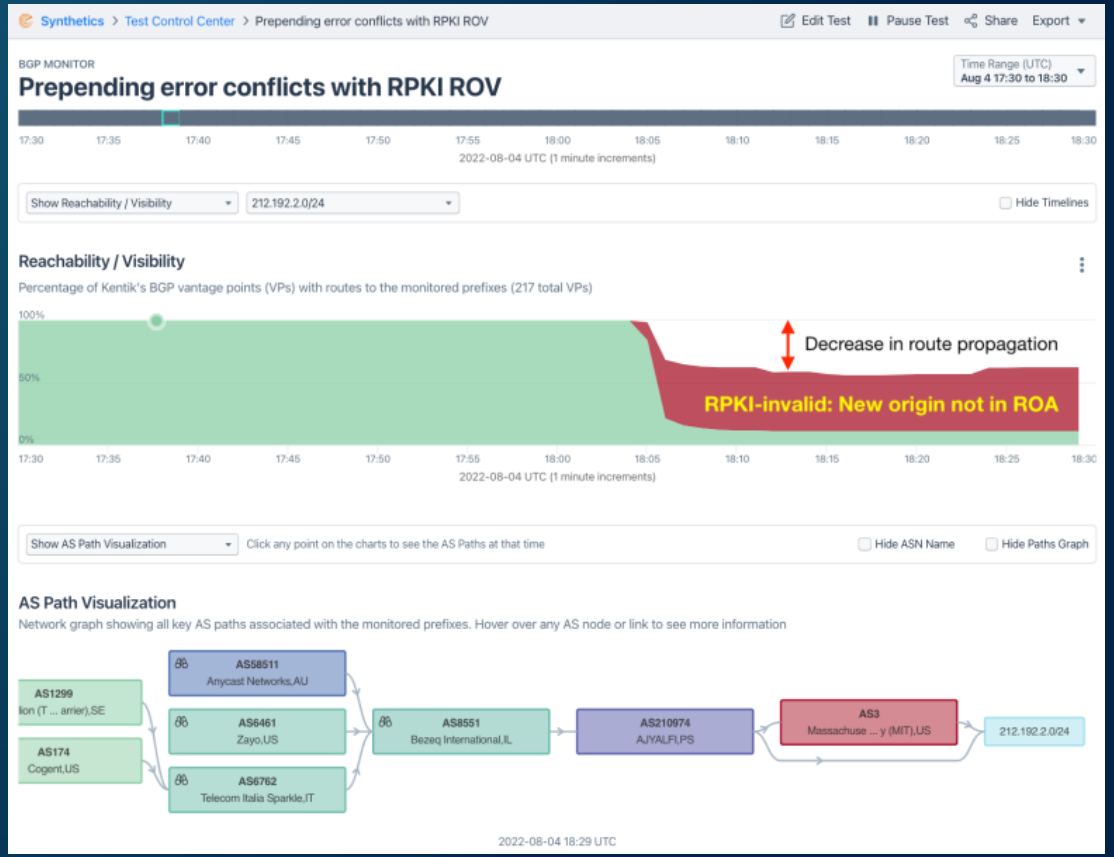


RPKI=invalid routes propagate far less than other types.



Example routes which change state from valid to invalid

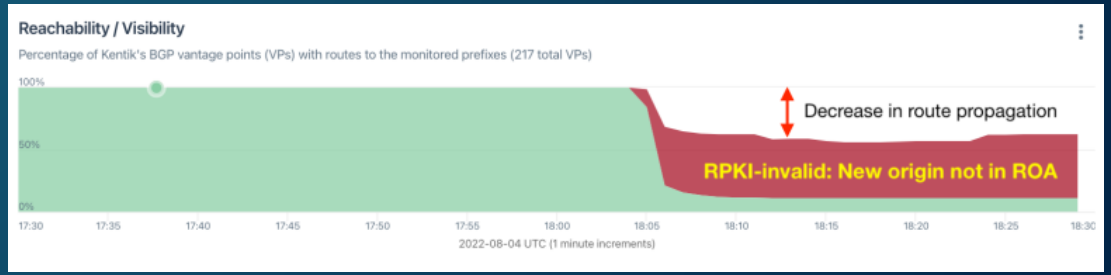
- These errors occur when a network engineer attempts to prepend an AS three times, for example, but instead ends up prepending the number 3 to the AS path.
- AS210974 changed how it announced 212.192.2.0/24 on August 4, 2022.
- It began prepending the number 3 to its AS path, however since there was a ROA for this prefix, it also caused the route to become invalid leading to a significant drop in propagation.



In Summary

Question: How much traffic goes to routes with valid ROAs?

Answer: Most of it!



Question: How much does RPKI reduce propagation of invalids?

Answer: *Evaluation of a route as RPKI-invalid reduces its propagation by 1/2 to 2/3.*

Best Current Practice – Reject RPKI-Invalid BGP routes!

Rejecting RPKI-Invalid routes on EBGP sessions…

1. Protects a majority of your outbound traffic from BGP hijacks due to typos, BGP mishaps.
2. Not a risk to legitimate traffic.

Other BCPs include:

1. Do NOT modify LOCAL_PREF based on validation states
2. Do NOT set / remove BGP communities based on validation states

Security issues like CVE-2021-41531 / CVE-2021-3761 are examples of how not following the above BCP could result in massive BGP churn!

https://bgpfilterguide.nlnog.net/guides/reject_invalids/

Questions?

dmadory @ Kentik.com
Twitter: @dougmadory