RPKI In 30 Minutes Or Less

A short introduction to the technology and operations of Resource Public Key Infrastructure for Routing Security

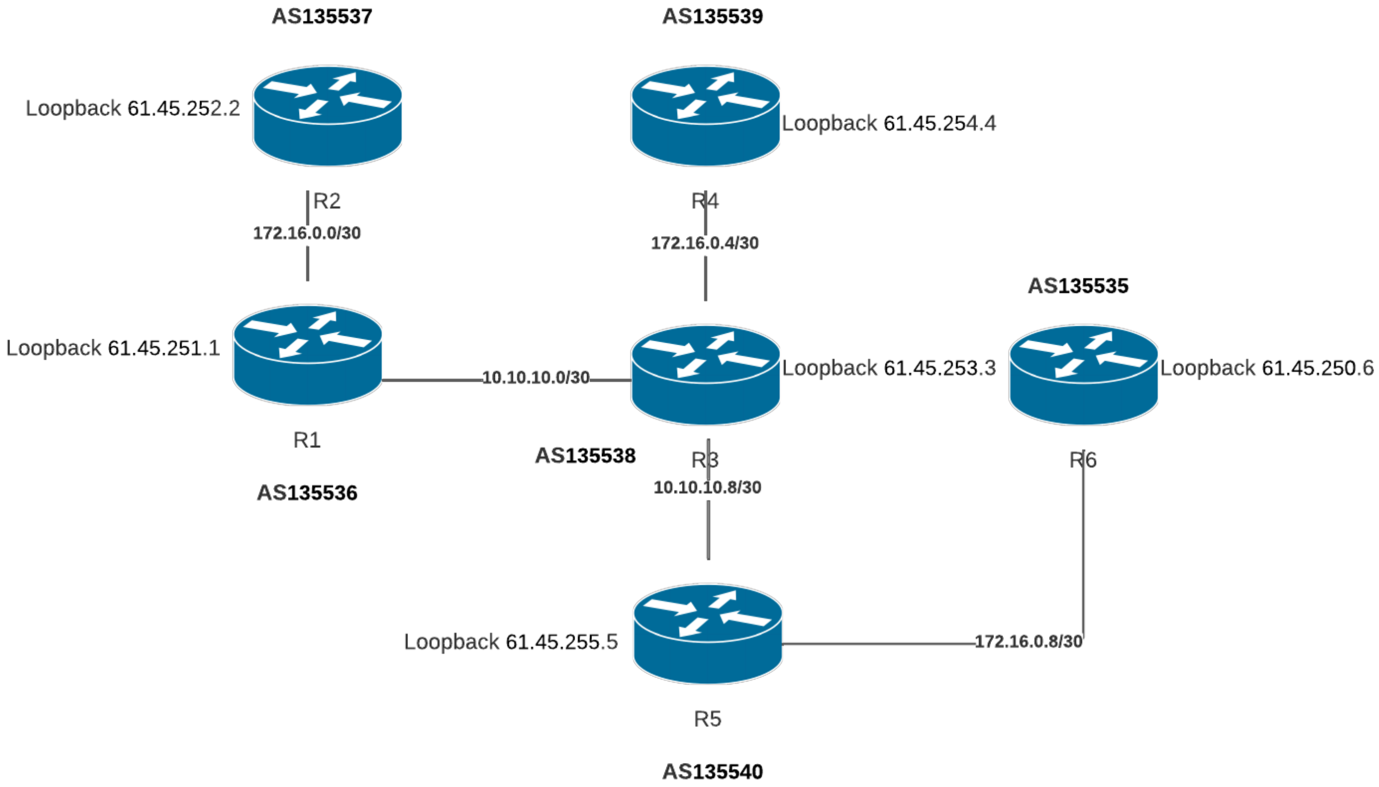
https://academy.apnic.net/

The Problem?

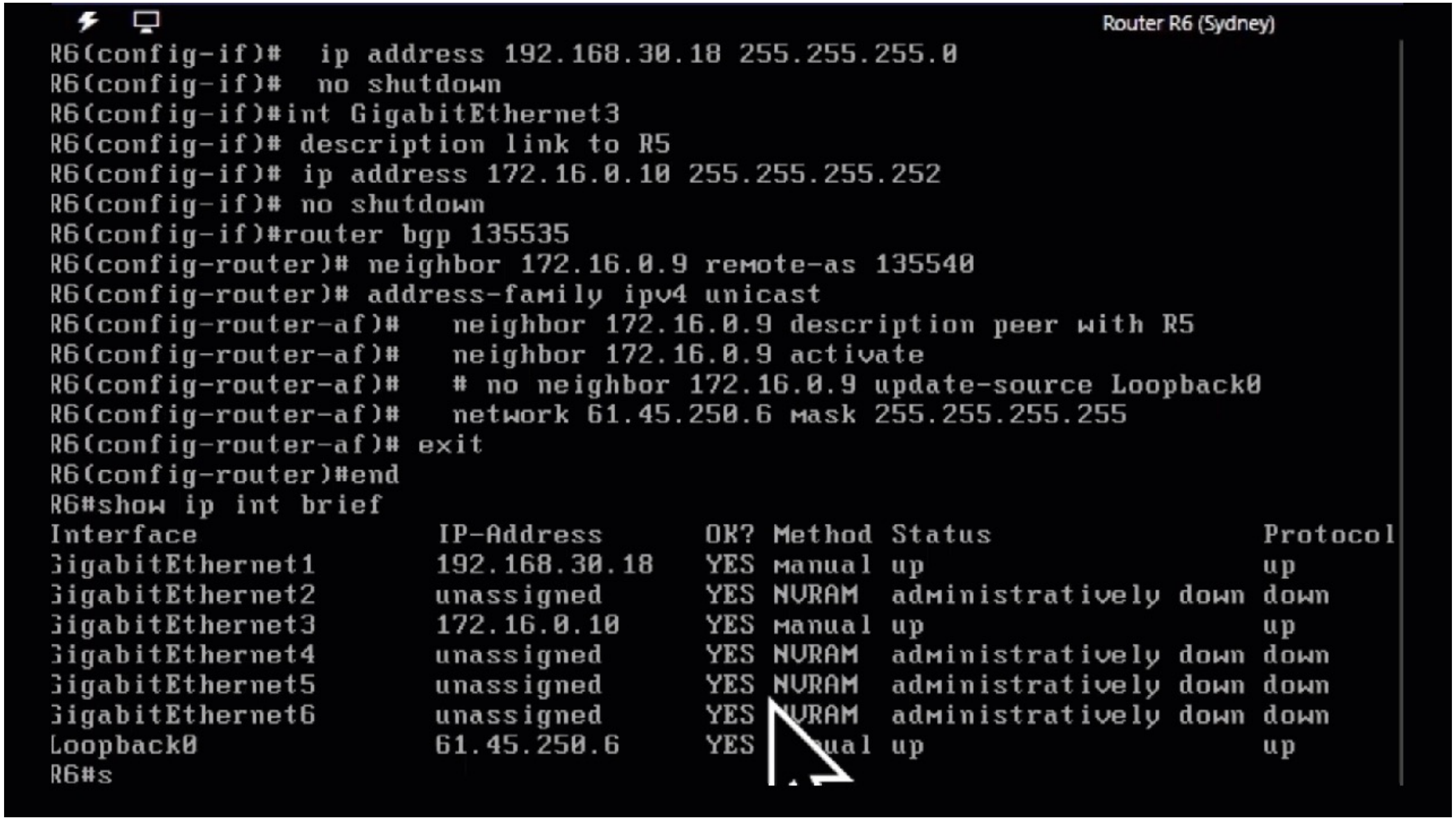
- BGP since inception has not been secure.
- Increasingly leakage of routes have caused outages.
- These incidents are not always accidents.
- Where to start?

https://blog.apnic.net/2021/07/13/readthedocs/

Demo: BGP Hijack

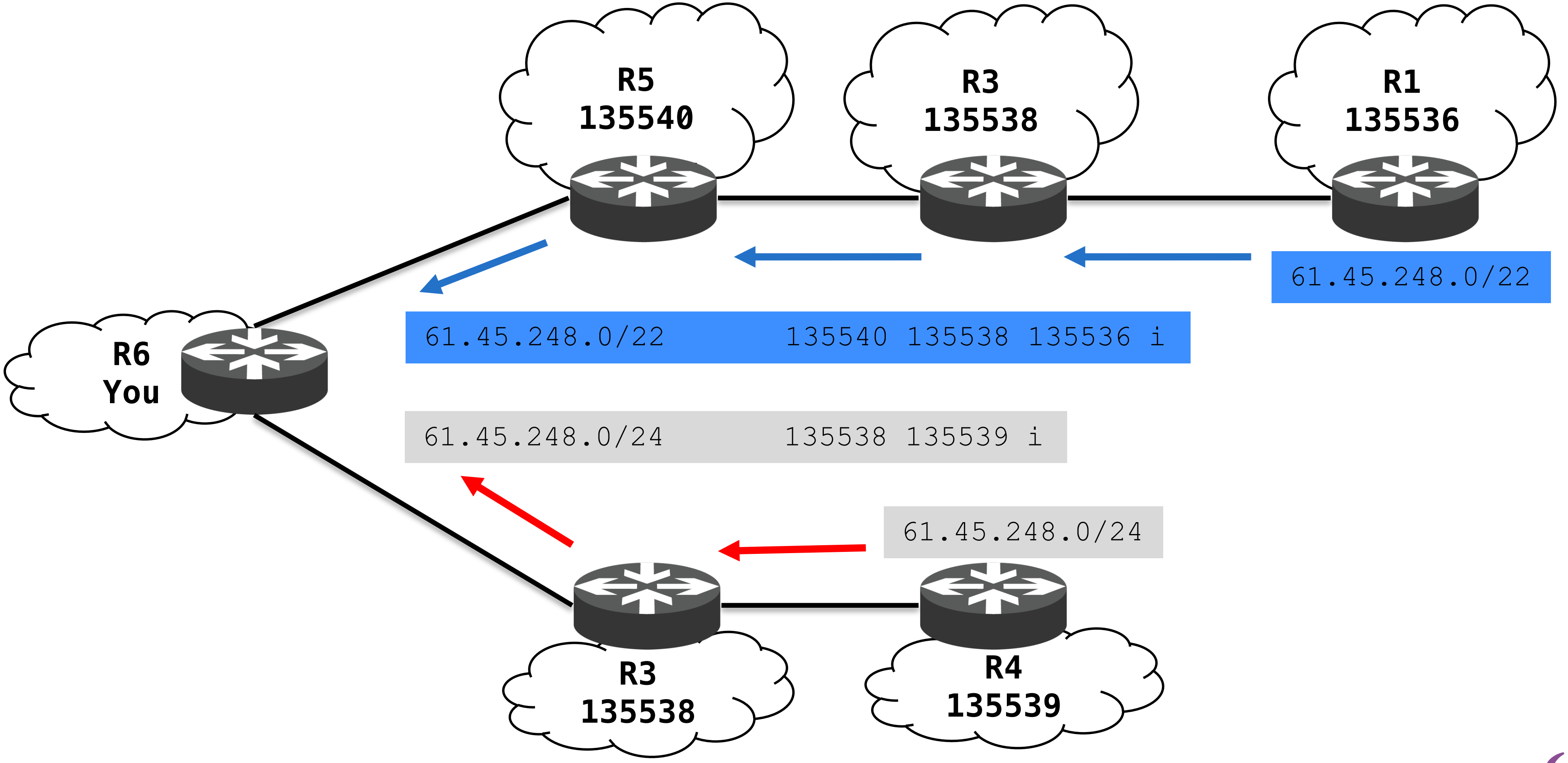


Demo: BGP Hijack



```
R6(config-if)#  ip address 192.168.30.18 255.255.255.0
R6(config-if)#  no shutdown
R6(config-if)#int GigabitEthernet3
R6(config-if)# description link to R5
R6(config-if)# ip address 172.16.0.10 255.255.255.252
R6(config-if)# no shutdown
R6(config-if)#router bgp 135535
R6(config-router)# neighbor 172.16.0.9 remote-as 135540
R6(config-router)# address-family ipv4 unicast
R6(config-router-af)#   neighbor 172.16.0.9 description peer with R5
R6(config-router-af)#   neighbor 172.16.0.9 activate
R6(config-router-af)#   # no neighbor 172.16.0.9 update-source Loopback0
R6(config-router-af)#   network 61.45.250.6 mask 255.255.255.255
R6(config-router-af)# exit
R6(config-router)#end
R6#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       192.168.30.18   YES manual up                    up
GigabitEthernet2       unassigned      YES NVRAM  administratively down down
GigabitEthernet3       172.16.0.10     YES manual up                    up
GigabitEthernet4       unassigned      YES NVRAM  administratively down down
GigabitEthernet5       unassigned      YES NVRAM  administratively down down
GigabitEthernet6       unassigned      YES NVRAM  administratively down down
Loopback0              61.45.250.6     YES manual up                    up
R6#s
```

IP Route Lookup



RPKI

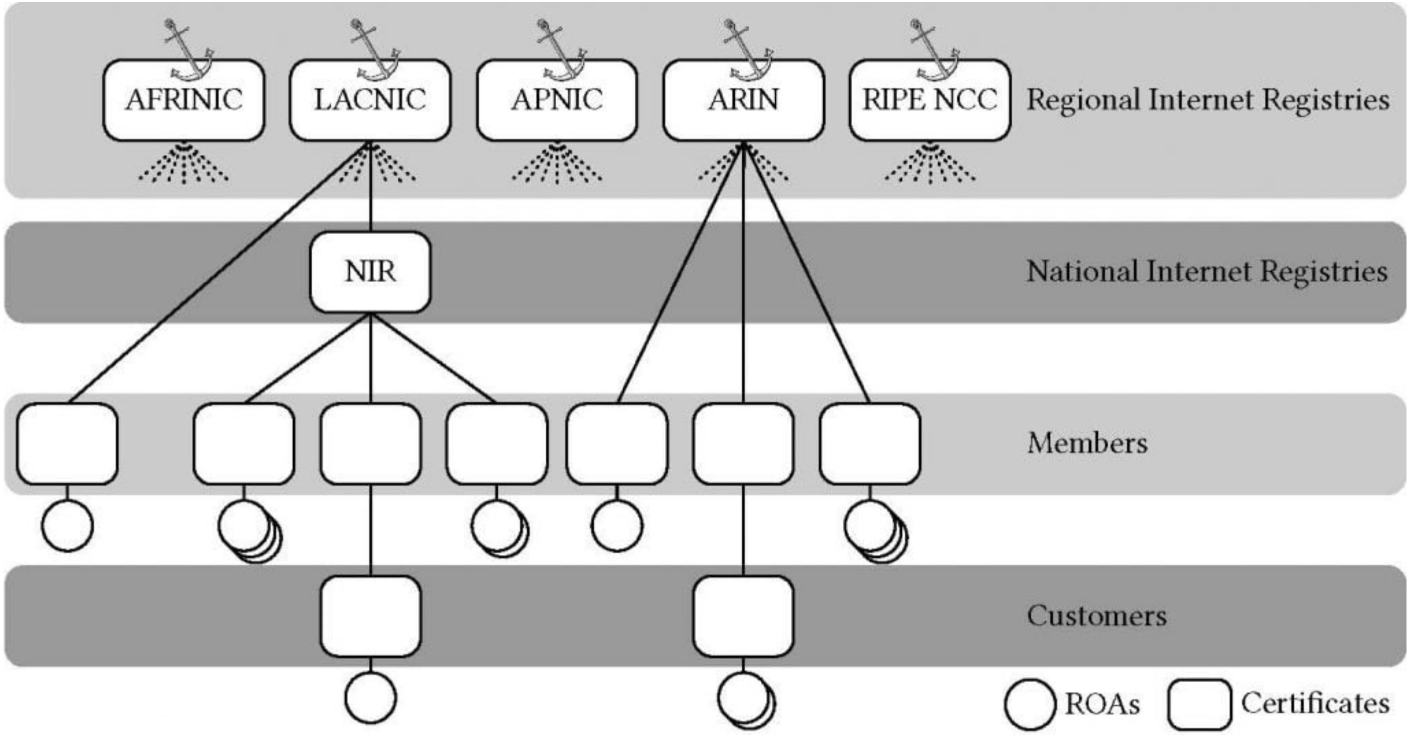
- Resource **Public Key Infrastructure**
- Real assignment data from the five (5) Regional Internet Registries
- Attestation of the ***ORIGIN*** *Autonomous System Number* for internet addresses.
- RSA Cryptography.

https://blog.apnic.net/2020/04/21/rpki-and-trust-anchors/

Certificates, Authorities and Routes: OH MY!

Key Concept 1:

ROUTE ORIGIN AUTHORISATION

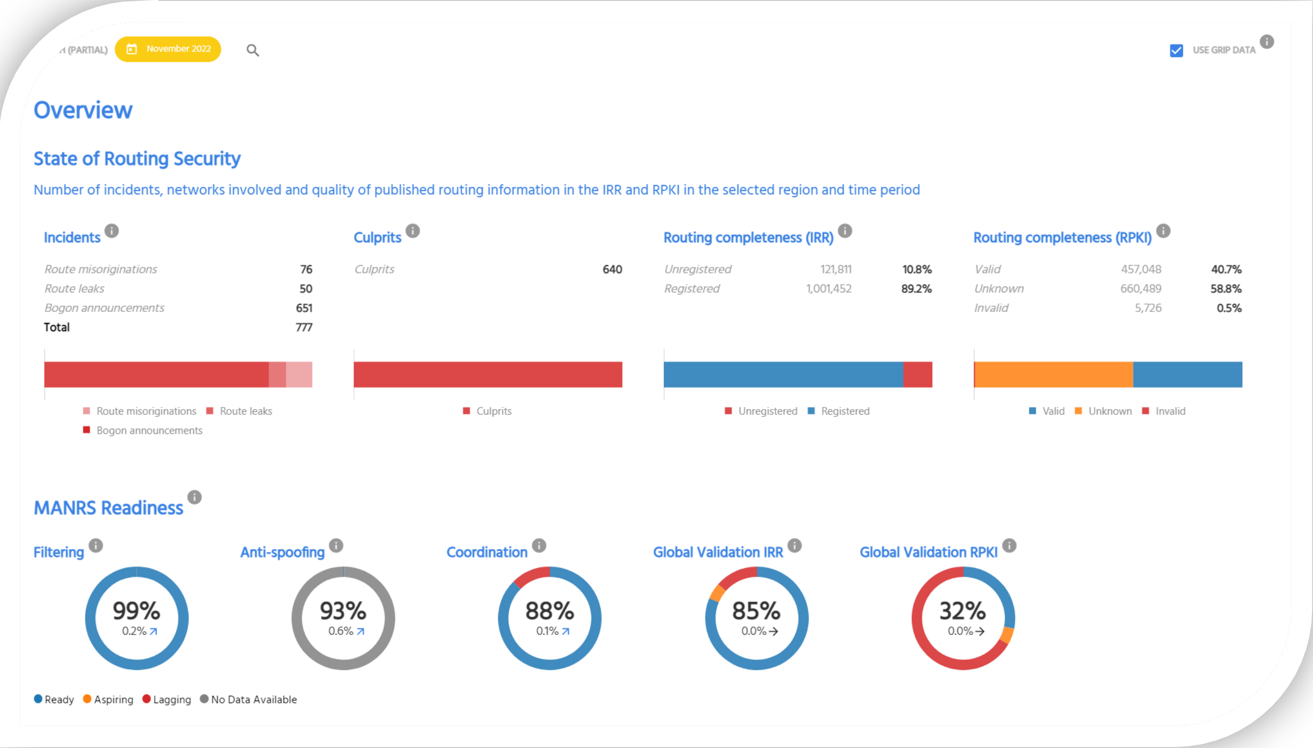


https://blog.apnic.net/2019/09/11/how-to-creating-rpki-roas-in-myapnic/

Check ROA Progress

https://observatory.manrs.org/#/overview

MANRS



(PARTIAL) November 2022

☑ USE GRIP DATA

Overview

State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents

Route misoriginations	76
Route leaks	50
Bogon announcements	651
Total	777

Culprits

Culprits	640

Routing completeness (IRR)

Unregistered	121,811	10.8%
Registered	1,001,452	89.2%

Routing completeness (RPKI)

Valid	457,048	40.7%
Unknown	660,489	58.8%
Invalid	5,726	0.5%

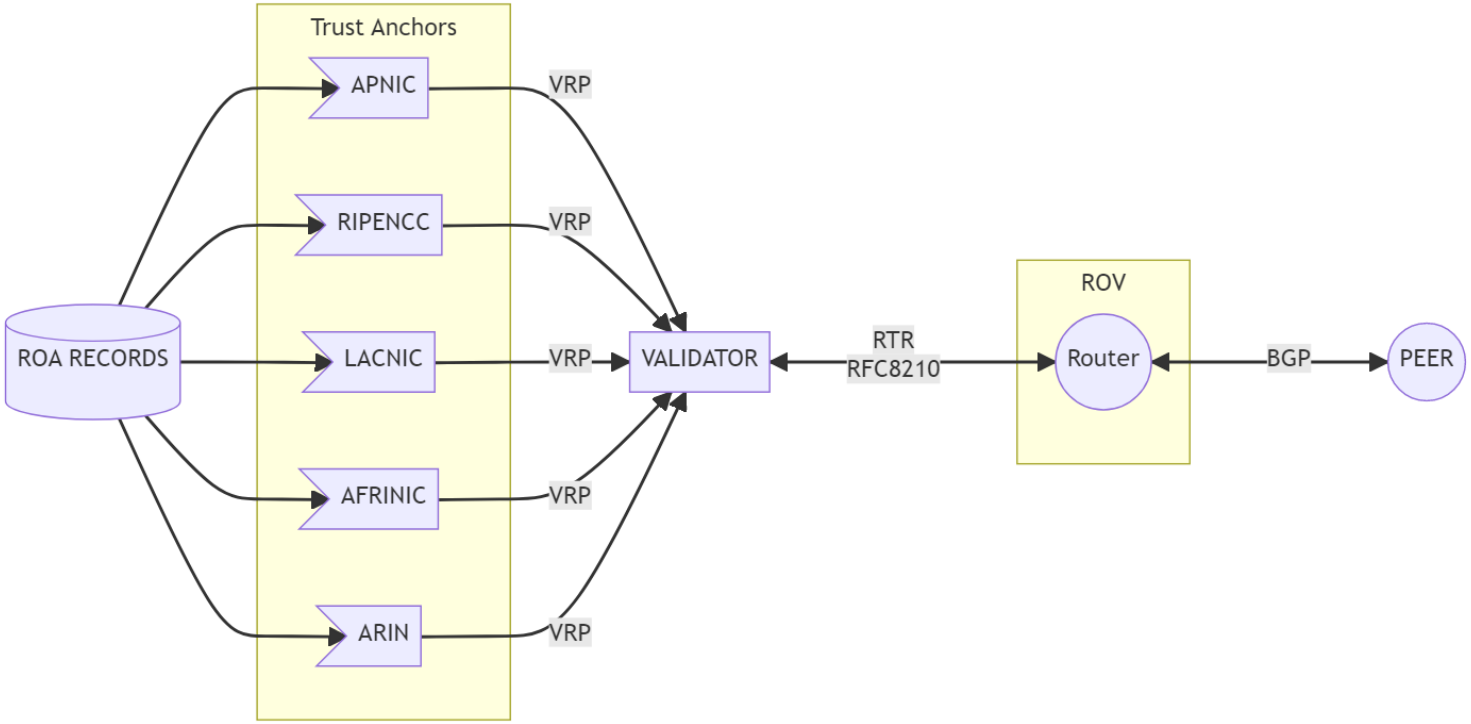
MANRS Readiness

Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
99% 0.2% ↗	93% 0.6% ↗	88% 0.1% ↗	85% 0.0% →	32% 0.0% →

There is more to do …

Key Concept 2:

ROUTE ORIGIN VALIDATION



https://rpki.readthedocs.io/en/latest/index.html#sec-rpki-ops

Are ROAs enough?

- What if I forge the origin AS in the AS path?
  - Would be accepted as good – pass origin validation!
- Which means, we need to secure the AS path as well
  - AS path validation (per-prefix)
- We can use RPKI certificates for this
- What if the IP address (IP spoofing) is forged?
  - Requires other methods, like ingress filtering refer to BCP38

What is missing from Routing Security?

☑ Origins RPKI

https://www.rfc-editor.org/rfc/rfc8210

☒ Pathways ASPA

https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-verification/

☒ ASN to ASN BGPSEC

https://www.rfc-editor.org/rfc/rfc8205.html

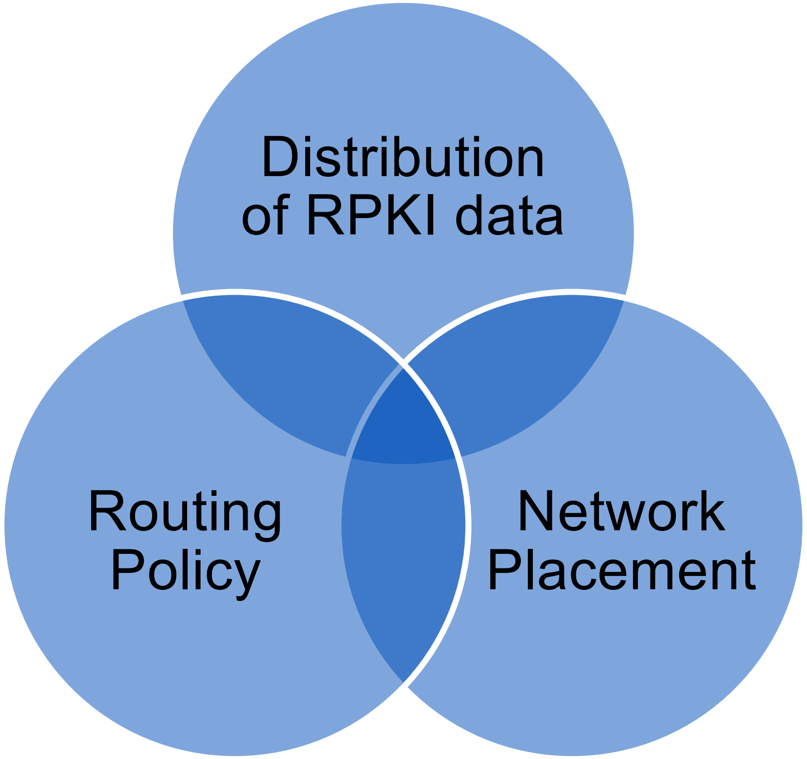
Deployment Considerations

“The Basics”

- RFC7115+RFC9319 / BCP185
- https://datatracker.ietf.org/doc/html/rfc7115
- https://datatracker.ietf.org/doc/html/rfc9319

https://www.google.com/search?q=rpki+deployment

“The Three”



Routing Policy?

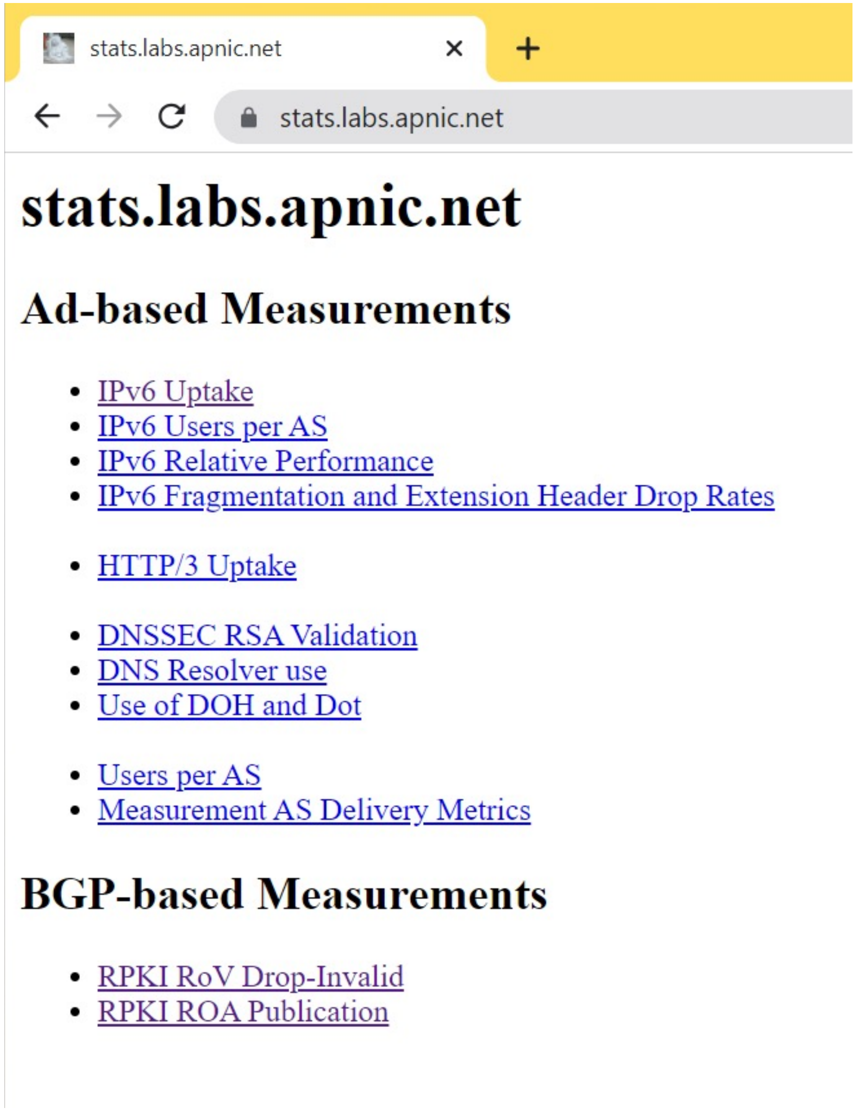
Photo by Markus Spiske on Unsplash

RPKI Uptake?

Stats.Labs.APNIC.Net

- RPKI RoV Drop-Invalid
- RPKI ROA Publication

Are ***your*** routes signed and have you started to ***drop*** invalid routes?



stats.labs.apnic.net

Ad-based Measurements

- IPv6 Uptake
- IPv6 Users per AS
- IPv6 Relative Performance
- IPv6 Fragmentation and Extension Header Drop Rates

- HTTP/3 Uptake

- DNSSEC RSA Validation
- DNS Resolver use
- Use of DOH and Dot

- Users per AS
- Measurement AS Delivery Metrics

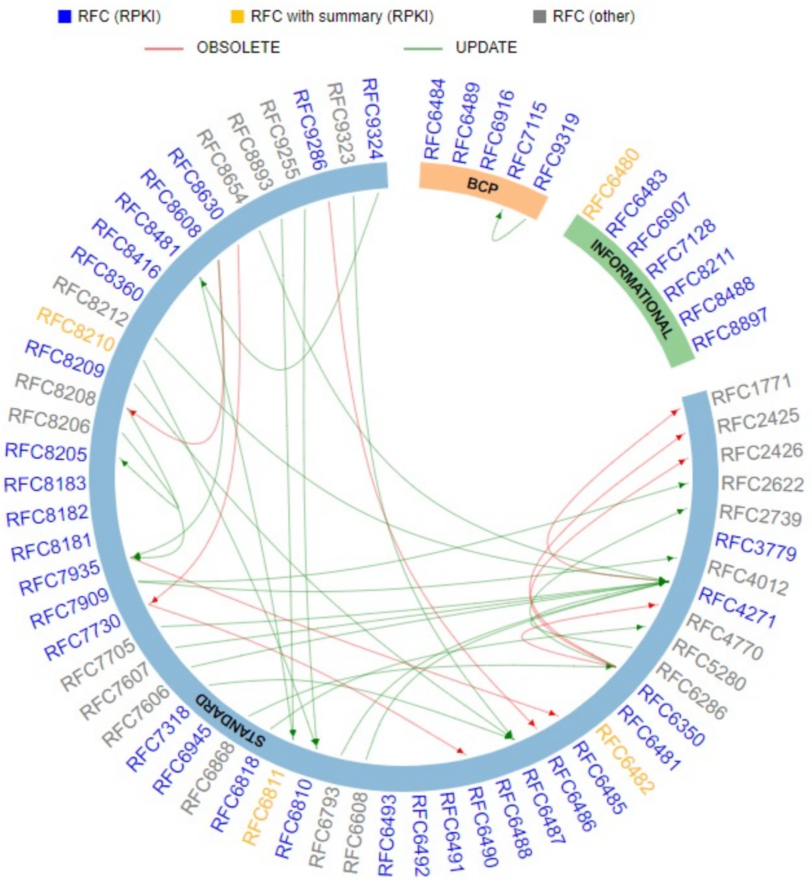
BGP-based Measurements

- RPKI RoV Drop-Invalid
- RPKI ROA Publication

Which RFC to read?

- Must read
- Should read
- May read

https://rpki-rfc.routingsecurity.net



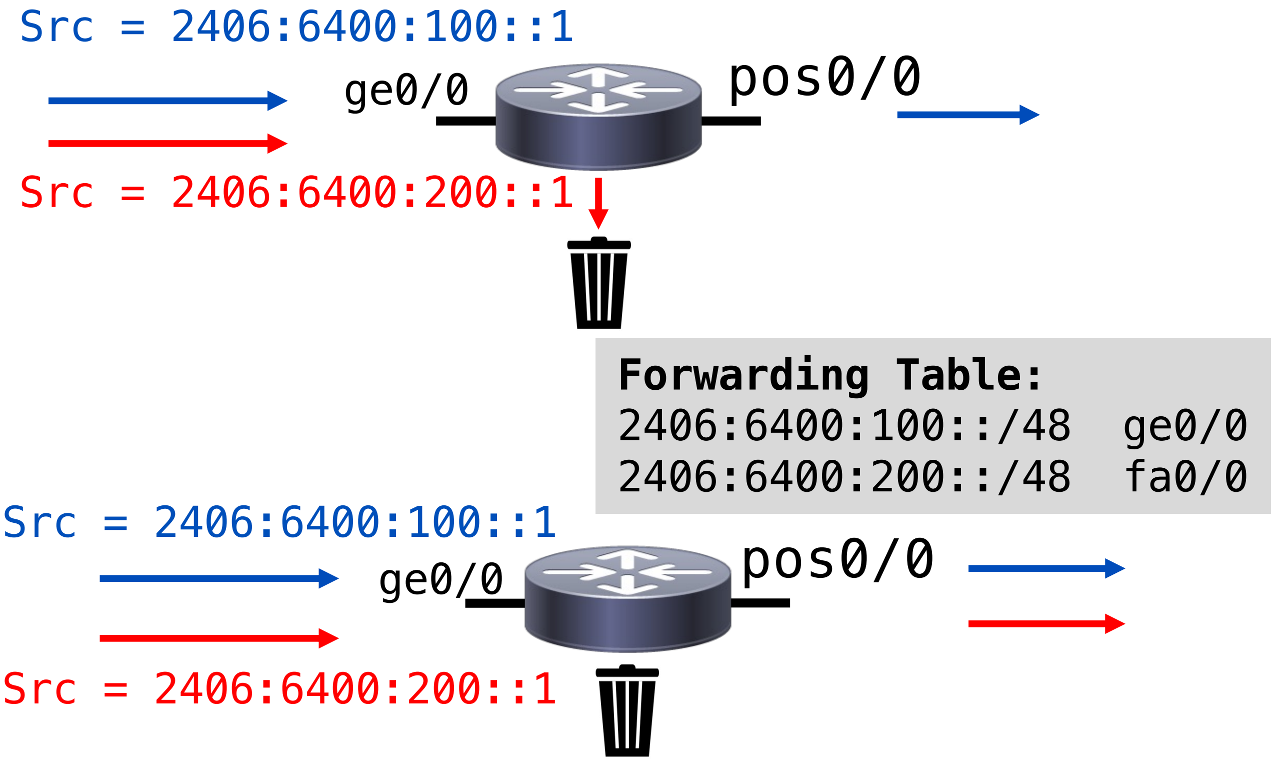
Source IP spoofing – Mitigation

- BCP38 (RFC2827)
  - Since 1998!
  - https://tools.ietf.org/html/bcp38

- Only allow traffic with valid source addresses to
  - Leave your network
    - Only from your own address space
  - To enter/transit your network
    - Only from downstream customer address space

uRPF – Unicast Reverse Path

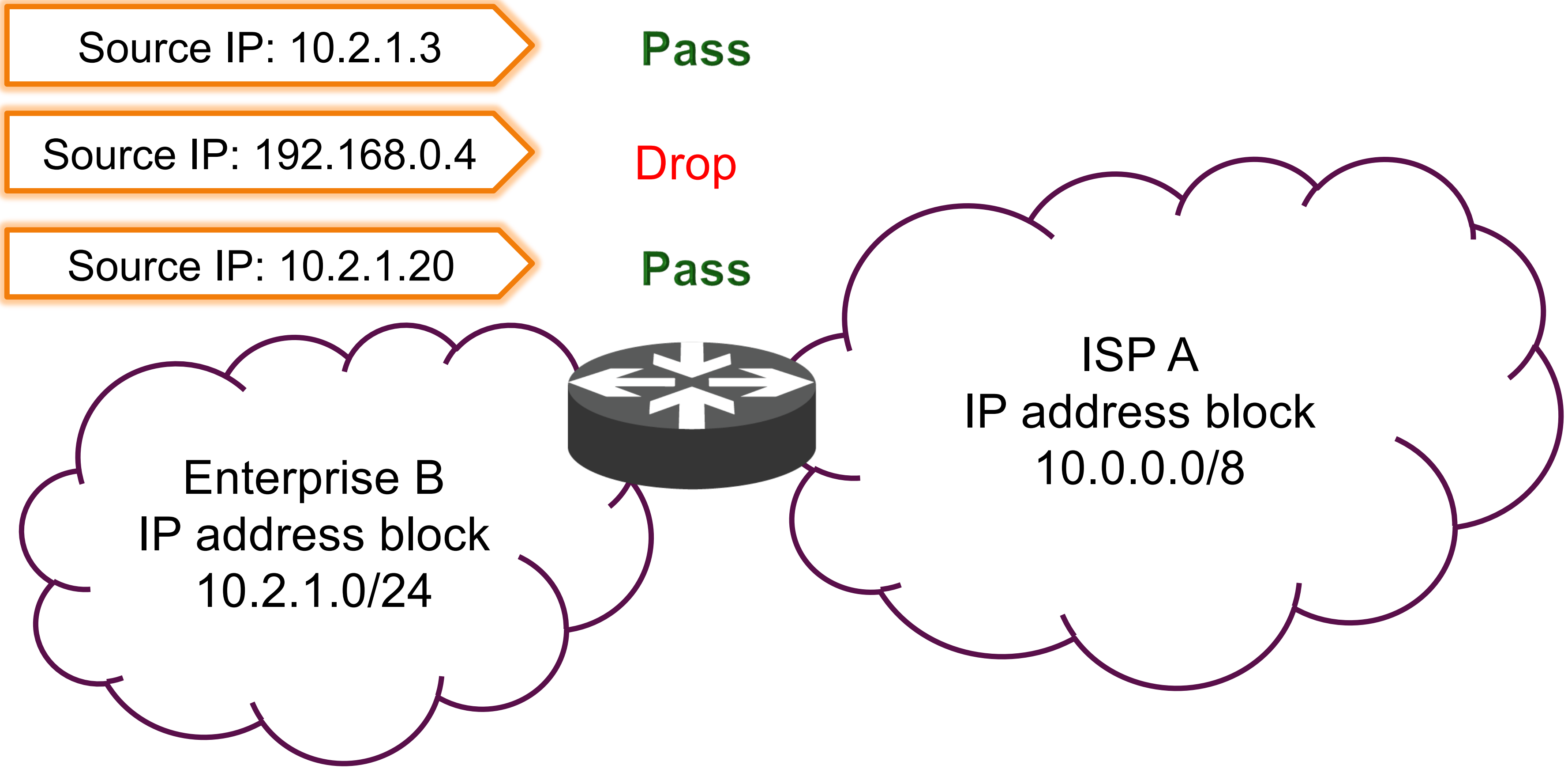
- Modes of Operation (IOS):
  - Strict: verifies both source address and incoming interface with entries in the forwarding table
  - Loose: verifies existence of route to source address



```
Forwarding Table:
2406:6400:100::/48  ge0/0
2406:6400:200::/48  fa0/0
```

Image source: “Cisco ISP Essentials”, Barry Greene & Philip Smith 2002

RFC2827 (BCP38) – Ingress Filtering



MANRS

- Mutually Agreed Norms of Routing Security
  - An ISOC led initiative to implement industry best practices to ensure security of routing system

- https://www.manrs.org/
  - Inbound/outbound filtering – prefix/as-path
  - Source address validation – BCP38
  - Coordination – correct & up to date contacts
  - Validation – ROAs/IRR objects

Discussion

Questions and Answers

Photo by Simone Secci on Unsplash