RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RPKI

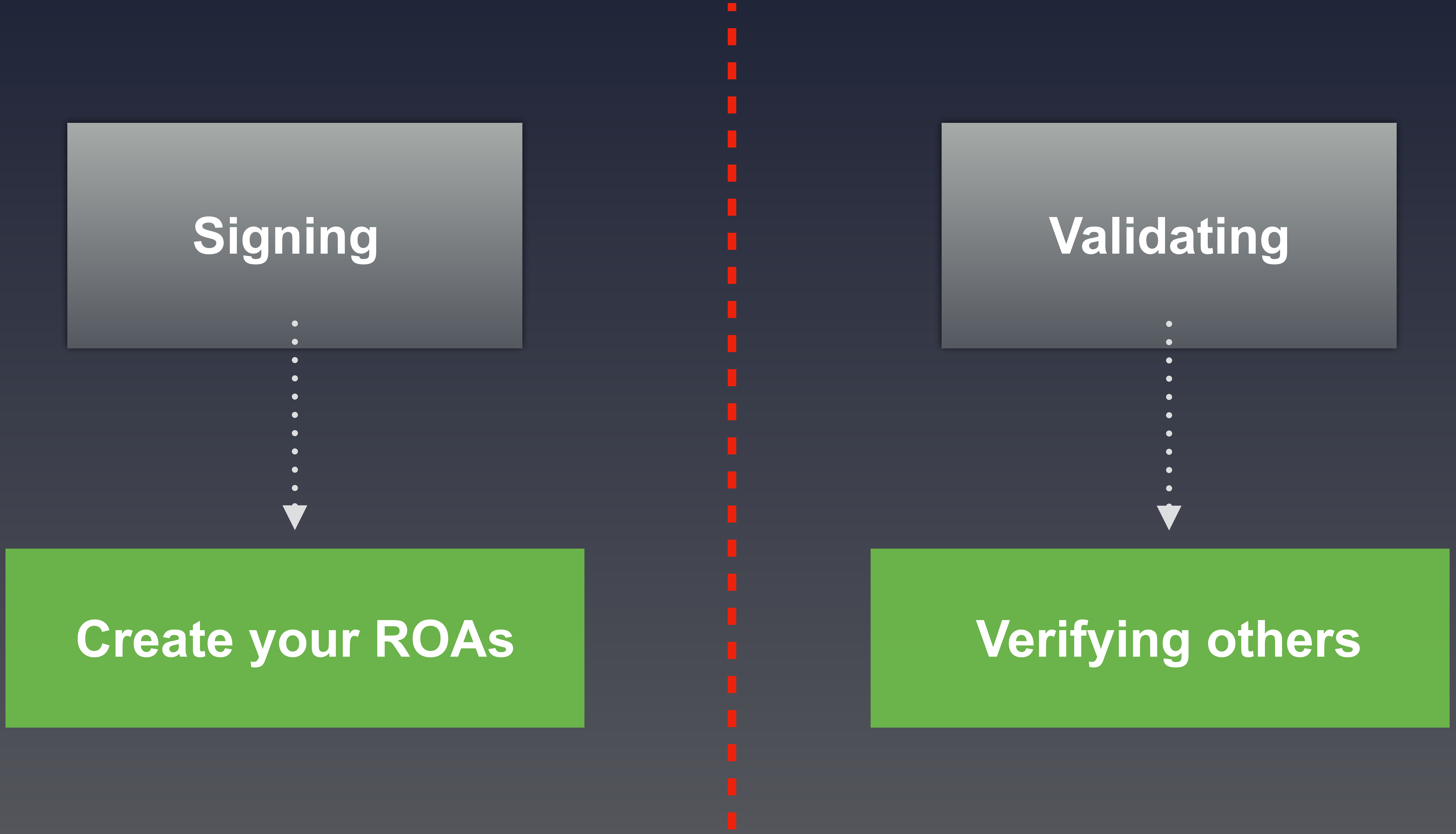
Securing the Internet One Hop at a Time

Nathalie Trenaman | LINX Presents | 26 January 2021

Resource Public Key Infrastructure

- Ties IP addresses and ASNs to public keys
- Follows the hierarchy of the registries
- Authorised statements from resource holders
  - “ASN X is authorised to announce my Prefix Y”
  - Signed, holder of Y

Two Elements of RPKI



Signing

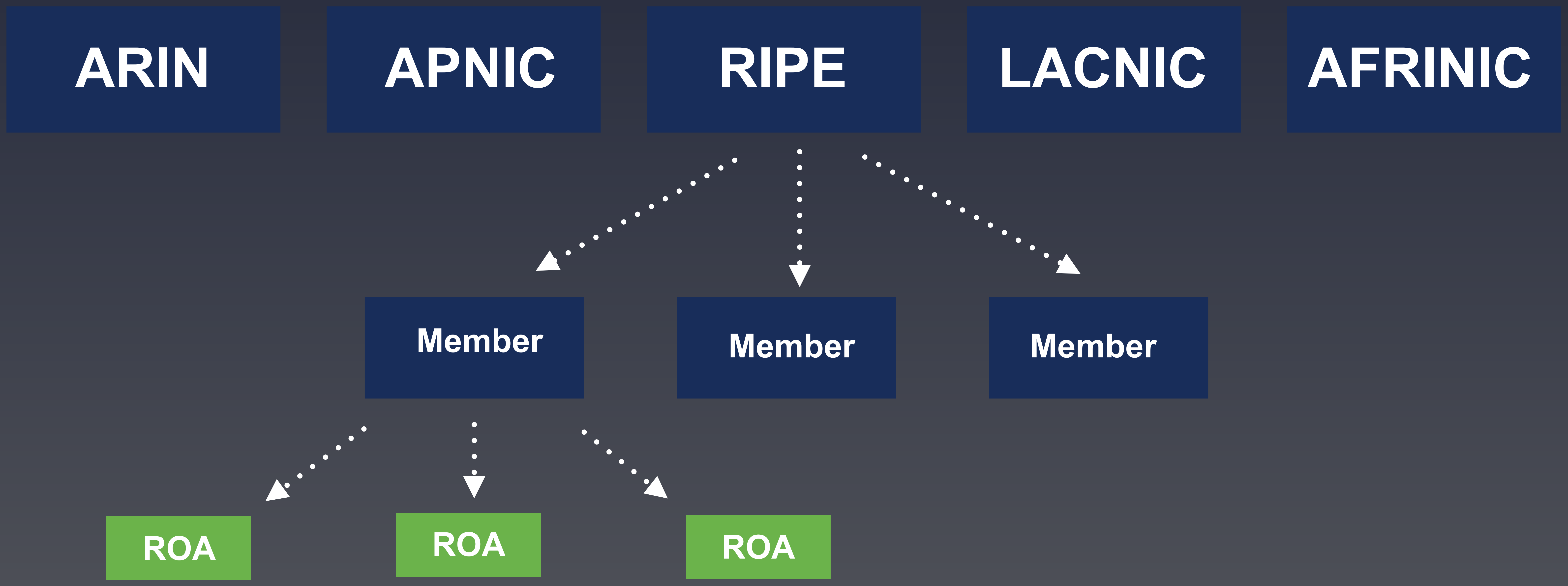
Create your ROAs

Validating

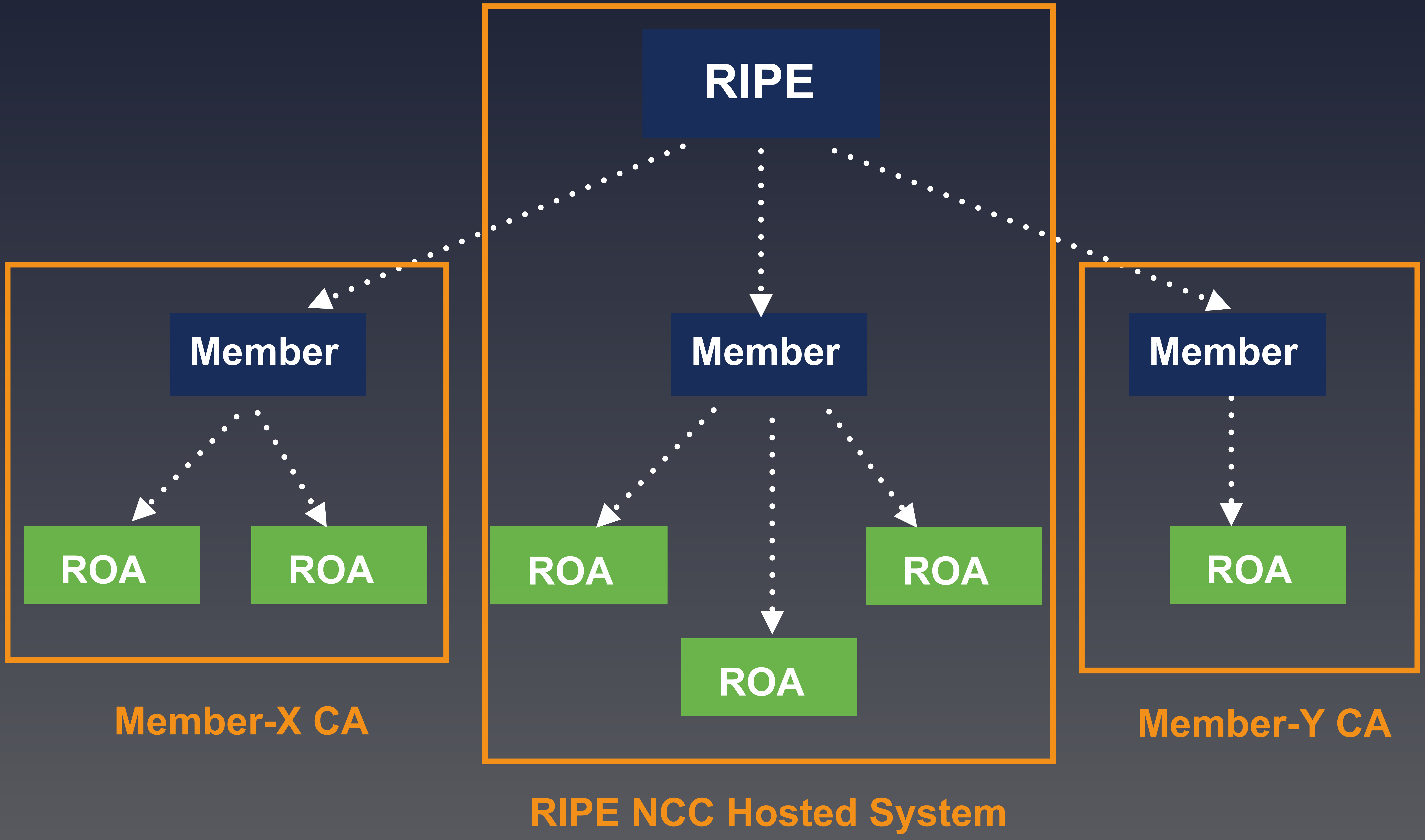
Verifying others

RPKI Certificate Structure

Certificate hierarchy follows allocation hierarchy



Hosted or Delegated RPKI



RPKI Challenges

2020: The Year of RPKI

- Serious uptake in Route Origin Validation at transits and IXPs
- Resulting in decrease of Invalid RPKI BGP announcements
- High uptake in signing objects at other Regional Internet Registries
- All major routing vendors are now on board
- Increase in delegated RPKI
- Also some outages at different Trust Anchors

What Happened?

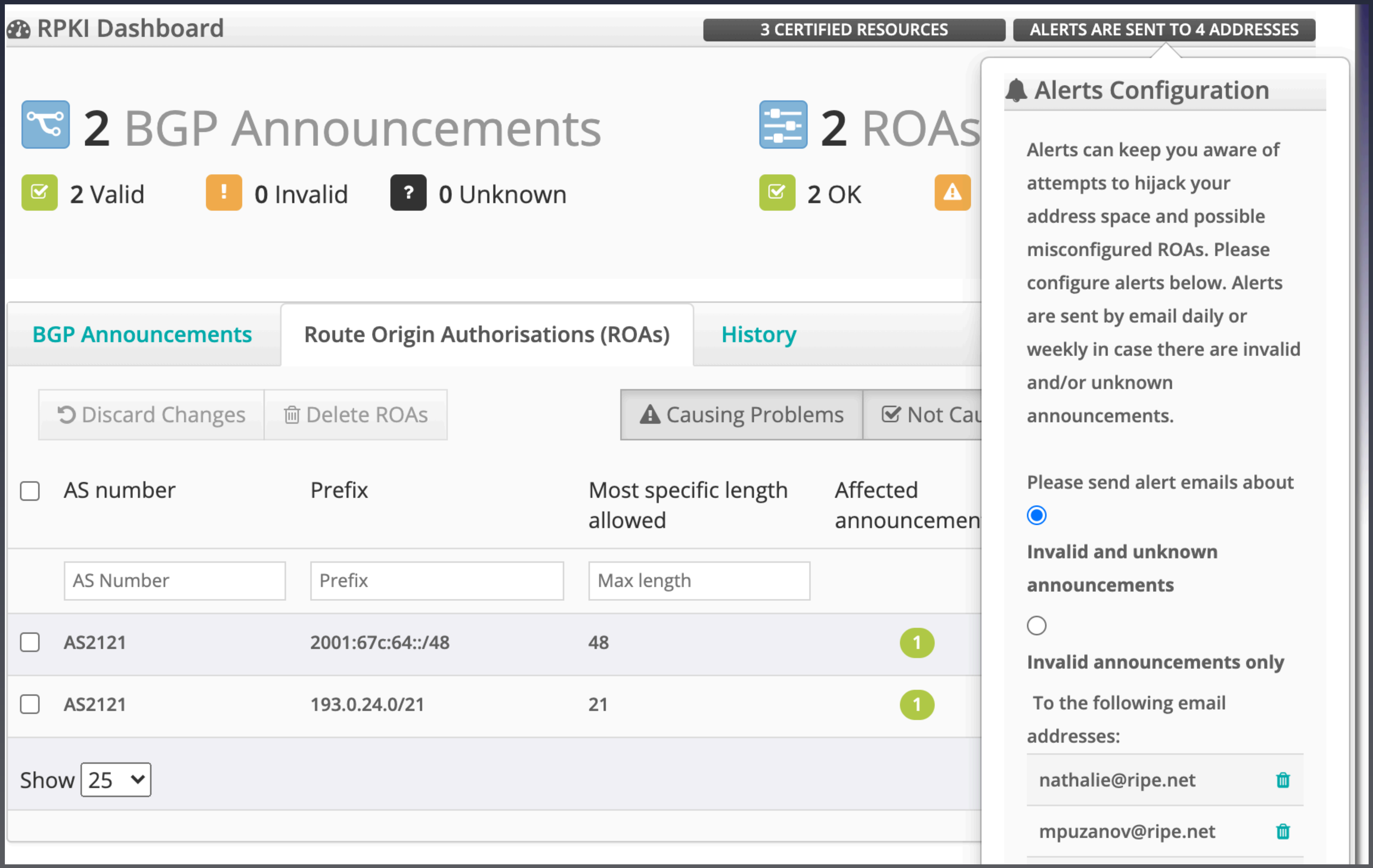
- 22 February 2020: Certificate Revocation List (CRL) expired
    - Full disk resulted in an expired CRL – went unnoticed on our side
    - Some Validators didn’t notice this
    - Sparked a discussion in the IETF about unified stricter behaviour of validation software
    - We improved our monitoring
- 3 April 2020: 2,669 ROAs got deleted
    - Update of the registry software resulted in a mismatch of resources in RPKI
    - RIPE NCC decided to restore all deleted ROAs
    - Added checks between the different software

And There Was More…..

- 6 April 2020: rsync repository was unavailable for 7 hours
  - Servers reached maximum capacity pool size
  - A malfunctioning client was hanging and established many new connections
  - We enhanced the maximum capacity pool size
  - We’re (also) moving rsync to the cloud
- 12 August 2020: Manifest encoding issue at ARIN
  - Went unnoticed for some Validator software
  - ARIN expanded their test environment with additional Validator software

What Can You Do?

- Set up alerts in the LIR Portal



RPKI Dashboard

3 CERTIFIED RESOURCES | ALERTS ARE SENT TO 4 ADDRESSES

2 BGP Announcements

☑ 2 Valid | ! 0 Invalid | ? 0 Unknown

2 ROAs

☑ 2 OK | ⚠

BGP Announcements | Route Origin Authorisations (ROAs) | History

Discard Changes | Delete ROAs | ⚠ Causing Problems | ☑ Not Cau

□	AS number	Prefix	Most specific length allowed	Affected announcemen
	AS Number	Prefix	Max length	
□	AS2121	2001:67c:64::/48	48	1
□	AS2121	193.0.24.0/21	21	1

Show 25

Alerts Configuration

Alerts can keep you aware of attempts to hijack your address space and possible misconfigured ROAs. Please configure alerts below. Alerts are sent by email daily or weekly in case there are invalid and/or unknown announcements.

Please send alert emails about

● **Invalid and unknown announcements**

○ **Invalid announcements only**

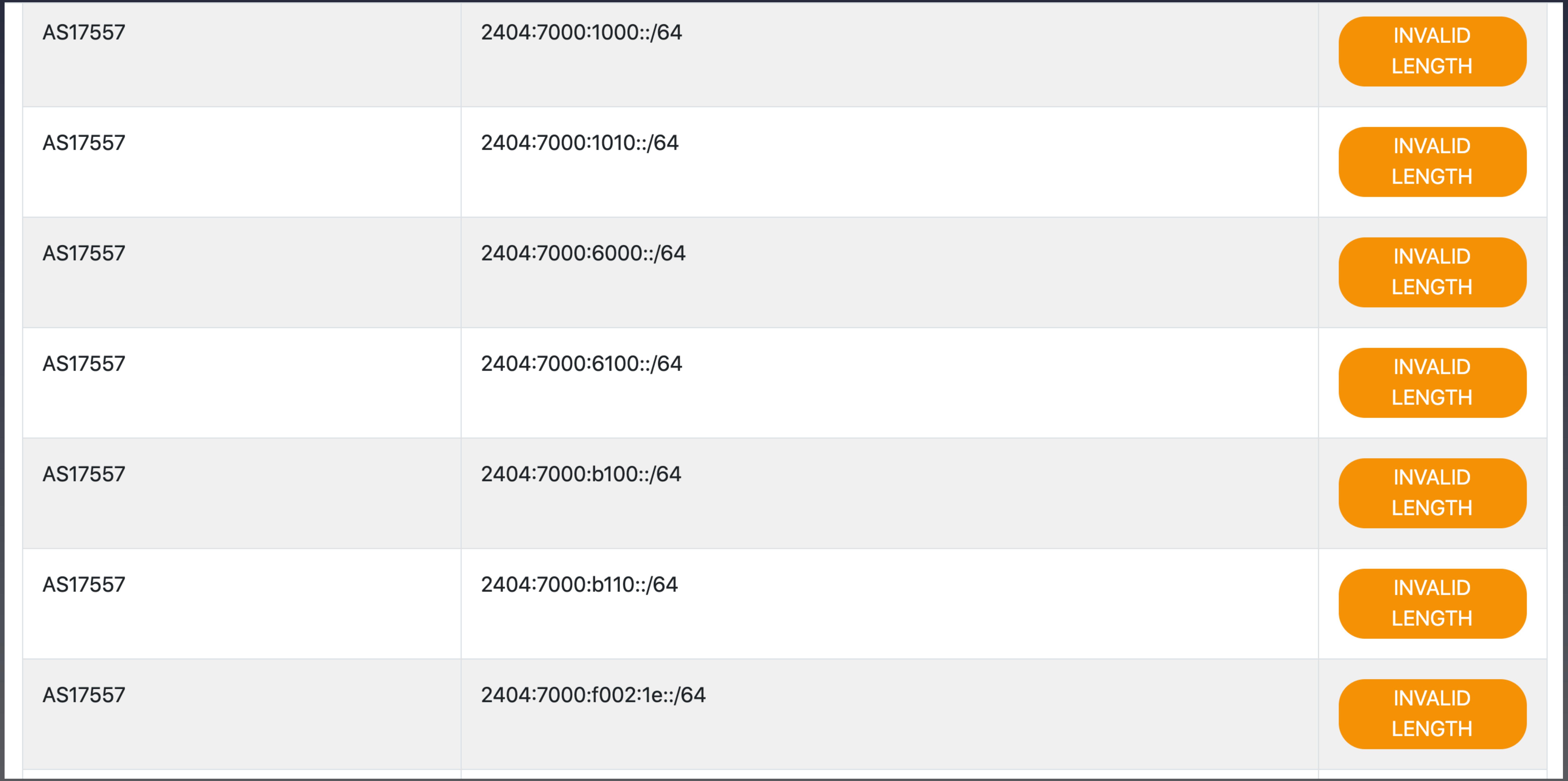
To the following email addresses:

nathalie@ripe.net

mpuzanov@ripe.net

What Else Can You Do?

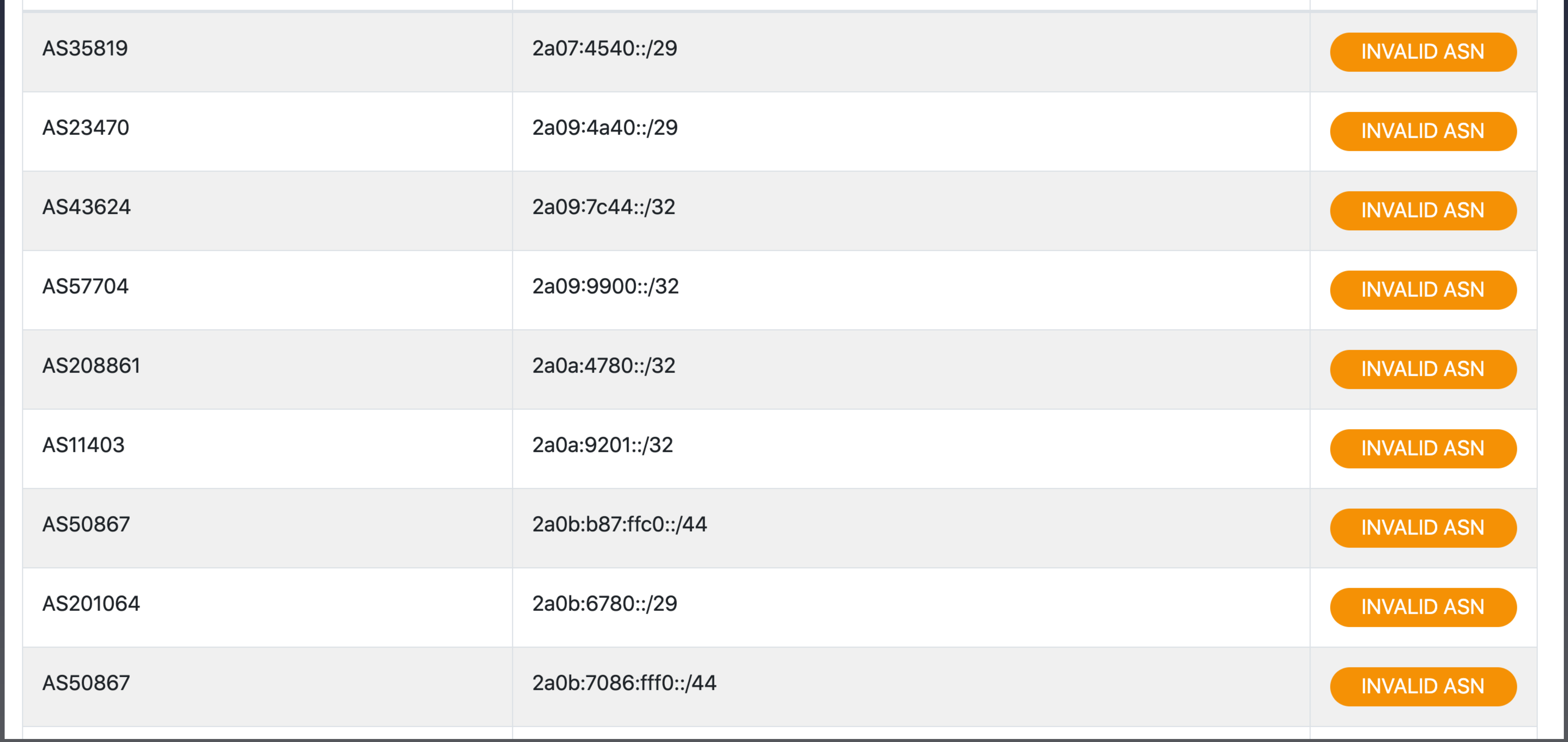
- Make sure your MaxLength matches your intent



AS17557	2404:7000:1000::/64	INVALID LENGTH
AS17557	2404:7000:1010::/64	INVALID LENGTH
AS17557	2404:7000:6000::/64	INVALID LENGTH
AS17557	2404:7000:6100::/64	INVALID LENGTH
AS17557	2404:7000:b100::/64	INVALID LENGTH
AS17557	2404:7000:b110::/64	INVALID LENGTH
AS17557	2404:7000:f002:1e::/64	INVALID LENGTH

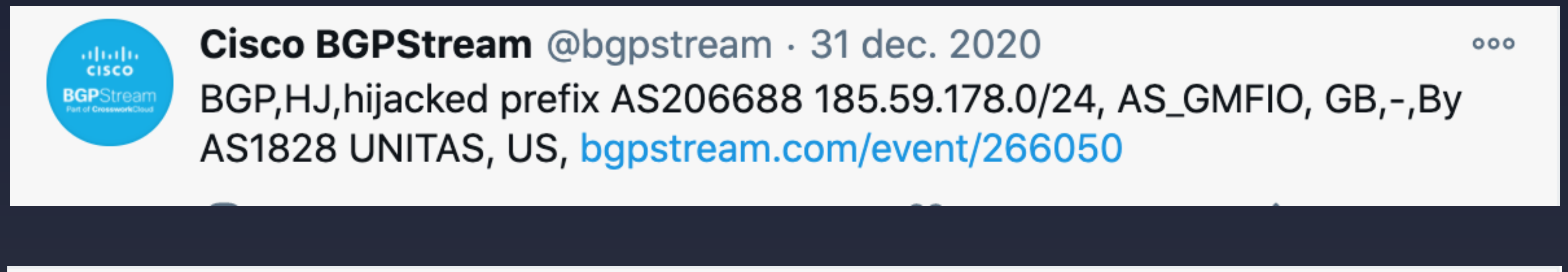
What Else Can You Do?

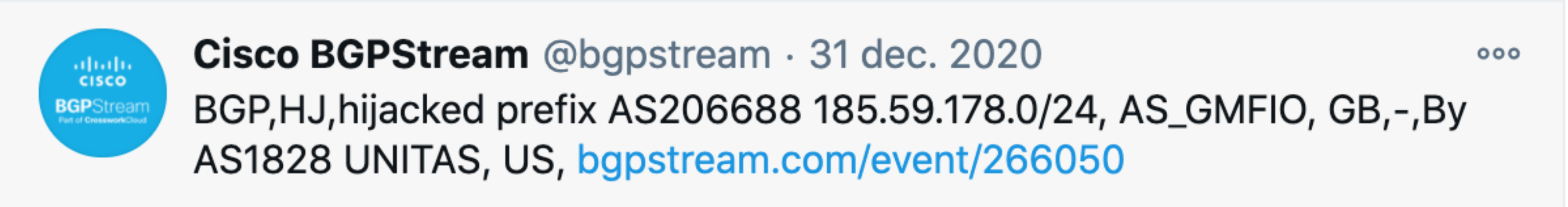
- Make sure your AS Number matches your intent

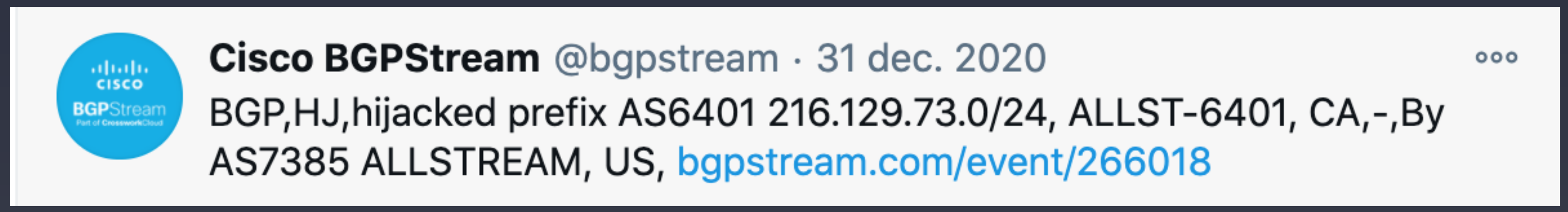


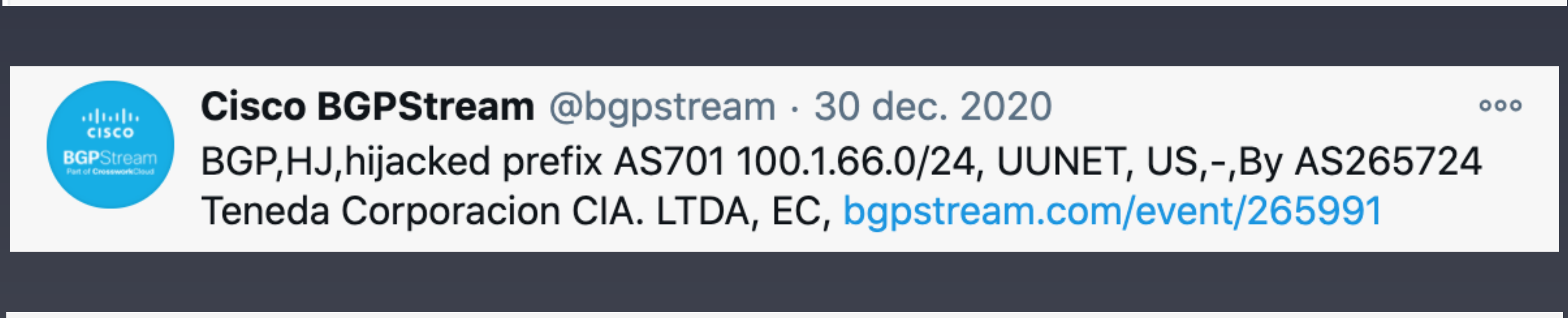
AS35819	2a07:4540::/29	INVALID ASN
AS23470	2a09:4a40::/29	INVALID ASN
AS43624	2a09:7c44::/32	INVALID ASN
AS57704	2a09:9900::/32	INVALID ASN
AS208861	2a0a:4780::/32	INVALID ASN
AS11403	2a0a:9201::/32	INVALID ASN
AS50867	2a0b:b87:ffc0::/44	INVALID ASN
AS201064	2a0b:6780::/29	INVALID ASN
AS50867	2a0b:7086:fff0::/44	INVALID ASN

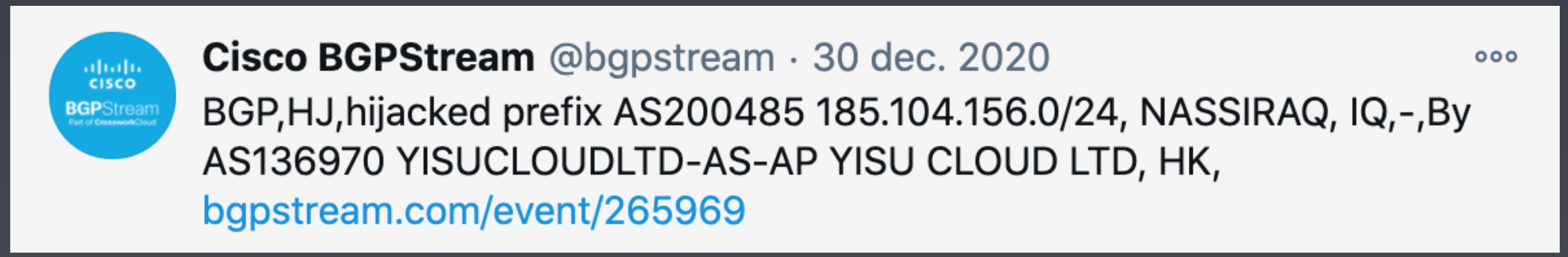
So, How Bad Are Things?

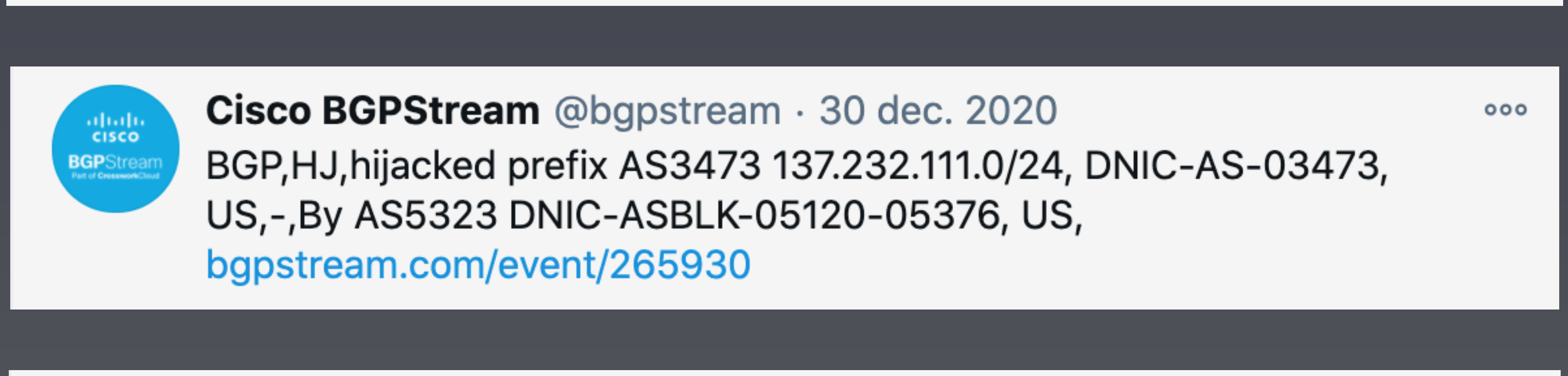

Cisco BGPStream @bgpstream · 31 dec. 2020
BGP,HJ,hijacked prefix AS206688 185.59.178.0/24, AS_GMFIO, GB,-,By AS1828 UNITAS, US, bgpstream.com/event/266050

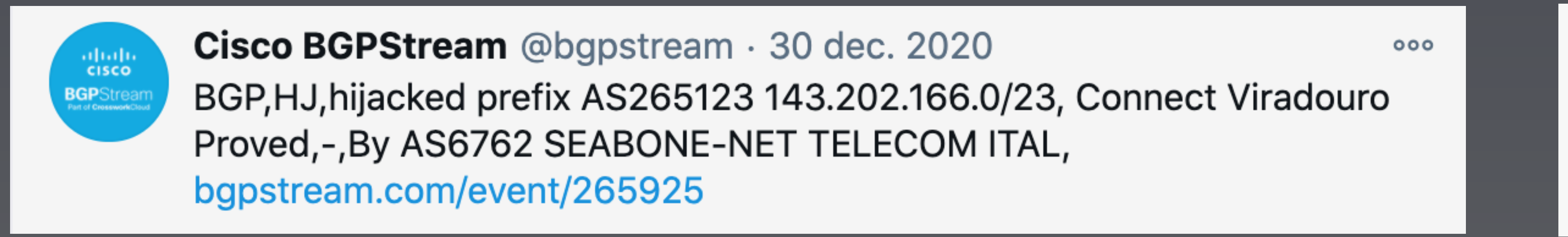

Cisco BGPStream @bgpstream · 31 dec. 2020
BGP,HJ,hijacked prefix AS206688 185.59.178.0/24, AS_GMFIO, GB,-,By AS1828 UNITAS, US, bgpstream.com/event/266050

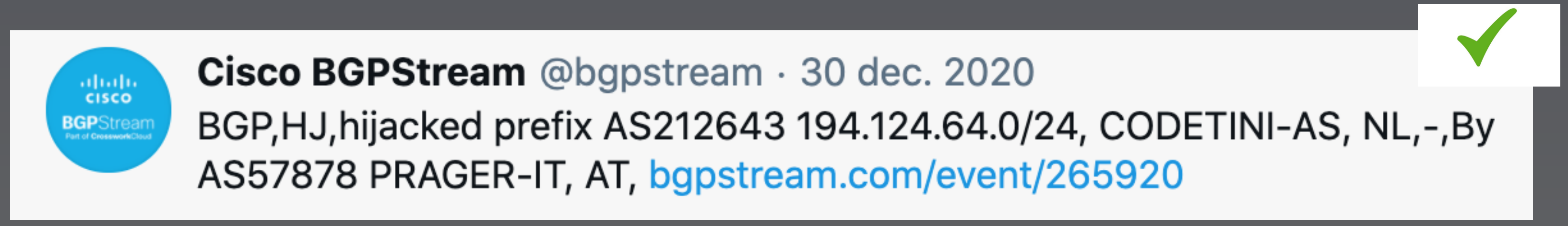

Cisco BGPStream @bgpstream · 31 dec. 2020
BGP,HJ,hijacked prefix AS6401 216.129.73.0/24, ALLST-6401, CA,-,By AS7385 ALLSTREAM, US, bgpstream.com/event/266018

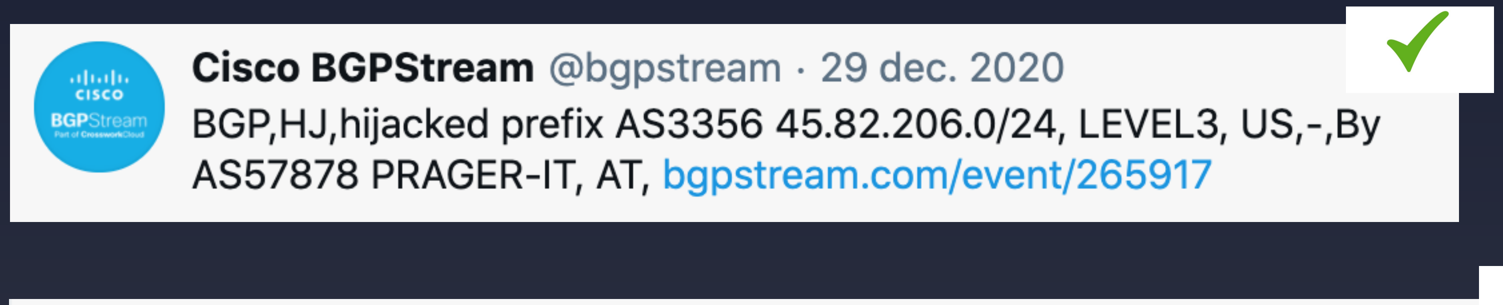

Cisco BGPStream @bgpstream · 30 dec. 2020
BGP,HJ,hijacked prefix AS701 100.1.66.0/24, UUNET, US,-,By AS265724 Teneda Corporacion CIA. LTDA, EC, bgpstream.com/event/265991

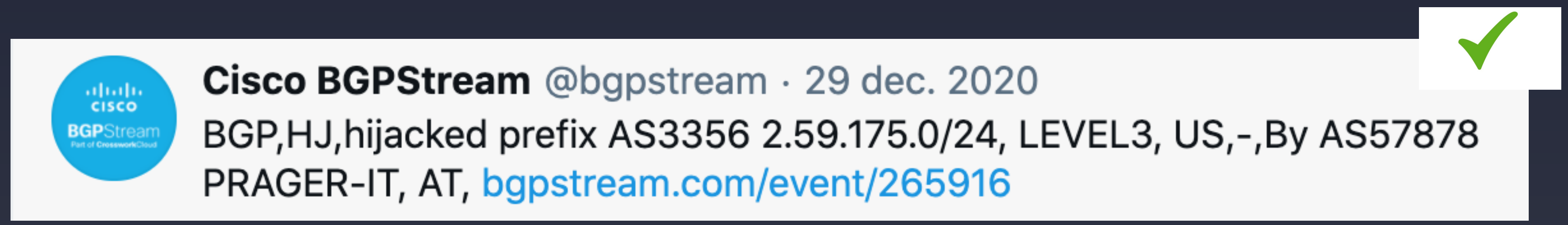

Cisco BGPStream @bgpstream · 30 dec. 2020
BGP,HJ,hijacked prefix AS200485 185.104.156.0/24, NASSIRAQ, IQ,-,By AS136970 YISUCLOUDLTD-AS-AP YISU CLOUD LTD, HK, bgpstream.com/event/265969

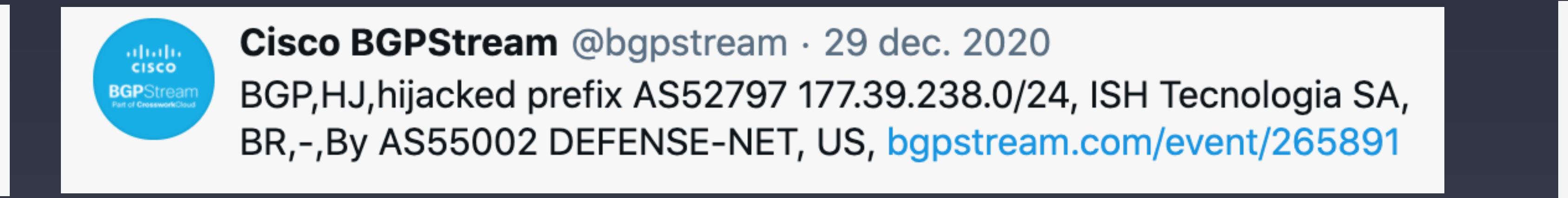

Cisco BGPStream @bgpstream · 30 dec. 2020
BGP,HJ,hijacked prefix AS3473 137.232.111.0/24, DNIC-AS-03473, US,-,By AS5323 DNIC-ASBLK-05120-05376, US, bgpstream.com/event/265930

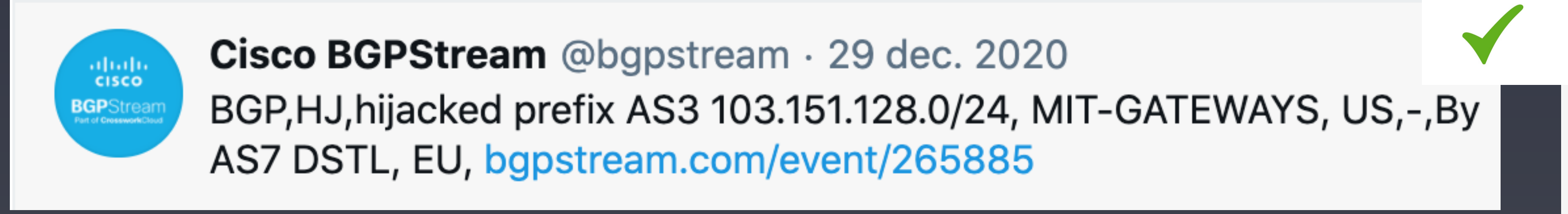

Cisco BGPStream @bgpstream · 30 dec. 2020
BGP,HJ,hijacked prefix AS265123 143.202.166.0/23, Connect Viradouro Proved,-,By AS6762 SEABONE-NET TELECOM ITAL, bgpstream.com/event/265925

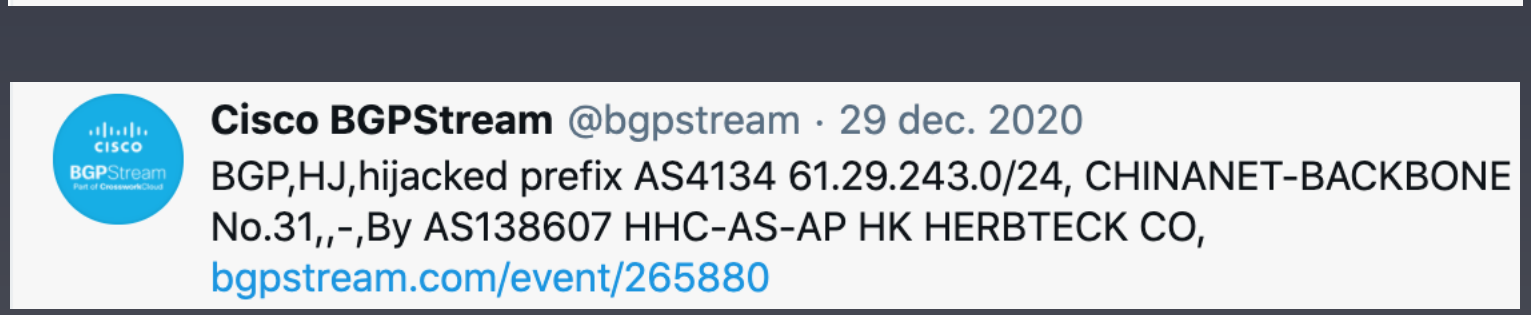

✓
Cisco BGPStream @bgpstream · 30 dec. 2020
BGP,HJ,hijacked prefix AS212643 194.124.64.0/24, CODETINI-AS, NL,-,By AS57878 PRAGER-IT, AT, bgpstream.com/event/265920

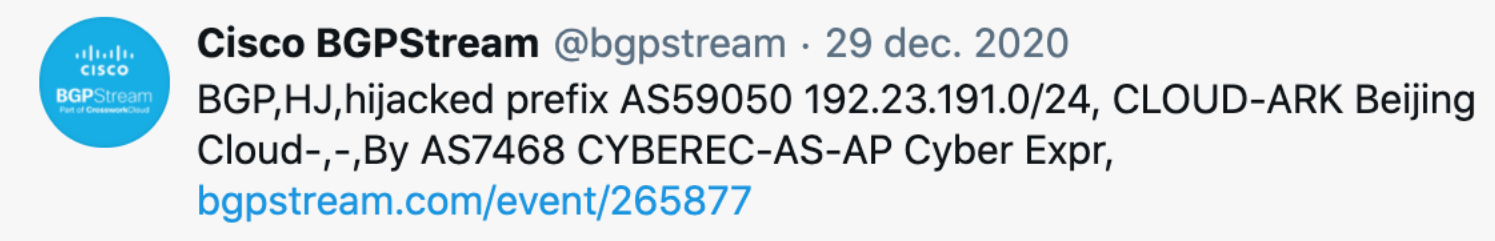

✓
Cisco BGPStream @bgpstream · 29 dec. 2020
BGP,HJ,hijacked prefix AS3356 45.82.206.0/24, LEVEL3, US,-,By AS57878 PRAGER-IT, AT, bgpstream.com/event/265917

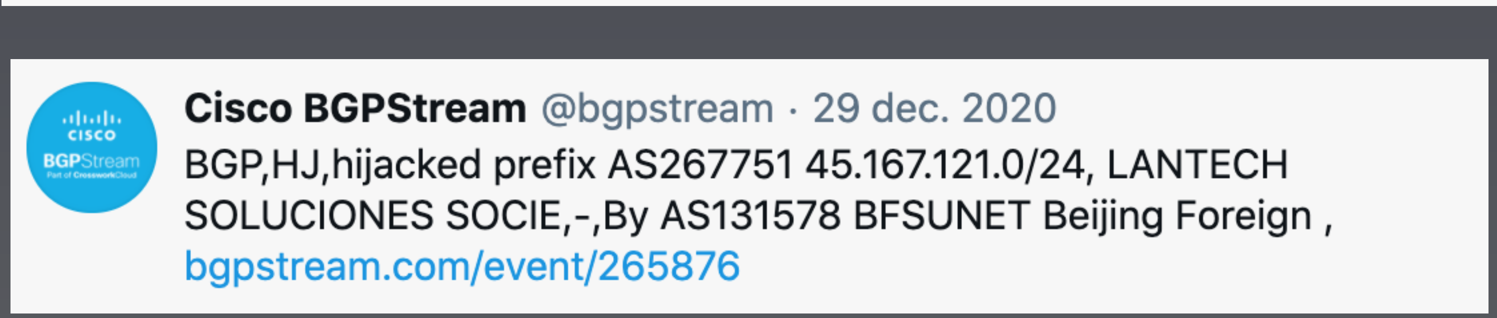

✓
Cisco BGPStream @bgpstream · 29 dec. 2020
BGP,HJ,hijacked prefix AS3356 2.59.175.0/24, LEVEL3, US,-,By AS57878 PRAGER-IT, AT, bgpstream.com/event/265916

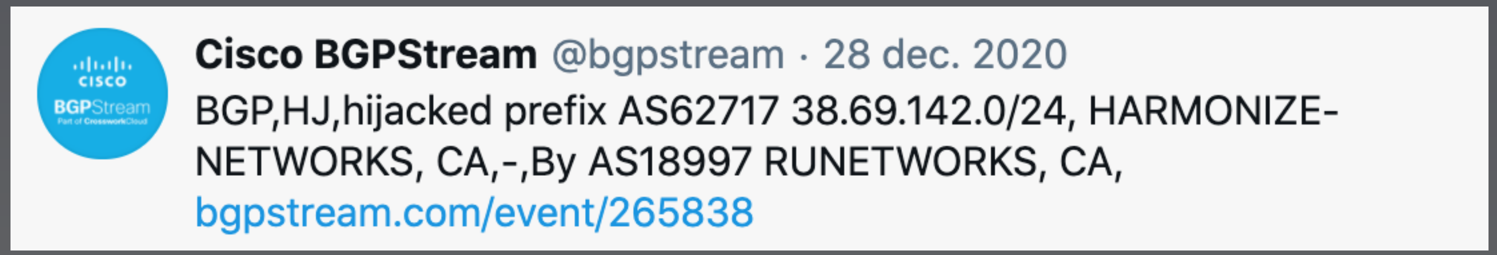

Cisco BGPStream @bgpstream · 29 dec. 2020
BGP,HJ,hijacked prefix AS52797 177.39.238.0/24, ISH Tecnologia SA, BR,-,By AS55002 DEFENSE-NET, US, bgpstream.com/event/265891

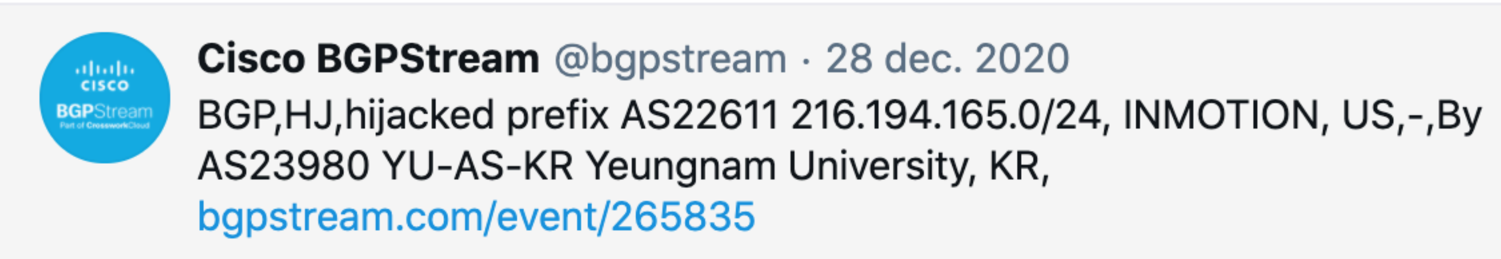

✓
Cisco BGPStream @bgpstream · 29 dec. 2020
BGP,HJ,hijacked prefix AS3 103.151.128.0/24, MIT-GATEWAYS, US,-,By AS7 DSTL, EU, bgpstream.com/event/265885

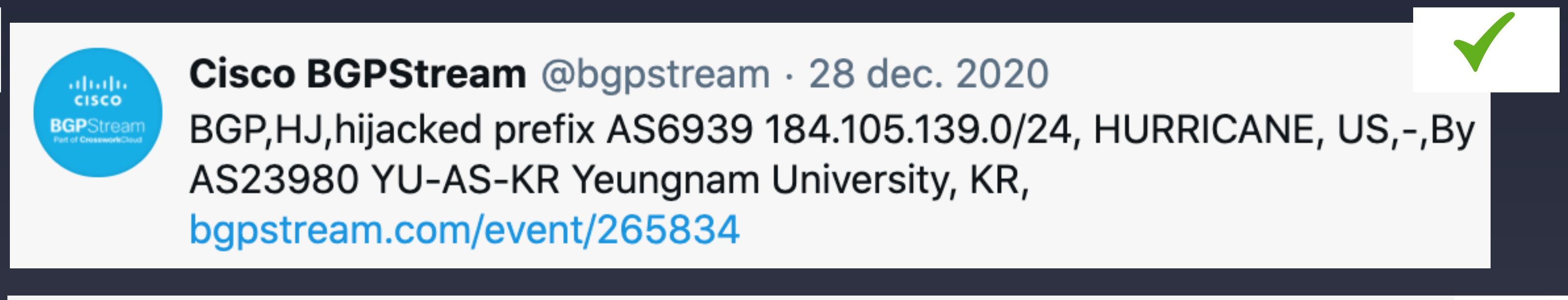

Cisco BGPStream @bgpstream · 29 dec. 2020
BGP,HJ,hijacked prefix AS4134 61.29.243.0/24, CHINANET-BACKBONE No.31,,-,By AS138607 HHC-AS-AP HK HERBTECK CO, bgpstream.com/event/265880

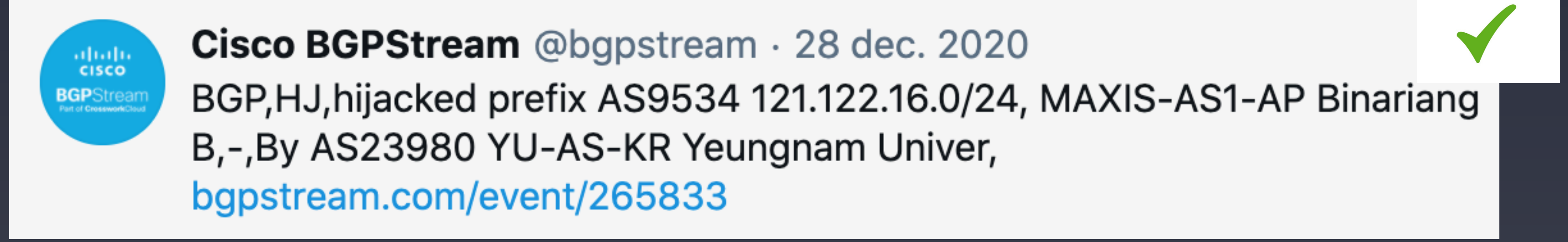

Cisco BGPStream @bgpstream · 29 dec. 2020
BGP,HJ,hijacked prefix AS59050 192.23.191.0/24, CLOUD-ARK Beijing Cloud-,-,By AS7468 CYBEREC-AS-AP Cyber Expr, bgpstream.com/event/265877

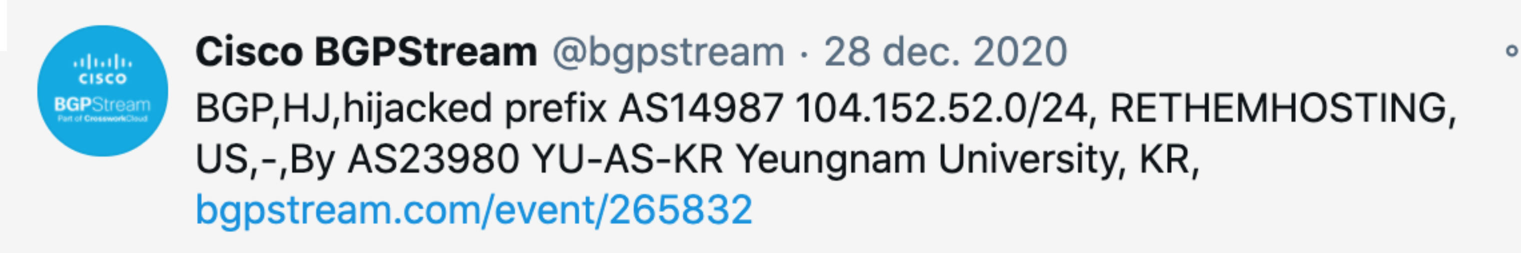

Cisco BGPStream @bgpstream · 29 dec. 2020
BGP,HJ,hijacked prefix AS267751 45.167.121.0/24, LANTECH SOLUCIONES SOCIE,-,By AS131578 BFSUNET Beijing Foreign , bgpstream.com/event/265876

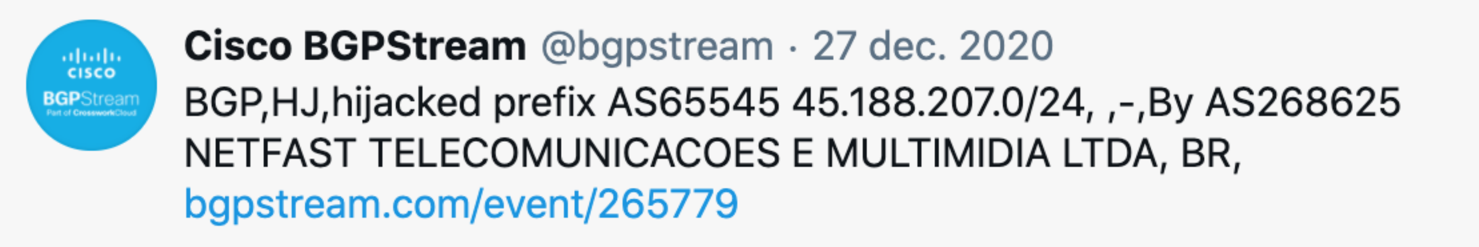

Cisco BGPStream @bgpstream · 28 dec. 2020
BGP,HJ,hijacked prefix AS62717 38.69.142.0/24, HARMONIZE-NETWORKS, CA,-,By AS18997 RUNETWORKS, CA, bgpstream.com/event/265838

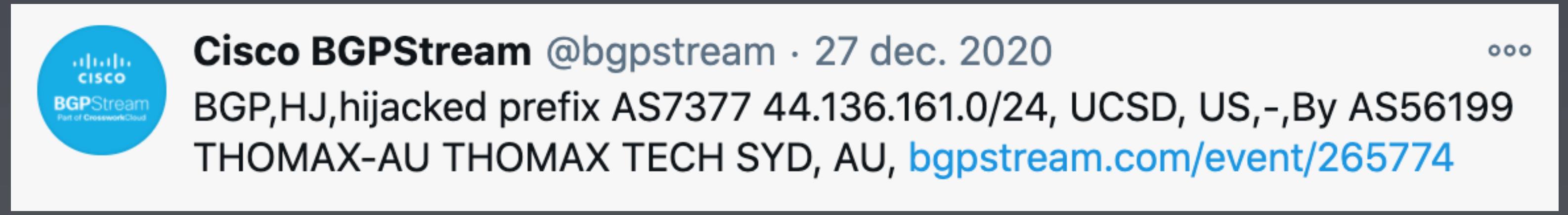

Cisco BGPStream @bgpstream · 28 dec. 2020
BGP,HJ,hijacked prefix AS22611 216.194.165.0/24, INMOTION, US,-,By AS23980 YU-AS-KR Yeungnam University, KR, bgpstream.com/event/265835

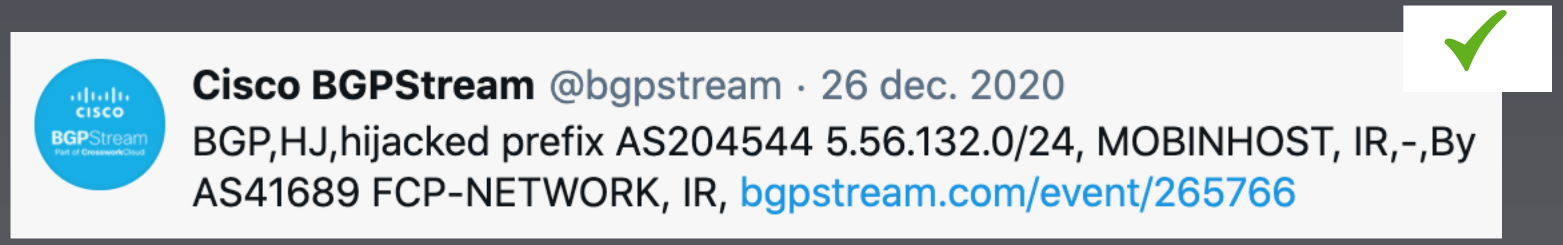

✓
Cisco BGPStream @bgpstream · 28 dec. 2020
BGP,HJ,hijacked prefix AS6939 184.105.139.0/24, HURRICANE, US,-,By AS23980 YU-AS-KR Yeungnam University, KR, bgpstream.com/event/265834

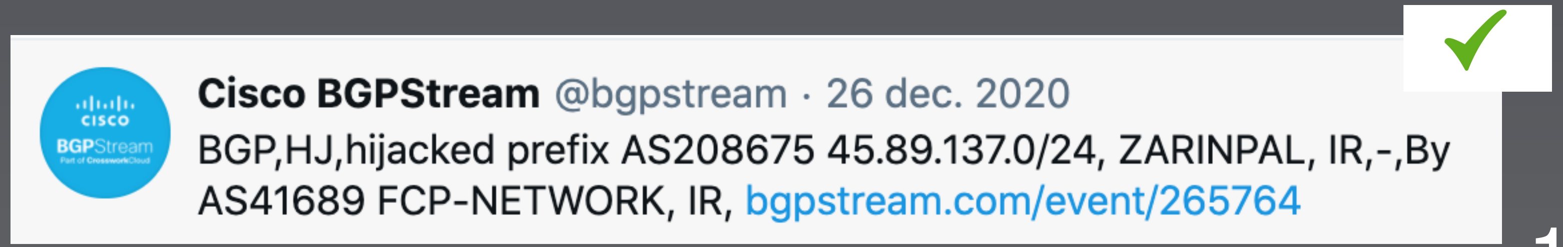

✓
Cisco BGPStream @bgpstream · 28 dec. 2020
BGP,HJ,hijacked prefix AS9534 121.122.16.0/24, MAXIS-AS1-AP Binariang B,-,By AS23980 YU-AS-KR Yeungnam Univer, bgpstream.com/event/265833


Cisco BGPStream @bgpstream · 28 dec. 2020
BGP,HJ,hijacked prefix AS14987 104.152.52.0/24, RETHEMHOSTING, US,-,By AS23980 YU-AS-KR Yeungnam University, KR, bgpstream.com/event/265832


Cisco BGPStream @bgpstream · 27 dec. 2020
BGP,HJ,hijacked prefix AS65545 45.188.207.0/24, ,-,By AS268625 NETFAST TELECOMUNICACOES E MULTIMIDIA LTDA, BR, bgpstream.com/event/265779


Cisco BGPStream @bgpstream · 27 dec. 2020
BGP,HJ,hijacked prefix AS7377 44.136.161.0/24, UCSD, US,-,By AS56199 THOMAX-AU THOMAX TECH SYD, AU, bgpstream.com/event/265774


✓
Cisco BGPStream @bgpstream · 26 dec. 2020
BGP,HJ,hijacked prefix AS204544 5.56.132.0/24, MOBINHOST, IR,-,By AS41689 FCP-NETWORK, IR, bgpstream.com/event/265766


✓
Cisco BGPStream @bgpstream · 26 dec. 2020
BGP,HJ,hijacked prefix AS208675 45.89.137.0/24, ZARINPAL, IR,-,By AS41689 FCP-NETWORK, IR, bgpstream.com/event/265764

Key Takeaways

- Creating a ROA helps – a lot!
- Most large transit providers and IXPs perform Route Origin Validation (ROV)
- Many ISPs that have BGP customers don’t. This is problematic.
- Just ROV is not the holy grail for all BGP mishaps.
  - We really need Path Validation

Plans for the Future of RPKI

At the RIPE NCC

Focus on Resiliency

- Significant improvements in metrics/monitoring finalised
  - Usage of Prometheus with Grafana for visualisations
  - Hooking up with SMS alerting for engineers on 24/7 duty
- Deployment of rsync/RRDP into AWS in progress
  - Multiple regions/availability zones with aim of very high availability
  - RRDP is already in AWS but with simpler architecture – the goal is to also move rsync to similar architecture
  - Redundant fully functional infrastructure in our current data centres to provide very high resiliency being evaluated by the teams

Focus on Security

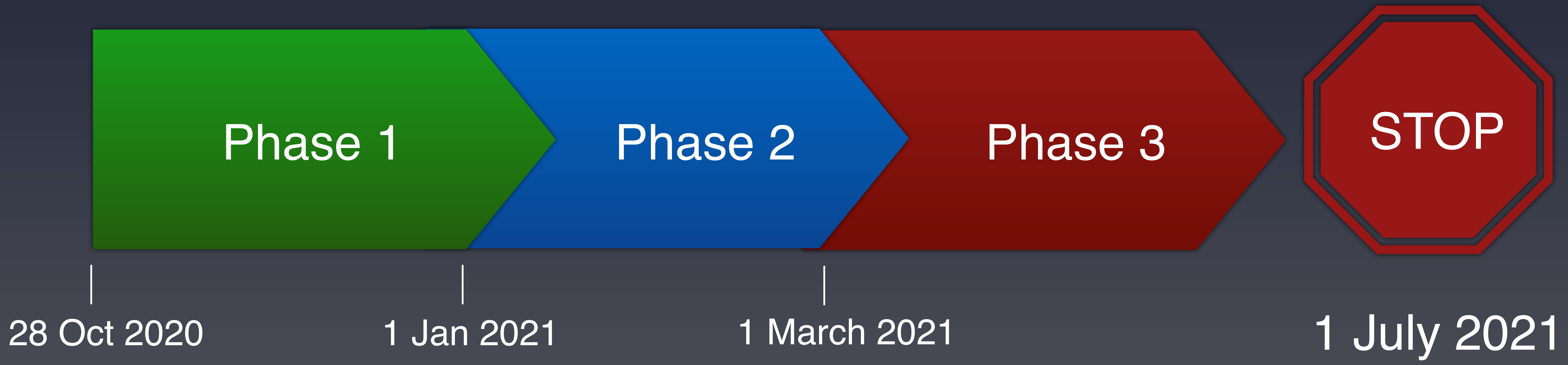
- Performed an RFC compliance audit
- Building an RPKI specific audit framework in SOC 2 type II
- For 2021:
  - Publish a report from the RFC compliance audit
  - Performing SOC 2 type II audit, publish a SOC 3 report
  - Performing penetration test
  - Performing Red Team test

Upcoming Work from the IETF

- Autonomous System Provider Authorisation (ASPA)
  - https://tools.ietf.org/html/draft-ietf-sidrops-aspa-profile-04
- Validation Reconsidered
  - https://tools.ietf.org/html/rfc8360
- Resource Tagged Attestations (RTA)
  - https://tools.ietf.org/html/draft-michaelson-rpki-rta-02

Deprecating the RIPE NCC Validator

Timeline



Phase 1

Phase 2

Phase 3

STOP

28 Oct 2020

1 Jan 2021

1 March 2021

1 July 2021

Phase 1

- 28 October 2020 - 31 December 2021
- Work continues as normal:
  - Features
  - RFC implementations
  - Policy implementations (AS0 in other regions)
  - Bug fixes
  - Security fixes
- Community will be informed of future timeline

Phase 2

- 1 January 2021 - 28 February 2021
- No new features will be implemented
- Continued work on:
  - RFC implementations
  - Policy implementations (AS0 in other regions)
  - Bug fixes
  - Security fixes
- Training material and website will be updated

Phase 3

- 1 March 2021 - 30 June 2021
- No more work on RFC and policy implementations
- Continued work on:
  - Bug fixes
  - Security fixes
- On 1 July 2021, we will archive the RIPE NCC RPKI Validator

Alternatives

- All are open source:
  - Routinator - https://github.com/NLnetLabs/routinator/
  - FORT - https://github.com/NICMx/FORT-validator/
  - OctoRPKI - https://github.com/cloudflare/cfrpki
  - RPKI-client - https://rpki-client.org/
  - Prover - https://github.com/lolepezy/rpki-prover
  - Rpstir2 - https://github.com/bgpsecurity/rpstir2

Insiders Tips

Insiders Tips & Tricks

- It might take a few hours from the moment you create your ROA to making them appear in all Validators and BGP
- If you run your own CA, be aware that your repository is critical infrastructure
- Maintaining route objects and maintaining filters in BGP are still very important

How Do I Get Started?

- Read up! This is a great starting point:
  - https://rpki.readthedocs.io/en/latest/
- Create your ROAs:
  - https://my.ripe.net/#/rpki (login required)
- Download a Validator
  - Not from RIPE NCC :)
- Share your experience or ask for advice
  - https://www.ripe.net/mailman/listinfo/routing-wg/

Questions

nathalie@ripe.net
rpki@ripe.net