ASPA

RPKI for path validation!

Anurag Bhatia, Hurricane Electric

Presentation overview

1. **How filtering is done presently**
2. Introduction to ASPA
3. Creating ASPA record
4. Configuring ASPA for path validation
5. ASPA deployment at Hurricane Electric

How is filtering done presently?

How filtering is done so far...

- Varies from operator to operator
- Some filter based on route object, some based on custom logic
- Some filter only customers, some peers, very few filter upstream
- No easy/standardized end to end tooling (e.g bgpq3 exists but needs mechanism to “push” rules to the router)

No standardised way to filter, it’s just broken...

Presentation overview

1. How filtering is done presently
2. **Introduction to ASPA**
3. Creating ASPA record
4. Configuring ASPA for path validation
5. ASPA deployment at Hurricane Electric

Introduction to ASPA

- Stands for Autonomous System Provider Authorization (ASPA)
- Brings RPKI into path validation like ROA did for origin validation
- Brings cryptography as well as easy to integrate tooling for filtering route leaks
- More secure than AS-SETs

Example of ASPA record

- Customer AS number
- Provider AS number (can be multiple)
- RPKI TA (Trust Anchor)
- Note: Provider = upstream only & not a peer


```
{
  "customer": "AS11358",
  "providers": [
    "AS835",
    "AS6939",
    "AS34927"
  ],
  "ta": "arin"
}
{
  "customer": "AS11708",
  "providers": [
    "AS32097"
  ],
  "ta": "arin"
}
{
  "customer": "AS11967",
  "providers": [
    "AS835",
    "AS1299",
    "AS6939",
    "AS34872",
    "AS34927",
    "AS50917",
    "AS58057",
    "AS213753",
    "AS214809",
    "AS215828"
  ],
  "ta": "arin"
}
```

ASPA validation logic

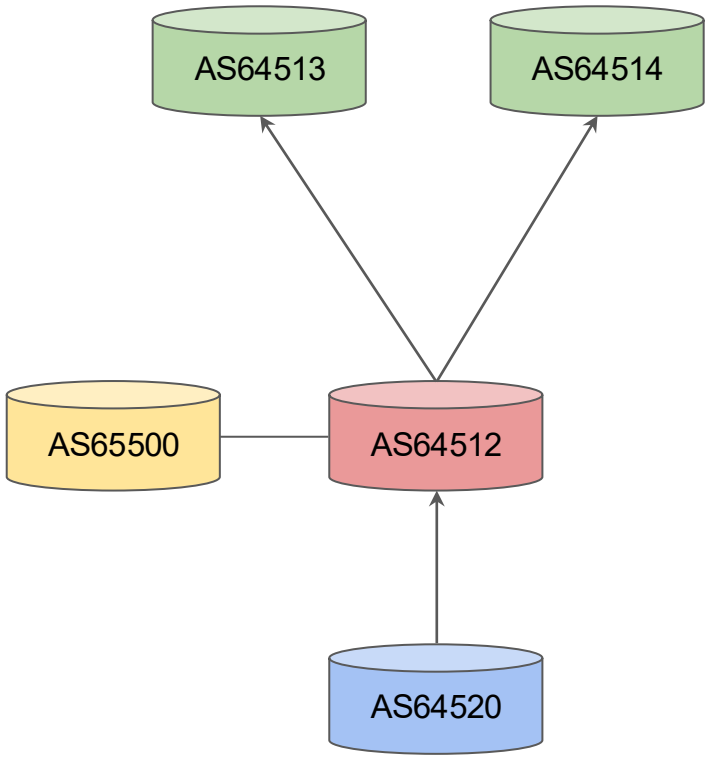
- Validation is done across the AS_PATH with possible states as: Provider, Not Provider or Unknown state
- Similar to RPKI ROA, routes are rejected if a “Not Provider” comes in the path. Lack of ASPA is not dropped
- ASPA doesn’t care if adjacency is upstream or downstream or peer but follows validation based on declared upstream by each ASN
- Logic for rejection is applied in policy and hence can be selectively applied for the rollout

ASPA validation logic

- AS64512 has upstream AS64513 and AS64514
- AS64512 has peering with AS65500
- AS64512 has a customer AS64520
- ASPA object:

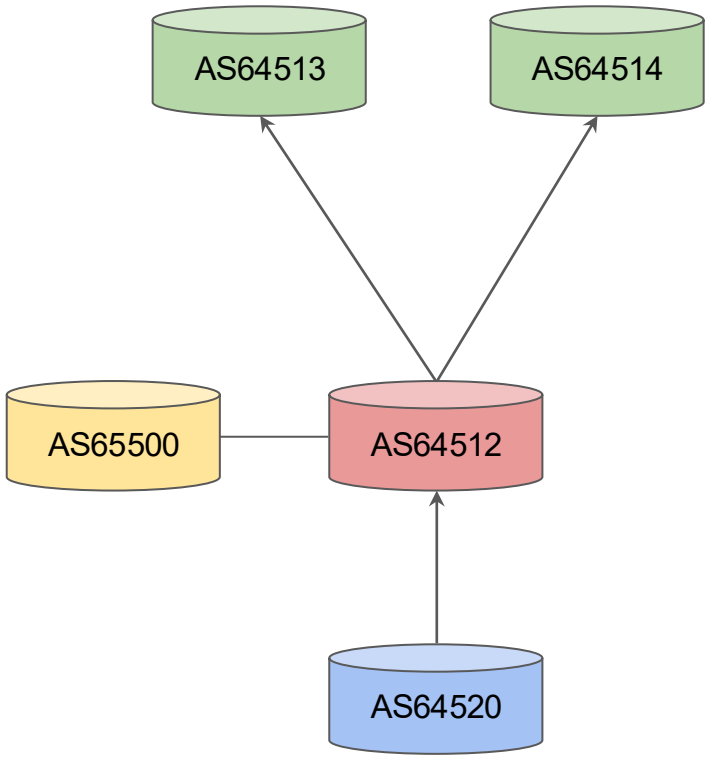
  Customer: AS64520
  Providers: AS64512

  Customer: AS64512
  Providers: “AS64513”, “AS64514”



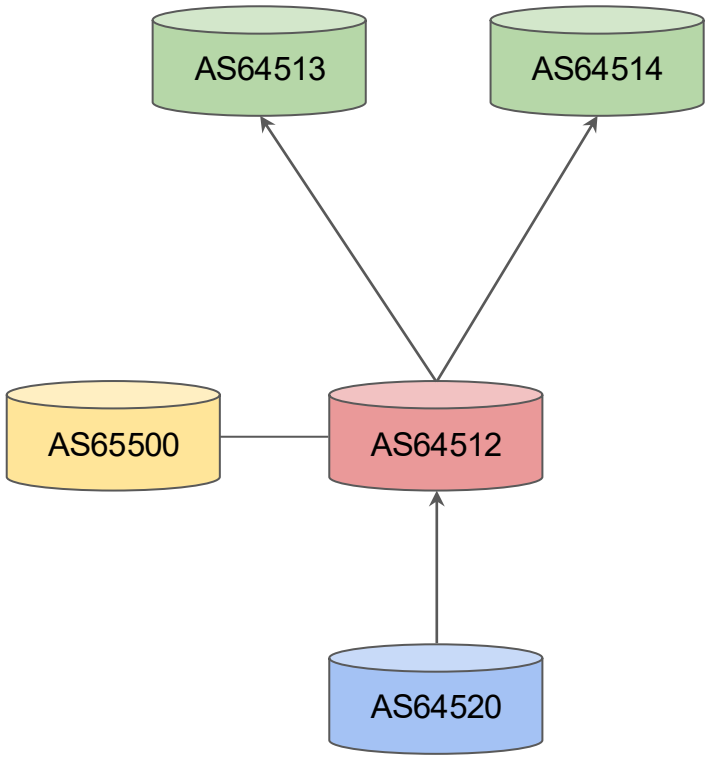
ASPA validation logic

- For AS64513 - they would see AS64520 as: 64513 64512 64520
- They can validate from ASPA object of AS64520 and will mark it as valid route



Case of route leak

- In this case AS64512 can leak AS65500 because of missing ASPA object by AS65500
- If AS65500 has a object, leak would be detected & dropped by network doing the validation

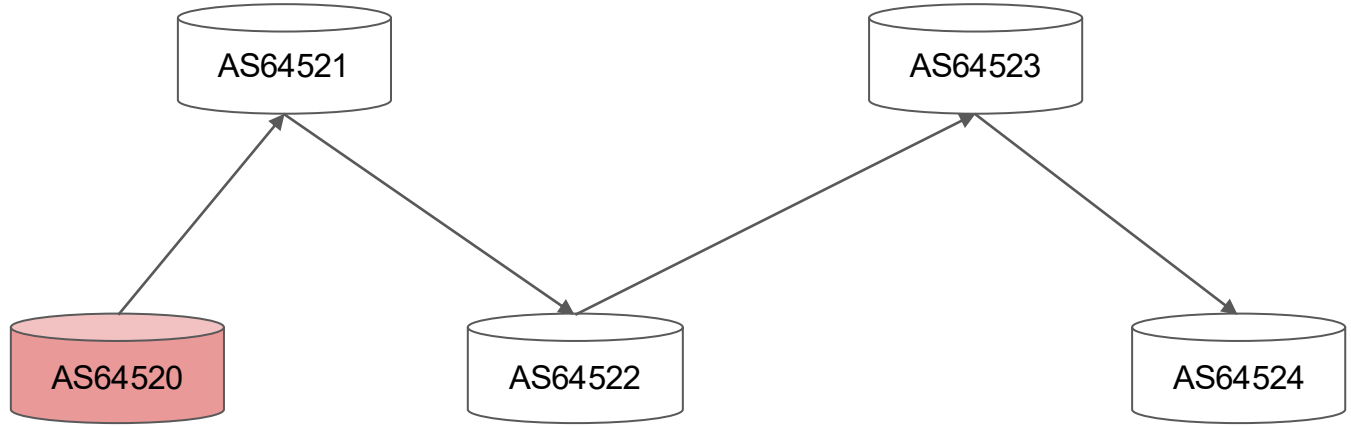


Concept of valley free routing...

Example of valley in routing

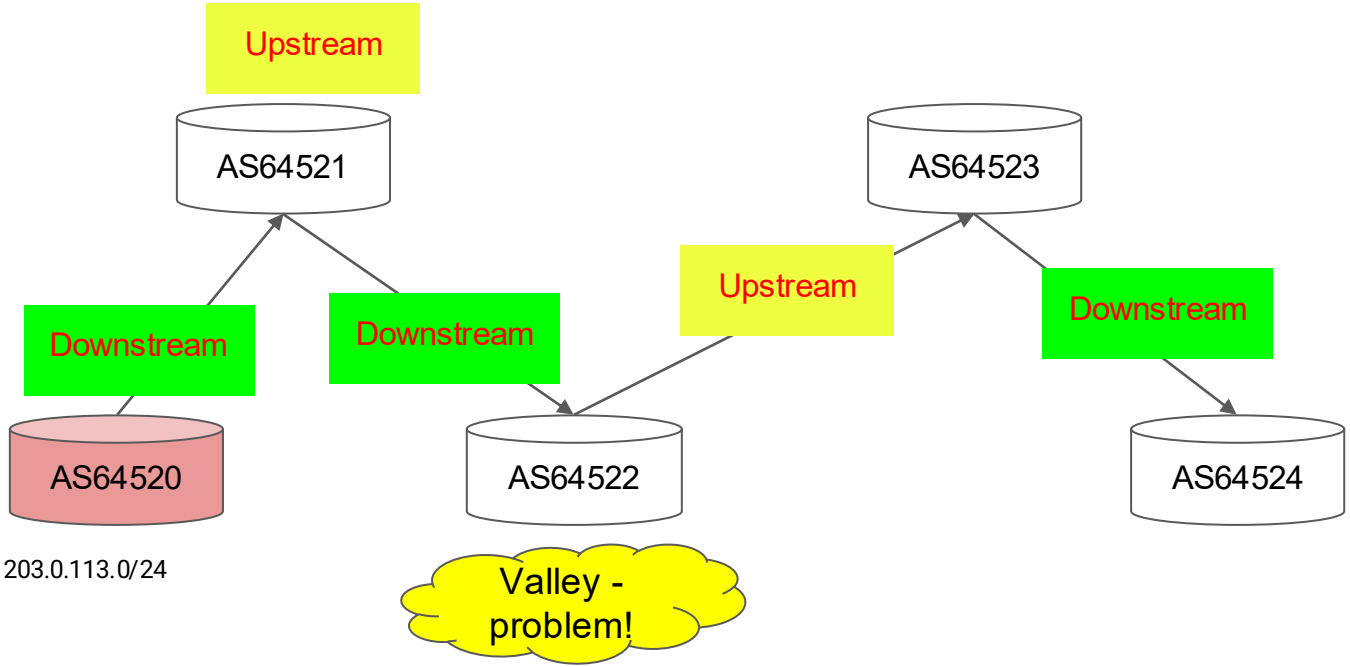
AS64524 table:

203.0.113.0/24
64523 64522 64521 64520



203.0.113.0/24

Example of valley in routing

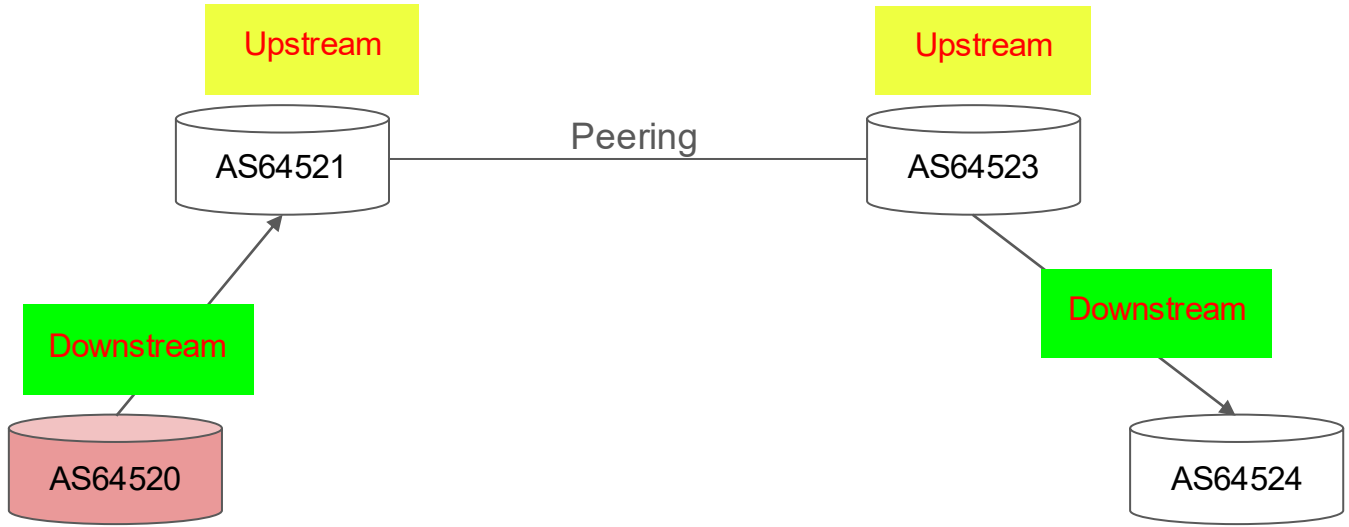


AS64524 table:

203.0.113.0/24
64523 64522 64521 64520

AS64521 does not have AS64522 as upstream (hence AS64522 is downstream) and if AS64522 marked AS64523 as upstream then it's a leak

Example of valley in routing



AS64524 table:

203.0.113.0/24
64523 64522 64521 64520

AS64520 -> AS64521 - Valid!

AS64521 -> AS64523 - No mention in ASPA object (peers)

AS64523 -> AS64524 - Valid!

No Valley - all good!

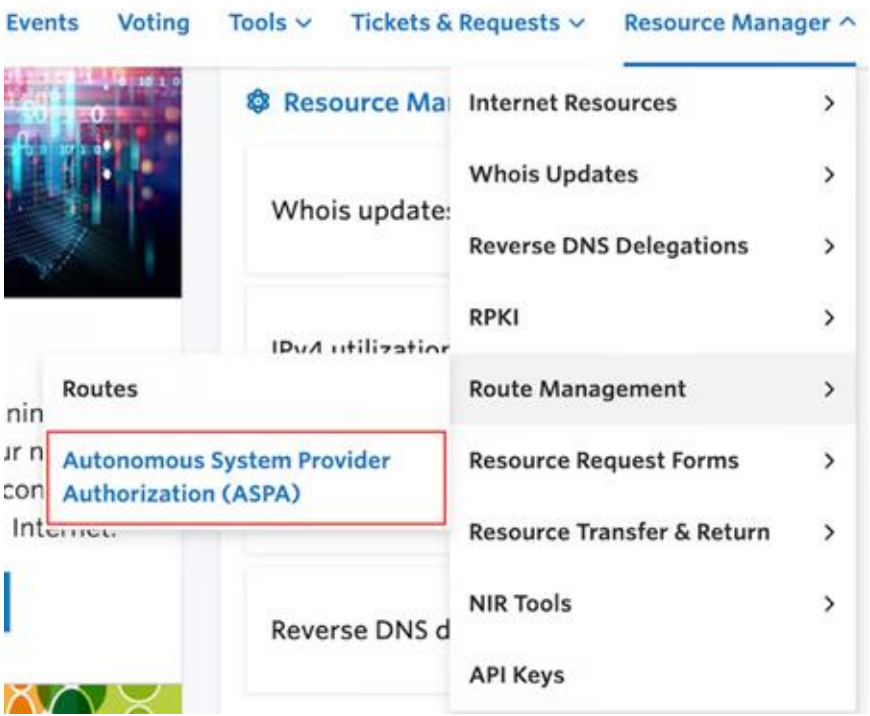
Presentation overview

1. How filtering is done presently
2. Introduction to ASPA
3. **Creating ASPA record**
4. Configuring ASPA for path validation
5. ASPA deployment at Hurricane Electric

How to create ASPA object?

- ASPA is part of RPKI and ASPA object can be created in same way as ROA on APNIC, ARIN & RIPE NCC
- APNIC launched ASPA support since 9th July 2026
- In RIR hosted model, ASPA is created at RIR via RIR interface and certificates are held in the RIR's infrastructure
- In delegated / self hosted model, ASPA is held in own infrastructure e.g on open source software like Krill

Creating ASPA record in APNIC



Source: https://help.apnic.net/s/article/ASPA

Presentation overview

1. How filtering is done presently
2. Introduction to ASPA
3. Creating ASPA record
4. **Configuring ASPA for path validation**
5. ASPA deployment at Hurricane Electric

Hardware support

- It is supported in BIRD 2.16
- IOS-XR - Cisco is running field trials since last year
- JunOS likely to support it by end of the year (~26.4)

How ASPA is configured for path validation?

- Routers supporting ASPA will be able to connect with RPKI validator like routinator over RTR
- Enable the ASPA validation
- Apply policy to reject “ASPA Invalid state” on the import policy

Routinator support

- Supported in latest version 0.15.1
- Enabled by --enable-aspa when bringing up or enable-aspa=true as static option in the config
- Gives output via RTR as well as json dump (alongside ROAs)

```
anurag@fmt01 ~> curl -s https://routinator.fmt.anuragbhatia.com/json | jq keys
[
  "aspas",
  "metadata",
  "roas"
]
anurag@fmt01 ~>
```

Presentation overview

1. How filtering is done presently
2. Introduction to ASPA
3. Creating ASPA record
4. Configuring ASPA for path validation
5. **ASPA deployment at Hurricane Electric**

ASPA deployment at Hurricane Electric AS6939 backbone

ASPA validation at Hurricane Electric / AS6939 backbone

- HE / AS6939 is doing ASPA validation across it’s backbone for downstreams and peers via our reactive system
- HE rejects routes where ASPA exists and upstream ASN is not matching the AS_PATH from the routing table
- Setup is integrated within existing reactive route filtering system

Hurricane Electric Route Filtering Algorithm

This is the route filtering algorithm for customers and peers that have explicit filtering:

1. Attempt to find an as-set to use for this network.

1.1 In peeringdb, for this ASN, check for an IRR as-set name.
Validate the as-set name by retrieving it. If it exists, use it.

1.2 In IRR, query for an aut-num for this ASN. If it exists, inspect the aut-num for this ASN to see if we can extract from their IRR policy an as-set for what they will announce to Hurricane by finding export or mp-export to AS6939, ANY, or AS-ANY.
Precedence is as follows: The first match is used, "export" is checked before "mp-export", and "export: to AS6939" is checked before "export: to ANY" or "export: to AS-ANY".
Validate the as-set name by retrieving it. If it exists, use it.

1.3 Check various internal lists maintained by Hurricane Electric's NOC that map ASNs to as-set names where we discovered or were told of them.
Validate the as-set name by retrieving it. If it exists, use it.

1.4 If no as-set name is found by the previous steps use the ASN.

2. Collect the received routes for all BGP sessions with this ASN. This details both accepted and filtered routes.

3. For each route, perform the following rejection tests:

3.1 Reject default routes 0.0.0.0/0 and ::/0.

3.2 Reject AS paths that use BGP AS_SET notation (i.e. {1} or {1 2}, etc). See RFC 9774 "Deprecation of AS_SET and AS_CONFED_SET in BGP".

3.3 Reject prefix lengths less than minimum and greater than maximum. For IPv4 this is 8 and 24. For IPv6 this is 16 and 48.

3.4 Reject bogons (RFC 1918, documentation prefix, etc).

3.5 Reject exchange prefixes for all exchanges Hurricane Electric is connected to.

3.6 Reject AS paths that exceed 50 hops in length. Excessive BGP AS Path Prepending is a Self-Inflicted Vulnerability.

3.7 Reject AS paths that use unallocated 32-bit ASNs between 1000000 and 4199999999. https://www.iana.org/assignments/as-numbers/as-numbers.xhtml

3.8 Reject AS paths that use unassigned 32-bit ASNs between 4200000000 and 4294967294. Reserved for Private Use by RFC 6996.

3.9 Reject AS paths that use AS 23456. AS 23456 should not be encountered in the AS paths of BGP speakers that support 32-bit ASNs.

3.10 Reject AS paths that use AS 0. As per RFC 7606, "A BGP speaker MUST NOT originate or propagate a route with an AS number of zero".

3.11 Reject routes that fail an ASPA (Autonomous System Provider Authorization) check for any hop of the path where a customer ASPA record exists and the provider ASN is not listed as a provider.

3.12 Reject routes that were learned via a route server and that contain a hop that is an ASN that has specified "Never via route servers" (peeringdb flag).

3.13 Reject routes that have RPKI status INVALID_ASN or INVALID_LENGTH based on the origin AS and prefix.

4. For each route, perform the following acceptance tests:

4.1 If the origin is the neighbor AS, accept routes that have RPKI status VALID based on the origin AS and prefix.

4.2 If the prefix is an announced downstream route that is a subnet of an accepted originated prefix that was accepted due to either RPKI or an RIR handle match, accept the prefix.

4.3 If RIR handles match for the prefix and the peer AS, accept the prefix.

4.4 If this prefix exactly matches a prefix allowed by the IRR policy of this peer, accept the prefix.

4.5 If the first AS in the path matches the peer and path is two hops long and the origin AS is in the expanded as-set for the peer AS and either the RPKI status is VALID or there is an RIR handle match for the origin AS and the prefix, accept the prefix.

5. Reject all prefixes not explicitly accepted

ASPA adoption coverage on bgp.he.net

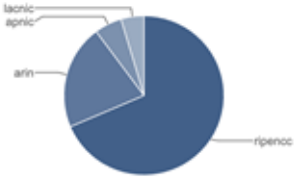
ASPA Adoption report - bgp.he.net/report/rpki_and_aspa

ASNs In Global Routing Table: 87,982

Routed ASNs Covered by ASPA: 2,216

Total ASPA Records: 2,483

ASPA Records By RIR



RIR	Count
ripencc	1,703
arin	527
apnic	138
lacnic	115

ASNs By RIR

RIR	With ASPA	Total	Coverage (%)
arin	458	20,488	2.24
ripencc	1,512	31,792	4.76
apnic	131	20,343	0.64
afrinic	0	2,126	0.00
lacnic	115	12,640	0.91

Limitations

- Has network effect: Useful when large number of networks do it and large number of AS_PATHs can be validated completely with no gaps
- Does not differ between mixed relation like if a network is “peer” in one continent, while transit in other
- No IPv4/IPv6 granularity: ASN is either provider or not a provider. No option to mark as provider only in IPv4 or IPv6.
- Both ASPA objects and validation has to happen to actually be effective. Similar to RoV situation in RPKI ROA.

Questions?

anurag@he.net