RPKI in South Asia

Resource Public Key Infrastructure

SANOG 40

16 October 2023

Colombo, Sri Lanka

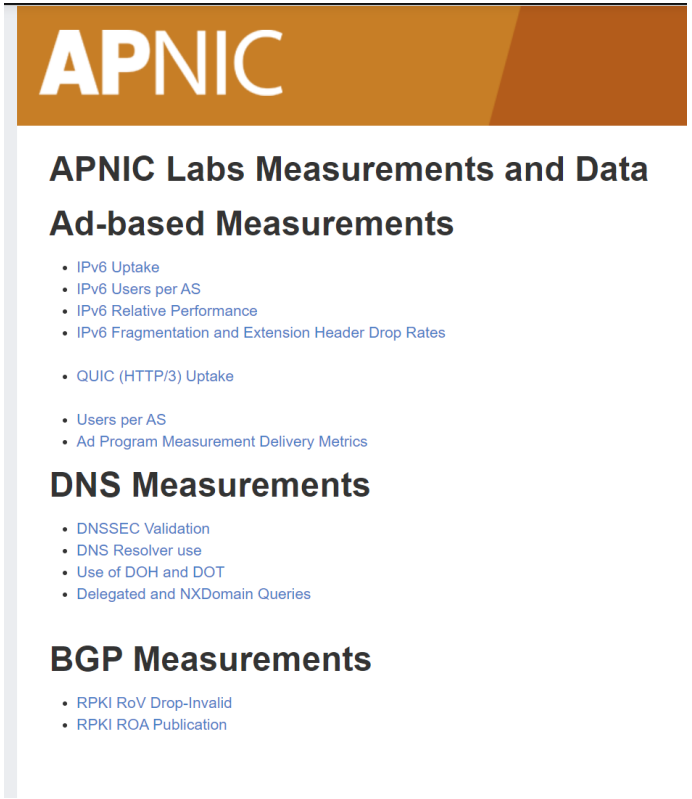
HOW ARE WE DOING?

RPKI Uptake?

Stats.Labs.APNIC.Net

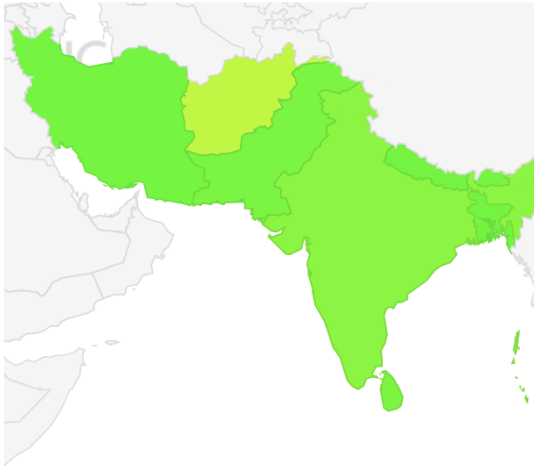
- RPKI RoV Drop-Invalid
- RPKI ROA Publication

Are ***your*** routes signed and have you started to ***drop*** invalid routes?



ROAs Signed

Southern Asia (034)

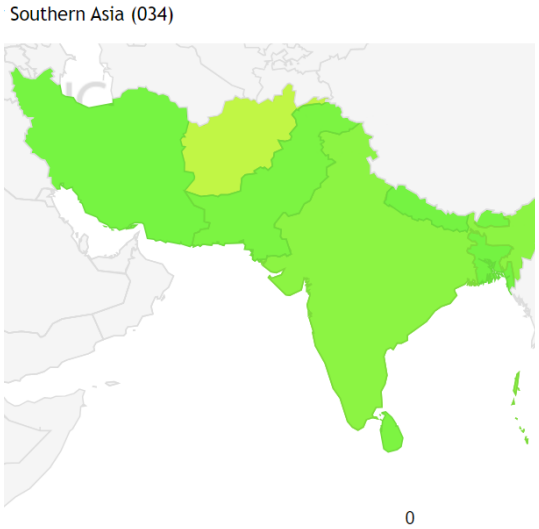


0

Use of Route Object Validation for Southern Asia (XT)

Display: **Addresses** (Advertised ROA-Valid Advertised Addresses), **Total** (IPv4 + IPv6), **Percent** (of Total)

Some Issues …



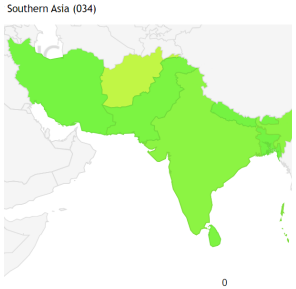
TOTAL ROA Prefixes	ROA Not Routed	Routed
184392	158391	26001

Highly Susceptible to
Route Origin Spoofing
(ASPATH + PREFIX) Hijacks

https://datatracker.ietf.org/doc/rfc9319/

Sample data from: Routes Views (SG) and RPKI data on 26th September.
IPv4 only.

ROA, Lots Of “Catch Alls”



Economy	Unique Prefixes	Single Subnet	Many Subnets Per ROA
INDIA	19817	17269	3499
BANGLADESH	3905	3463	630
PAKISTAN	3455	3525	529
NEPAL	1158	1077	112
AFGHANISTAN	241	239	21
MALDIVES	129	25	105
BHUTAN	44	33	14
BRITISH INDIAN OCEAN TERRITORY	9	9	0

https://datatracker.ietf.org/doc/rfc9319/

Sample data from: Routes Views (SG) and RPKI data on 26th September.
IPv4 only.

British Who?

Ref: https://en.wikipedia.org/wiki/Diego_Garcia

```
rpki=# select * from south_asia_roas where country = 'BRITISH INDIAN OCEAN TERRITORY';
   asn    |     prefix      | msa |  tal   |            country
----------+-----------------+-----+--------+--------------------------------
 AS17458 | 203.83.48.0/24 |  24 | apnic | BRITISH INDIAN OCEAN TERRITORY
 AS17458 | 203.83.48.0/21 |  21 | apnic | BRITISH INDIAN OCEAN TERRITORY
 AS17458 | 203.83.49.0/24 |  24 | apnic | BRITISH INDIAN OCEAN TERRITORY
 AS17458 | 203.83.50.0/24 |  24 | apnic | BRITISH INDIAN OCEAN TERRITORY
 AS17458 | 203.83.51.0/24 |  24 | apnic | BRITISH INDIAN OCEAN TERRITORY
 AS17458 | 203.83.52.0/24 |  24 | apnic | BRITISH INDIAN OCEAN TERRITORY
 AS17458 | 203.83.53.0/24 |  24 | apnic | BRITISH INDIAN OCEAN TERRITORY
 AS17458 | 203.83.54.0/24 |  24 | apnic | BRITISH INDIAN OCEAN TERRITORY
 AS17458 | 203.83.55.0/24 |  24 | apnic | BRITISH INDIAN OCEAN TERRITORY
(9 rows)
```

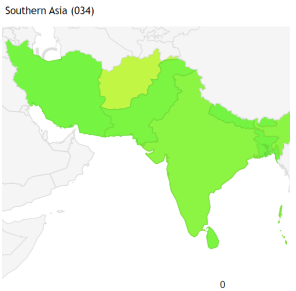
British Who?

Ref: https://en.wikipedia.org/wiki/Diego_Garcia

```
rpki=# select * from south_asia_routes where country = 'BRITISH INDIAN OCEAN TERRITORY';
     prefix     |            country
----------------+-------------------------------
 203.83.48.0/21 | BRITISH INDIAN OCEAN TERRITORY
 203.83.48.0/24 | BRITISH INDIAN OCEAN TERRITORY
 203.83.49.0/24 | BRITISH INDIAN OCEAN TERRITORY
 203.83.50.0/24 | BRITISH INDIAN OCEAN TERRITORY
 203.83.51.0/24 | BRITISH INDIAN OCEAN TERRITORY
 203.83.52.0/24 | BRITISH INDIAN OCEAN TERRITORY
 203.83.53.0/24 | BRITISH INDIAN OCEAN TERRITORY
 203.83.54.0/24 | BRITISH INDIAN OCEAN TERRITORY
 203.83.55.0/24 | BRITISH INDIAN OCEAN TERRITORY
(9 rows)
```

“forged-origin” “attack surface”

Economy	ROAs	Expanded ROAs	Unique Routes
INDIA	3332	91524	15990
BANGLADESH	588	6438	3396
PAKISTAN	404	34932	2992
MALDIVES	105	442	230
NEPAL	98	1850	702
AFGHANISTAN	21	186	72
BHUTAN	13	112	30



https://datatracker.ietf.org/doc/rfc9319/

Sample data from: Routes Views (SG) and RPKI data on 26th September.
IPv4 only.

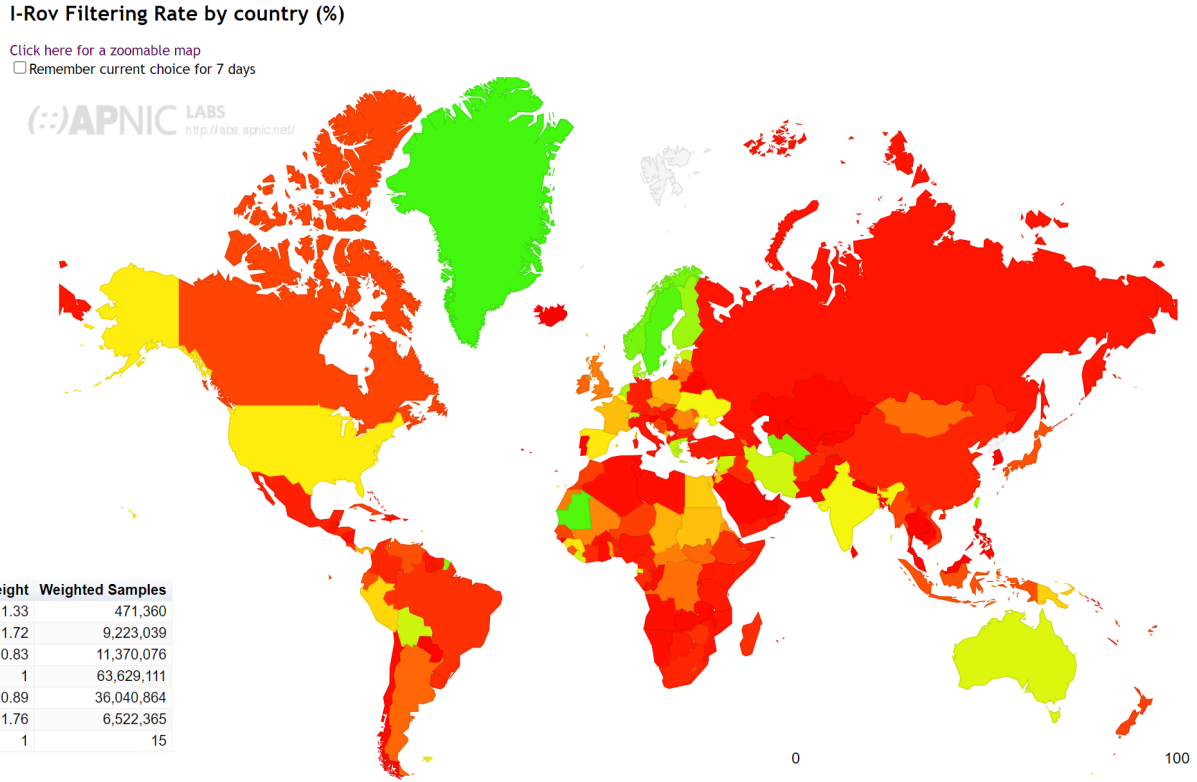
```
rpki=# select * from south_asia_expanded_roas a left join south_asia_routes b on a.prefix=b.prefix or
a.split_cidr=b.prefix where a.msa = 14;
   asn    |    prefix     | msa |  tal   | country |  split_cidr   |    prefix     | country
----------+---------------+-----+--------+---------+---------------+---------------+---------
 AS55836 | 49.32.0.0/12 |  14 | apnic | INDIA   | 49.32.0.0/13 | 49.32.0.0/13 | INDIA
 AS55836 | 49.32.0.0/12 |  14 | apnic | INDIA   | 49.40.0.0/14 | 49.40.0.0/14 | INDIA
 AS55836 | 49.32.0.0/12 |  14 | apnic | INDIA   | 49.44.0.0/14 |               |
 AS55836 | 49.32.0.0/12 |  14 | apnic | INDIA   | 49.32.0.0/14 |               |
 AS55836 | 49.32.0.0/12 |  14 | apnic | INDIA   | 49.36.0.0/14 |               |
 AS55836 | 49.32.0.0/12 |  14 | apnic | INDIA   | 49.40.0.0/13 |               |
(6 rows)

rpki=# select * from south_asia_routes where prefix = '49.32.0.0/12'::cidr;
 prefix | country
--------+---------
(0 rows)

rpki=# select asn,count(*) from south_asia_roas where prefix << '49.32.0.0/12'::cidr group by asn;
   asn    | count
----------+-------
 AS55836 |   334
 AS64049 |     2
(2 rows)
```

```
rpki=# select count(*) from south_asia_routes where prefix << '49.32.0.0/12'::cidr;
 count
-------
   153
(1 row)
```

https://datatracker.ietf.org/doc/rfc9319/

Validation … Are we there yet?

NOT EVEN CLOSE

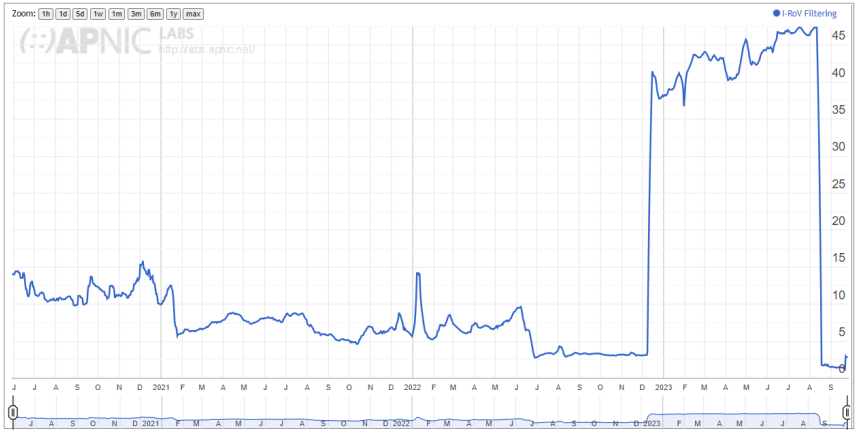


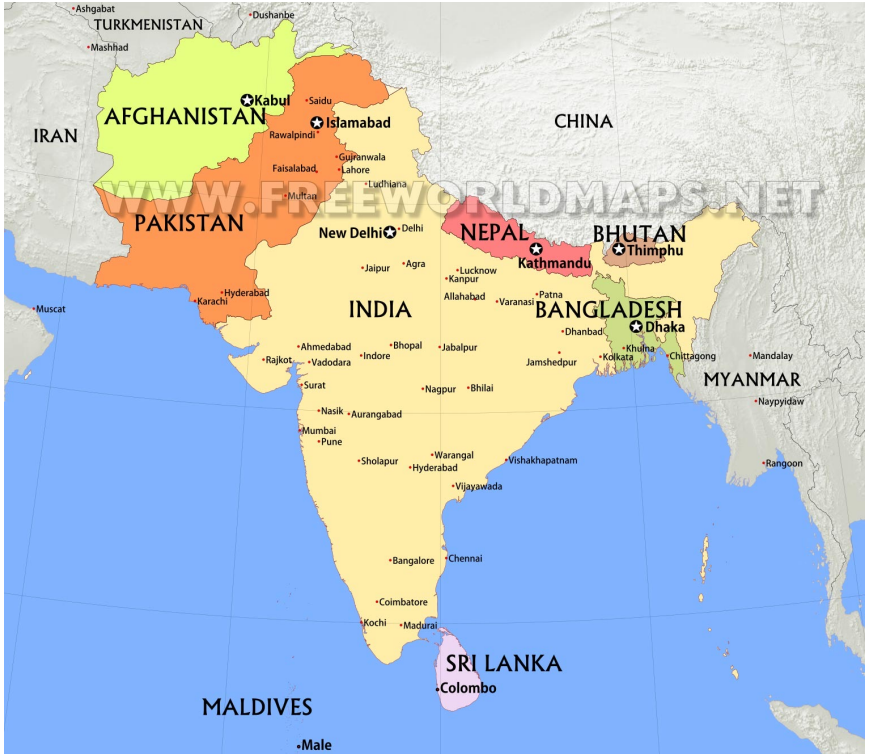
Code	Region	I-RoV Filtering	Samples	Weight	Weighted Samples
XF	Oceania	47.60%	354,451	1.33	471,360
XE	Europe	29.81%	5,375,471	1.72	9,223,039
XC	Americas	25.42%	13,692,309	0.83	11,370,076
XA	World	24.66%	63,629,111	1	63,629,111
XD	Asia	24.39%	40,507,732	0.89	36,040,864
XB	Africa	15.16%	3,699,133	1.76	6,522,365
XG	Unclassified	0	15	1	15

South Asia ROV

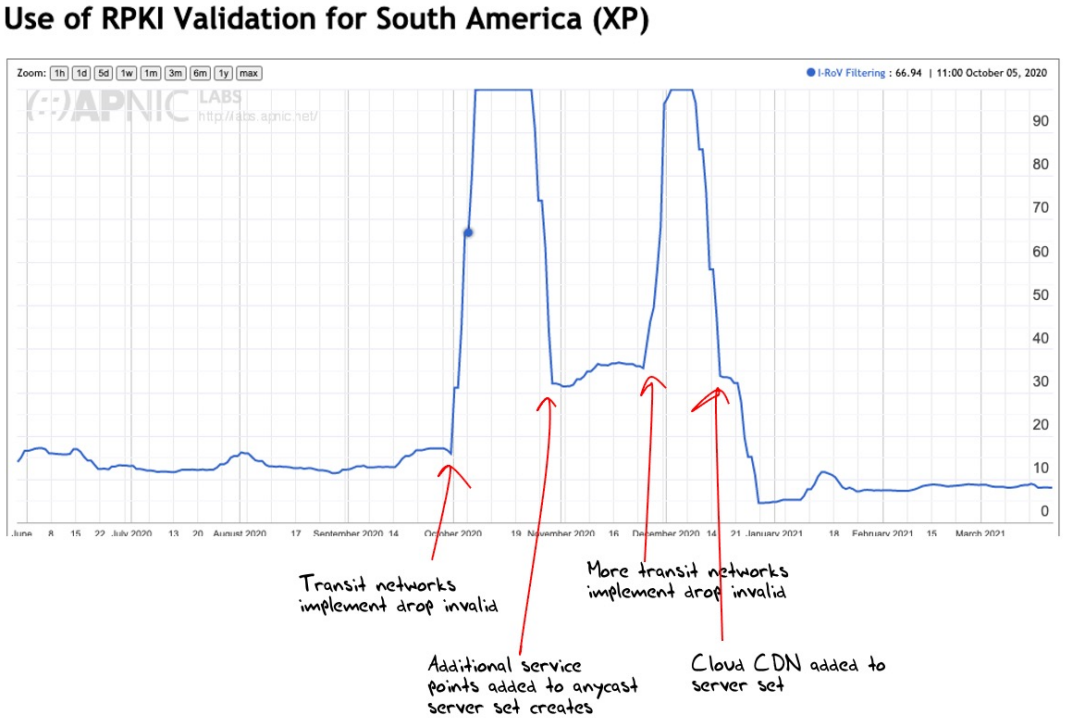
WHAT HAPPENED?

Use of RPKI Validation for Southern Asia (XT)





ROV Measurements Are Hard



https://labs.apnic.net/index.php/2021/03/23/measuring-roas-and-rov/

Call To Action

https://datatracker.ietf.org/doc/rfc9319/

> For this reason, this document recommends that, whenever possible, operators SHOULD use "minimal ROAs" that authorize only those IP prefixes that are actually originated in BGP, and no other prefixes. Further, it recommends ways to reduce the forged-origin attack surface by prudently limiting the address space that is included in ROAs. One recommendation is to avoid using the maxLength attribute in ROAs except in some specific cases. The recommendations complement and extend those in [RFC7115]. The document also

Hint: when an RFC says “should” in capitals … YOU DO IT!

So, where to from here?

Origins RPKI

https://www.rfc-editor.org/rfc/rfc8210

Pathways ASPA

https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-verification/

ASN to ASN BGPSEC

https://www.rfc-editor.org/rfc/rfc8205.html

Your TODO List is:

- Attend an APNIC workshop on RPKI.
- Decide on your ROA deployment: there's more than one way to sign routes.
- Plan for and set up VALIDATION on your network border routers.
- Implement MANRS and apply for the relevant program.
- Keep up to date on Best Current Operational Practices.
- Ask for Help ☺ techassist@apnic.net

Terry Sweetser

Been doing this “Internet thing” since 1989.

Former APNIC Community Trainer, CTO, Founder, Engineering Manager, etc

APNIC Training Delivery Manager for South Asia and Oceania

Nationality: Australian

Languages: English

about.me/terry.sweetser