RPKI

TMA PARIS 2019

NLNET LABS?


Purveyors of fine
open source software
since 1999

OPENDNSSEC

STUBBY

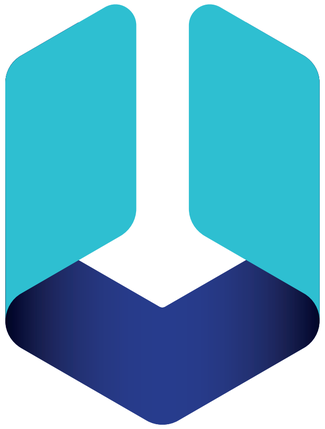
NSD

ROUTINATOR

Krill

LDNS

GETDNS



unbound

DNSTHOUGHT

DNSSEC TRIGGER

NET::DNS

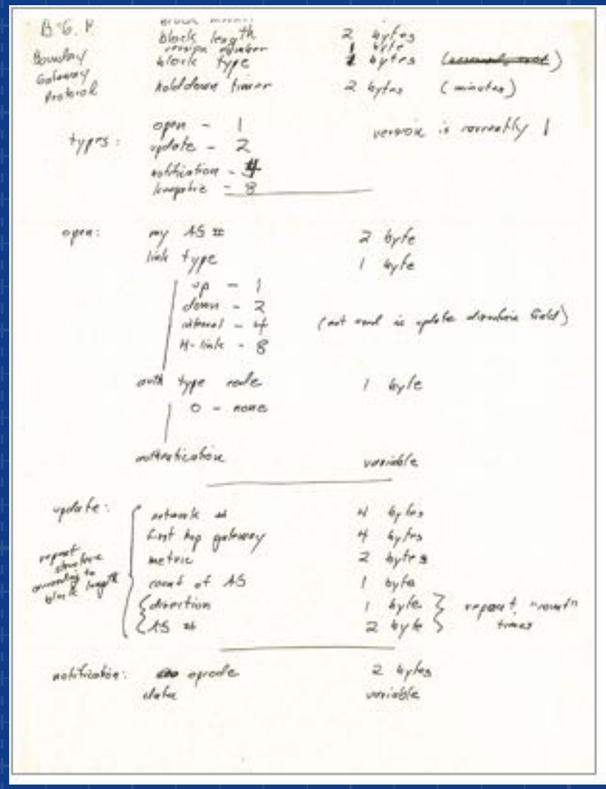
AGENDA

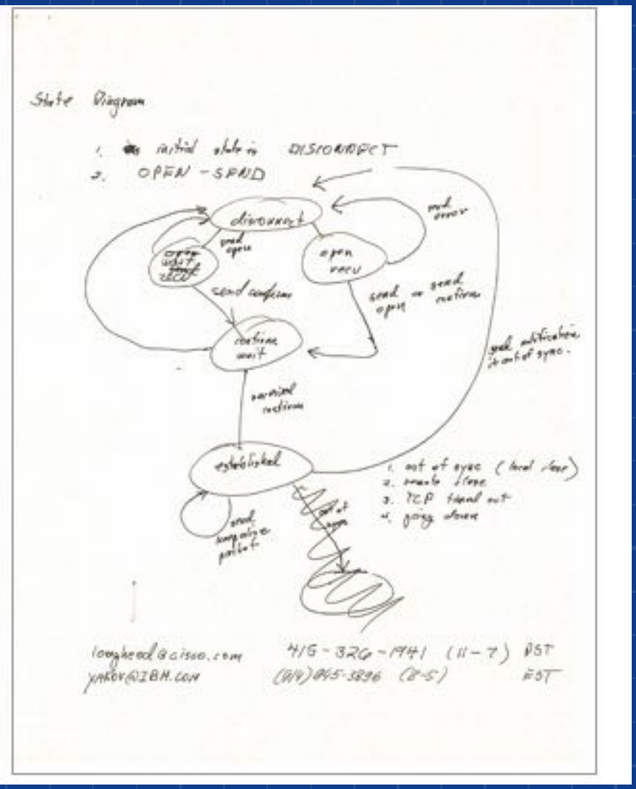
- Part 1 - Theory (1,5 hours)
  - Introduction into BGP routing concepts and RPKI
  - RPKI repository and object structure
  - RPKI uptake, data quality and future
- Part 2 - Workshop (1,5 hours)
  - Protect yourself
  - Hijack your neighbour

PART 1
INTRODUCTION

BGP?

1989





1989: RFC 1105 (BGP)
1990 RFC 1163 (BGP-2)
1991: RFC 1267 (BGP-3)
1994: RFC 1654 (BGP-4)
1995: RFC 1771 (BGP-4)
2006: RFC 4271 (BGP-4)

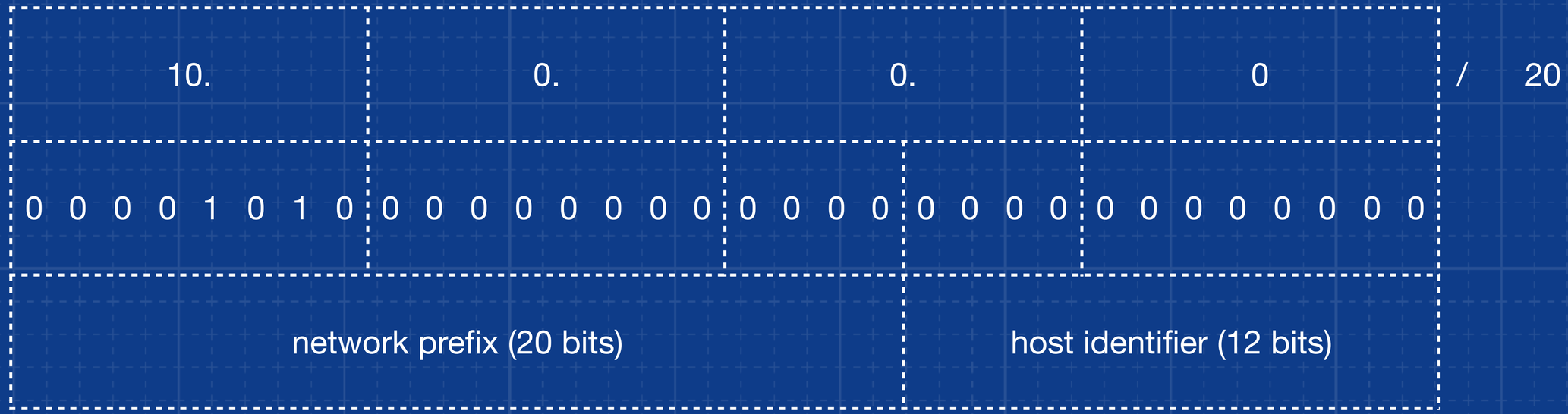
Many updates (extensions), but not obsoleted

https://weare.cisco.com/c/r/weare/amazing-stories/amazing-things/two-napkin.html

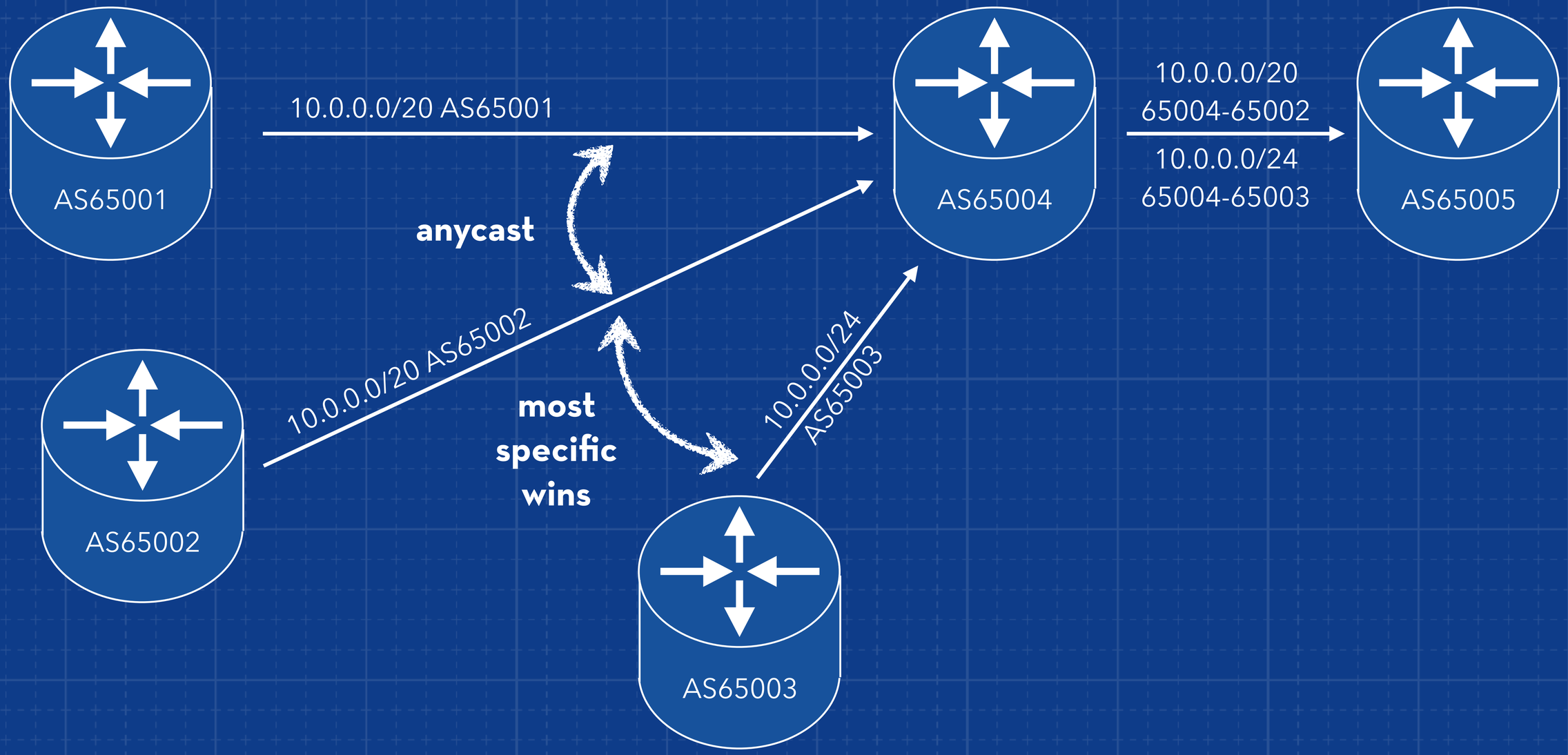
BGP

- Networks are identified by Autonomous System Numbers (AS)
- ASNs announce their own routes (IP Prefixes and own AS) to neighbours
- ASNs import routes (Prefix and AS path) from neighbours
- ASNs do best path selection
- ASNs export routes to neighbours

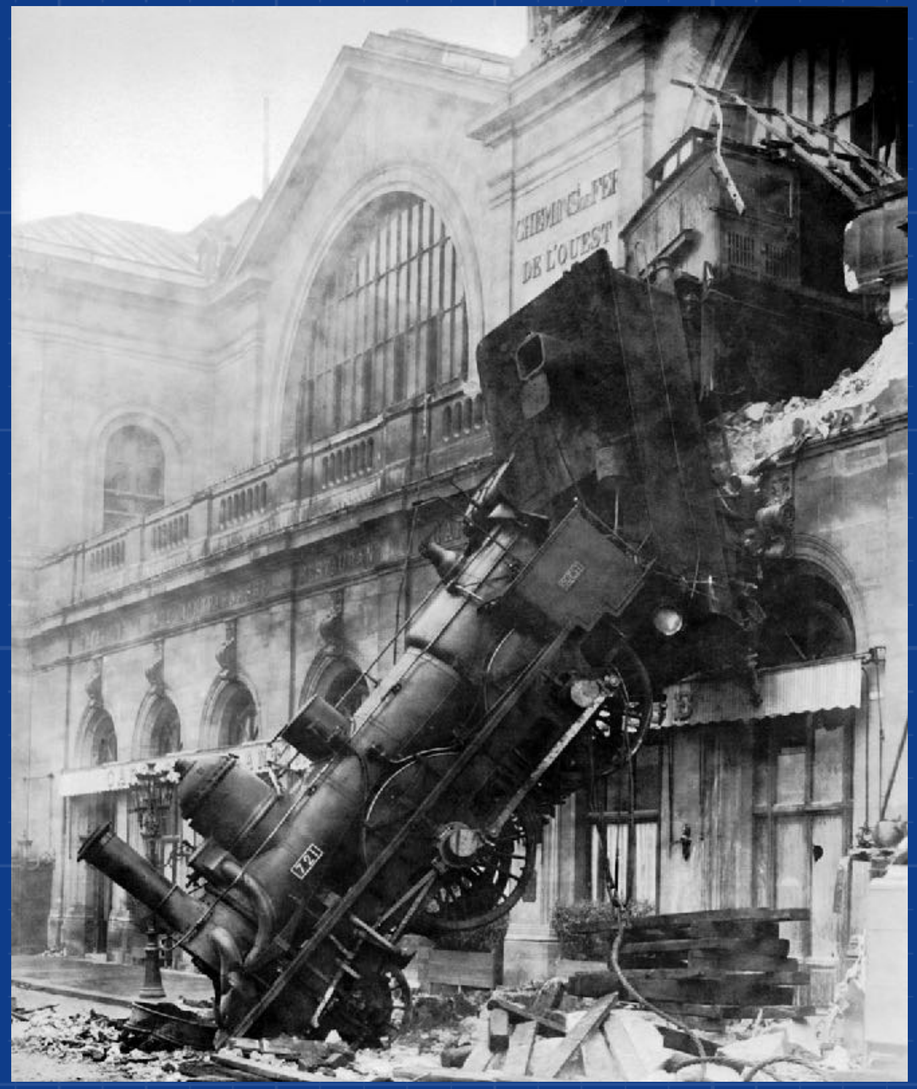
PREFIX


10.
0.
0.
0
/ 20
0 0 0 0 1 0 1 0
0 0 0 0 0 0 0 0
0 0 0 0
0 0 0 0
0 0 0 0 0 0 0 0
network prefix (20 bits)
host identifier (12 bits)

BGP BASICS

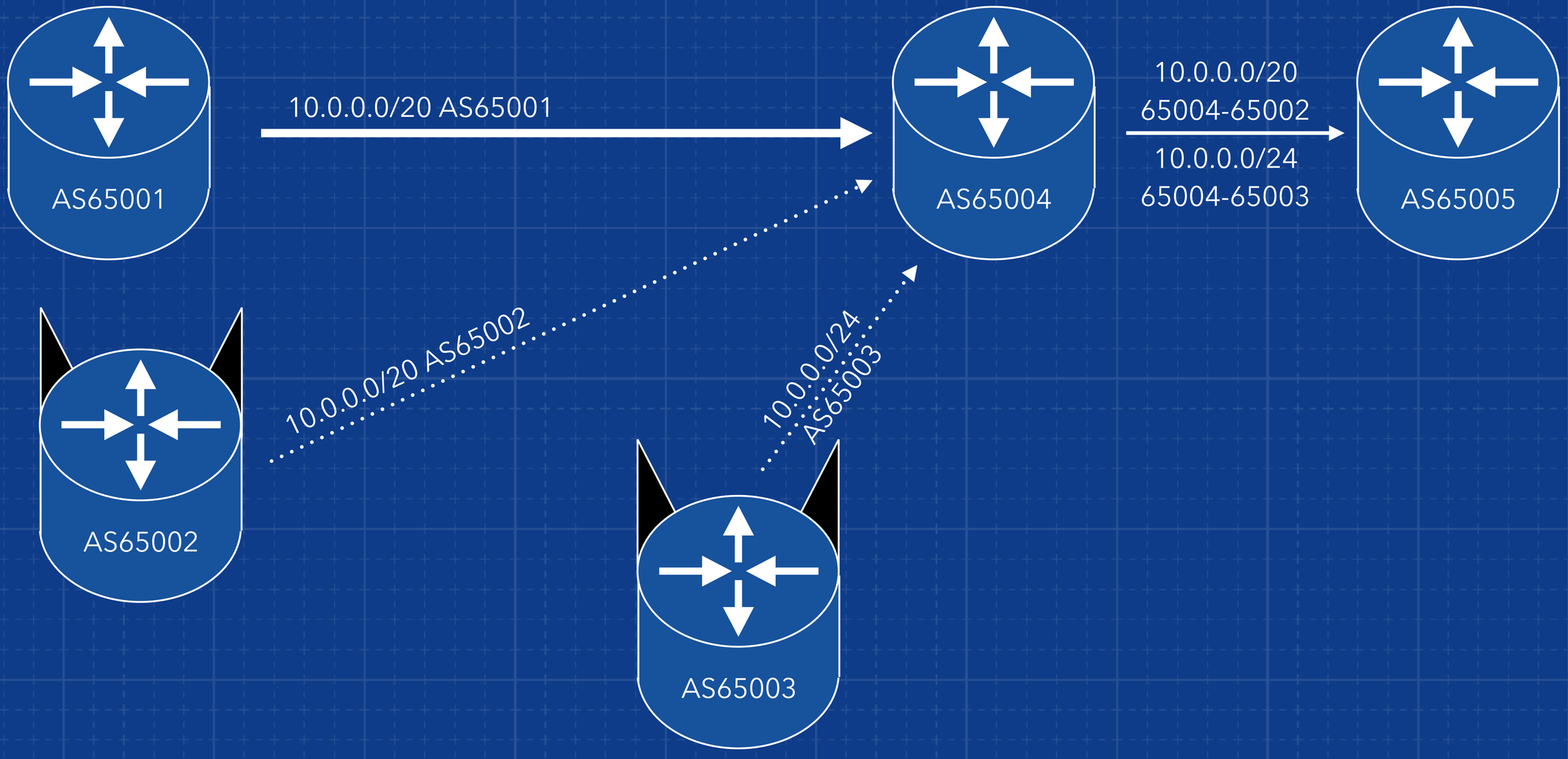

AS65001
10.0.0.0/20 AS65001
AS65004
10.0.0.0/20
65004-65002
10.0.0.0/24
65004-65003
AS65005
anycast
AS65002
10.0.0.0/20 AS65002
most
specific
wins
10.0.0.0/24
AS65003
AS65003

BGP



- Anyone can claim any ASN
- Or add any ASN anywhere in the path
- Anyone can claim any prefix as their own
- Leaking.. (should have filtered)
- The numbers on a keyboard are really close together..

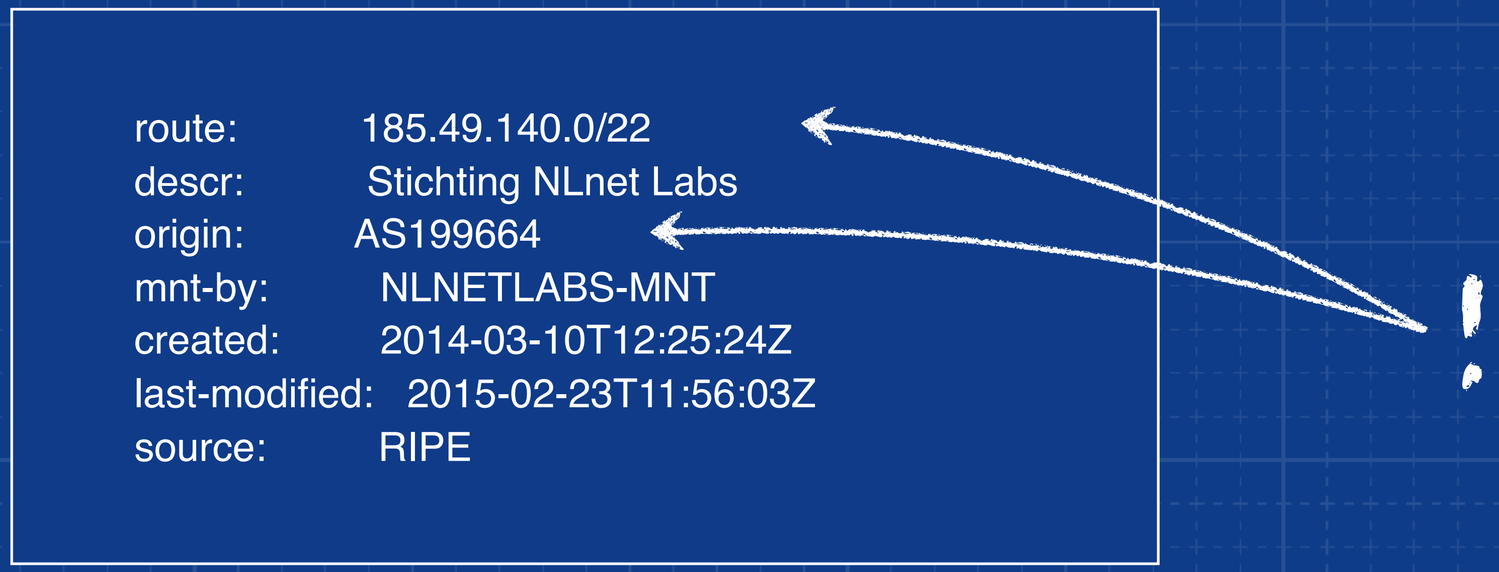
SIMPLE HIJACKS



“Is this BGP route origination authorised by the legitimate holder of the IP space?”

INTERNET ROUTING REGISTRY (IRR)

INTERNET ROUTING REGISTRY

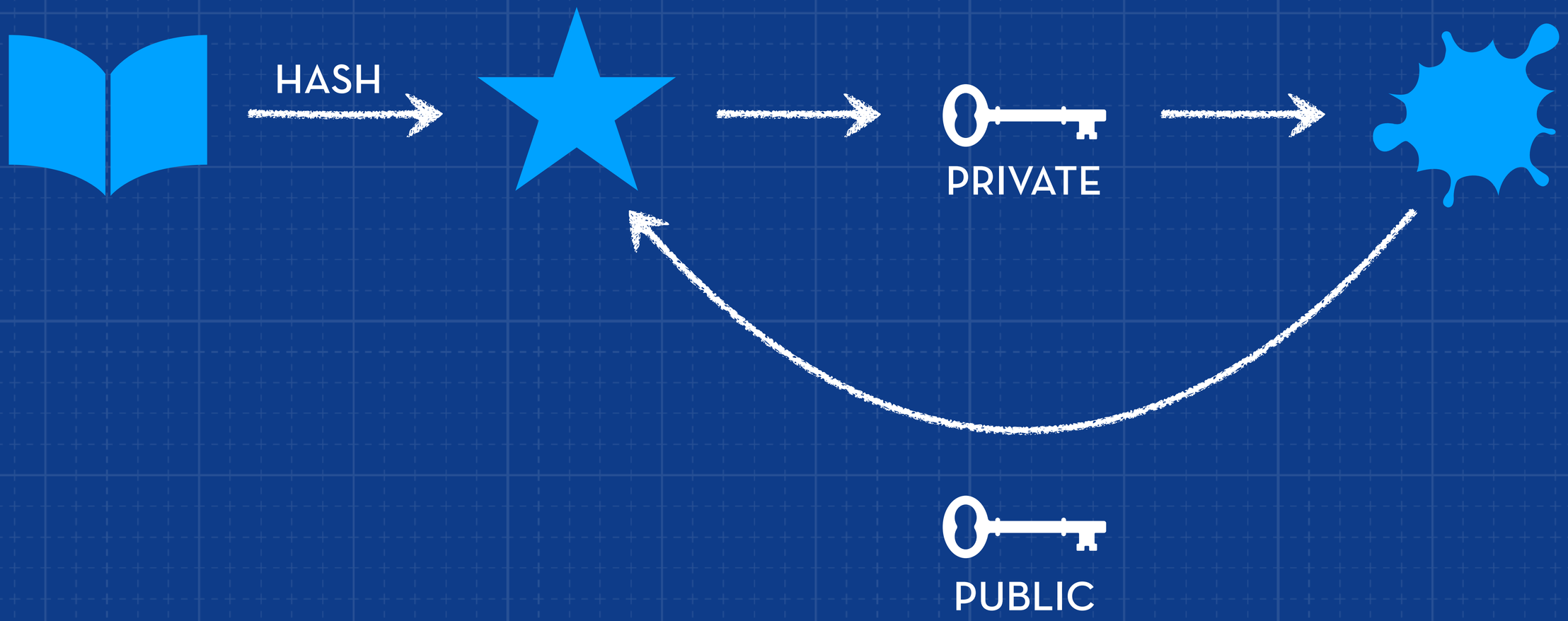


AFRINIC, ALTDB, AOLTW, APNIC, ARIN, BELL, BBOI, CANARIE, EASYNET, EPOCH, HOST, JPIRR, LEVEL3, NESTEGG, NTTCOM, OPENFACE, OTTIX, PANIX, RADB, REACH, RGNET, RIPE, RISQ, ROGERS, TC

irr.net/docs/list.html

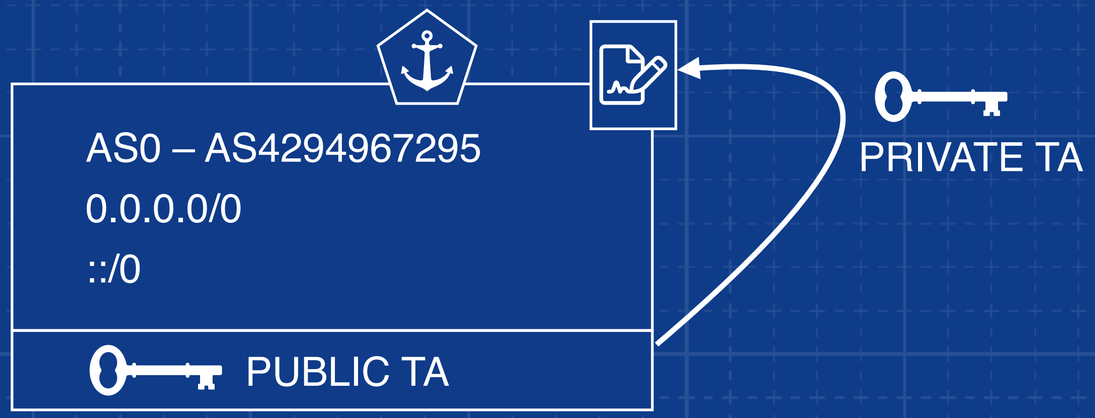
RESOURCE PUBLIC KEY INFRASTRUCTURE (RPKI)

SIGN WITH ASYMMETRIC KEYS



“How does one learn about public keys?”

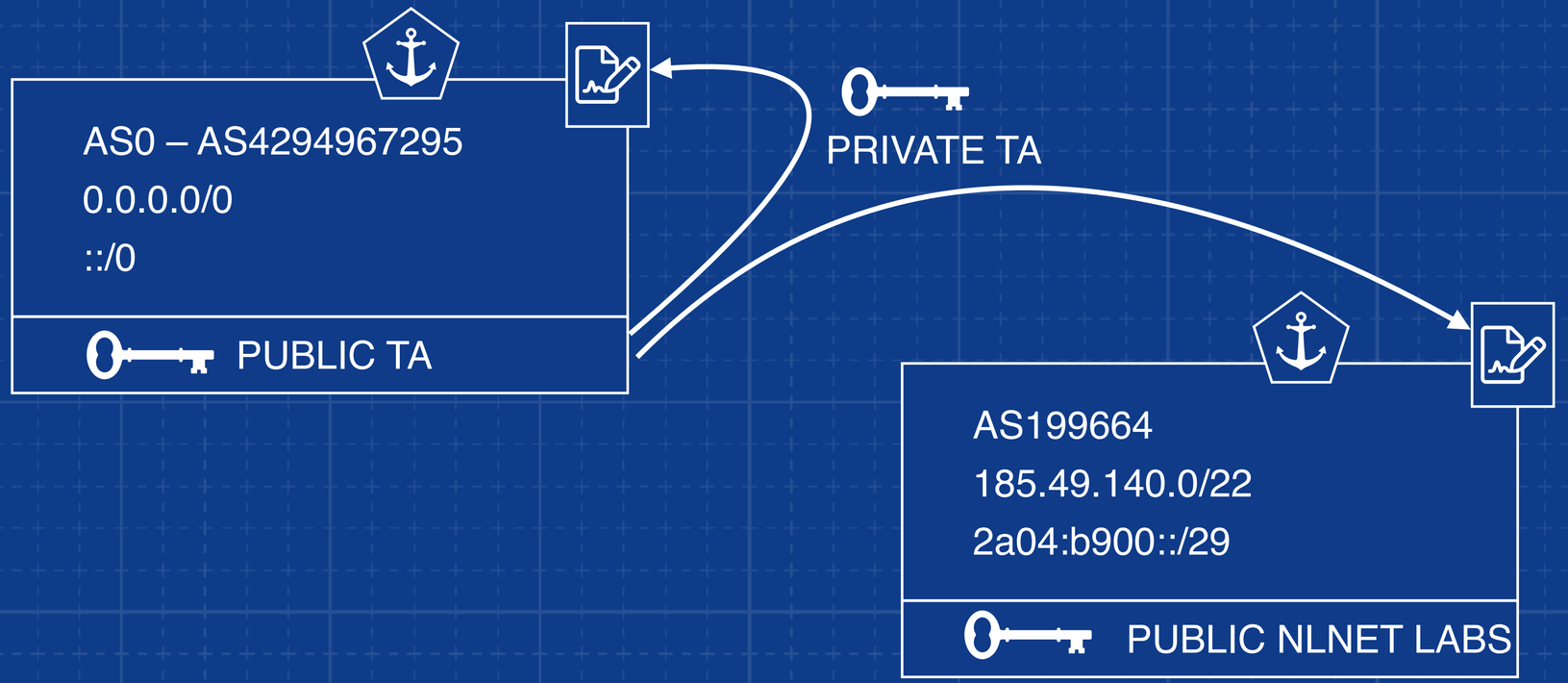
TRUST ANCHOR



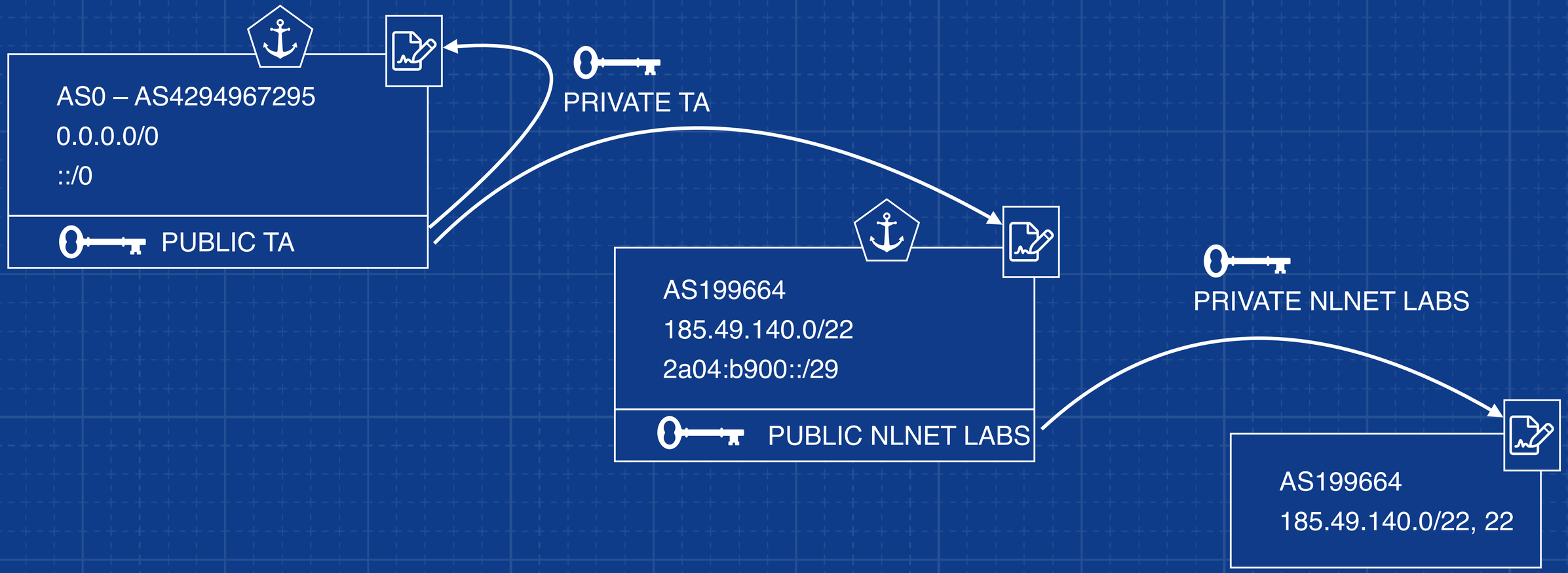
A certificate ties a *public key* to a set of Internet Number Resources and is signed by the private key of the parent.

Trust starts with a so-called Trust Anchor (TA) which has no parent. It is self-signed and inherently trusted.

PUBLIC KEY INFRASTRUCTURE

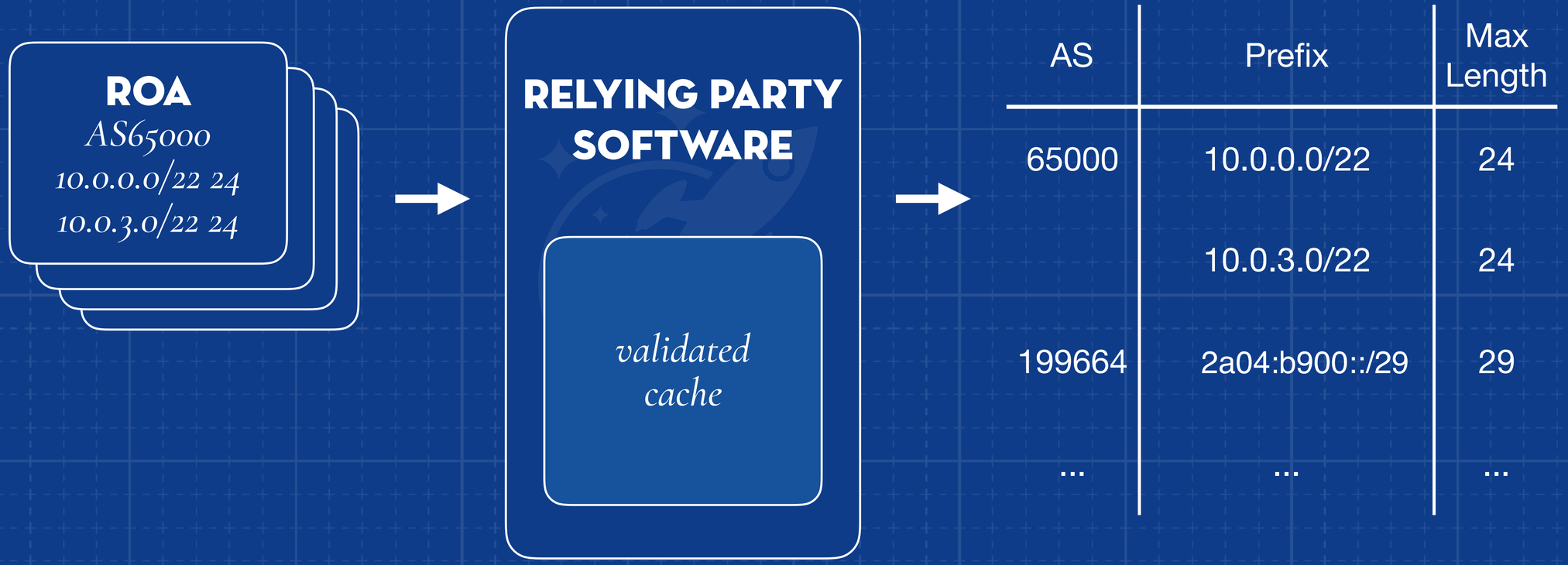


ROUTE ORIGIN AUTHORIZATION



ROV

VERIFIED ROA PAYLOADS



AS	Prefix	Max Length
65000	10.0.0.0/22	24
	10.0.3.0/22	24
199664	2a04:b900::/29	29
...	...	...

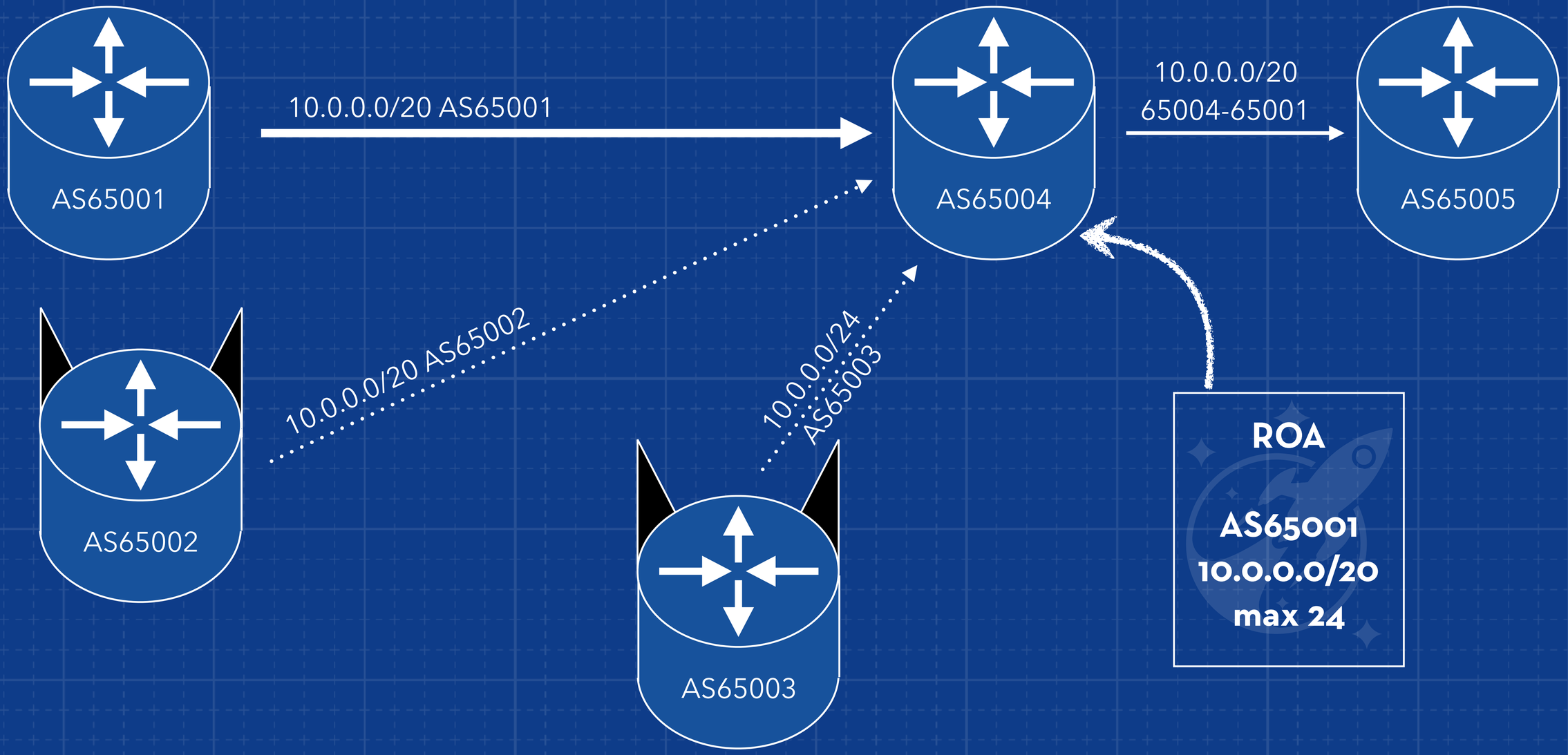
ROA ORIGIN VALIDATION

AS	Prefix	Max
65000	10.0.0.0/22	24
	10.0.3.0/22	24
65001	10.0.0.0/20	20
...	...	...

AS	Prefix	Max
65000	10.0.0.0/22	24
65001	10.0.0.0/20	20

0 covering	NOT FOUND
at least 1 valid	VALID
covering, no valids	INVALID

ROUTE ORIGIN VALIDATION



THE MOVING PARTS

SEPARATE COMPONENTS

CERTIFICATE AUTHORITY

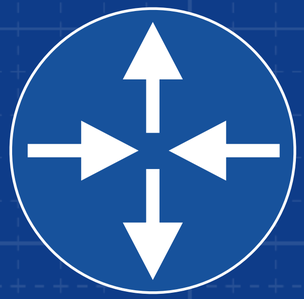
creates & signs

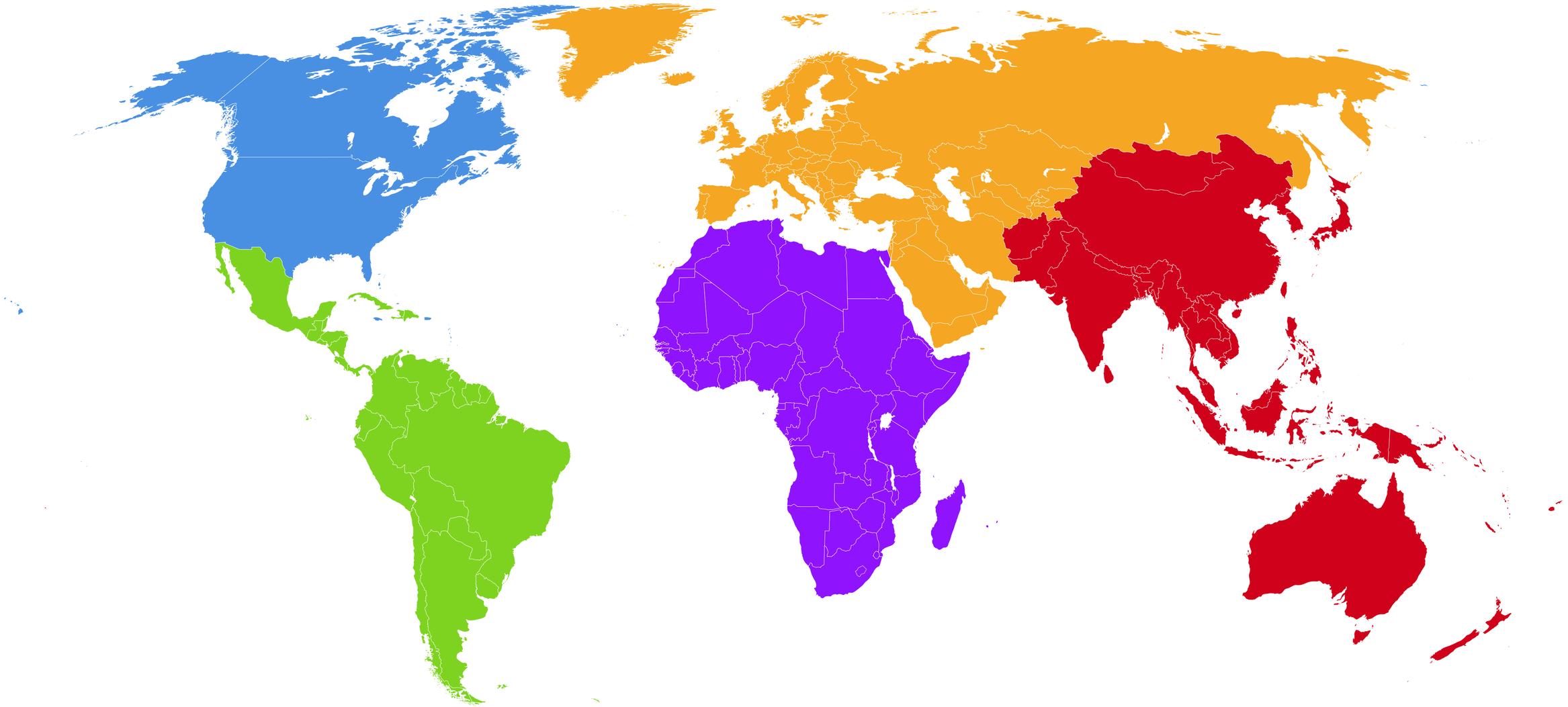
PUBLICATION SERVER

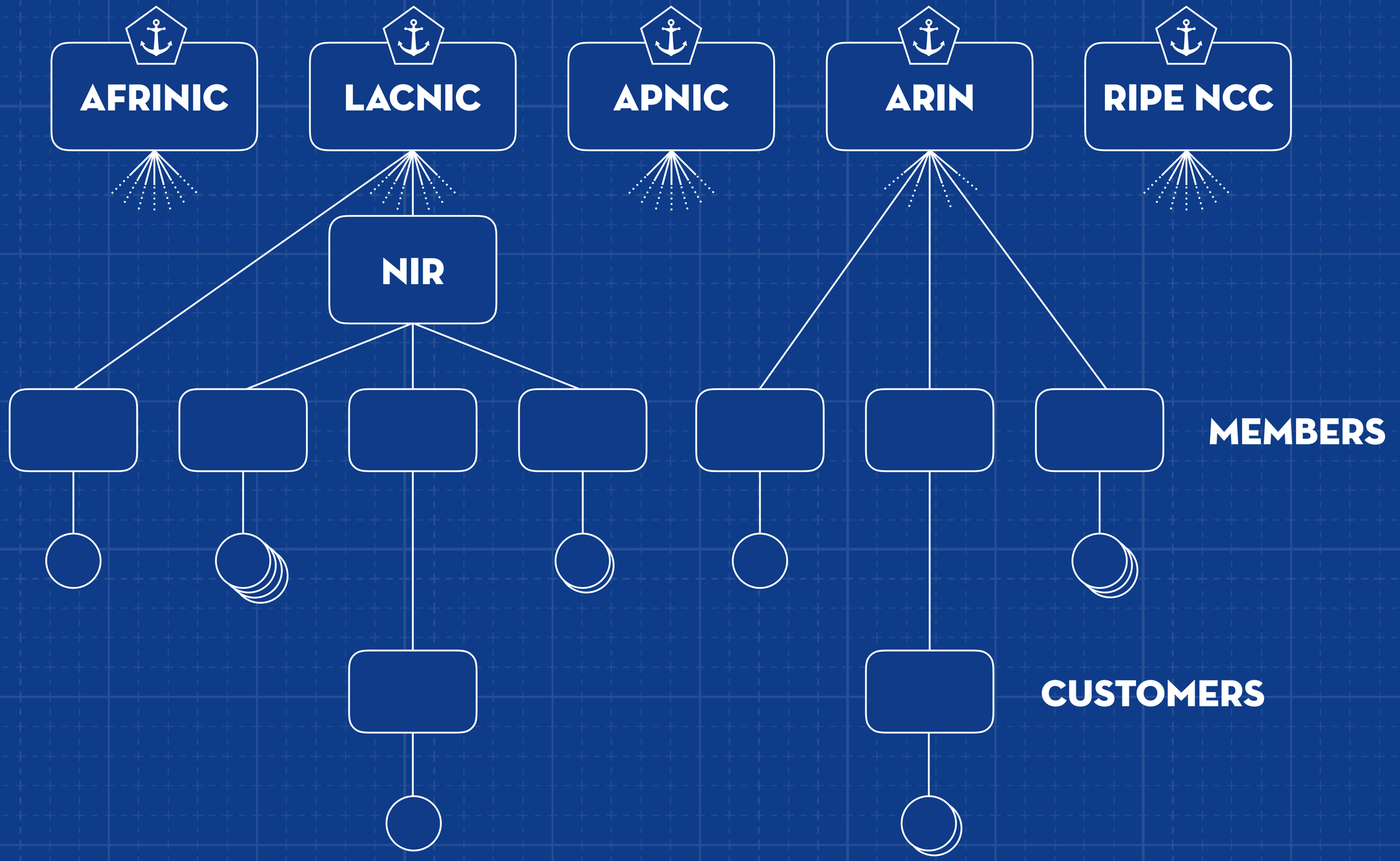
makes available

RELYING PARTY

validates




ARIN
LACNIC
AFRINIC
RIPE NCC
APNIC


AFRINIC
LACNIC
APNIC
ARIN
RIPE NCC
NIR
MEMBERS
CUSTOMERS

HOSTED VS. DELEGATED RPKI

- **Hosted RPKI**
  - The resource issuer — RIR, NIR, LIR — offers RPKI as a service
  - Certificates, keys, and signed products are all kept and published in their infrastructure
- **Delegated RPKI**
  - Run your own Certificate Authority, generate your own signed products and publish them yourself

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RIPE Database (Whois) | Website

Search IP Address and ASN

Manage IPs and ASNs | Analyse | Participate | Get Support | Publications | About Us

You are here: Home > Manage IPs and ASNs > LIR Portal

You are editing: Stichting NLnet Labs

- My LIR
- Resources
  - My Resources
  - Request Resources
  - Request Transfer
  - IPv4 Transfer Listing Service
  - RPKI Dashboard
- RIPE Database

RPKI Dashboard

2 CERTIFIED RESOURCES | ALERTS ARE SENT TO 1 ADDRESS

2 BGP Announcements

2 Valid | 0 Invalid | 0 Unknown

2 ROAs

2 OK | 0 Causing problems

BGP Announcements | Route Origin Authorisations (ROAs) | History

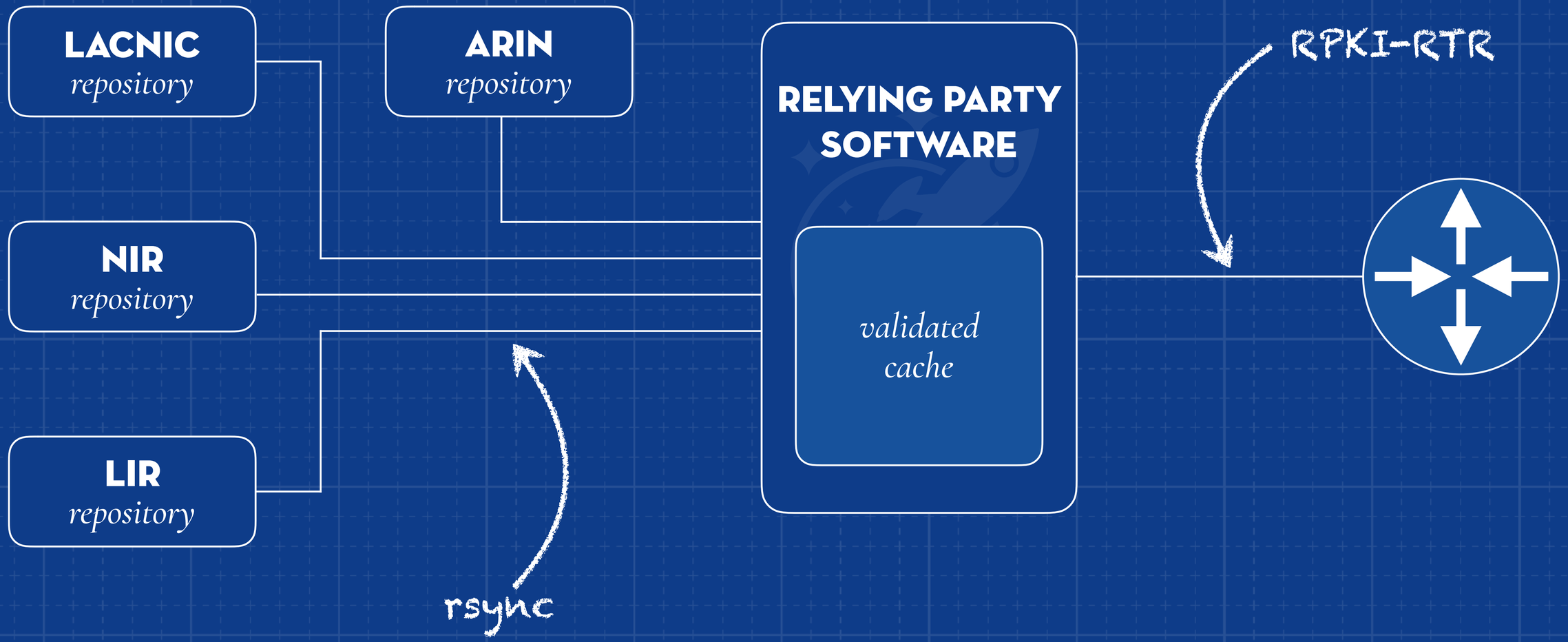
Search...

Discard Changes | Delete ROAs | Causing Problems | Not Causing Problems | + New ROA

AS number	Prefix	Most specific length allowed	Affects
AS Number	Prefix	Max length	
AS199664	2a04:b900::/29	29	1
AS199664	185.49.140.0/22	22	1

Show 25 of 2 items

RPKI VALIDATION



RPKI RP SOFTWARE — TODAY

- rcynic, by Dragon Research Labs (in Python)
- RIPE NCC RPKI Validator (v2 in scala, v3 in Java)
- RPSTIR, by Raytheon BBN Technologies (in C)
- Routinator, by NLnet Labs (in Rust)
- OctoRPKI, by Cloudflare (in Go)
- *Coming soon:* OpenBSD rpki-client(1) (in C)
- *Coming soon:* FORT Validator, by NIC.mx (in C)

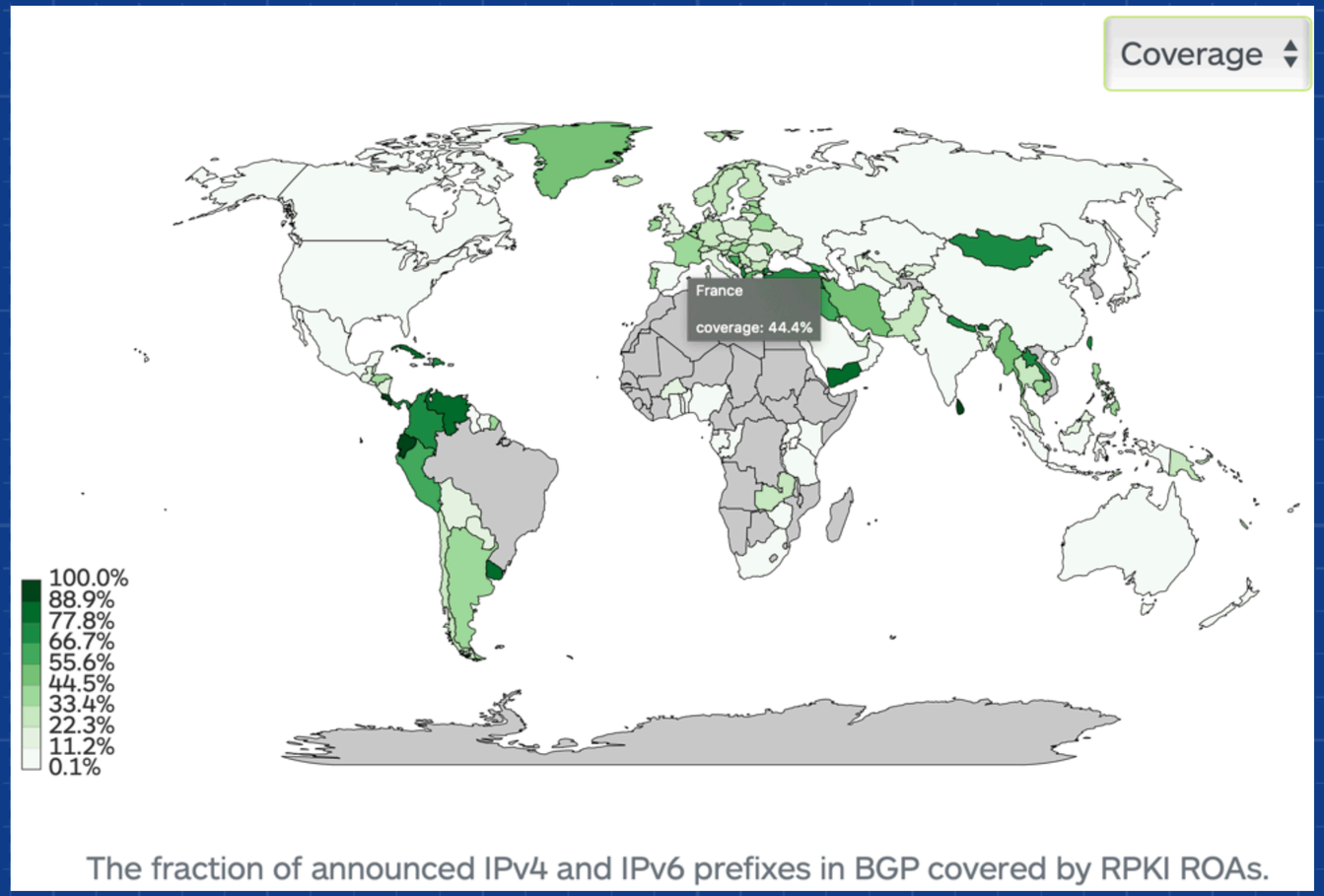
RPKI CA SOFTWARE — TODAY

- RIR implementations (closed source)
- rpki, by Dragon Research Labs (in Python)
- *Coming soon:* Krill by NLnet Labs (in Rust)

PART 2
THE RPKI REPOSITORY

PART 3
UPTAKE, DATA, FUTURE..

COVERAGE



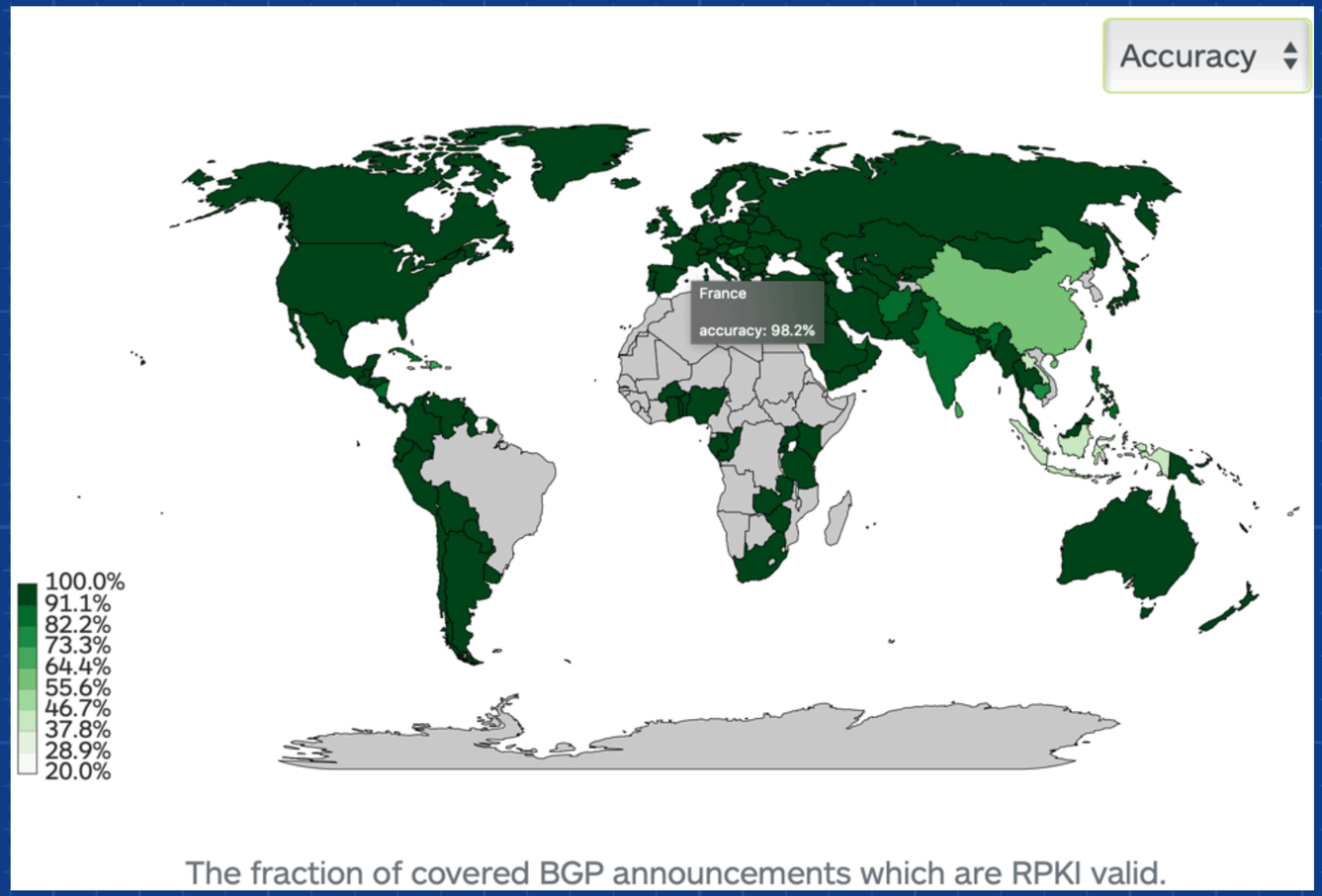
Take aggregated routes from the RIPE RIS Route Collectors

Compare to RIR stats for country codes

Analyse fraction of all IPv4 and IPv6 announcements covered by at least one ROA

https://nlnetlabs.nl/projects/rpki/rpki-analytics/
https://github.com/NLnetLabs/secure-routing-stats

ACCURACY

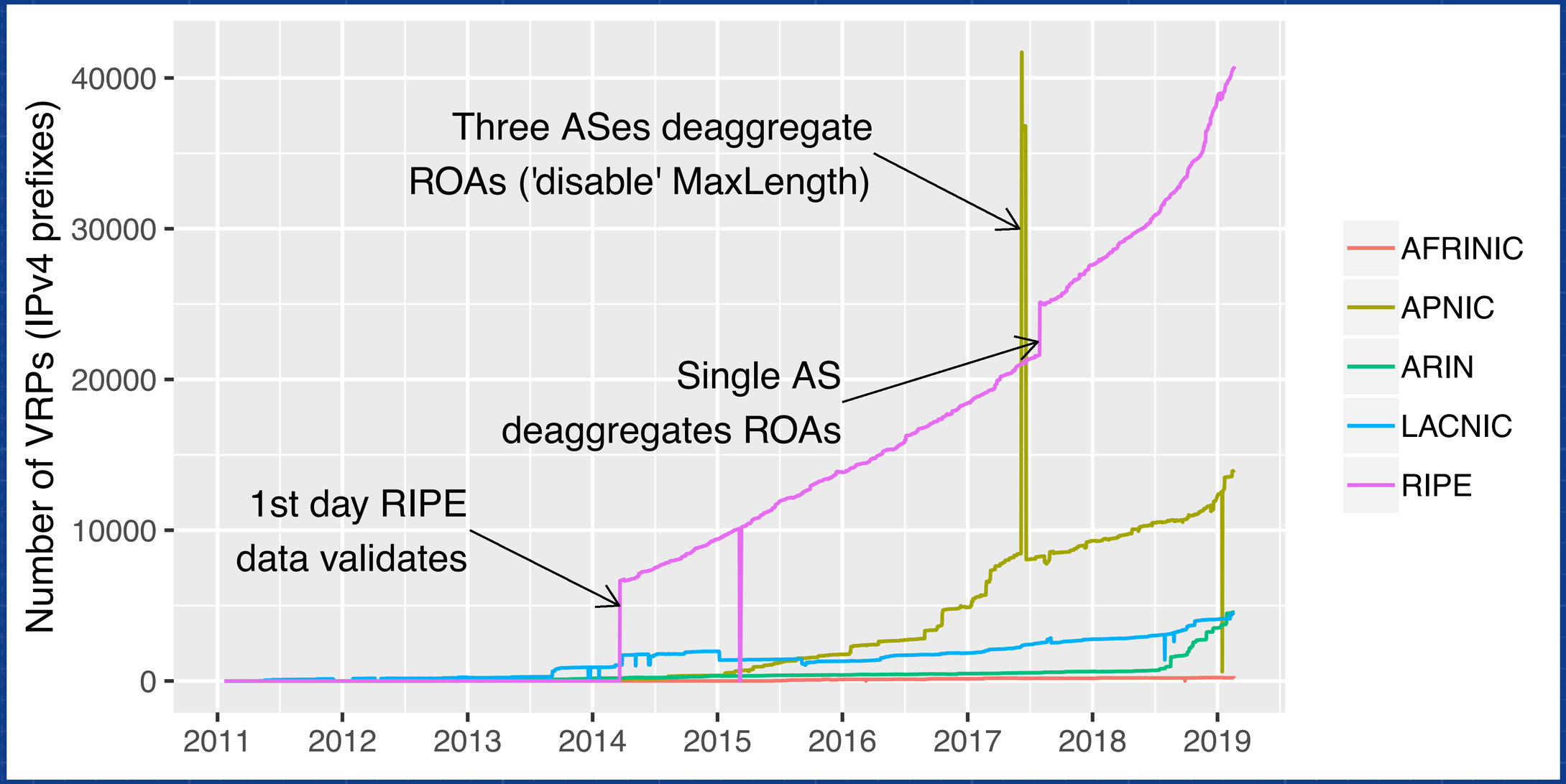


The fraction of valid announcements out of all covered announcements.

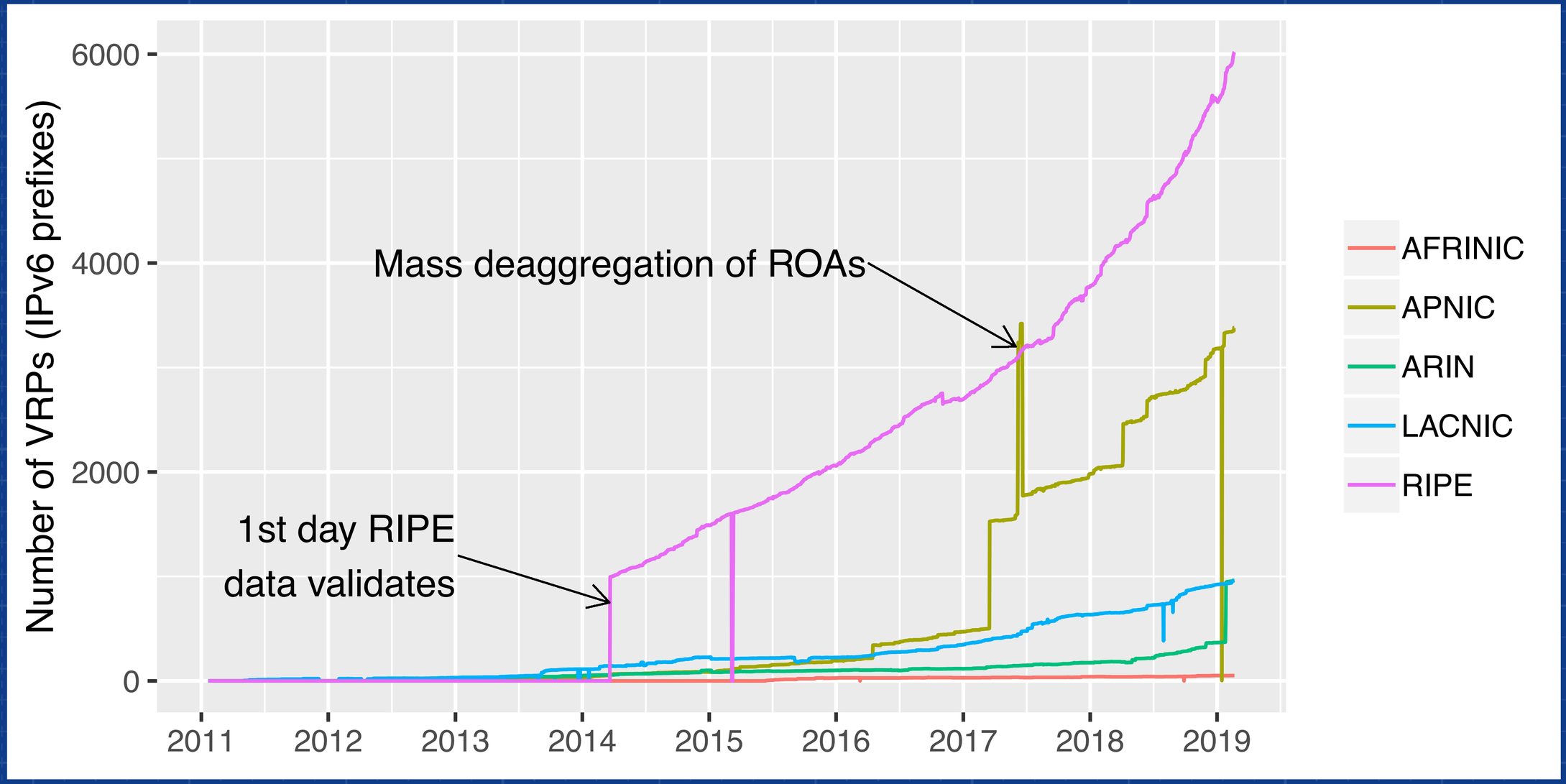
In most countries with serious uptake the value is 98%+

https://nlnetlabs.nl/projects/rpki/rpki-analytics/
https://github.com/NLnetLabs/secure-routing-stats

VRPS OVER TIME



VRPS OVER TIME (V6)



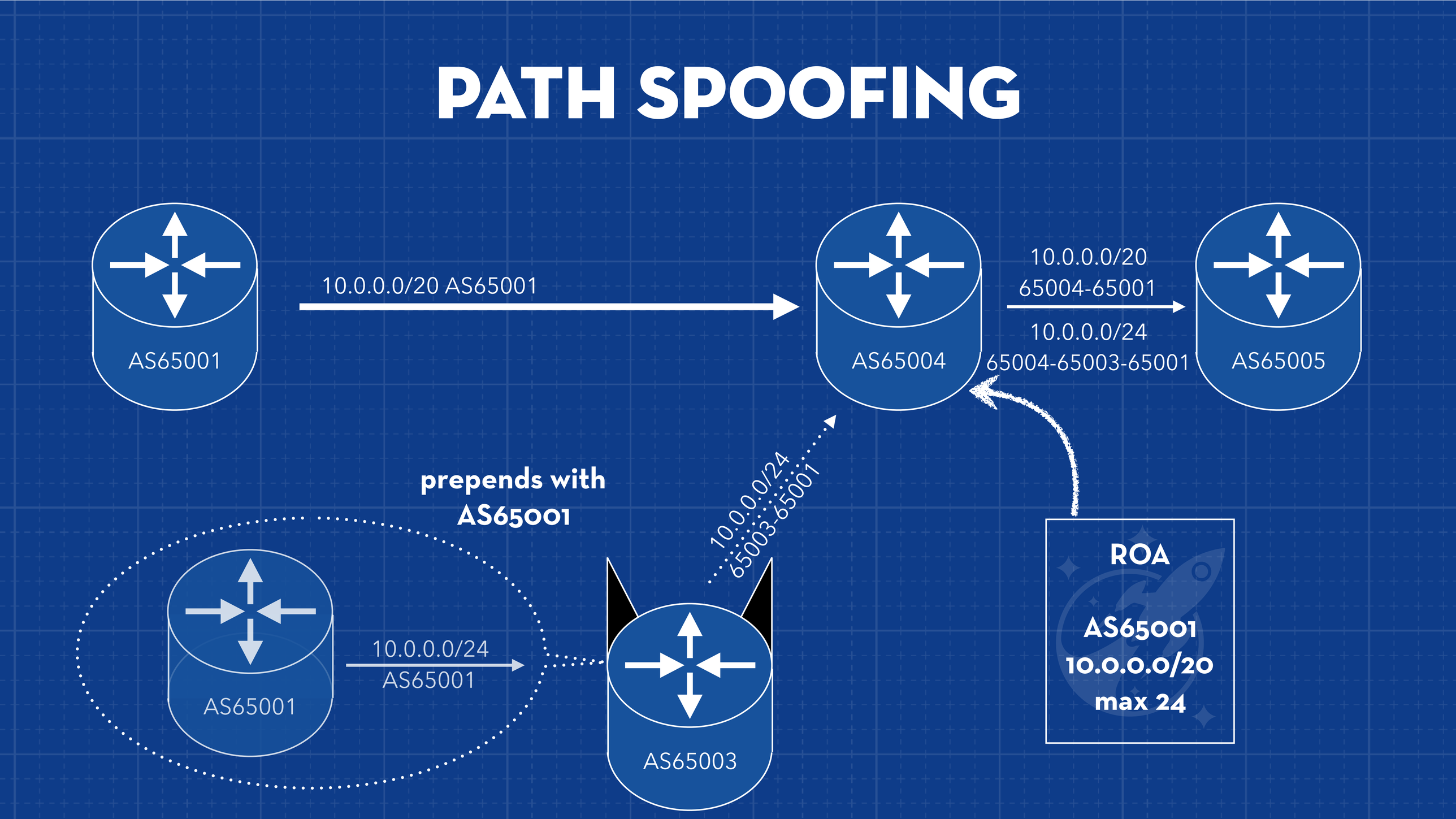
ASNS DROPPING INVALIDS?

- Hard to measure
- For a long time people were not dropping
- However, this changed mid 2018
    - Improved data quality
    - Amazon (AS16509) Route53 hijack – April2018

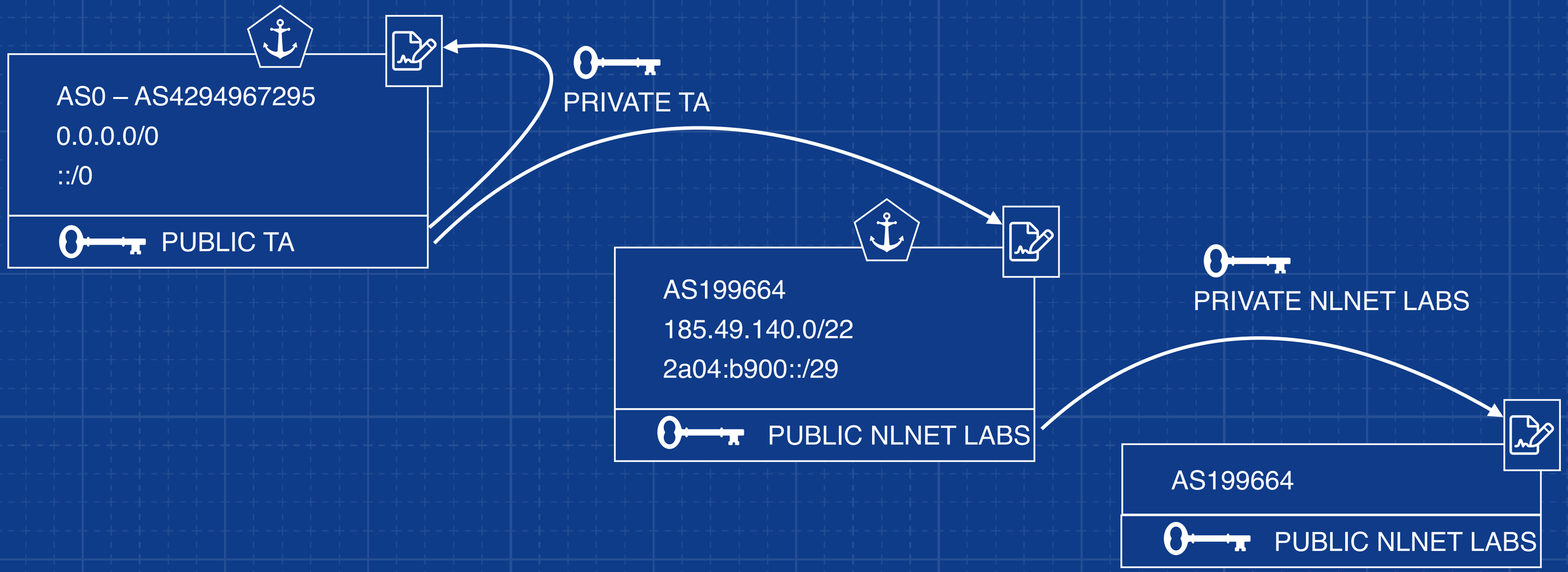
- Many IX's offer as service, many Dutch networks (fusix, xs4all,..), cloudlfare, AT&T

FUTURE WORK?

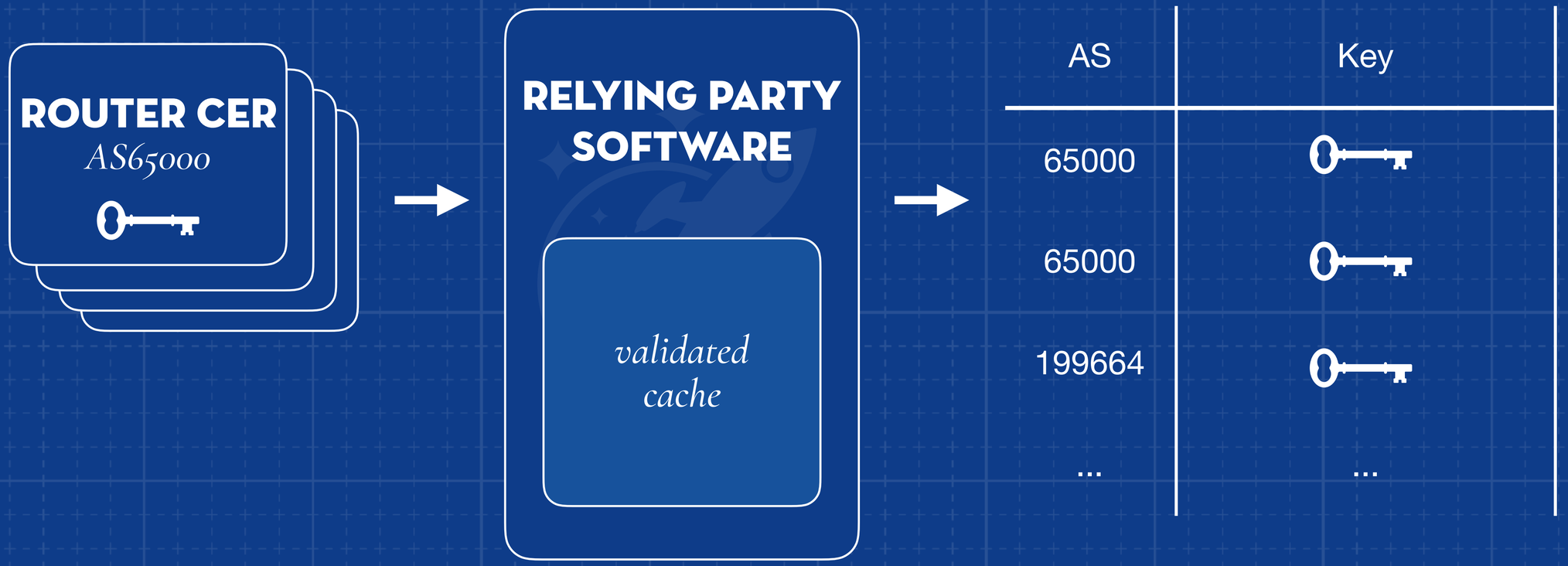
PATH SPOOFING



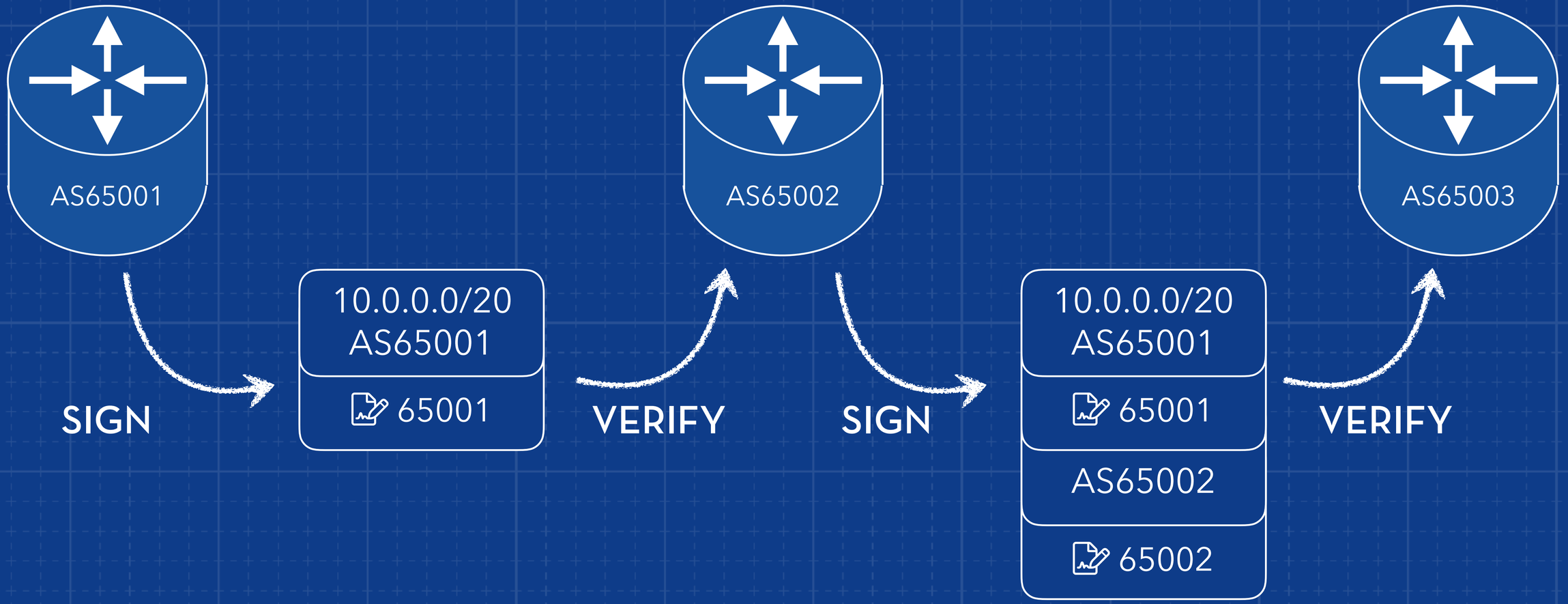
BGPSEC: ROUTER CERTIFICATE



BGPSEC: VALIDATORS



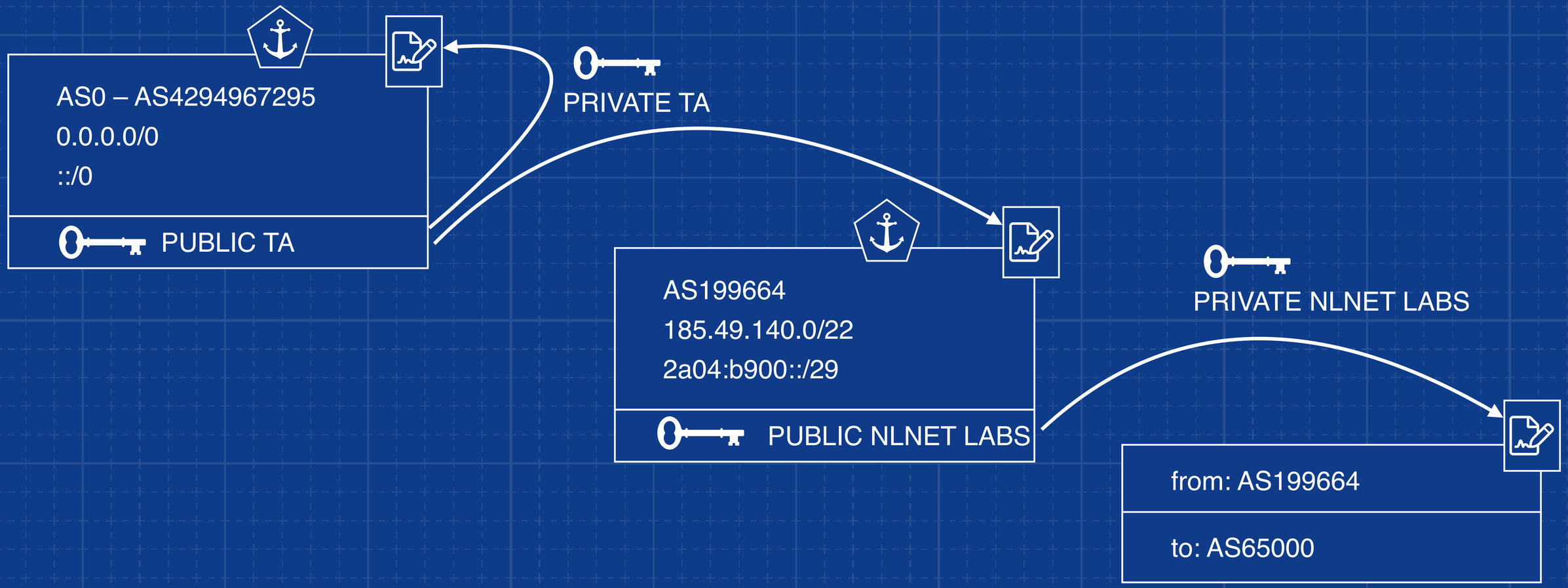
BGPSEC: ROUTERS



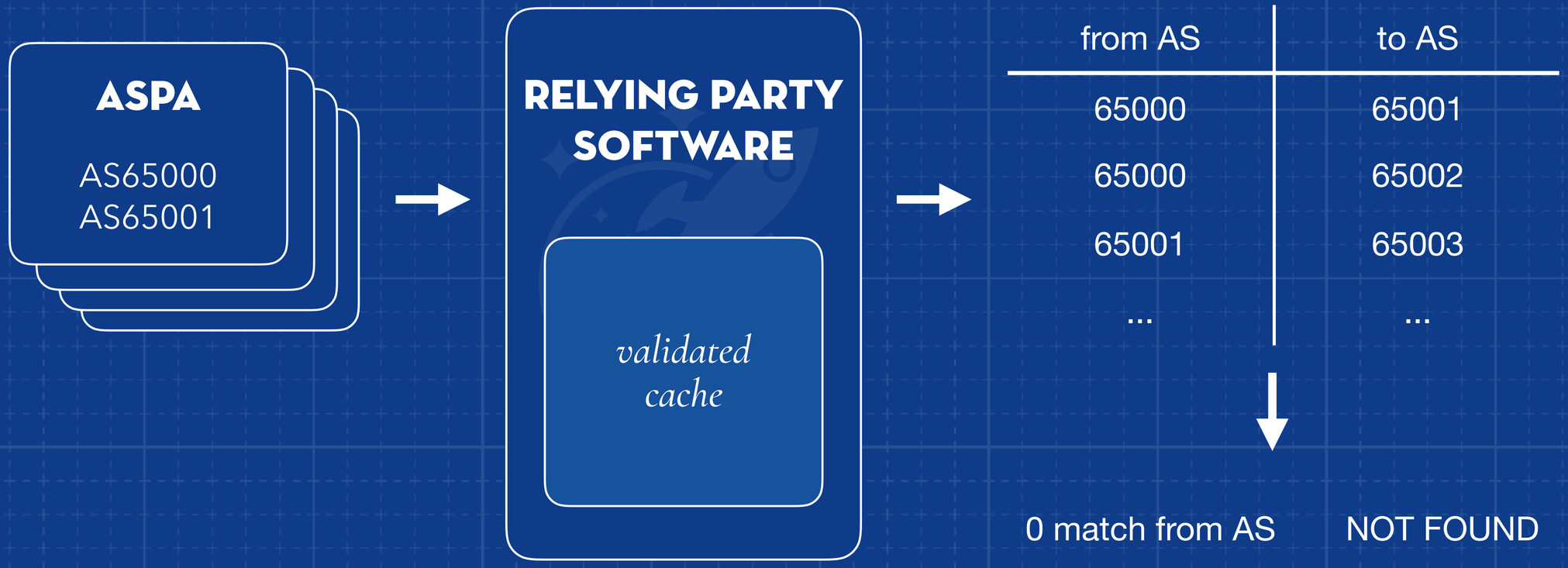
BGPSEC: UNDEPLOYABLE

- Downgrade is not signing. Only two states: VALID, INVALID
- No incremental deployment (NOT FOUND), everyone has to do it
- No support in hardware routers (too resource expensive)

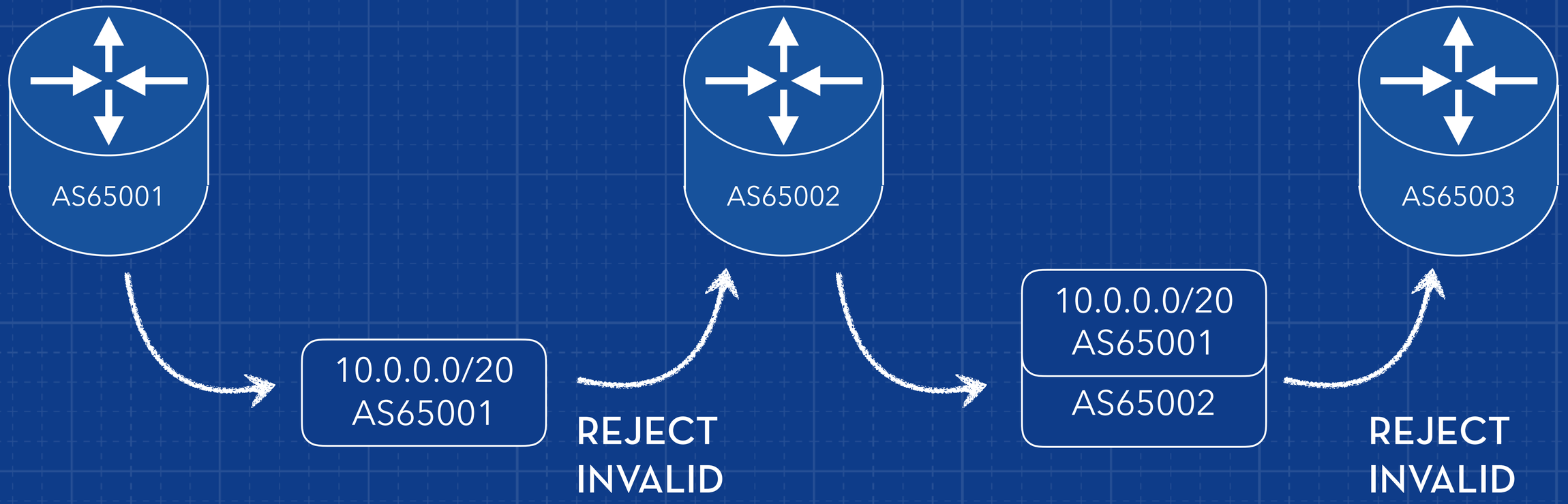
ASPA: PRAGMATIC PATH SEC



ASPA: VALIDATORS



BGPSEC: ROUTERS



ASPA: DEPLOYABILITY

- Drafts recently adopted in IETF sidrops WG
- Incremental possible (VALID, INVALID, NOT FOUND)
- Incremental value: protect your own better, even if it's a bit

- Spoofing requires longer and longer documented path fragments, path is **plausible**, but not guaranteed to be the actual path. 80% solution that can be used in the real world

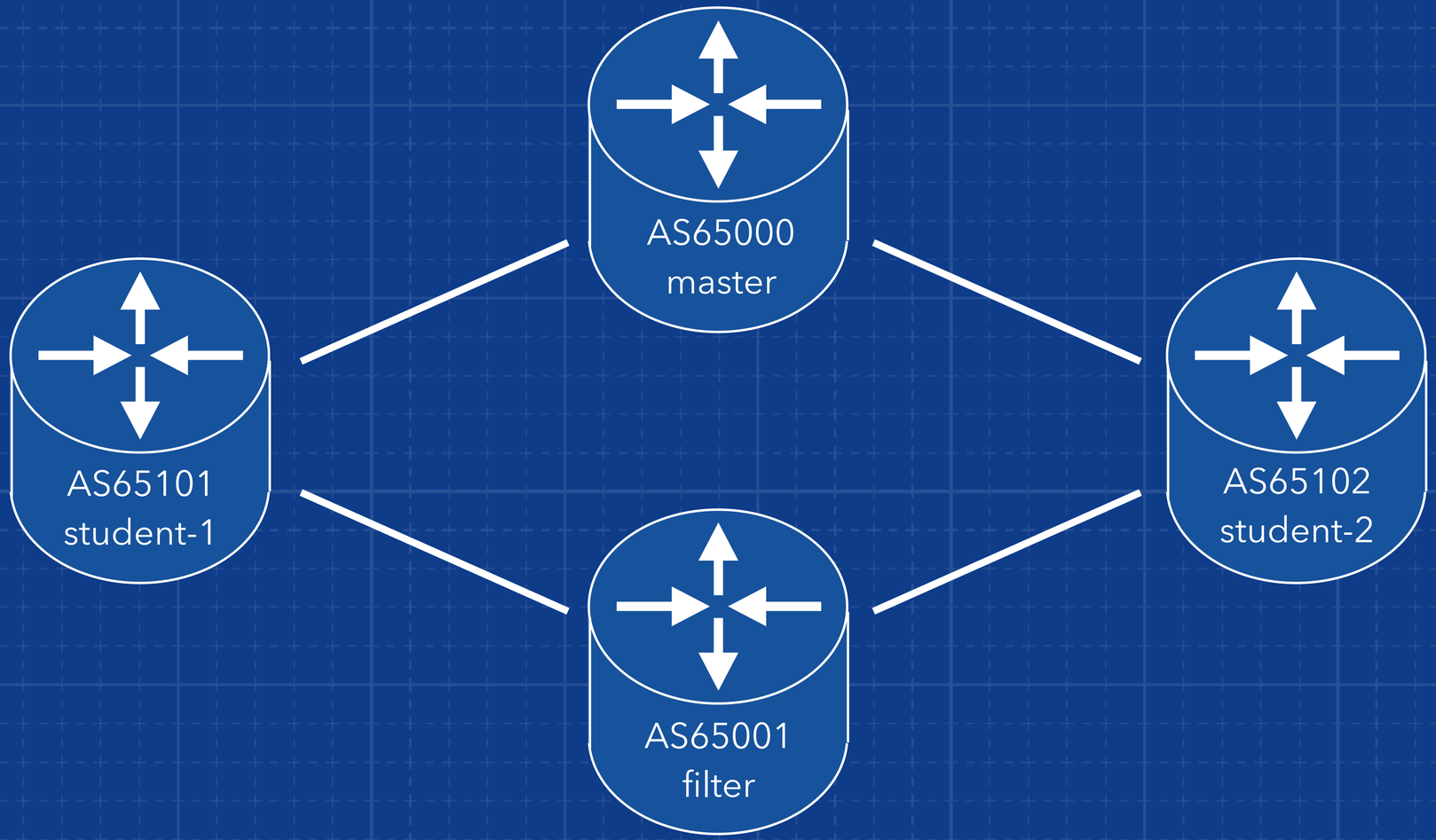
WORKSHOP

WORKSHOP

- 1 virtual machine acting as a transit AS without filtering
- 1 virtual machine acting as a transit AS with filtering
- 17 virtual machines, connected to both transit AS's
  - No filtering done by default
  - Announcing some address space, and hijacking some other space

- Objectives
  - Authorise your own announcements
  - Fix your own hijacks, or be evil. Choose your path!
  - Enable RPKI filtering on your sessions

NETWORK TOPOLOGY



MATERIALS

https://github.com/NLnetLabs/tma-phd-school-2019