RIPE NCC
RIPE NETWORK COORDINATION CENTER

Autonomous System Provider Authorisation

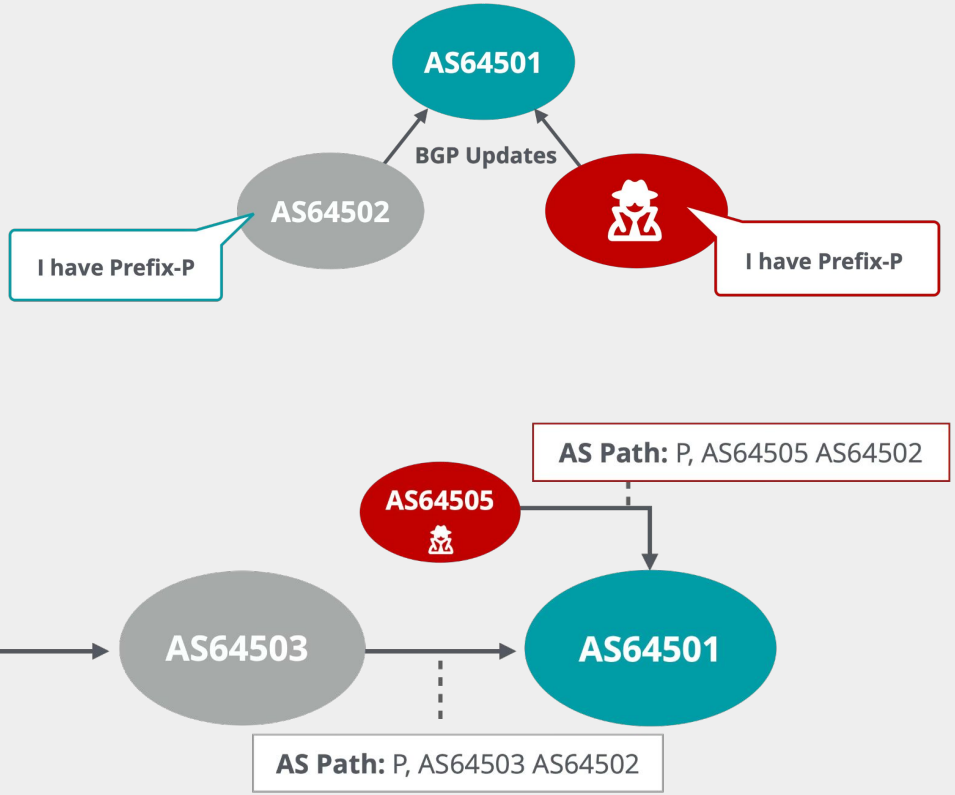
A new tool for routing security

Ondřej Caletka | INEX | 17 September 2026

The Need for Routing Security

BGP is based on trust

- Plain-text protocol **without authentication** or encryption
- Any Autonomous System can **announce any prefix**
- Any router can **spoof attributes** like AS path



Resource Public Key Infrastructure (RPKI)

RPKI is not just Origin Validation

- Route Origin Validation is the **first and most popular** service of RPKI
- ROV **prevents misorigination** or **more specific** hijacks
- ROV does not protect against **AS path spoofing**
- ROV does not prevent route leaks that **preserve AS path** (route leaks type 1 - 4)

Autonomous System Provider Authorisation

Resource Public Key Infrastructure (RPKI)

Autonomous System Provider Authorisation

- New protocol using the **RPKI ecosystem**
- Allows BGP **path verification**
- Partial deployment is supported
- Address family agnostic

Two components of ASPA

Signing

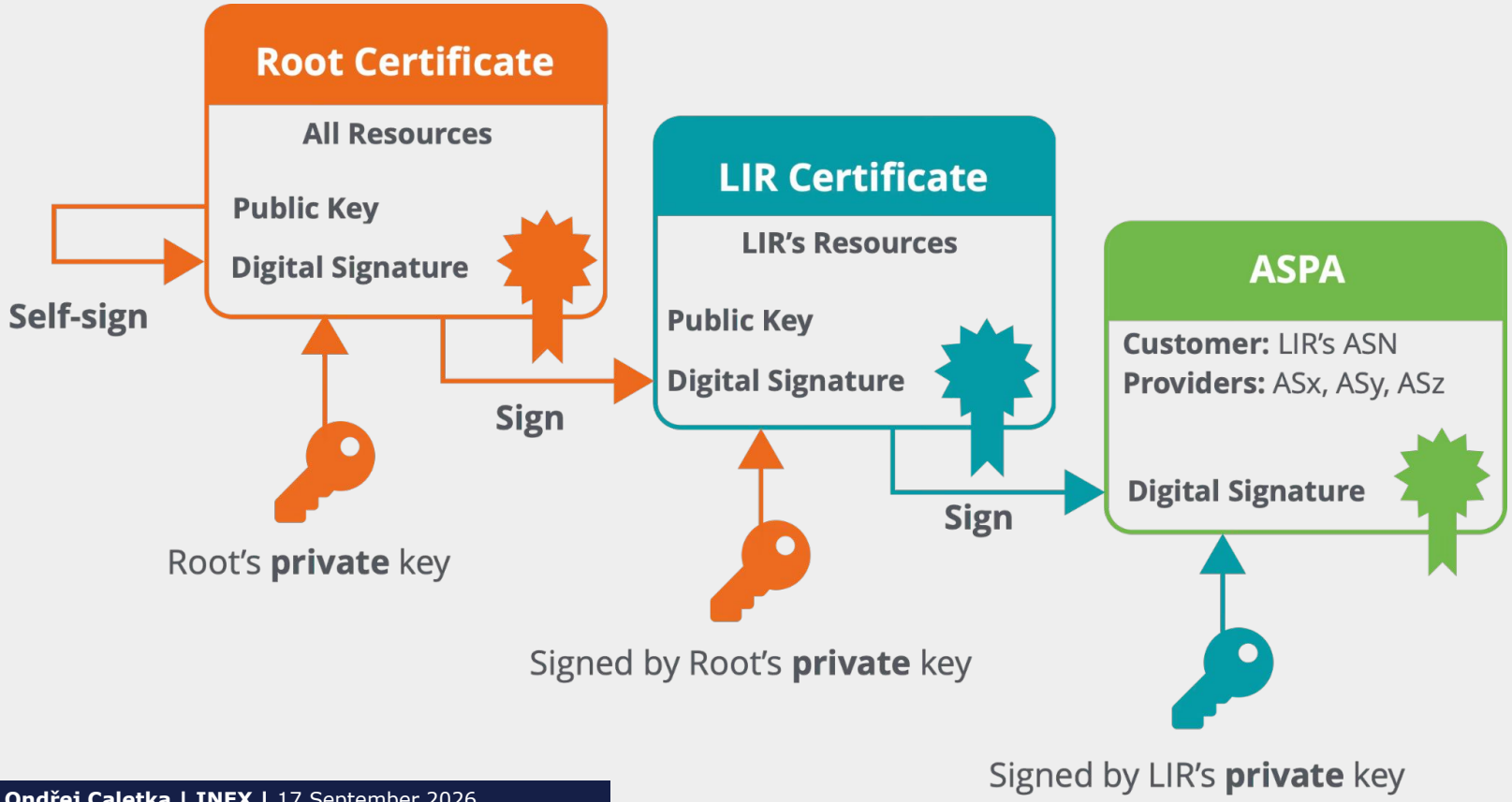
- Done by ASN holders
- Lists set of **Provider ASNs**
- Published in a RPKI repository on the Internet

Validation

- Ideally done by every network on the Internet
- Downloads **ASPA objects**
- Validates **digital signatures**
- Loads validated data into routers to support **ASPA verification**
- Makes better routing decisions

Signing ASPA

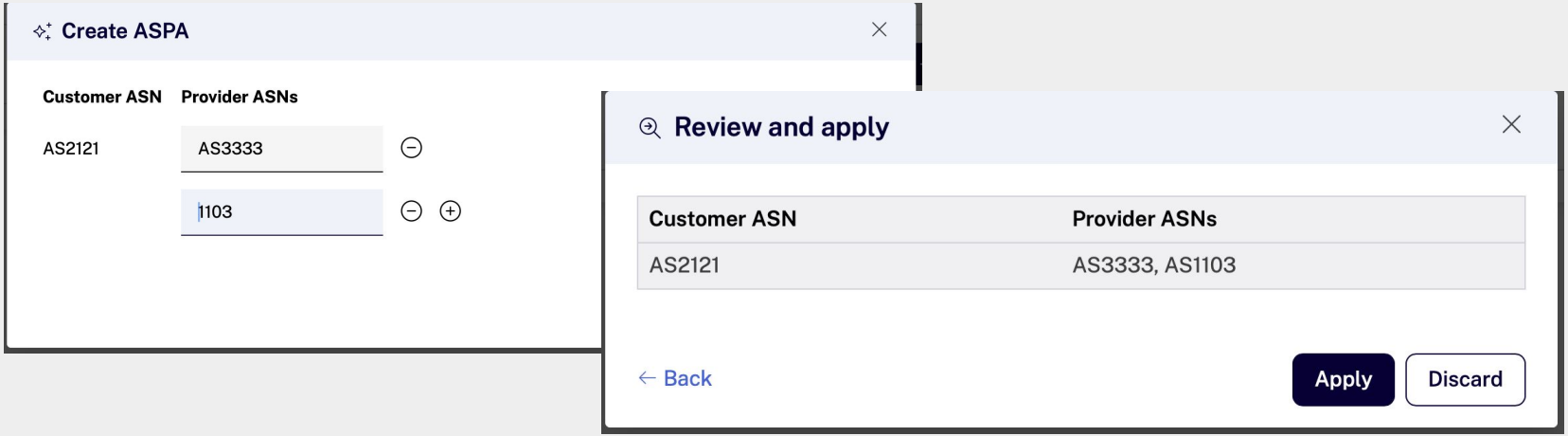
RPKI Chain of Trust



Signing ASPA

ASPA Object

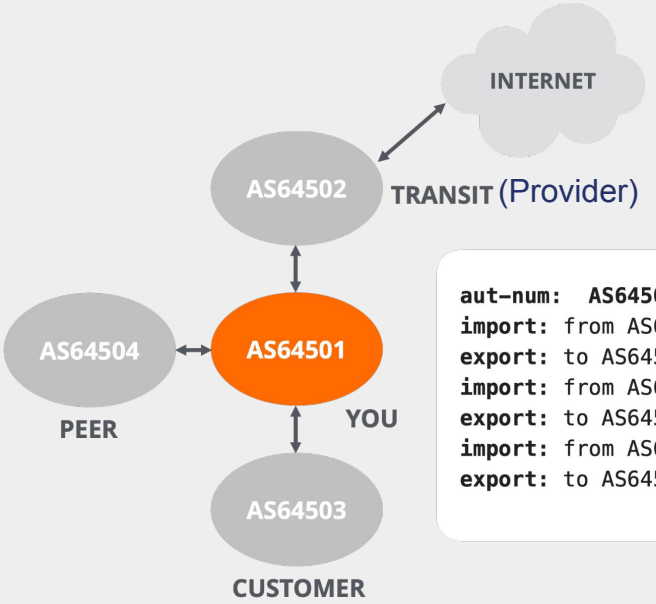
- Object issued by a **holder of an AS number**
- Contains a set of **Provider AS numbers**
- Must be **signed by a RPKI certificate** proving holdership of the **customer AS number**



Signing ASPA

What to put into ASPA object?

- ASNs of your (transit) **providers**
  - Also **partial** providers
  - Think of **backup** providers, **DDoS scrubbing** providers
  - Non-transparent route servers in IXPs
- **Not** your customers
- **Not** your (lateral) peers
  - Unless they can **act as providers** under some circumstances



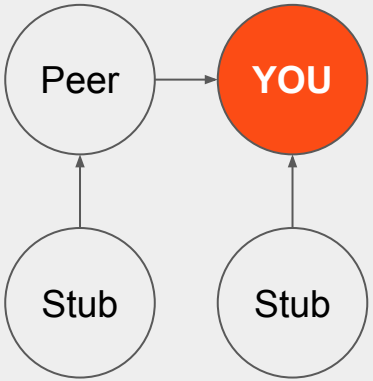

```
aut-num:  AS64501
import:  from AS64502 accept ANY
export:  to AS64502 announce AS64501 AS64503
import:  from AS64503 accept AS64503
export:  to AS64503 announce ANY
import:  from AS64504 accept AS64504
export:  to AS64504 announce AS64501 AS64503
```

ASPA Path Verification

ASPA Path Verification

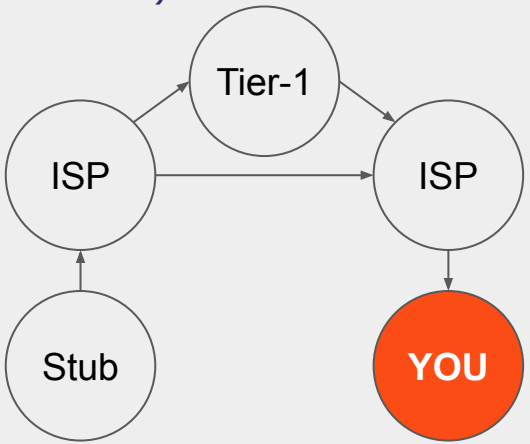
Upstream Path Verification

- For BGP sessions with **customers** and **peers**
- Simpler and stricter
- Only **up-ramp** is allowed



Downstream Path Verification

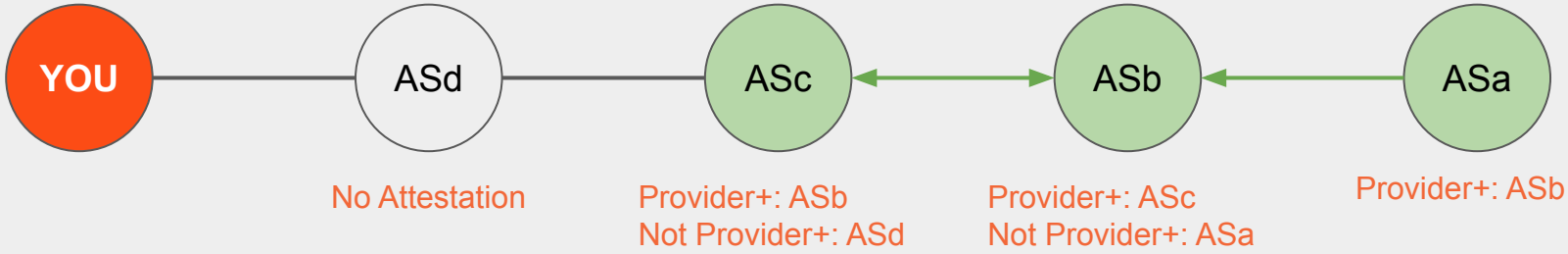
- For BGP sessions with **transit providers**
- Allows **one up-ramp** (to the transit provider) and **one down-ramp** (to your network)



ASPA Path Verification

Attesting BGP neighbours

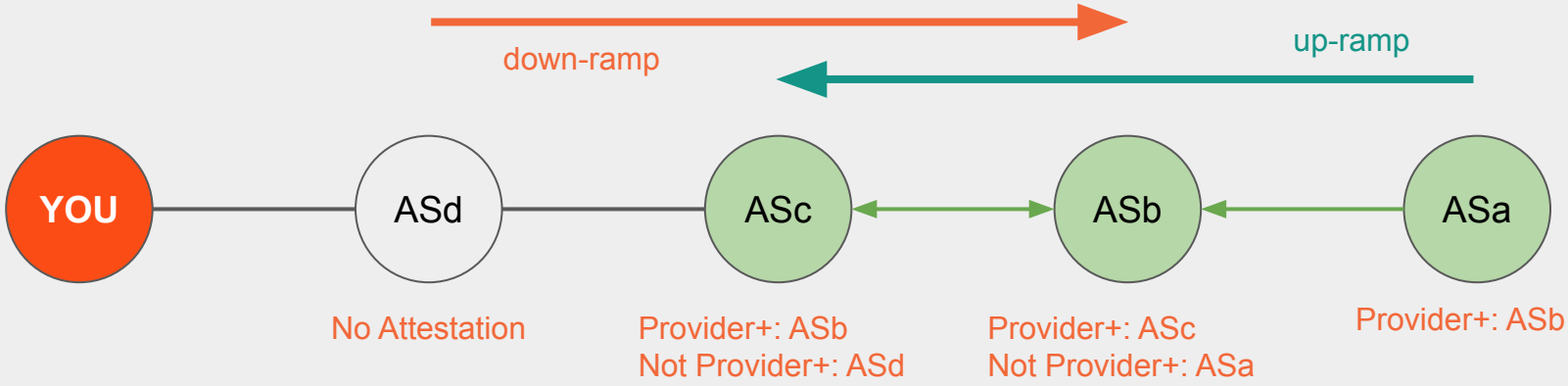
- The router only sees **a sequence of AS numbers**
  - The leftmost is your **BGP neighbour**
  - The rightmost is the **origin ASN**
  - The sequence is **compressed** - series of the same ASNs are reduced to one
- For each **directional** pair of (ASx, ASy) ASPA verifies that either:
  - ASy is **Provider+** of ASx, or
  - ASy is **Not Provider+** of ASx, or
  - There is **No Attestation** about providers of ASx (there is no ASPA for ASx)



ASPA path verification

Building Ramps

- **Up-ramp** always starts at the origin
- **Up-ramp** grows towards you **until Not Provider+** relationship is encountered
- **Down-ramp** always starts at your **BGP neighbour**
- **Down-ramp** grows away from you **until Not Provider+** relationship is encountered



Upstream Path Verification

Upstream Path Verification

Spoofed origin AS

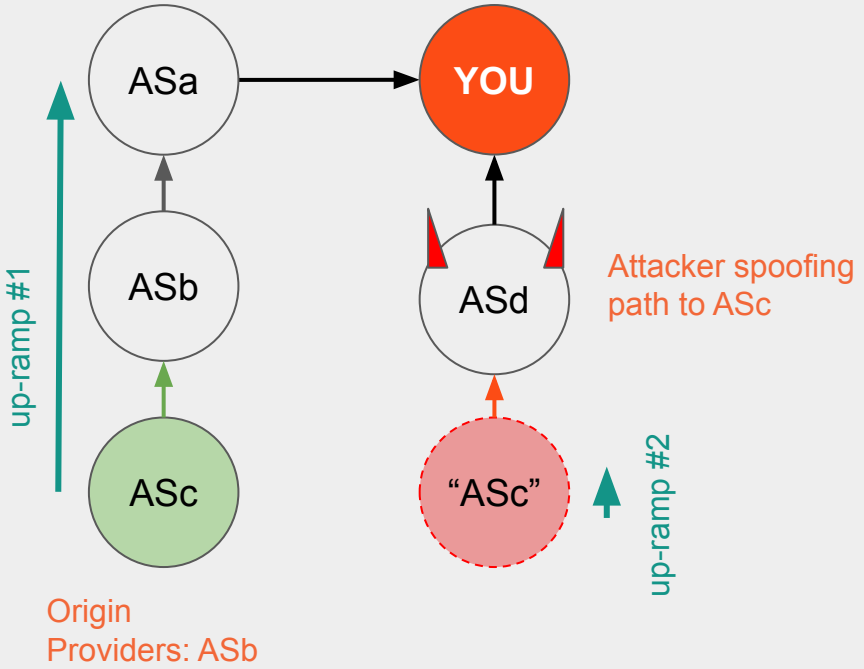
Your router sees **two paths** to the same network:

1. ASa ASb ASc
2. ASd ASc

The **origin ASN** is the same, so **ROA check will pass** in both cases.

ASPA states that ASd is **Not Provider+** of ASc.

Your router therefore **drops path #2**, mitigating the attack.



Upstream Path Verification

Nothing malicious, just a route leak

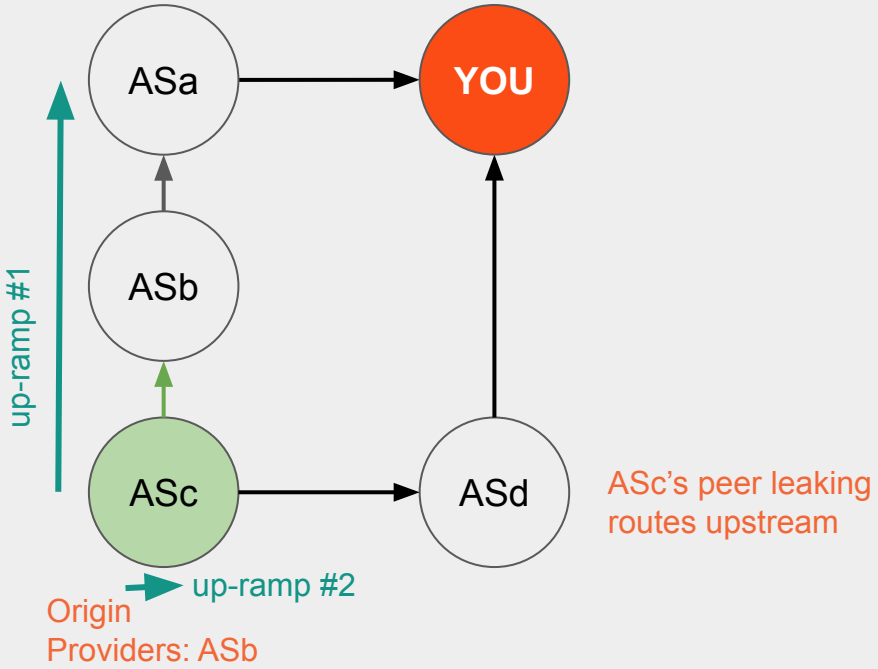
Your router sees **two paths** to the same network:

1. ASa ASb ASc
2. ASd ASc

The **origin ASN** is the same, so **ROA check will pass** in both cases.

ASPA states that ASd is **Not Provider+** of ASc.

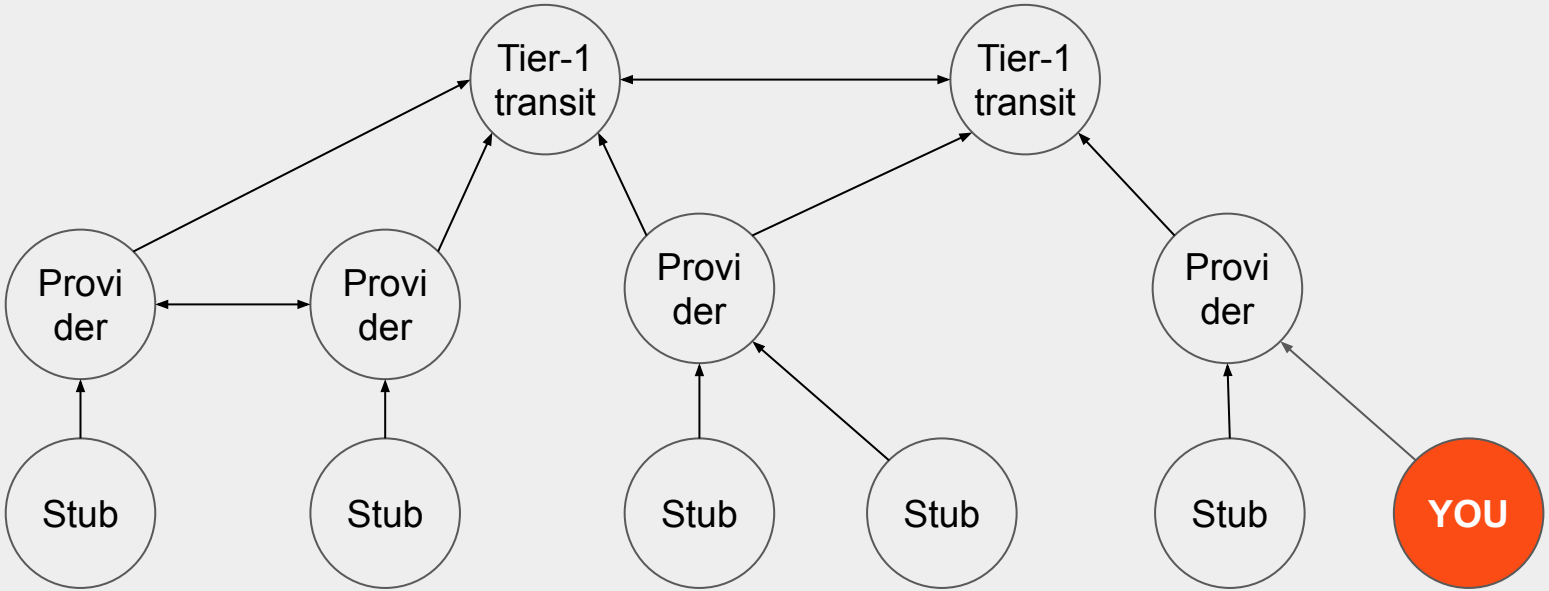
Your router therefore **drops path #2**, mitigating the route leak.



Downstream Path Verification

Valley-Free Routing

Up, to the side, and then down

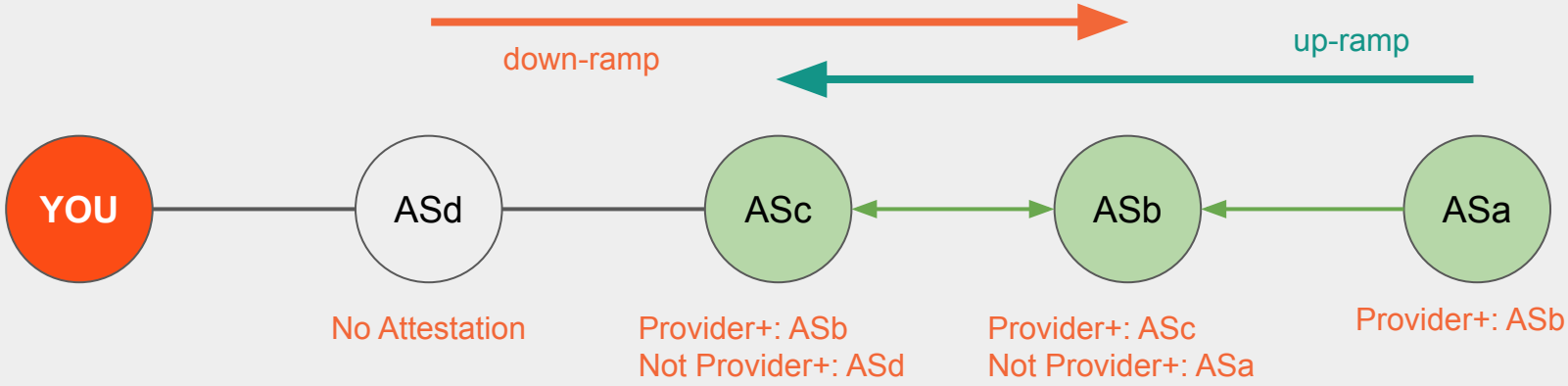


Downstream Path Verification

Using the ramps to determine implausible paths

- **Up-ramp** represents the path from the origin to **their Tier-1 provider**
- **Down-ramp** represents the path from **your Tier-1 provider** to you

But the router **does not know anything** about tiers, it only **considers the ASPA data.**

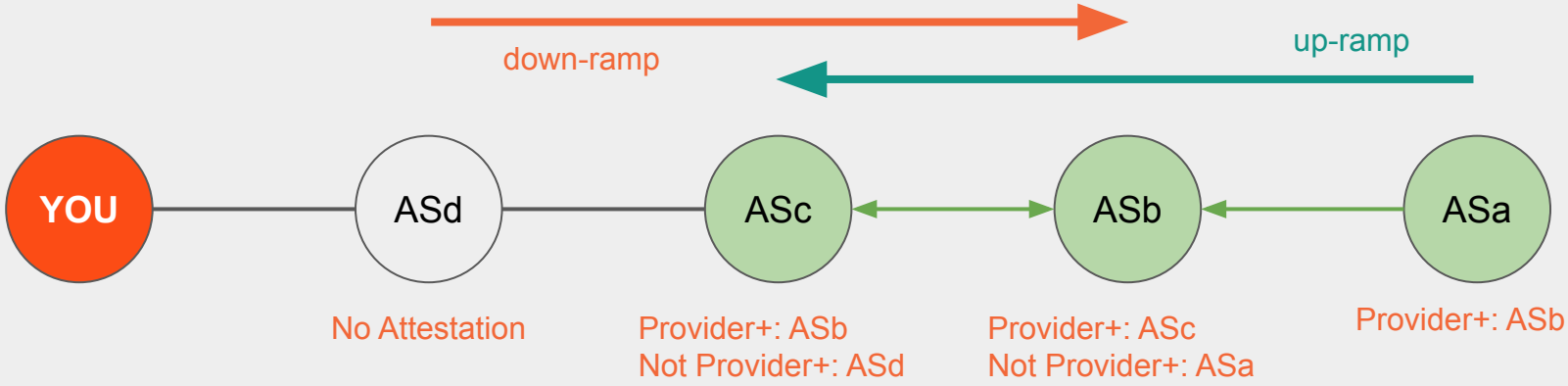


Downstream Path Verification

Using the ramps to determine implausible paths

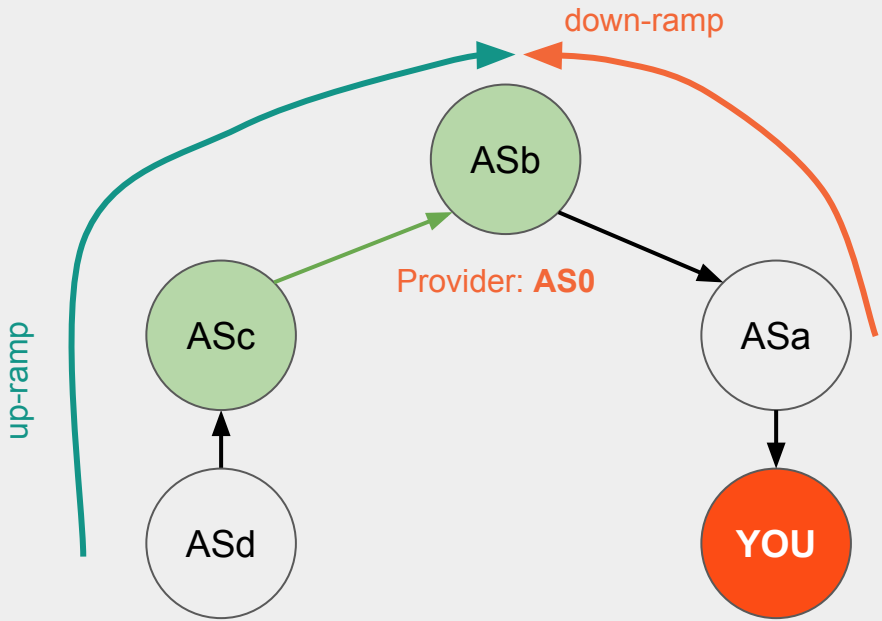
- A path is only **plausible** if:
  - The ramps are **touching** or (partially) **overlapping, or**
  - The ramps are **meeting at neighbouring Autonomous Systems**

In other words, **each AS** along the path needs to be part of **at least one ramp.**



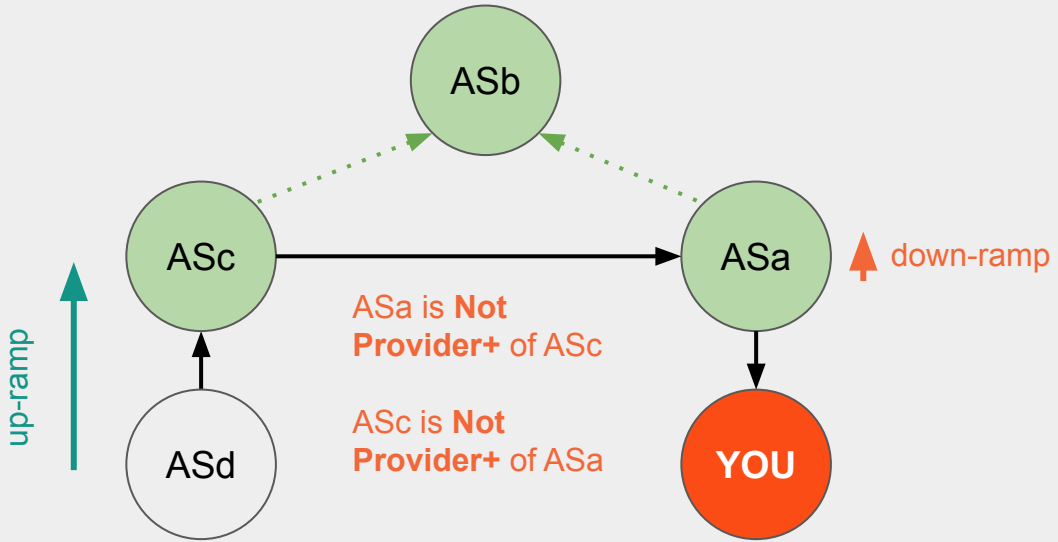
Downstream Path Verification

Valley-free example - Tier-1 deploying ASPA



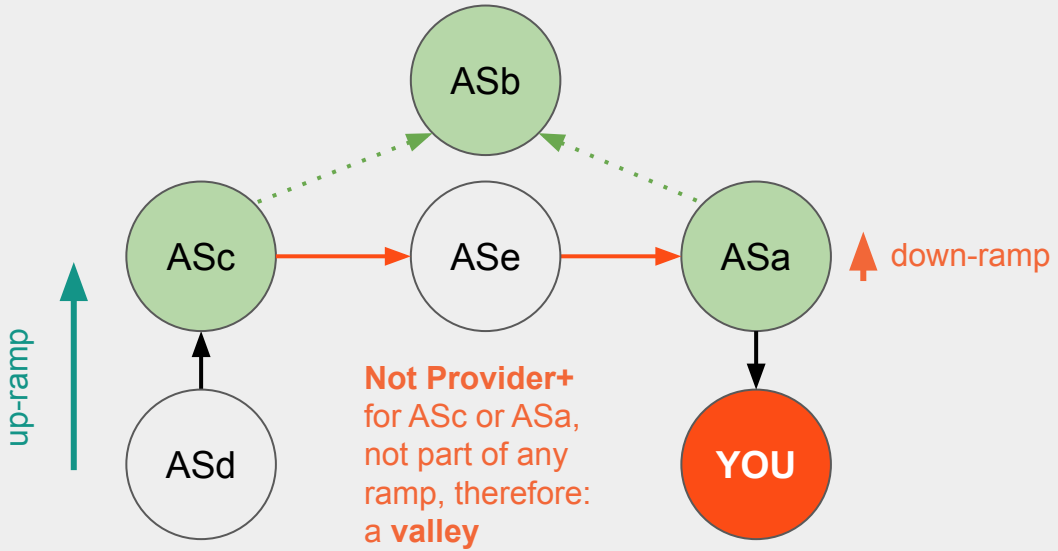
Downstream Path Verification

Valley-free example - ISPs with ASPA are peering



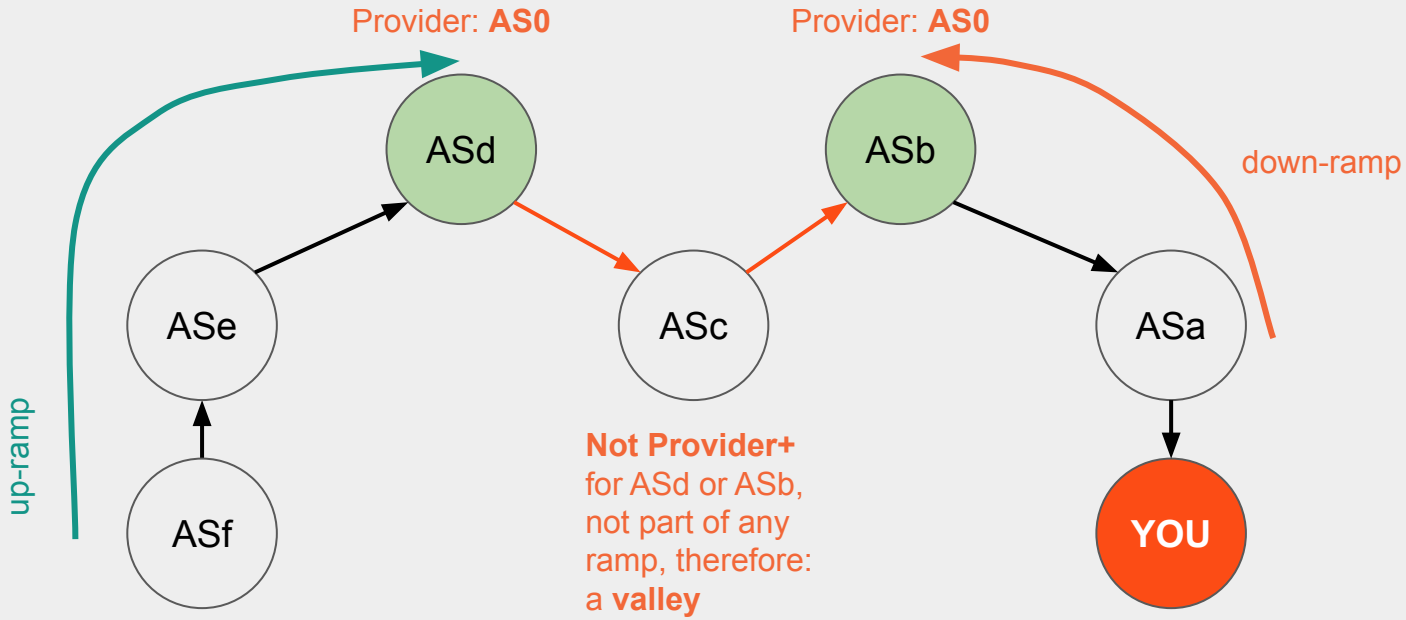
Downstream Path Verification

Not valley-free example - route leak via a peer



Downstream Path Verification

Not valley-free example - route leak during multihoming

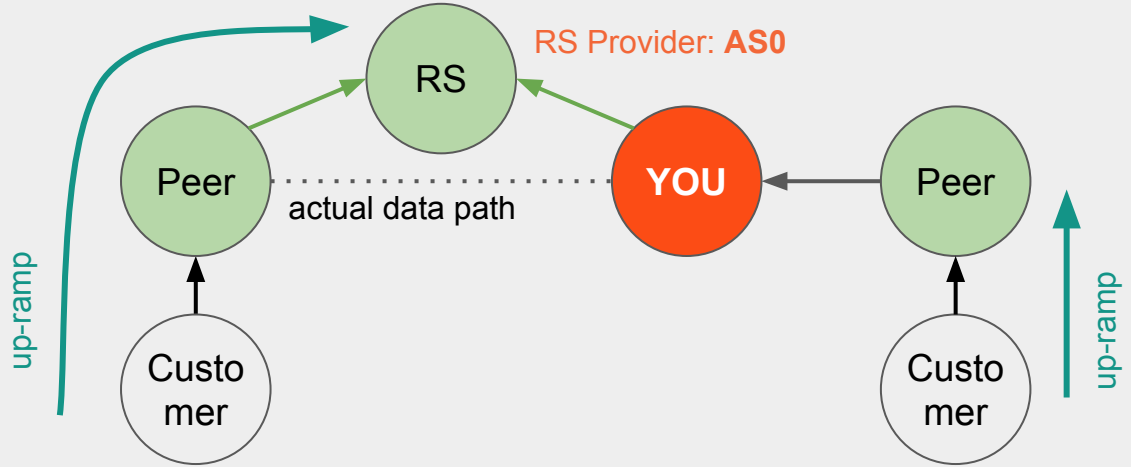


Complex Autonomous System Relationships

Complex Autonomous System Relationships

The + in Provider+ stands for non-transparent route servers

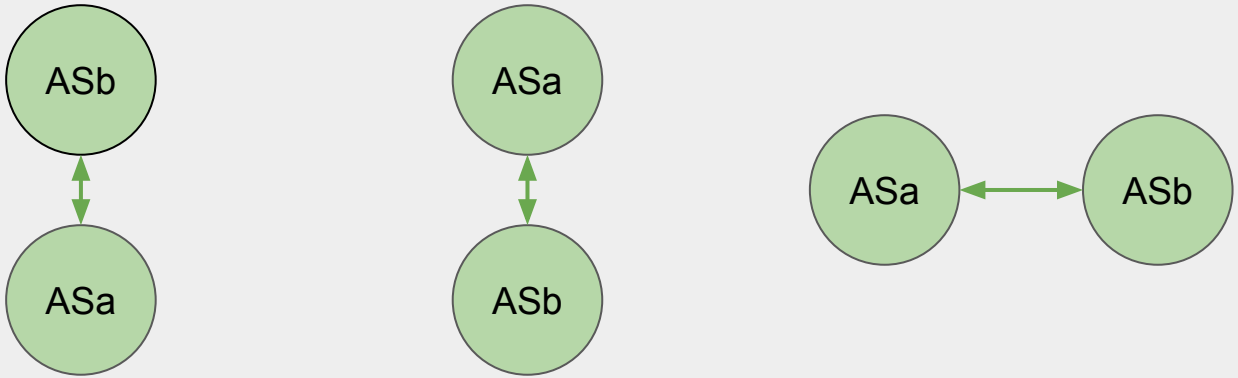
- Normally, route servers in an IXP are *transparent*. They are **not visible** in the AS path attribute.
- If an IXP uses a **non-transparent route server**, it has to be **listed as a Provider** for ASPA verification to work properly.



Complex Autonomous System Relationships

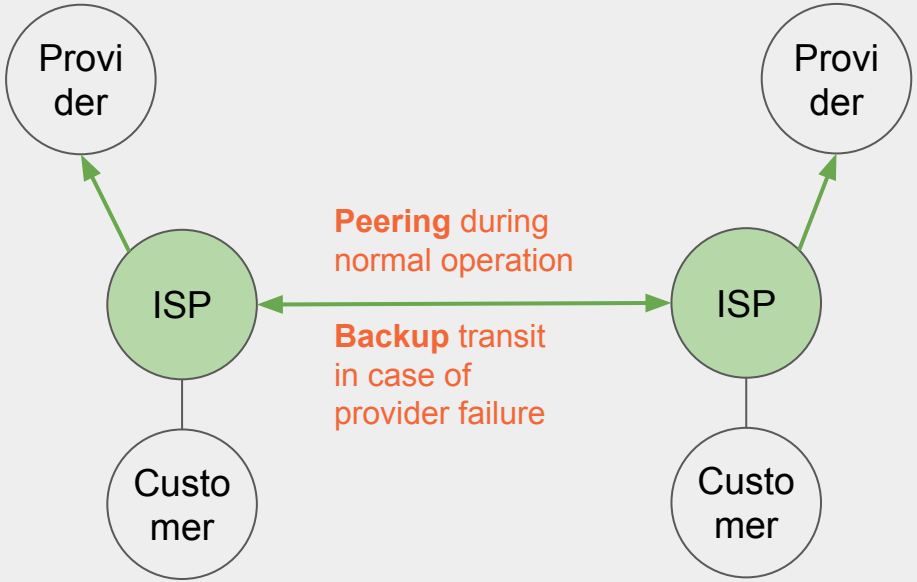
Sometimes, ASNs have multiple relationships at the same time

- Networks have to declare each other as **Provider+**
- ASPA verification will always succeed
- BGP Roles and the **OTC attribute** (RFC 9234) may help here



Complex Autonomous System Relationships

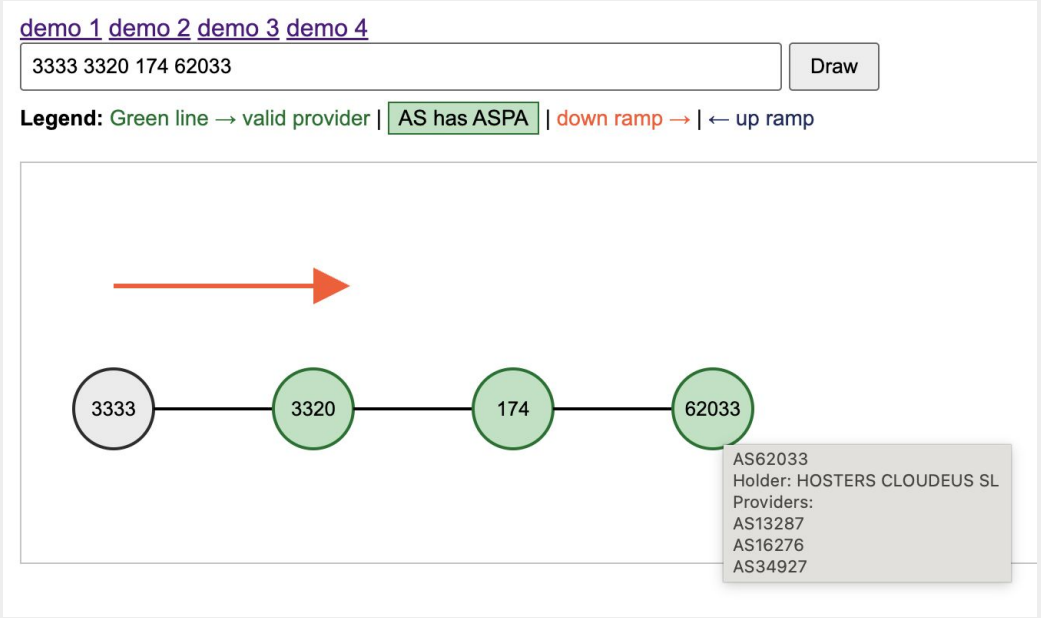
Peering doubling as backup provider



Troubleshooting ASPA Verification Failures

ASPA Path Viewer in a Web Browser

- Uses data from **rpki-validator.ripe.net**
- ASPA - **green circle**
- Provider relation - **green arrow**
- Draws maximum possible **up- and down- ramps**
- Each AS has a tooltip and a link to RIPEstat
- AS path is stored in the URL

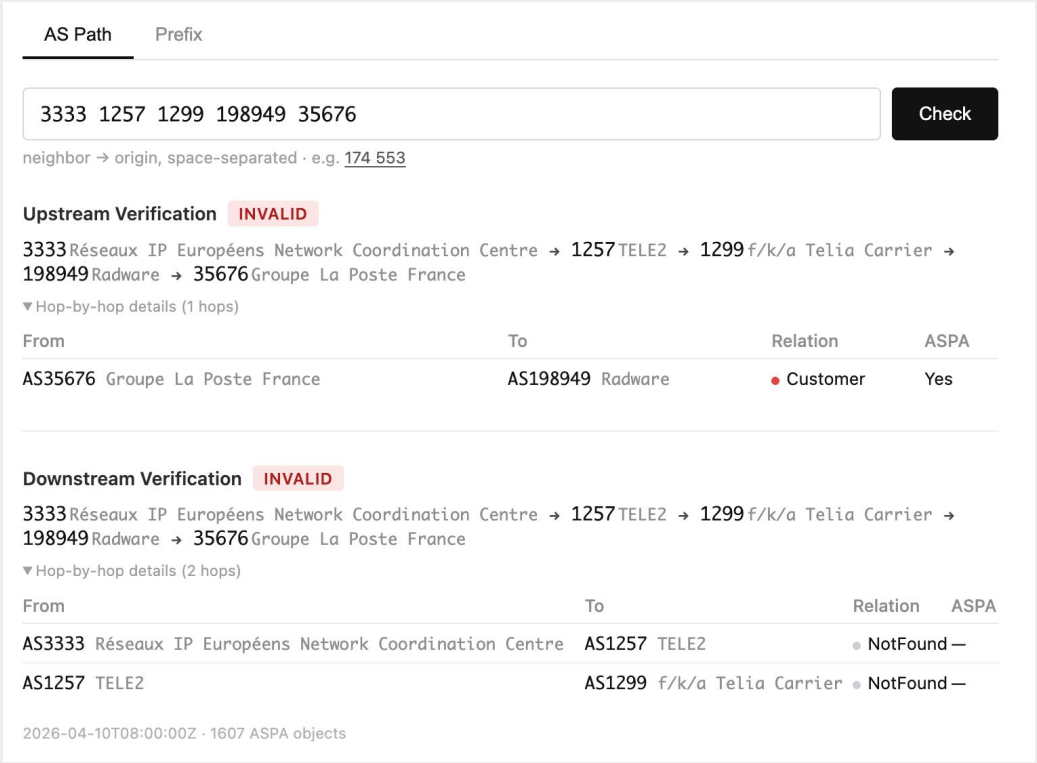


https://oskar456.github.io/aspa.html

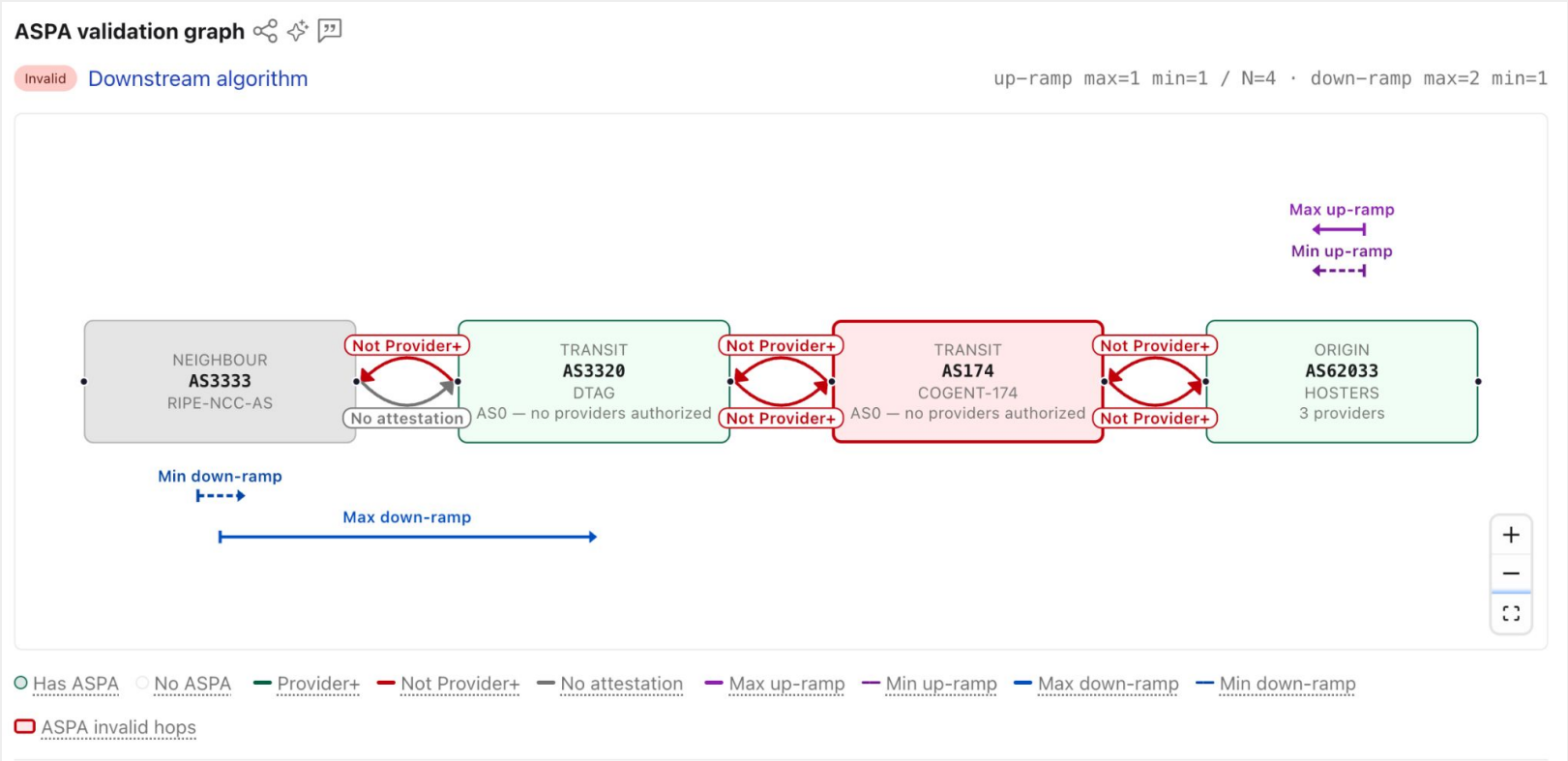
Another ASPA Checker

- Uses Cloudflare Radar
- Can also directly check a prefix

https://aspa-checker.win



ASPA Validation in Cloudflare Radar



https://radar.cloudflare.com/routing/aspa-validation

Conclusion

Conclusion

Creating ASPA is a commitment

- Creating ASPA is easy
- But you need to **know what you are doing**
- And be committed to **keep the data up to date**

Conclusion

ASPA Verification is getting there

- Ask your router vendor about it
- Reuse your existing ROV infrastructure
- Deploy **Upstream path verification** for your **customers** and **peers**
  - Detect early if your customers forget listing you as their Provider
  - **Drop ASPA-invalids** as early as possible
- Deploy **Downstream path verification** for your **providers**
  - Carefully **monitor ASPA-invalids**
  - It might be harder to reach out to the network causing the validation failures
  - Eventually **start dropping them** as well

Questions & Comments



Ondrej.Caletka@ripe.net