RPKI and Whois Updates: RSCs, ASPAs, NRTMv4, RDAP

AusNOG 2023

What is an RSC?

- **R**PKI **S**igned **C**hecklist
- Defined in RFC 9323
- The specification provides for:
  - signing one or more arbitrary files using an RPKI certificate
  - packaging the signature, filenames, and hashes into an object (the **RSC** itself)
  - verifying the signature (i.e. “these files were signed by somebody with authority to route 192.0.2.0/24”)

Why is it useful?

- Arbitrary files can be signed
  - More flexible than existing RPKI functions
  - Supports ad hoc/people-driven processes
- No need to publish in a public repository
  - Associated business operations can remain private

Use cases

- BYOIP services
- Third-party databases
- Custom RPKI applications

BYOIP services

- Support use of RIR-delegated IP addresses for BGP announcements in cloud infrastructure
- RSCs can help to streamline the registration process

aws

Microsoft Azure

1. Get token from portal
2. Make RSC with token
3. Upload RSC to portal
4. Make ROA

…

Third-party databases

- Acting as cross-RIR interfaces for specific use cases (e.g. peering)
- RSCs can be used to prove resource holdership

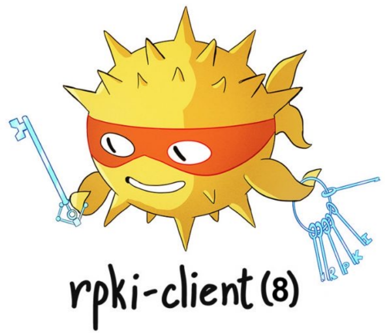
PeeringDB

Custom RPKI applications

- Define new object type and use RSCs for signing/packaging
- Useful for testing/prototyping, or for use within a closed group of participants
- No need to go through IETF process

Current status

- Specification published in November 2022
  - https://www.rfc-editor.org/rfc/rfc9323.txt
- Production code
  - https://www.rpki-client.org
- Proof-of-concept code
  - https://github.com/APNIC-net/rpki-rsc-demo
  - https://github.com/job/draft-rpki-checklists
  - https://github.com/benmaddison/rpkimancer
- APNIC implementing in early 2024
  - Deferred from Q2 of this year
  - In-principle support from other RIRs



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 defines its upstream ASes
  - a network operator using that data to verify the AS_PATH of a received route

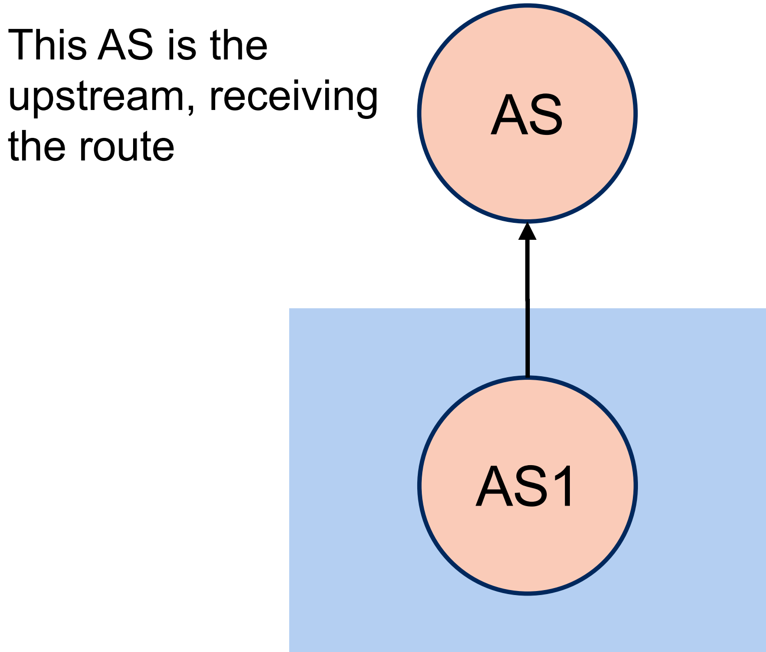
Why is it useful?

- 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 → i
- 4. Otherwise, all hops are from customer to provider → ✓

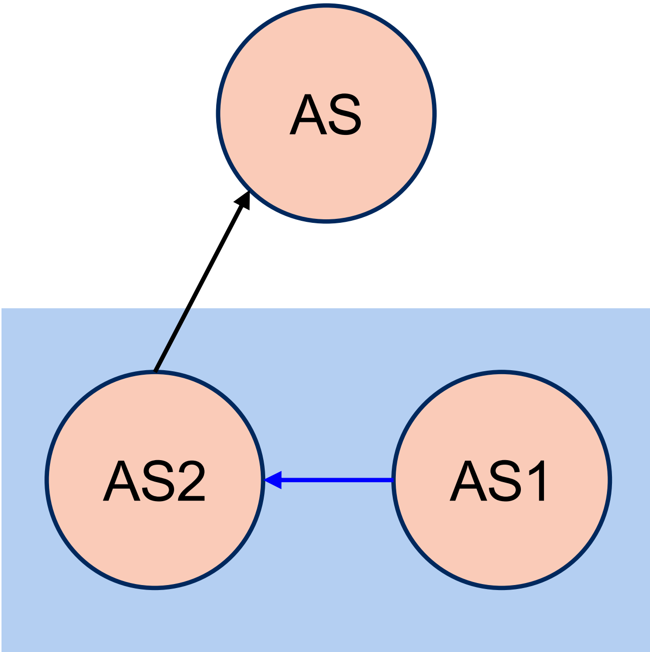
Upstream validation examples (1)



- 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

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

Upstream validation examples (2)



Blue line: no ASPA for customer-provider pair

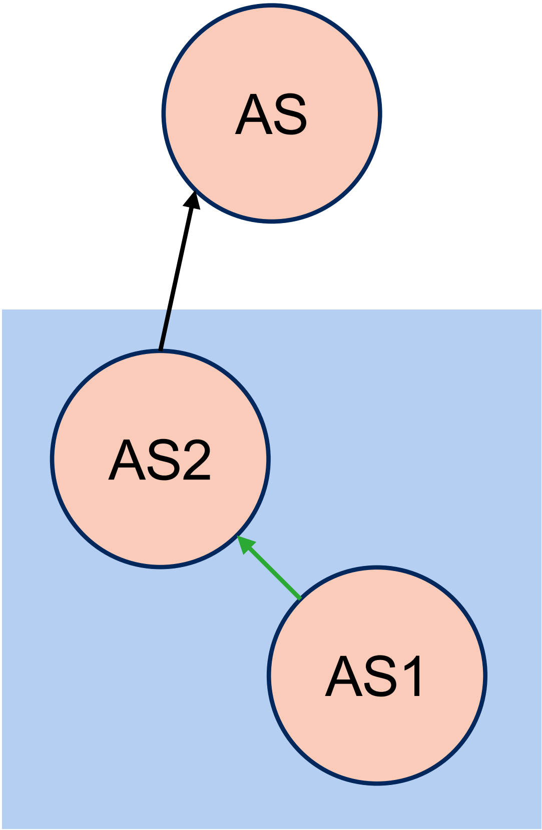
- Two-element AS path
- No ASPAs
- Unable to determine validity

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



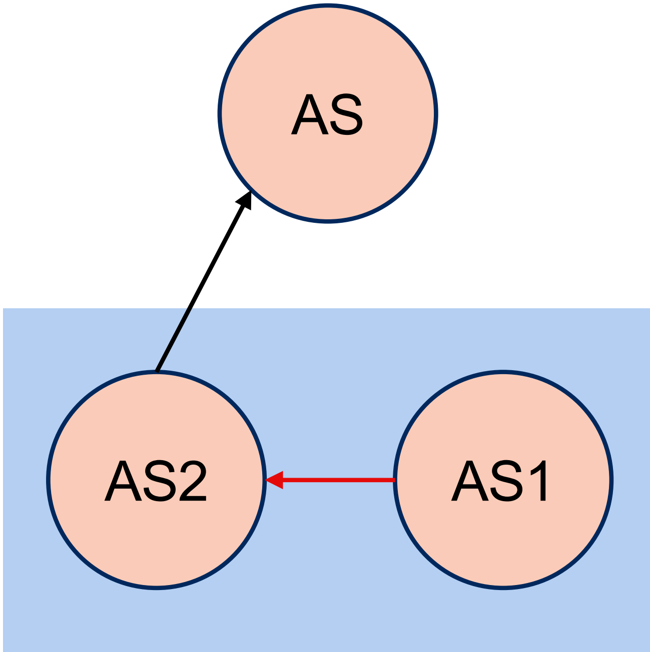
- Two-element AS path
- ASPA exists for AS1 (origin)
- Able to determine validity

Upstream validation examples (4)

ASPAs

AS	Providers
AS1	AS3

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

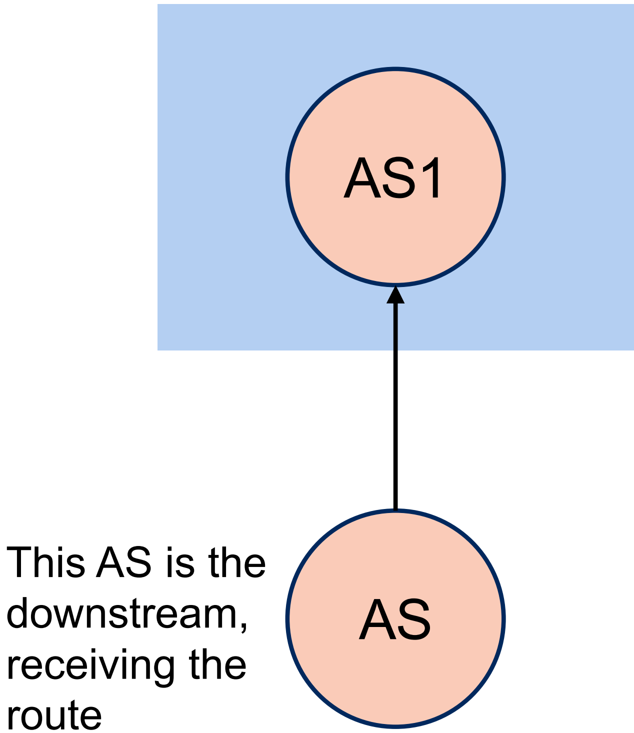


- Two-element AS path
- ASPA exists for AS1 (origin), but disclaims AS2 as provider
- Able to determine validity

Downstream validation

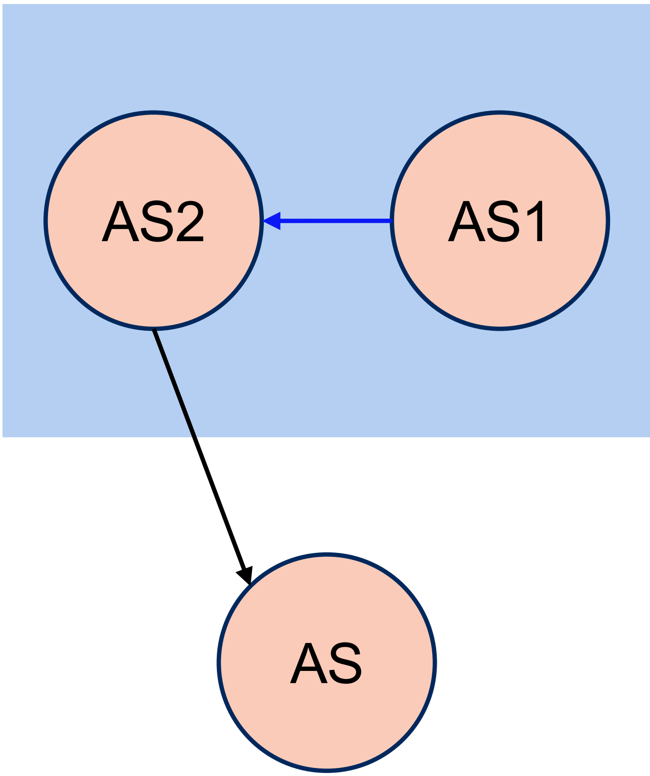
- 1. If AS path has:
  - Up-ramp, customer(s) through provider(s)
  - Down-ramp, provider(s) through customer(s)
  - No hops in the middle, or single lateral hop
- 2. If AS path contains ‘valley’ (hop from provider to customer, then from customer to provider)
- 3. Otherwise, unable to determine validity

Downstream validation examples (1)



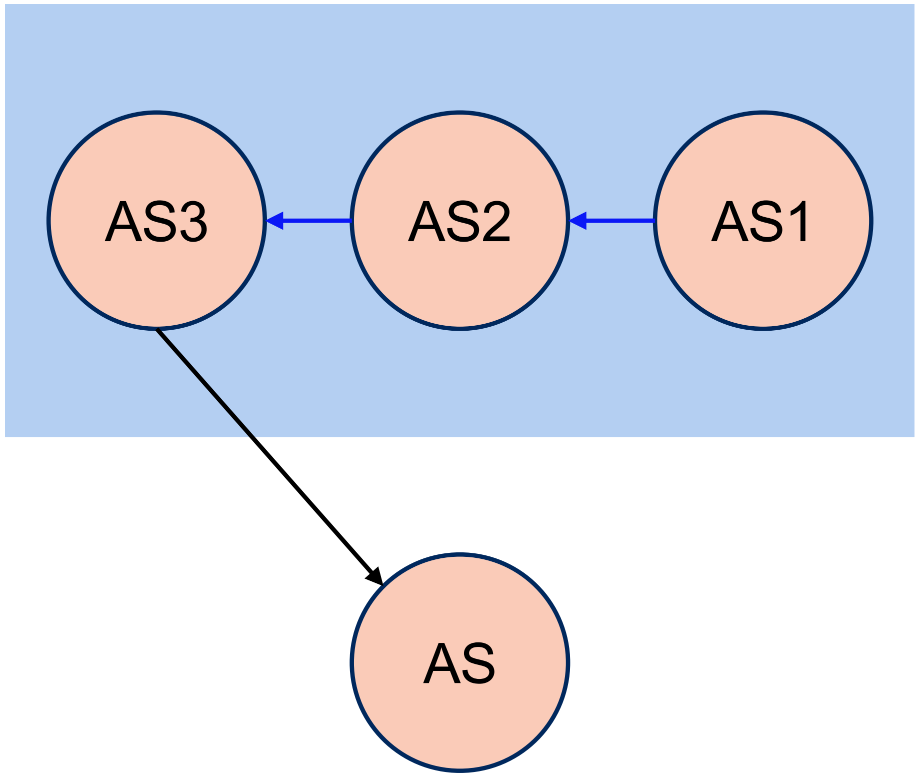
- Single-element AS path
- ASPA state not relevant
- Not possible for it to be a route leak

Downstream validation examples (2)



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

Downstream validation examples (3)

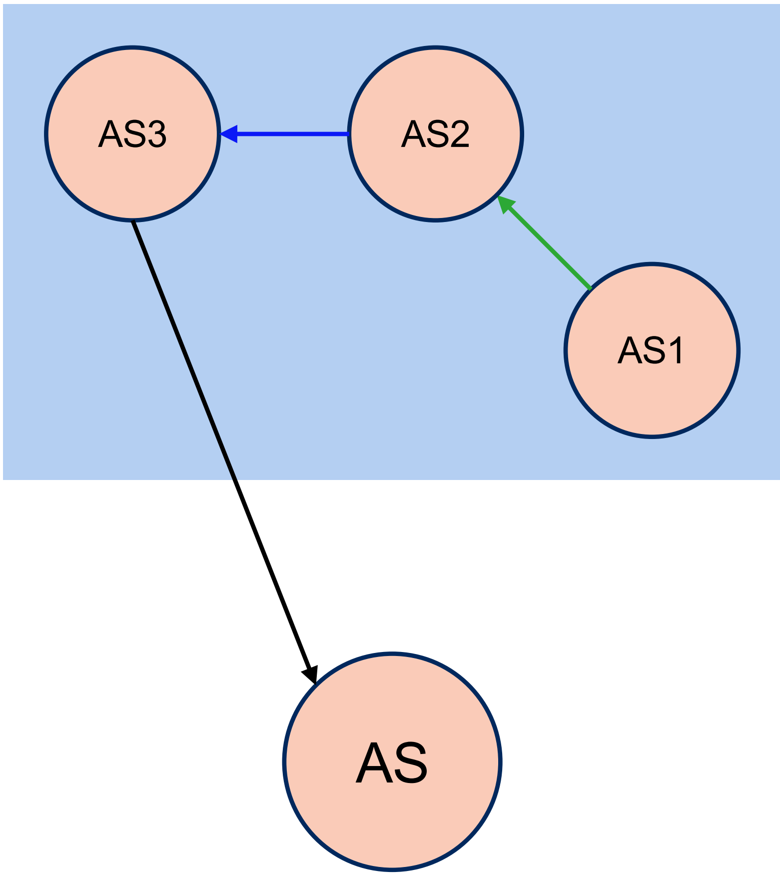


- Three-element AS path
- No ASPAs
- Unable to determine validity

Downstream validation examples (4)

ASPAs

AS	Providers
AS1	AS2



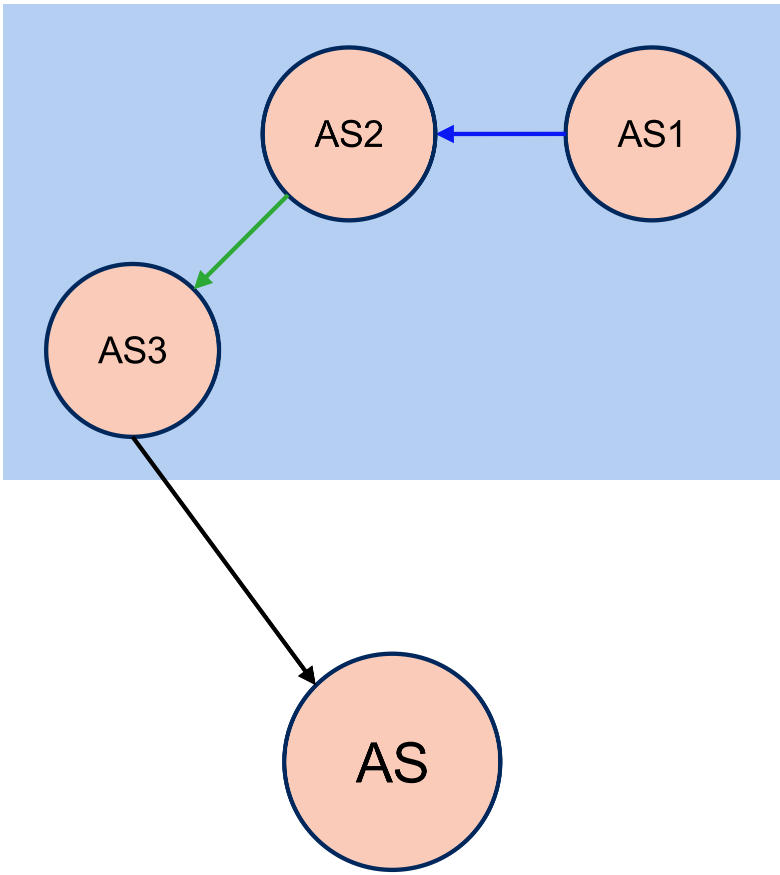
- Three-element AS path
- ASPA exists for AS1 (origin)
- Route leak not possible

Downstream validation examples (5)

Within route, lower ASes are customers of higher ASes

ASPAs

AS	Providers
AS3	AS2

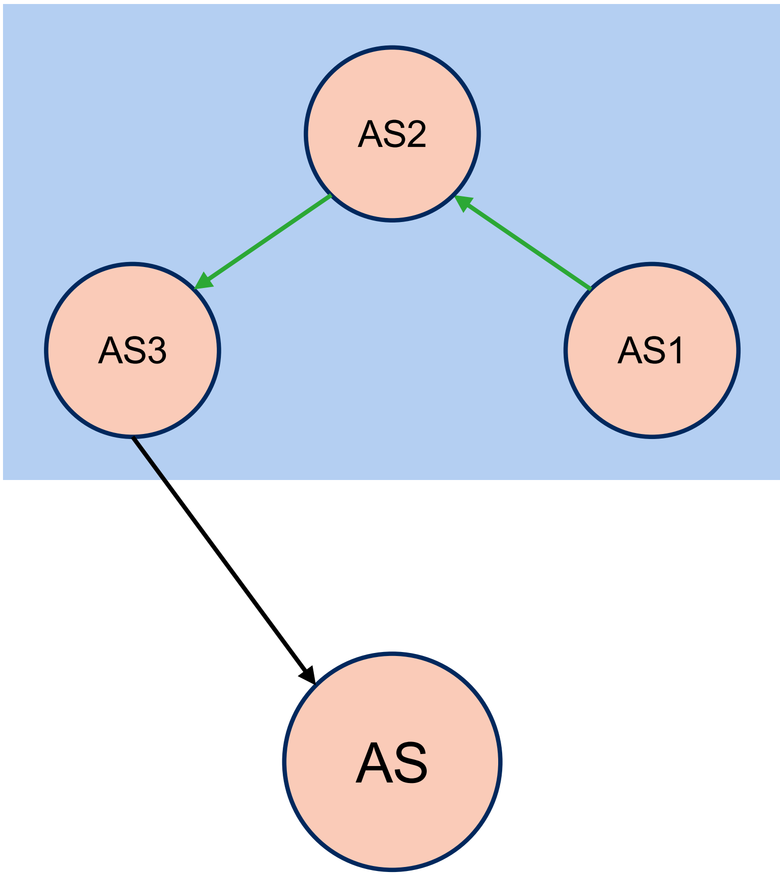


- Three-element AS path
- ASPA exists for AS3 (neighbour)
- Route leak not possible

Downstream validation examples (6)

ASPAs

AS	Providers
AS1	AS2
AS3	AS2

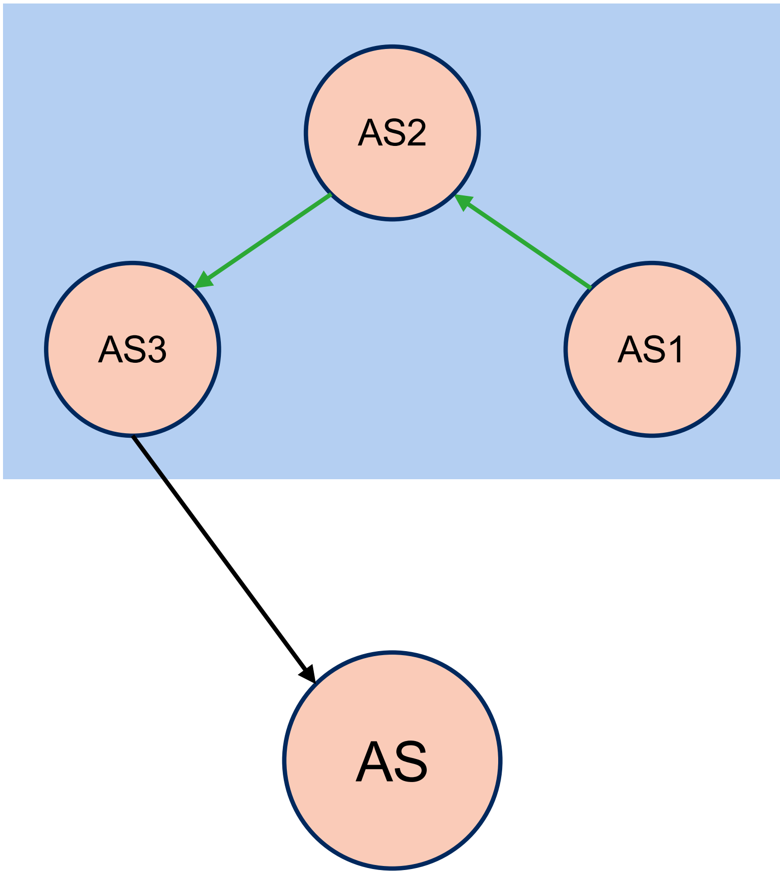


- Three-element AS path
- ASPAs exist for AS1 and AS3
- Route leak not possible

Downstream validation examples (7)

ASPAs

AS	Providers
AS1	AS2
AS2	AS0
AS3	AS2

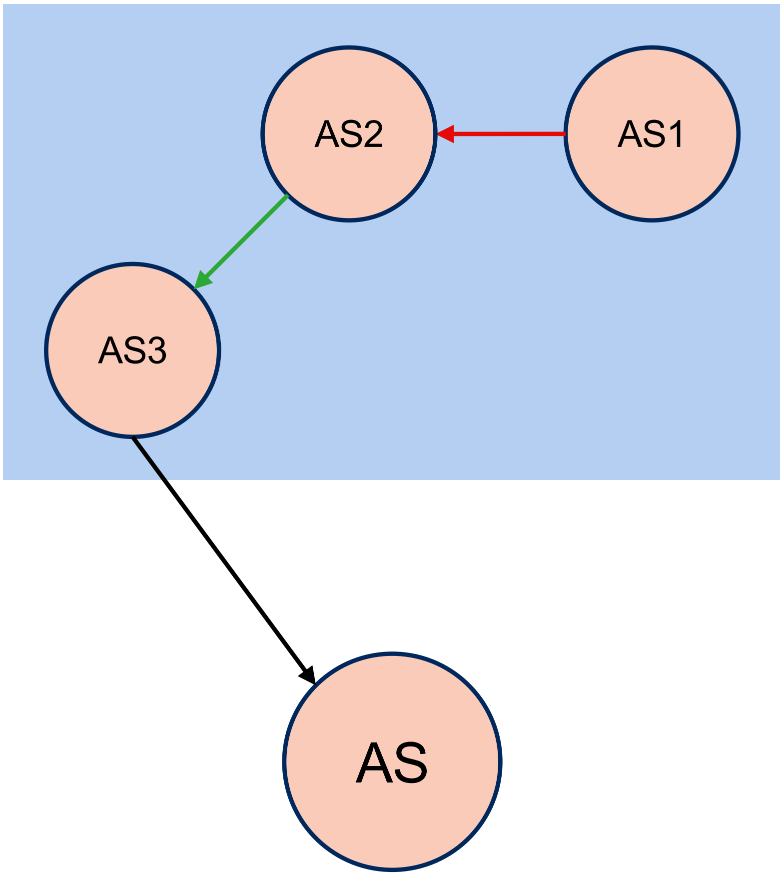


- Three-element AS path
- AS0 ASPA now exists for AS2, to indicate absence of providers
- Route leak not possible

Downstream validation examples (8)

ASPAs

AS	Providers
AS1	AS4
AS3	AS2

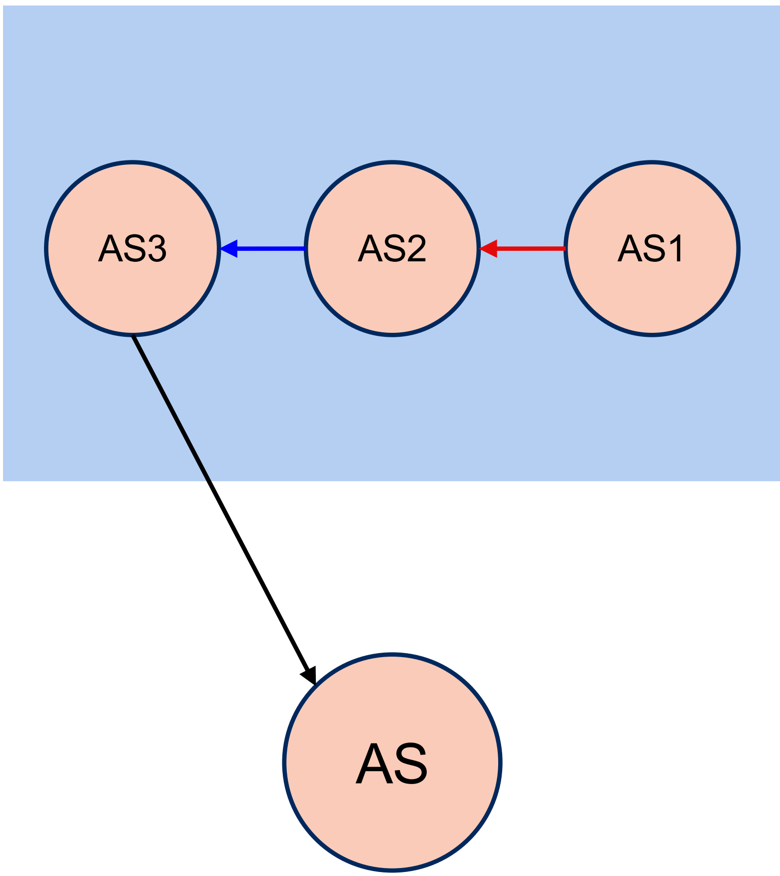


- Three-element AS path
- AS1 ASPA exists, but does not include AS2
- Route leak still not possible

Downstream validation examples (9)

ASPAs

AS	Providers
AS1	AS4

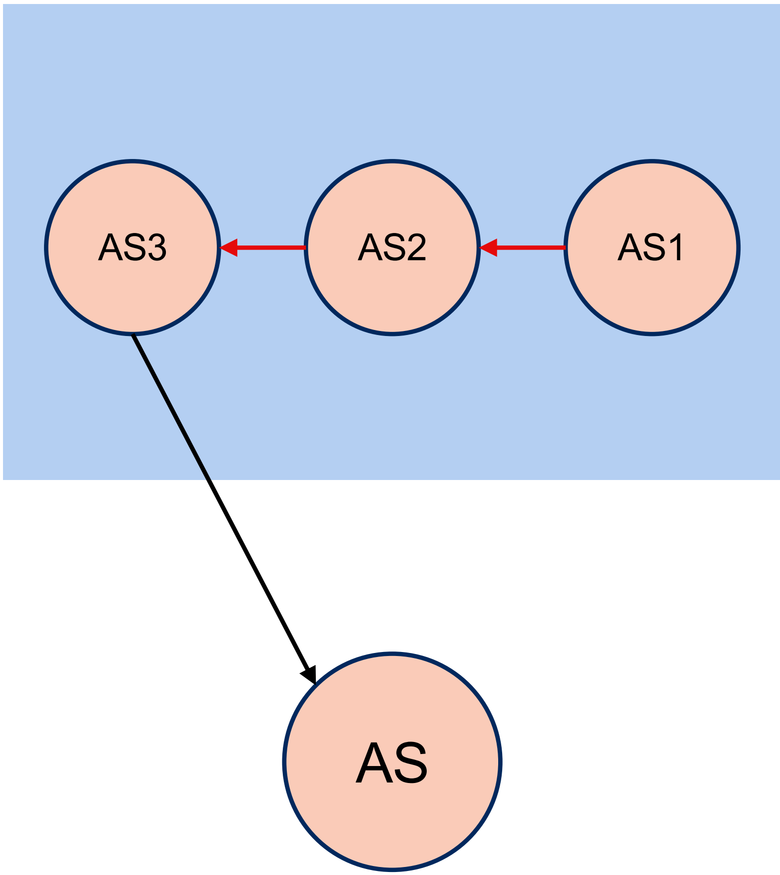


- Three-element AS path
- AS1 ASPA exists, but does not include AS2
- No AS3 ASPA
- Unable to determine validity status

Downstream validation examples (10)

ASPAs

AS	Providers
AS1	AS4
AS3	AS5

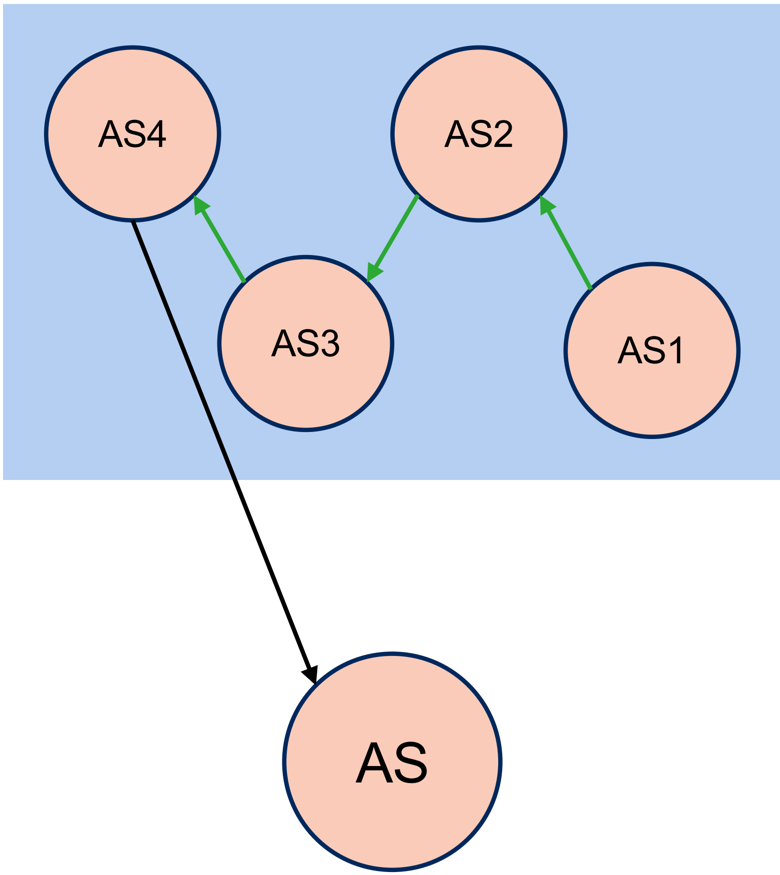


- Three-element AS path
- AS1 and AS3 ASPAs both present, but neither lists AS2
- Route leak

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

- Attacker uses correct origin (AS1), but inserts own ASN into the AS path immediately after the origin
  - If AS1 has registered an ASPA, and AS2 (target recipient) receives route over lateral peer, AS2 will classify the route as invalid
- Attacker can evade this by adding a valid upstream ASN after the origin and before its own ASN
  - But if the ASN that is added also has an ASPA, then the attacker needs to add more ASNs until it reaches an ASN without an ASPA
  - Plus, this all makes the path longer, and the route less likely to be used/preferred

Risks

- "If I turn this on, do I get more helpdesk calls?"
  - A single mistaken ASPA change can invalidate all routes that pass through the affected AS
  - But the damage here is akin to the relevant AS disappearing: if it's a SPOF today, it will be a SPOF with ASPA enabled
  - Also, ASPAs for apex ASes have no effect in practice: it's not possible to invalidate routes by way of changes to such ASPAs

Current status

- Specifications currently in IETF Working Group Last Call
- Production code
    - Krill (CA)
    - Routinator (RP)
    - rpki-client (RP)
    - OpenBGPD (router)
    - NIST BGP-SRx (router)
    - (No Cisco/Juniper/similar yet)
- RIPE provide API for creating ASPA objects in the localcert.ripe.net environment (test)
- APNIC planning to implement hosted CA functionality in 2024

What is NRTMv4?

- **N**ear **R**eal **T**ime **M**irroring (**v4**)
- Defined in draft-ietf-grow-nrtm-v4
- Provides for maintaining a local, up-to-date (< 10 minutes) copy of a remote Whois/IRR database:
    - RADb, RIPE, APNIC, etc.
- Successor to earlier, less formal versions of NRTM

Why is it useful?

- NRTM v3 and earlier have various shortcomings
- Ad hoc response structuring
- Underspecified:
  - No formal documentation
  - Error states not clear
  - End of stream not clear
- Initial state not handled in-band
  - Sync failure requires manual intervention

```
$ whois -hnrtm.apnic.net -p43003 -- -g APNIC:3:11088811-11088812

% How to use this server        http://www.apnic.net/db/

%START Version: 3 APNIC 11088811-11088812 FILTERED

ADD

inetnum:        123.243.122.216 - 123.243.122.219
netname:        TPGInternetPtyLtd
descr:          TPG Internet Pty Ltd.
...
last-modified:  2023-06-30T03:44:27Z
source:         APNIC

DEL

inetnum:        14.201.196.140 - 14.201.196.143
netname:        TPGInternetPtyLtd
descr:          TPG Internet Pty Ltd.
...
last-modified:  2023-06-28T01:16:39Z
source:         APNIC

%END APNIC

$
```

Why is it useful?

- NRTMv4 addresses these problems
- HTTP/JSON
- Standardised via IETF
- All data is signed
- Based on RRDP: snapshots available in-band

```
$ curl -s https://nrtm-rc.db.ripe.net/nrtmv4/RIPE/update-notification-file.json | jq .
{
  "nrtm_version": 4,
  "timestamp": "2023-06-30T00:06:00Z",
  "type": "notification",
  "source": "RIPE",
  "session_id": "912dbc2b-3d9a-4731-81a3-fd03f10afa67",
  "version": 5,
  "snapshot": {
    "version": 5,
    "url": "https://nrtm-rc.db.ripe.net/nrtmv4/RIPE/nrtm-snapshot.5.RIPE.912dbc2b-3d9a-4731-81a3-fd03f10afa67.4720f594658f35d29f3106da47096242.json.gz",
    "hash": "36ba8e20b36f03514d314e660b390cfc2f0a248e9516d7de869a4577c7e5d072"
  },
  "deltas": []
}
$
```

Current status

- Specification currently being worked on in IETF Global Routing Operations (grow) WG
- Proof-of-concept code
  - https://github.com/RIPE-NCC/whois
  - https://github.com/petchells/nrtm4client
- RIPE provide public test service
- Developed by IRRd v4 maintainer, so will be implemented there as well
  - IRRd used by e.g. RADb
- Depending on interest, APNIC will deploy based on RIPE's implementation

RDAP updates: RIR RDAP profile

- Available at https://www.iana.org/assignments/rdap-extensions/rdap-extensions.xhtml
- Implemented by all RIRs except LACNIC, who plan to implement later this year
- Ensures cross-RIR consistency
  - Redirects
  - Resource status
  - Contact data formatting/elements

RDAP updates: reverse search

`draft-ietf-regext-rdap-reverse-search`

- Supports operations like finding resources associated with a given contact
- Most RIRs provide this functionality today via their Whois services

RDAP updates: RIR search

`draft-ietf-regext-rdap-rir-search`

- Basic IP/ASN search
- Reverse search extensions for IP/ASN records
- Searches for more-specific and less-specific resources

Questions?