Securing Internet Routing:
The Puzzle Pieces (revisited)

Tashi Phuntsho

[NSRC & FLEXOPTIX]

Why BGP incidents?

Routing (still) works by RUMOUR

- TELL your neighbors what you know
- LEARN/accept what your neighbors know
- Assume everyone is *honest* (and correct)

Why BGP incidents?

NO one is in charge

- No single *authority* point for the Internet
- No *reference* point for what is *right* in routing

Routing is VARIABLE

- My view of the network depends on where I am
- No reference view to compare the local view against

Why BGP incidents?

We (still) don’t have the E(evil) bit

- RFC3514

Puzzle Pieces: RFC8212

BGP is permissive by default (RFC4271):

- What you learn/accept from one peer, (best path) is advertised to all other peers
- AS-to-AS leaks happen

RFC8212 changes this (`through code`):

- From default Allow/Permit to default Deny/Reject
- For all eBGP sessions: Without an explicit Import or Export policy, DO NOT use routes received from, or send routes to eBGP peers.

Note: Does not stop applying a Permit ALL policy

Puzzle Pieces: RFC8212

https://github.com/bgp/RFC8212 tracks implementations:

Default ON (COTS Vendors)	• IOS-XR • SR OS (>19.5.R1) • SR Linux (>19.11.R1)
Default ON (Routing daemons)	• BIRD (>2.0.1 • OpenBGPD (>6.4) • FRR (>7.4)
Configurable knobs	• EOS (4.18.0f) • IOS-XE (17.2.1) • Junos (20.3R1)

Puzzle Pieces: WHOIS

At the very least, verify the resource holder:

```
whois -h whois.apnic.net 202.144.128.0/19
whois -h whois.apnic.net 2405:d000::/32

whois -h whois.apnic.net AS17660
whois -h whois.apnic.net AS18024
```

```
inetnum:        202.144.128.0 - 202.144.159.255
netname:        BTTELECOM
descr:          DrukNet, Bhutan Telecom
descr:          Thimphu
country:        BT
org:            ORG-BTL2-AP
admin-c:        JT106-AP
tech-c:         JT106-AP
abuse-c:        AB1276-AP
status:         ALLOCATED PORTABLE
mnt-by:         APNIC-HM
mnt-lower:      MAINT-BT-DRUKNET
mnt-routes:     MAINT-BT-DRUKNET
mnt-irt:        IRT-BTTELECOM-BT
last-modified:  2020-10-20T01:02:25Z
source:         APNIC
```

```
inet6num:       2405:d000::/32
netname:        DRUKNET-BT-20080204
descr:          Bhutan Telecom Ltd
descr:          Internet Service Provider
country:        BT
org:            ORG-BTL2-AP
admin-c:        JT106-AP
tech-c:         JT106-AP
abuse-c:        AB1276-AP
status:         ALLOCATED PORTABLE
mnt-by:         APNIC-HM
mnt-lower:      MAINT-BT-DRUKNET
mnt-routes:     MAINT-BT-DRUKNET
mnt-irt:        IRT-BTTELECOM-BT
last-modified:  2021-01-14T06:16:00Z
source:         APNIC
```

```
aut-num:        AS17660
as-name:        DRUKNET-AS
descr:          DrukNet ISP
descr:          Bhutan Telecom
descr:          Thimphu
country:        BT
import:         from AS6461 action pref=100; accept ANY
export:         to AS6461 announce AS-DRUKNET-TRANSIT
import:         from AS2914 action pref=150; accept ANY
export:         to AS2914 announce AS-DRUKNET-TRANSIT
```

```
aut-num:        AS18024
as-name:        BTTELECOM-AS-AP
descr:          Bhutan Telecom Ltd
country:        BT
org:            ORG-BTL2-AP
admin-c:        DNO1-AP
tech-c:         DNO1-AP
abuse-c:        AB1276-AP
mnt-lower:      MAINT-BT-DRUKNET
mnt-routes:     MAINT-BT-DRUKNET
mnt-by:         APNIC-HM
mnt-irt:        IRT-BTTELECOM-BT
last-modified:  2021-01-14T06:16:00Z
source:         APNIC
```

Puzzle Pieces: IRR

Internet Routing Registry - IRR

- Where networks publish their routing intents
- ~ route/route6 objects

```
route:          202.144.128.0/19
descr:          DRUKNET-BLOCK
origin:         AS17660
mnt-by:         MAINT-BT-DRUKNET
last-modified:  2021-03-03T09:40:47Z
source:         APNIC
```

```
route6:         2405:d000::/32
descr:          DRUKNET-IPV6-BLOCK
origin:         AS17660
notify:         netops@bt.bt
mnt-by:         MAINT-BT-DRUKNET
last-modified:  2010-07-21T03:46:02Z
source:         APNIC
```

Puzzle Pieces: IRR

Can be used to build route filters:

- With RPSL tools (bgpq4)
- Accept (permit) if an entry exists in the IRR database

✓ Note the output diff when pointing to different sources

- bgpq4 defaults to rr.ntt.net

```
→ bgpq4 -6bl PEERv6-IN AS17660
PEERv6-IN = [
    2405:d000::/32,
    2405:d000:7000::/36
];

~
→ bgpq4 -S APNIC -6bl PEERv6-IN AS17660
PEERv6-IN = [
    2405:d000::/32,
    2405:d000:7000::/36
];
```

```
→ bgpq4 -Abl PEERv4-IN AS17660
PEERv4-IN = [
    45.64.248.0/22,
    103.245.240.0/22,
    103.245.242.0/23,
    119.2.96.0/19,
    163.227.12.0/23{23,24},
    163.227.18.0/23{23,24},
    163.227.20.0/22{23,24},
    163.227.24.0/21{23,24},
    202.144.128.0/19{19,20},
    202.144.128.0/23,
    202.144.148.0/22
];

~
→ bgpq4 -S APNIC -Abl PEERv4-IN AS17660
PEERv4-IN = [
    45.64.248.0/22,
    103.245.240.0/22,
    103.245.242.0/23,
    119.2.96.0/19,
    163.227.12.0/23{23,24},
    163.227.18.0/23{23,24},
    163.227.20.0/22{23,24},
    163.227.24.0/21{23,24},
    202.144.128.0/19
];
```

Puzzle Pieces: IRR

Sometimes, transit provider relationships (as-set) published too:

- To aggregate downstream networks, it maybe providing transit for

```
route:          X.1.2.0/24
origin:         AS18024

route6:         2001:db8:a::/48
origin:         AS18024
```

```
route:          X.1.3.0/24
origin:         AS18025

route6:         2001:db8:b::/48
origin:         AS18025
```

```
→ whois -h whois.apnic.net "AS-DRUKNET-TRANSIT"
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic

% Information related to 'AS-DRUKNET-TRANSIT'

as-set:         AS-DRUKNET-TRANSIT
descr:          DrukNet transit networks
members:        AS17660
members:        AS132232
members:        AS134715
members:        AS135666
members:        AS137925
members:        AS59219
members:        AS18024
members:        AS18025
members:        AS137994
members:        AS140695
members:        AS151498
members:        AS151955
members:        AS152317
members:        AS138558
members:        AS13335
members:        AS132894
members:        AS138529
members:        AS153779
members:        AS153740
admin-c:        DNO1-AP
tech-c:         DNO1-AP
notify:         netops@bt.bt
mnt-by:         MAINT-BT-DRUKNET
last-modified:  2025-06-09T11:07:14Z
source:         APNIC
```

Puzzle Pieces: IRR

AS-SET can be used to build:

- AS-PATH filters or route filters

bgpq4 -f 17660 -l BT-AS-IN AS-DRUKNET-TRANSIT

```
→ bgpq4 -f 17660 -l BT-AS-IN AS-DRUKNET-TRANSIT
no ip as-path access-list BT-AS-IN
ip as-path access-list BT-AS-IN permit ^17660(_17660)*$
ip as-path access-list BT-AS-IN permit ^17660(_[0-9]+)*_(13335|18024|18025|59219)$
ip as-path access-list BT-AS-IN permit ^17660(_[0-9]+)*_(132232|132894|134715|135666)$
ip as-path access-list BT-AS-IN permit ^17660(_[0-9]+)*_(137925|137994|138529|138558)$
ip as-path access-list BT-AS-IN permit ^17660(_[0-9]+)*_(140695|151498|151955|152317)$
ip as-path access-list BT-AS-IN permit ^17660(_[0-9]+)*_(153740|153779)$
```

bgpq4 -S APNIC -Al BTv4-IN AS-DRUKNET-TRANSIT

```
→ bgpq4 -S APNIC -Al BTv4-IN AS-DRUKNET-TRANSIT
no ip prefix-list BTv4-IN
ip prefix-list BTv4-IN permit 1.0.0.0/24
ip prefix-list BTv4-IN permit 1.1.1.0/24
ip prefix-list BTv4-IN permit 1.32.192.0/18
ip prefix-list BTv4-IN permit 27.124.0.0/18
ip prefix-list BTv4-IN permit 36.50.37.0/24
ip prefix-list BTv4-IN permit 43.226.16.0/21 ge 22 le 24
ip prefix-list BTv4-IN permit 43.226.124.0/22 le 24
ip prefix-list BTv4-IN permit 43.230.208.0/24
ip prefix-list BTv4-IN permit 43.240.36.0/22 le 24
ip prefix-list BTv4-IN permit 43.243.28.0/22 le 24
ip prefix-list BTv4-IN permit 43.243.68.0/22 le 24
ip prefix-list BTv4-IN permit 43.243.72.0/22 le 24
ip prefix-list BTv4-IN permit 43.243.108.0/22 le 24
ip prefix-list BTv4-IN permit 43.249.204.0/22 le 24
ip prefix-list BTv4-IN permit 45.64.52.0/22 le 24
ip prefix-list BTv4-IN permit 45.64.248.0/22
ip prefix-list BTv4-IN permit 45.64.248.0/23
ip prefix-list BTv4-IN permit 45.64.250.0/23 ge 24 le 24
```

bgpq4 -S APNIC -6Al BTv6-IN AS-DRUKNET-TRANSIT

```
→ bgpq4 -S APNIC -6Al BTv6-IN AS-DRUKNET-TRANSIT
no ipv6 prefix-list BTv6-IN
ipv6 prefix-list BTv6-IN permit 2001:df0:eb80::/48
ipv6 prefix-list BTv6-IN permit 2001:df2:a8c0::/48
ipv6 prefix-list BTv6-IN permit 2001:df3:e180::/48
ipv6 prefix-list BTv6-IN permit 2001:df4:3440::/48
ipv6 prefix-list BTv6-IN permit 2001:df5:a300::/48
ipv6 prefix-list BTv6-IN permit 2001:df5:acc0::/48
ipv6 prefix-list BTv6-IN permit 2400:1440::/32
ipv6 prefix-list BTv6-IN permit 2400:1c80::/32 le 40
ipv6 prefix-list BTv6-IN permit 2400:4e60::/32 le 33
```

AS-SET Problems

- Cannot verify the integrity and authenticity of member ASNs
- No limit to the number of member ASNs ~ bloated AS-SETs

Example: the AS-SET called `AS9498:AS-BHARTI-IN` expands

https://bgp.tools/as-set/as9498:as-bharti-in

- 69960 ASNs
- IPv4 prefixes: 1,946,190
- IPv6 prefixes: 1,147,378

CIDR report as of 03/07/2026:

- 78967 ASNs (IPv4) | 37002 ASNs (IPv6)
- IPv4 prefixes: 1,063,276
- IPv6 prefixes: 253,686

AS-SET Problems

Prevalence of non-hierarchical AS-SETs:

- Name collision

```
as-set:          AS-GEMNET
descr:           GEMNET s.r.o. ASes
members:         AS59479
members:         AS202733
tech-c:          DUMY-RIPE
admin-c:         DUMY-RIPE
mnt-by:          GEMNETCZ-MNT
created:         2013-08-19T09:49:13Z
last-modified:   2024-08-27T14:09:27Z
source:          RIPE
```

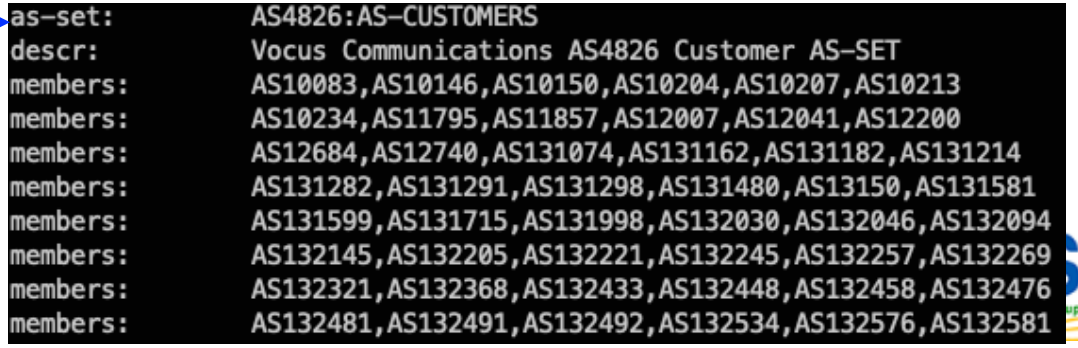


```
as-set:          AS-GEMNET
descr:           GEMNET LLC
country:         MN
members:         AS9934, AS9484, AS10219, AS9789,
                 AS38038, AS24496, AS24559, AS4850,
                 AS38042, AS38051, AS10076,
                 AS17882, AS38218, AS38454, AS38805,
                 AS38818, AS38273, AS10109, AS38869,
                 AS45237, AS45509, AS17463, AS24302,
                 AS45203, AS45204, AS45923, AS24320,
                 AS24496, AS45237, AS55342, AS55805,
                 AS55801, AS55408, AS55882, AS56194,
                 AS58598, AS58625, AS133177, AS135136,
                 AS138907, AS134074, AS45204:AS-GEMNET
tech-c:          GA263-AP
admin-c:         GA263-AP
mnt-by:          MAINT-GEMNET-MN
mnt-lower:       MAINT-GEMNET-MN
last-modified:   2024-10-08T02:49:37Z
source:          APNIC
```

Adopt hierarchical AS-SET:

- RFC2622 defines `[AS#]:AS-[as-set-name]`

```
as-set:          AS4826:AS-VOCUS
descr:           Vocus Communications AS4826 AS-SET
members:         AS4826, AS4826:AS-CUSTOMERS
admin-c:         VPL1-AP
tech-c:          VPL1-AP
remarks:         For queries please email the below contacts
remarks:         NOC - noc@vocus.net
remarks:         IRR Data - irr@vocus.com.au
remarks:         Peering enquiries - peering@vocus.com.au
notify:          irr@vocus.com.au
mnt-by:          MAINT-AU-VOCUS
last-modified:   2022-05-29T00:28:23Z
source:          APNIC
```



```
as-set:          AS4826:AS-CUSTOMERS
descr:           Vocus Communications AS4826 Customer AS-SET
members:         AS10083,AS10146,AS10150,AS10204,AS10207,AS10213
members:         AS10234,AS11795,AS11857,AS12007,AS12041,AS12200
members:         AS12684,AS12740,AS131074,AS131162,AS131182,AS131214
members:         AS131282,AS131291,AS131298,AS131480,AS13150,AS131581
members:         AS131599,AS131715,AS131998,AS132030,AS132046,AS132094
members:         AS132145,AS132205,AS132221,AS132245,AS132257,AS132269
members:         AS132321,AS132368,AS132433,AS132448,AS132458,AS132476
members:         AS132481,AS132491,AS132492,AS132534,AS132576,AS132581
```

AS-SET Transition

1. Create a new hierarchical AS-SET
   - `AS199121:AS-FLEXOPTIX` (ensure same members as old one)
2. Add the new AS-SET as member of the old one
   - Add the new AS-SET as member of the old one
     - » `AS-FLEXOPTIX [members: AS199121:AS-FLEXOPTIX]`
   - From here on, only update your new AS-SET
3. Inform your peers & update PeeringDB
   - Ask your peers / providers to use your new AS-SET
4. Then delete the old AS-SET

Puzzle Pieces: BGP Roles (RFC9234)

Defines a ROLE for your local AS with respect to your BGP neighbors:

- Roles:
  - Provider: I provide transit to my neighbor
  - Customer: I am customer of my neighbor
  - Peer: We are peers
  - RS: I am a route server
  - RS-client: I am a client to a RS
- Allowed relationships:
  - Provider <> Customer
  - Customer <> Provider
  - Peer <> Peer
  - RS <> RS-client
  - RS-client <> RS

Puzzle Pieces: BGP Roles (RFC9234)

Role capability negotiated through BGP open message

- Loose vs Strict

```
set protocols bgp group TRANSIT description 'My Transit Providers'
set protocols bgp group TRANSIT otc-local-role customer
set protocols bgp group TRANSIT neighbor 172.16.200.101 peer-as 64501
```

Configuring roles: Junos (>25.2R1)

```
router bgp 64522
 neighbor 172.16.200.101 remote-as 64501
 neighbor 172.16.200.101 description 'Transit from ISP-A'
 neighbor 172.16.200.101 local-role customer
```

Configuring roles: FRR

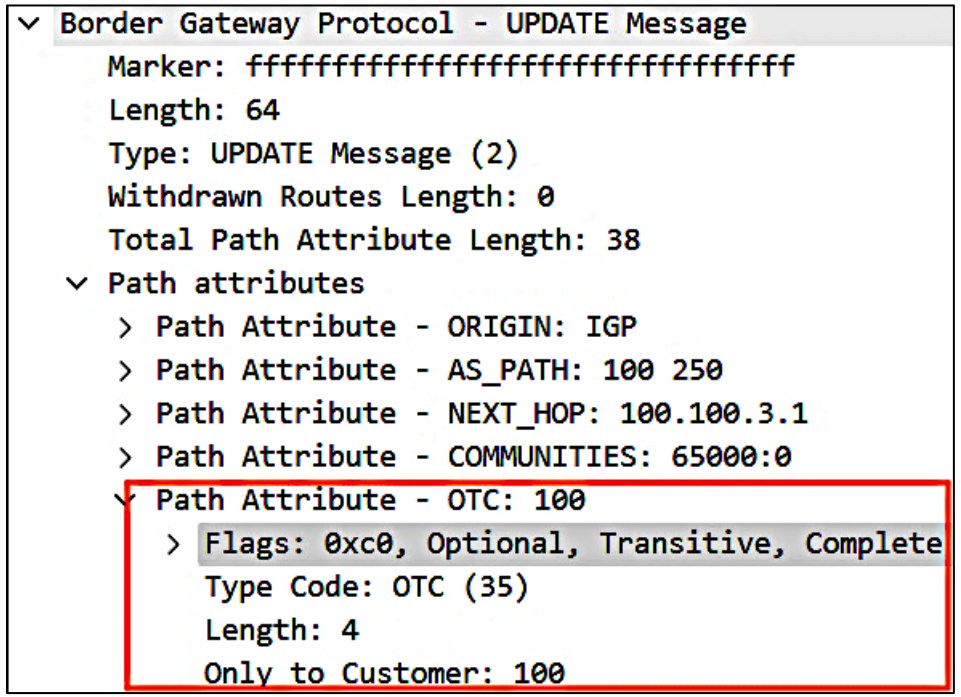
Puzzle Pieces: BGP Roles (RFC9234)

If role capability negotiated successfully:

- OTC (Only-to-Customer) attribute is exchanged
- User only sets the role; OTC works in code (no config needed ☺)
- Protects without need for explicit policy

OTC setting:

- Outbound marking:
  - If a route is sent to Customer, Peer, RS-client set OTC attribute (*ASN of the sender*)
- Inbound marking:
  - If route is received from Provider, Peer, RS and OTC not set, mark with OTC attribute.



Puzzle Pieces: BGP Roles (RFC9234)

OTC Check:

- Outbound check (before marking)
  - A route with OTC attribute MUST NOT be sent to Provider, Peer, RS
- Inbound check (before marking)
  - If route with OTC is received from Customer or RS-client, it is a route leak. Discard!
  - If a route with OTC received from a Peer, and its value is != to the peer ASN, it is a leak. Discard!

Puzzle Pieces: RPKI [Origin Validation]

ROA – Route Origin Authorization

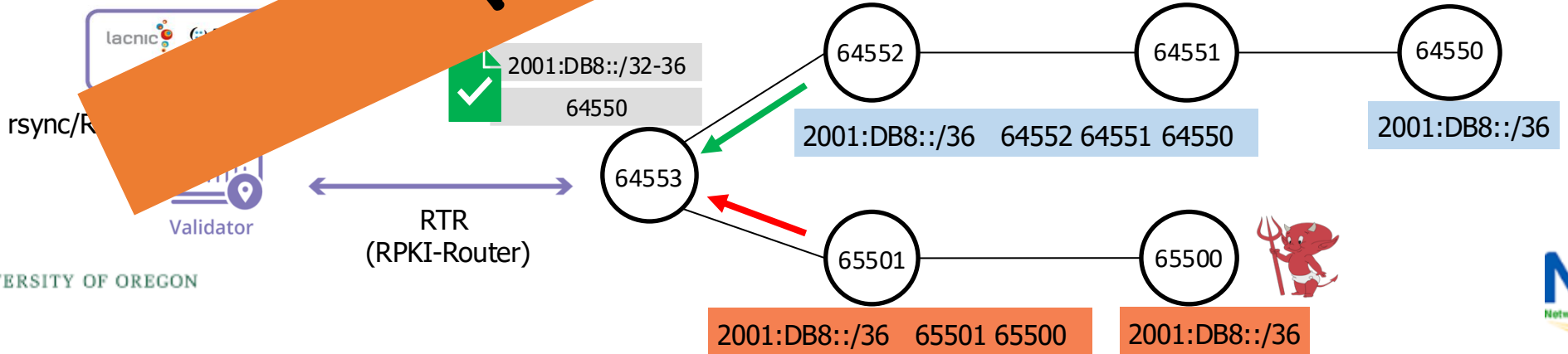
- Digitally signed ~ binds prefixes and nominated ASN
- Can be verified crypto-magically

Prefix	/32
M	/36
	AS64550

ROV – Route Origin Validation

- Helps validate if an ASN is perm… a route
- Mis-origination / origin h…

We all know this!



Puzzle Pieces: RPKI [Origin Validation]

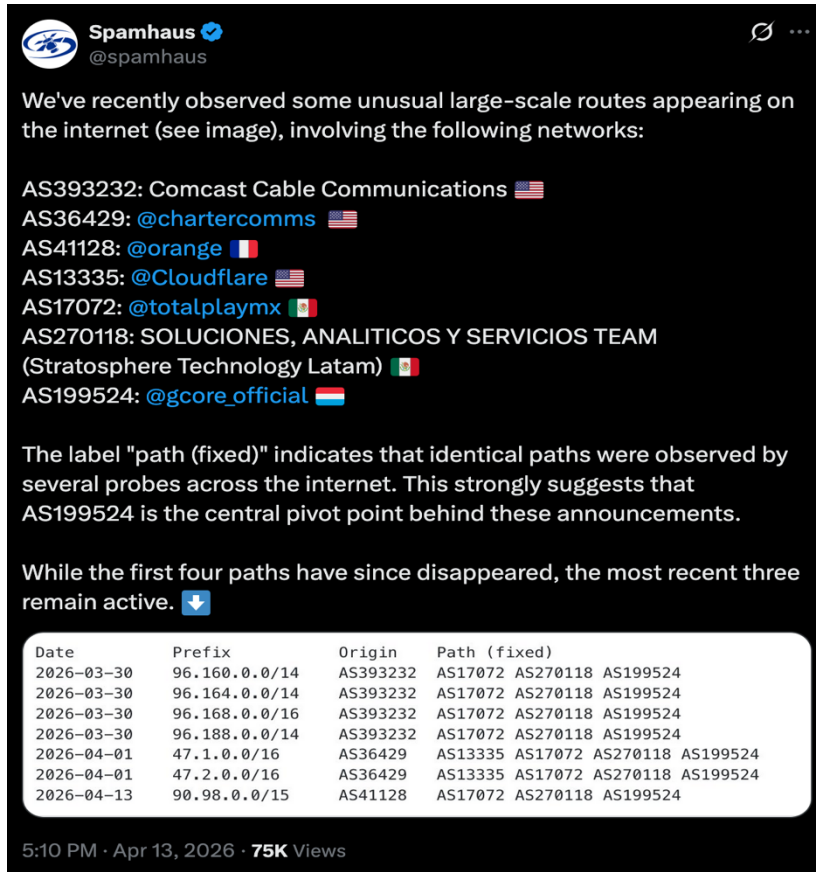
ROA Best Practices

- Minimal ROA (RFC9319):
  - ROA should only cover prefixes announced in BGP ~ use maxLength judiciously
- Multi ASN networks
  - More specific ROAs: Access ASNs
  - Aggregates and sub-aggregates: Transit ASN
- AS0 origin (RFC7607)
  - For unused/undelegated address space
  - (refer April 2026 Orange 90.98.0.0/15 hijack)

Puzzle Pieces: BGP “enforce-first-as”

During the April 2026 routing incident:

- AS0 ROA and/or ASPA would have detected the forged AS_PATH
- But also revealed lack of best practices ~ first AS check/enforcement by AS199524



Spamhaus
@spamhaus

We've recently observed some unusual large-scale routes appearing on the internet (see image), involving the following networks:

AS393232: Comcast Cable Communications
AS36429: @chartercomms
AS41128: @orange
AS13335: @Cloudflare
AS17072: @totalplaymx
AS270118: SOLUCIONES, ANALITICOS Y SERVICIOS TEAM (Stratosphere Technology Latam)
AS199524: @gcore_official

The label "path (fixed)" indicates that identical paths were observed by several probes across the internet. This strongly suggests that AS199524 is the central pivot point behind these announcements.

While the first four paths have since disappeared, the most recent three remain active.

Date	Prefix	Origin	Path (fixed)
2026-03-30	96.160.0.0/14	AS393232	AS17072 AS270118 AS199524
2026-03-30	96.164.0.0/14	AS393232	AS17072 AS270118 AS199524
2026-03-30	96.168.0.0/16	AS393232	AS17072 AS270118 AS199524
2026-03-30	96.188.0.0/14	AS393232	AS17072 AS270118 AS199524
2026-04-01	47.1.0.0/16	AS36429	AS13335 AS17072 AS270118 AS199524
2026-04-01	47.2.0.0/16	AS36429	AS13335 AS17072 AS270118 AS199524
2026-04-13	90.98.0.0/15	AS41128	AS17072 AS270118 AS199524

5:10 PM · Apr 13, 2026 · **75K** Views

Rekhter, et al. Standards Track [Page 33]

RFC 4271 BGP-4 January 2006

If the UPDATE message is received from an external peer, the local system MAY check whether the leftmost (with respect to the position of octets in the protocol message) AS in the AS_PATH attribute is equal to the autonomous system number of the peer that sent the message. If the check determines this is not the case, the Error Subcode MUST be set to Malformed AS_PATH.

RFC 7606 Revised Error Handling for BGP August 2015

o It has a Path Segment Length field of zero.

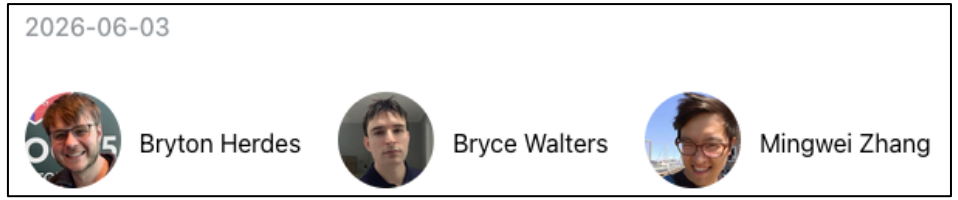
An UPDATE message with a malformed AS_PATH attribute SHALL be handled using the approach of "treat-as-withdraw".

[RFC4271] also says that an implementation optionally "MAY check whether the leftmost ... AS in the AS_PATH attribute is equal to the autonomous system number of the peer that sent the message". A BGP implementation SHOULD also handle routes that violate this check using "treat-as-withdraw" but MAY follow the "session reset" behavior if configured to do so.

Routes to be removed from Adj-RIB-In

Puzzle Pieces: BGP “enforce-first-as”

https://blog.cloudflare.com/enforce-first-as-bgp/ revealed:



Networks:

- Enforce ‘first AS’ check:
  - `AS174 | AS1299 | AS3257 | AS3491 | AS5511 | AS6453 | AS7018`
- Did NOT enforce:
  - `AS701 | AS2914 | AS3356 | AS6461 | AS6762 | AS6830 | AS12956`

Vendors:

- `JunOS | SR OS | RouterOS | SLX-OS | BIRD` did NOT enforce ‘first AS’ check by default!
- available as configuration knobs (except `RouterOS`)

Puzzle Pieces: RPKI [Path Validation]

Forged origin ASN will pass the ROV test

- Need to secure/validate the PATH too!

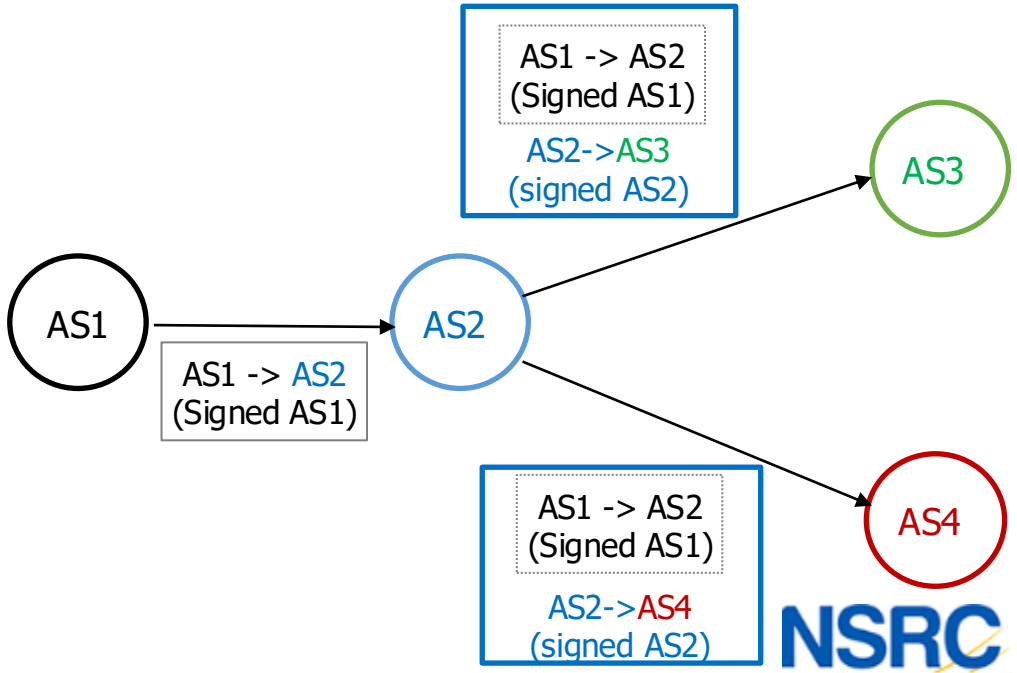
One idea was RFC8205 (BGPsec) → The future of AS path validation!

Forward Path Signing

1. AS1 signs message to AS2
2. AS2 signs message to AS3/AS4, encapsulating AS1's message

Validation

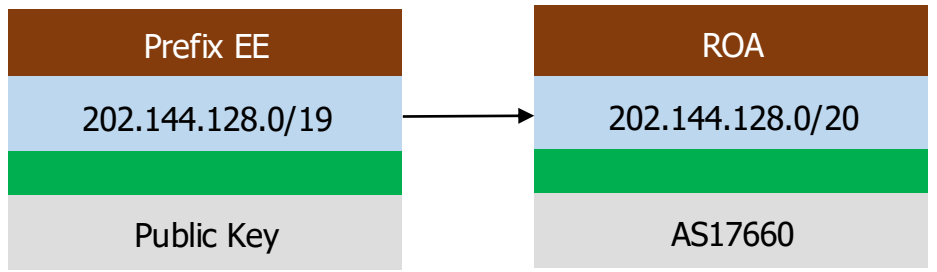
1. ROA check for the received prefix (if valid, go to 2)
2. Validate AS_PATH against the chain of signatures (for each AS in the path)



RFC8205 (BGPsec) Challenges

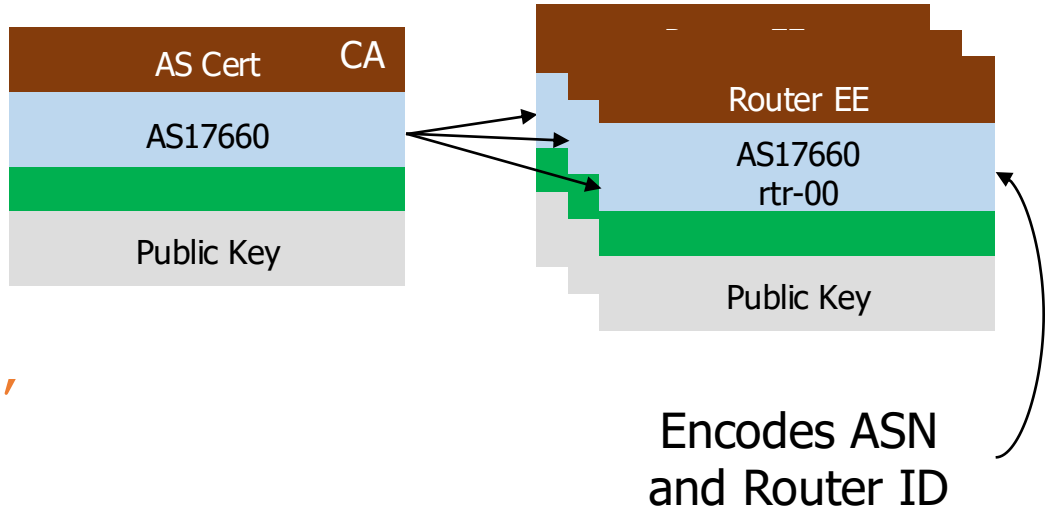
Cannot jump across non-BGPsec routers (networks)

- Traditional BGP: no BGPsec `update` messages



Complex crypto on the router

- CPU heavy ~ validate chain of signatures
- Memory heavy
  - Per-prefix BGP update
  - New attributes to carry `signatures, certs, key IDs` for every AS in the AS_PATH
- Current HW tech does not support BGPsec!



Puzzle Pieces: RPKI [Path Validation]

ASPA – Autonomous System Provider Authorization

- Binds a set of Provider ASNs to a Customer ASN
  - signed by the holder of the Customer ASN
- (Re)uses existing tool chains - No crypto on routers!

```
tashi@Toebs ~
➜ monocle rpki aspas --customer 55722 --format markdown
Data source: Cloudflare (cached at 2026-07-03 05:07:16 UTC, 2252 ASPAs)
Found 1 ASPAs
| Customer ASN | Customer Name | Country | Providers   |
|--------------|---------------|---------|-------------|
| AS55722      | CENPAC-AS-AP  | NR      | 7131, 14593 |
```

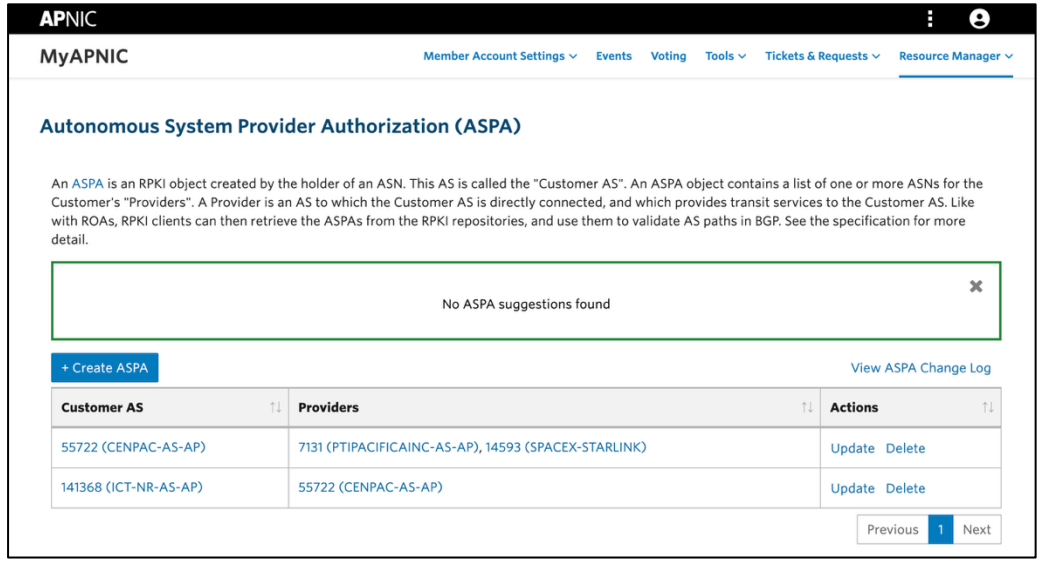
```
tashi@Toebs ~
➜ monocle rpki aspas --customer 1299 --format markdown
Data source: Cloudflare (cached at 2026-07-03 05:07:16 UTC, 2252 ASPAs)
Found 1 ASPAs
| Customer ASN | Customer Name        | Country | Providers |
|--------------|----------------------|---------|-----------|
| AS1299       | f/k/a Telia Carrier  | SE      | 0         |
```

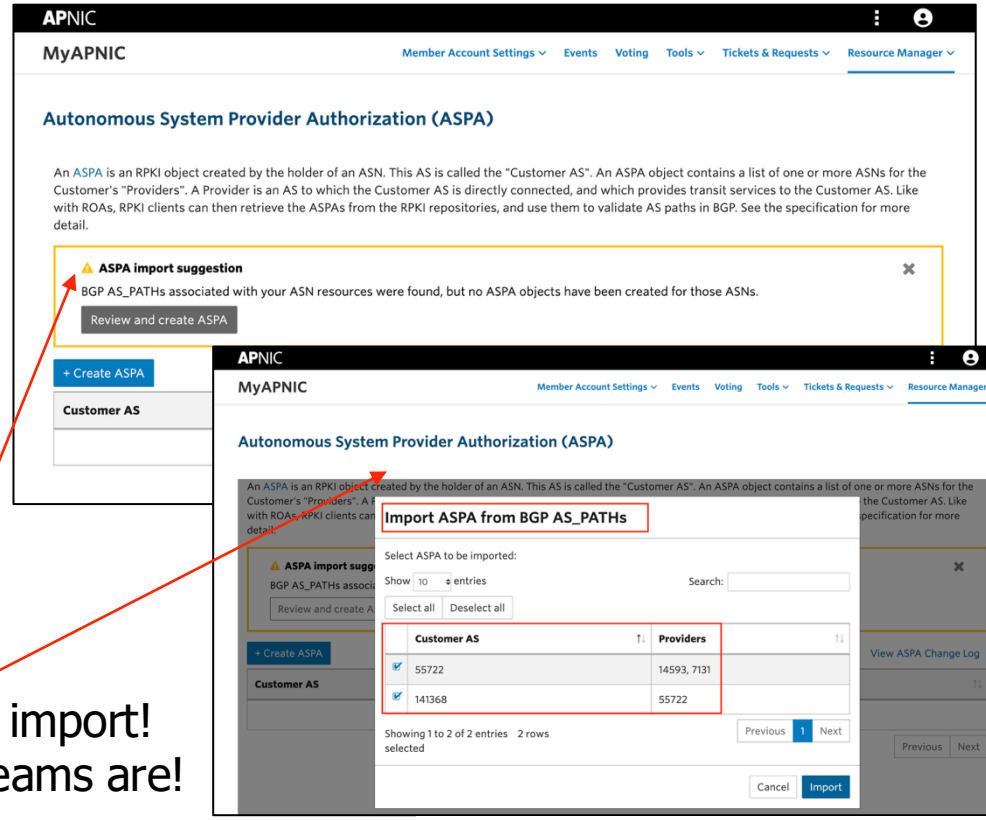
AS0 ASPA is special!

Puzzle Pieces: ASPA

APNIC ASPA Signer/Dashboard ready end of June 2026

- Shout out to Tom Harrison and the Registry team @APNIC





Be careful:

- Verify what is seen in BGP before import!
- You should know who your upstreams are!

Screenshot Credit: Dr.Philip Smith

Puzzle Pieces: ASPA

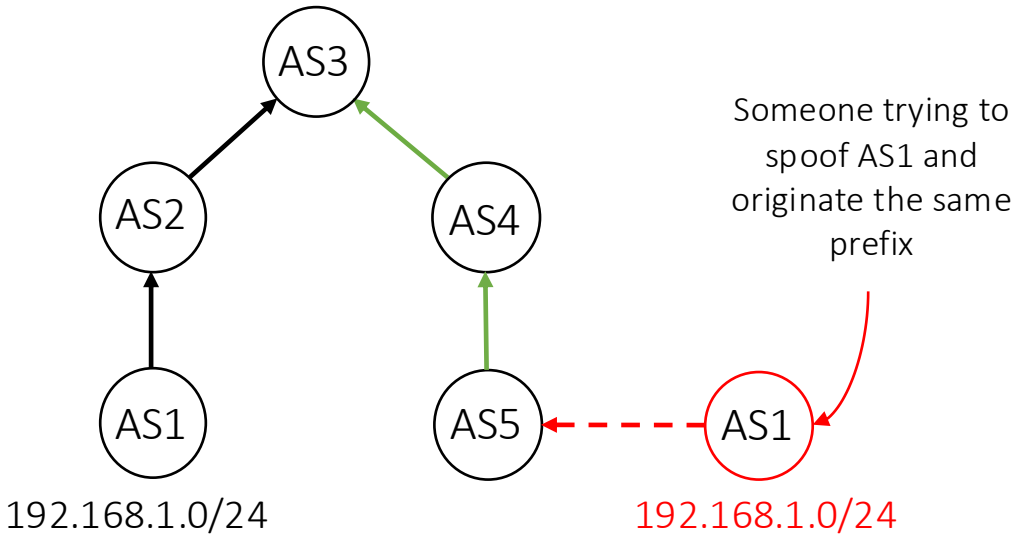
AS-to-AS hop verification (Upstream: Customer to Provider)

At each hop, look at the customer AS, check if the next AS is listed as one of its providers in the ASPA data

- If every hop in the path lines up, path is VALID (Provider)
- If any hop contradicts ASPA data (a customer AS says "this AS is not my provider"), path is INVALID
- If for one or more hops in the path, there is no ASPA data – it is Unknown (No Attestation)

Puzzle Pieces: ASPA

ASPA: spoofed origin AS



https://github.com/APNIC-net/rpki-rtr-demo

- AS1, announce 192.168.1.0/24
- ASPA:

```
AS1 > [AS2]
AS2 > [AS3]
AS3 > [AS0]
AS4 > [AS3]
```

- AS4 sees:

```
          5 1   192.168.1.0/24
      3 2 1     192.168.1.0/24
```

- AS4 knows
  - AS5 is 'Not Provider' for AS1
- Hence, INVALID

Puzzle Pieces: ASPA

ASPA can find valleys (detect leaks):

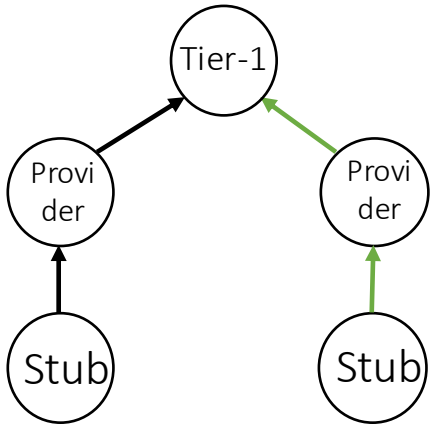
Take the longest possible:

- Customer to Provider path from the origin as UP ramp
- Provider to Customer on the reverse end as DOWN ramp

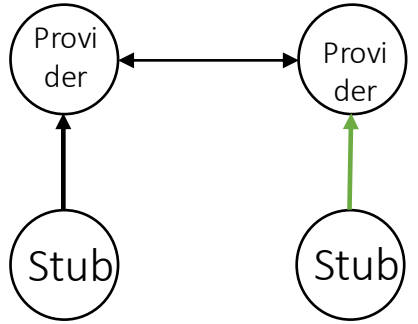
UP and DOWN must either:

- Meet at adjacent peers
- Meet at a shared provider
- Overlap with multiple hops

A gap in the UP and DOWN indicates there is a valley - Invalid



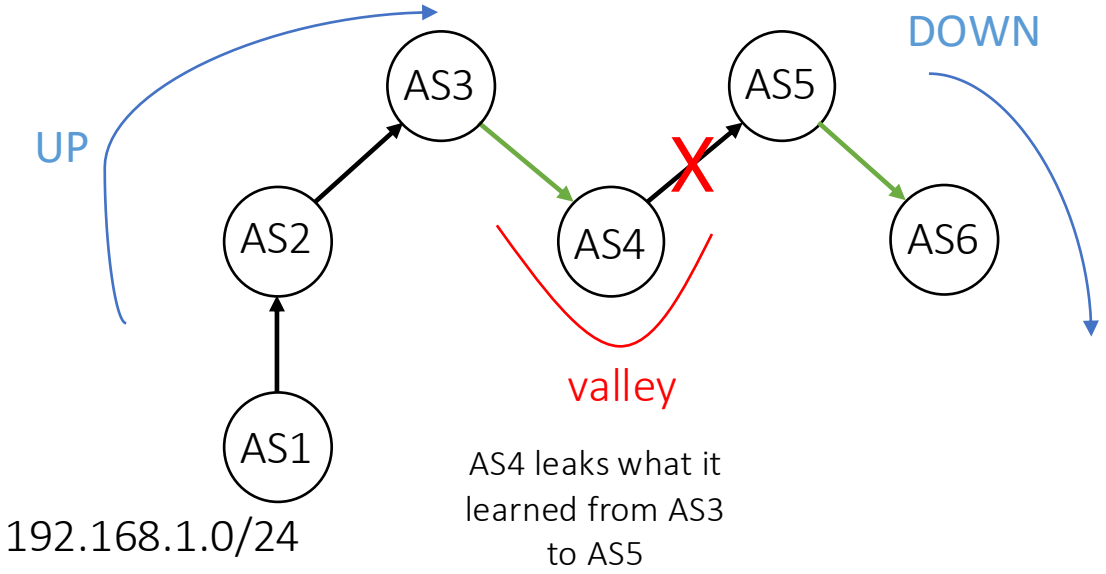
192.168.1.0/24



192.168.1.0/24

Puzzle Pieces: ASPA

ASPA: Provide to Provider leak



https://github.com/APNIC-net/rpki-rtr-demo

- AS1, announce 192.168.1.0/24
- ASPA:

```
AS1 > [AS2]
AS2 > [AS3]
AS4 > [AS3,AS5] - two upstreams
AS6 > [AS5]
AS3 > [AS0] and AS5 > [AS0]
```

- AS6 sees: `5 4 3 2 1  192.168.1.0/24`
  - ASPA says: AS4 is 'Not Provider' for AS3
    - `UP: 3 2 1 (from origin) - 2 hops`
  - ASPA says: AS4 is 'Not Provider' for AS5
    - `DOWN: 6 5 (AS6 verifying) - 1 hop`
  - There is a gap (UP/DOWN don't cover the full AS_PATH)
- AS4 is a valley → INVALID

ASPA Timeline

Standards	Still in draft/discussion: ratification by end of 2026? - RTRv2 - ASPA
Signers	Support: - ARIN - RIPE - APNIC (as of 25th June 2026) – shout out to Tom H and team @ APNIC! TBC: LACNIC, AfriNIC

Relying Party	Known Support: - Routinator (RP + RTR) - rpkiclient (RP) - RTRTR (RTR proxy/server) - FORT - Krill (delegated CA)
COTS BGP Speakers	- Huawei: NetEngine? - Nokia: SROS R27 ~ 2027 - JunOS: 26.4 (end of 2026) - Cisco: IOS-XR 27.1? - Arista?
Routing Daemons	- OpenBGPD (>7.8)

Questions?