SECURE ROUTING WITH RPKI

Sheryl Hermoso (Shane)

PACNOG 23

Majuro, Marshall Islands

Current Situation

- BGP is a “trustful” protocol
- Route hijacking incidents (either malicious or accidental) are quite common
- Route information (route objects) in the IRR may be old and unreliable

Routing security has become more important

What is RPKI?

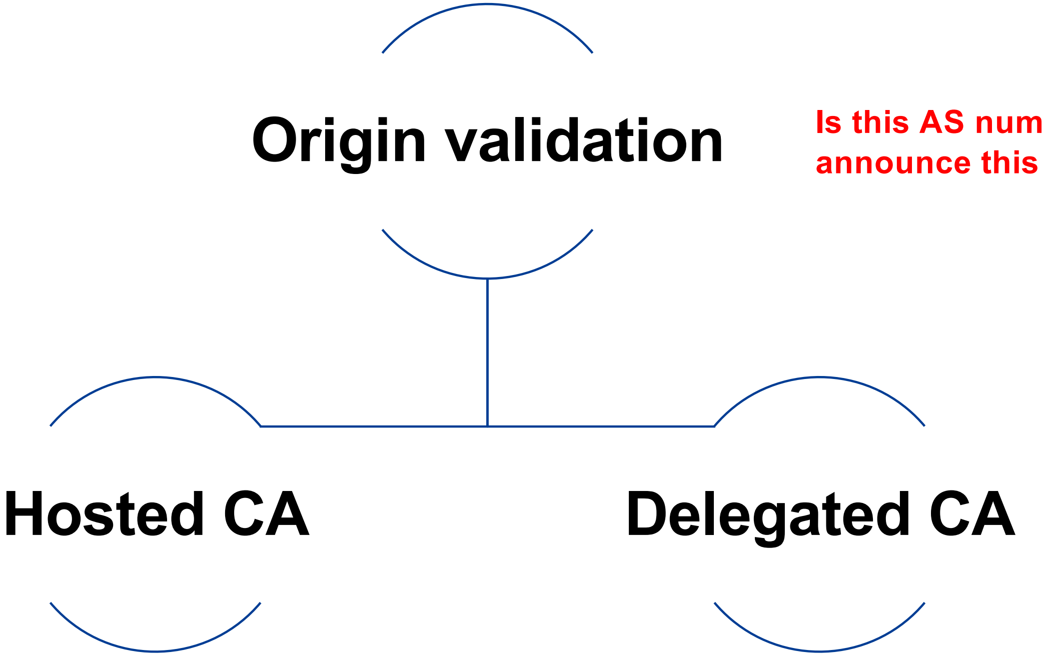
- Resource Public Key Infrastructure
- A robust security framework for verifying the association between <u>resource holder</u> and <u>Internet resource</u>
- Helps to secure Internet routing by validating routes

What does it solve?

- Prevents **route hijacking**
  - A prefix originated by an AS without authorization due to malicious intent

- Prevents **mis-origination**
  - A prefix that is mistakenly originated by an AS which does not own it
  - Also route leakage
  - due to configuration mistake or fat finger

RPKI implementation



Origin validation

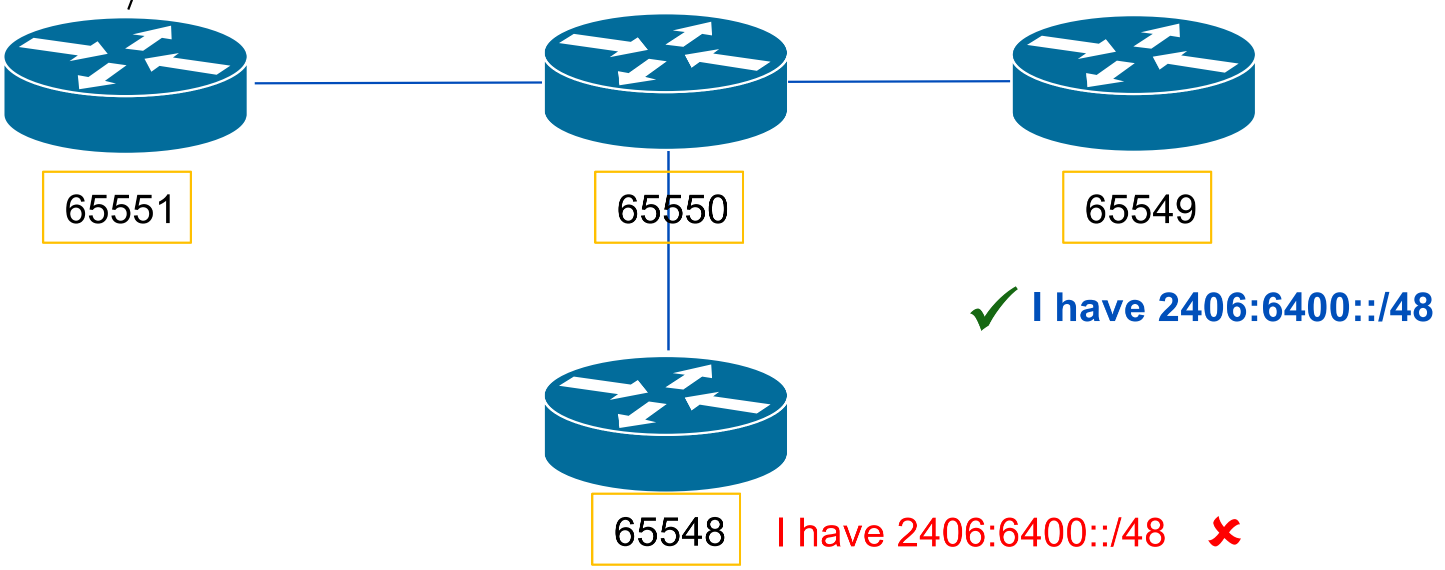
Hosted CA

Delegated CA

Is this AS number (ASN) authorized to announce this IP address range?

RPKI Origin Validation

2406:6400::/48	65551 65550 65549	VALID
2406:6400::/48	65551 65550 65548	INVALID



65551

65550

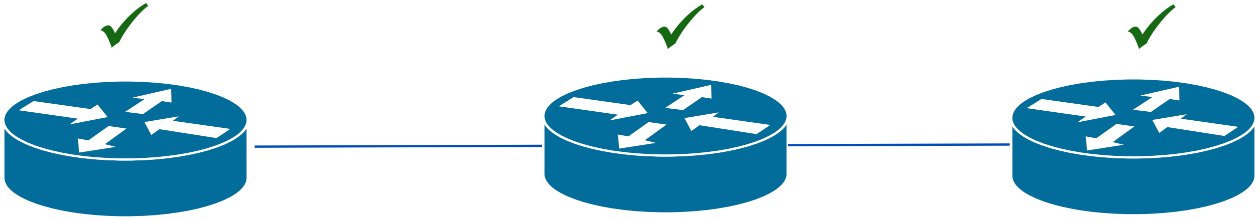
65549

✓ I have 2406:6400::/48

65548

I have 2406:6400::/48 ✗

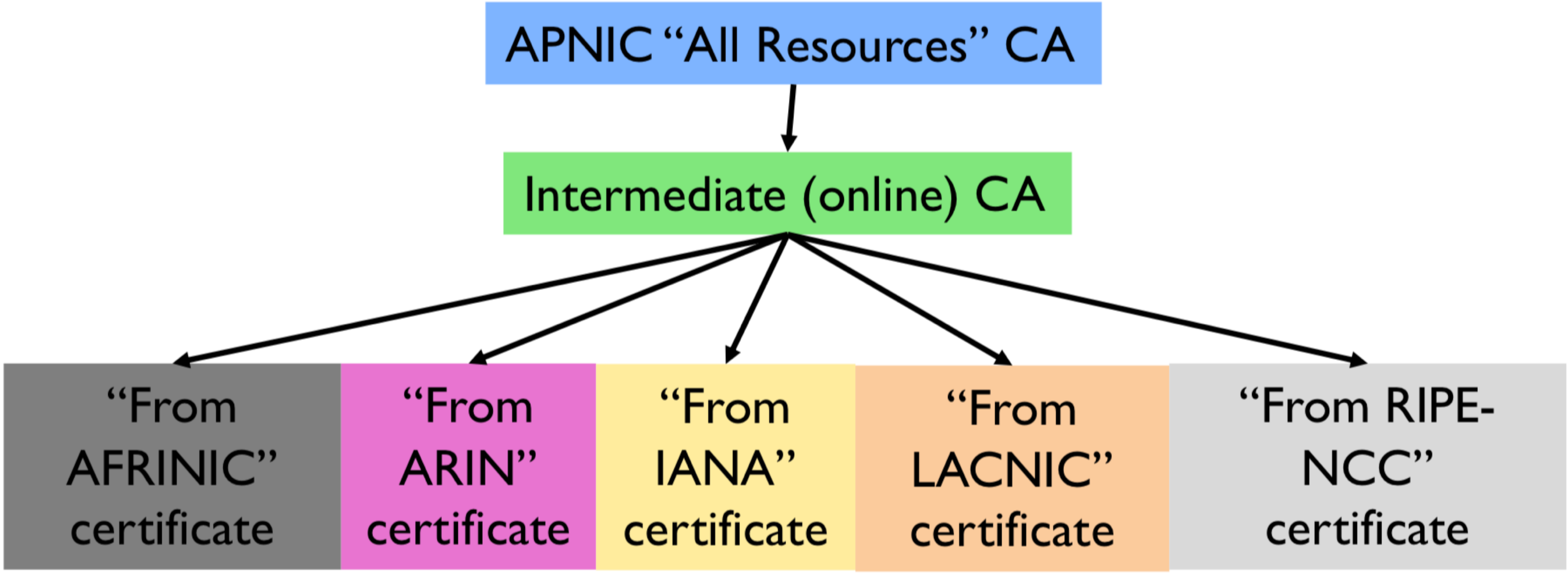
RPKI Path Validation (BGPsec)



2406:6400::/48	65551 65550 65549

Check and verify the complete path (BGPSEC)

RPKI Trust Anchors



APNIC "All Resources" CA

Intermediate (online) CA

"From AFRINIC" certificate

"From ARIN" certificate

"From IANA" certificate

"From LACNIC" certificate

"From RIPE-NCC" certificate

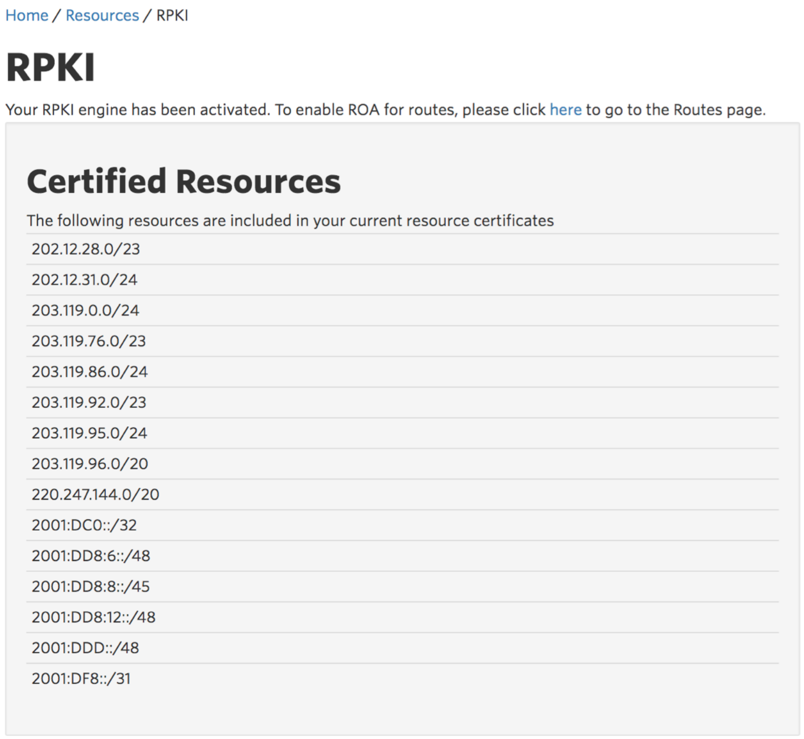
Route Origin Authorization (ROA)

- A signed digital object that contains a list of address prefixes and one AS number
- It is an authority created by a prefix holder to authorize an AS Number to originate one or more specific route advertisements

Prefix originated	203.176.189.0
Maximum prefix length	/24
Origin ASN	AS17821

- ROA is valid if a valid certificate which signs it has the prefix in its RFC 3779 extension

Adding ROAs



Home / Resources / RPKI

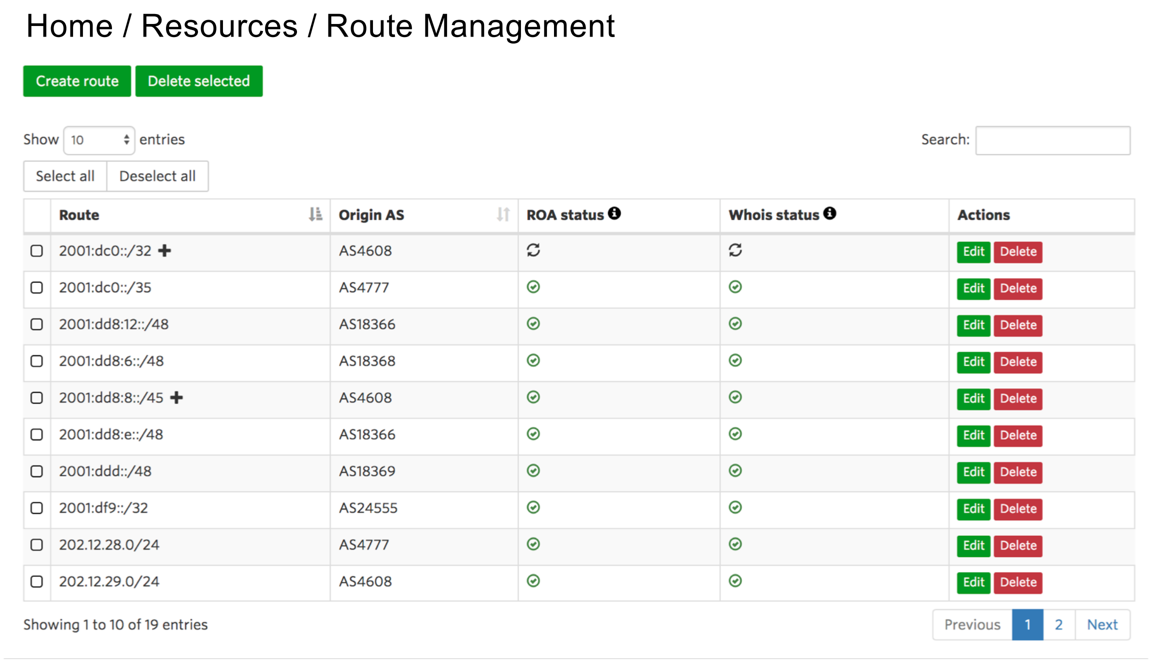
RPKI

Your RPKI engine has been activated. To enable ROA for routes, please click here to go to the Routes page.

Certified Resources

The following resources are included in your current resource certificates

- 202.12.28.0/23
- 202.12.31.0/24
- 203.119.0.0/24
- 203.119.76.0/23
- 203.119.86.0/24
- 203.119.92.0/23
- 203.119.95.0/24
- 203.119.96.0/20
- 220.247.144.0/20
- 2001:DC0::/32
- 2001:DD8:6::/48
- 2001:DD8:8::/45
- 2001:DD8:12::/48
- 2001:DDD::/48
- 2001:DF8::/31



Home / Resources / Route Management

Show 10 entries

Search:

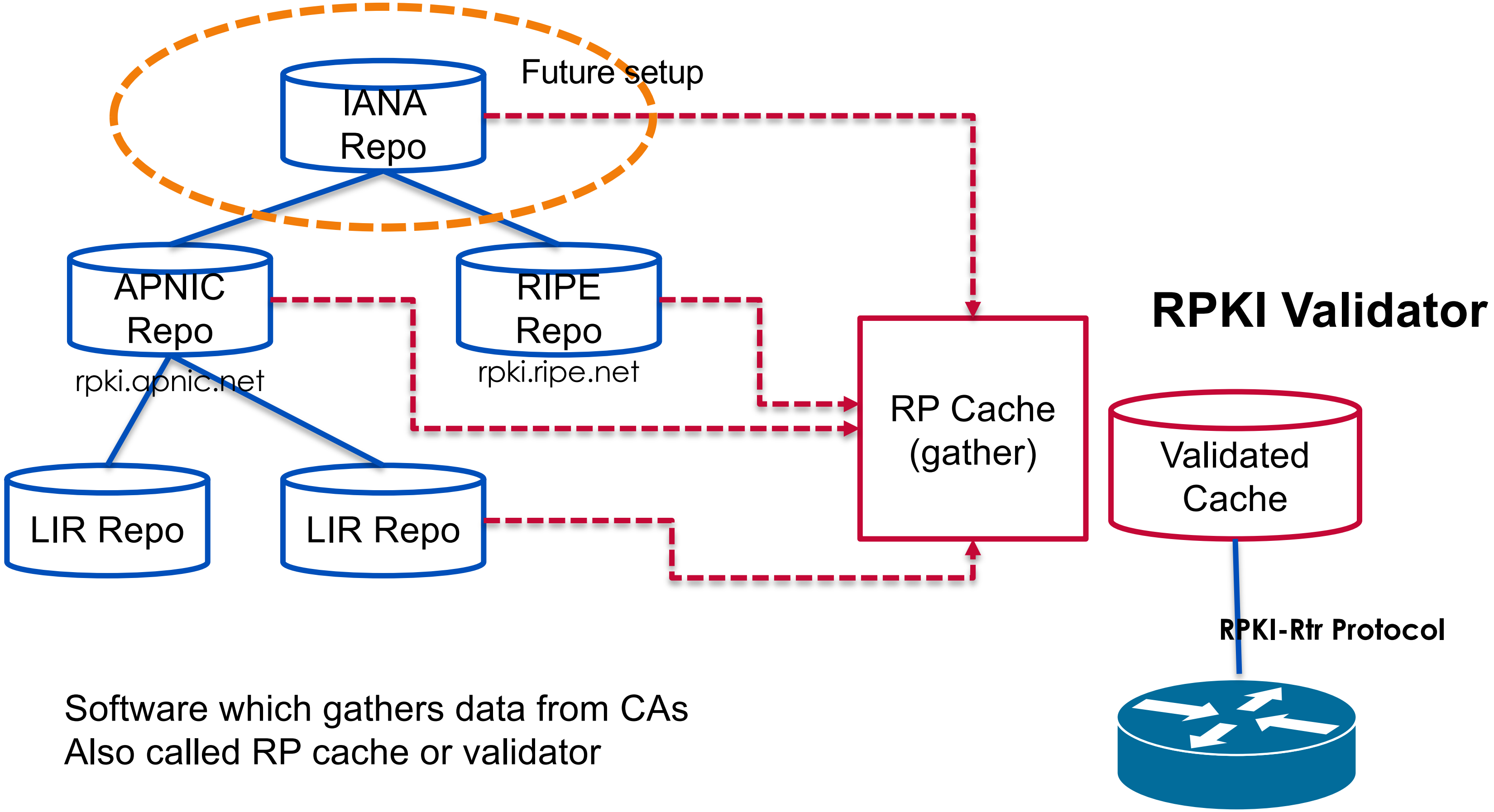
	Route	Origin AS	ROA status	Whois status	Actions
□	2001:dc0::/32 +	AS4608	↻	↻	Edit Delete
□	2001:dc0::/35	AS4777	✓	✓	Edit Delete
□	2001:dd8:12::/48	AS18366	✓	✓	Edit Delete
□	2001:dd8:6::/48	AS18368	✓	✓	Edit Delete
□	2001:dd8:8::/45 +	AS4608	✓	✓	Edit Delete
□	2001:dd8:e::/48	AS18366	✓	✓	Edit Delete
□	2001:ddd::/48	AS18369	✓	✓	Edit Delete
□	2001:df9::/32	AS24555	✓	✓	Edit Delete
□	202.12.28.0/24	AS4777	✓	✓	Edit Delete
□	202.12.29.0/24	AS4608	✓	✓	Edit Delete

Showing 1 to 10 of 19 entries

AS0

- a special ASN not allocated to any AS
- “Don’t route me”
- Binding a list of addresses to Origin-AS AS0 specifiies that this set of resources should not be seen in routing”
- RFC 7607

Relying Party



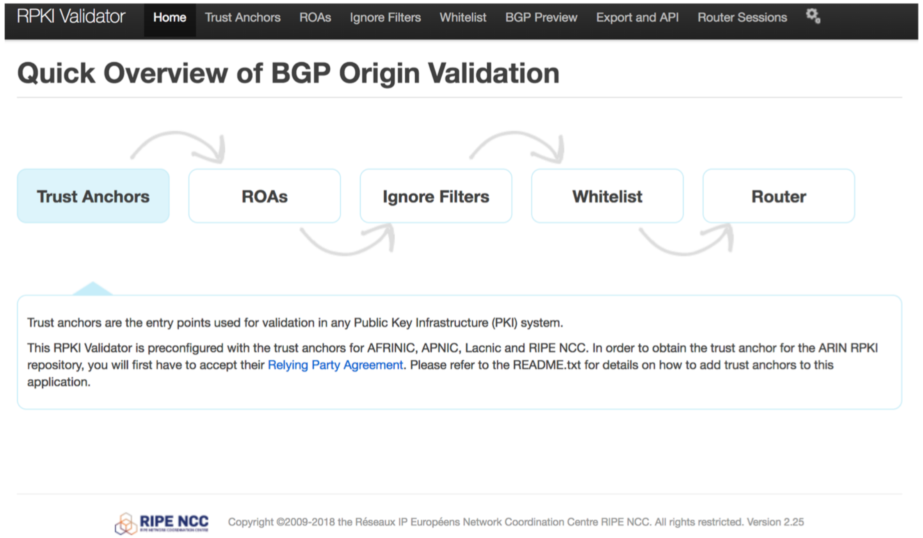
Software which gathers data from CAs
Also called RP cache or validator

RPKI Validation

- RPKI-capable routers can fetch the validated ROA dataset from a validated cache

VALID	Indicates that the prefix and ASN pair has been found in the database
INVALID	Indicates that the prefix is found, but • ASN received did not match, or • the prefix length is longer than the maximum length
NOT FOUND / UNKNOWN	Indicates that the prefix does not match any in the database

RPKI Validators



RPKI Validator | Home | Trust Anchors | ROAs | Ignore Filters | Whitelist | BGP Preview | Export and API | Router Sessions

Quick Overview of BGP Origin Validation

Trust Anchors → ROAs → Ignore Filters → Whitelist → Router

Trust anchors are the entry points used for validation in any Public Key Infrastructure (PKI) system.

This RPKI Validator is preconfigured with the trust anchors for AFRINIC, APNIC, Lacnic and RIPE NCC. In order to obtain the trust anchor for the ARIN RPKI repository, you will first have to accept their Relying Party Agreement. Please refer to the README.txt for details on how to add trust anchors to this application.

RIPE NCC Copyright ©2009-2018 the Réseaux IP Européens Network Coordination Centre RIPE NCC. All rights restricted. Version 2.25

RIPE-NCC Validator

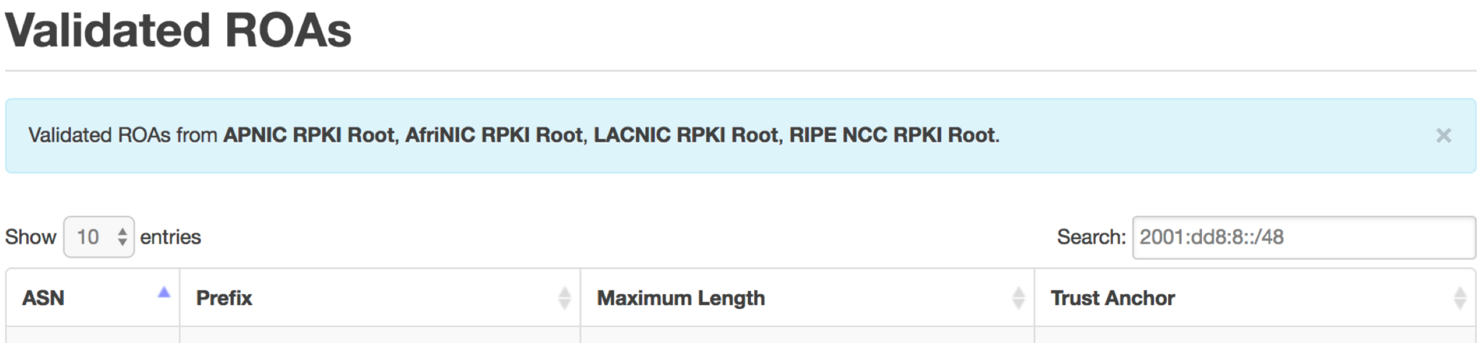
Routinator 3000

DragonResearch Toolkit

RTRlib.

RTRLib

RPKI Validators



Validated ROAs

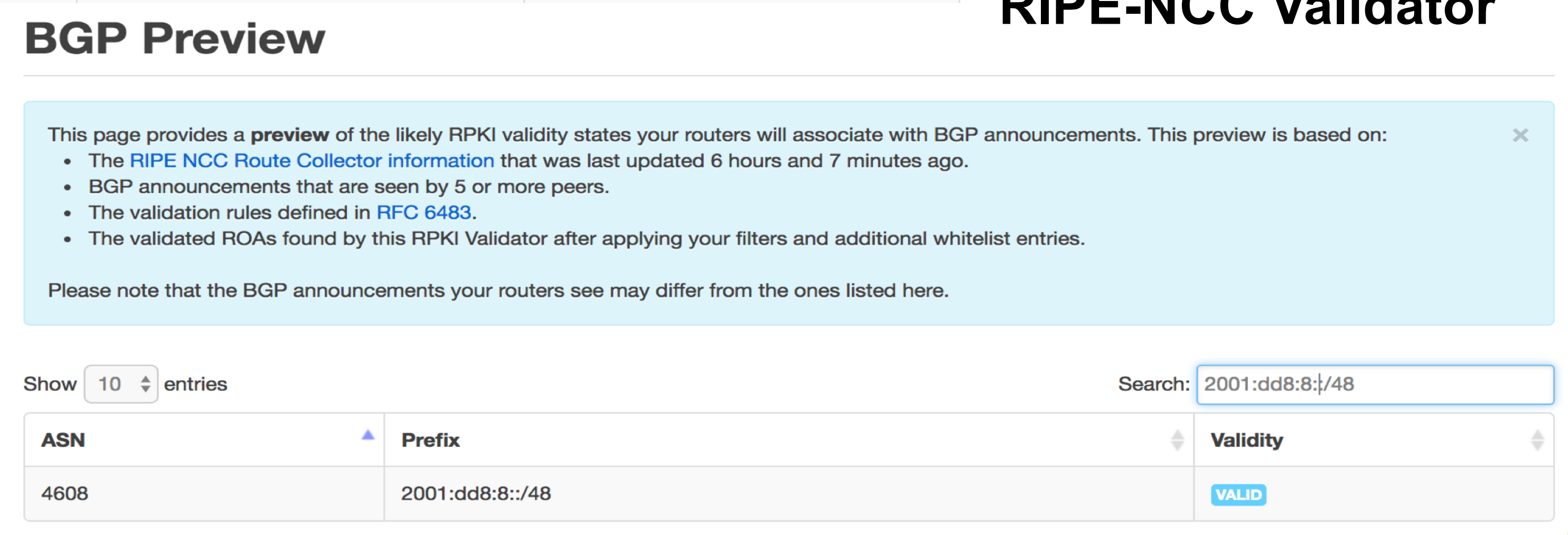
Validated ROAs from **APNIC RPKI Root**, **AfriNIC RPKI Root**, **LACNIC RPKI Root**, **RIPE NCC RPKI Root**. ×

Show 10 entries

Search: 2001:dd8:8::/48

ASN	Prefix	Maximum Length	Trust Anchor
4608	2001:dd8:8::/45		
4608	2001:dd8:8::/46		

RIPE-NCC Validator



BGP Preview

This page provides a **preview** of the likely RPKI validity states your routers will associate with BGP announcements. This preview is based on: ×

- The RIPE NCC Route Collector information that was last updated 6 hours and 7 minutes ago.
- BGP announcements that are seen by 5 or more peers.
- The validation rules defined in RFC 6483.
- The validated ROAs found by this RPKI Validator after applying your filters and additional whitelist entries.

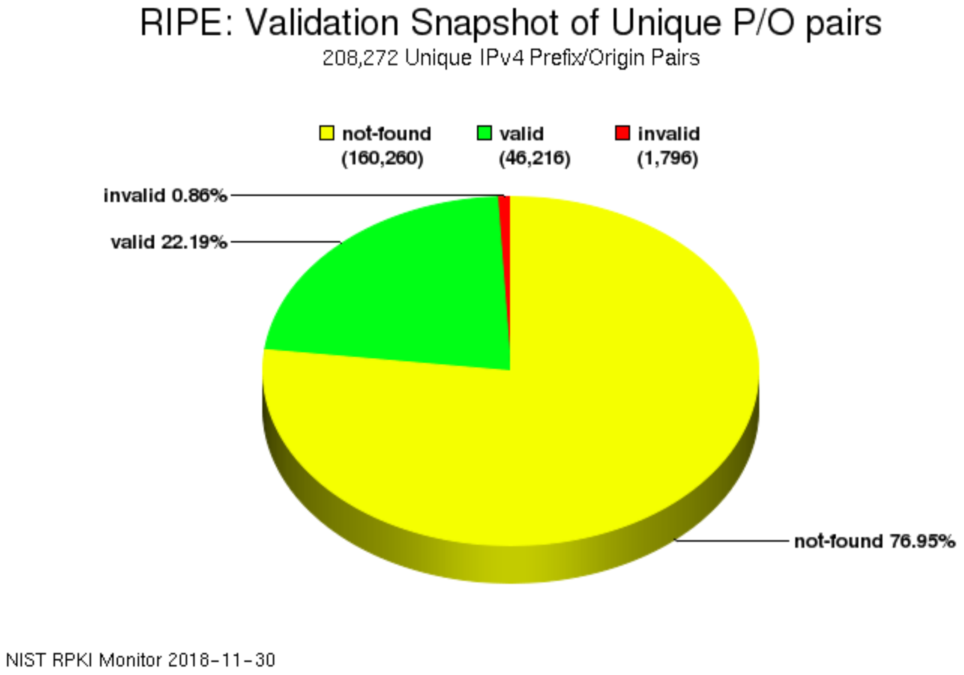
Please note that the BGP announcements your routers see may differ from the ones listed here.

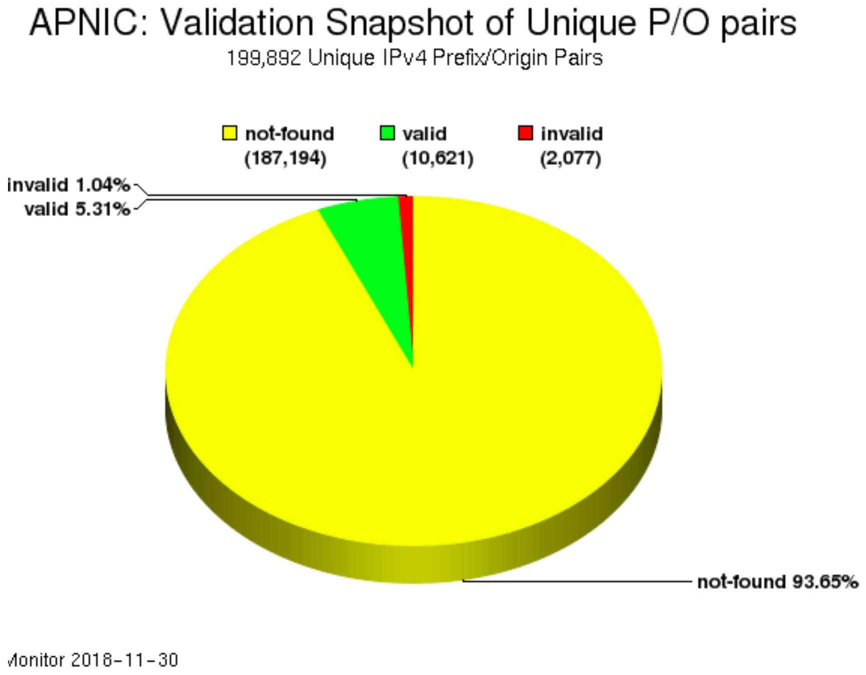
Show 10 entries

Search: 2001:dd8:8::/48

ASN	Prefix	Validity
4608	2001:dd8::/48	VALID

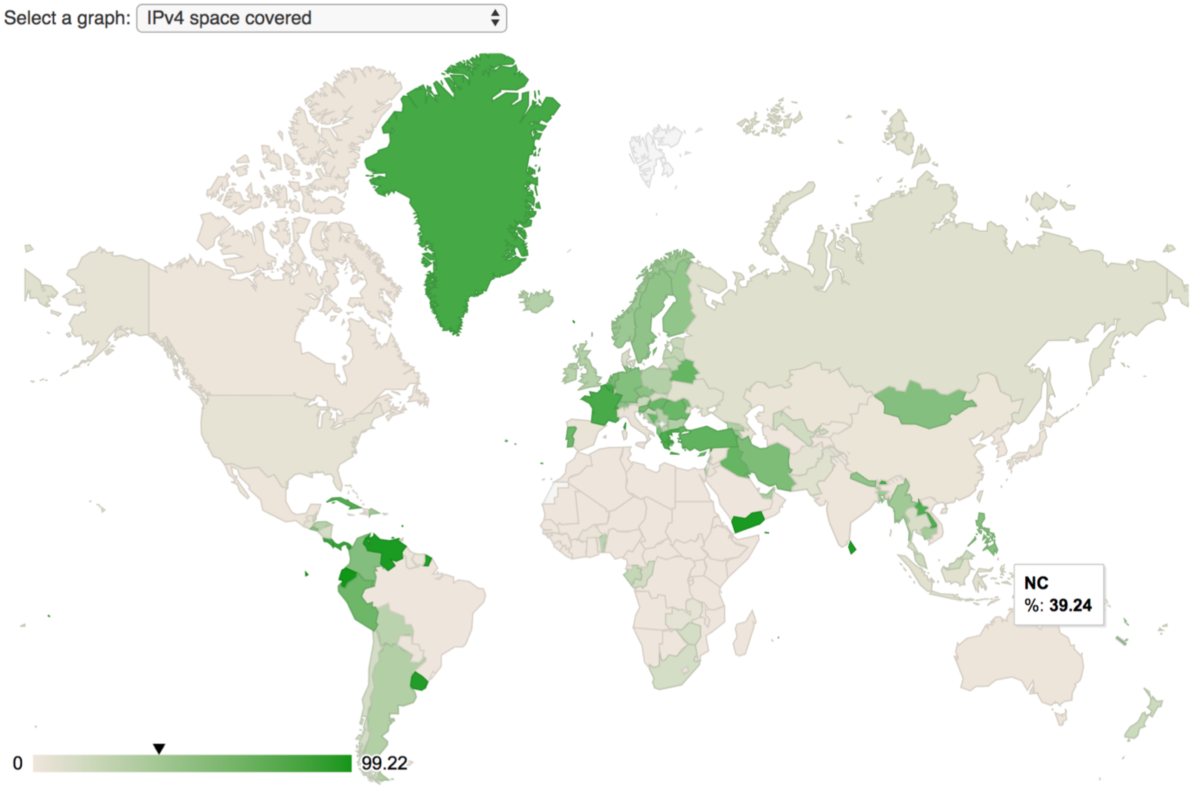
RPKI Adoption at the RIRs





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

ROAs in Pacific



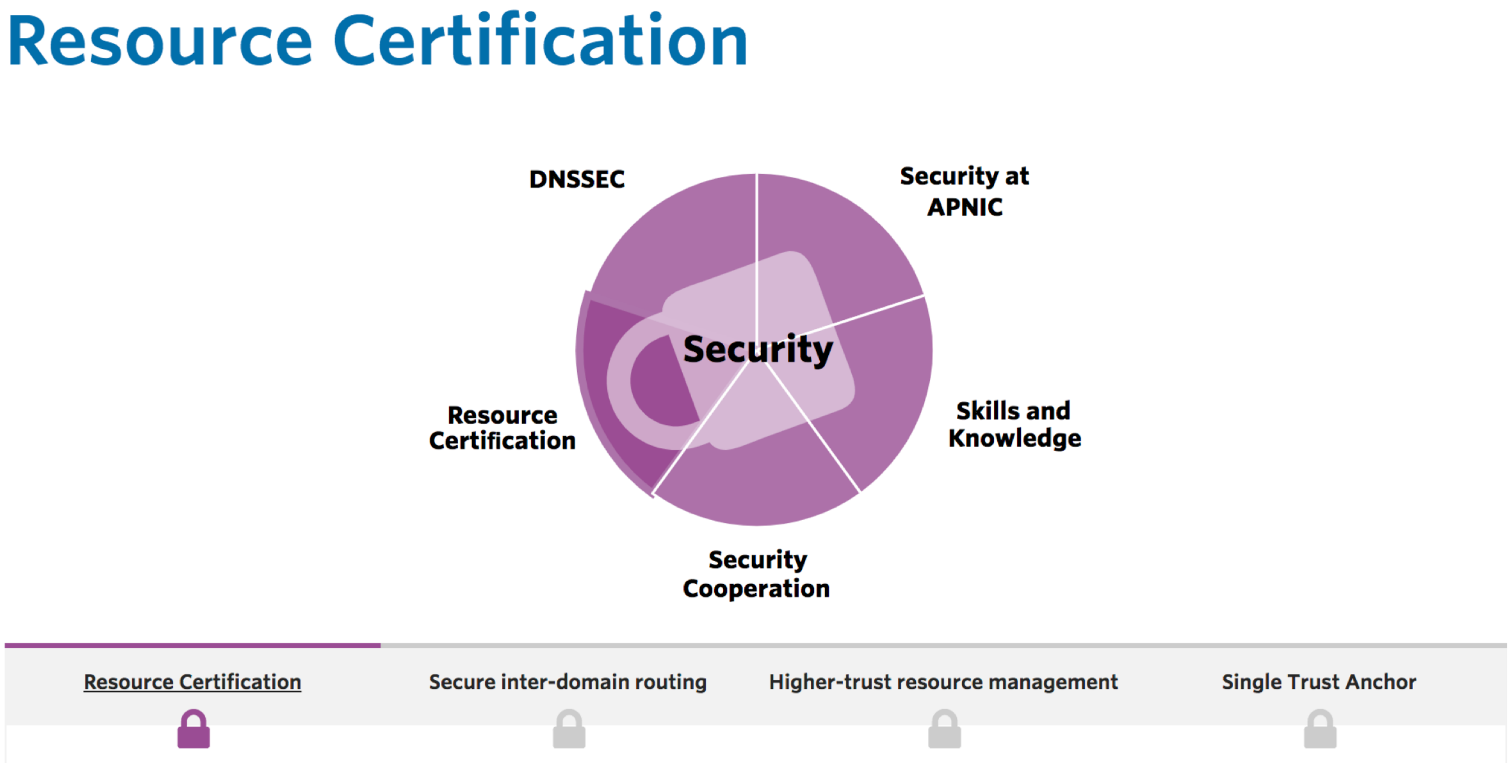
Select a graph: IPv4 space covered

NC	39.24%
VU	33.33%
PG	18.69%
NZ	15.22%
FJ	8.8%

So who’s implementing ROV?

- Some research says* not even 1% of the networks are rejecting invalid routes
- There’s a call to shift routing behavior from de-preferencing ROA-invalid routes to dropping those routes
- Efforts to “map” RPKI ROAs to IRR

More information



Resource Certification

Resource Certification

Secure inter-domain routing

Higher-trust resource management

Single Trust Anchor

https://www.apnic.net/community/security/resource-certification/#resource-certification