

Understanding ASPA

The next step in routing security

Tom Harrison
Product Manager Registry
30 September 2026

What is RPKI?

- **R**esource **P**ublic **K**ey **I**nfrastructure
- Run by the Regional Internet Registries
- Enables resource holders to make cryptographically-verifiable statements about their resources
- Each RIR has a separate Trust Anchor (TA), and issues CA certificates to members, enumerating their resources
- Members then issue objects relating to those resources
- Most commonly-used object is the Route Origin Authorization (ROA)

What is an ASPA?

- **A**utonomous **S**ystem **P**rovider **A**uthorization
- Defined in two documents:
 - draft-ietf-sidrops-aspa-profile
 - draft-ietf-sidrops-aspa-verification
- The specifications provide for:
 - an ASN holder signing an object that links its own ASN (the **customer ASN**) to its upstream ASes (the **provider ASNs**)
 - a network operator using that data to verify the AS_PATH of a received route (valid/invalid/unknown - similar to ROV)

Why is it useful?

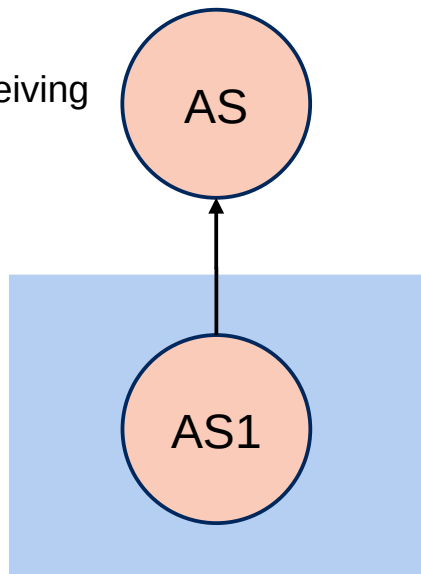
- Detect and mitigate route leaks
 - Compare ROV, which is about the origin only
- Protect against certain types of forged-origin/forged-path attacks
 - Attacker must resort to longer AS paths for route to be accepted

Upstream validation

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

Upstream validation examples (1)

This AS is the upstream, receiving the route

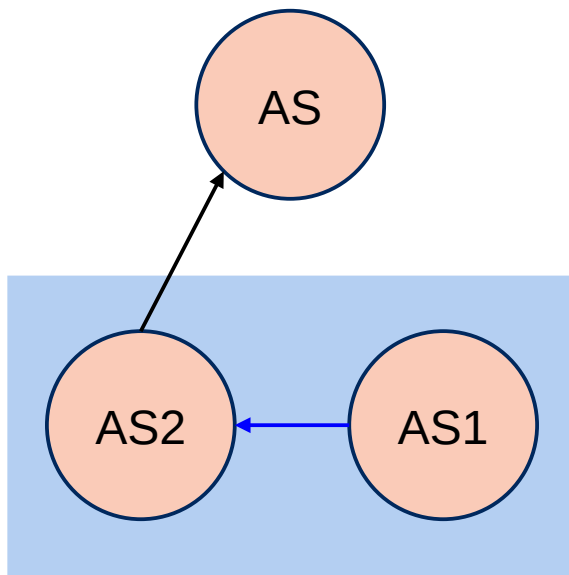


- Single-element AS path
- ASPA state not relevant
- Not possible for it to be a route leak



- 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 ASPAs
- Unable to determine validity

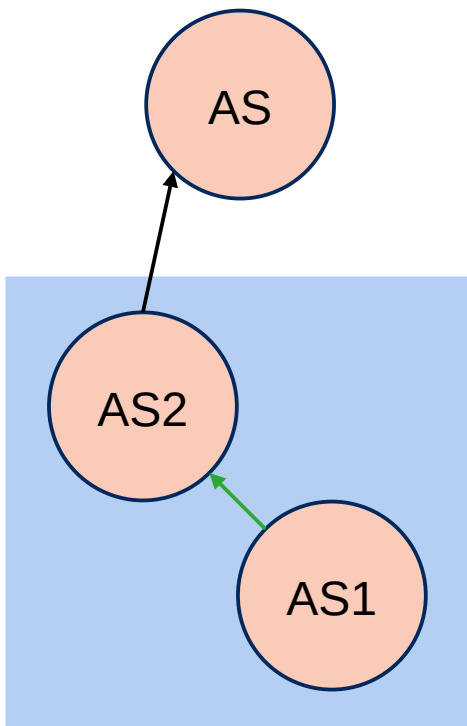


Upstream validation examples (3)

ASPAs

AS	Providers
AS1	AS2

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



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

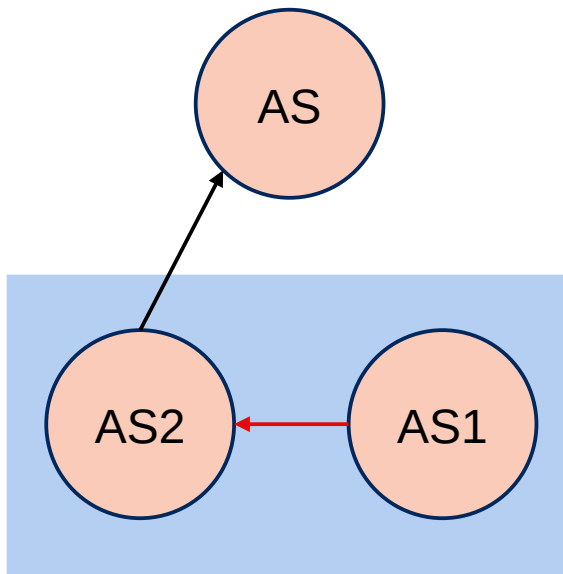


Upstream validation examples (4)

ASPAs

AS	Providers
AS1	AS3

- Red line: ASPA exists for customer, but does not contain provider ASN



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



Downstream validation

1) If AS path has:

1) Up-ramp, customer(s) through provider(s)

2) Down-ramp, provider(s) through customer(s)

3) No hops in the middle, or single lateral hop



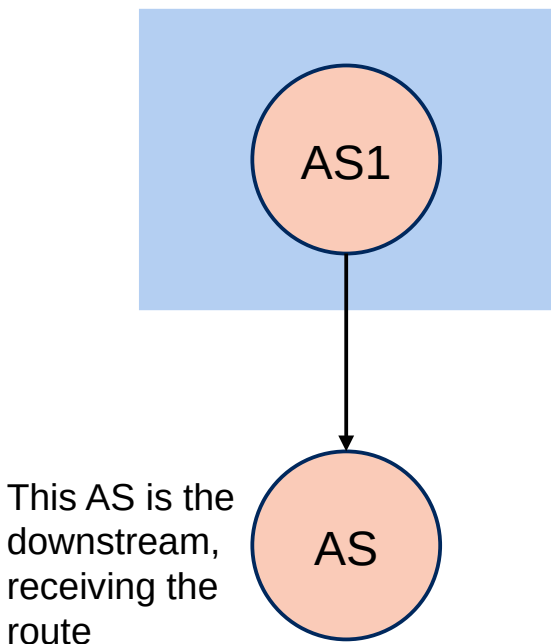
2) If AS path contains 'valley' (hop from provider to customer, then from customer to provider)



3) Otherwise, unable to determine validity



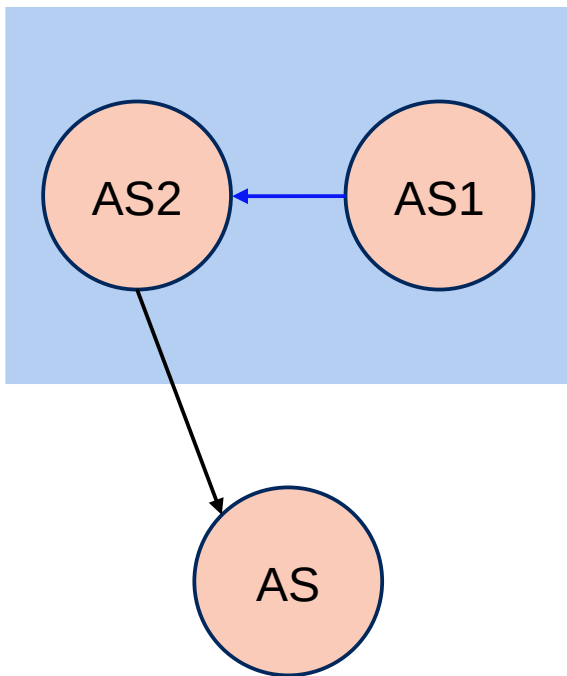
Downstream validation examples (1)



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



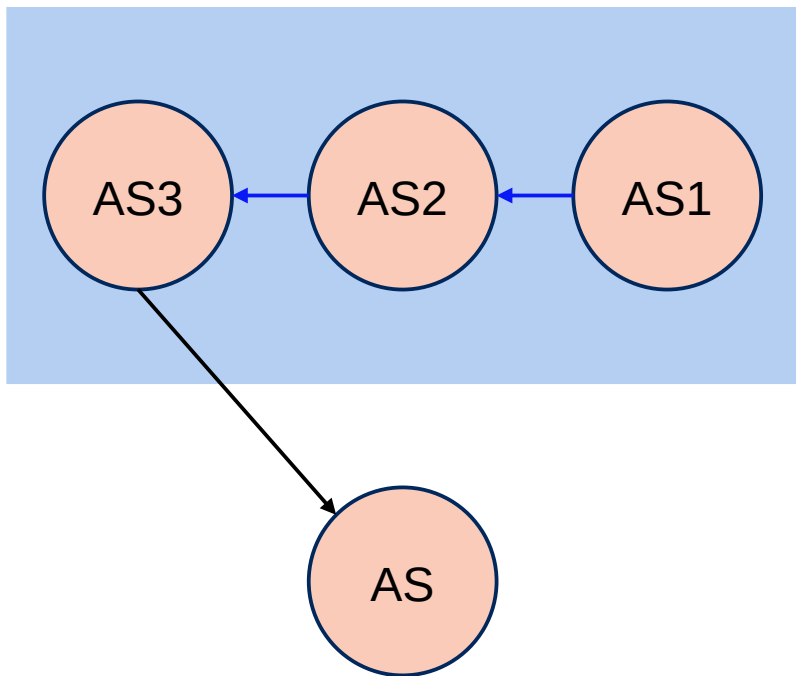
Downstream validation examples (2)



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



Downstream validation examples (3)



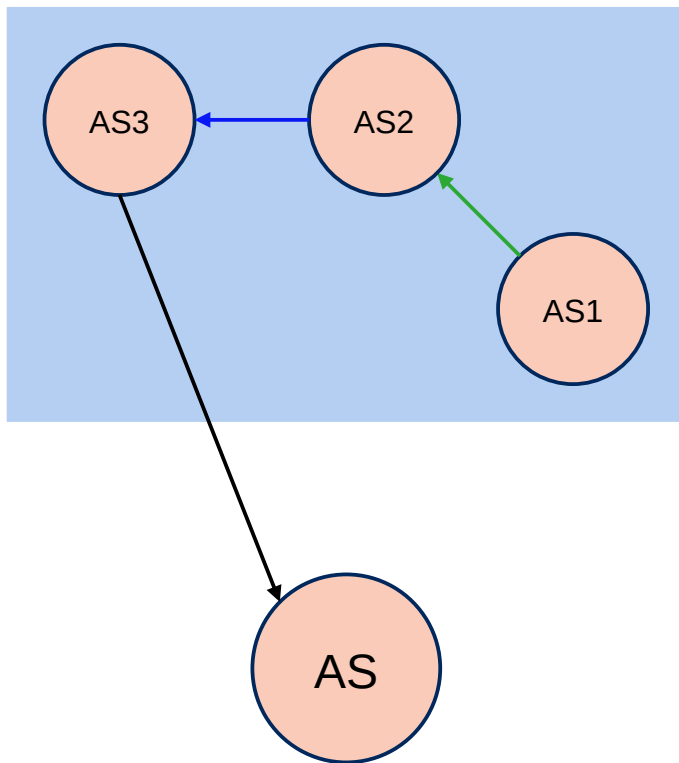
- Three-element AS path
- No ASPAs
- Unable to determine validity



Downstream validation examples (4)

ASPAs

AS	Providers
AS1	AS2



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

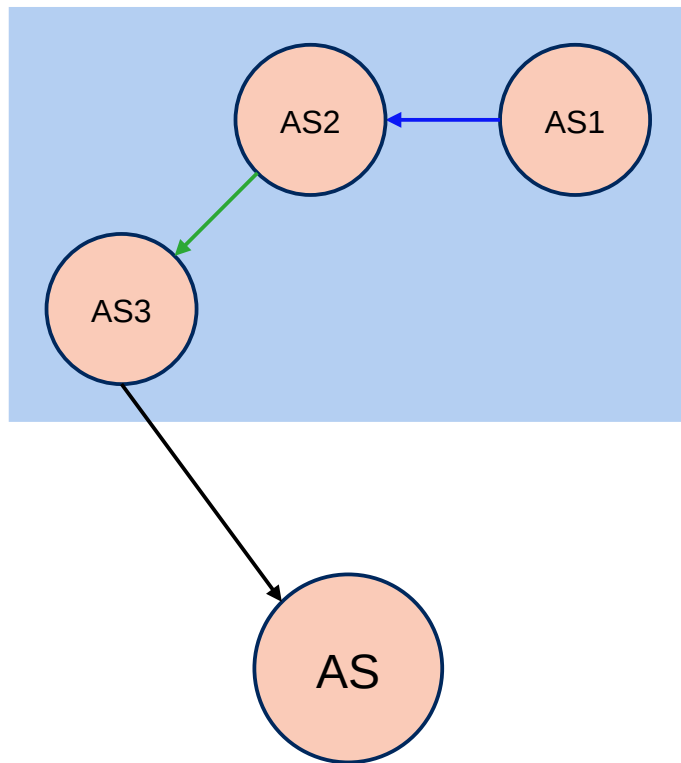


Downstream validation examples (5)

Within route, lower ASes are customers of higher ASes

ASPAs

AS	Providers
AS3	AS2



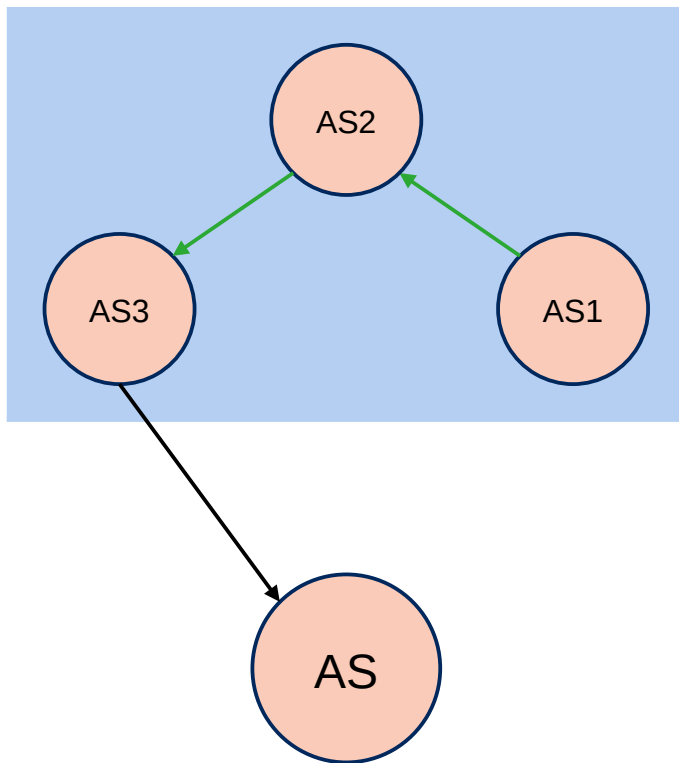
- Three-element AS path
- ASPA exists for AS3 (neighbour)
- Route leak not possible



Downstream validation examples (6)

ASPAs

AS	Providers
AS1	AS2
AS3	AS2



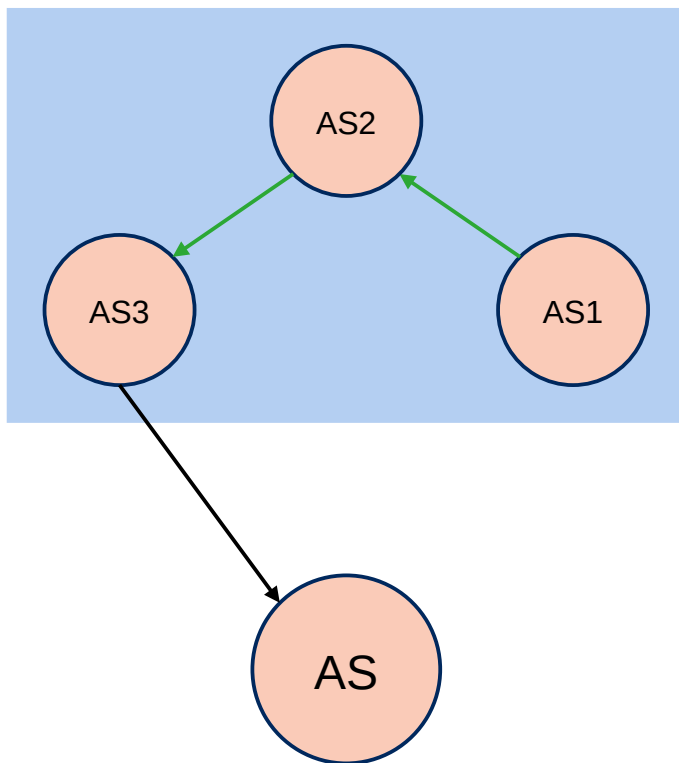
- Three-element AS path
- ASPAs exist for AS1 and AS3
- Route leak not possible



Downstream validation examples (7)

ASPAs

AS	Providers
AS1	AS2
AS2	AS0
AS3	AS2



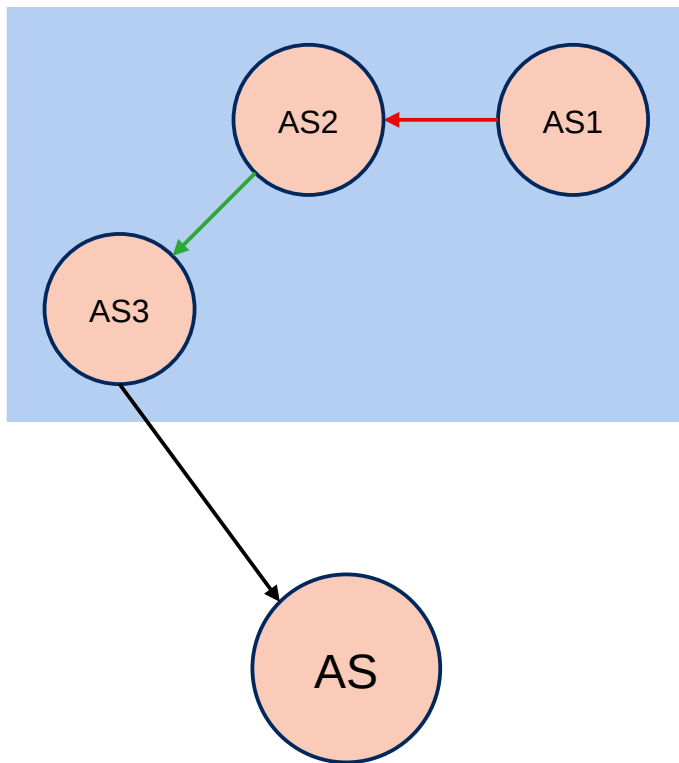
- Three-element AS path
- AS0 ASPA now exists for AS2, to indicate absence of providers
- Route leak not possible



Downstream validation examples (8)

ASPAs

AS	Providers
AS1	AS4
AS3	AS2



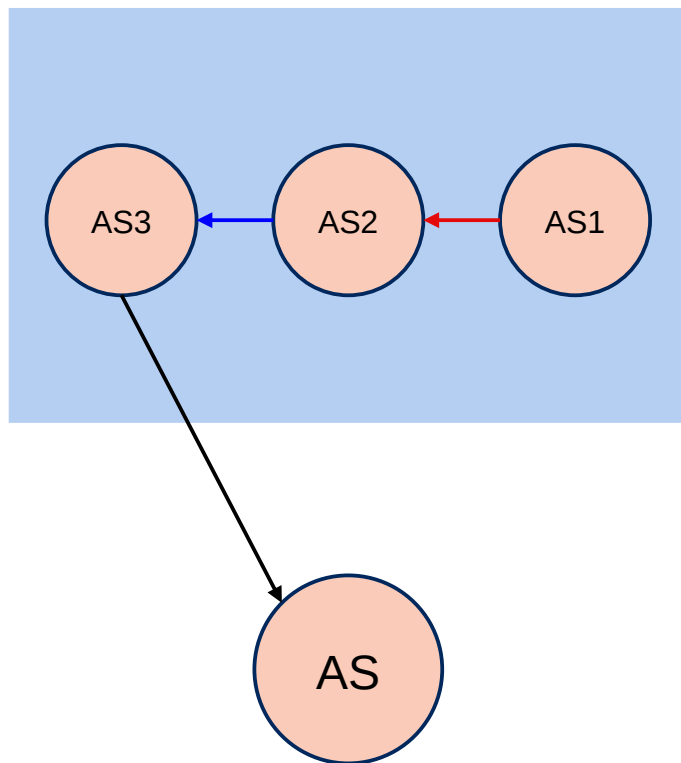
- Three-element AS path
- AS1 ASPA exists, but does not include AS2
- Route leak still not possible



Downstream validation examples (9)

ASPAs

AS	Providers
AS1	AS4



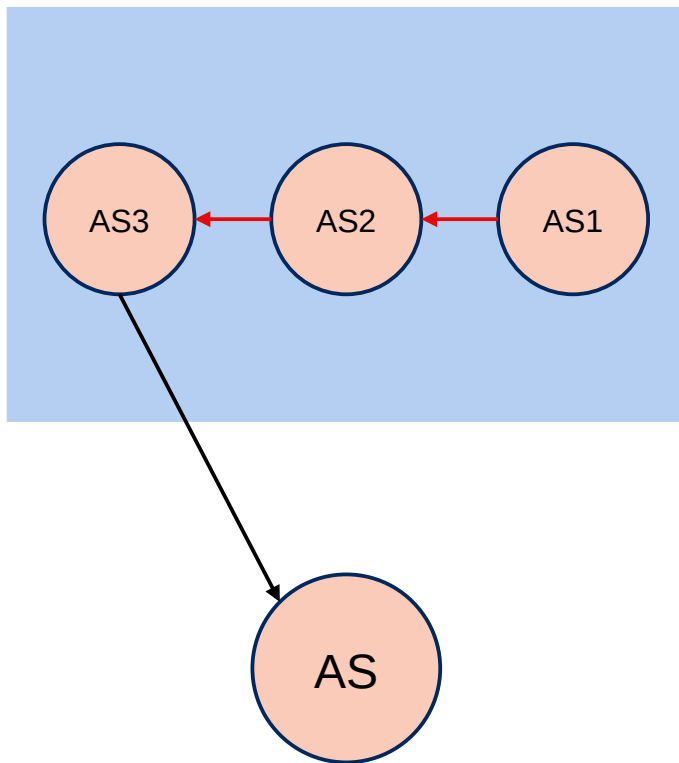
- Three-element AS path
- AS1 ASPA exists, but does not include AS2
- No AS3 ASPA
- Unable to determine validity status



Downstream validation examples (10)

ASPAs

AS	Providers
AS1	AS4
AS3	AS5

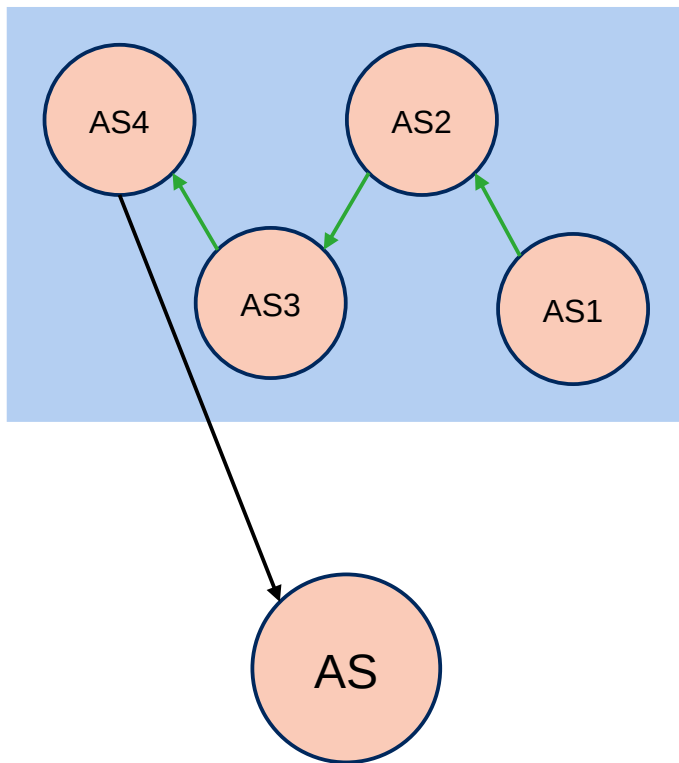


- Three-element AS path
- AS1 and AS3 ASPAs both present, but neither lists AS2
- Route leak

Downstream validation examples (11)

ASPAs

AS	Providers
AS1	AS2
AS2	AS0
AS3	AS2, AS4
AS4	AS0



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



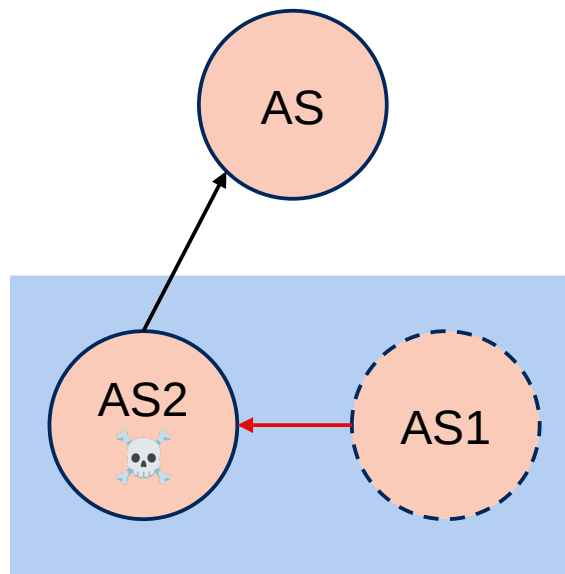
Forged-origin/path attacks

- Upstream and downstream validation examples demonstrate functionality for inadvertent problems
- But validation also helps with certain attacks

Forged-origin/path attack examples (1)

ASPAs

AS	Providers
AS1	AS3



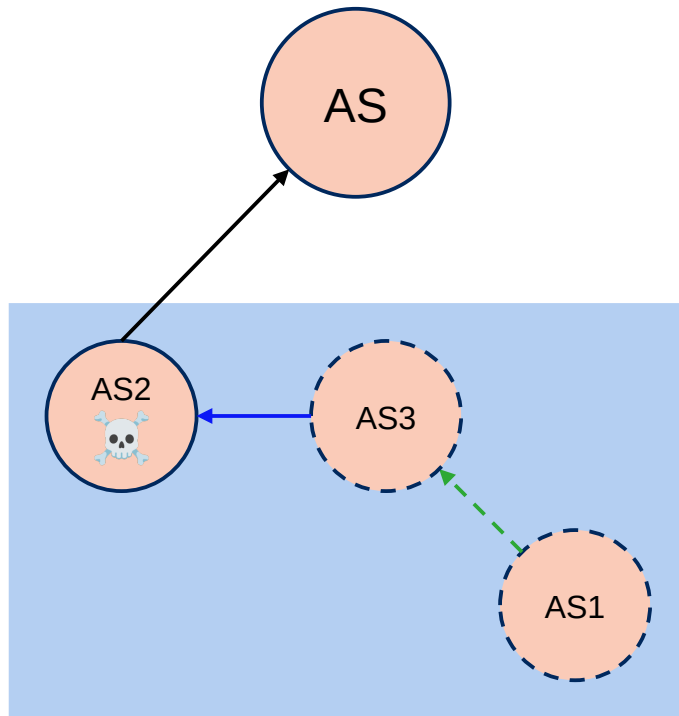
- AS2 is attacker
- Provides forged path contrary to ASPA
- Able to determine validity



Forged-origin/path attack examples (2)

ASPAs

AS	Providers
AS1	AS3



- So attacker adds AS3
- Recipient now unable to determine validity



- But - path now longer, so less likely to be chosen
- And path forgery forced to become longer as more ASPAs are created

What is a provider?

- Common point of confusion
- From the object definition draft:

A Provider AS (PAS) is a network providing connectivity between networks - it provides transit services to the customer. That is:

- a. The provider may propagate Border Gateway Protocol (BGP) routes received from any direction to their customers. For example, routes the provider learned from its own providers, lateral peers, and other customers. The provider may also announce a default route to their customers.
- b. The provider may propagate BGP routes received from the customer in any direction. For example, to the provider's providers, lateral peers, and other customers.

What is a provider? (2)

- Important points:
 - If it looks like a provider and acts like a provider, it has to be listed as a provider
 - When creating an ASPA, make sure that you know your full set of providers
 - It is possible for AS1 to be a provider for AS2, and vice versa (described as a “complex” peering relationship)

Risks

- A mistaken ASPA change can invalidate all routes that pass through the affected AS
 - But this is similar to how ROAs work
 - Operators understand potential severity of RPKI misconfiguration in that context
 - Earlier deployment of ASPA validation can help here
 - Problems are more easily linked to object operations, rather than validation being enabled
- Also, ASPAs for apex ASes (i.e. tier-1 networks) have no effect in practice: it's not possible to invalidate routes by way of changes to such ASPAs

Document status

- The ASPA drafts are progressing as a group, alongside the associated rpki-rtr protocol changes (draft-ietf-sidrops-8210bis)
- Each is past working group last call, but there are some changes and reviews pending before they progress to IETF last call
- Time required from here to RFC varies, but probably somewhere between six months and a year

Tools for CA operators

- CA operators (generally IP address and/or ASN holders) have two main options for object issuance:
 - Use RIR portal to manage the CA ('RIR-hosted')
 - Run local CA ('delegated')
 - Krill from NLNetLabs is the most common option
 - The vast majority of CA operators use their RIR portal for this
- Delegated CA does have some use cases, though

APNIC
MyAPNIC

Autonomous System Provider Authorization (ASPA)

An ASPA is called the ASNs for th Customer AS the Custome from the RP the specifi

Update ASPA

Customer AS*
45163
A customer AS number for the ASPA.

Provider(s)
1221,7575
Use commas to separate multiple provider ASes.

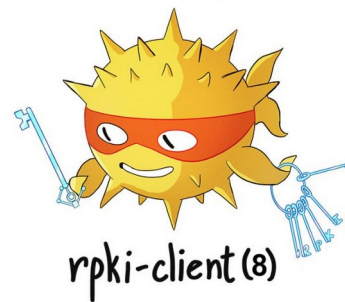
Cancel Submit

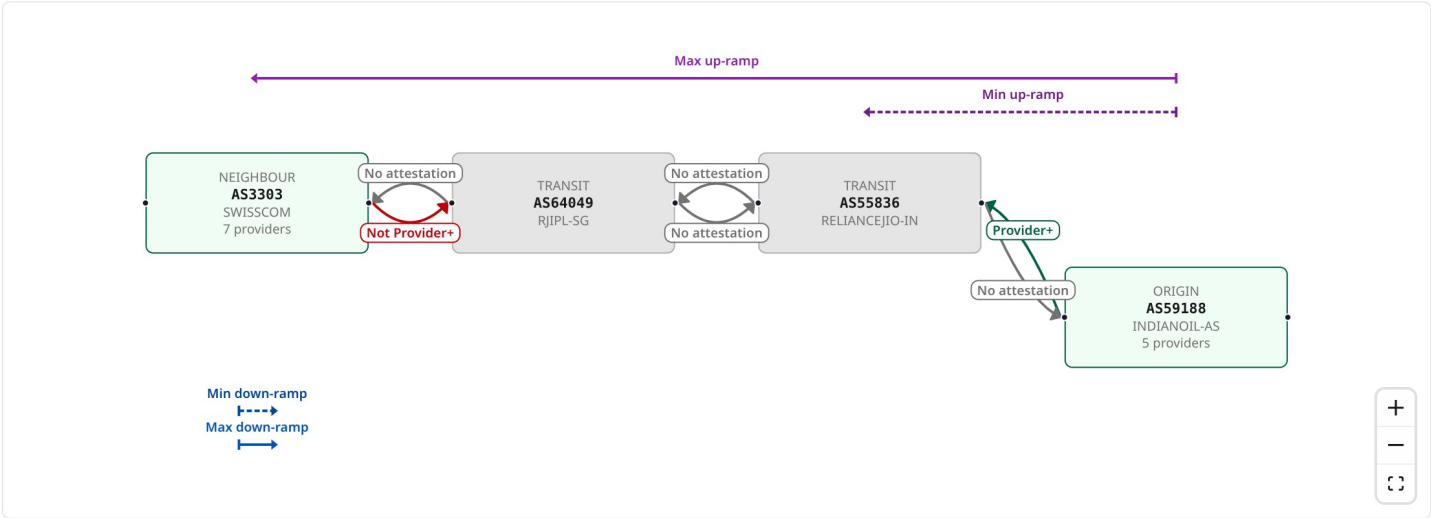
45163 (APNIC-TUI2-AU)
131211 (APNIC-SERVICES) 0

Previous 1 Next

Tools for relying parties (RPs)

- Several good common options for validating RPKI information:
 - Routinator
 - rpki-client
 - FORT
- Similarly for rpki-rtr service:
 - rtrtr
 - StayRTR
 - OpenRTRd





Has ASPA No ASPA Provider+ Not Provider+ No attestation Max up-ramp Min up-ramp Max down-ramp Min down-ramp

ASPA records

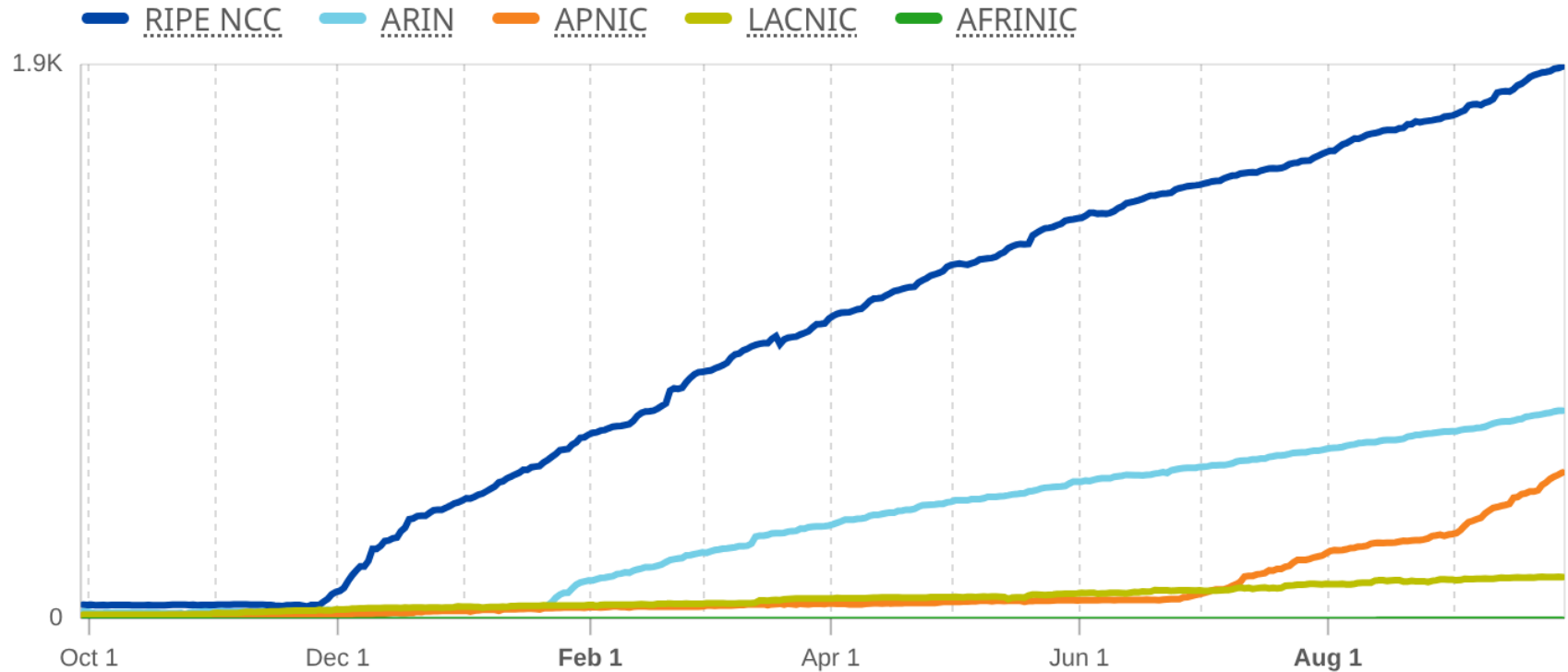
ASN	Name	ASPA status	Providers
AS3303	SWISSCOM	ASPA	AS174 AS2914 AS3320 AS6939 AS7473 AS12956 AS33891
AS64049	RJIPL-SG	No ASPA	-
AS55836	RELIANCEJIO-IN	No ASPA	-
AS59188	INDIANOIL-AS	ASPA	AS4755 AS9498 AS9829 AS45117 AS55836

```
$ git clone https://github.com/APNIC-net/rpki-rtr-demo
...
$ APNIC_DEBUG=1 rpki-rtr-client client-data-dir aspa-validation --announcement "TABLE_DUMP2|1698933600|B|
64.71.137.241|6939|1.0.0.0/24|6939 13335|IGP|64.71.137.241|0|0||NAG|13335 10.34.0.16|" --provider-asns 6939
623878: validation-aspa: unique path: 6939 13335
623878: validation-aspa: max_up_ramp check for 13335 -> 6939 results in provider
623878: validation-aspa: did not find not-provider hop on up ramp, max_up_ramp defaults to 2
623878: validation-aspa: min_up_ramp check for 13335 -> 6939 results in provider
623878: validation-aspa: did not find not-provider/no-attestation hop on up ramp, min_up_ramp defaults to 2
623878: validation-aspa: max_down_ramp check for 6939 -> 13335 results in no-attestation
623878: validation-aspa: did not find not-provider hop on down ramp, max_down_ramp defaults to 2
623878: validation-aspa: min_down_ramp check for 6939 -> 13335 results in no-attestation
623878: validation-aspa: reached min_down_ramp (1) at 6939 -> 13335 (no-attestation)
623878: validation-aspa: downstream
623878: validation-aspa: max_up_ramp: 2
623878: validation-aspa: min_up_ramp: 2
623878: validation-aspa: max_down_ramp: 2
623878: validation-aspa: min_down_ramp: 1
623878: validation-aspa: valid
Valid
$
```

RPKI ASPA deployment

Show full history ☐

Number of RPKI ASPA entries over time ?



Related techniques

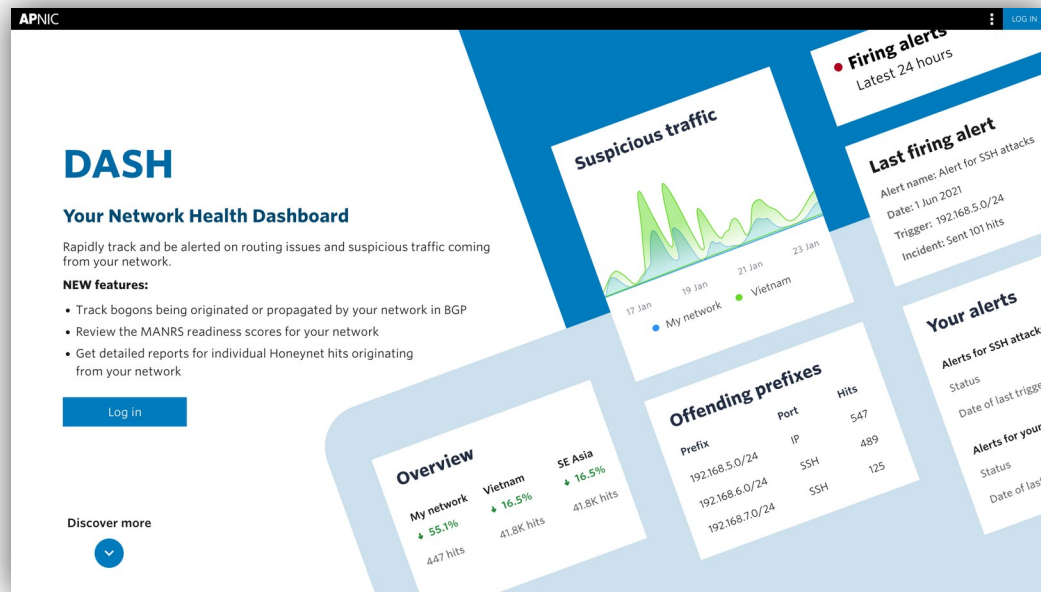
- Route Origin Validation (ROV) (RFC 6483)
- BGP Roles (RFC 9234)
- First AS check
- Maximum prefix limits

Monitoring ASPAs with APNIC DASH

Rafael Cintra
Product Manager - Information
30/09/2026

DASH

- APNIC's Network Health Dashboard
- Available to all APNIC Members at dash.apnic.net



DASH Services

- Current services
 - Routing status (now including ASPA status)
 - Suspicious traffic
 - Potential security vulnerabilities
 - Bogons
 - MANRS readiness score
 - Weekly network health report

ASPA status

- On the new ASPA status page, Members can review the current ASPA status of their ASNs and the ASNs originating their prefixes.
- The Routing status dashboard page has also been updated with ASPA status information.

New ASPA status page

APNIC

DASH «

ASPA status Member account: MEMBER-AP ▼

Review ASPA coverage for your Internet number resources

Check ASPA object coverage in your network to prevent route leaks, forged-origin attacks, and forged-path attacks. ?

Your ASNs

❗ AS65001 - ASPA not published	
⚠ AS65002 - ASPA published (upstream has no published ASPA)	^
Provider ASNs from ASPA:	
❗ AS65005 - ASPA not published	
✅ AS65003 - ASPA published	^
Provider ASNs from ASPA:	
✅ AS65002 - ASPA published	
✅ AS65004 - ASPA published	^
Provider ASNs from ASPA:	
✅ AS65002 - ASPA published	

Other ASNs originating your prefixes

❗ AS65005 - ASPA not published
❗ AS65006 - ASPA not published

Useful Links

- What's new
- Help
- Data sources
- Disclaimer

New ASPA column in Routing status

APNIC

DASH

Overview

Routing status

Dashboard

ASPA status

Alerts 3

Suspicious traffic

Dashboard

Alerts

Vulnerabilities

Bogons

Dashboard

Alerts

MANRS readiness

Weekly Report

Security blog posts

Useful Links

What's new

Help

Data sources

Disclaimer

Routing status

Member account: MEMBER-AP

Showing routes for: your prefixes

Review the routing information for your prefixes

Prevent network misconfigurations and detect BGP hijacks.

Overview of inconsistencies for your prefixes

Status of ROAs and route objects as seen in BGP:

ROA mismatches 2

Route object mismatches 0

ROA not published 0

Route object not published 2

View prefixes

Routing status for your prefixes

* indicate ASNs I am NOT the holder of

Show 20 entries

Search by prefix or ASN

Prefix	BGP route	Origin AS	ROA	ASPA	Route object
10.120.0.0/13	10.120.0.0/13	AS65001	Published	Published + info	Published
10.128.0.0/11	10.128.0.0/11	AS65001	Published	Published + info	Published
127.172.0.0/14	127.173.112.0/24	*AS65002	Mismatch + info	Not published	Not published
127.172.0.0/14	127.173.113.0/24	*AS65002	Mismatch + info	Not published	Not published

Future features

- ASPA validation status for BGP routes
- Alerts
 - Potential route leaks and hijacks
 - ASN listed or removed as a provider in a ASPA object