Routing Security: Path Validation with RPKI ASPA

KHNOG 8 Conference

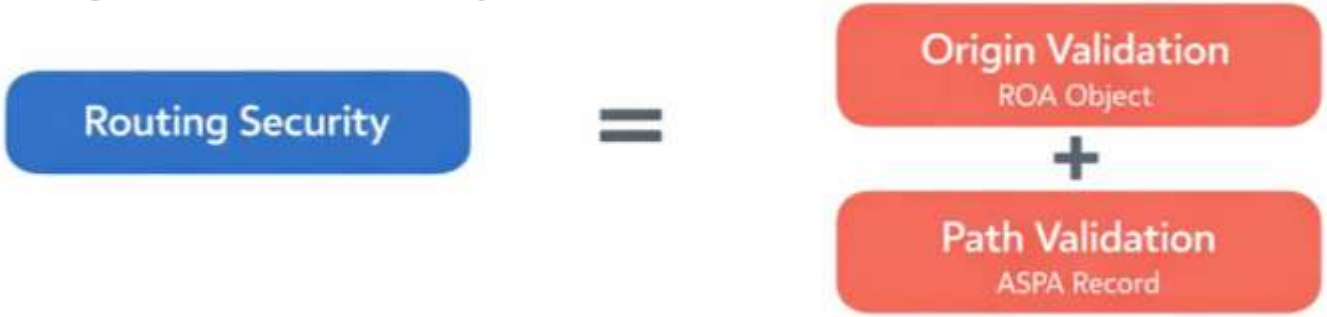
Makito Lay
Network Analyst / Technical Trainer
APNIC

About Me

- **Makito Lay**
  - Network Analyst / Technical Trainer @ APNIC
  - Volunteering:
    - TWNOG Multi-Stakeholder Group Member
    - KHNOG Executive Committee Member
  - Experiences:
    - 18 years in ISP and Telecom industry
    - MikroTik Certified Trainer
    - Ex-programmer
  - Certifications: CCIE # 47682, JNCIP-SP, MTCINE…etc.
  - Areas of Interest: BGP, MPLS, IPv6, Coding & Databases



Routing Security



Resource Public Key Infrastructure (RPKI) Globally distributed cryptographic security framework supporting secure internet routing	**Route Origin Authorization (ROA)** Resource holders create ROA objects to authorize an AS to originate its prefix	**Autonomous System Provider Authorization (ASPA)** Resource holders create ASPA objects to authorize their provider ASNs to forward route announcement
	Route Origin Validation (ROV) Routers validate route entries against the RPKI cache	**ASPA Verification** Route entries are verified by routers against the RPKI cache

What is ASPA?

- Autonomous System Provider Authorization.
- Cryptographically signed object that allows the **resource holder** of an Autonomous System Number (ASN) to **authorize** other ASNs as their **provider networks**.

Customer AS (CAS)	45192
Set of Provider ASes (SPA)	1. 4608 2. 4826

- Defined in two documents:
  - draft-ietf-sidrops-aspa-profile
  - draft-ietf-sidrops-aspa-verification



Why is it Useful?

- Detect and mitigate **route leaks**
  - In comparison, ROV is about the origin only

- Protect against certain types of **forged-origin/forged-path attacks**
  - Attacker must resort to longer AS paths for route to be accepted



ROA vs. ASPA

- ROA verifies the ***origin***.
- ROA record requires ASN and prefixes.
- ROA links an IP address prefix to an origin ASN.

- *Answers:*
  - *who is allowed to announce this prefix?*
  - *Is this BGP announcement originating from a valid source?*

- ASPA verifies the ***path***.
- ASPA record only needs ASNs.
- ASPA links an ASN to its upstream ASNs.

- *Answers:*
  - *Is this route taking a legitimate path through the network?*
  - *Is this BGP announcement's path plausibly correct?*

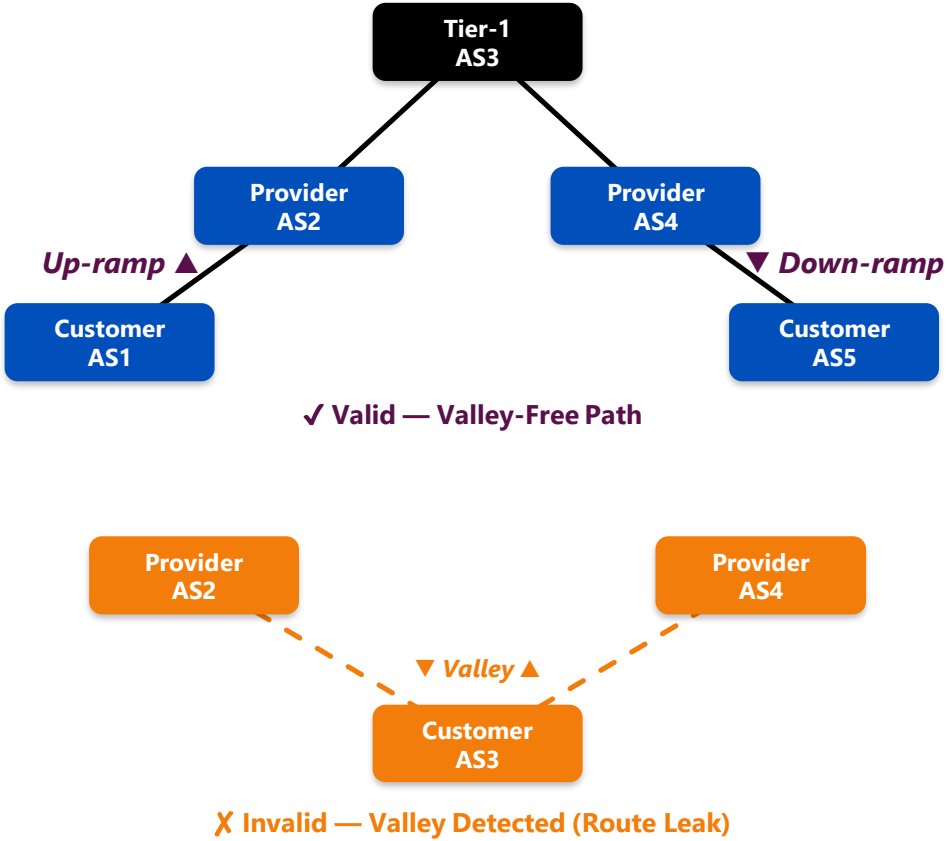
Step #1 Attestation

- Customer AS creates a digital signed object.
- **“These specific ASNs are my legitimate upstream providers”.**

- Why the customer AS?
  - “Bottom-up” security model wherein customer is the “authoritative source” responsible for keeping track of their transit/upstream provider(s)

Step #2 Verification

- BGP router checks the AS Path of each route entry against the ASPA object.
- "**Valley Free**" Routing:
  - Expect up-down structure →
    - Customer to Provider (up) and Provider to Customer (down)
  - Rule:
    - Provider to Customer (down) then Customer to Provider (up) creates a "valley" or a dip which indicates a route leak



Validation Outcomes

Outcomes

Provider

ASPA record exists

Hop is confirmed

Not Provider

ASPA record exists

Next AS is not on the list

No Attestation

No ASPA record

States

Valid

Each AS-to-AS Authorization Function yields "provider"

Invalid

At least one AS-to-AS Authorization Function yields "not provider"

Unknown

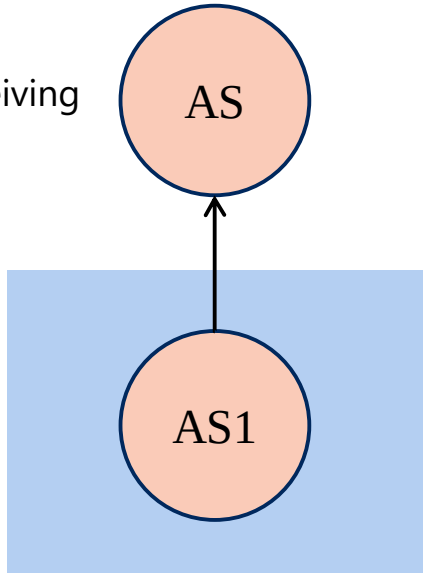
At least one AS-to-AS Authorization Function yields "no attestation", but there is no occurrence of "not provider"

Upstream Validation

1. If AS path has single entry → VALID 
2. If AS path contains hop from provider to customer → INVALID 
3. If AS path contains hop without ASPA → UNKNOWN 
4. Otherwise, all hops are from customer to provider → VALID 

Upstream Validation Examples (1)

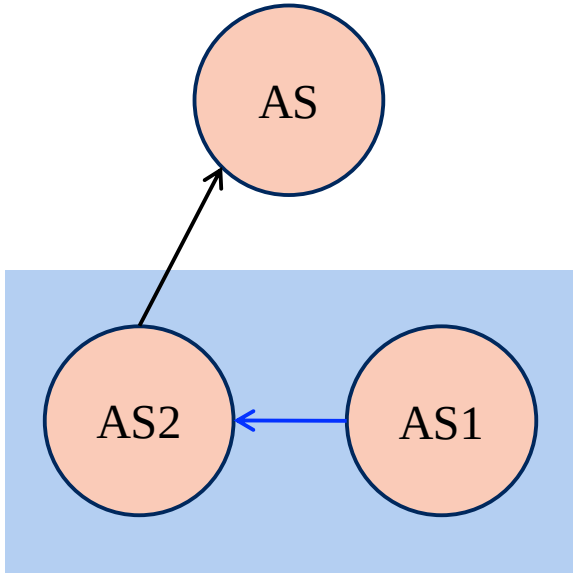
This AS is the upstream, receiving the route.



- Single-element AS path.
- ASPA state not relevant.
- Not possible for it to be a route leak.

- Arrows indicate AS path, from origin through peers.
- Blue box contains route. Only the AS path is relevant to ASPA validation, so the prefix is omitted.
- Black arrow: ASPA state between the two ASNs is irrelevant.

Upstream Validation Examples (2)

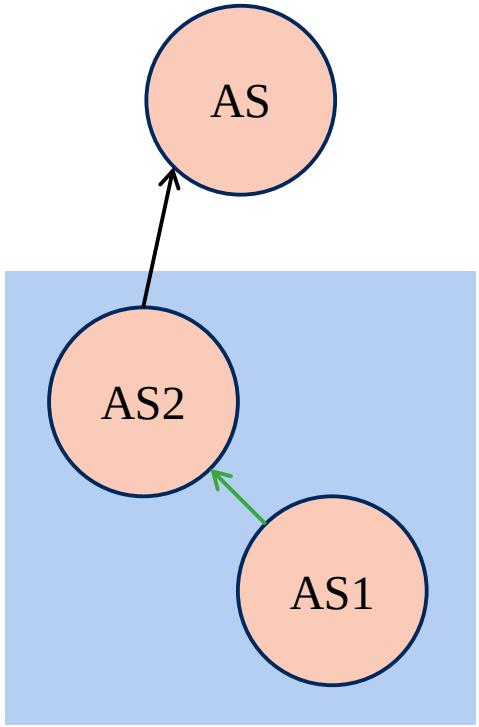


•Blue line: No ASPA for customer-provider pair.

- Two-element AS path.
- No ASPA.
- Unable to determine validity.

Upstream Validation Examples (3)

AS	Providers
1	2

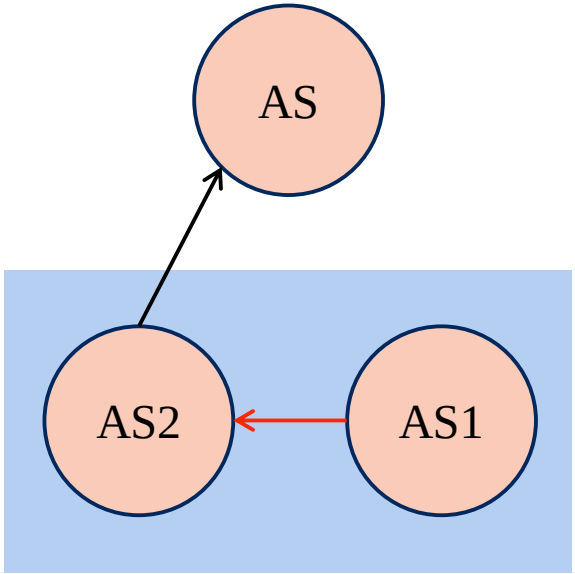


- Two-element AS path.
- ASPA exists for AS1 (origin).
- Able to determine validity.

•Within route, higher ASes are providers for lower ASes.
•Green line: ASPA exists for customer-provider pair.

Upstream Validation Examples (4)

AS	Providers
1	3



- Two-element AS path.
- ASPA exists for AS1 (origin) but disclaims AS2 as provider.
- Able to determine validity.



•Red line: ASPA exists for customer but does not contain provider ASN.

Downstream Validation

1. If AS path has…
   - up-ramp, customer(s) through provider(s)
   - down-ramp, provider(s) through customer(s)
   - no hops in the middle, or single lateral hop



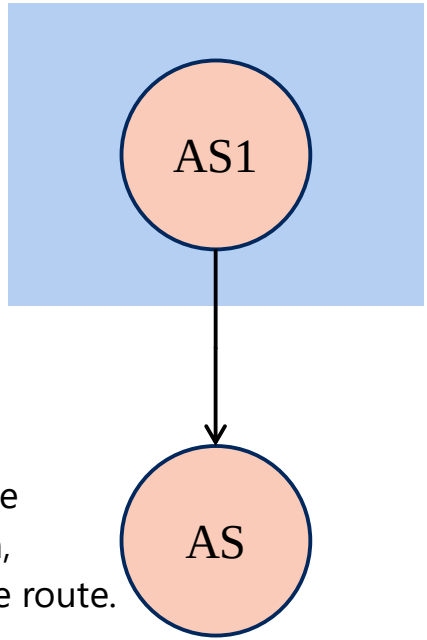
2. If AS path contains “valley” (hop from provider to customer, then from customer to provider)



3. Otherwise, unable to determine validity

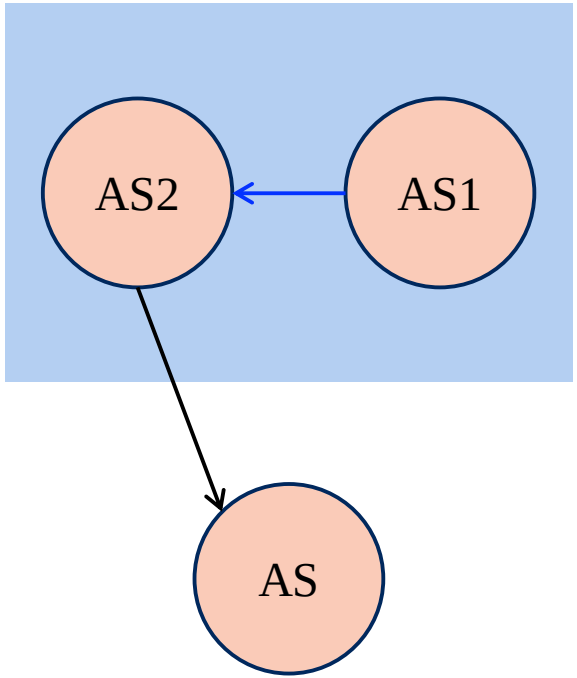


Downstream Validation Examples (1)



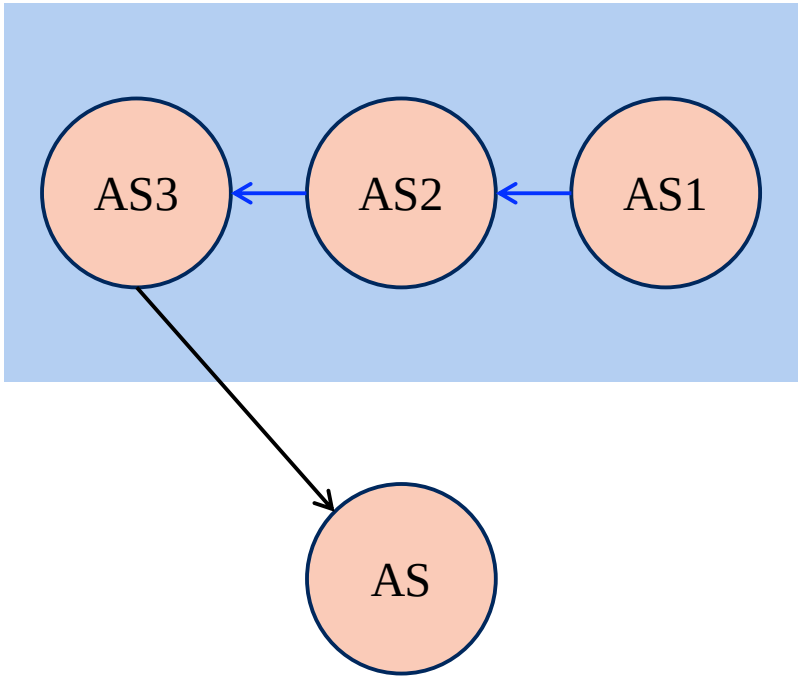
- Single-element AS path.
- ASPA state not relevant.
- Not possible for it to be a route leak.

Downstream Validation Examples (2)



- Two-element AS path.
- No ASPA.
- Not possible for it to be a route leak.

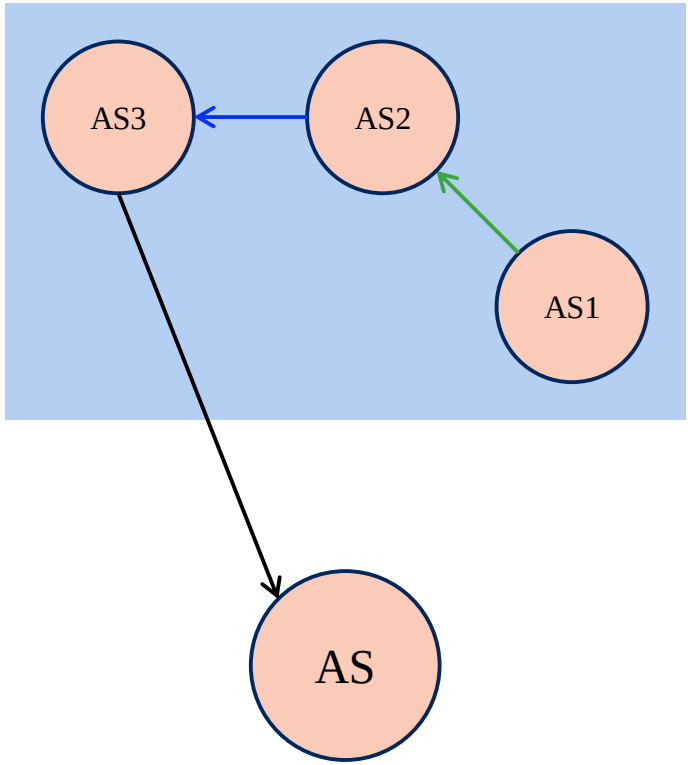
Downstream Validation Examples (3)



- Three-element AS path.
- No ASPA.
- Unable to determine validity.

Downstream Validation Examples (4)

AS	Providers
1	2

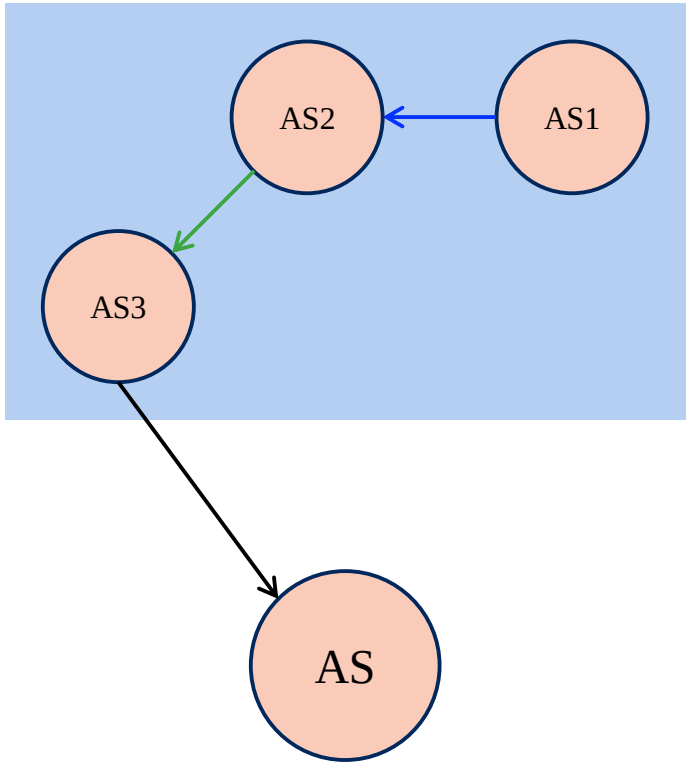


- Three-element AS path.
- ASPA exists for AS1 (origin).
- Route leak not possible.

Downstream Validation Examples (5)

Within route, lower ASes are customers of higher ASes.

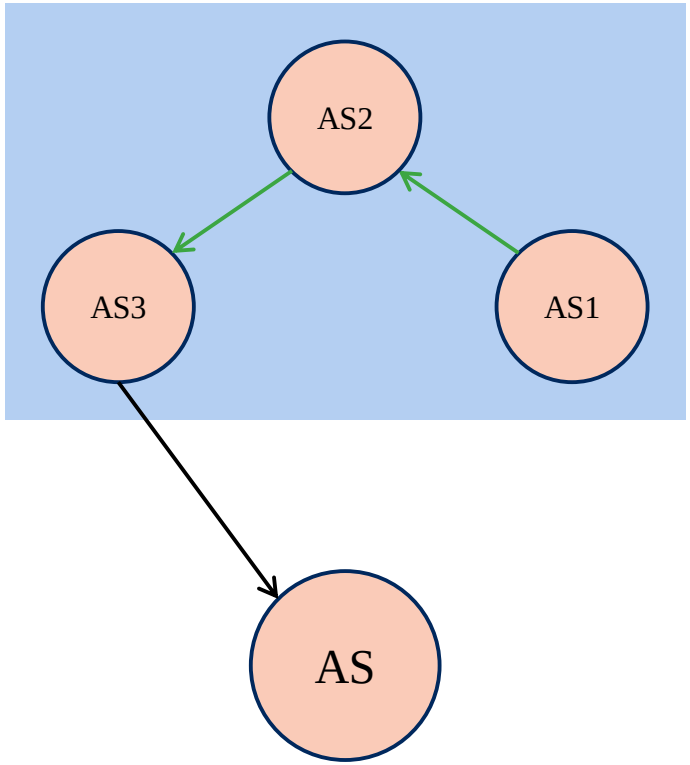
AS	Providers
3	2



- Three-element AS path.
- ASPA exists for AS3 (neighbor).
- Route leak not possible.

Downstream Validation Examples (6)

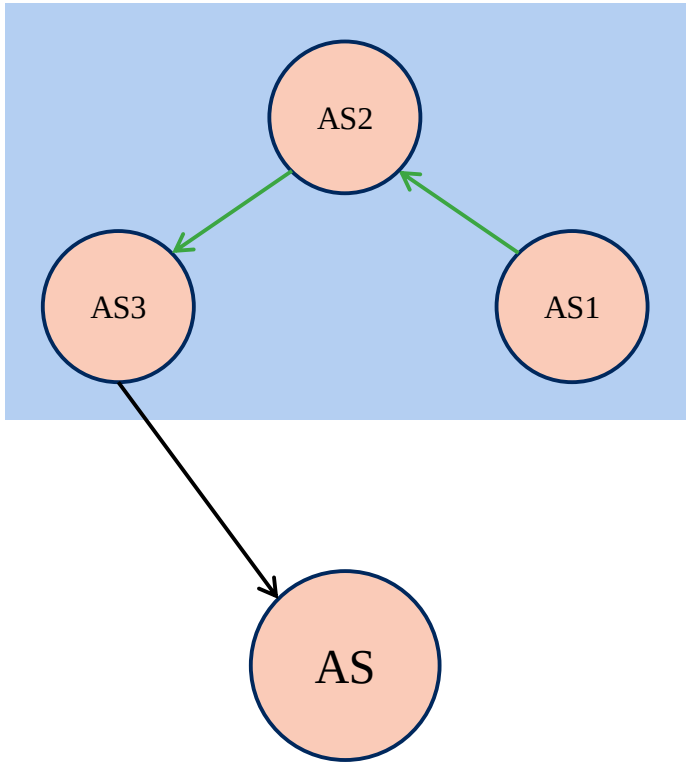
AS	Providers
1	2
3	2



- Three-element AS path.
- ASPAs exist for AS1 and AS3.
- Route leak not possible.

Downstream Validation Examples (7)

AS	Providers
1	2
2	0
3	2

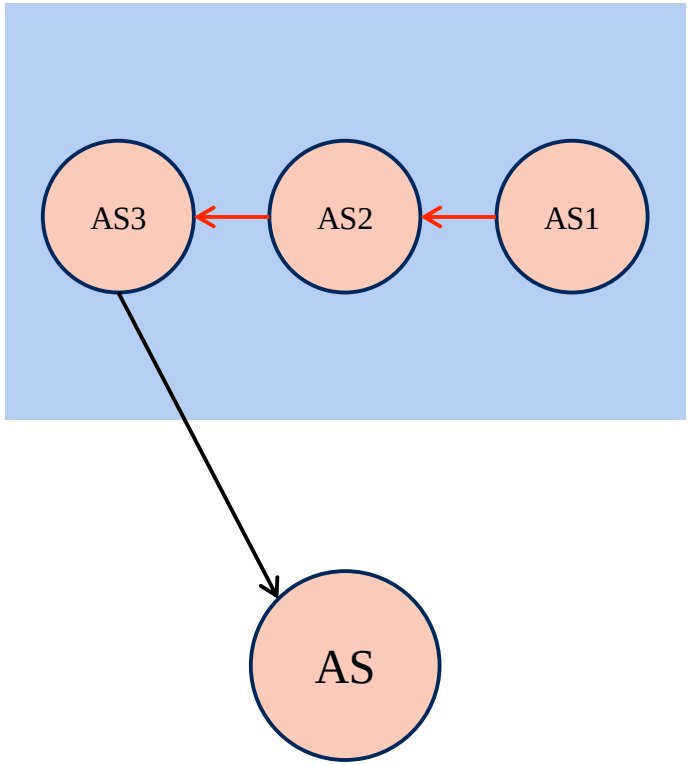


- AS path with three elements.
- AS2 has an AS0 ASPA, signaling no providers.
- Route leaks cannot occur.



Downstream Validation Examples (8)

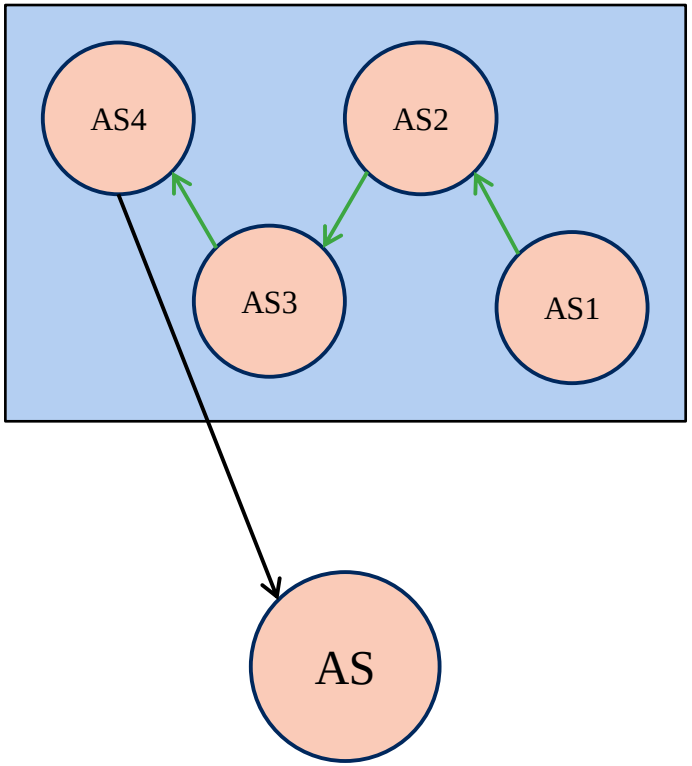
AS	Providers
1	4
2	0
3	5



- Three-element AS path.
- Up-ramp and down-ramp ASPAs do not include AS2.
- Route leak.

Downstream Validation Examples (9)

AS	Providers
1	2
2	0
3	2, 4
4	0

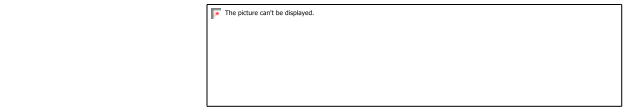


- Four-element AS path.
- Valley from AS2 to AS3 (customer) to AS4 indicates route leak.

ASPA Support – RPKI Software

The following software has ASPA support:

- Krill (Signer/CA)
- Routinator (Validator/RP)
- rpki-client
- FORT Validator









ASPA in Routinator

Add as an option with the “routinator” command:

```
routinator --enable-aspa vrps -f json -o dump.json --no-route-origins --no-router-keys
```

Or update the configuration file in “/etc/routinator/routinator.conf”:

```
enable-aspa = true
```

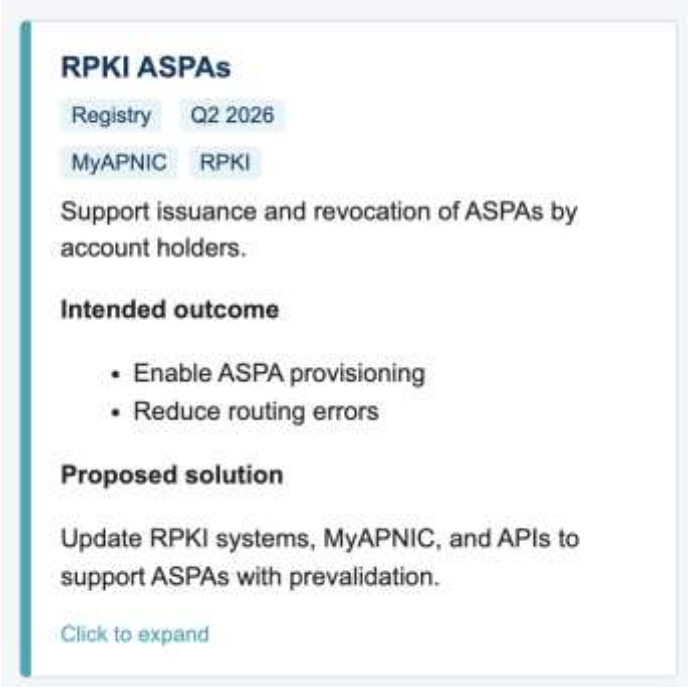


ASPA Support – BGP Software/OS

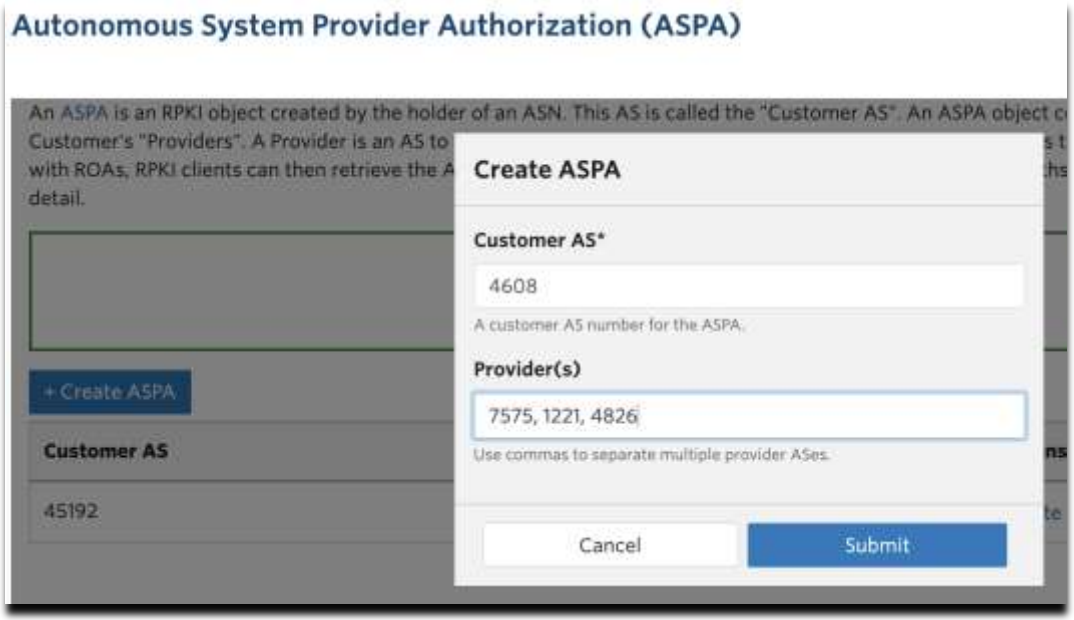
BGP Routing Software / OS	Version Supported	Supported since/from
BIRD Internet Routing	v2.16+	Dec 2024
OpenBGPD	v7.8+	March 2023
Cisco IOS-XR	27.1	Early Field Trial
JunOS	Next major release	Target Sep 2027
Arista		soon

ASPA Implementation @ RIR

- **RIPE NCC** has integrated ASPA into the RIPE RPKI Dashboard since December 2025.
- **ARIN** has deployed ASPA as of January 2026.
- **APNIC** has implemented by July 2026.
- Goal to have ASPA support in all RIRs this year.



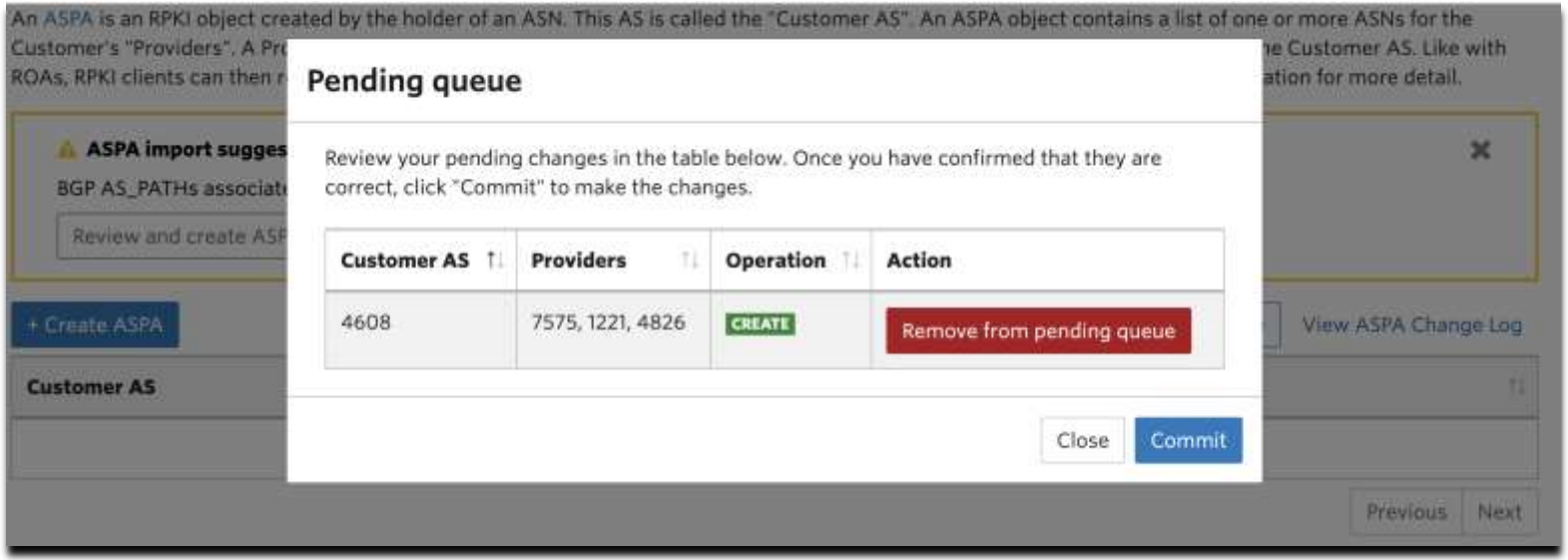
Creating ASPA Objects in MyAPNIC (Step 1 of 2)



- Log in to MyAPNIC.
- Navigate to Route Management.
- Click on **Create ASPA**.
- Enter your ASPA details and click **Submit**.

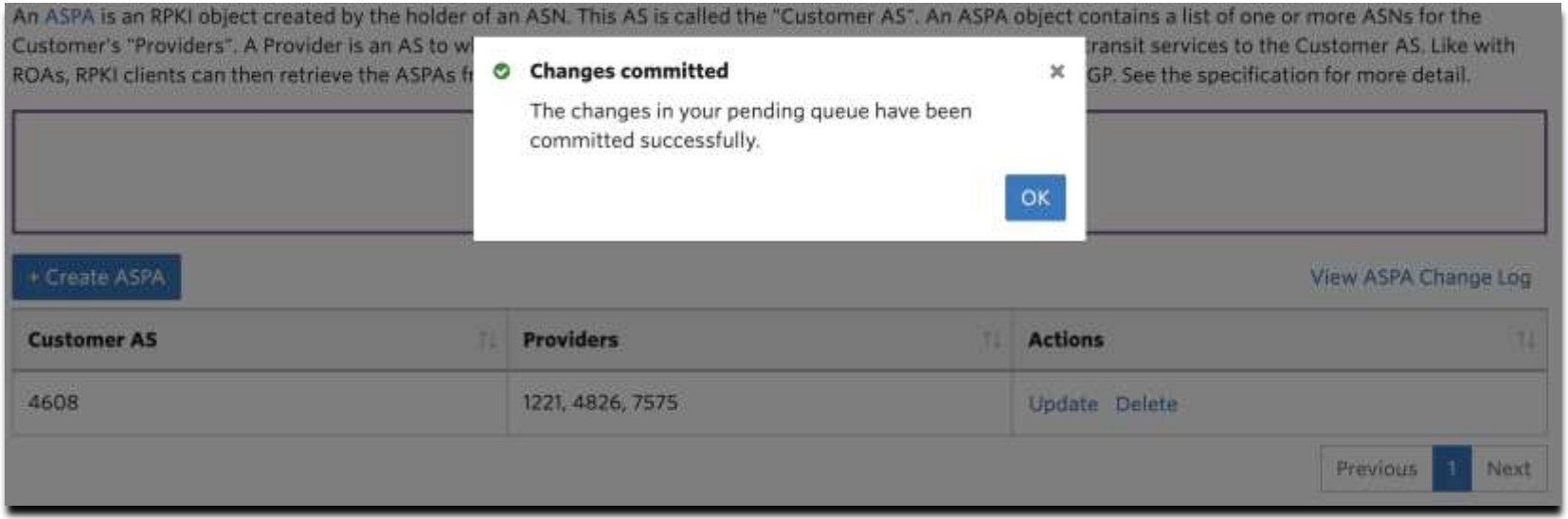
Creating ASPA Objects in MyAPNIC (Step 2 of 2)

- Review your pending changes and click on **Commit** once confirmed.

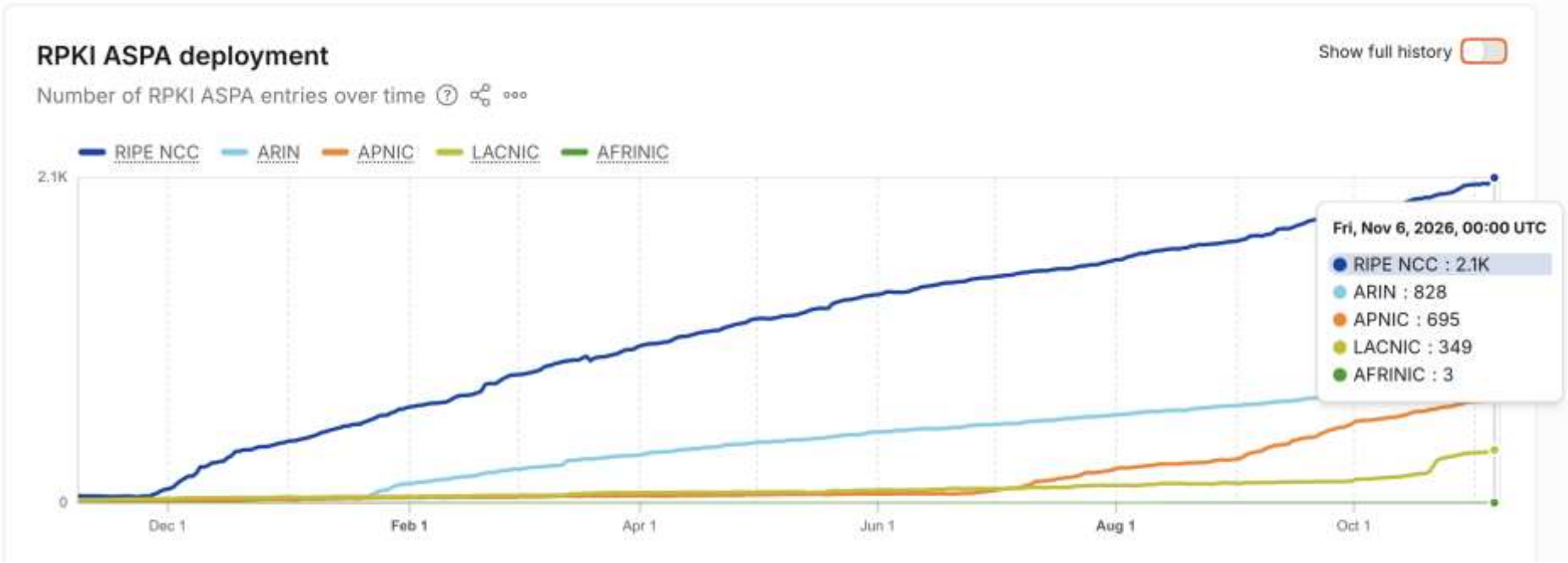


Creating ASPA Objects in MyAPNIC

- Your ASPA object is now published.



ASPA Uptake in the Region



Reference: https://radar.cloudflare.com/routing/rpki

Resources

- **RIPE NCC ASPA Documentation:** https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/aspa/

- **ARIN ASPA Documentation:** https://www.arin.net/resources/manage/rpki/aspa/

Thank you for your attention!

Contact Me

- E-mail: makito.lay@apnic.net
- LinkedIn: https://www.linkedin.com/in/ogawamakito

