RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RPKI Usability 2024

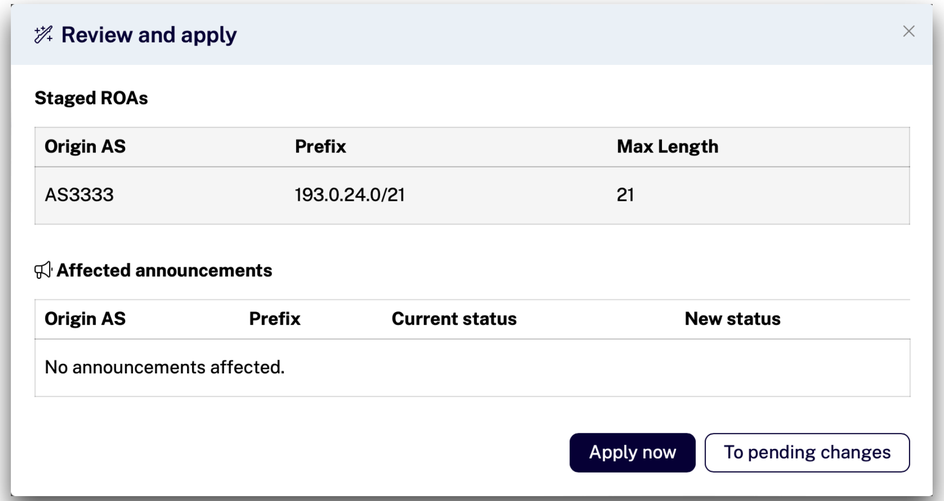
A new UI and ASPA!

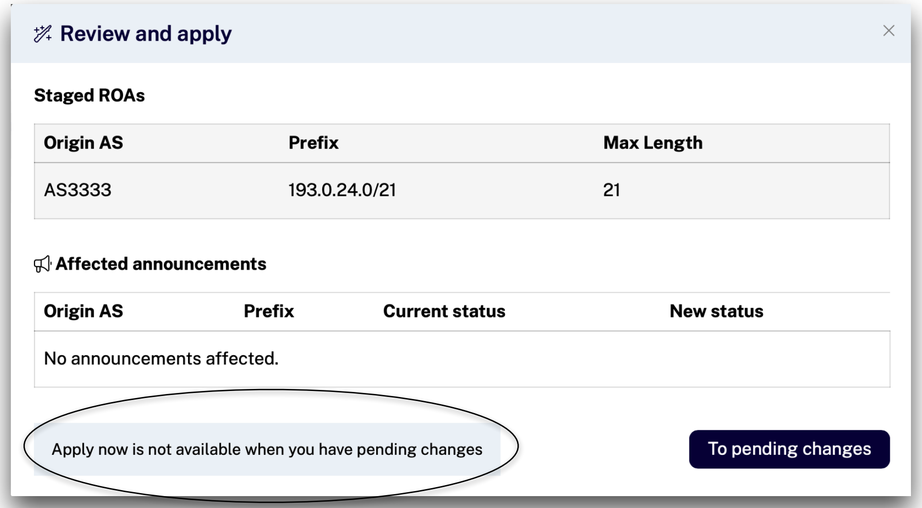
Tim Bruijnzeels | 23 April 2024 | SEE 12

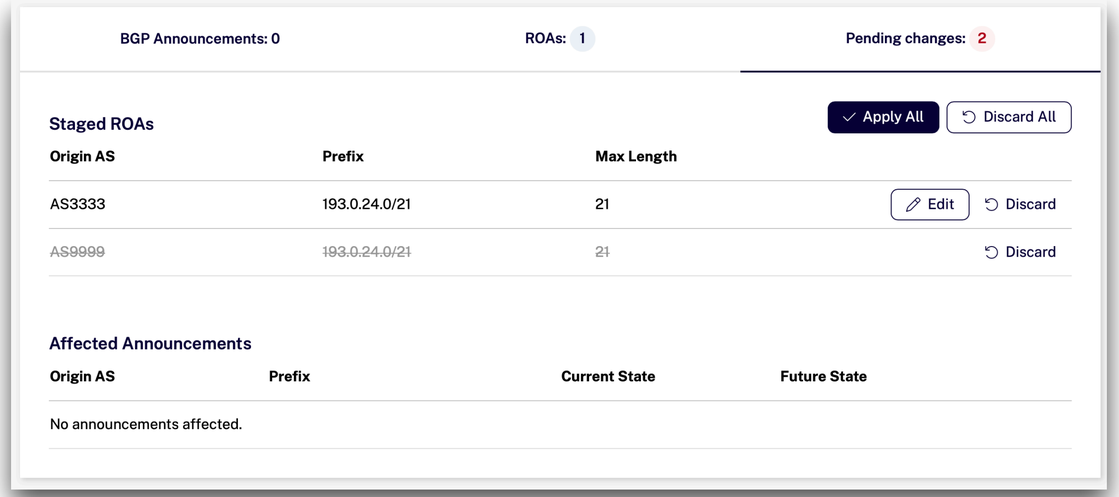
A New UI?

- Why?
  - Improve sub-optimal processes: staging ROAs, alerts, etc
  - Improve maintainability
  - Add support for new RPKI object types more easily
- How?
  - UX interviews with users
  - Incremental development alongside current UI
  - Implementation is happening right now!

For Example: Pending Changes







The Plan

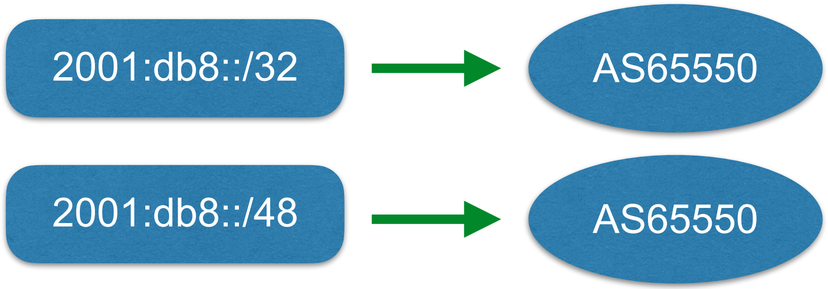
- Development is ongoing:
  - ROA support is nearly complete
  - Alerts, history, delegated (non-hosted) Certification Authorities
- Beta tests can start soon:
  - Let me know if you're interested in early testing!
- Launch when ready:
  - Feature parity
  - No known bugs
  - Summer 2024

Future Usability Work

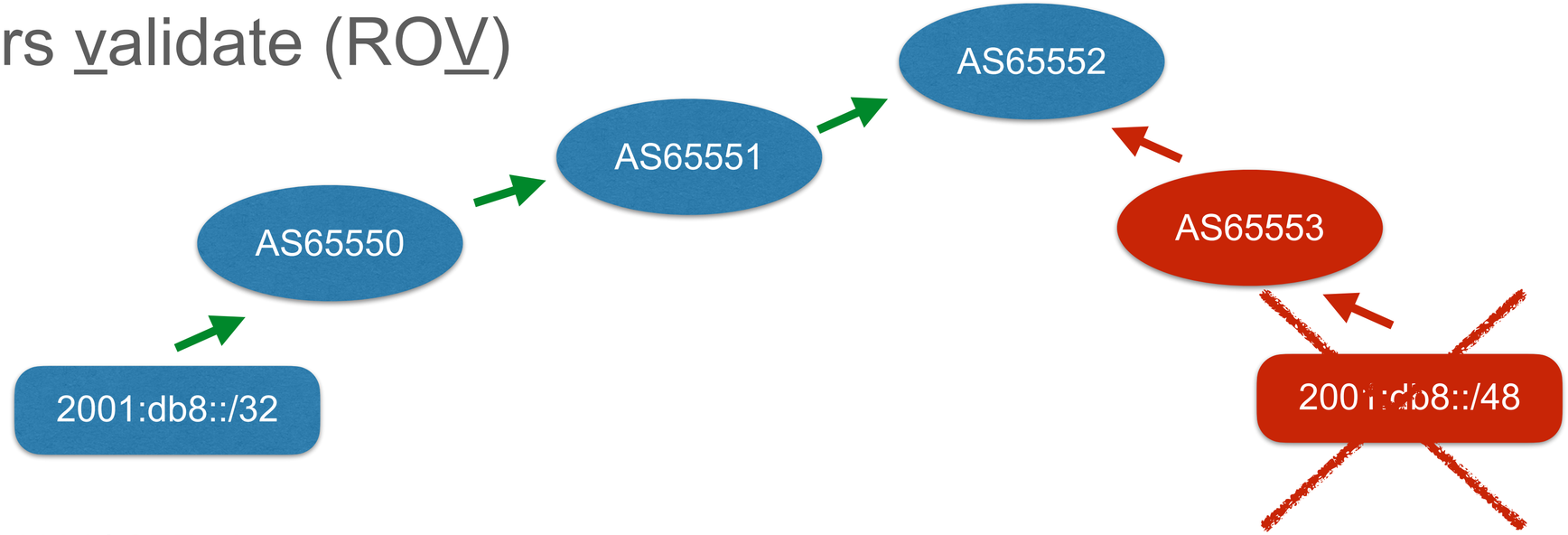
- New RPKI object types:
  - ASPA!
  - BGPSec router certificates (API)
  - Resource Signed Checklists (API)
- Faster BGP information?
  - Current BGP information is up to eight hours old
- Have an idea?
  - Anything missing?
  - Talk to me!

ROAs and ROV

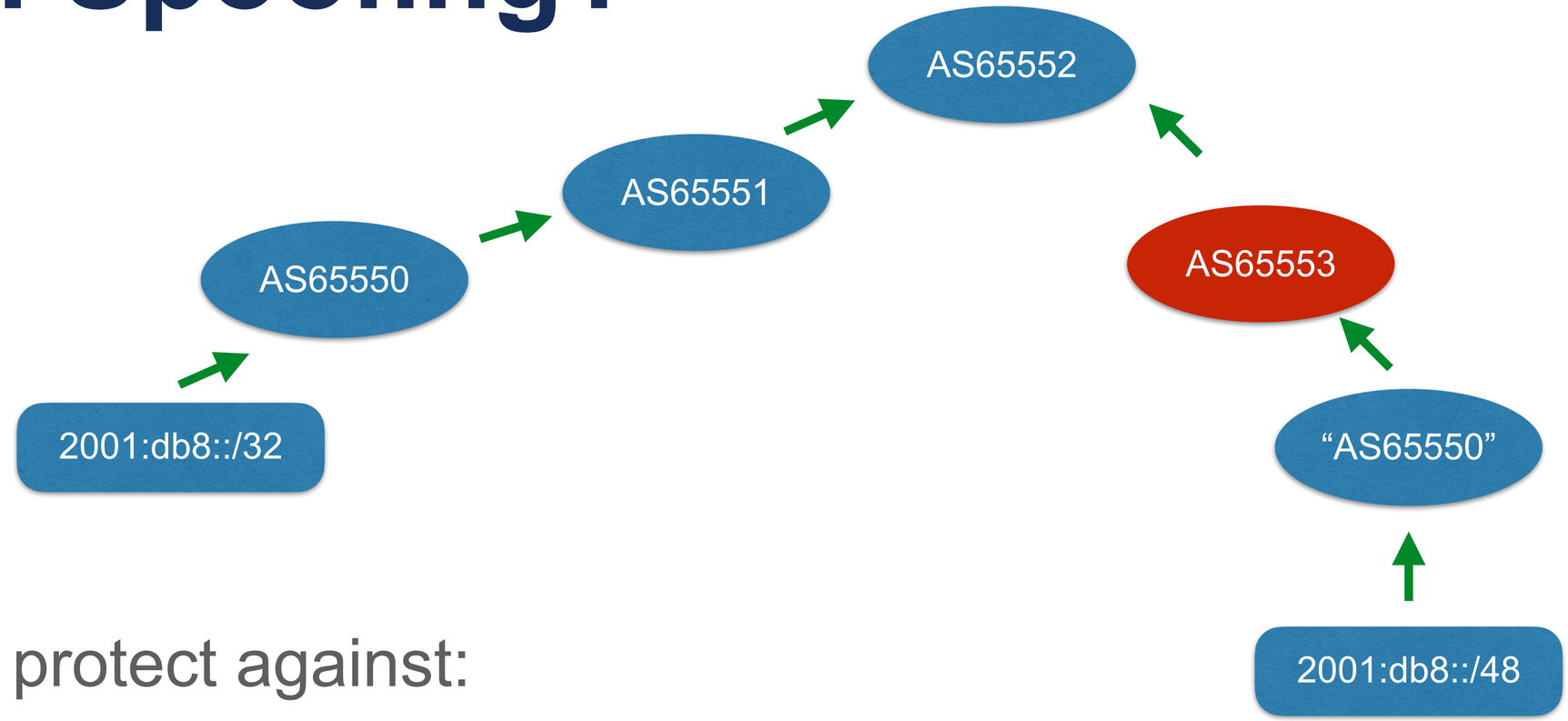
- Let prefix holders authorise (ROA)



- Let operators validate (ROV)



Path Spoofing?



- ROAs protect against:
  - Typos
  - Hijack attempts without spoofing
  - Hijack attempts where a provider knows which ASNs to allow

RPKI Beyond ROV

- ASPA
  - Detect route leaks
  - Designed for incremental deployment
  - Describe **plausible** hops in the AS path
  - Declare provider ASNs for your (customer's) ASN
  - RPKI object **signed** by an ASN holder
  - Crypto handled by RPKI validator
  - Router knows the provider ASNs for customer ASNs

Alternatives to ASPA?

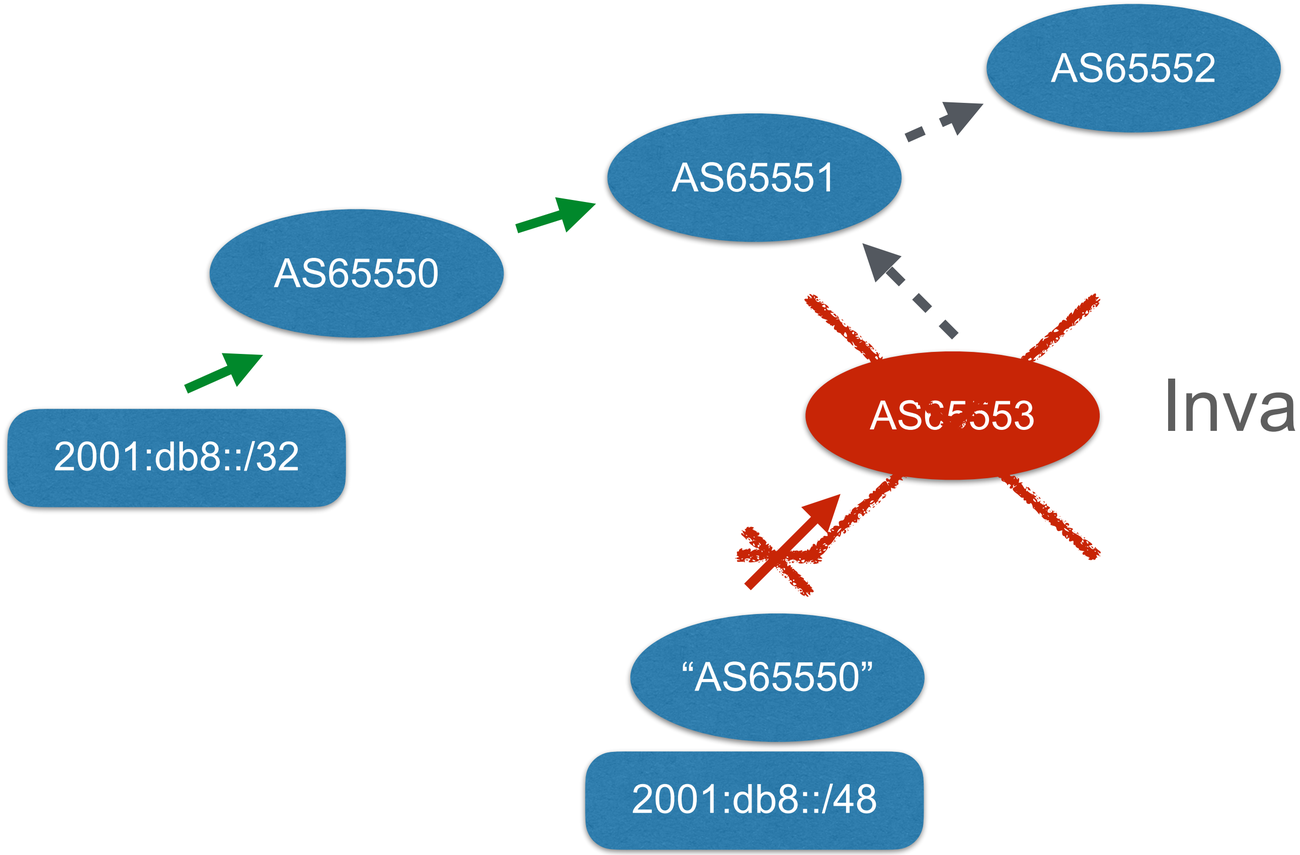
- BGPSec
  - Routers have keys, sign and validate updates
  - Designed to solve a **different** issue:
    - Protects against insertions in the BGP path
    - Does not deal with leaks
- Peerlock
  - No signatures (different system, not in RPKI)
  - Harder to scale
  - Not that easy to maintain (regexes)

How Does It Work?

- Formal explanations:
  - IETF draft: draft-ietf-sidrops-aspa-verification
  - Formal proof of correctness: https://datatracker.ietf.org/meeting/110/materials/slides-110-sidrops-sriram-aspa-alg-accuracy-01
  - In-depth presentation by Ben Maddison: https://livestream.com/internetsociety/afpif2023/videos/237341493

- The gist of it:
  - Valley free routing (multiple transits)
  - Clearly flag invalid relations
  - Let’s look at examples…

Example: From Customer/Peer



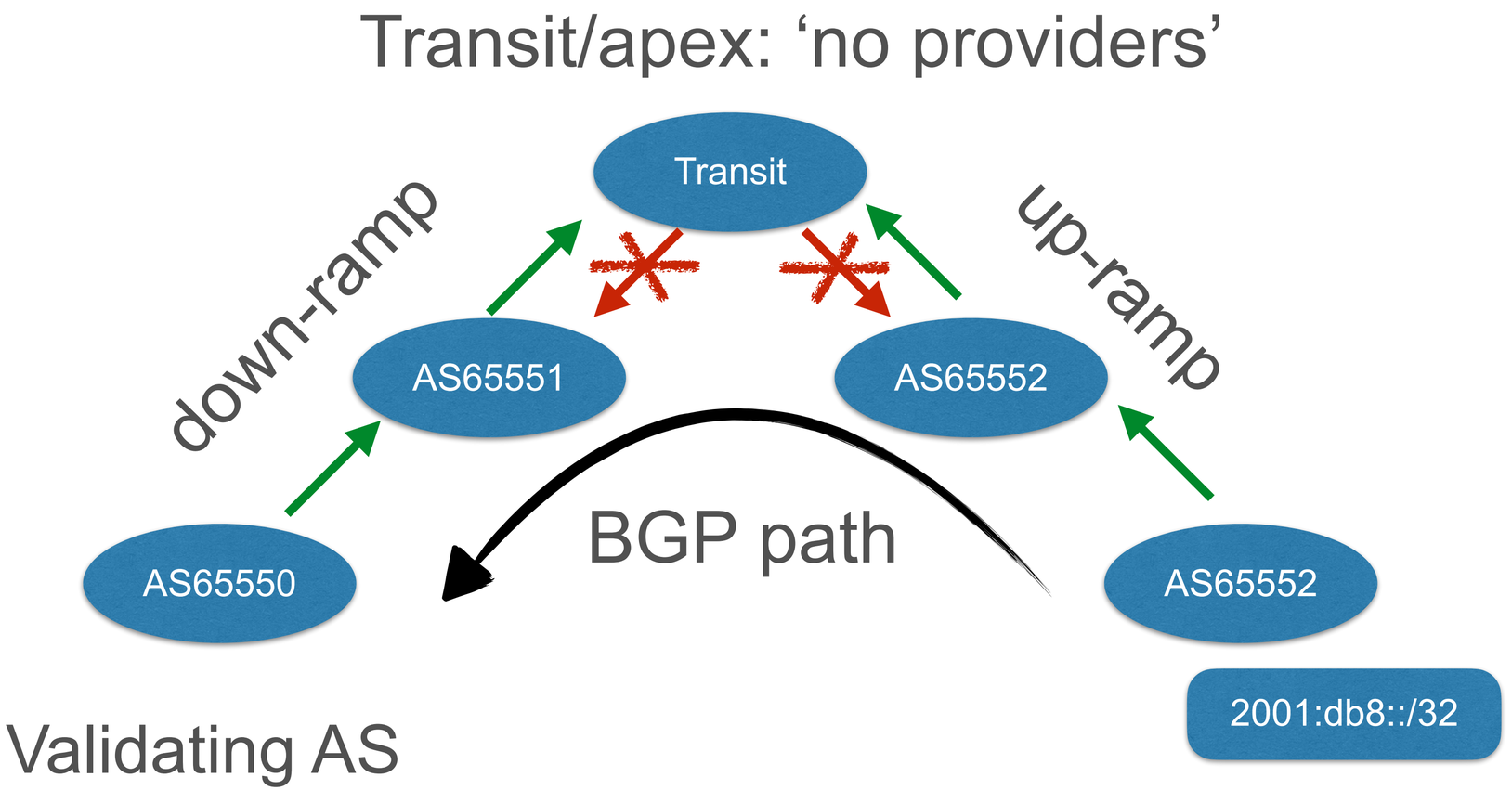
Invalid provider AS65553 rejected

provider

not provider

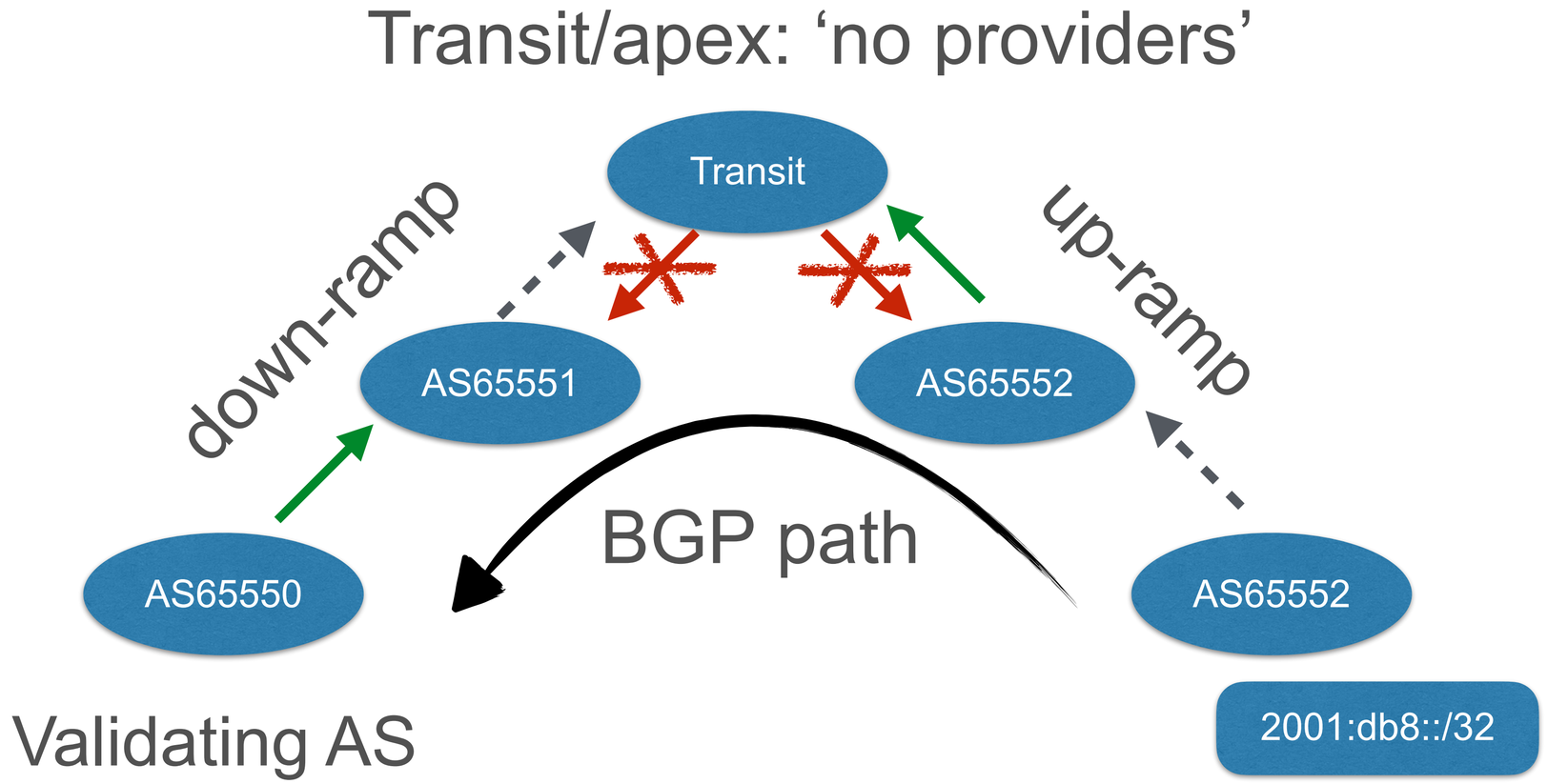
unknown

Example: Valid From Provider



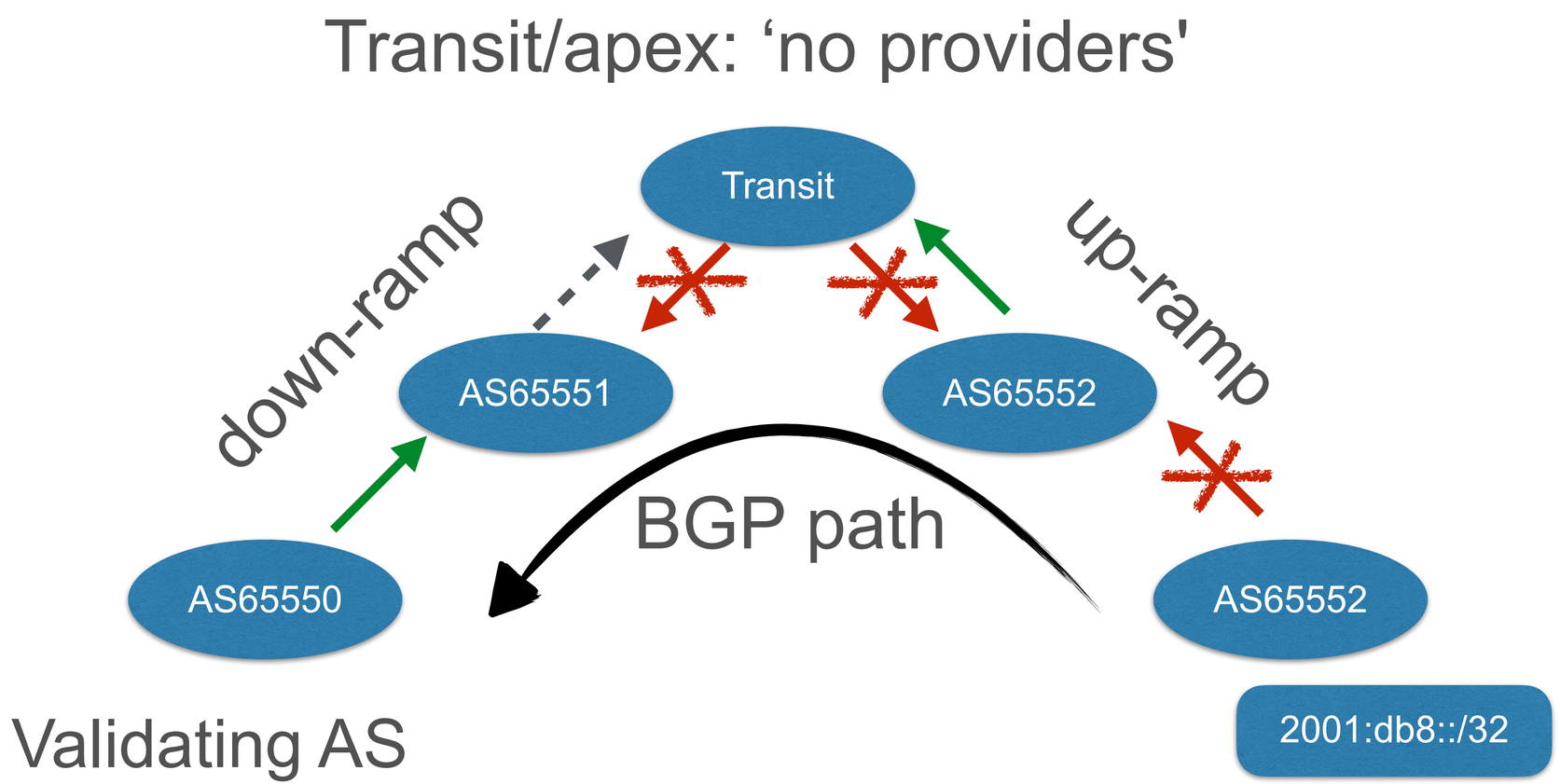
Plausible up and down and one apex

Example: Unknown From Provider



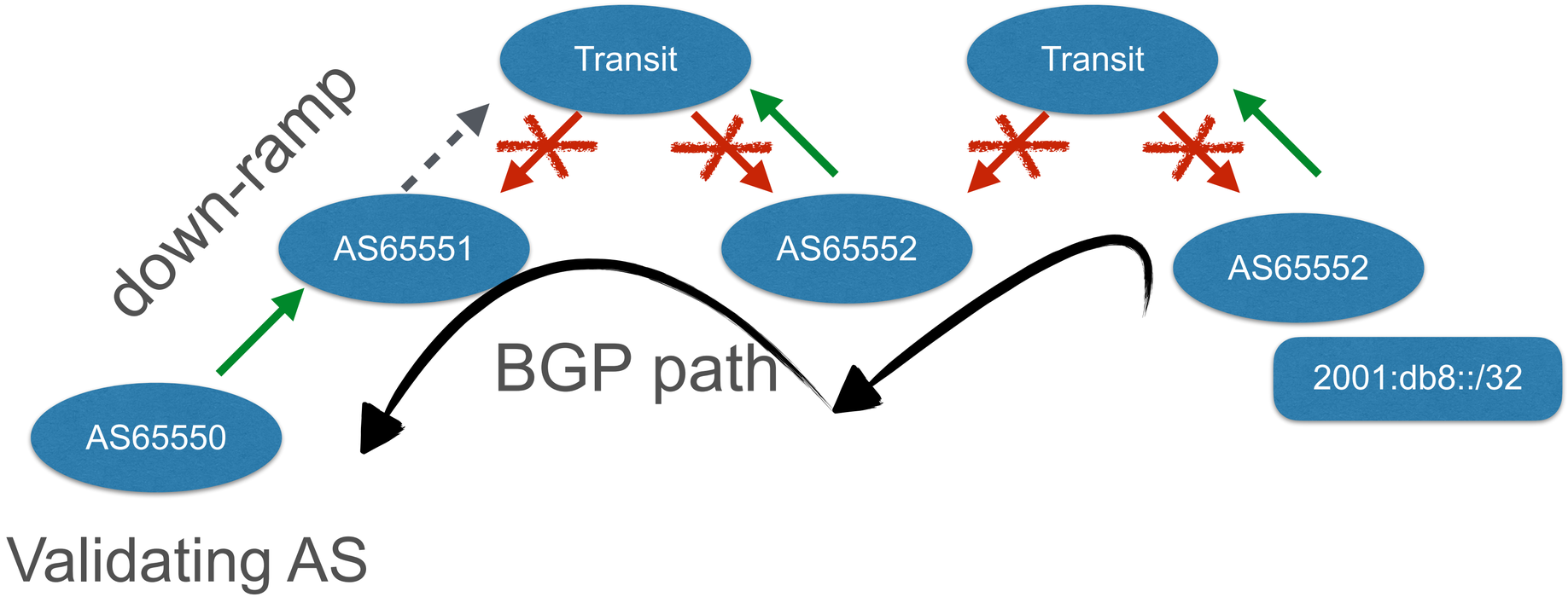
Incremental deployment

Example: Invalid From Provider



No plausible up

Example: Leak



Dual apex: valley

Is it Ready?

- IETF - Close but not yet called
- Supported in a RIPE NCC test and Krill
- RIPE NCC Hosted RPKI UI/API planned for 2024
  - After IETF last call on the profile
  - AS holder (customer) declares providers
  - Possibly give information on providers seen in BGP
- RPKI validators (routinator, rpki-client, etc)
- Routers (OpenBGPD, NIST)
  - Early adopter: Calgary Internet Exchange (YYCIX)

Questions

tbruijnzeels@ripe.net