APNIC

RPKI
A year in review

RPKI
The Numbers

RPKI: The Numbers (ROA)

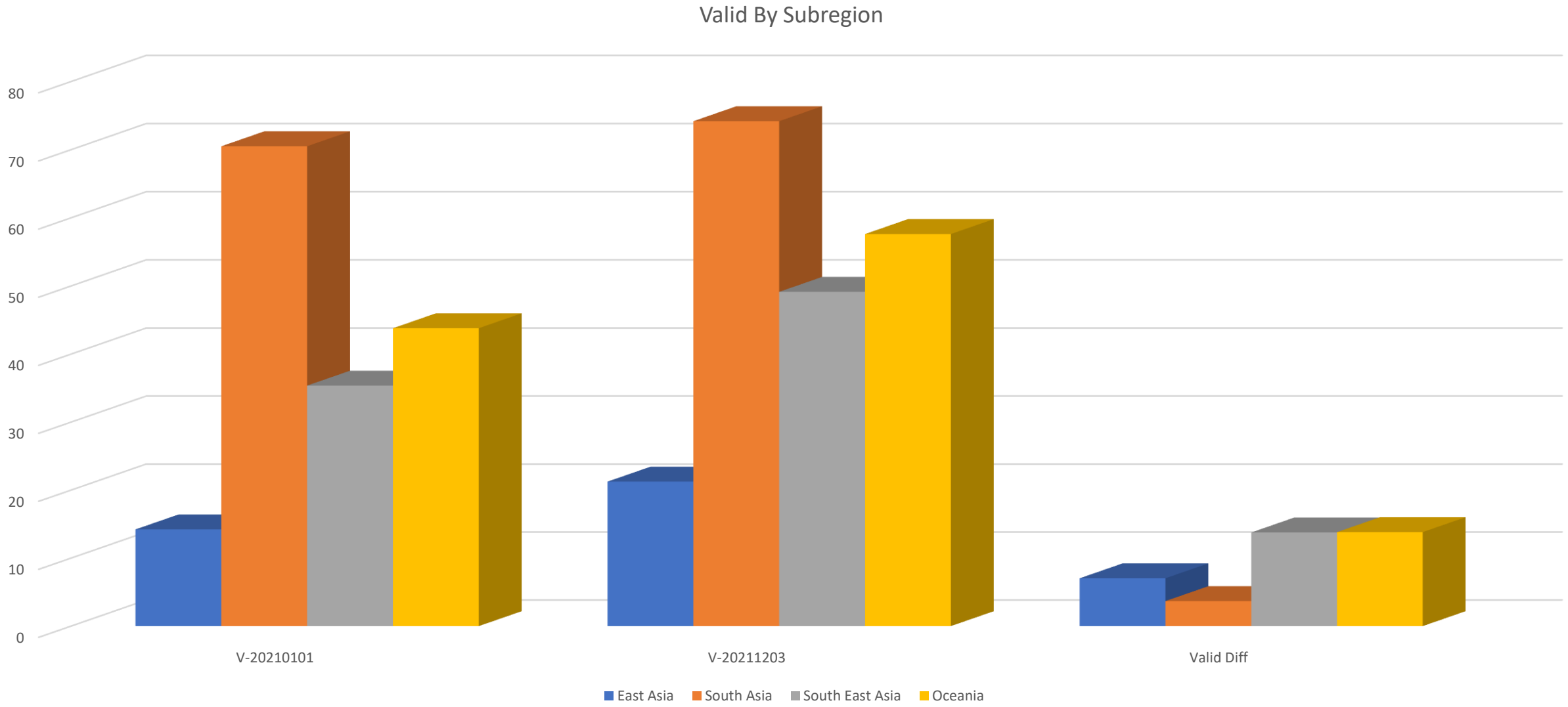
- **Global (IPv4)**
  - IPv4 Table Increase 864297 to 922699 (6.3%)
  - VALID Increase from 36.27% to 46.24% (9.97%)
  - INVALID Increase from 0.07% to 0.2% (0.13%)
    - ML 4154 to 5472 (24% Increase)
    - AS 1303 to 1681 (22% Increase)
    - ASML 1048 to 1238 (15% Increase)
  - NOT FOUND Decrease from 73.17 to 67.91%(5.26%)
  - Why have NOT FOUND not dropped in proportion to VALID?
    - New Allocations?
    - De-aggregation?

RPKI: The Numbers (ROA)

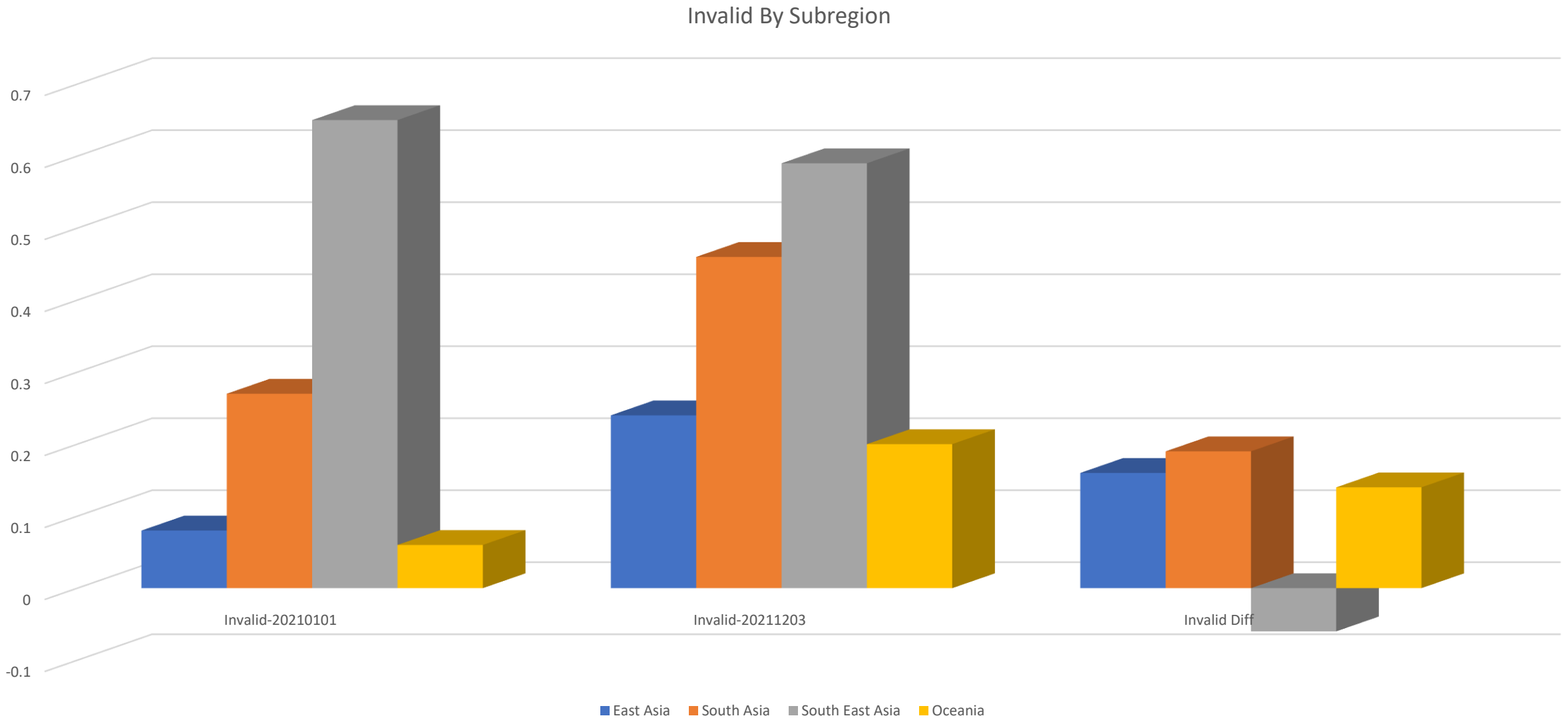
- **APAC (IPv4)**
  - IPv4 Delegations (/23) Net Increase of 0.16% (2782 X /23)
  - VALID Increase from 40.97% to 50.55% (9.57%)
  - INVALID Increase from 0.26% to 0.37% (0.11%)
  - NOT FOUND Decrease from 59.27% to 49.25%(10.02%)

  - Valid increase is on par with Global
    - We are a well represented region (we'll come to that soon)
  - Invalid is marginally better than Global
  - Not found is pleasing
    - Some large scale aggregation in some sub-regions
    - Push from Upstream providers to downstreams for entities to sign.

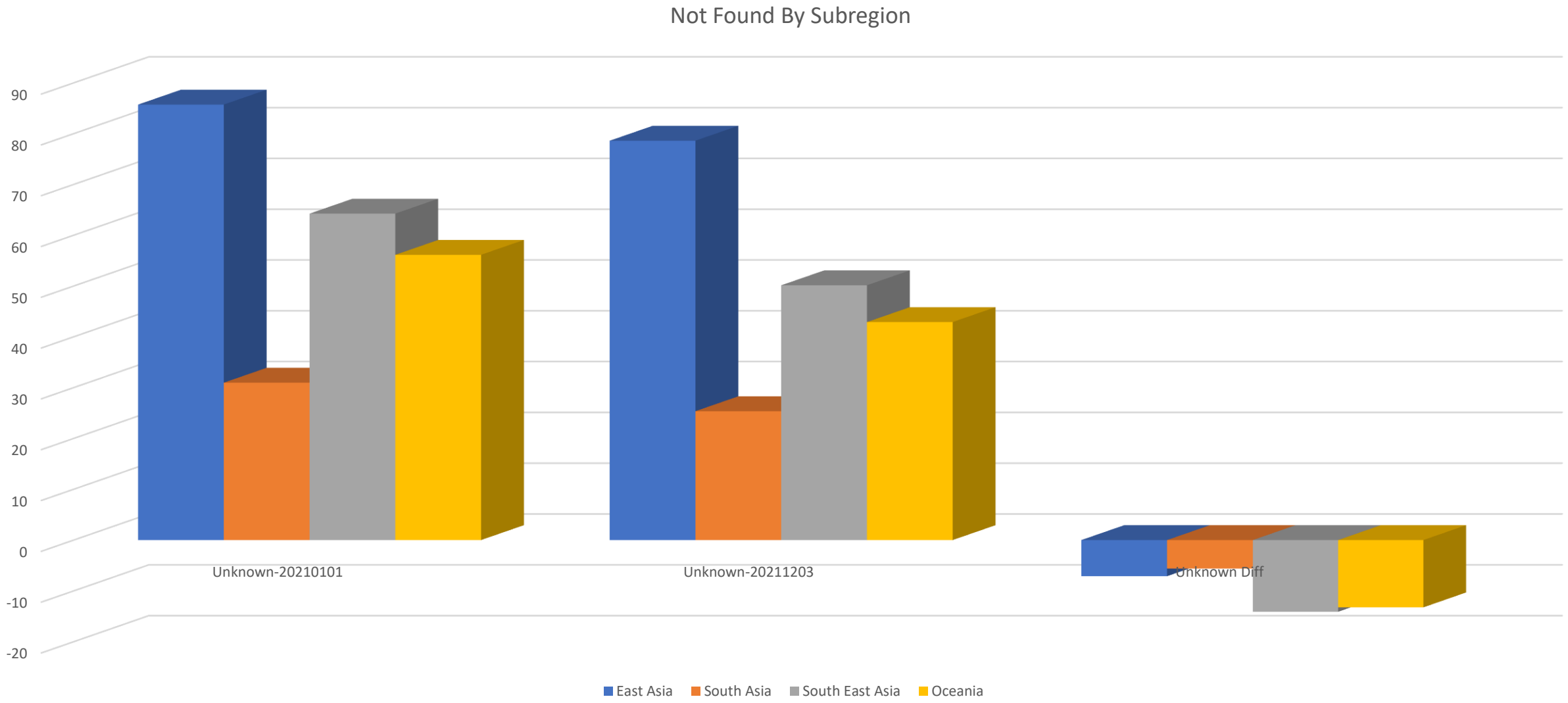
RPKI: The Numbers(Subregions)



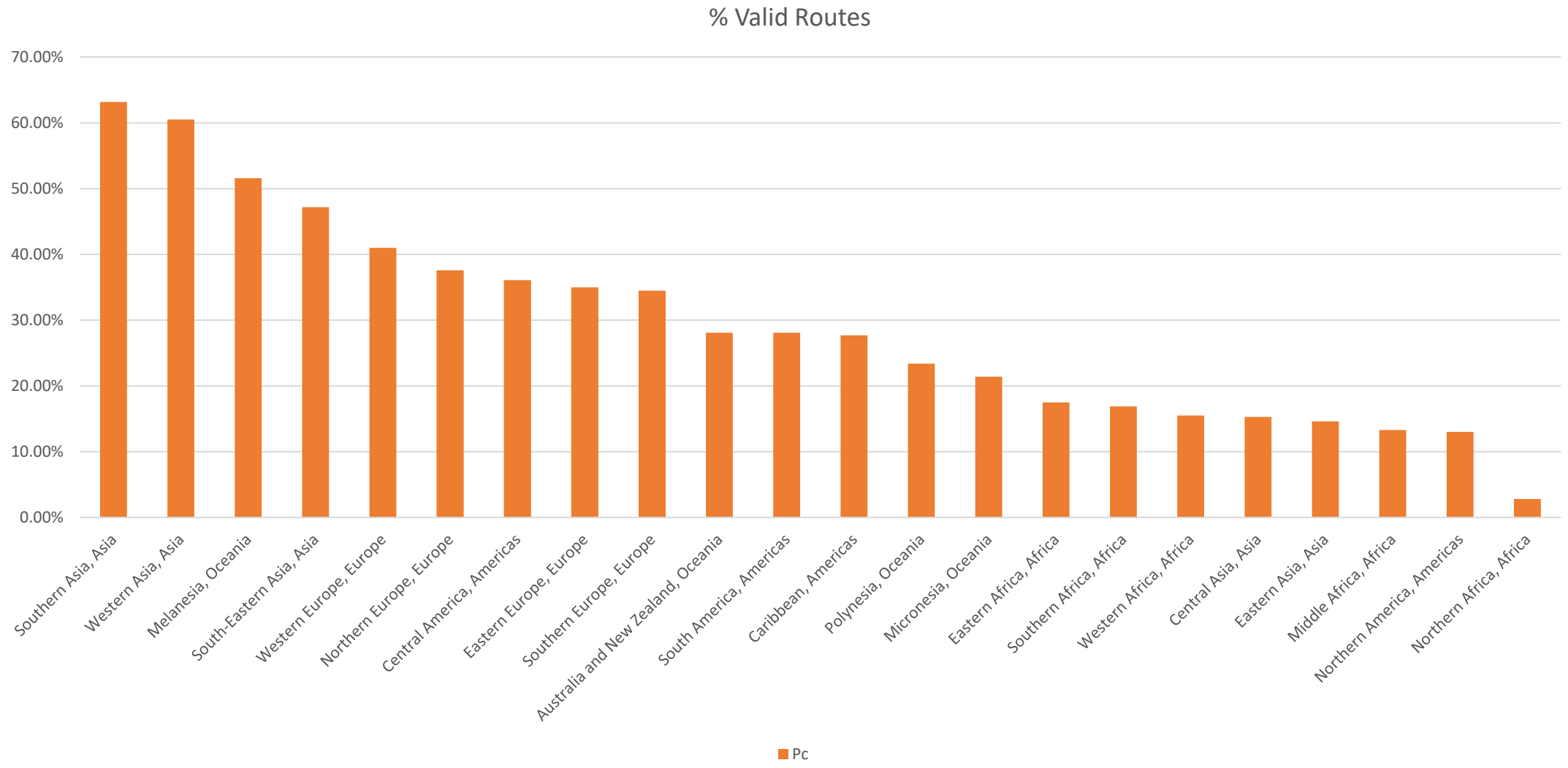
RPKI: The Numbers(Subregions)



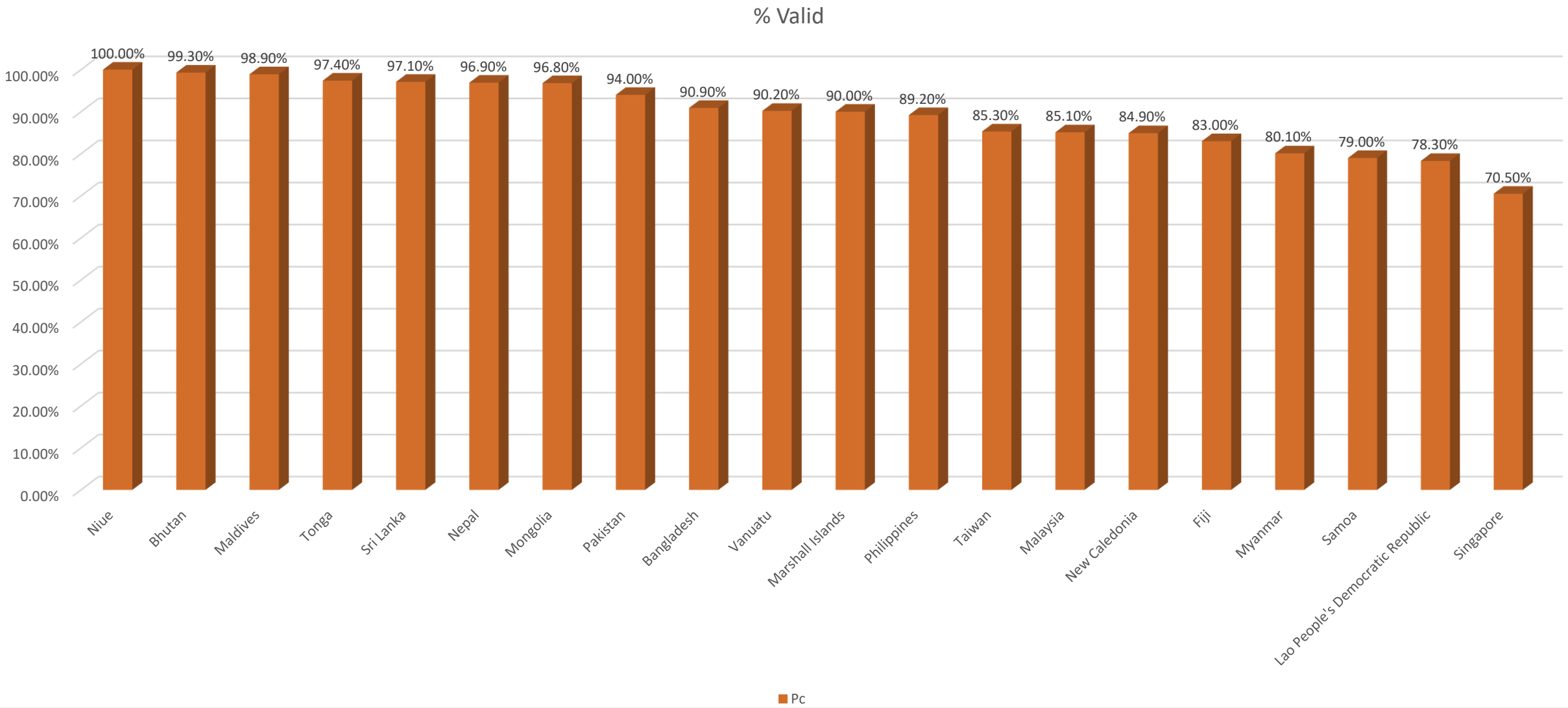
RPKI: The Numbers(Subregions)



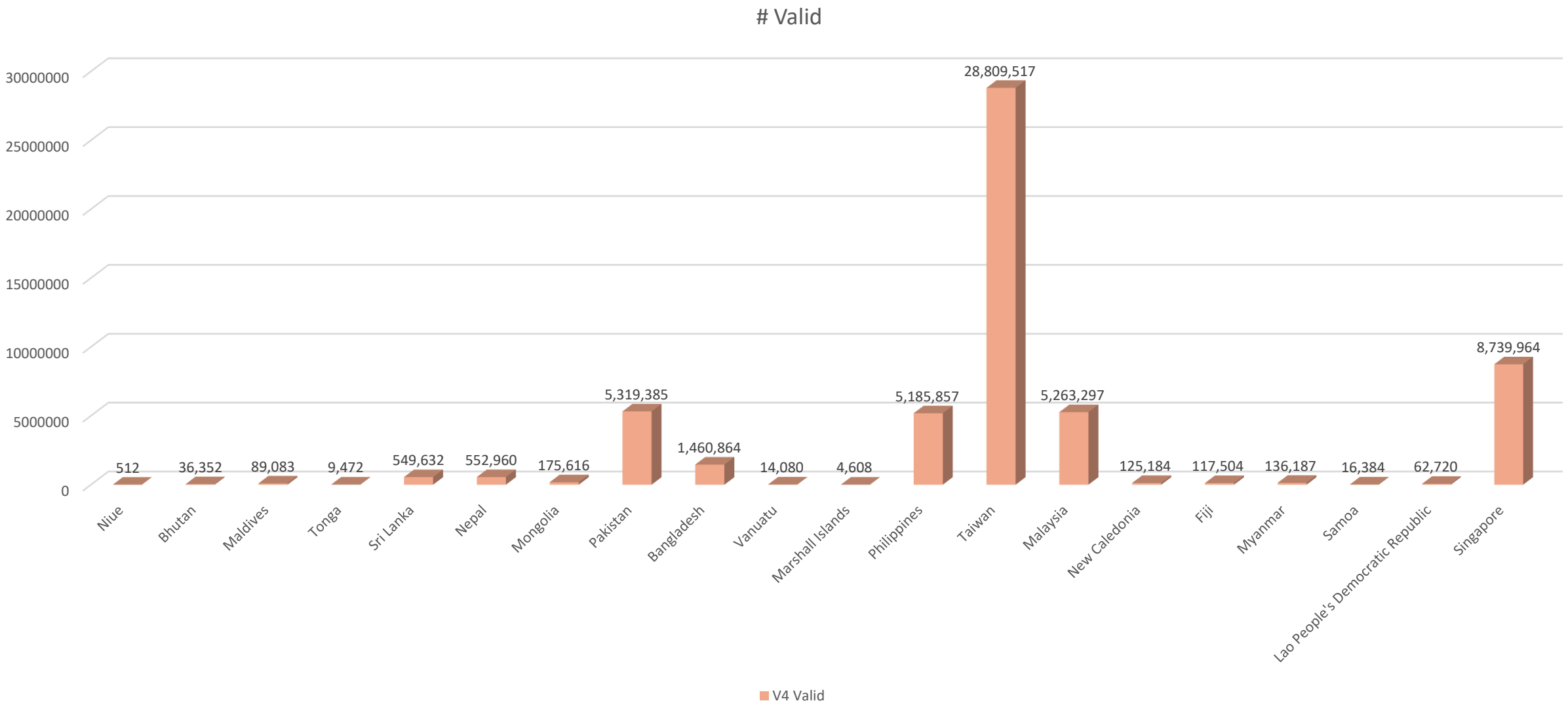
RPKI: The Numbers – Global Leaderboard



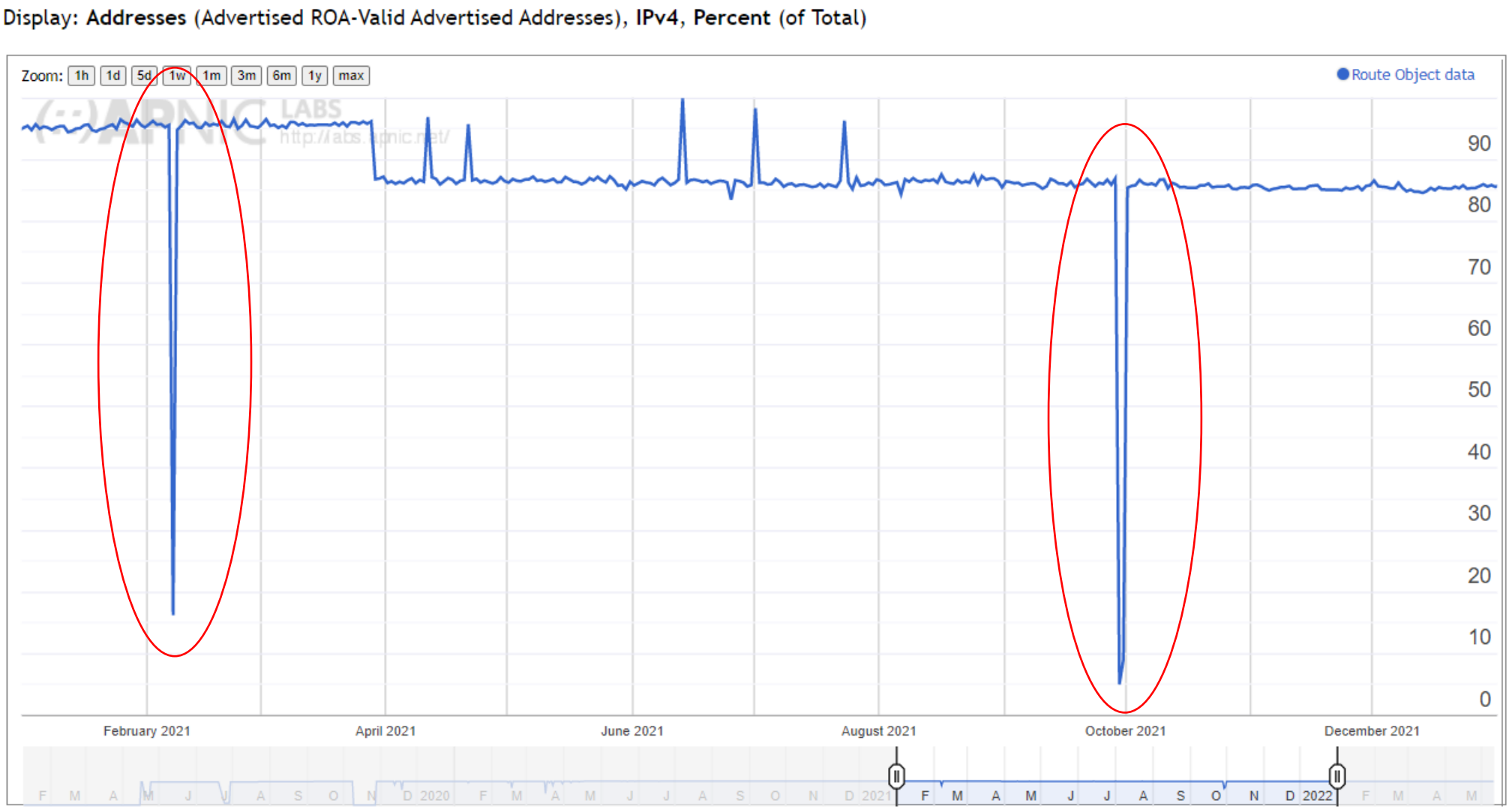
RPKI: The Numbers – APAC Top 20



RPKI: The Numbers – APAC Top 20



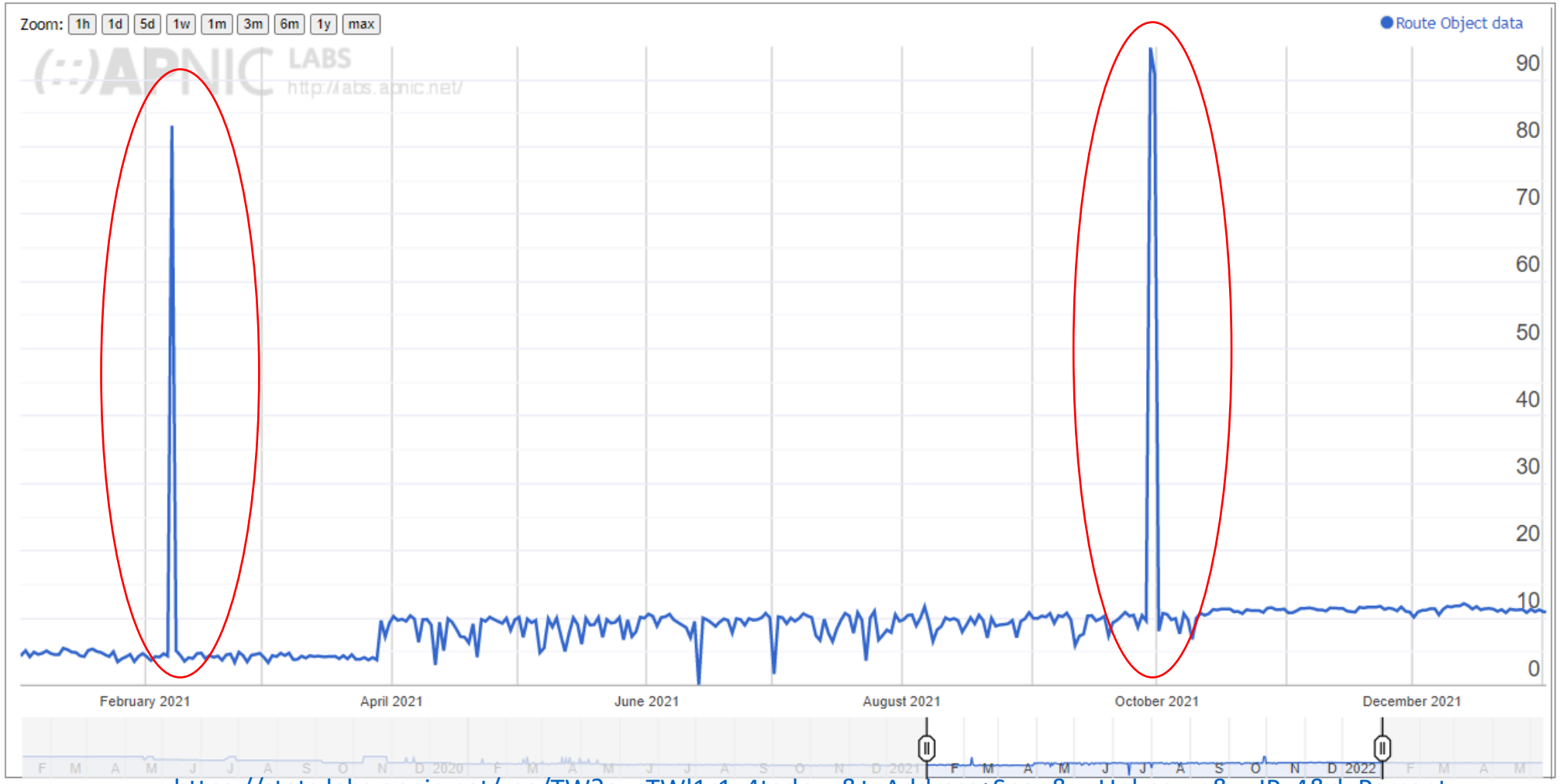
RPKI: The Numbers – TW - Valid



https://stats.labs.apnic.net/roa/TW?o=cTWI1r1v4tadpxu&t=Address+Span&x=Valid&v=IPv4&d=Percent

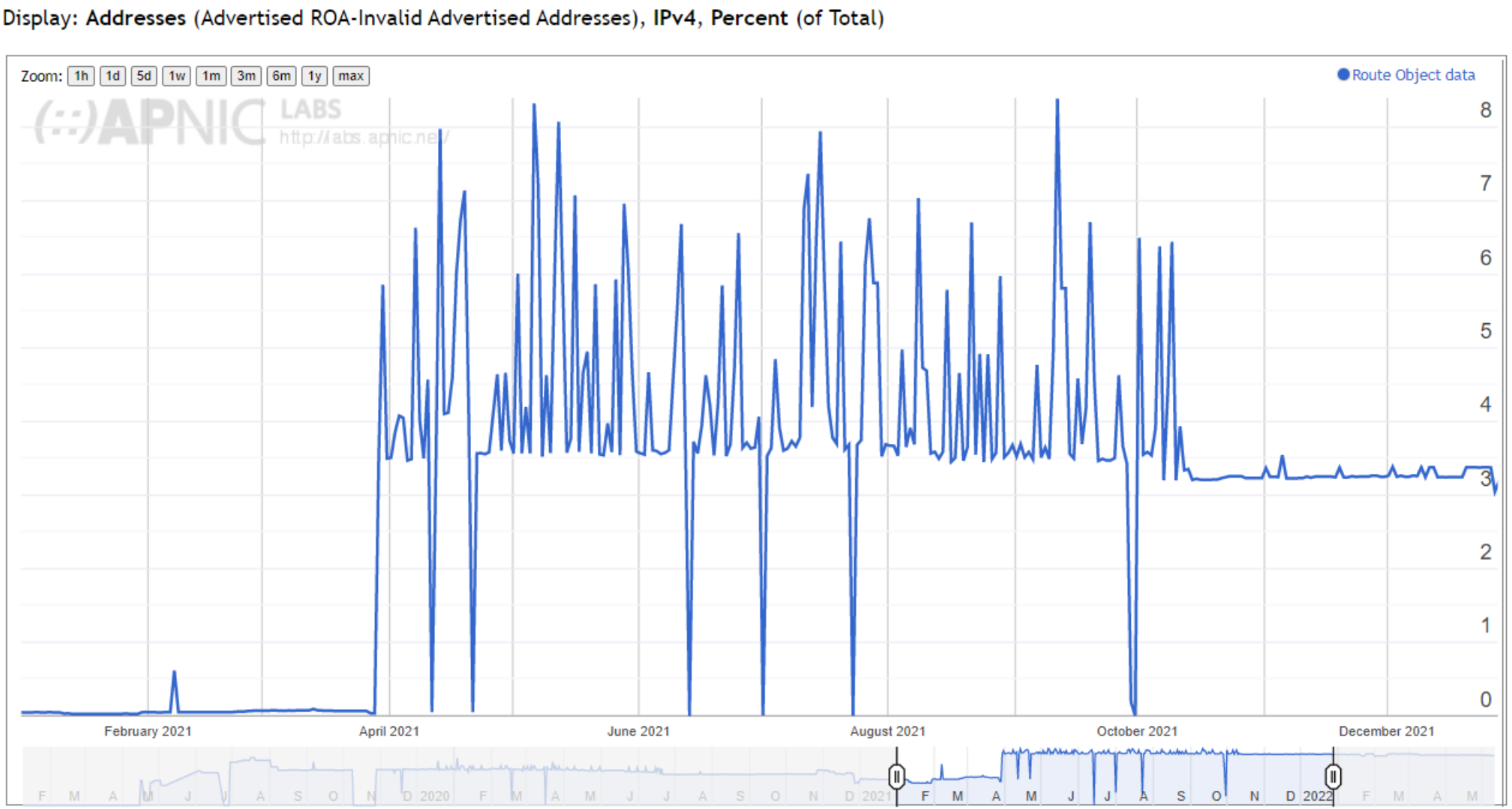
RPKI: The Numbers – TW - Unknown

Display: **Addresses** (Advertised ROA-Unknown Advertised Addresses), **IPv4**, **Percent** (of Total)



https://stats.labs.apnic.net/roa/TW?o=cTWl1r1v4tadpxu&t=Address+Span&x=Unknown&v=IPv4&d=Percent

RPKI: The Numbers – TW - Invalid



https://stats.labs.apnic.net/roa/TW?o=cTWl1r1v4tadpxu&t=Address+Span&x=Invalid&v=IPv4&d=Percent

RPKI: The Numbers – TW - Invalid

ASN	ASN Name	V4 Valid	Pc	V4 Invalid	Pc2	V4 Unknown	Pc3	V4 Total Addrs
AS17713	NSYSU-TW National Sun Yat-sen University	65,536	11.40%	295,680	51.40%	214,016	37.20%	575,232.00
AS1659	ERX-TANET-ASN1 Taiwan Academic Network TANet Information Center	2,669,055	74.80%	232,192	6.50%	664,832	18.60%	3,566,079.00
AS18177	NCKU-TW National Cheng Kung University	-	0.00%	117,760	26.00%	335,360	74.00%	453,120.00
AS17712	CCU-TW National Chung Cheng University	-	0.00%	74,752	21.10%	279,040	78.90%	353,792.00
AS9916	NCTU-TW National Chiao Tung University	94,208	21.90%	71,424	16.60%	264,448	61.50%	430,080.00
AS17716	NTU-TW National Taiwan University	76,800	25.20%	58,624	19.20%	169,728	55.60%	305,152.00
AS17711	NDHU-TW National Dong Hwa University	-	0.00%	28,416	97.40%	768	2.60%	29,184.00
AS38841	KBRO-AS-TW kbro CO. Ltd.	502,524	99.00%	1,920	0.40%	3,072	0.60%	507,516.00
AS24167	ASGCNET Academia Sinica Grid Computing Center	12,544	90.70%	1,280	9.30%	-	0.00%	13,824.00

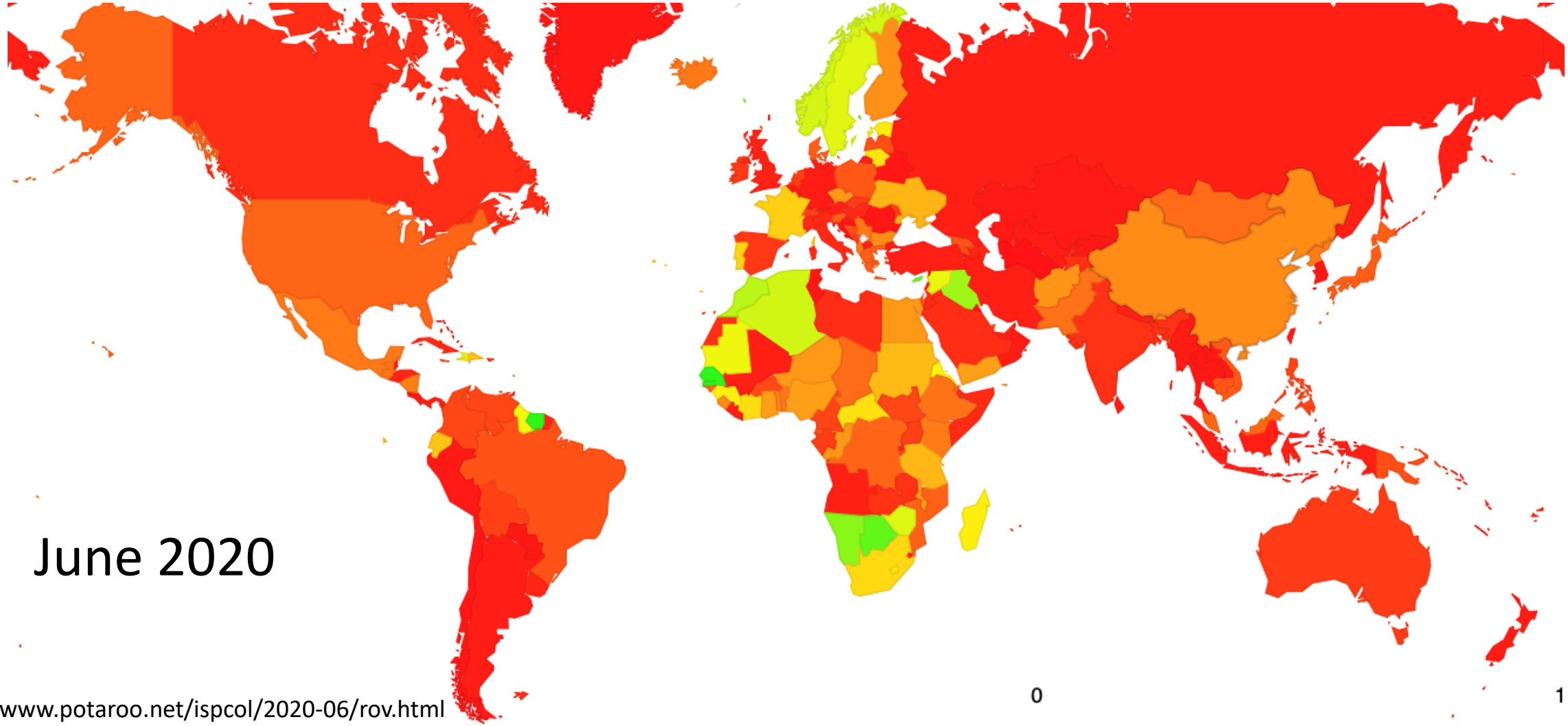
https://stats.labs.apnic.net/roa/TW?o=cTWl1r1v4tadpxv&t=Address+Span&x=Valid&v=IPv4&d=Percent&r=0

RPKI: The Numbers – TW- Invalid

AS	Prefix	Span	CC	Visibility	ROV State	ROAs
AS17713	163.15.0.0/16	65536	TW	1	INV	[Addr:163.14.0.0/15,Max:15,AS:1659]
AS17713	163.16.0.0/16	65536	TW	1	INV	[Addr:163.16.0.0/13,Max:19,AS:1659]
AS17713	163.18.0.0/16	65536	TW	1	INV	[Addr:163.16.0.0/13,Max:19,AS:1659]
AS17713	163.24.0.0/16	65536	TW	1	INV	[Addr:163.24.0.0/14,Max:14,AS:1659]
AS17713	163.28.128.0/20	4096	TW	1	INV	[Addr:163.28.0.0/16,Max:16,AS:1659]
AS17713	192.83.194.0/23	512	TW	1	INV	[Addr:192.83.192.0/22,Max:22,AS:1659]
AS17713	192.192.178.0/24	256	TW	1	INV	[Addr:192.192.0.0/16,Max:16,AS:1659]
AS17713	192.192.190.0/23	512	TW	1	INV	[Addr:192.192.0.0/16,Max:16,AS:1659]
AS17713	192.192.192.0/22	1024	TW	1	INV	[Addr:192.192.0.0/16,Max:16,AS:1659]
AS17713	192.192.200.0/22	1024	TW	1	INV	[Addr:192.192.0.0/16,Max:16,AS:1659]

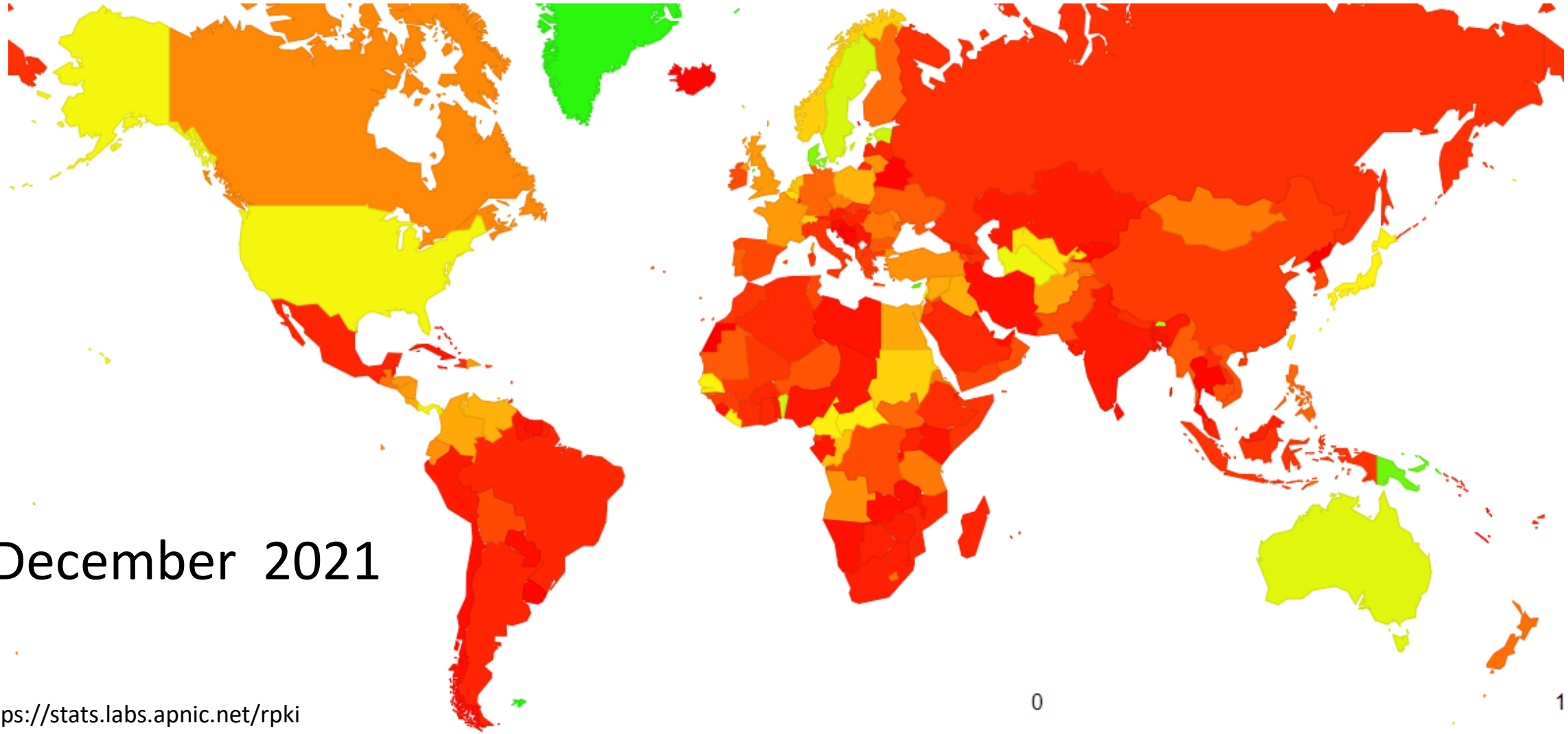
https://stats.labs.apnic.net/roa/AS17713?c=TW&l=1&v=4&t=thist&d=thisd

RPKI: The Numbers - ROV



https://www.potaroo.net/ispcol/2020-06/rov.html

RPKI: The Numbers - ROV

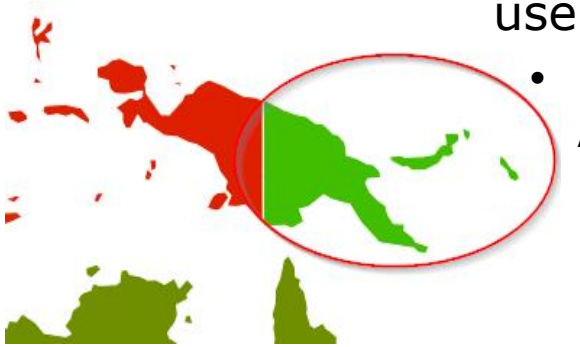


https://stats.labs.apnic.net/rpki

RPKI: The Numbers - ROV

- But what about Validation?
  - Harder to measure. Why?

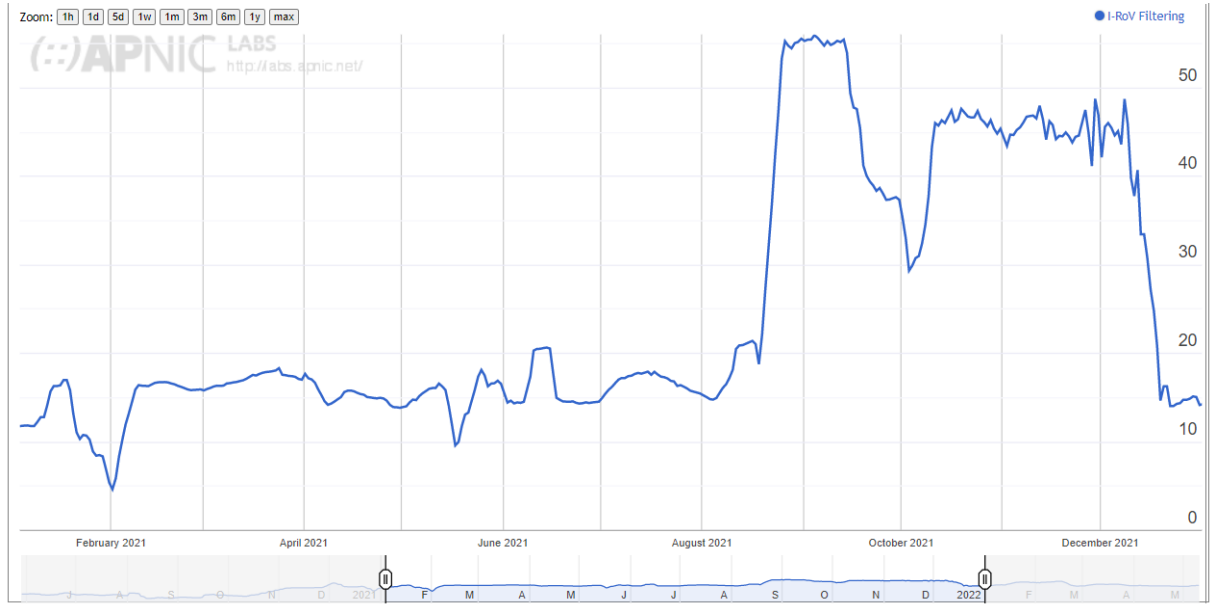
- What if my network is not doing Validation, but my upstream is?
  - My network is seen as filtering INVALIDS.
  - Eg:
    - PNG is seen as ~80% Filtering BUT
      - Those ~80% transit through Dataco(AS17828), who upstream to Vocus(AS4826)
        - AS4826 is filtering invalids.
      - The remaining may have links with AS17828 but they appear to prepend and use others for their upstreams
        - EG: DATEC(AS55792) heavy prepends towards AS17828 and appear to use ABS-Global(AS45572) for their transit.



https://blog.apnic.net/2021/05/13/vocus-rpki-implementation/

RPKI: The Numbers – ROV - TW

- Currently showing ~13%
  - Has been as High as 55%!
- Is it the same reasons as PNG?
  - It depends on the measurement points
  - Do they have to traverse the DFZ?



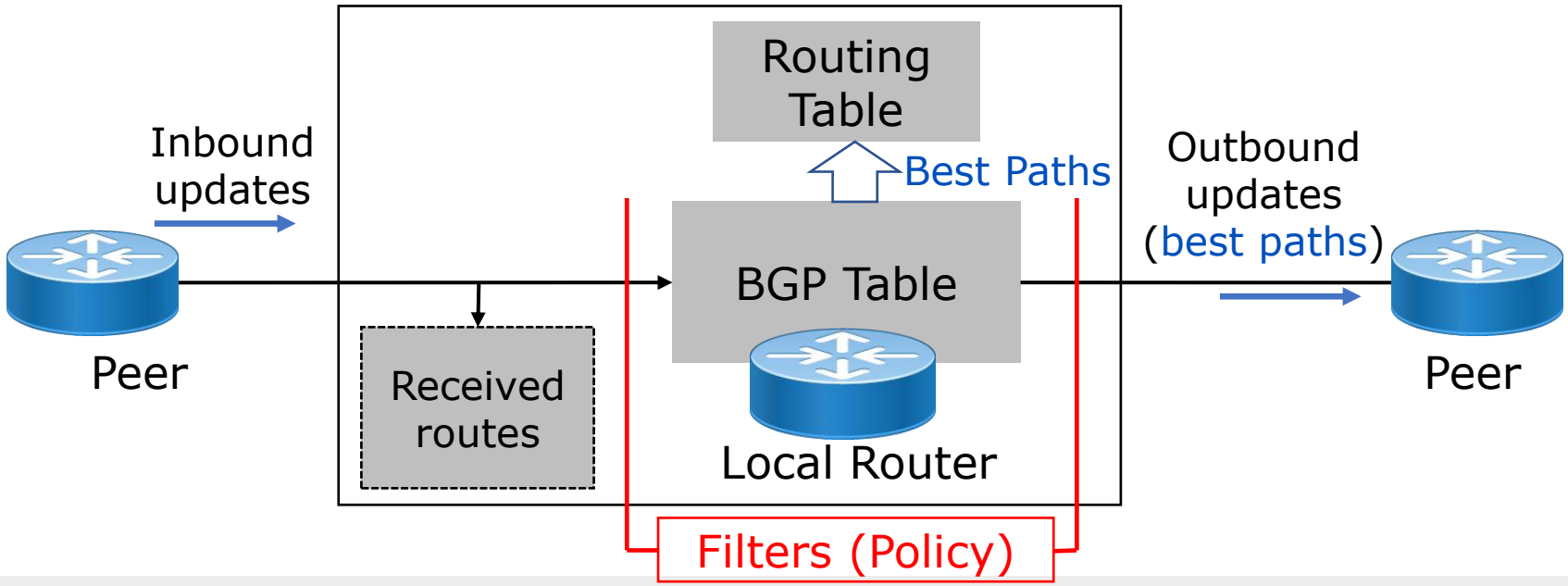
RPKI
Lessons Learned

RPKI: Lessons Learned

- Adjacency RIBs are important
- NCSC CVE Disclosures
- APNIC Portal Issues
- RPKI Chain of trust

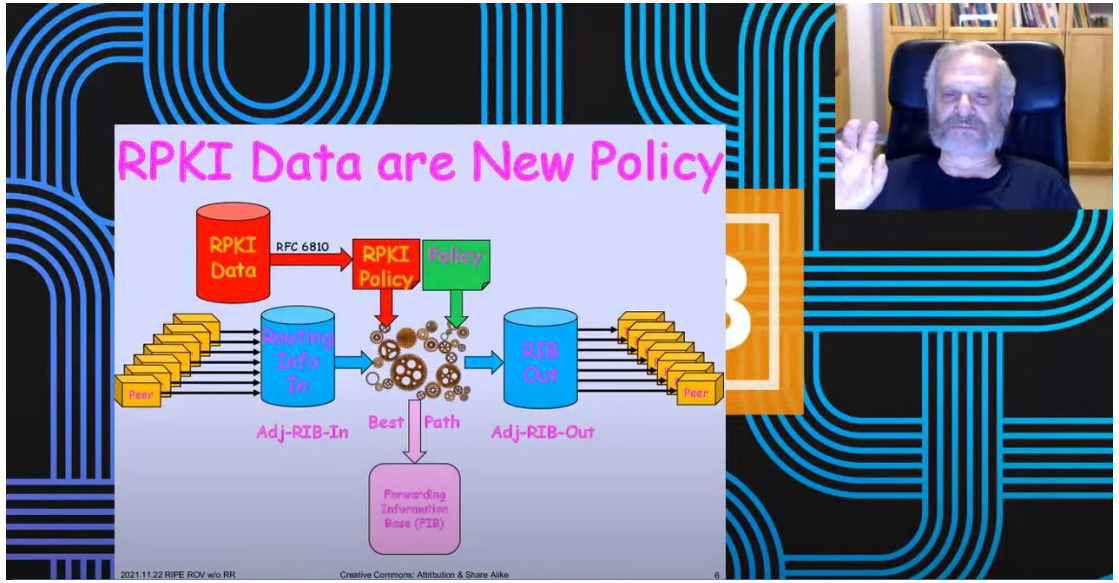
RPKI: Lessons Learned – Adj RIB

- First brought to our attention in August
- RPKI RTR causing Route Refresh with eBGP Peers
- Only Observed on IOS-XE/XR
  - Cisco TAC advised turning on Soft Reconfig, but WHY did this fix it?
    - We need to go back to how BGP on routers work!



RPKI: Lessons Learned – Adj RIB

- Fast Forward to RIPE-83 (23 November 2021)
  - draft-ymbk-sidrops-rov-no-rr (https://datatracker.ietf.org/doc/draft-ymbk-sidrops-rov-no-rr/)
  - Randy Bush, Mark Tinka, Philip Smith, and Kayur Patel co-author a draft RFC
  - "A BGP Speaker performing RPKI-based policy should not issue Route Refresh to its neighbors when receiving new RPKI data"



https://youtu.be/g722hpSxmOE?t=22467

RPKI: Lessons Learned – Adj RIB

- Proposed Fixes
  - Keep A Full ADJ-RIB-IN

    OR
  - If no Adj-RIB-In, then when BGP drops an Invalid, keep the path, but mark it as dead, a minimal Adj-RIB-Dropped

    OR
  - Do not run RPKI policy on any router which can not do either of the above

RPKI: NCSC Disclosures

- NCSC-NL Released a number of vulnerabilities relating to RPKI and the Validators on 9th of November 2021
  - This was not received well initially due to the lack of consultation with the various devs involved (in some part) and was delayed by 10 days to allow to patches and advice to be done
  - Full List of CVE covered available at https://www.ncsc.nl/actueel/advisory?id=NCSC%2D2021%2D0987

- Validators that have been patched/fixed
  - OcktoRPKI (https://github.com/cloudflare/cfrpki/releases/tag/v1.4.0)
  - FORT (https://github.com/NICMx/FORT-validator/releases/tag/1.5.3)
  - rpki-client (https://marc.info/?l=openbsd-tech&m=163646702631430)
  - Rpki-prover (https://github.com/lolepezy/rpki-prover/releases/tag/v0.2.0-6201cf49)

CHECK WHICH VERSION YOU ARE RUNNING!!

RPKI: NCSC Disclosures

- What did they find?
  - Some Validators ran as root
  - Some crashed when presented with invalid ROA Data
  - Some crashed when the repository contained to many bits for the IP address
  - Some had no bounds when processing infinite lengths of certificate chains
  - Some had strange processing of time-out values
  - Some were vulnerable to gzip-white-space attacks (causing out of memory)

BUT

- To make use of these attacks, you have to be SOMEWHERE in the trust chain to begin with.
  - So, who are you open to attack from?

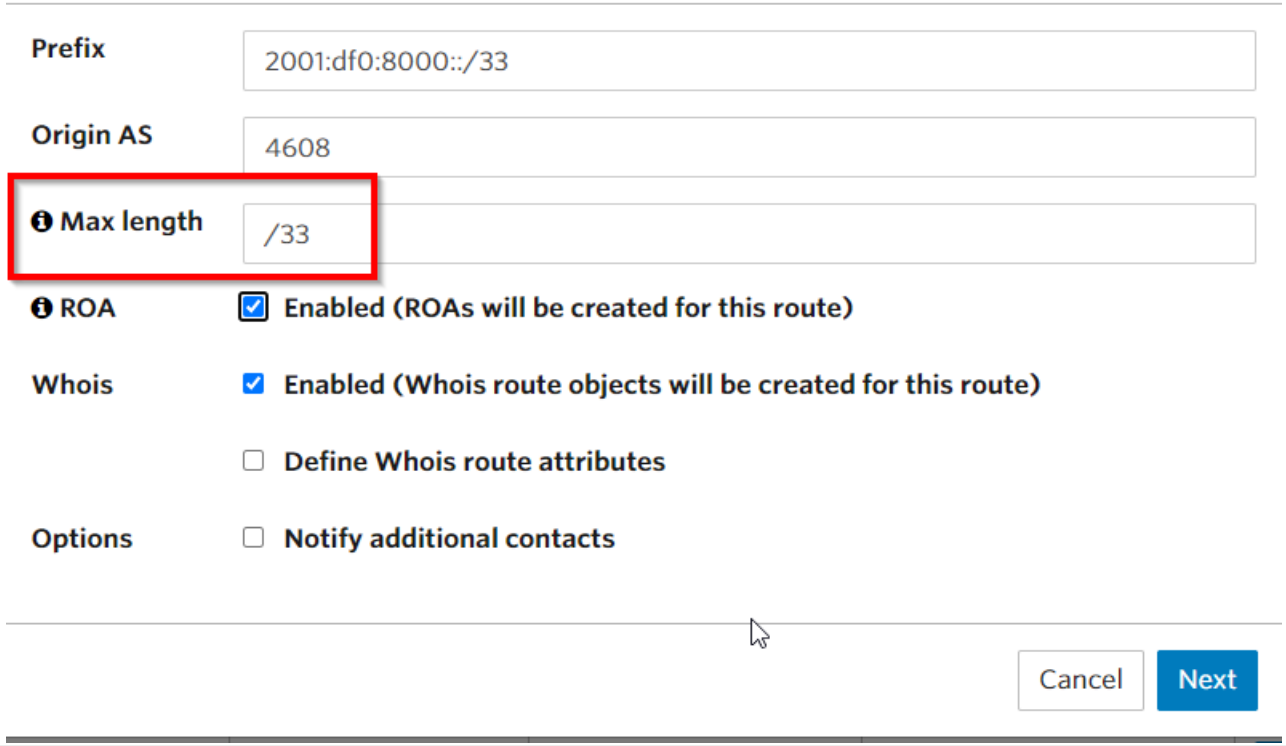
RPKI: NCSC Disclosures

- Why is the RIPE validator not mentioned
  - RIPE had already announced that they would not be supporting their validator POST July 1st 2021
  - https://github.com/RIPE-NCC/rpki-validator-3
- Good write up from NCSC on RIPE Blog
  - https://labs.ripe.net/author/koen-van-hove/improving-the-resiliency-of-rpki-relying-party-software/
  - Not all issues can be fixed by the RP software
    - Some are router side
    - Some are on the protocol
    - New draft rfc https://datatracker.ietf.org/doc/draft-kwvanhove-sidrops-rpki-tree-hints/

RPKI: APNIC Portal

- Rise of the invalids (https://blog.apnic.net/2020/04/10/rise-of-the-invalids/)

- PROBLEM:
  - Max Length issues could be caused by applying an assumed default ML at ROA creation
- Solution:
  - Remove the default in MYAPNIC UI



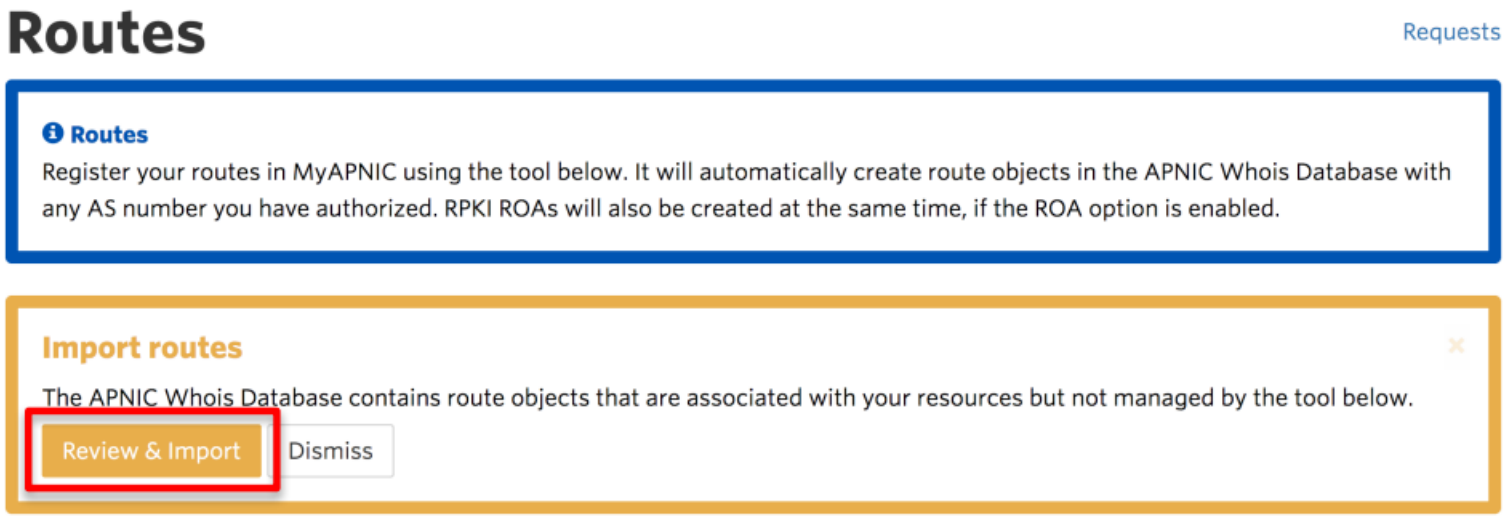
RPKI: APNIC Portal

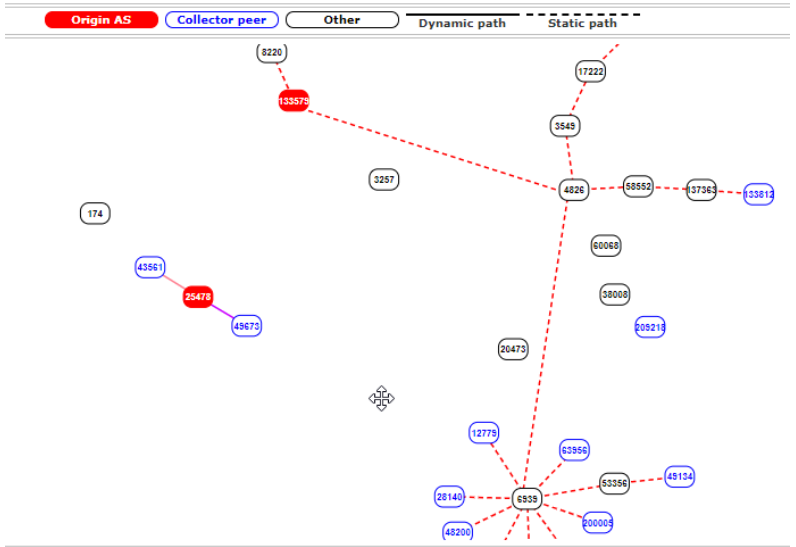
- What can I do to fix this?
  - Clean up your BGP Before you create ROAs
    - Make sure YOU understand what you are announcing to your peers
  - Only create ROA for what you advertise in BGP
    - Follow the “Minimal ROA” concept
  - If you are running a multi ASN Network(eg Different transit and access ASN)
    - Check and double check where your routes are originating from
      - This will solve the “Invalid ASN” Problems

- REMEMBER you can have multiple ROAs for the same address space
  - Valid will win over Invalid
  - Not Found is better than Invalid

RPKI: APNIC Portal

- Problem:
  - Observed during our Perth RPKI Workshop in November
  - Active Hijack occurring during the session (AS25478 iHOME-AS, RU)
  - MYAPNIC portal route import feature recommended importing hijacked routes

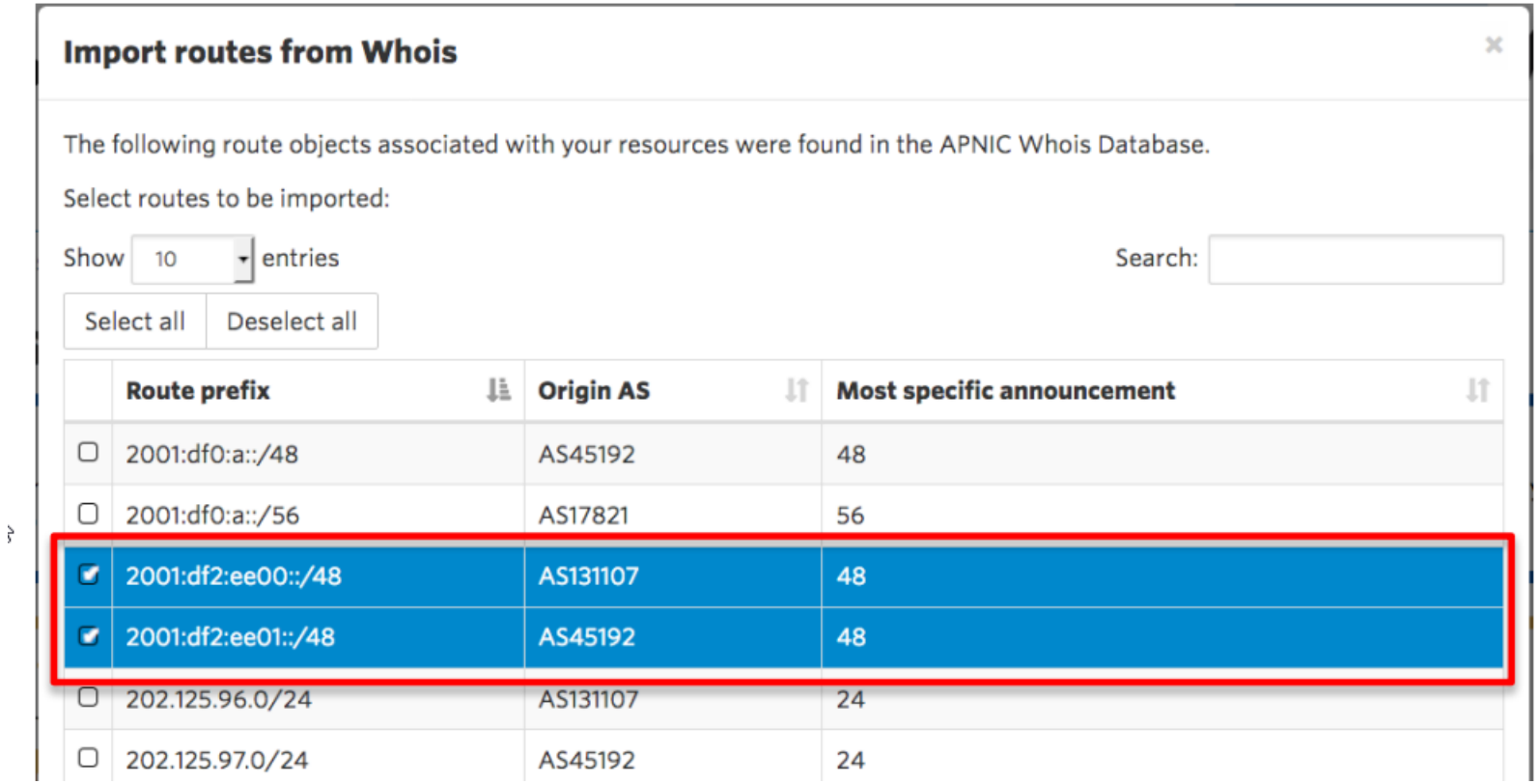




https://bgpstream.com/event/283485

RPKI: APNIC Portal

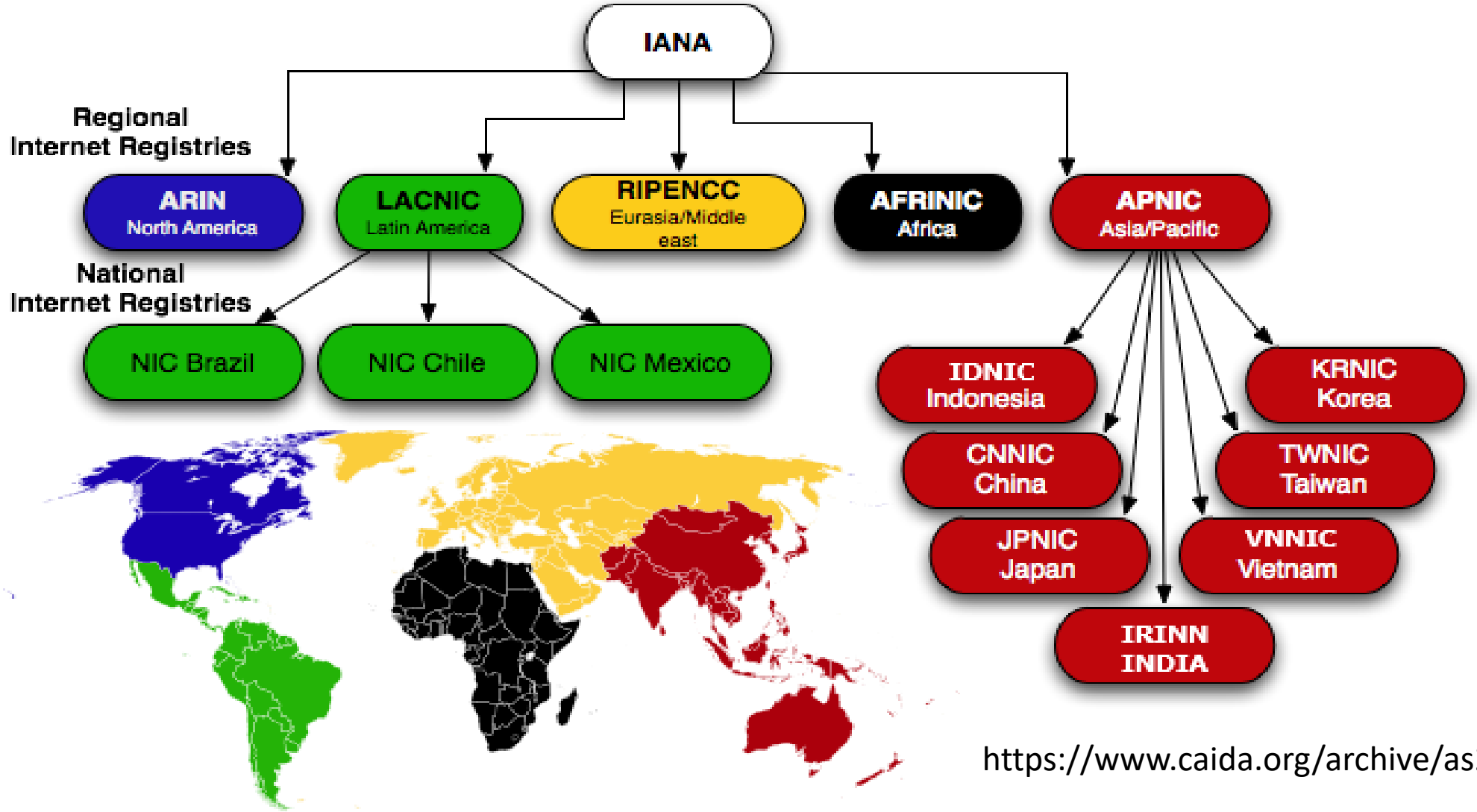
- Problem:



RPKI: APNIC Portal

- Solution:
  - Short Term:
    - Check the recommended routes before importing.
    - Validate the import data against what you KNOW you are originating
  - Longer Term:
    - Some back-end validation will be put in place to match resources against the visible routes and Warn or Filter these from view.

RPKI: Chain of Trust



https://www.caida.org/archive/as2org/

RPKI: Chain Of Trust

- NIR status for RPKI
  - JPNIC – Full Self hosted with delegation
  - TWNIC – Full Self hosted with delegation
  - CNNIC – Full Self hosted with delegation
  - IDNIC – Self Hosted with Delegation
  - KRNIC – Still Implementing

- What about the others?
  - IRRIN
    - Contact IRRIN for ROA creation
      - No Delegated option for LIR
  - VNNIC
    - Contact VNNIC for ROA creation
      - No Delegated Option for LIR

https://www.apnic.net/community/security/resource-certification/#routing

Any questions?