CENIC
Connecting California

CENIC’s RPKI Journey

Christopher Bruton (he/him), Core Engineer at CENIC

APAN55, Kathmandu, Nepal

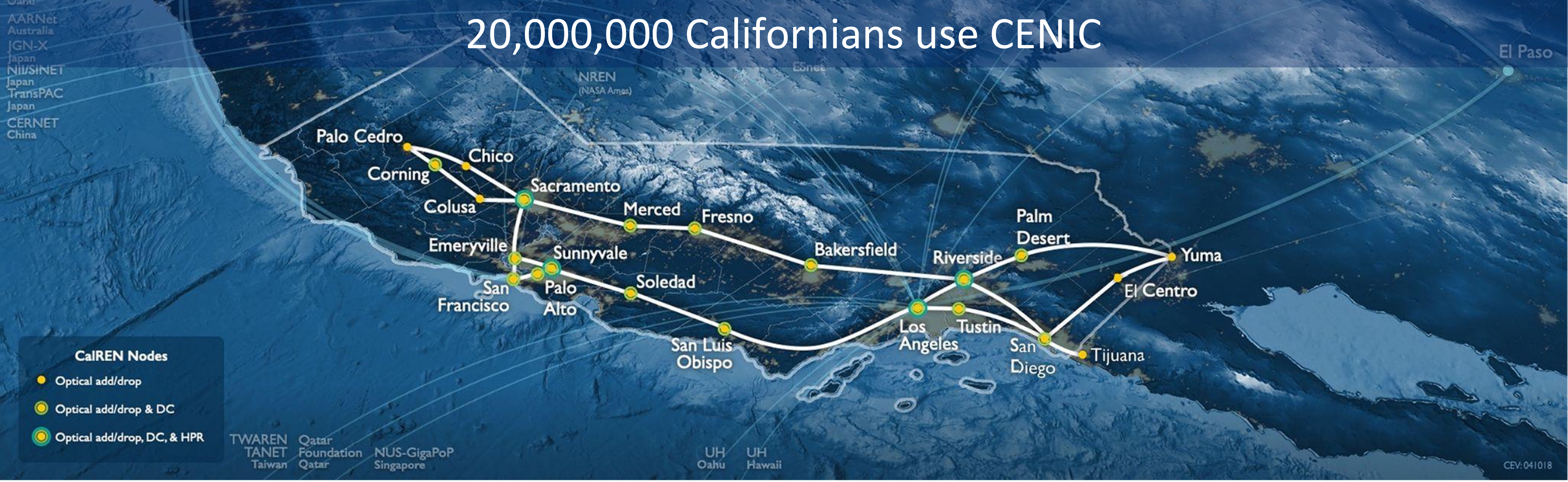
March 15, 2023

CENIC is a 501(c)(3) **with the mission to advance education and research statewide by providing the world-class network essential for innovation, collaboration, and economic growth.**

Charter Associates:

- California K-12 System
- California Community Colleges
- California State University System
- Stanford, Caltech, USC
- University of California System
- California Public Libraries
- Naval Postgraduate School

20,000,000 Californians use CENIC

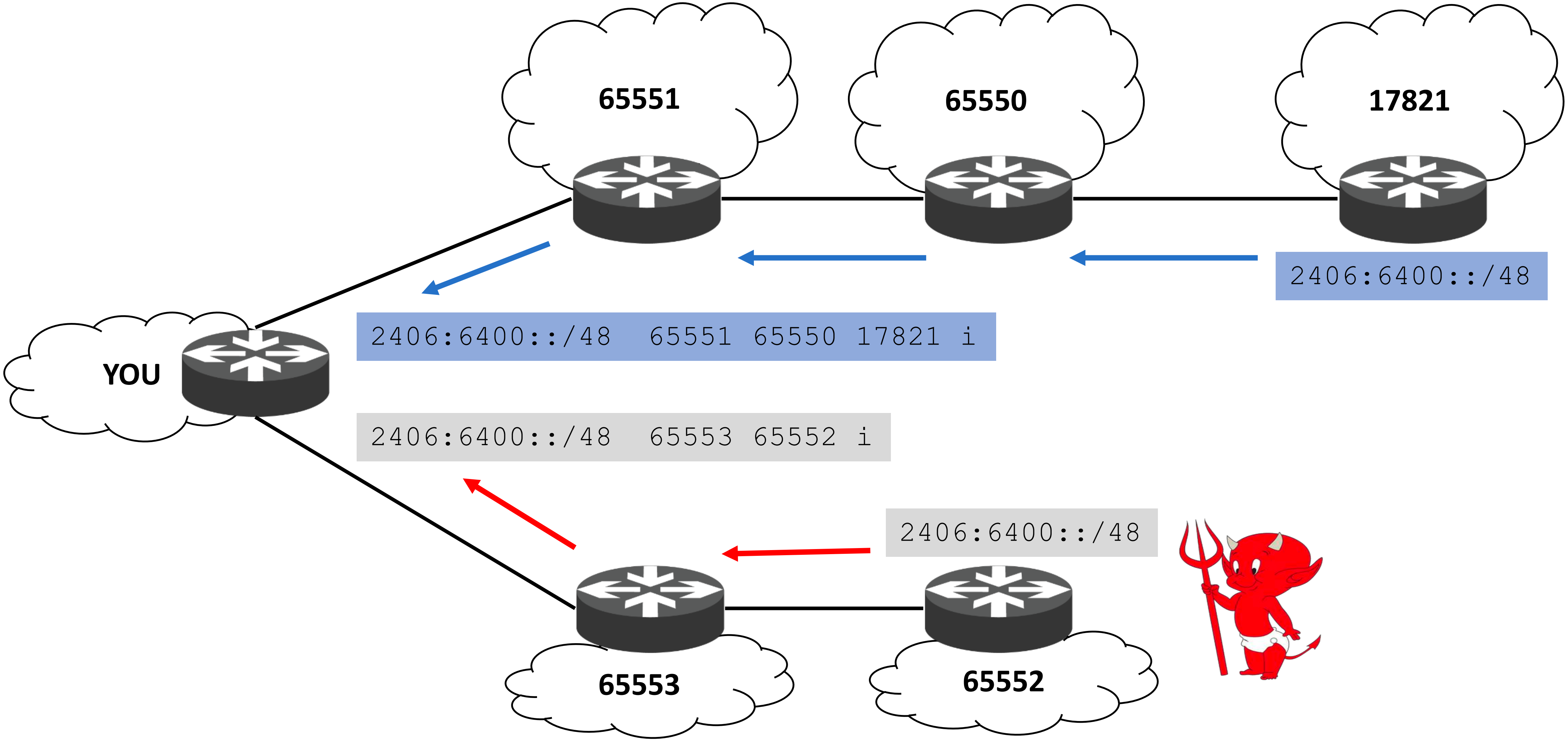


- **8,000+ miles of optical fiber**
- **Members in all 58 counties connect via fiber-optic cable or leased circuits from telecom carriers**
- **Over 12,000 sites connect to CENIC**

- **A non-profit** chartered & governed by its members
- Collaborates with over **750 private sector partners and contributes > $100,000,000** to the CA Economy
- **24 plus years** of connecting California

RPKI: What does it solve?

Route Origin Validation (ROV)



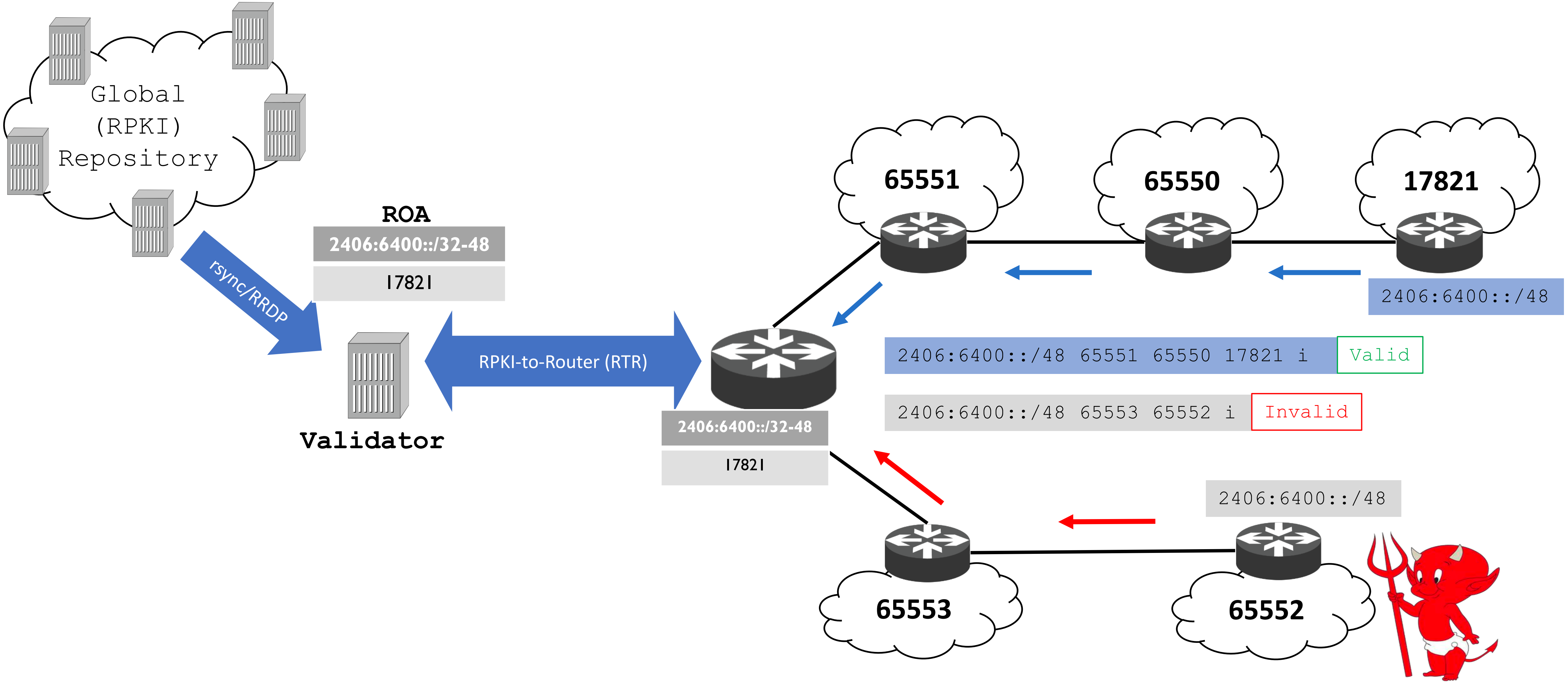
2406:6400::/48

2406:6400::/48   65551 65550 17821 i

2406:6400::/48   65553 65552 i

2406:6400::/48

Route Origin Validation (ROV)



RPKI Architecture

From repository to router…

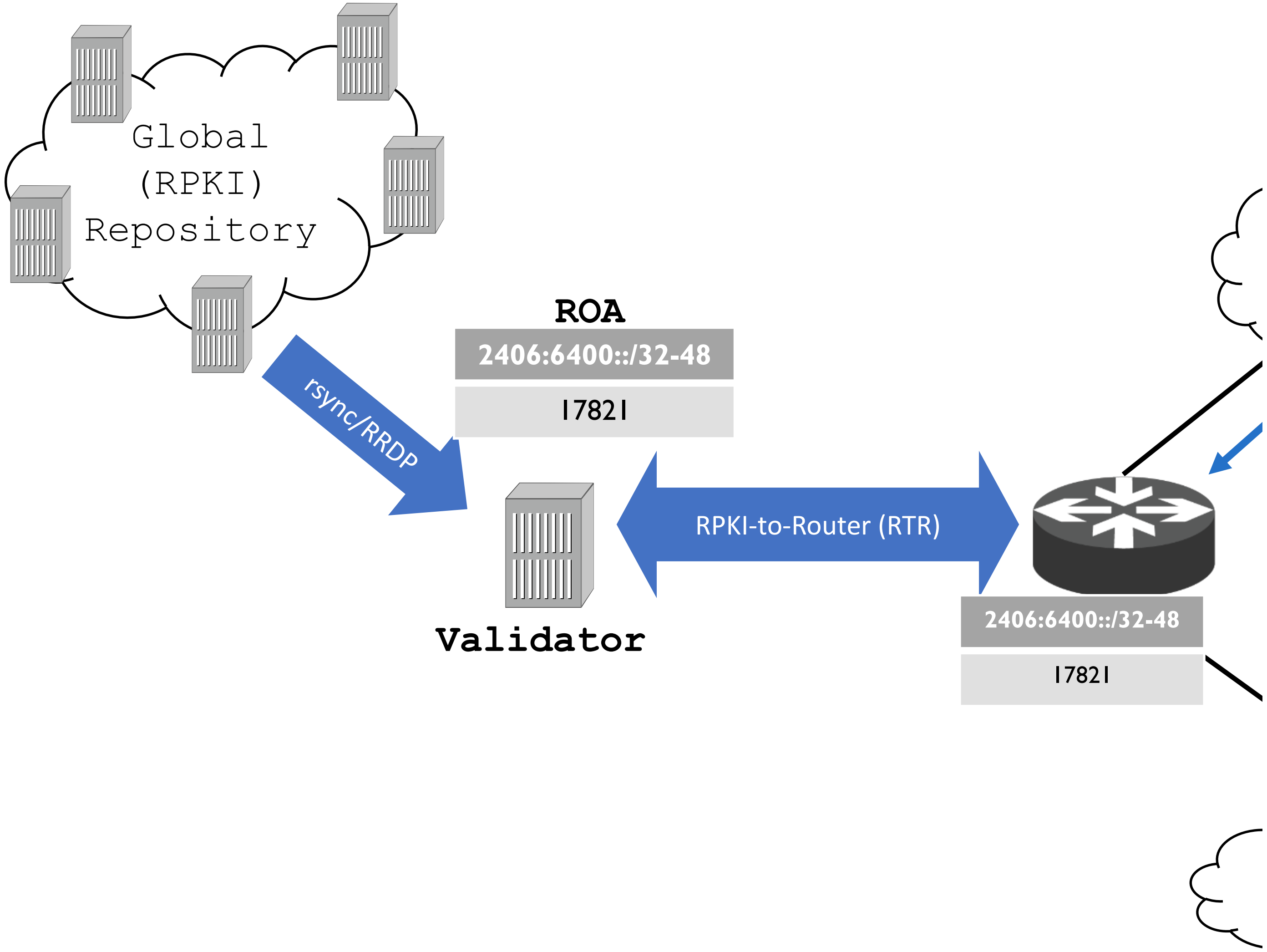
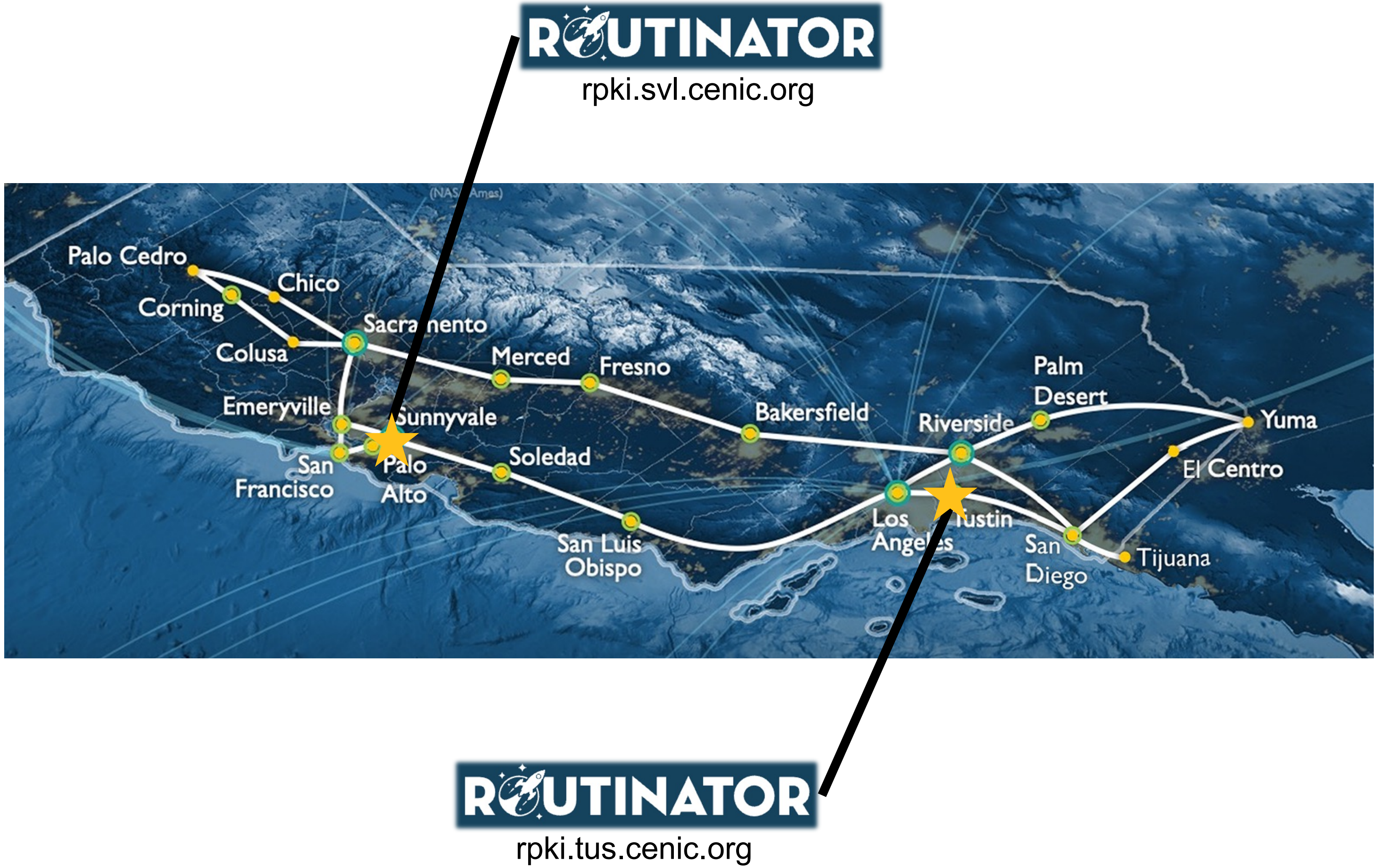


Diagram by APNIC, CC BY-NC-SA

- **Repositories:**
  - Hosted by RIRs (ARIN, APNIC, etc.) or delegated
  - Contain cryptographically signed ROAs
- **Validators:**
  - Typically hosted locally
  - Pull from repositories and cryptographically validate
  - Serve a cache of validated ROAs
- **Routers:**
  - Pull from validator cache
  - Don’t need to perform cryptography themselves

Validators at CENIC

- **Routinator:** An open-source RPKI validator by NLnet Labs
- CENIC installed two instances for redundancy
- Running on VMs with minimal resources:
  - 4GB RAM
  - 1 vCPU
  - 15GB storage
  - Deployed via Ansible role

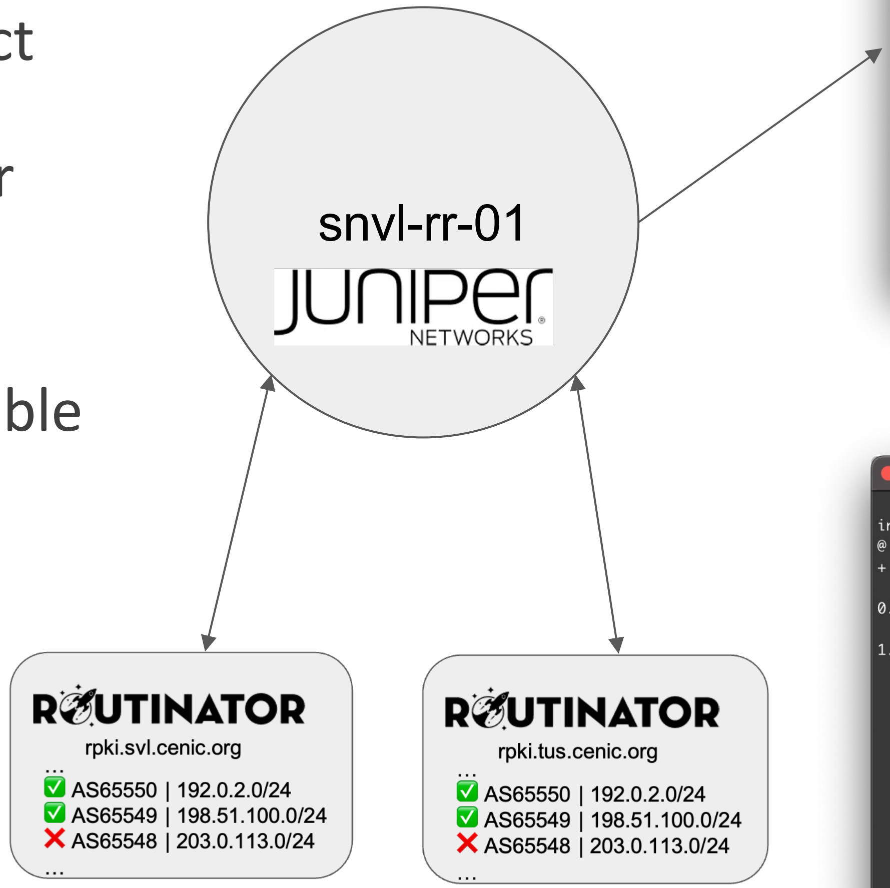


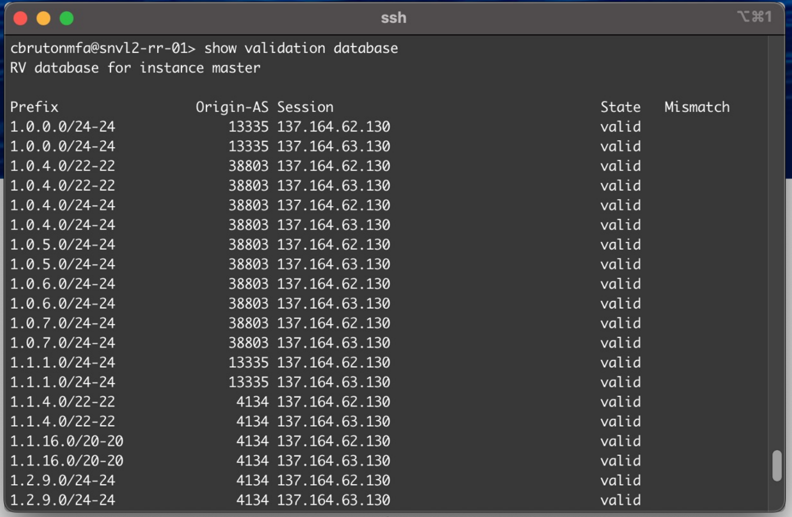
rpki.svl.cenic.org

rpki.tus.cenic.org

Validation pilot

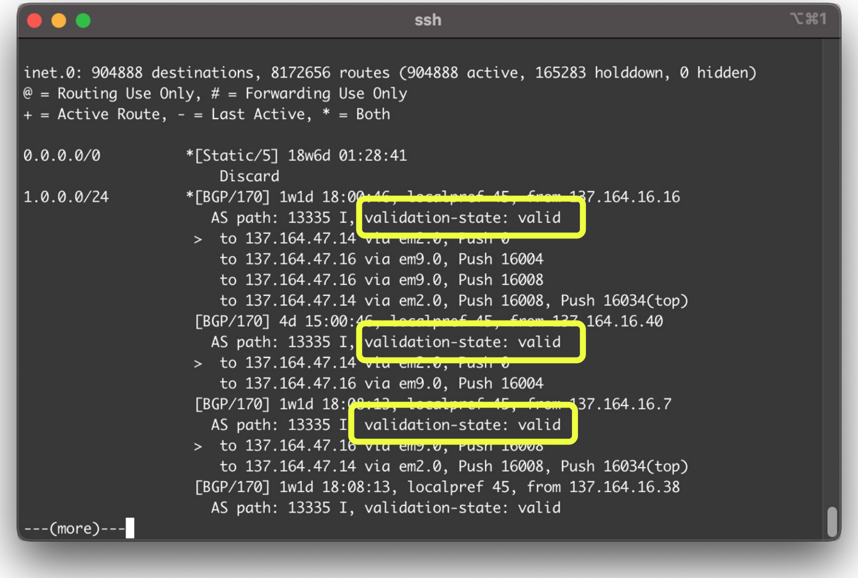
- CENIC chose a low-impact router to test the connection to Routinator instances
- Validation state now appears in the routing table
- **Not yet rejecting invalid routes**





```
cbrutonmfa@snvl2-rr-01> show validation database
RV database for instance master

Prefix                 Origin-AS Session                                 State   Mismatch
1.0.0.0/24-24              13335 137.164.62.130                          valid
1.0.0.0/24-24              13335 137.164.63.130                          valid
1.0.4.0/22-22              38803 137.164.62.130                          valid
1.0.4.0/22-22              38803 137.164.63.130                          valid
1.0.4.0/24-24              38803 137.164.62.130                          valid
1.0.4.0/24-24              38803 137.164.63.130                          valid
1.0.5.0/24-24              38803 137.164.62.130                          valid
1.0.5.0/24-24              38803 137.164.63.130                          valid
1.0.6.0/24-24              38803 137.164.62.130                          valid
1.0.6.0/24-24              38803 137.164.63.130                          valid
1.0.7.0/24-24              38803 137.164.62.130                          valid
1.0.7.0/24-24              38803 137.164.63.130                          valid
1.1.1.0/24-24              13335 137.164.62.130                          valid
1.1.1.0/24-24              13335 137.164.63.130                          valid
1.1.4.0/22-22               4134 137.164.62.130                          valid
1.1.4.0/22-22               4134 137.164.63.130                          valid
1.1.16.0/20-20              4134 137.164.62.130                          valid
1.1.16.0/20-20              4134 137.164.63.130                          valid
1.2.9.0/24-24               4134 137.164.62.130                          valid
1.2.9.0/24-24               4134 137.164.63.130                          valid
```



```
inet.0: 904888 destinations, 8172656 routes (904888 active, 165283 holddown, 0 hidden)
@ = Routing Use Only, # = Forwarding Use Only
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Static/5] 18w6d 01:28:41
                      Discard
1.0.0.0/24         *[BGP/170] 1w1d 18:00:46, localpref 45, from 137.164.16.16
                     AS path: 13335 I, validation-state: valid
                   >  to 137.164.47.14 via em2.0, Push 0
                      to 137.164.47.16 via em9.0, Push 16004
                      to 137.164.47.16 via em9.0, Push 16008
                      to 137.164.47.14 via em2.0, Push 16008, Push 16034(top)
                    [BGP/170] 4d 15:00:46, localpref 45, from 137.164.16.40
                     AS path: 13335 I, validation-state: valid
                   >  to 137.164.47.14 via em2.0, Push 0
                      to 137.164.47.16 via em9.0, Push 16004
                    [BGP/170] 1w1d 18:08:13, localpref 45, from 137.164.16.7
                     AS path: 13335 I, validation-state: valid
                   >  to 137.164.47.16 via em9.0, Push 16008
                      to 137.164.47.14 via em2.0, Push 16008, Push 16034(top)
                    [BGP/170] 1w1d 18:08:13, localpref 45, from 137.164.16.38
                     AS path: 13335 I, validation-state: valid
---(more)---
```

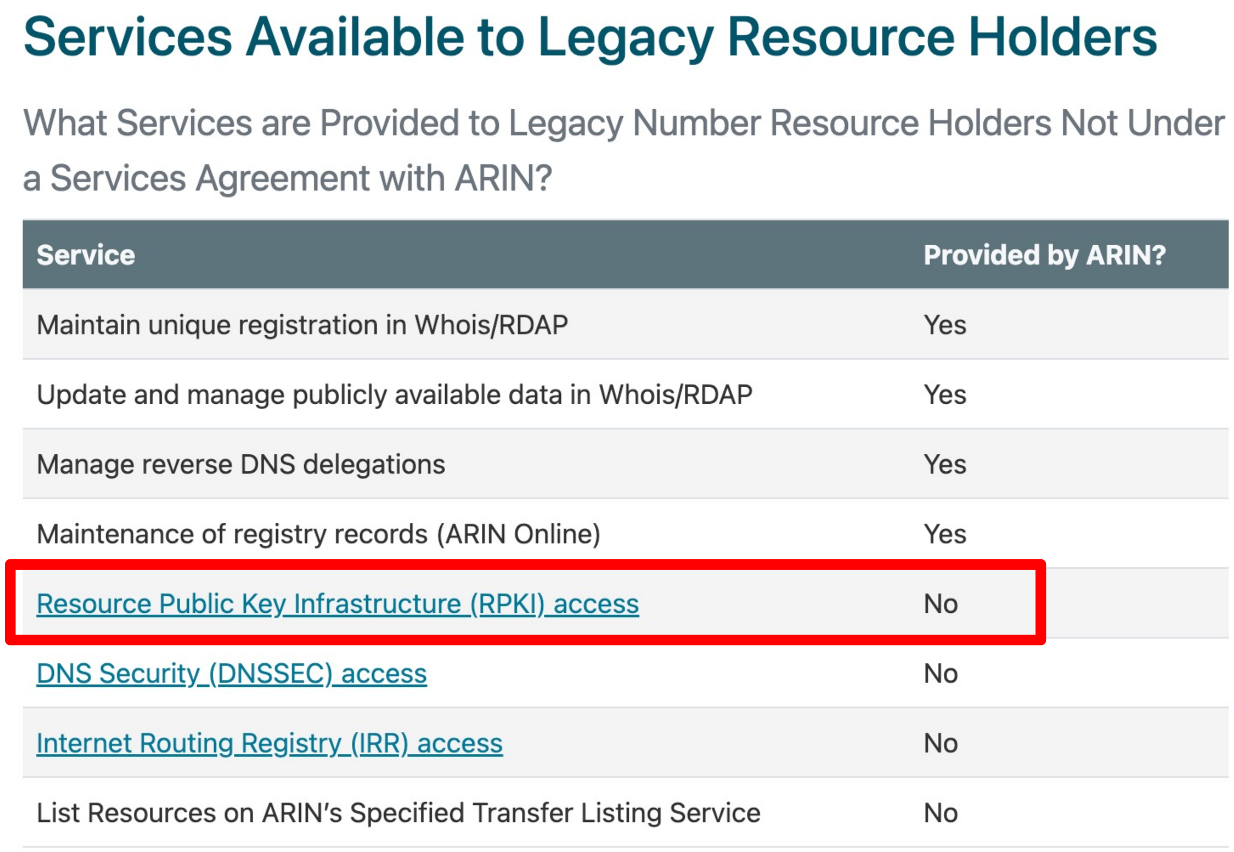
What’s next?

Plan: Validate at network edges

- In Q2 2023 we plan to implement validation on our aggregation routers for **PNI and exchange peers**
- We will begin **rejecting RPKI-invalid routes** from our peers
- No timeline yet to validate routes from our associates

What about our associates?

- Lots of support, education, and resources will need to be provided before we implement RPKI validation for our associates
- Big challenge: ARIN legacy resources
- Like virtually all providers, we have no plans to drop **RPKI-unknown** prefixes for the foreseeable future
- But many possible pitfalls for associates who choose to sign ROAs for their prefixes—could inadvertently become **RPKI-invalid**



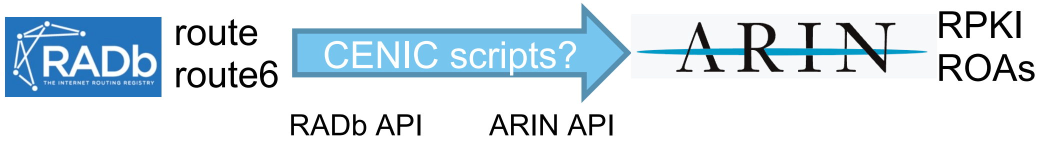
Services Available to Legacy Resource Holders

What Services are Provided to Legacy Number Resource Holders Not Under a Services Agreement with ARIN?

Service	Provided by ARIN?
Maintain unique registration in Whois/RDAP	Yes
Update and manage publicly available data in Whois/RDAP	Yes
Manage reverse DNS delegations	Yes
Maintenance of registry records (ARIN Online)	Yes
Resource Public Key Infrastructure (RPKI) access	No
DNS Security (DNSSEC) access	No
Internet Routing Registry (IRR) access	No
List Resources on ARIN's Specified Transfer Listing Service	No

Challenge: Generating our own ROAs (1/3)

- Best practice is to generate ROAs for the **exact** prefixes that we advertise—avoid using max-length parameter (RFC 7115/BCP 185)
- In some cases we advertise prefixes smaller than /24 and /48
- We do not want anyone to inadvertently reject a prefix because we forgot to create an ROA
- Possibilities for automation and syncing with IRR objects



ROA

ASN	Prefix	Max Length
65420	10.0.0.0/16	18

BGP Routes

ASN	Prefix	RPKI State
65420	10.0.0.0/16	VALID
65420	10.0.128.0/17	VALID
65421	10.0.0.0/16	INVALID
65420	10.0.10.0/24	INVALID
65430	10.0.0.0/8	NOT FOUND

Diagram by APNIC, CC BY-NC-SA

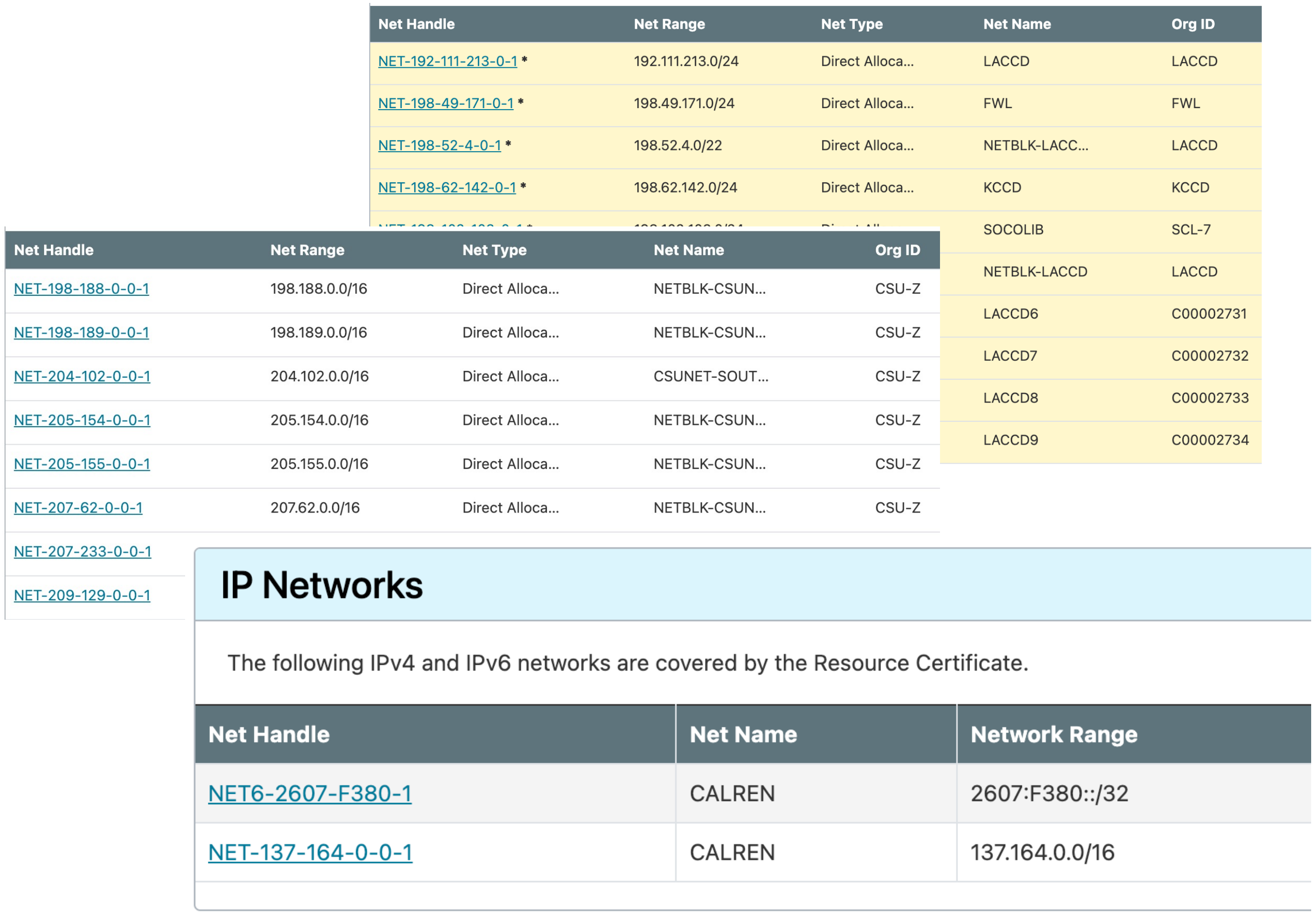
Challenge: Generating our own ROAs (2/3)

- Challenges with legacy resources and ARIN assignments; CENIC can currently only generate ROAs for:
  - 137.164.0.0/16
  - 2607:f380::/32
- Working with CSU and ARIN to formally transfer more resources to us
- We also have to be very careful not to invalidate associates' prefixes that fall within our own allocations

✅ 2607:f380::/32 : AS2152 : CENIC

⇩

❌ 2607:f380:804::/48 : AS257 : NNIC
❌ 2607:f380:864::/48 : AS23483 : Shasta COE
❌ 2607:f380:a4f::/48 : AS32361 : Caltech



Net Handle	Net Range	Net Type	Net Name	Org ID
NET-192-111-213-0-1 *	192.111.213.0/24	Direct Alloca...	LACCD	LACCD
NET-198-49-171-0-1 *	198.49.171.0/24	Direct Alloca...	FWL	FWL
NET-198-52-4-0-1 *	198.52.4.0/22	Direct Alloca...	NETBLK-LACC...	LACCD
NET-198-62-142-0-1 *	198.62.142.0/24	Direct Alloca...	KCCD	KCCD
[illegible]	[illegible]	[illegible]	SOCOLIB	SCL-7
			NETBLK-LACCD	LACCD
			LACCD6	C00002731
			LACCD7	C00002732
			LACCD8	C00002733
			LACCD9	C00002734

Net Handle	Net Range	Net Type	Net Name	Org ID
NET-198-188-0-0-1	198.188.0.0/16	Direct Alloca...	NETBLK-CSUN...	CSU-Z
NET-198-189-0-0-1	198.189.0.0/16	Direct Alloca...	NETBLK-CSUN...	CSU-Z
NET-204-102-0-0-1	204.102.0.0/16	Direct Alloca...	CSUNET-SOUT...	CSU-Z
NET-205-154-0-0-1	205.154.0.0/16	Direct Alloca...	NETBLK-CSUN...	CSU-Z
NET-205-155-0-0-1	205.155.0.0/16	Direct Alloca...	NETBLK-CSUN...	CSU-Z
NET-207-62-0-0-1	207.62.0.0/16	Direct Alloca...	NETBLK-CSUN...	CSU-Z
NET-207-233-0-0-1				
NET-209-129-0-0-1				

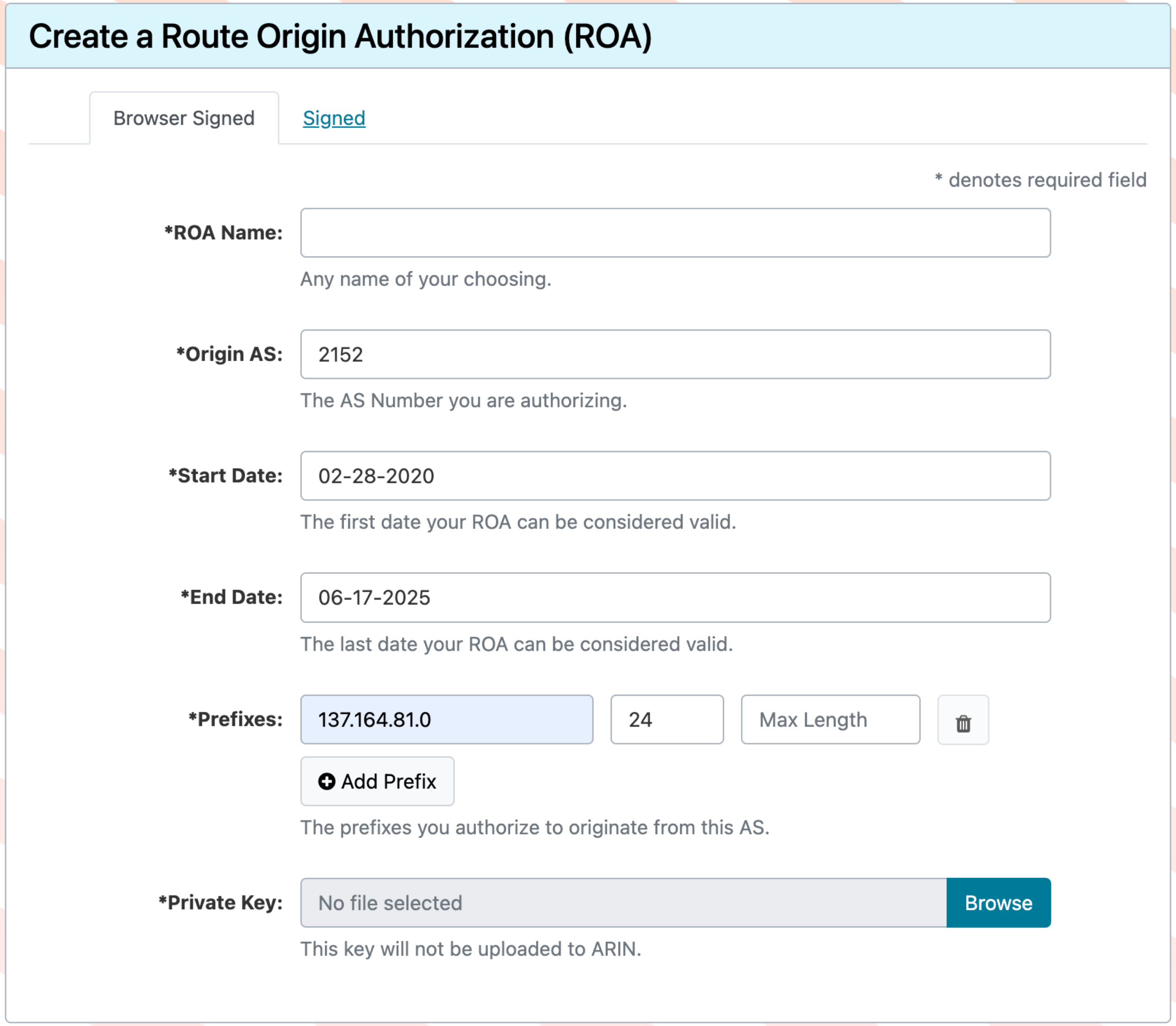
IP Networks

The following IPv4 and IPv6 networks are covered by the Resource Certificate.

Net Handle	Net Name	Network Range
NET6-2607-F380-1	CALREN	2607:F380::/32
NET-137-164-0-0-1	CALREN	137.164.0.0/16

Challenge: Generating our own ROAs (3/3)

- Cryptographic considerations:
  - What validity period? 2y? 5y? 10y?
  - How soon before expiration to renew?
  - How do we renew these in bulk?
- Security considerations:
  - Where do we store our private key for signing?
  - Who has access?
  - What if the key gets compromised?
  - If ARIN begins to offer private key hosting, do we take advantage?



Create a Route Origin Authorization (ROA)

* denotes required field

*ROA Name:

Any name of your choosing.

*Origin AS: 2152

The AS Number you are authorizing.

*Start Date: 02-28-2020

The first date your ROA can be considered valid.

*End Date: 06-17-2025

The last date your ROA can be considered valid.

*Prefixes: 137.164.81.0 24 Max Length

The prefixes you authorize to originate from this AS.

*Private Key: No file selected

This key will not be uploaded to ARIN.

Thank You

Christopher Bruton (he/him)
Core Engineer at CENIC (AS 2152)
cbruton@cenic.org
https://www.linkedin.com/in/christopherbruton