



RIPE NCC
RIPE NETWORK COORDINATION CENTER

RIPE NCC RPKI Features 2025

RPKI Features at RIPE NCC in 2025



1. Now

- a. **ROA History Improvements**
- b. **ROA Config Change Alerts**
- c. **Revert to point in time**

2. Next

- a. **BGPsec Signing**
- b. **ASPA**



Features Done So Far in 2025

ROA History Improvements



History

Romeo India Echo November
nl.ripencc-ts

Show changes:

All

✓ ROA

Search history

Time (UTC)	User	Summary					Roll back
14/05/2025, 00:15:09	60c8c3af-b9a0-441e-aed9-0092bcd79559	ROA created:	AS: AS0	Prefix: 2001:67c:64:ffff:0:196:cc1b:30ee/128	Max Length: 128		
13/05/2025, 00:15:42	60c8c3af-b9a0-441e-aed9-0092bcd79559	ROA created:	AS: AS0	Prefix: 2001:67c:64:ffff:0:196:c6f4:cc93/128	Max Length: 128		
11/05/2025, 00:15:16	60c8c3af-b9a0-441e-aed9-0092bcd79559	ROA created:	AS: AS0	Prefix: 2001:67c:64:ffff:0:196:bca8:56d5/128	Max Length: 128		Roll back
10/05/2025, 00:15:29	60c8c3af-b9a0-441e-aed9-0092bcd79559	ROA created:	AS: AS0	Prefix: 2001:67c:64:ffff:0:196:b781:d26c/128	Max Length: 128		Roll back
09/05/2025,	60c8c3af-b9a0-441e-	ROA	AS:	Prefix:	Max		Roll back

Roll back all changes to the ROA configuration state up to the time before the given change. You can review and edit the changes before they are applied.

- Filter
- Search
- Formatting
- Roll back

ROA Roll Back and Review



[Go to overview](#)

History

Show changes: A

Time (UTC)	Use
14/05/2025, 00:15:09	60c aed
13/05/2025, 00:15:42	60c aed
11/05/2025, 00:15:16	60c aed
10/05/2025, 00:15:29	60c aed9-0092bcd79559

Roll back changes

The following changes will roll back your configuration to the state before the change on 13/05/2025, 00:15:42 (UTC).

		Revert to	Origin AS	Prefix	Max Length
→		Delete	AS0	2001:67c:64:ffff:0:196:cc1b:30ee/128	128
→		Delete	AS0	2001:67c:64:ffff:0:196:c6f4:cc93/128	128

Affected announcements

Origin AS	Prefix	Current status	New status
No affected announcements			


Review in pending changes

Tim Bruijnzeels | RIPE 90 | 15 May 2025

5

ROA Change Alerts





 **Alert Configuration**

Reseaux IP Europeens Network Cc
nl.ripecc-ts


Notification Preferences

Current Alerts


Recipients


opsmtg@ripe.net  


Type of alerts




Invalid announcements
If you subscribe to alerts you will receive emails about announcements for your certified resources that are not permitted by your ROAs.



Unknown announcements
Optionally, you can receive alerts about announcements for your certified resources not covered by any of your ROAs. 



ROA changes
Receive an alert if any of your ROAs are changed. 

Frequency of alert emails

☒ Daily ☐ Weekly

Receive alerts when ROA configurations change.



BGPsec

Verifiable Paths

BGPsec Router Certificate Signing



- BGPsec
 - Signed paths
 - Detect path spoofing
 - RPKI CA signs Router Certificate
 - Associate AS number with Router Key
 - Routers sign and validate
- Challenges
 - Performance, see “A Look at BGPsec Performance” by Ignas Bagdonas [@RIPE84](#)
 - Downgrades
 - Fail closed
- Why support signing BGPsec Router Certificates now?
 - Signing is the easy part
 - Support in API only
 - Help implementers improve standards



AS Provider Attestations (ASPA)

Plausible Paths



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 *Customer AS number* declares that listed *Provider AS* numbers may be seen after it in BGP paths



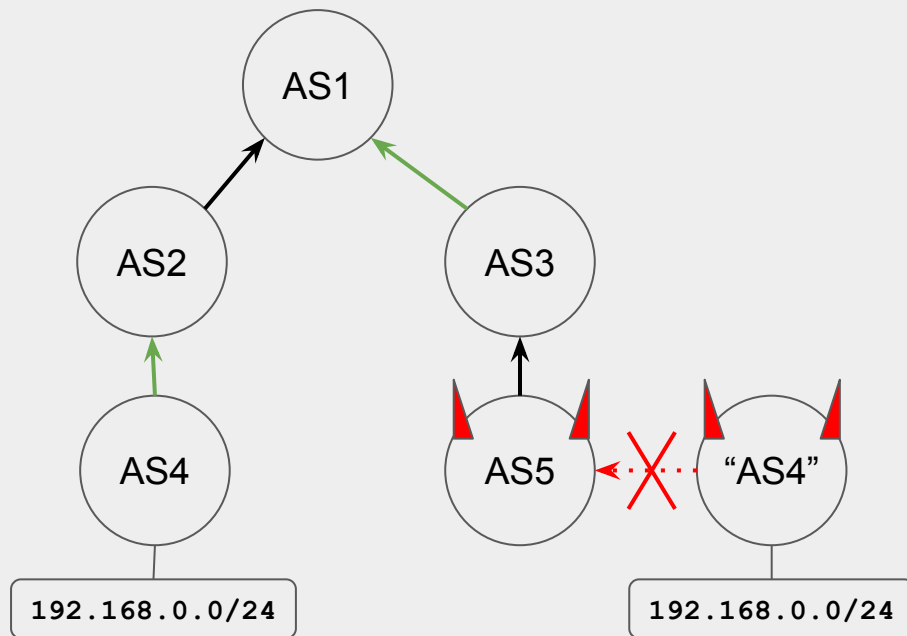
Plausible, well... *Not Implausible* Paths

- Each AS - to - AS hop is *verified* as:
 - Provider
 - Not Provider
 - No Attestation
(no ASPA exist for customer AS)
- A path from origin is plausible as long as no “Not Provider” is encountered
 - Proven unexpected hop
 - Support partial deployment
 - Fail open in case of an issue with RPKI *validation* itself

Routes learned from Customer AS networks MUST NOT have Not Provider



Partial Deployment From Customer



Consider:

192.168.0.0/24 => AS4

AS3 => [AS1]

AS4 => [AS2]

PATH 4->5->3->1

ASPA 4->~~X~~

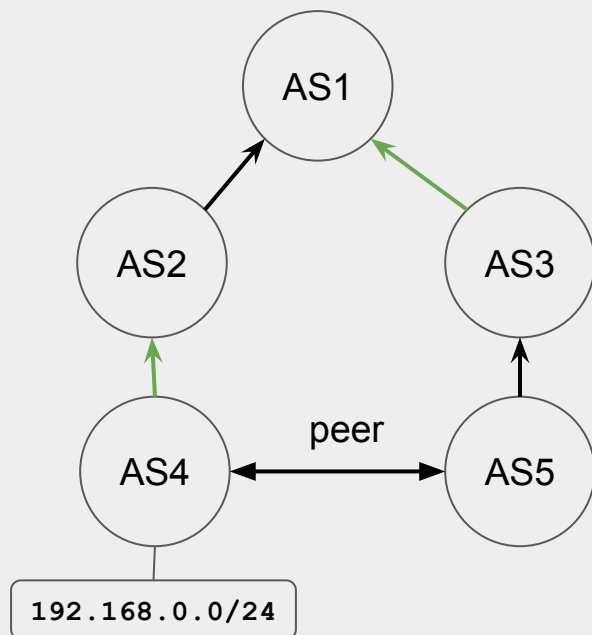
PATH 4->2->1

ASPA 4->2->1

AS1 knows that AS3 is a customer, and therefore paths MUST NOT have NOT Provider towards them.



Partial Deployment From Customer



Consider:

`192.168.0.0/24 => AS4`

`AS3 => [AS1]`

`AS4 => [AS2]`

`PATH 4->5->3->1`

`ASPA 4->X`

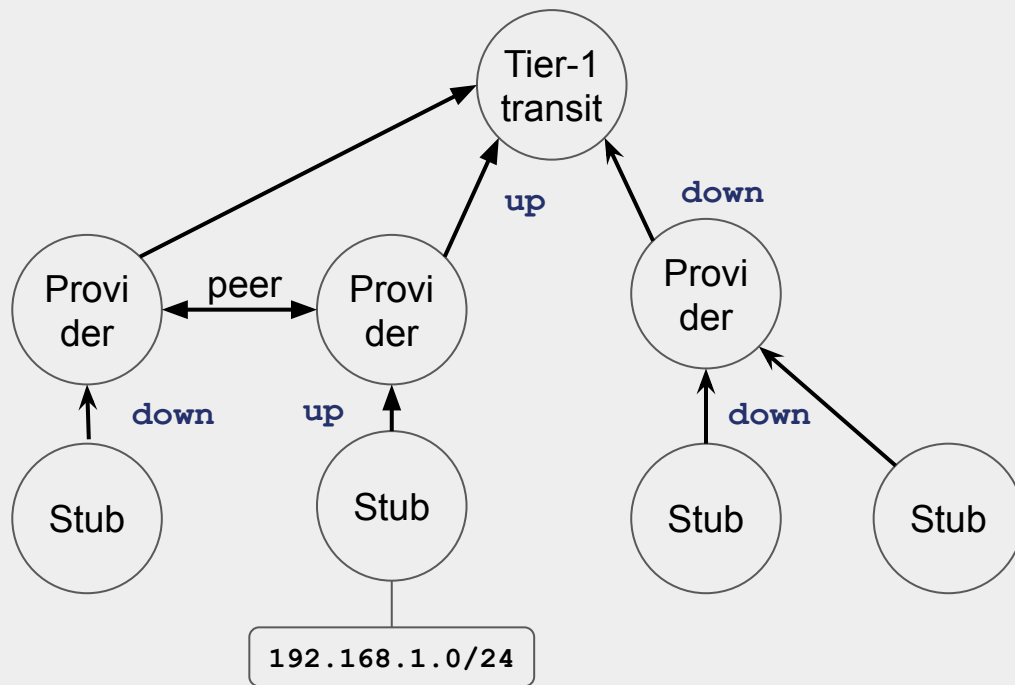
`PATH 4->2->1`

`ASPA 4->2->1`

AS1 can detect leak by AS5



Topology - "Up and Down Ramps"

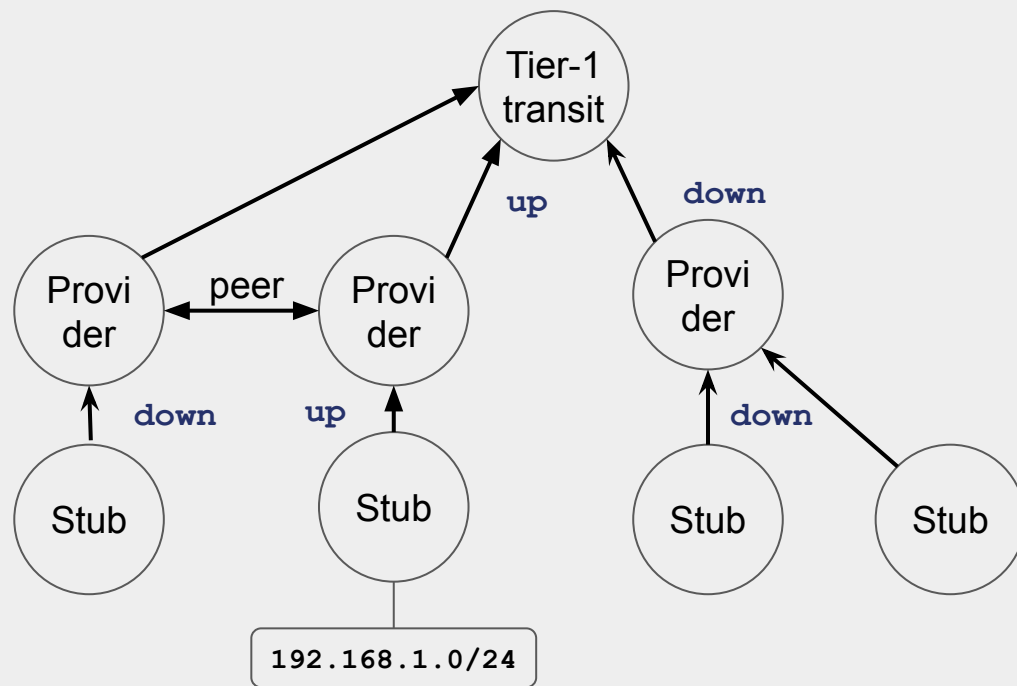


The announcement for 192.168.1.0/24 goes:

- **"up"**
customer to provider
- to a common provider apex, or peer pair
- **"down"**
reverse provider to customer



Verification: Combine Up and Down



Find the longest possible up and down ramps by looking at plausible c2p hops in the path from both ends

Valid in case up and down ramps:

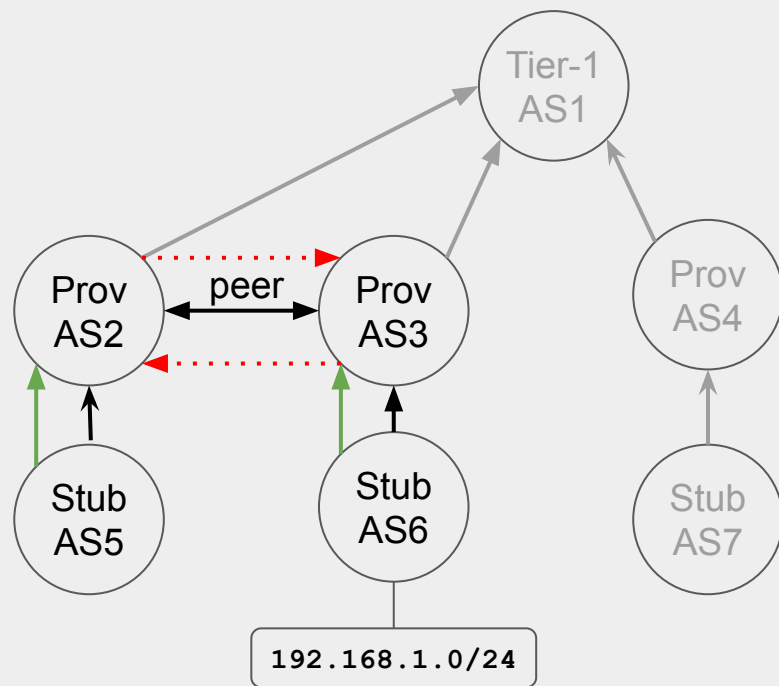
- overlap (partial deployment) - or
- meet at an apex provider - or
- meet at a peer pair (1 hop)

Invalid in case up and down ramps:

- are separated by more than 1 hop



AS5 Verifies



Consider:

192.168.0.0/24 => AS6

AS6 => [AS3]

AS3 => [AS1]

AS2 => [AS1]

AS5 => [AS2]

PATH 6->3->2->5

UP 6->3->X

DOWN X<-2<-5

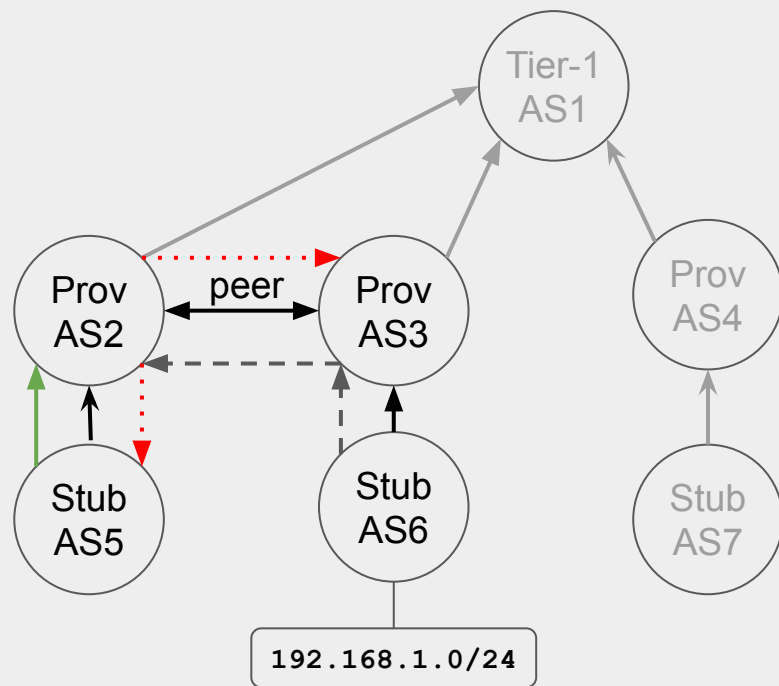
Meet at pair AS2-AS3

Accept :D

NOTE: Think IX peers



AS5 Verifies



Consider:

192.168.0.0/24 => AS6

~~AS6~~ => [~~AS3~~]

AS5 => [AS2]

AS2 => [AS1]

~~AS3~~ => [~~AS1~~]

PATH 6->3->2->5

UP 6->3->2->~~X~~

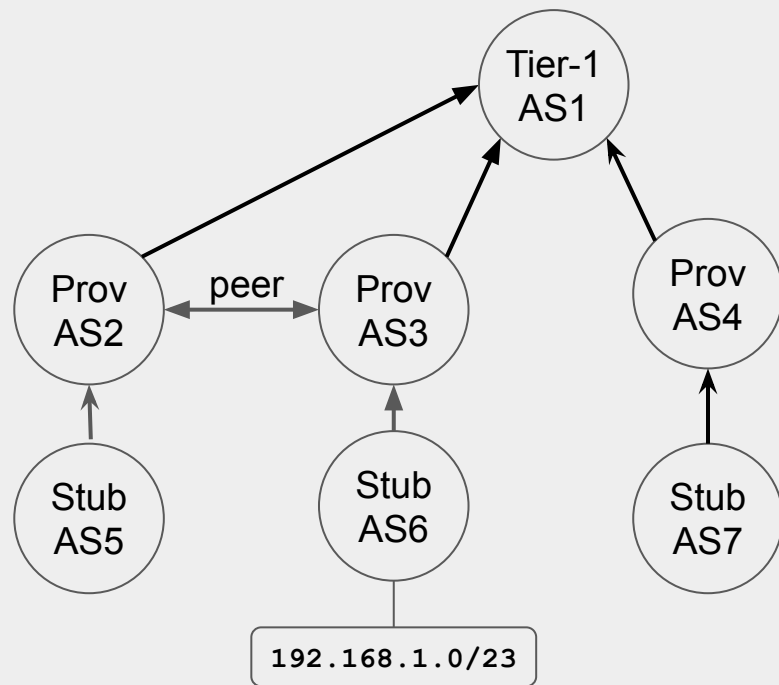
DOWN ~~X~~<-2<-5

Meet at AS2

Accept :D



AS5 Verifies



Consider:

$192.168.0.0/23-24 \Rightarrow AS6$

$AS5 \Rightarrow [AS2]$

PATH $6 \rightarrow 3 \rightarrow 2 \rightarrow 5$

UP $6 \rightarrow 3 \rightarrow 2 \rightarrow 5$

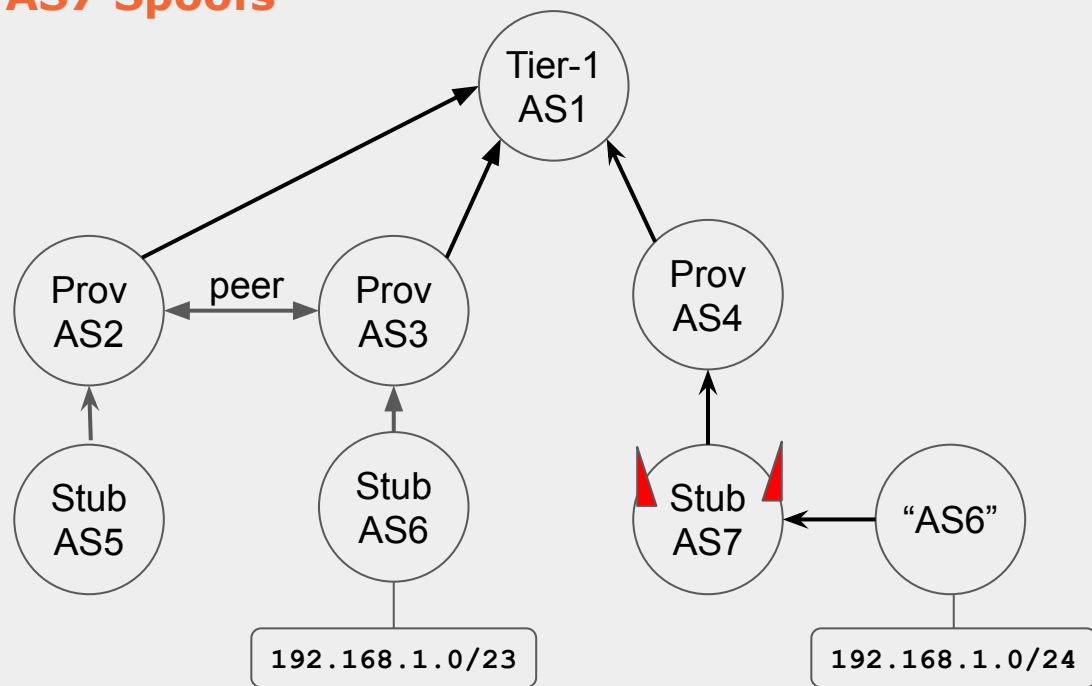
DOWN $6 \leftarrow 3 \leftarrow 2 \leftarrow 5$

Paths overlap
(no conflicting attestations)

Accept :D



AS5 Verifies AS7 Spoofs



Consider:

$192.168.0.0/23-24 \Rightarrow \text{AS6}$

$\text{AS5} \Rightarrow [\text{AS2}]$

PATH $192.168.0.0/24$
 $6 \rightarrow 7 \rightarrow 4 \rightarrow 1 \rightarrow 2 \rightarrow 5$

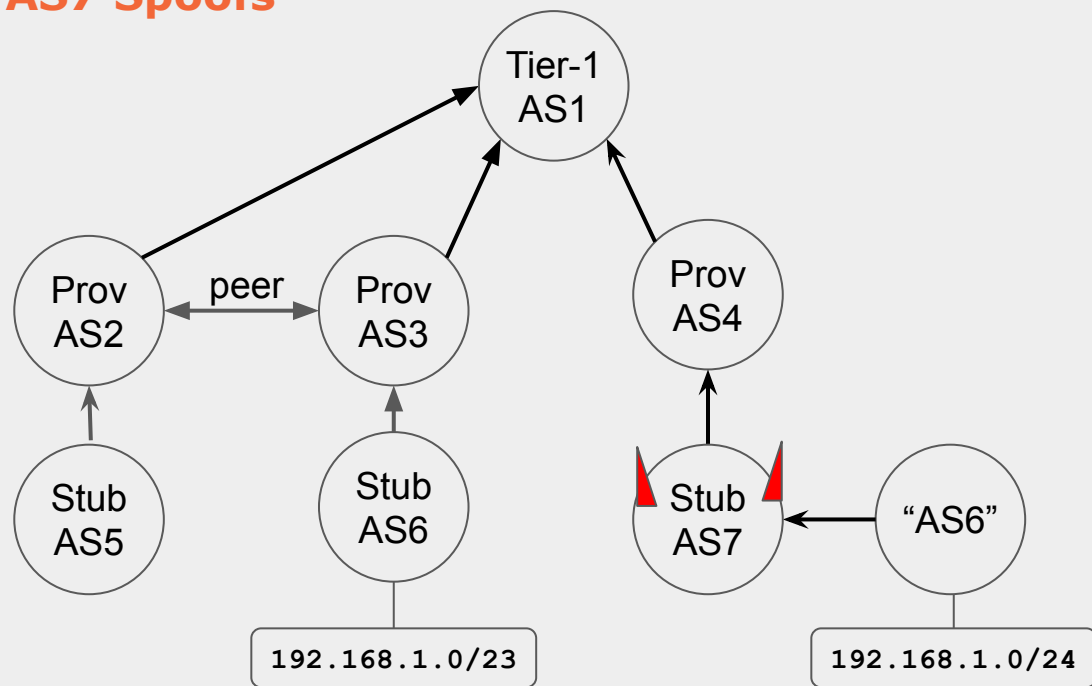
UP $6 \rightarrow 7 \rightarrow 4 \rightarrow 1 \rightarrow 2 \rightarrow 5$
DOWN $6 \leftarrow 7 \leftarrow 4 \leftarrow 1 \leftarrow 2 \leftarrow 5$

(no ASPAs disagree)

Accept more specific hijack :(



AS5 Verifies AS7 Spoofs



Consider:

192.168.0.0/23-24 => AS6

AS5 => [AS2]

+ AS6 => [AS3]

PATH 192.168.0.0/24
6->7->4->1->2->5

UP 6->X

DOWN 6<-7<-4<-1<-2<-5

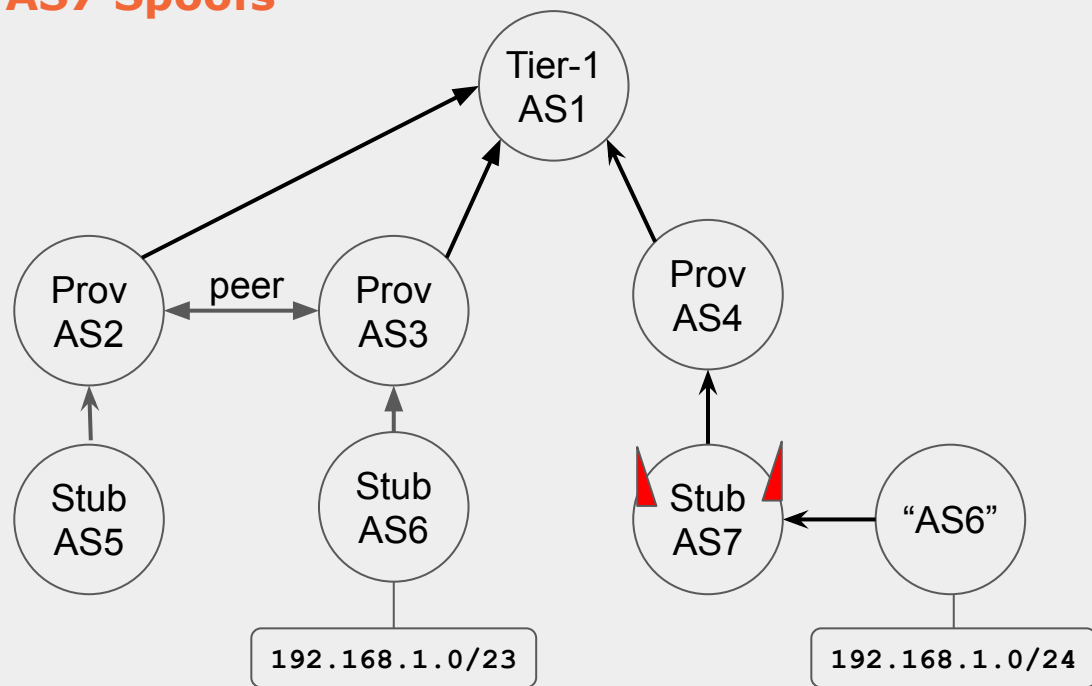
Accept, despite AS6 ASPA

Also, do not use max length lightly!

ASPA Verification - Provider - More, More Deployment



AS5 Verifies AS7 Spoofs



Consider:

192.168.0.0/23-24 => AS6

AS5 => [AS2]

AS6 => [AS3]

+ AS1 => [AS0] (PROVIDER FREE)

PATH 192.168.0.0/24
6->7->4->1->2->5

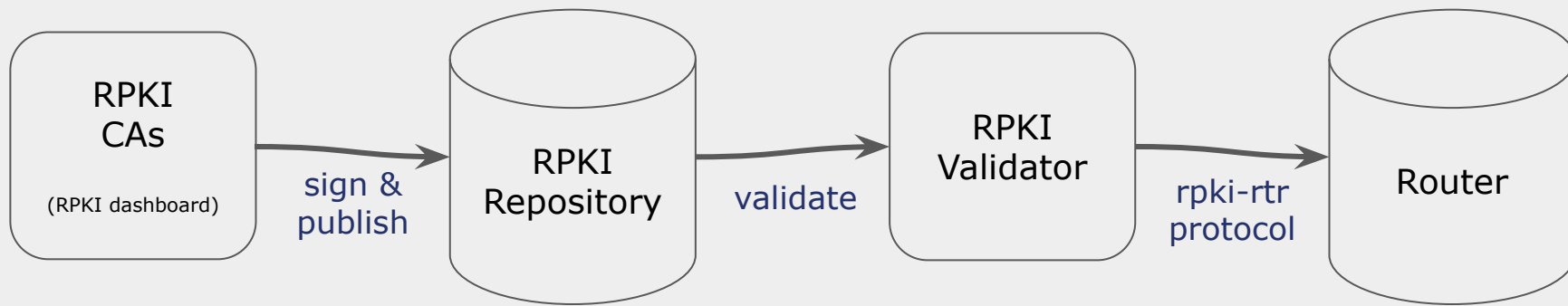
UP 6->X

DOWN X<-1<-2<-5

REJECT

**Provider/Tier-1 ASPA helps, but
AS3 should also deploy to stop AS7
spoofing -3-6-PFX**

ASPA Deployment Model



- Same deployment model as ROAs
- Crypto handled by RPKI CAs and Validators
- Router gets table with validated ASPA content (could run on modest hardware)
- IETF drafts very close to last call



- Signing
 - Krill (e.g. delegated CA under RIR)
 - RIPE NCC
 - At the moment API only test environment
- Validation
 - Routinator
 - rpki-client
- Routers
 - OpenBGPd
 - BIRD
 - Cisco is working on it



- Support in UI
- No ASPA suggestions yet
 - But planned for the future
- Talk to me or Antonella de Bellis about UX ideas!
- Plan to implement this summer
 - Testbed first (feature flag)
 - Enable in prod after IETF LC?
 - ARIN and APNIC also plan test implementations in 2025

ASPA Validation - More Reading



- ASPA Verification Draft:
<https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification>
- ASPA Examples:
https://github.com/ksriram25/IETF/blob/main/ASPA_path_verification_examples.pdf
- Formal Proof:
<https://datatracker.ietf.org/meeting/110/materials/slides-110-sidrops-sriram-aspa-alg-accuracy-01>



Questions & Comments



tbruijnzeels@ripe.net