RPKI for Peering

Che-Hoo Cheng

APNIC

@Peering Asia 2.0 in HK

2018-10-24

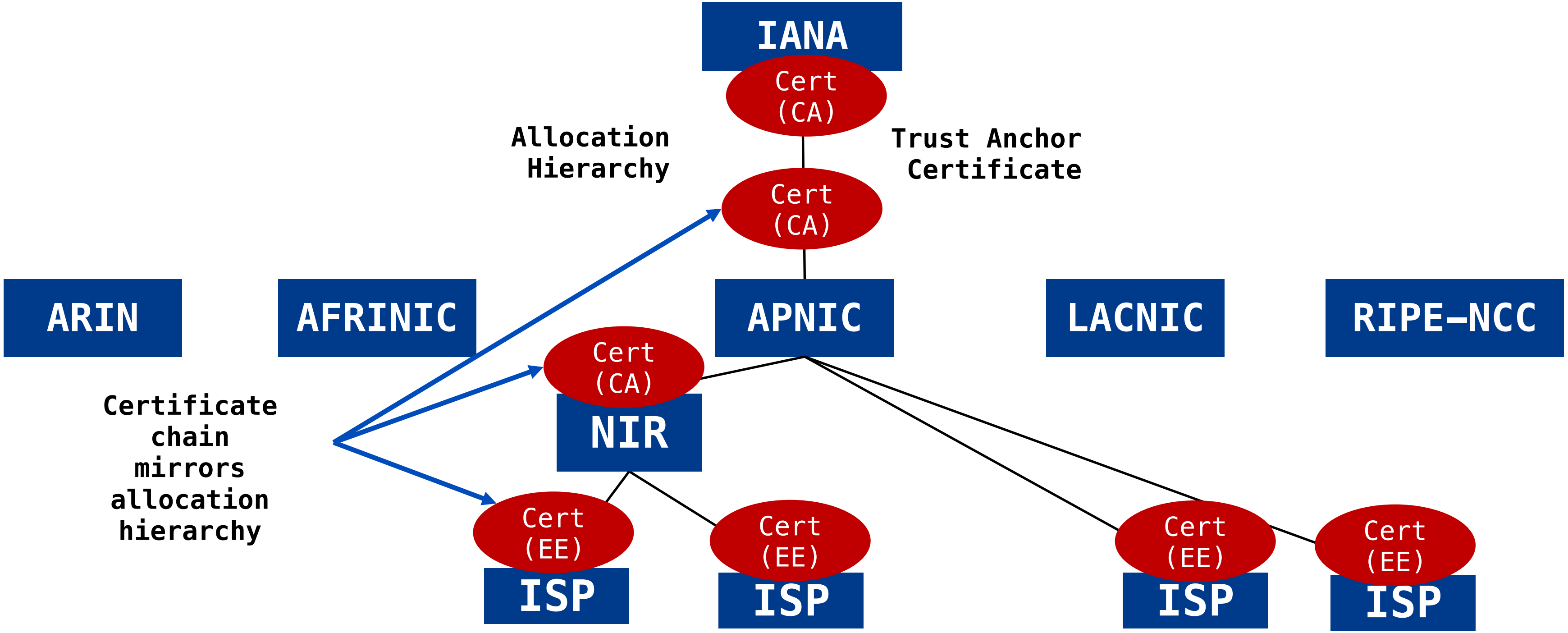
Security matters when doing peering

- You do NOT want to receive bad routing information from your peers or customers and then propagate it to your customers or peers
- You also do NOT want your own routes to be hijacked by anyone, maliciously or accidentally
- Basic measures:
  - Bogons and martians filtering
  - Max prefix count
  - IRR (Internet Routing Registry) database checking
  - *So on and so forth*
- Additional measure:
  - **RPKI (Resource Public Key Infrastructure)**

Routing Security is becoming more important than ever

- Route-hijacking cases (malicious and accidental) are more and more common
  - Big incentive for hackers
    - Hijack DNS, hijack websites, steal passwords and so on
  - Misconfiguration does happen from time to time
- And, it is extremely easy to do route-hijacking, if protection measure is not implemented
- A lot of route objects on IRR-DB are not authenticated properly and so cannot be fully trusted
- Need better authenticity for routing info, i.e. need to make sure that the route originators are the true “owners” of the relevant IP resources

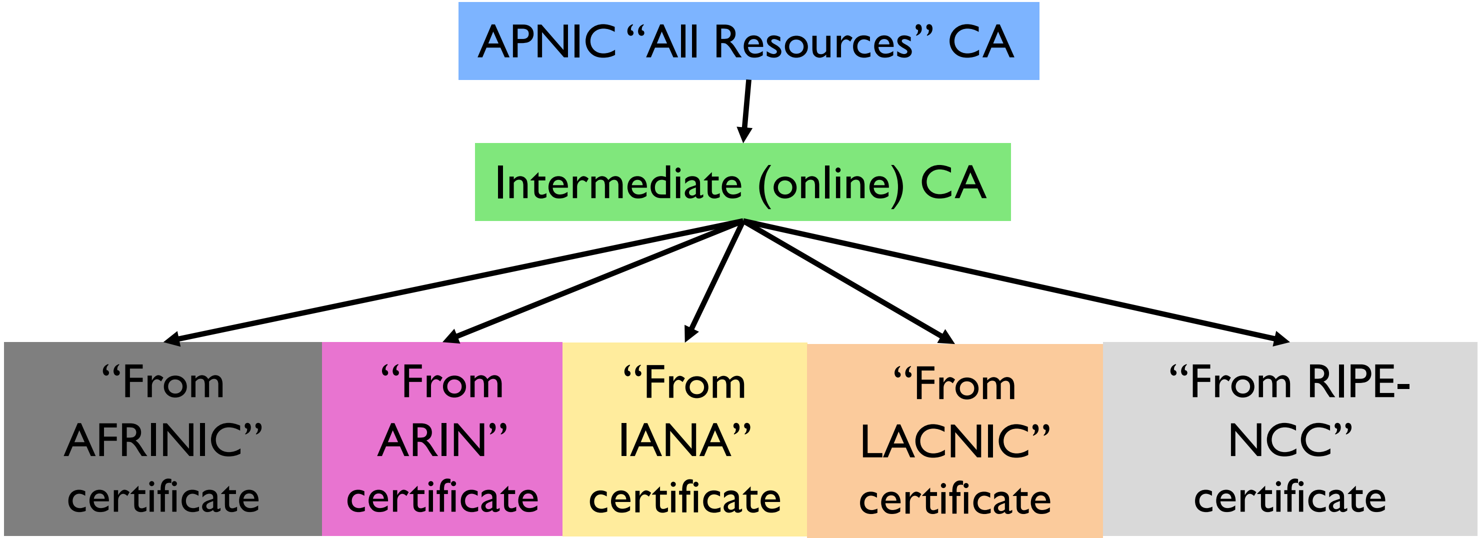
RPKI – Trust Anchor



Source : http://isoc.org/wp/ietfjournal/?p=2438

RPKI – Single Trust Anchor

- Feb 2018: a single expanded trust anchor
  - https://blog.apnic.net/2018/02/27/updating-rpki-trust-anchor-configuration/



RPKI – ROA

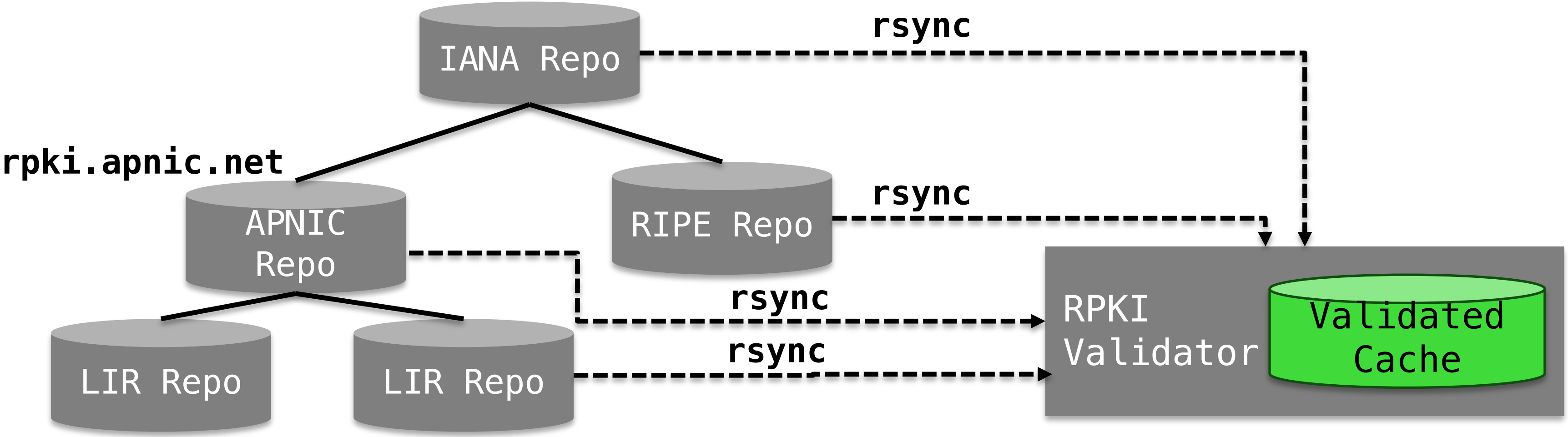
- Route Origin Authorization
  - Digitally signed object – list of prefixes and nominated ASN

Prefix	203.176.32.0/19
Max-length	/24
Origin ASN	**AS17821**

  - Multiple ROAs can exist for the same prefix

RPKI Validator

- Gathers ROAs from the distributed RPKI database
- Validates each entry's (ROA) signature
  - Creates a validated cache



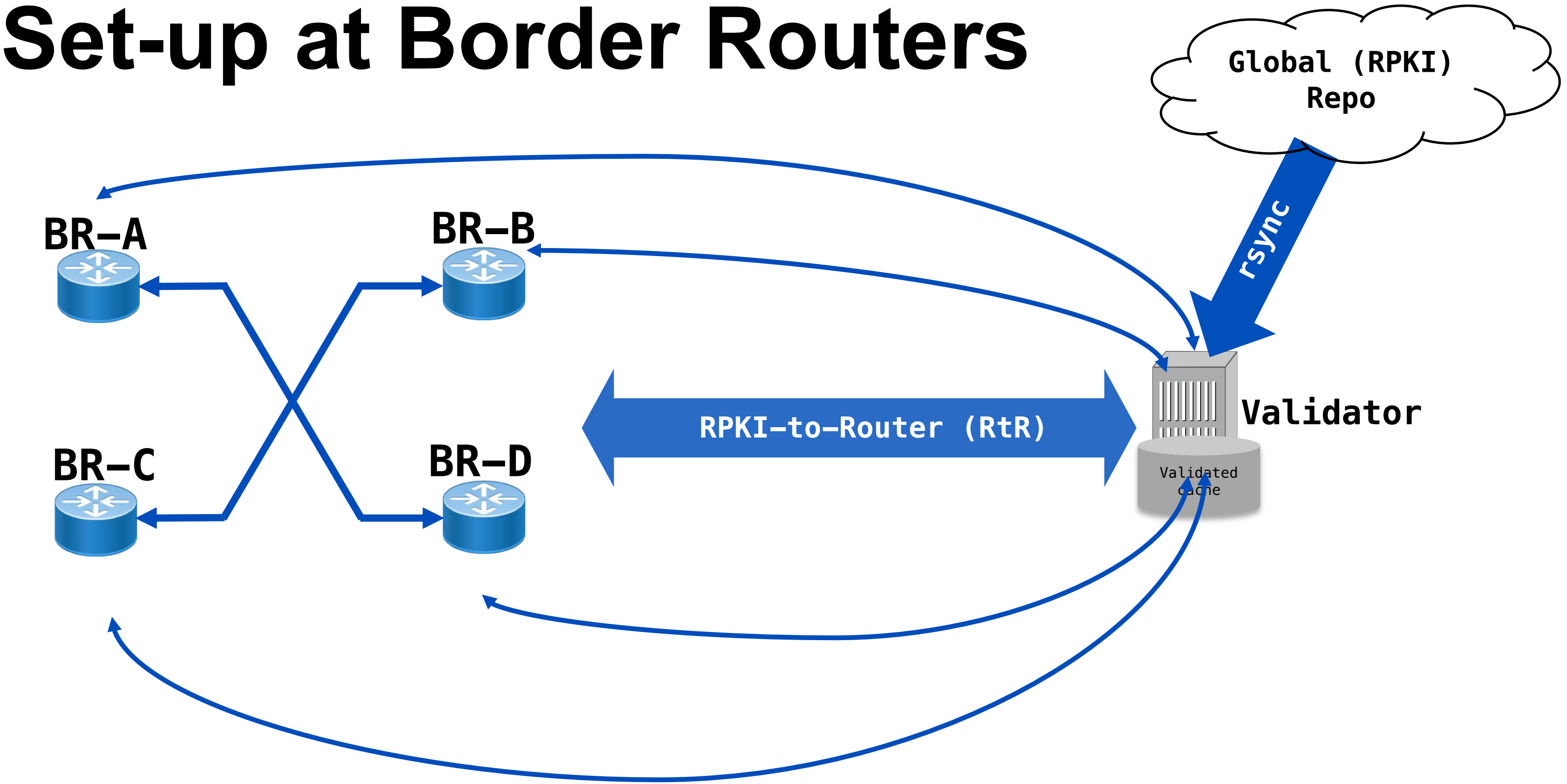
RPKI Validator Options

- Available validators
  - Dragon Research toolkit
    - https://github.com/dragonresearch/rpki.net
  - RIPE validator :
    - https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources
  - Routinator
    - https://github.com/NLnetLabs/routinator
  - RTRlib (bird, FRR, Quagga…)
    - https://rtrlib.realmv6.org/

RPKI Validation States

- **Valid**
  - Prefix, Origin ASN and prefix-length match those found on database
- **Not Found (Unknown)**
  - No valid ROA found
    - Neither valid nor invalid (perhaps ROA not created)
- **Invalid**
  - Prefix is found on database, but Origin ASN is wrong, OR
  - Prefix-length is longer than the Max-length

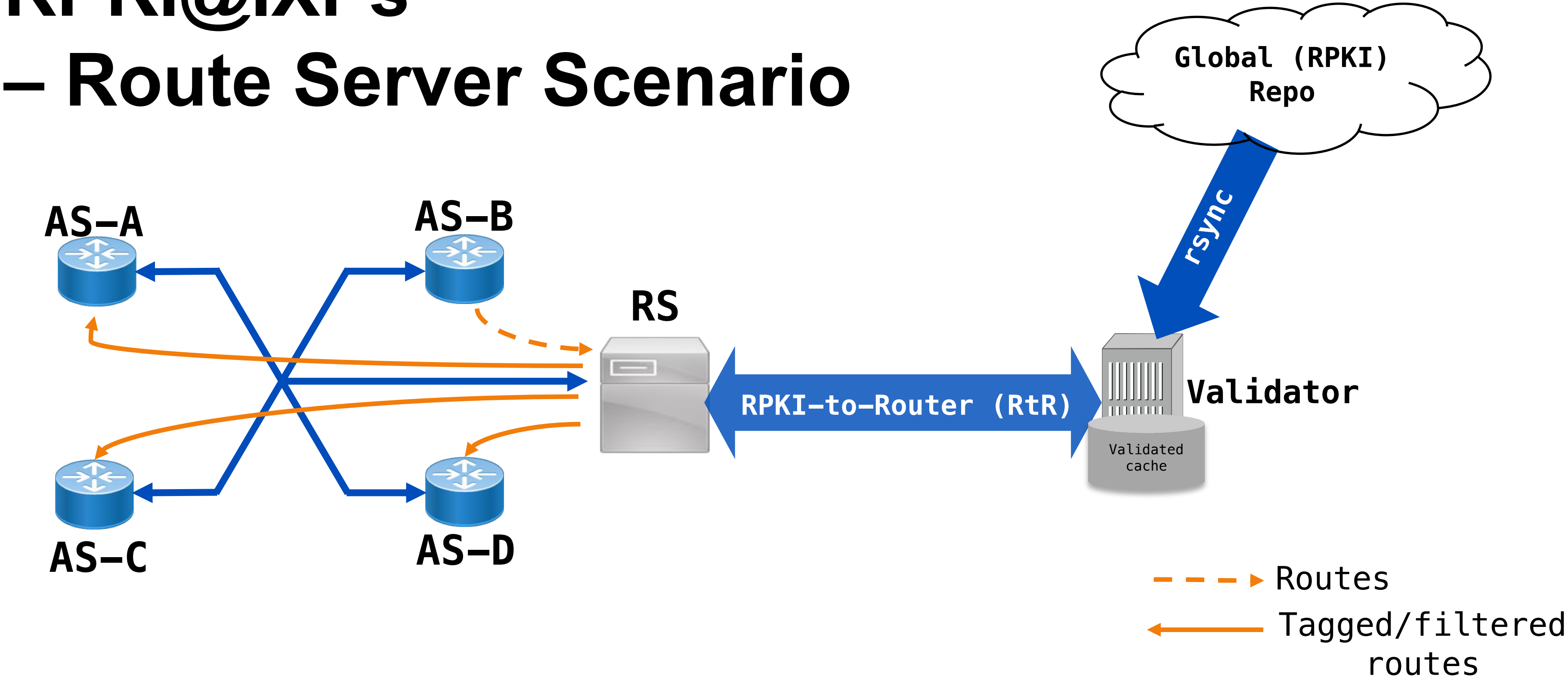
Set-up at Border Routers



Options when seeing invalid routes

- For End/Stub Networks:
  - Drop them, OR
  - Give them lower LOCAL_PREF, OR
  - Do nothing (not recommended)
- For Transit Networks:
  - For inbound routes from upstreams / peers:
    - Give them lower LOCAL_PREF, OR
    - Drop them, OR
    - Do nothing (not recommended)
  - For outbound routes to customers:
    - Tag them before re-distributing them to customers and allow customers to make their own choices

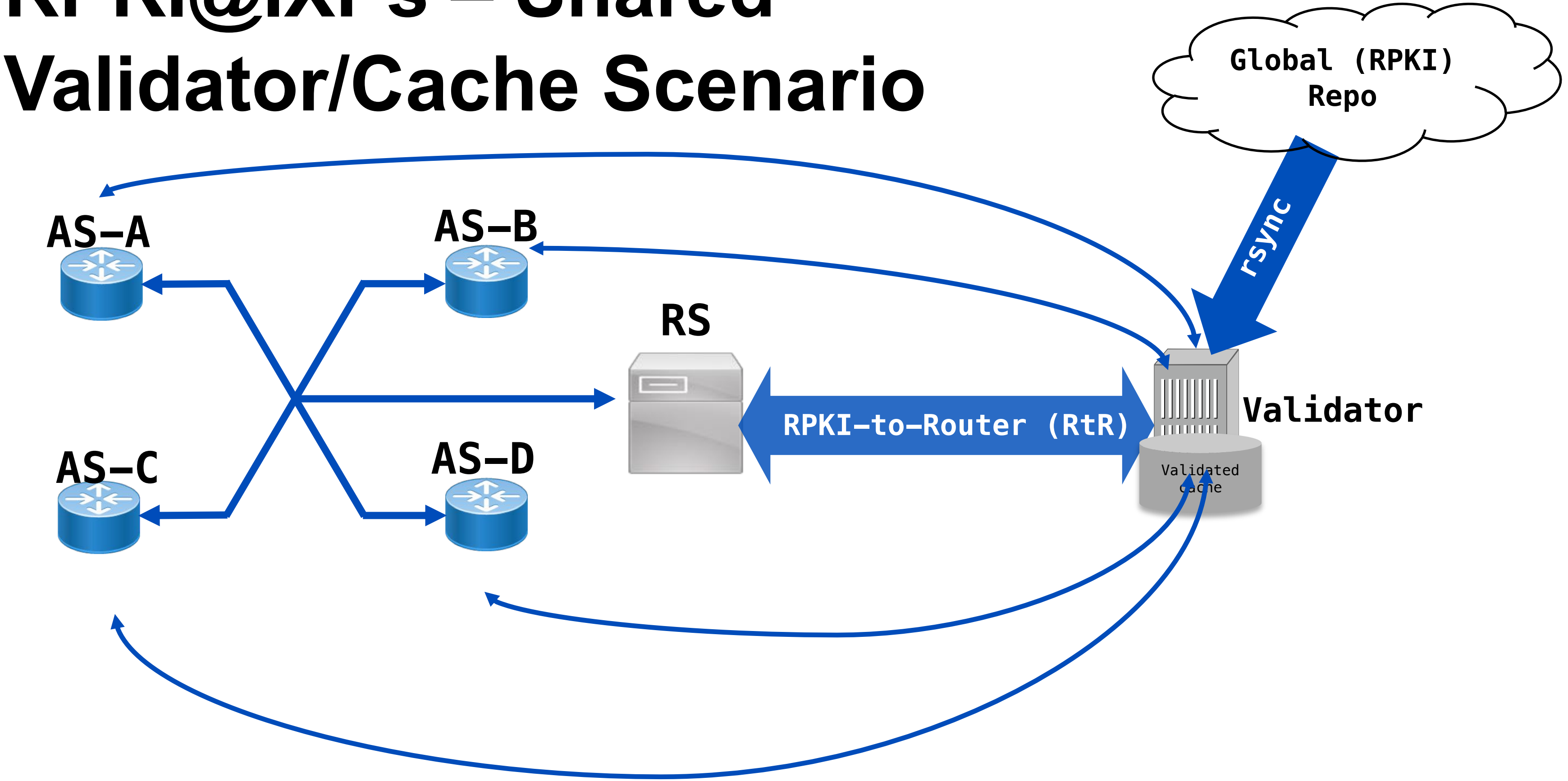
RPKI@IXPs – Route Server Scenario



RPKI@IXPs – RS Usage Options

- Similar to the case of Transit Networks
- Lower LOCAL_PREF, OR
- Filtering
  - Do not advertise **Invalid** routes
  - Need to publish on RS policy
- Tagging
  - Apply community tags based on the validation state
    - let individual member ASNs act on the validation states
  - Example:
    - **Valid** (*ASN:65XX1*)
    - **Not Found** (*ASN:65XX2*)
    - **Invalid** (*ASN:65XX3*)

RPKI@IXPs – Shared Validator/Cache Scenario



RPKI@IXPs – Examples in Asia Pacific

- Shared Validator/Cache
  - JPNAP, BKNIX & Cloudflare (non-IXP)
- Other IXPs?
  - You may push your IXPs to support it to ease your burden of setting up your own Validator/Cache
  - IXPs are good locations to place shared Validator/Cache as they are just one hop away from their participants and they are mostly trustable

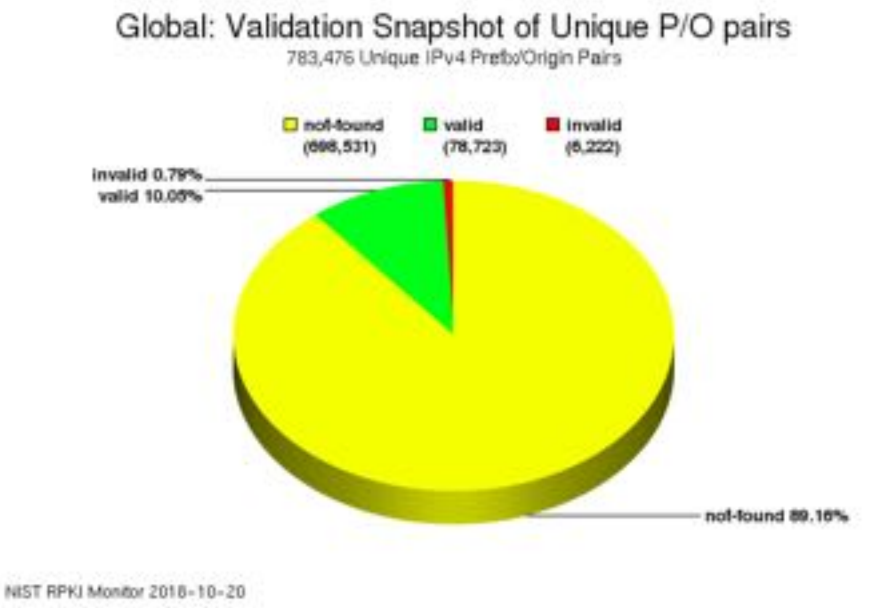
RPKI for Peering – Why?

- Contribute to Global Routing Security
  - Help reduce the effect of route hijacking or misconfiguration
  - Protect your own networks and your customers better
- Collaborative effort among network operators is key

RPKI is NOT a bullet-proof solution

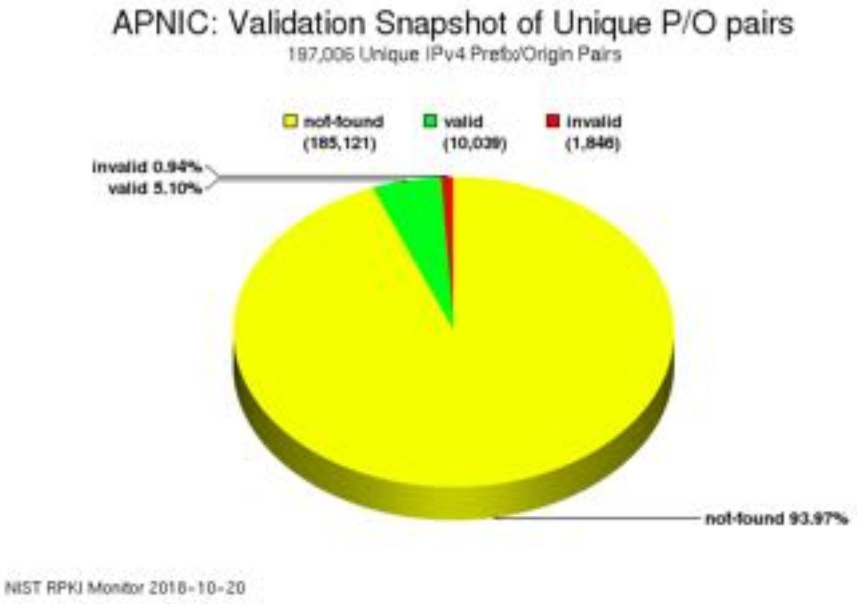
- But it helps improve the situation, especially if everybody does it
- Coupled with more and more direct peering, the protection for routing security should be more effective

RPKI Situation Globally



- Source: https://rpki-monitor.antd.nist.gov/?p=0&s=0

RPKI Situation of APNIC Region



- Source: https://rpki-monitor.antd.nist.gov/?p=3&s=0

Important First Step

- Create your own ROAs at relevant registries to better protect your own routes
  - And encourage your peers/customers to do the same
  - **For APNIC members, it is easy to do it on MyAPNIC**
    - **If you need help or want to learn more, please feel free to contact our colleague Tom Do who is here these 2 days**
    - **Or you can contact APNIC Helpdesk any time (https://www.apnic.net/get-ip/helpdesk/)**
- Next step is to do route validation at your border routers
  - With or without your own validators

References

- https://datatracker.ietf.org/meeting/100/materials/slides-100-sidrops-rpki-deployment-with-ixps-01
- https://datatracker.ietf.org/meeting/90/materials/slides-90-opsec-0
- https://www.ripe.net/support/training/ripe-ncc-educa/presentations/use-cases-stavros-konstantaras.pdf
- https://www.franceix.net/en/technical/france-ix-route-servers/
- https://blog.cloudflare.com/rpki-details/

Questions?