RIPE NCC
RIPE NETWORK COORDINATION CENTER

Autonomous System Provider Authorization

New tool for routing security

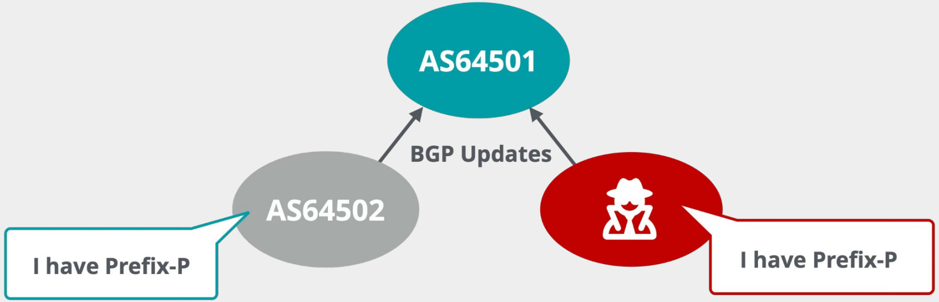
Ondřej Caletka | CSNOG 2026 | 22 January 2026

Current Routing Security

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



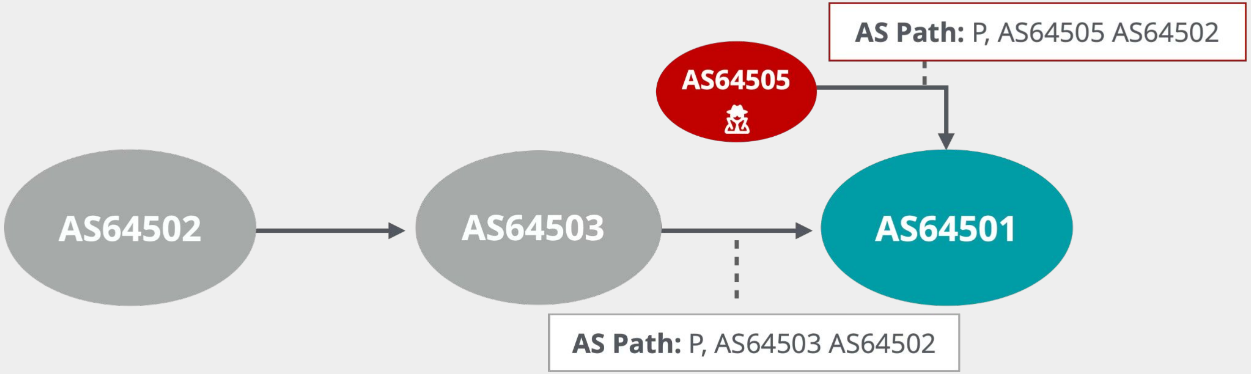
AS64501

BGP Updates

AS64502

I have Prefix-P

I have Prefix-P



AS Path: P, AS64505 AS64502

AS64505

AS64502

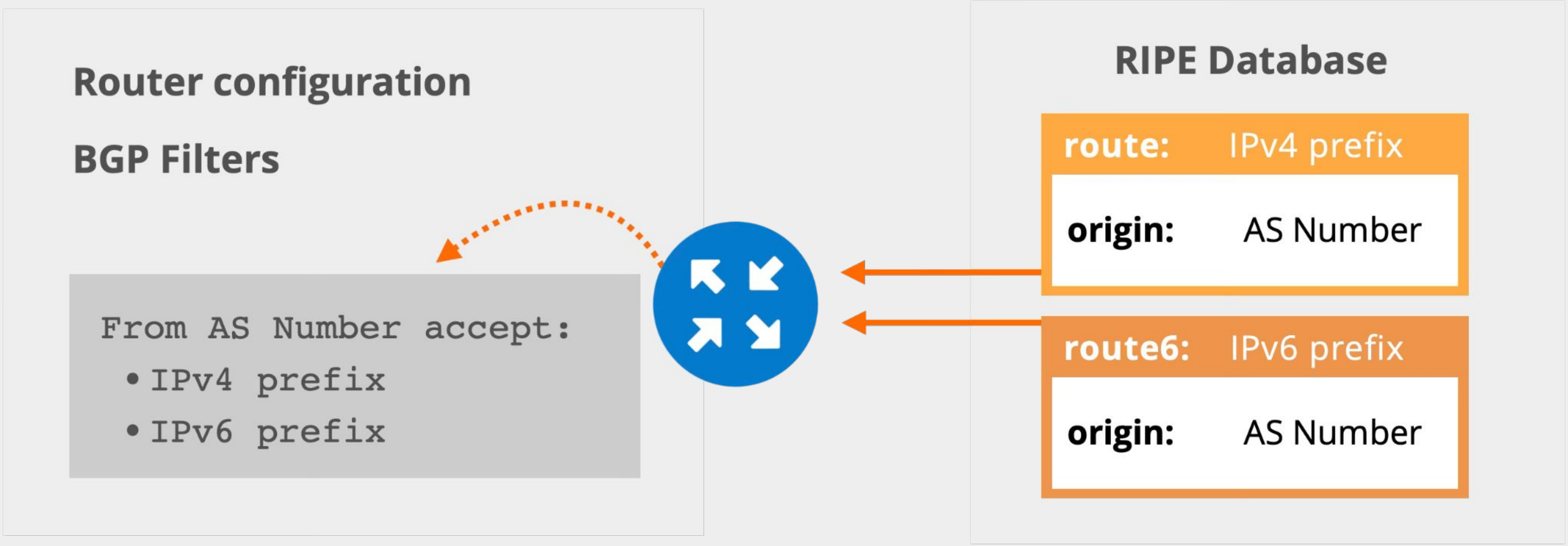
AS64503

AS64501

AS Path: P, AS64503 AS64502

Internet Routing Registries

Route objects bind prefixes to Autonomous Systems



Router configuration

BGP Filters

```
From AS Number accept:
  • IPv4 prefix
  • IPv6 prefix
```

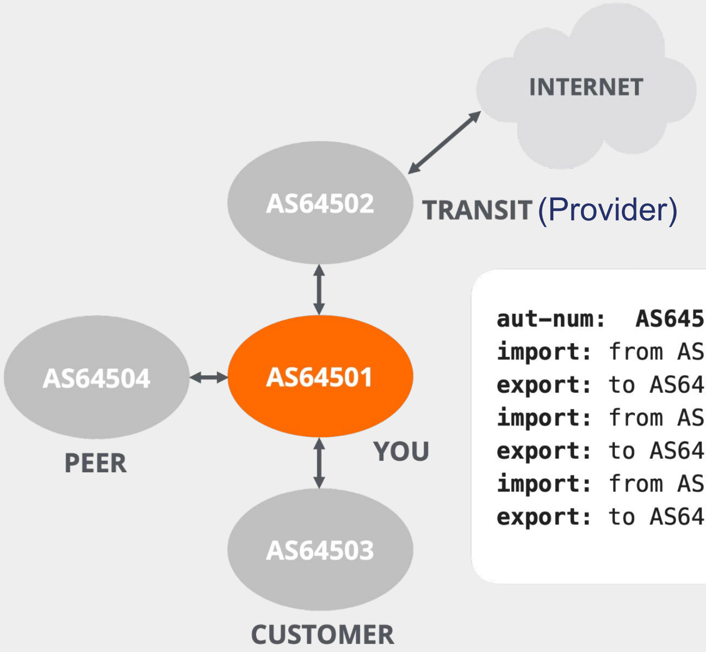
RIPE Database

route: IPv4 prefix
origin: AS Number

route6: IPv6 prefix
origin: AS Number

Internet Routing Registries

Aut-num objects describe the routing policy



```
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
```

Internet Routing Registries

The Limits of the IRR system

- Multiple **inconsistent** databases
- Limited **holdership checks**
- Stale data

You download **plaintext data** from **random sources** on the Internet and put them into the configuration of your routers to **make the Internet more secure**. What could possibly go wrong?

https://irrexplorer.nlnog.net/

Resource Public Key Infrastructure

Resource Public Key Infrastructure

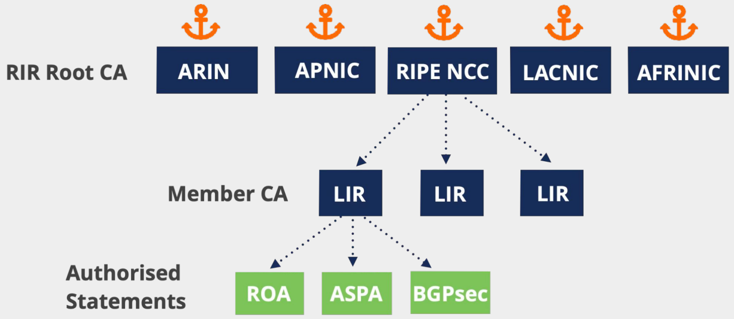
What is RPKI?

- A security framework for the Internet
- Verifies the association between **resource holders** and their **resources**
  - Attaches digital **certificate** to IP addresses and AS numbers
  - Does not contain other information about the holders (no PII)
- Growing list of use cases:
  - **BGP Origin Validation** (BGP OV)
  - **Autonomous System Provider Authorization** (ASPA)
  - **BGPsec**

Resource Public Key Infrastructure

RPKI in a nutshell

- Resource holders get certificate from their RIRs
  - It contains the list of resources
- Holders can create digitally signed objects:
  - **ROA** for authorizing an Autonomous System to **originate a prefix**
  - **ASPA** for authorizing Provider Autonomous Systems
  - **BGPsec** router certificates
- Network operators **use validated data** for **filtering BGP announcements**



Resource Public Key Infrastructure

RPKI is not just Origin Validation

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

Autonomous System Provider Authorization

Autonomous System Provider Authorization

ASPA Object Structure (simplified)

```
EE Certificate
     Public Key
     AS Number
     Signed by CA Private Key
     Not Before
     Not After

eContent
     Customer AS Number
     Provider AS Numbers

Signature
     SHA256 Hash
     Signed by EE Private Key
```

- RPKI Signed Object Template (RFC 6488)

- Intermediate End-Entity (EE) Certificate
  - Customer AS used in content
  - **MUST** be included in CA certificate
  - Signed by CA certificate private key

- eContent
  - Specific format for ASPA
  - One Customer AS (**held by signer**)
  - One or more Provider AS

The holder of the Customer AS Number declares which *AS* Numbers may appear as their Providers in BGP paths

Plausible Paths from Customer to Provider

Plausible, well… *Not Implausible* Paths

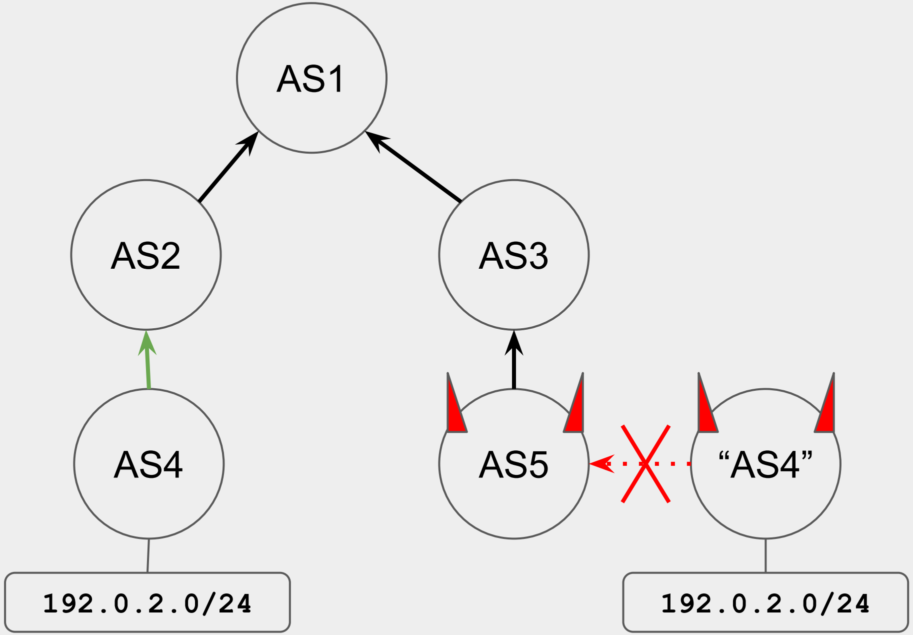
- Each **AS-to-AS hop** is *verified* as:
  - **Provider**
  - **Not Provider**
  - **No Attestation**
    (no ASPA exists for customer AS)

- A path received from a customer is **invalid** if “**Not Provider**” encountered:
  - Proven unexpected hop
  - Support **partial deployment** (no attestation is okay)
  - **Fail open** in case of an issue with RPKI *validation* itself

Routes learned from Customer AS networks MUST NOT have “Not Provider”

ASPA Verification - Routes from Customers

Spoofed origin AS



```
Given:
192.0.2.0/24 => AS4
AS4 => [ AS2 ]

AS1 sees 1 3 5 4 192.0.2.0/24
```

AS1 knows:

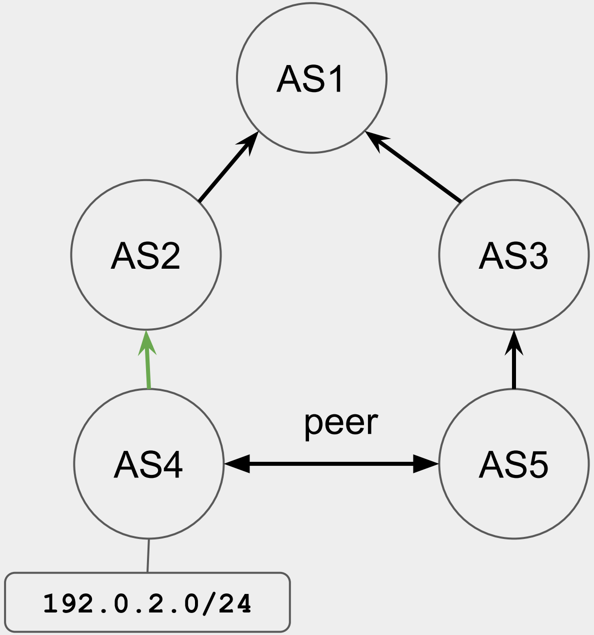
- AS3 is a **customer** session
- AS5 is "**Not Provider**" for AS4

Therefore this is **invalid**.

*Note: ASPA defines two validation algorithms: "**Upstream**" and "**Downstream**". For routes from customers or peers, the stricter "**Upstream**" algorithm should be used.*

ASPA Verification - Routes from Customers

Or.. perhaps just a leak?



```
Given:
192.0.2.0/24 => AS4
AS4 => [ AS2 ]

AS1 sees 1 3 5 4 192.0.2.0/24
```

AS1 knows:

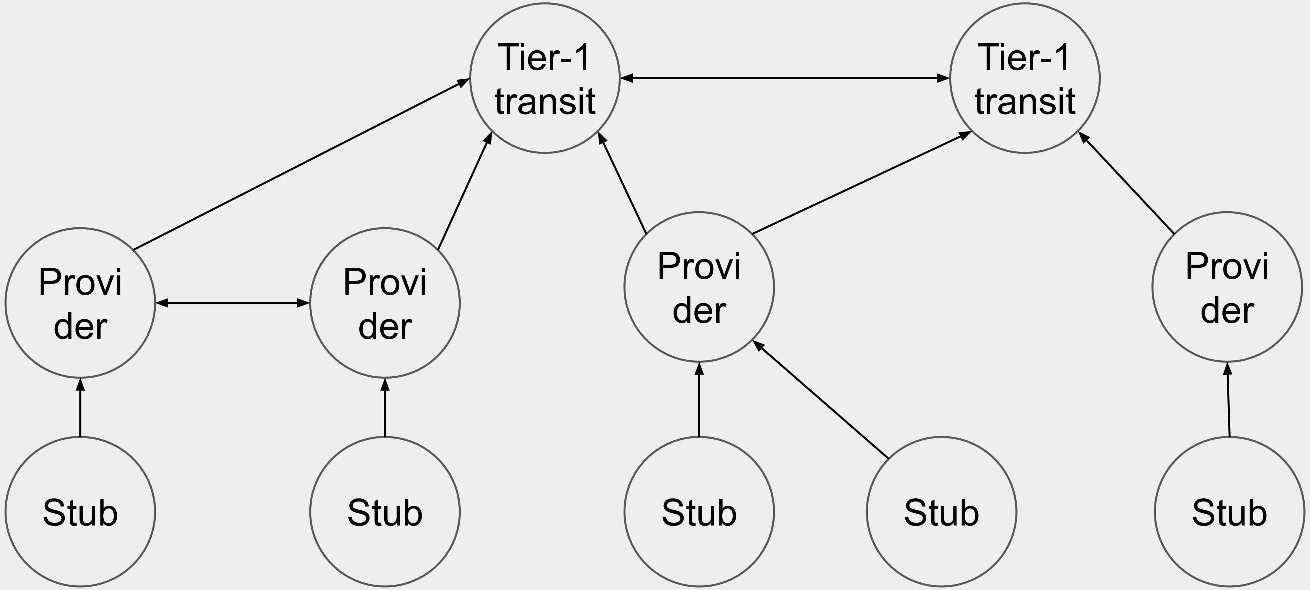
- AS3 is a **customer** session
- AS5 is “**Not Provider**” for AS4

Therefore this is **invalid**.

Note: it does not matter if it’s an accidental leak, or malicious spoofing.

Valley Free Routing - Routes from Providers

Up, to the side and then down



Data should **never flow Up-Down-Up**

ASPA can **detect valleys** in the AS path using the “**Downstream**” validation algorithm

How ASPA Finds Valleys in AS paths

Downstream Path validation algorithm

1. Each **AS-to-AS hop** is *verified* as:
   a. Provider
   b. Not Provider
   c. No Attestation

2. The longest **Up-ramp** is found starting from the origin ASN until a “**Not Provider**” relation is encountered

3. The longest **Down-ramp** is found starting from local ASN until a “**Not Provider**” relation is encountered

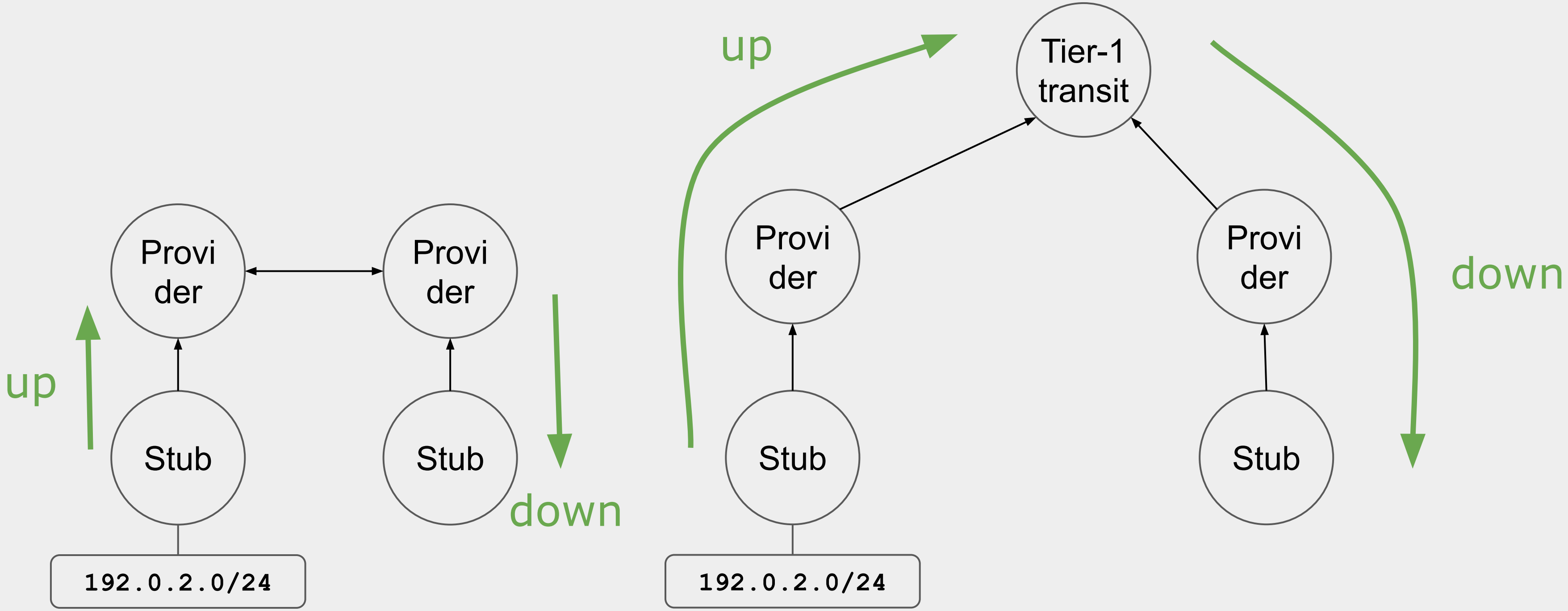
4. The path is **only plausible if**:
   a. The **Up** and **Down** ramps **meet at adjacent peers**, or
   b. The **Up** and **Down** ramps (partially) **overlap**

5. One or more hops between **Up** and **Down** ramps are **valleys**, such paths are **invalid**

6. If “**No Attestation**” is encountered, the path is **unknown**. Otherwise it is **valid**.

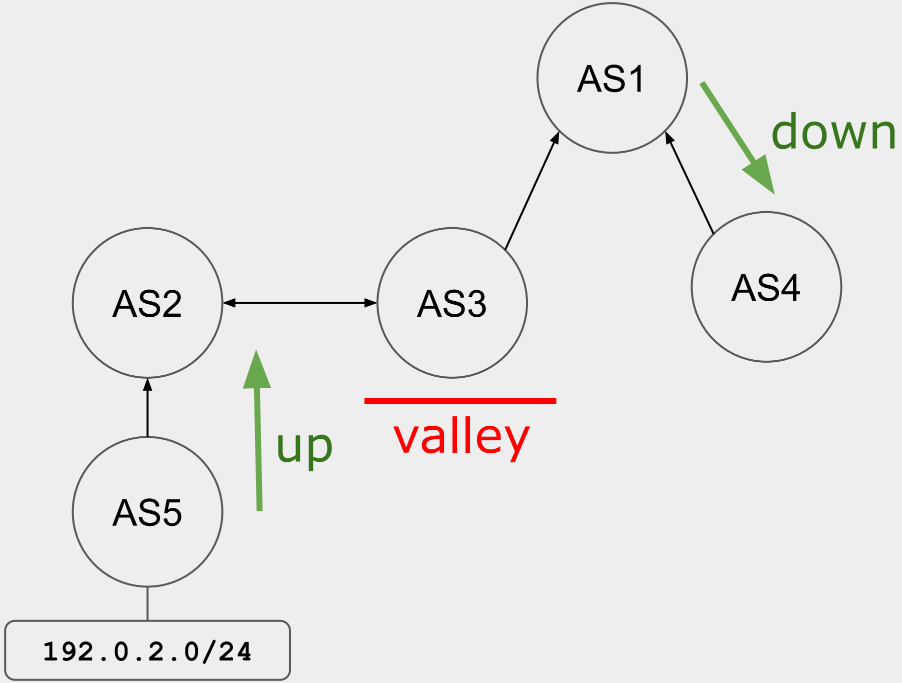
Valley Free Routing

Valley Free Examples



Valley Free Routing

Not Valley Free - Leak by adjacent peer



```
Given:
192.0.2.0/24 => AS5

AS1 => [ AS0 ] # provider free
AS2 => [ AS1 ]


AS4 sees 4 1 3 2 5 192.0.2.0/24
```

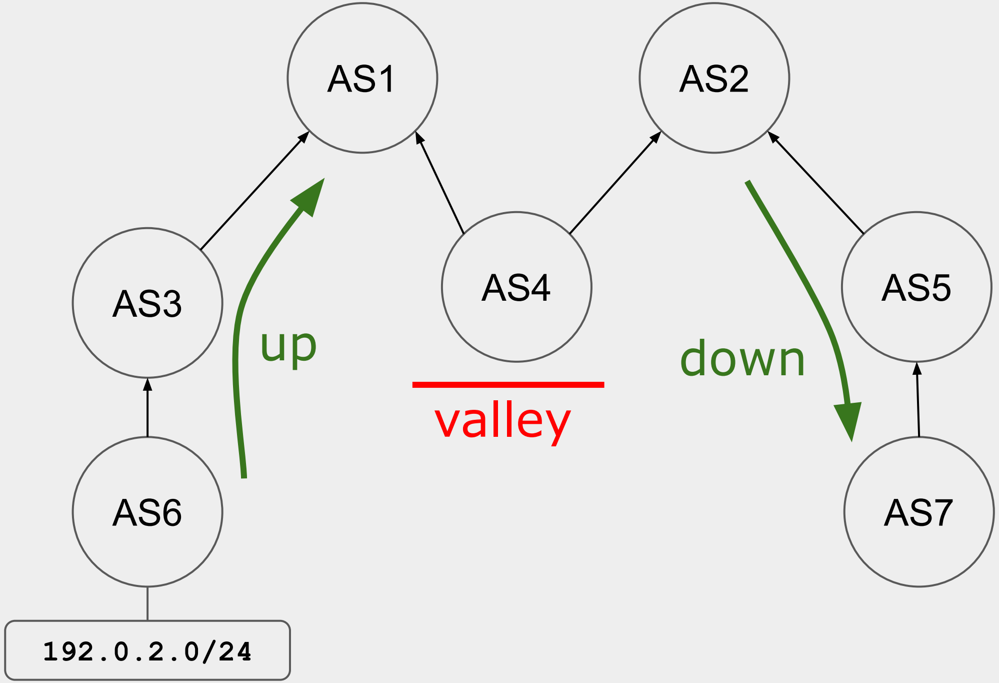
- AS3 is “Not Provider” for AS2
  Up: 2 5

- AS3 is “Not Provider” for AS1
  Down: 4 1

AS3 is a valley, therefore this is **invalid**.

Valley Free Routing

Not Valley Free - Leak to second Transit



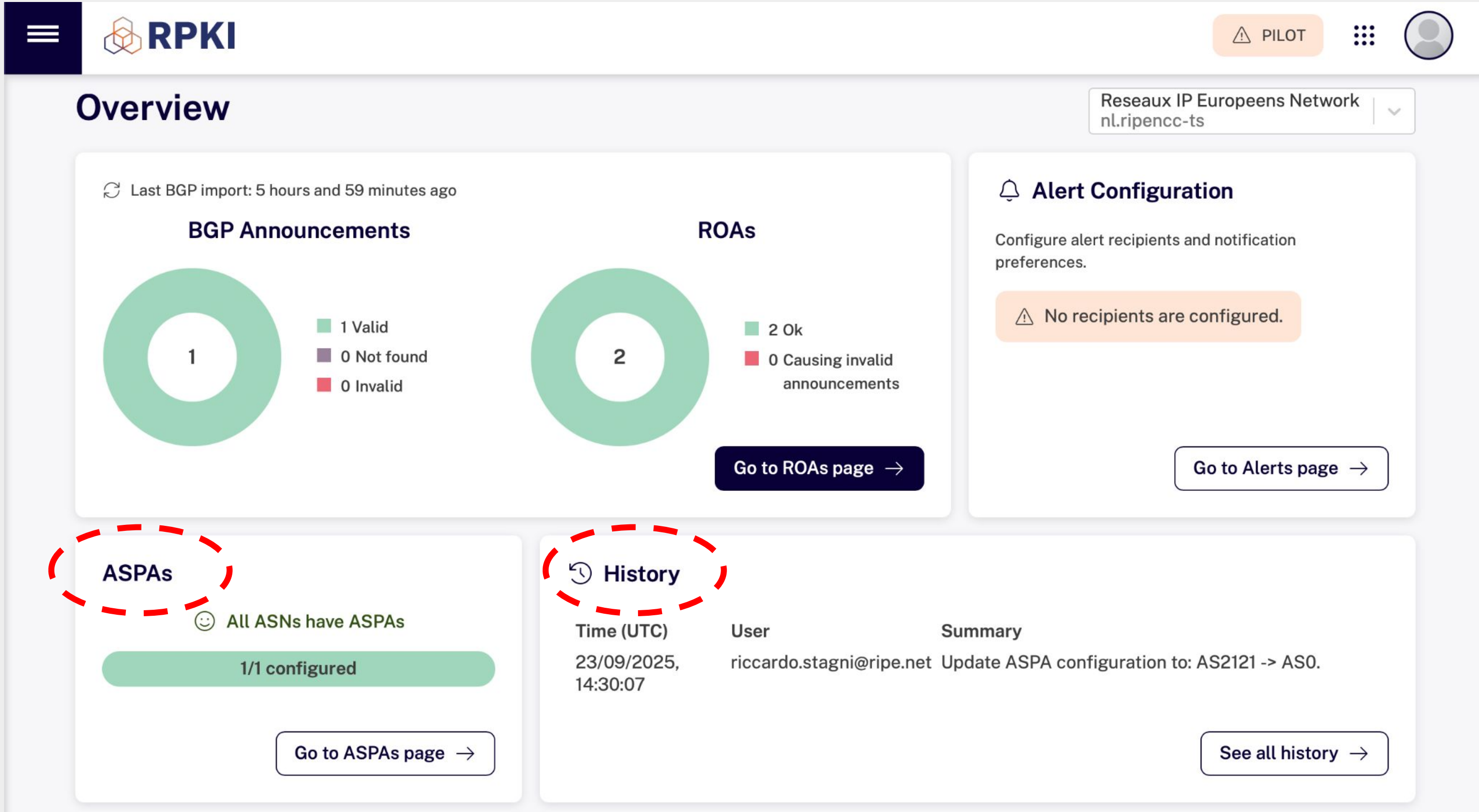
```
Given:
192.0.2.0/24 => AS6

AS1 => [ AS0 ] # provider free
AS2 => [ AS0 ] # provider free


AS5 sees 5 2 4 1 3 6 192.0.2.0/24
```

- AS4 is “Not Provider” for AS1
  Up: 1 3 6
- AS4 is “Not Provider” for AS2
  Down: 5 2

AS4 is a valley, therefore this is **invalid**.

ASPA in the RPKI Dashboard

Overview Page



Overview

Reseaux IP Europeens Network
nl.ripencc-ts

Last BGP import: 5 hours and 59 minutes ago

BGP Announcements

1

- 🟩 1 Valid
- ▨ 0 Not found
- 🟥 0 Invalid

ROAs

2

- 🟩 2 Ok
- 🟥 0 Causing invalid announcements

Alert Configuration

Configure alert recipients and notification preferences.

⚠ No recipients are configured.

ASPAs

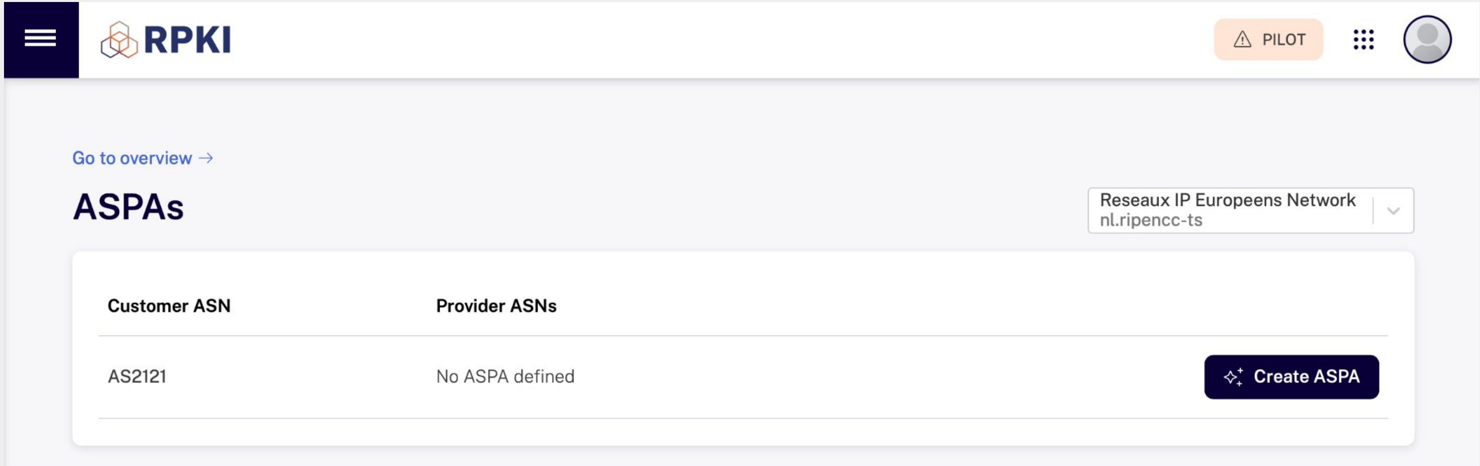
☺ All ASNs have ASPAs

1/1 configured

History

Time (UTC)	User	Summary
23/09/2025, 14:30:07	riccardo.stagni@ripe.net	Update ASPA configuration to: AS2121 -> AS0.

Manage ASPAs



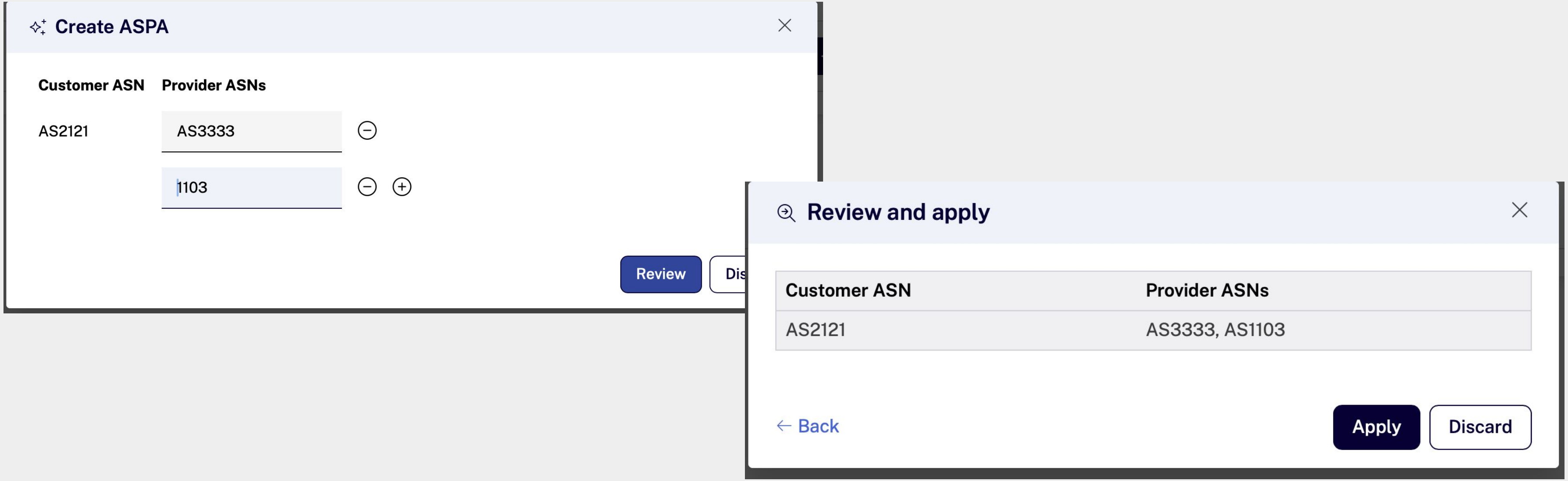
ASPAs

Reseaux IP Europeens Network
nl.ripencc-ts

Customer ASN	Provider ASNs
AS2121	No ASPA defined

ASPA configuration options are only shown for the **AS number(s) you hold**

Create / Review ASPAs



Customer ASN	Provider ASNs
AS2121	AS3333
	1103

Customer ASN	Provider ASNs
AS2121	AS3333, AS1103

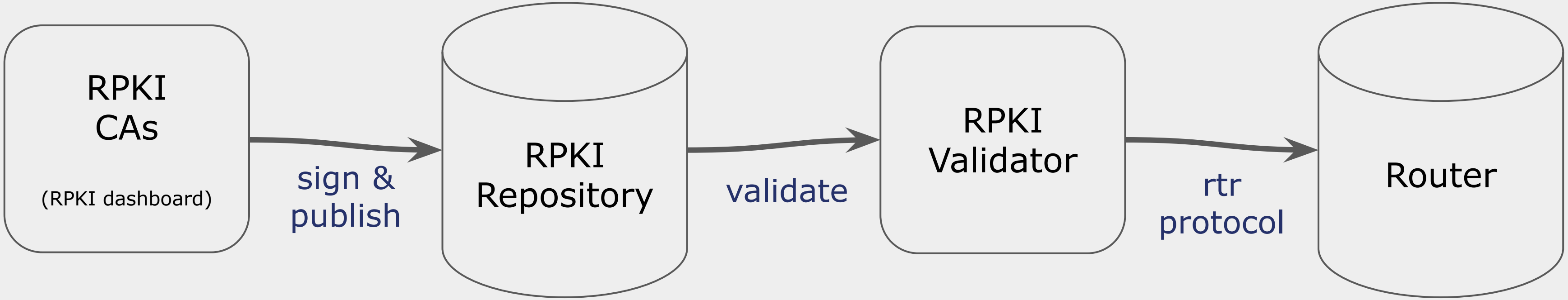
You need to check which providers to include, there are **no suggestions**

Which Providers should go on your ASPA objects?

- **All your Providers!**
  - Including **backup ones** even if they are not visible in AS path at the moment
- **Not your lateral peers**
  - Unless those peers that *can* act as your Provider
- Also include **non-transparent route servers**
  - Otherwise the non-transparent route server AS would be considered a valley
- Make this the part of your **IRR update procedure**

ASPA in the Routers

From Signing to Router



- **Same deployment model** as BGP Origin Validation
- No crypto in the router

ASPA Validation Deployment

It’s a sharp tool

- As with **BGP Origin Validation**: reject invalid, do not just lower preference
- Use “**Upstream** Path Validation” for your **customers** and **peers**
- Use “**Downstream** Path Validation” for your **providers**

But it’s early days

- Not yet available on many routers, talk to your vendor!
- Probably wise to start by logging
- Warn customers if they **did not include you as a provider**

Questions & Comments ?

✉ Ondrej.Caletka@ripe.net