Securing the Internet Routing:
The Puzzle Pieces (revisited)

Tashi Phuntsho

[NSRC/FLEXOPTIX]

tashi@nsrc.org | tashi@flexoptix.net

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):

- Without a policy, eBGP permits routes to be accepted and advertised
- 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 (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:          1.1.1.0/24
origin:         AS13335
descr:          APNIC Research and Development
                6 Cordelia St
mnt-by:         MAINT-APNICRANDNET
last-modified:  2023-04-26T02:42:44Z
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

```
→ bgpq4 -bAl PEERv4-IN AS4608
PEERv4-IN = [
    103.246.136.0/22,
    110.76.136.0/22,
    202.12.29.0/24,
    203.30.127.0/24,
    203.119.76.0/23,
    203.119.92.0/23,
    203.119.92.0/24,
    203.119.96.0/20,
    203.119.100.0/22,
    203.119.104.0/21,
    203.133.248.0/23,
    203.133.248.0/24
];
```

```
→ bgpq4 -6bAl PEERv6-IN AS4608
PEERv6-IN = [
    2001:dc0:2000::/35,
    2001:dc0:4000::/34{35,35},
    2001:dc0:8000::/34{35,35},
    2001:dc0:e000::/35,
    2001:dd8:8::/45,
    2001:dd8:8::/46{48,48},
    2001:dd8:c::/47{48,48},
    2001:dd8:f::/48,
    2001:df0:90::/48,
    2001:df2:ee00::/47{47,48},
    2401:2000::/32,
    2401:2000:6000::/35,
    2408:2000::/24
];
```

✓ Note the output diff when pointing to different sources

- bgpq4 defaults to rr.ntt.net

```
→ bgpq4 -S APNIC -bAl PEERv4-IN AS4608
PEERv4-IN = [
    202.12.29.0/24,
    203.119.76.0/23,
    203.119.100.0/22,
    203.119.104.0/21,
    203.133.248.0/23,
    203.133.248.0/24
];
```

```
→ bgpq4 -S APNIC -6bAl PEERv6-IN AS4608
PEERv6-IN = [
    2001:dc0:2000::/35,
    2001:dc0:4000::/34{35,35},
    2001:dc0:8000::/34{35,35},
    2001:dc0:e000::/35,
    2001:dd8:8::/46{48,48},
    2001:dd8:c::/47{48,48},
    2001:dd8:f::/48,
    2001:df0:90::/48,
    2401:2000::/32,
    2401:2000:6000::/35,
    2408:2000::/24
];
```

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
```

```
as-set:         AS17660:AS-DRUKNET
descr:          Druknet Internal & Transit Customers
tech-c:         DNO1-AP
admin-c:        DNO1-AP
mnt-by:         MAINT-BT-DRUKNET
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
members:        AS152480
members:        AS141680
members:        AS151782
notify:         netops@bt.bt
last-modified:  2026-08-06T08:56:47Z
source:         APNIC
```

Puzzle Pieces: IRR

AS-SET can be used to build:

- AS-PATH filters / prefix filters

bgpq4 -Xf 17660 -l BT-AS-IN AS17660:AS-DRUKNET

```
→ bgpq4 -Xf 17660 -l BT-IN AS17660:AS-DRUKNET
as-path-set BT-IN
  ios-regex '^17660(_17660)*$',
  ios-regex '^17660(_[0-9]+)*_(13335|18024|18025|59219|132232|132894)$',
  ios-regex '^17660(_[0-9]+)*_(134715|135666|137925|137994|138529|138558)$',
  ios-regex '^17660(_[0-9]+)*_(140695|141680|151498|151782|151955|152317)$',
  ios-regex '^17660(_[0-9]+)*_(152480|153740|153779)$'
end-set
```

bgpq4 -S APNIC -XAl BTv4-IN AS17660:AS-DRUKNET

```
→ bgpq4 -S APNIC -XAl BTv4-IN AS17660:AS-DRUKNET
no prefix-set BTv4-IN
prefix-set BTv4-IN
 1.0.0.0/24,
 1.1.1.0/24,
 1.32.192.0/18,
 27.124.0.0/18,
 36.50.37.0/24,
 42.61.47.0/24,
 43.226.16.0/21 ge 22 le 24,
 43.226.124.0/22 le 24,
 43.228.232.0/23 ge 24 le 24,
```

bgpq4 -S APNIC -6XAl BTv6-IN AS17660:AS-DRUKNET

```
→ bgpq4 -S APNIC -6XAl BTv6-IN AS17660:AS-DRUKNET
no prefix-set BTv6-IN
prefix-set BTv6-IN
 2001:df0:eb80::/48,
 2001:df2:a8c0::/48,
 2001:df3:e180::/48,
 2001:df4:3440::/48,
 2001:df5:a300::/48,
 2001:df5:acc0::/48,
 2001:df5:d880::/47 le 48,
```

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 **`AS-CAIS`** (source: RADB) expands to:

https://bgp.tools/as-set/as-cais

- 89,446 ASNs
- IPv4 prefixes: 2,162,073
- IPv6 prefixes: 1,286,167

CIDR report as of 17th Oct 2026:

- 79,662 ASNs
- IPv4 prefixes: 1,086,175
- IPv6 prefixes: 259,094

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:          OK3789-RIPE
admin-c:         OK3789-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
```

Non-hierarchical AS-SET: Hong Kong

Only looking at few networks I know:

```
AS-CAIS (PCCW Global)
AS-HKBN (RADB | NTT IRR)
AS9231:AS-CUSTOMERS
```

The next slide should help transition ☺

AS-SET Transition

1. Create a new hierarchical AS-SET

   `AS45204:AS-GEMNET` (same members as old one!)

2. Add the new AS-SET as member of the old one

   `AS-GEMNET [members: AS45204:AS-GEMNET]`

   – 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

```
as-set:          AS45204:AS-GEMNET
descr:           as set for GEMNET LLC
country:         MN
members:         AS9934,AS9484,AS10219,AS9789,AS38038,AS56301
members:         AS24496,AS24559,AS4850,AS38042,AS38051
members:         AS10076,AS17882,AS38218,AS38454,AS38805,AS38818
members:         AS38273,AS10109,AS38869,AS45237,AS45509,AS17463
members:         AS24302,AS45203,AS45204,AS131199,AS45923,AS55342
members:         AS24320,AS55805,AS55801,AS55408,AS55882,AS56194
members:         AS56293,AS58439,AS58598,AS58625,AS133177,AS58726
members:         AS58406,AS59354,AS133453,AS63962,AS134074,AS134241
members:         AS135033,AS135136,AS131240,AS18172,AS136254,AS136936
members:         AS137261,AS137511,AS56038,AS13335,AS137982,AS133050,
members:         AS139579,AS134356,AS141681,AS152337,AS152692,AS15163
tech-c:          GA263-AP
admin-c:         GA263-AP
mnt-lower:       MAINT-GEMNET-MN
mnt-by:          MAINT-GEMNET-MN
last-modified:   2026-05-28T07:57:52Z
source:          APNIC
```

```
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
```

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

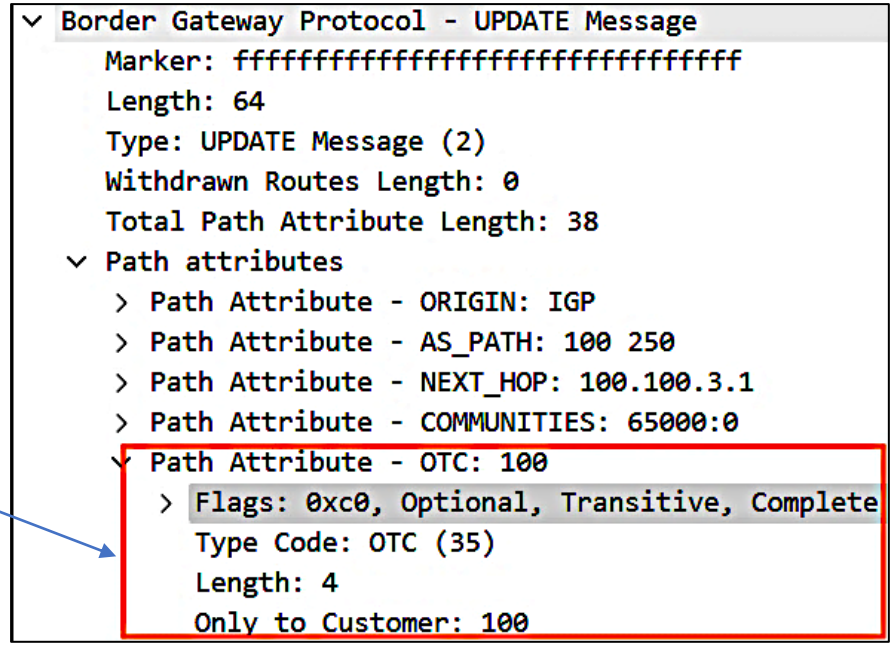
Puzzle Pieces: BGP Roles (RFC9234)

If role capability negotiated successfully:

- OTC (Only-to-Customer) attribute is exchanged
- User only sets the role: OTC works in code
- no OTC policy config needed ☺

OTC setting:

- Announcing
  - If a route is sent to Customer, Peer, RS-client set OTC attribute (ASN of the sender)
- Receiving:
  - If route is received from Provider, Peer, or an RS and OTC not set, mark with OTC attribute



Puzzle Pieces: BGP Roles (RFC9234)

OTC Check:

- Outbound
  - A route with OTC attribute MUST NOT be sent to Provider, Peer, RS
- Inbound
  - 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, with a value other than its own ASN, it is a leak. Discard!

Puzzle Pieces: BGP Roles (RFC9234)

https://blog.cloudflare.com/rfc9234-bgp-role-model/

- Supported
  - JunOS | Router OS | BIRD | OpenBGPD | FRR
- Announced
  - IOS XR (in release 26.4.1)
- Not supported
  - Arista EOS | SR OS | Huawei | SLX-OS | ArcOS | GoBGP | ExaBGP

Puzzle Pieces: RPKI [Origin Validation]

ROA – Route Origin Authorization

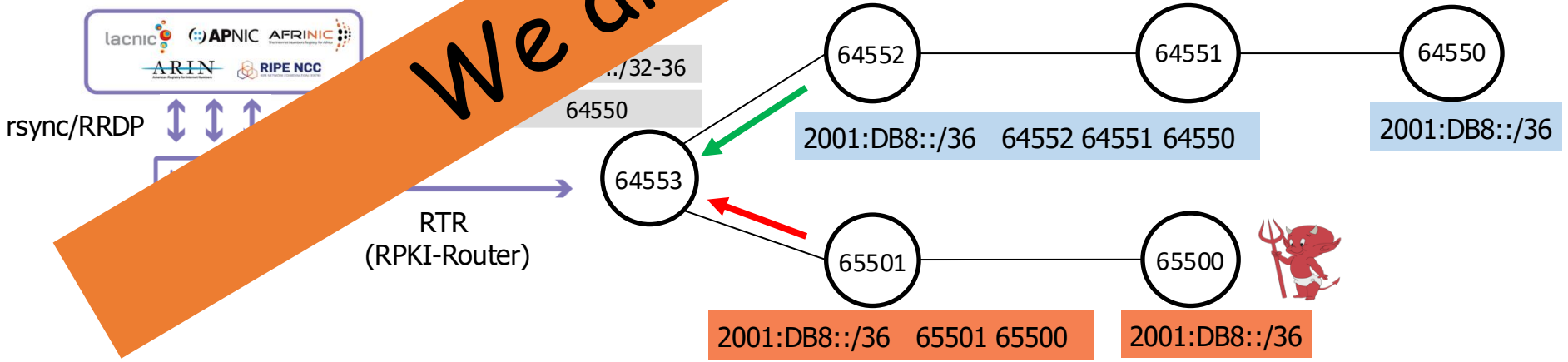
- Digitally signed ~ binds prefixes and nominated ASN
- Can be verified crypto-magically

P	:DB8::/32
n	/36
gin ASN	AS64550

ROV – Route Origin Validation

- Helps validate if an ASN is permitte a route
- Mis-origination / origin hijack

We all know this!



Puzzle Pieces: RPKI [Origin Validation]

ROA Best Practices

https://stat.ripe.net/

"timestamp":"2026-08-28T20:57:30, "target_prefix":"162.55.80.0/24", "path":[20912,6204,62390,24940}
"timestamp":"2026-08-28T20:57:30", "target_prefix":"162.55.80.0/24","path":[209823,5511,6204,62390,24940]

Minimal ROA (RFC9319):

- ROA should only cover prefixes announced in BGP (maxLength)
- August 2026 Hetzner 162.55.80.0/24 hijack

ROA (before 2 Sept 2026)
Prefix: 162.55.0.0/16
Max-length: 24
Origin: AS24940

AS0 ROA (codified in RFC6483)

- For unused/undelegated address space
  - maxLength: /32 v4 and /128 v6
- April 2026 Orange 90.98.0.0/15 hijack

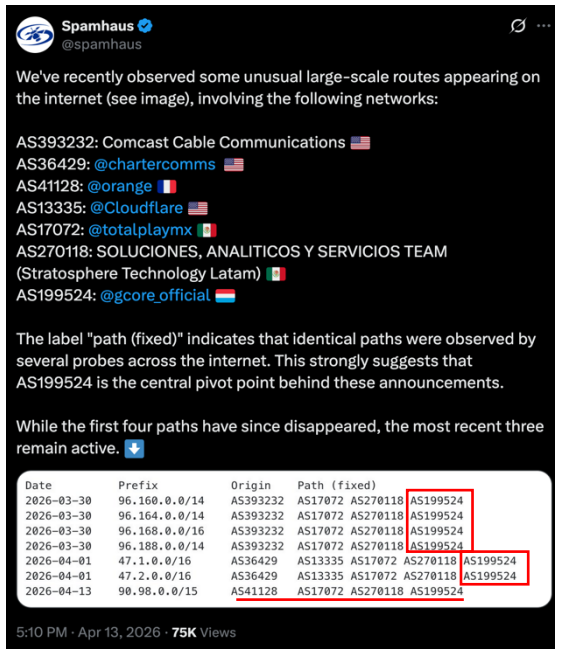


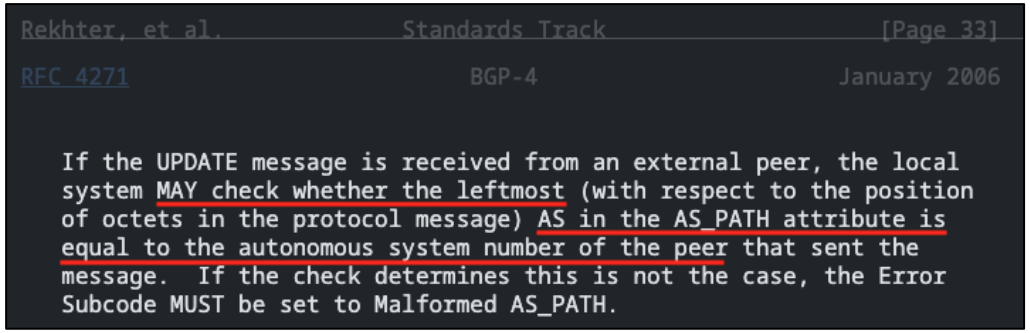
…..
A ROA with a subject of AS 0 (AS 0 ROA) is an attestation by the holder of a prefix that the prefix described in the ROA, and any more specific prefix, should not be used in a routing context.

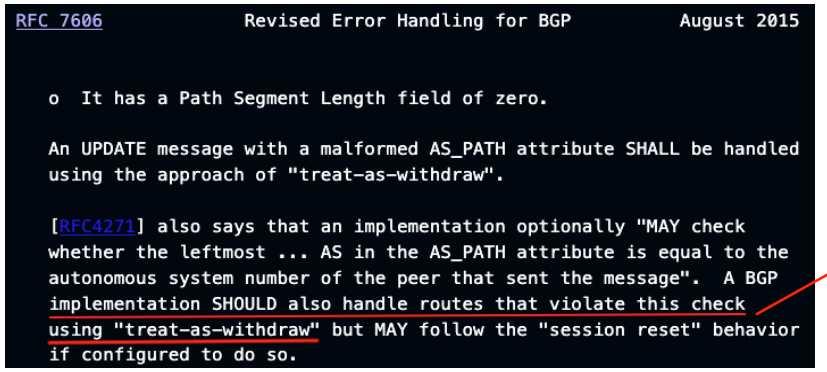
Puzzle Pieces: BGP “enforce First-AS”

During the April 2026 Orange incident:

- *AS0 ROA would mark as Invalid | ASPA could detect the forged origin AS and forged AS_PATH*
- Also revealed lack of basi BGP sanity check ~ first AS check/enforcement by AS199524 (and some well-known Tier-1s)



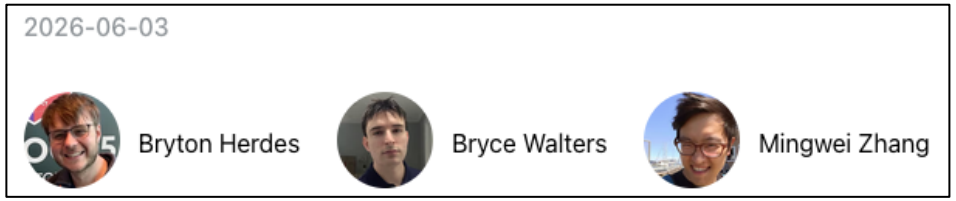




Routes to be removed from Adj-RIB-In

Puzzle Pieces: BGP “enforce First-AS”

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



1. Allocated two IP prefixes, one for IPv4 and one for IPv6, to advertise to Tier 1 External BGP (EBGP) neighbours
2. Purposely prepended the test prefix advertisements to Tier 1 neighbours with a Cloudflare-owned, non-13335 ASN (AS402542) in front of 13335

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’ by default!
- available as configuration knobs (except RouterOS)

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!

```
➜ monocle rpki aspas --customer 17660 --format markdown
Data source: Cloudflare (cached at 2026-09-08 04:33:56 UTC, 2947 ASPAs)
Found 1 ASPAs
| Customer ASN | Customer Name | Country | Providers  |
|--------------|---------------|---------|------------|
| AS17660      | BT            | BT      | 2914, 6453 |
```

```
➜ monocle rpki aspas --customer 18024 --format markdown
Data source: Cloudflare (cached at 2026-09-08 04:33:56 UTC, 2947 ASPAs)
Found 1 ASPAs
| Customer ASN | Customer Name | Country | Providers |
|--------------|---------------|---------|-----------|
| AS18024      | BT            | BT      | 17660     |
```

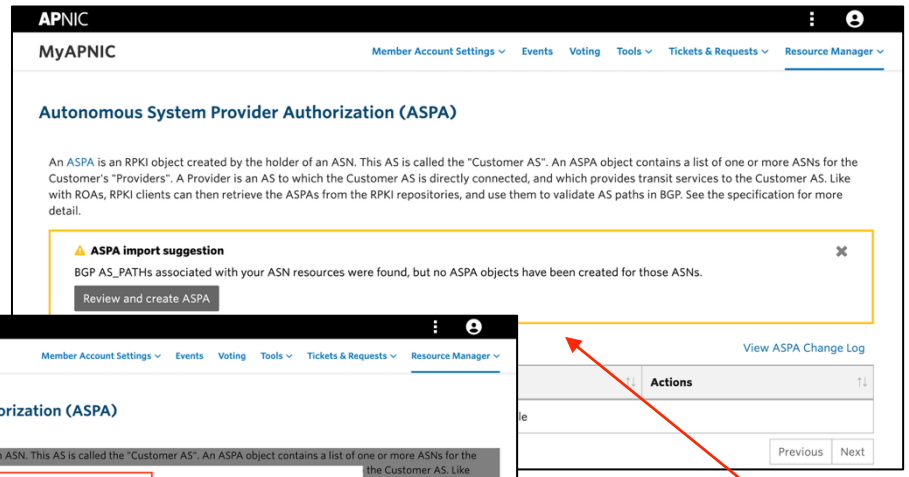
```
➜ monocle rpki aspas --customer 1299 --format markdown
Data source: Cloudflare (cached at 2026-08-26 04:08:51 UTC, 2782 ASPAs)
Found 1 ASPAs
| Customer ASN | Customer Name        | Country | Providers |
|--------------|----------------------|---------|-----------|
| AS1299       | f/k/a Telia Carrier  | SE      | 0         |
```

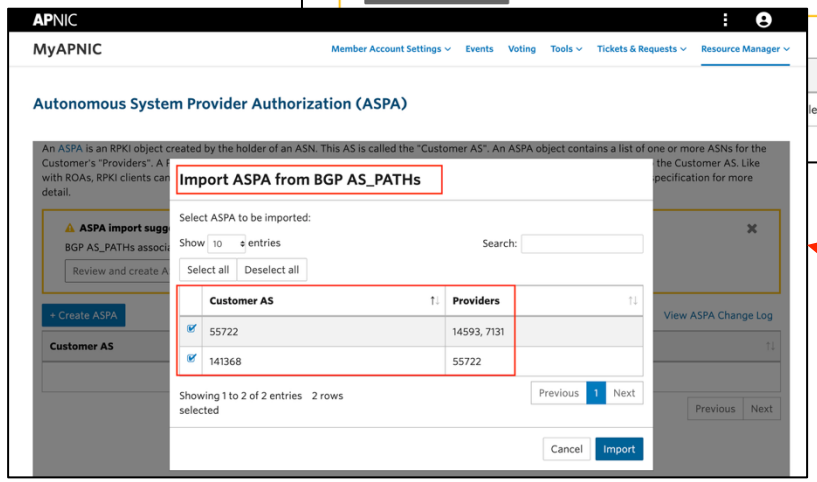
AS0 ~ I have no transit providers!

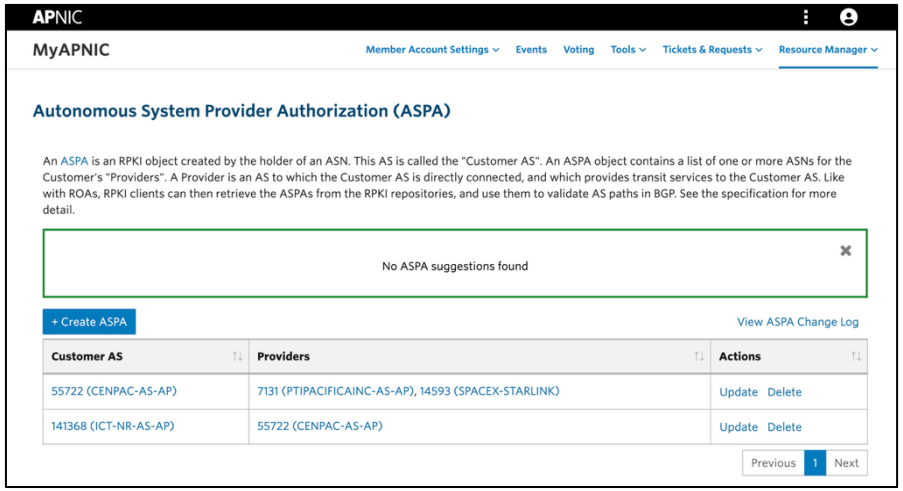
Puzzle Pieces: ASPA

APNIC ASPA Signer/Dashboard available ~ 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.
- Include any non-transparent Route Server AS(es)

Puzzle Pieces: ASPA

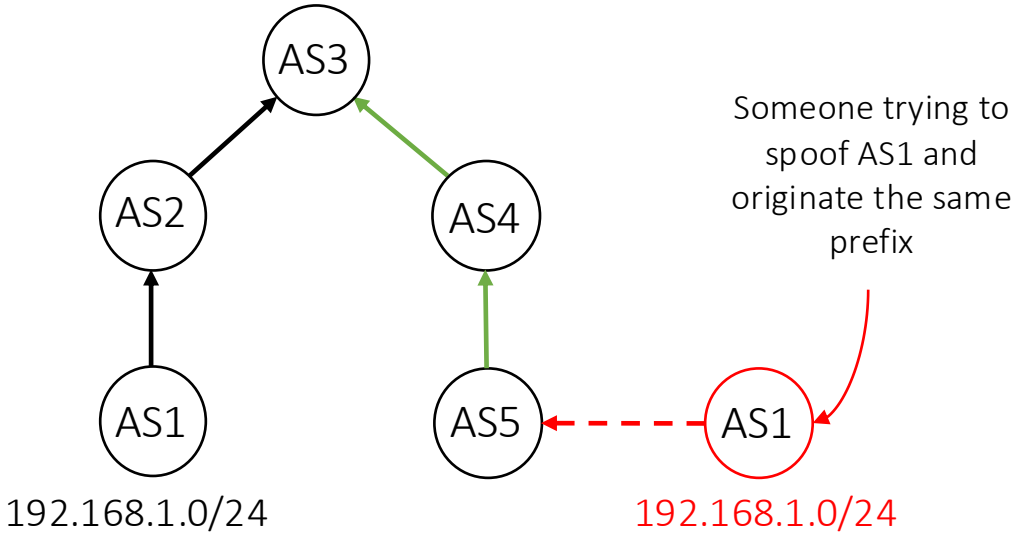
AS-to-AS hop verification (Upstream: Customer to Provider)

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 (ROA exists)
- 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
```

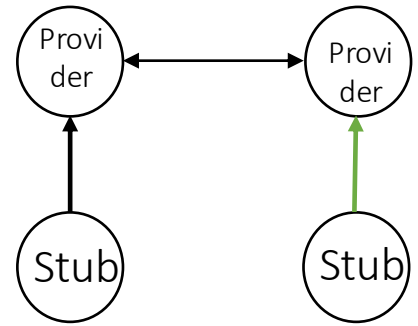
- AS4 checks ASPA
  - AS5 is 'Not Provider' for AS1
- Hence, INVALID

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

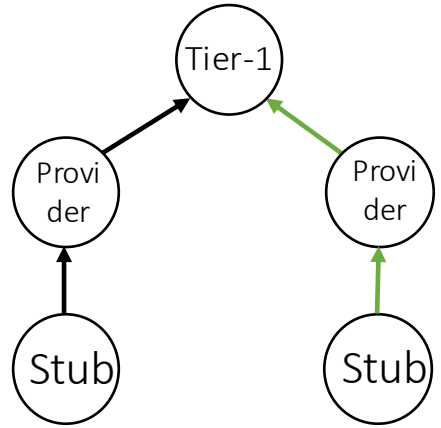


192.168.1.0/24

UP and DOWN must either:

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

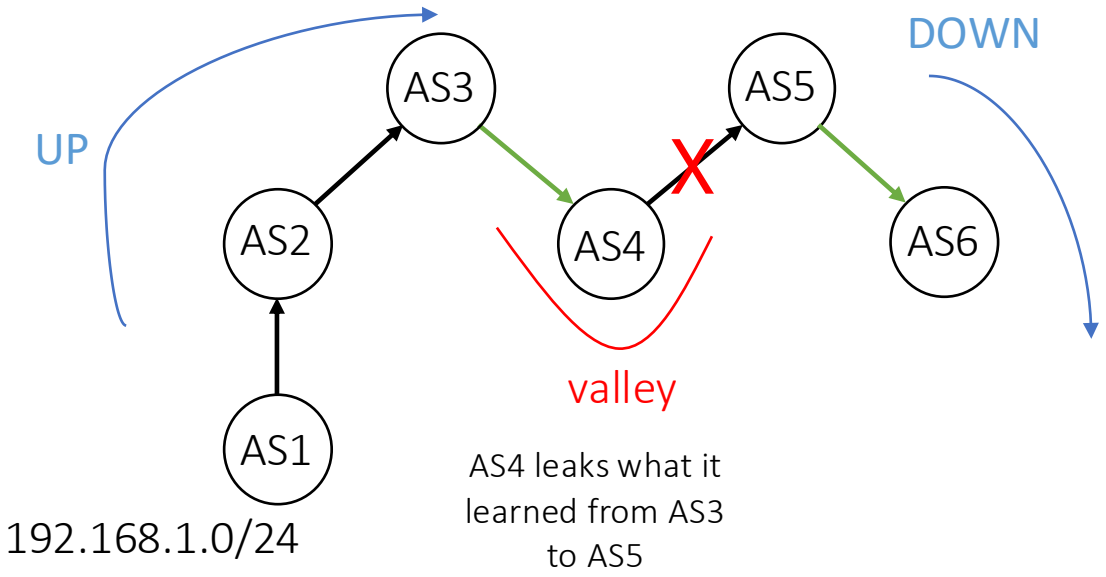
A gap in the UP and DOWN indicates there is a valley - Invalid



192.168.1.0/24

Puzzle Pieces: ASPA

ASPA: Provide to Provider leak



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

- AS1 announce 192.168.1.0/24 (ROA exists)
- 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: as of Aug-Sept 2026

	Available Now	Announced / Underway	TBC
Standards		RTRv2 and ASPA Both still in draft – maybe end of 2026?	
Signers	- ARIN - RIPE - APNIC		- AfriNIC - LACNIC
RP	- Routinator (RP + RTR) - rpkiclient (RP) - RTRTR (RTR proxy & server) - FORT - Krill (delegated CA)		
Vendor BGP		- Nokia: SROS R27 ~ 2027 - JunOS: 26.4 (Q4 2026) - Cisco: IOS-XR 27.1?	- Huawei: NetEngine? - Arista?
Routing Daemons	- OpenBGPD (>7.8) - BIRD		

Analysis Tool: RouteViews

When incidents happen, folks need access to BGP data to understand when and how it happened?



- Public collectors like RouteViews become crucial

- RouteViews collects and archives BGP routing tables (RIBs) and BGP updates:
  - archives every 2 hours
  - 27-year-old data archive

Summary

RFC8212: No policy? No routes!

Enforce-first-as:

- Did I receive the update from my actual neighbour?
- Watch out for transparent AS peers (route servers)

ROA/ROV: Is this ASN allowed to originate this prefix?

BGP Roles: am I allowed to advertise this route to this neighbour?

ASPA: Is the AS_PATH consistent with authorised providers?