The Internet – By the numbers

What are we doing?

Dave Phelan - APNIC

Who Am I?

- Dave Phelan
  - Network and Infrastructure engineer for a LONG time
  - Policy Manager Trainer at APNIC
  - Likes Cat memes



What are we going to talk about?

- Numbers Numbers Numbers!!!
- IPv6 Stats
  - What are we doing and why we need to do better
- RPKI Stats
  - What and why this important
- Security Stats
  - How many doors are open?
  - How does this affect me (and the rest of the internet)

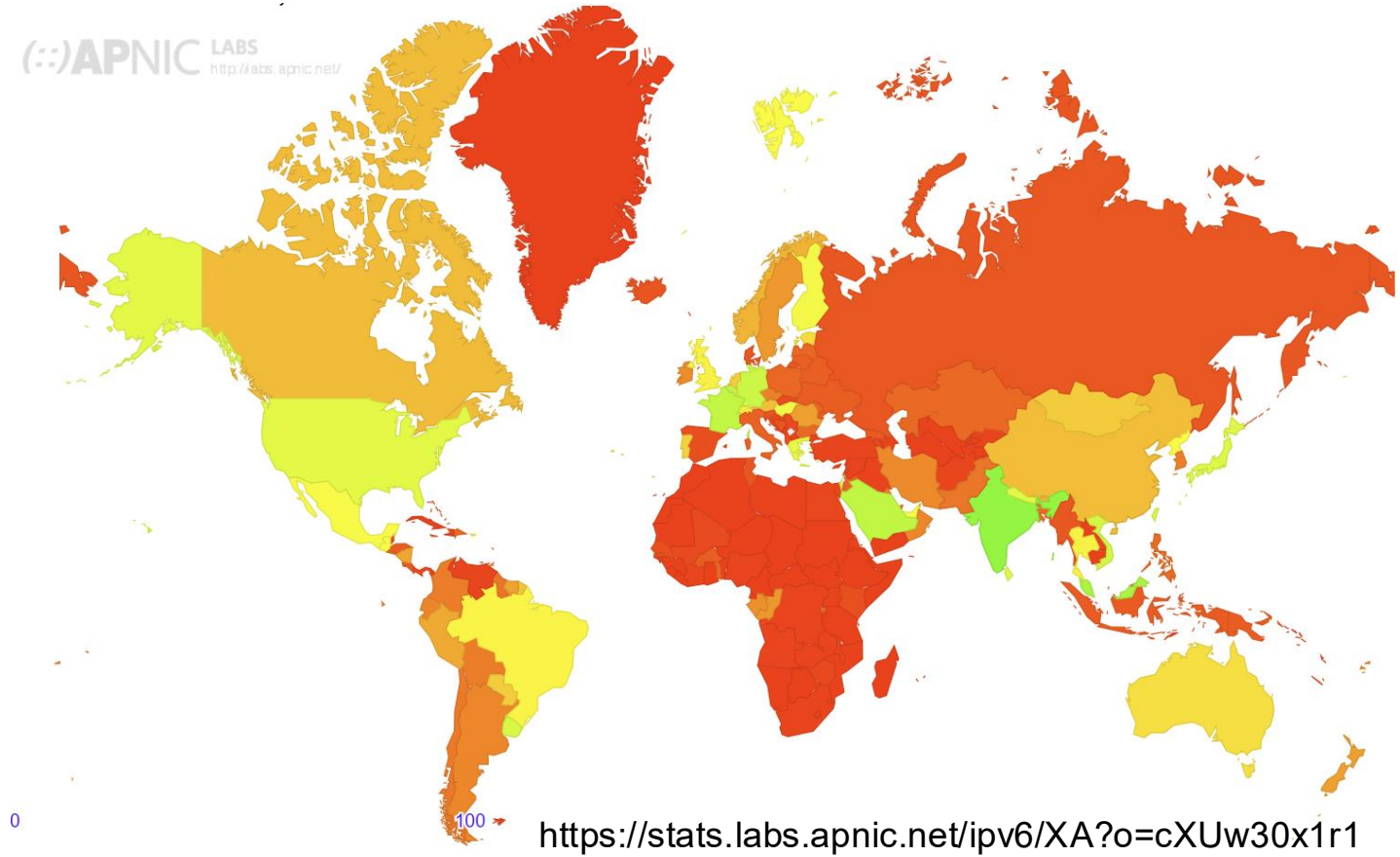
Why do we care about the numbers?

- We can use this as a benchmark
  - How are we performing
    - Network to Network
    - Economy to Economy
    - Region to Region
- What do we need to “fix”
  - Are we doing all we can within our region (see Benchmarks Above)
- Can we do better
  - For our Networks and our Users

Sources

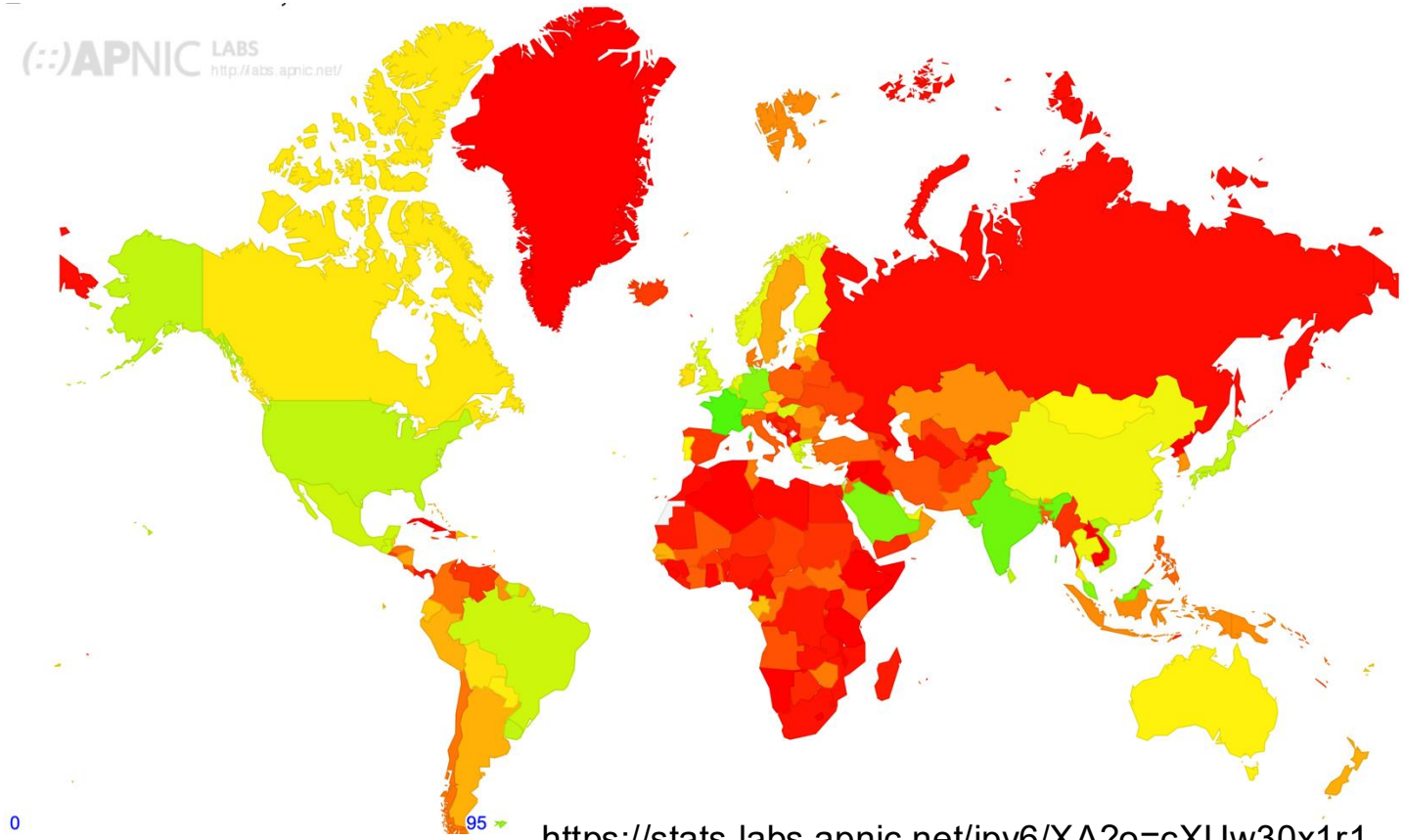
- Data for this presentation have come from numerous sources
  - https://stats.labs.apnic.net
  - https://radar.cloudflare.com
  - https://shodan.io
  - My own collection of stats

IPv6 – Global Snapshot - 2024



https://stats.labs.apnic.net/ipv6/XA?o=cXUw30x1r1

IPv6 – Global Snapshot - 2026



https://stats.labs.apnic.net/ipv6/XA?o=cXUw30x1r1

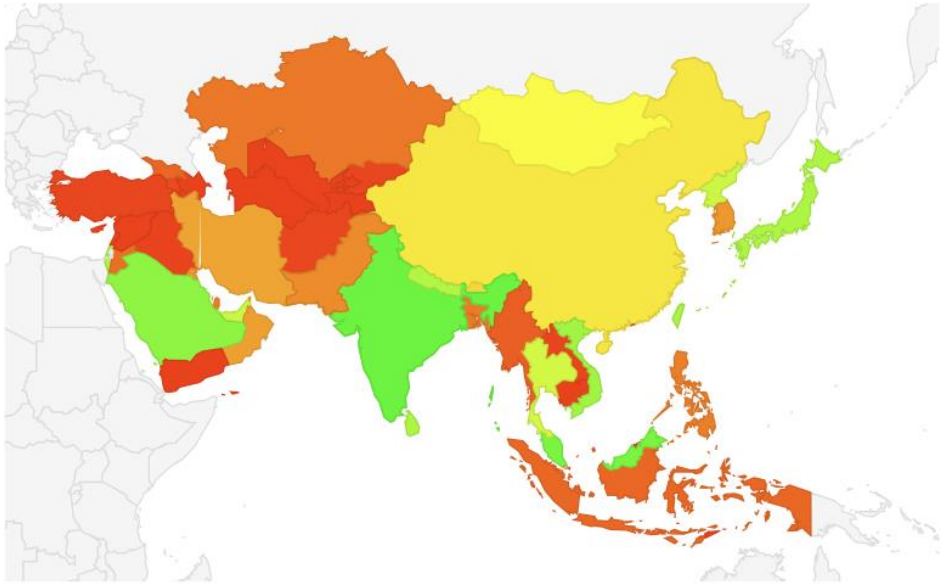
IPv6 – Global Snapshot 2026 vs. 2024

- 41.63% - 38% Global Preference
- 47.65% - 43.14% Asia
- 59.1% - 53% North America
- 44.1% - 36% South America
- 35.2% - 30% Europe
- 6.01% - 2.4% Africa
- 40.5% - 35.8% Oceania

https://stats.labs.apnic.net/ipv6/XA?o=cXUw30x1r1

IPv6 – Asia Sub-Region 2024

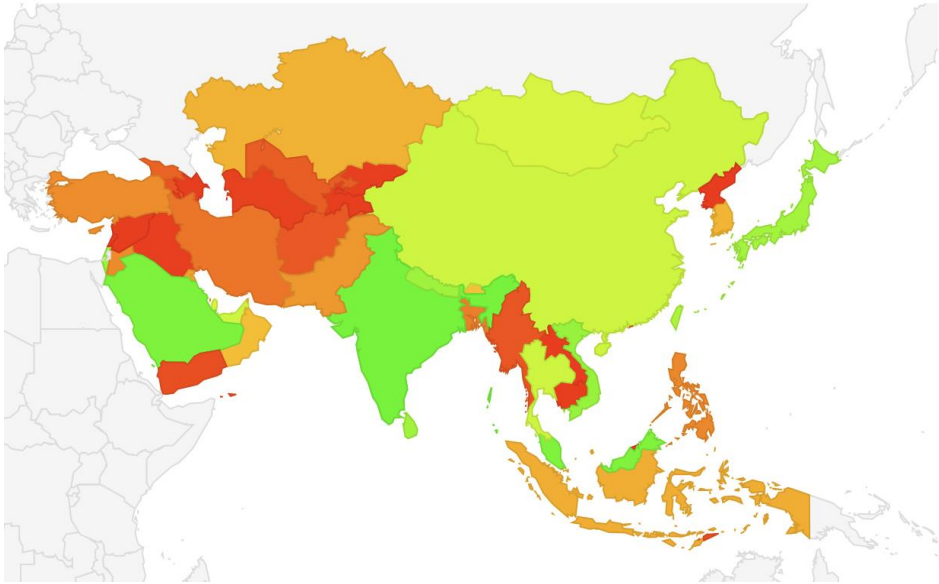
- 3 Sub-regions
  - 67.17% South Asia
    - IN,LK,NP,BT,PK,BD,AF,MV
  - 35.92% East Asia
    - TW,JP,MN,CN,MO,KR,HK,KP
  - 29.86% South-East Asia
    - MY,VN,TH,SG,PH,ID,MM,LA,BN,KH,TL



https://stats.labs.apnic.net/ipv6/XD?o=cXAw30x1r1

IPv6 – Asia Sub-Region 2026

- 3 Sub-regions
  - 65.71% South Asia
    - IN,LK,NP,BT,PK,BD,AF,MV
  - 44.63% East Asia
    - TW,JP,MN,CN,MO,KR,HK,KP
  - 35.84% South-East Asia
    - MY,VN,TH,SG,PH,ID,MM,LA,BN,KH,TL



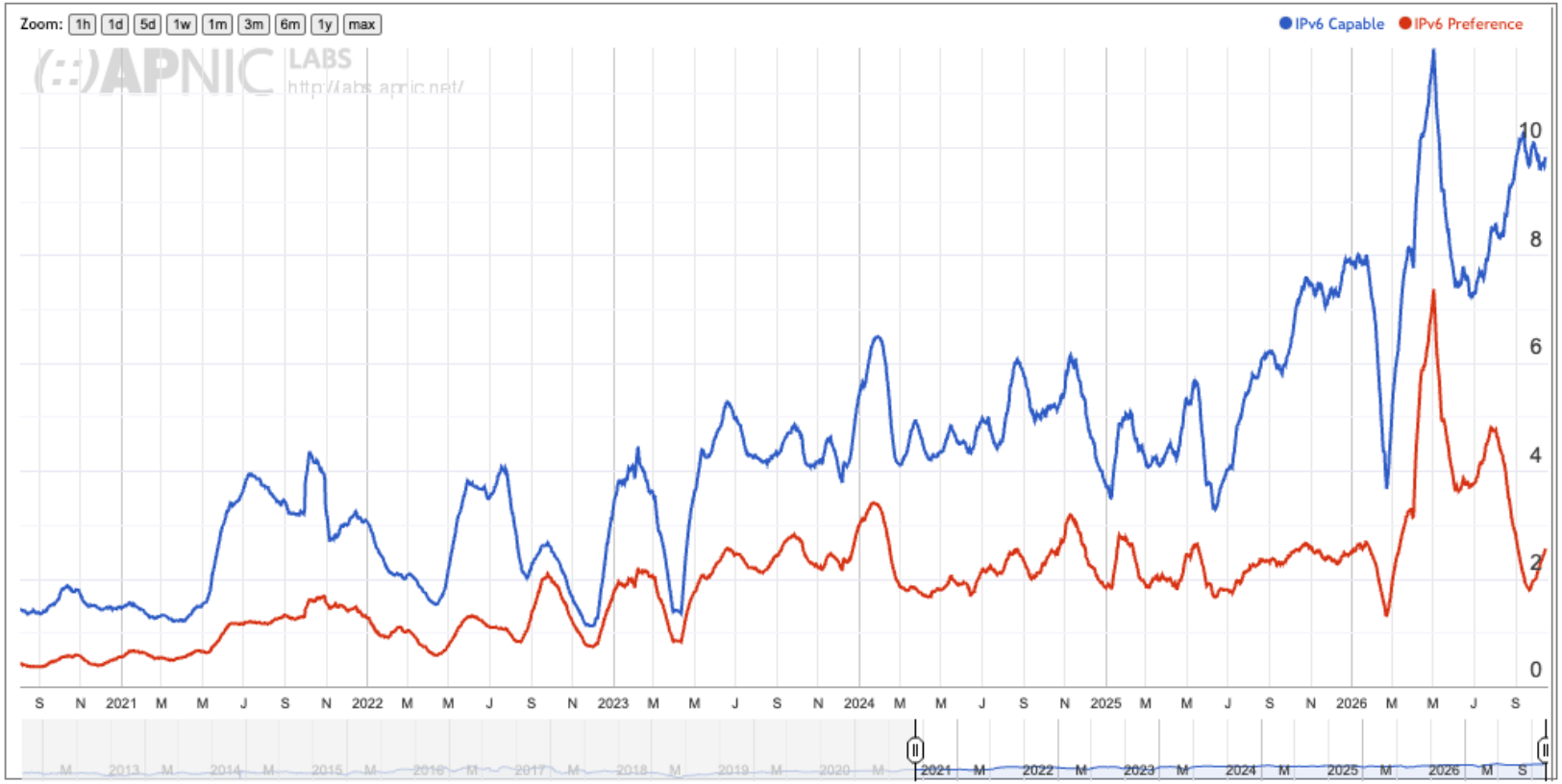
https://stats.labs.apnic.net/ipv6/XD?o=cXAw30x1r1

IPv6 – East Asia Sub-Region

CC	Country	IPv6 Preferred	IPv6 Pref 2020	IPv6 Pref 2023	IPv6 Pref 2026
TW	Taiwan, Eastern Asia, Asia	47.04%	41.82%	50.02%	56.26%
JP	Japan, Eastern Asia, Asia	47.22%	34.02%	47.13%	59.65%
CN	China, Eastern Asia, Asia	21.50%	15.11%	28.18%	40.81%
MO	Macao Special Administrative Region of China, Eastern Asia, Asia	23.55%	11.63%	27.24%	44.89%
KR	Republic of Korea, Eastern Asia, Asia	15.22%	13.87%	18.05%	28.39%
HK	**Hong Kong Special Administrative Region of China, Eastern Asia, Asia**	**0.98%**	**0.29%**	**4.82%**	**2.57%**
MN	Mongolia, Eastern Asia, Asia	0.08%	0.01%	1.37%	44.90%
KP	Democratic People's Republic of Korea, Eastern Asia, Asia	0	0	0	0

https://stats.labs.apnic.net/ipv6/XS

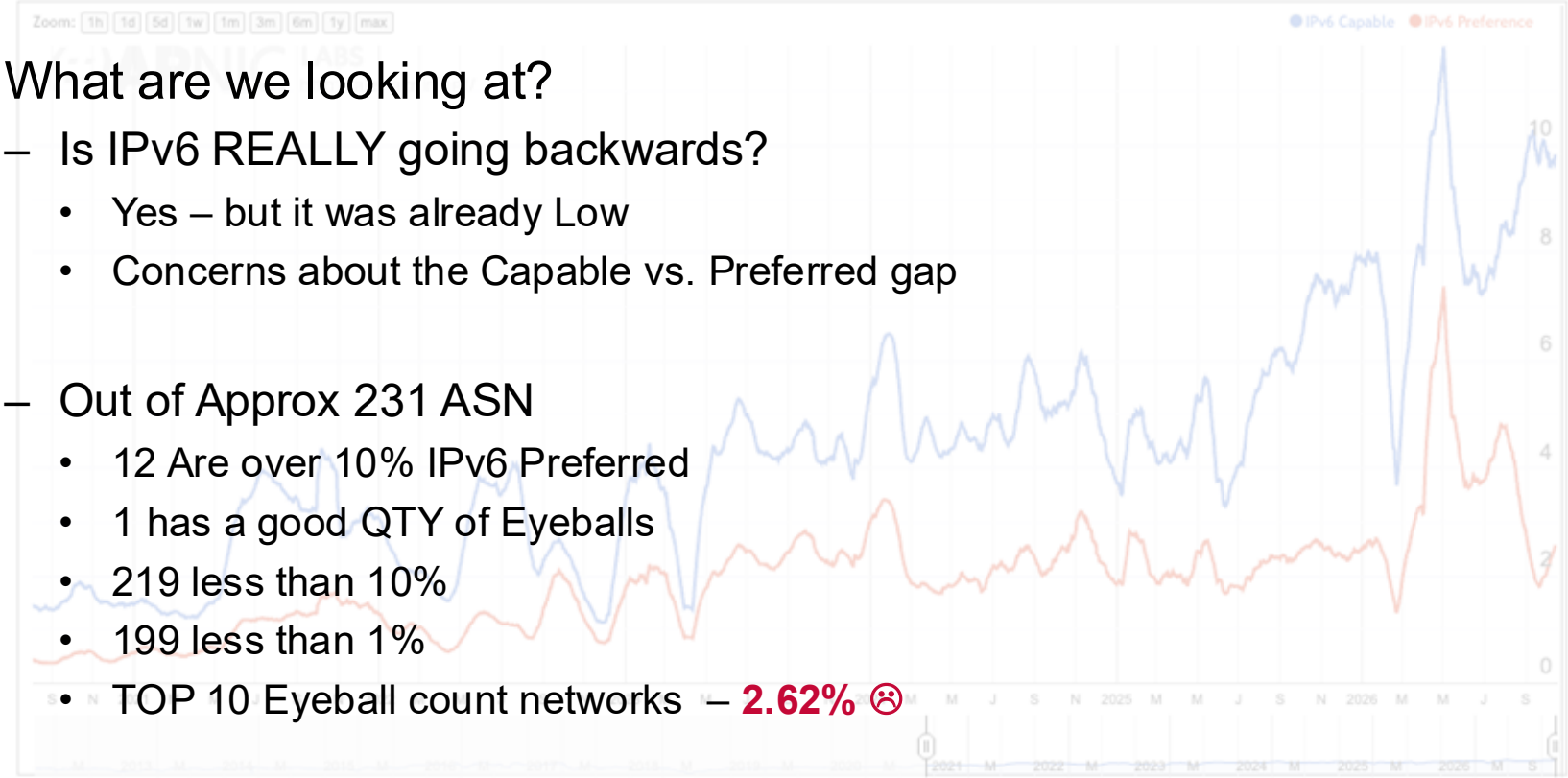
IPv6 – Hong Kong



https://stats.labs.apnic.net/ipv6/HK?c=HK&x=1&v=1&p=1&r=1&w=7

IPv6 – Hong Kong

- What are we looking at?
  - Is IPv6 REALLY going backwards?
    - Yes – but it was already Low
    - Concerns about the Capable vs. Preferred gap
  - Out of Approx 231 ASN
    - 12 Are over 10% IPv6 Preferred
    - 1 has a good QTY of Eyeballs
    - 219 less than 10%
    - 199 less than 1%
    - TOP 10 Eyeball count networks – **2.62%** ☹



https://stats.labs.apnic.net/ipv6/HK?c=HK&x=1&v=1&p=1&r=1&w=7

Challenges

IPv6 Challenges

- End user acceptance
  - Residential and Mobile
  - Business and Enterprise
- Networks not ready
  - Older equipment – *This should not be an issue in 2026*
  - Software (Billing/LOB)
  - Additional Licencing cost(especially Mobile)
- People
  - Staff are not adequately trained
    - Current Tertiary/Industry training rarely addresses IPv6(Pun Intended)
  - Misconception on use
  - Lack of ability to adequately address plan
  - Management not willing make changes

Why Deploy IPv6?

IPv6 Deployment

- Cost
  - IPv4 Address space ~US$10-15 Per IP
    - US$3,800 /24
  - Hardware
    - CGNAT is not free



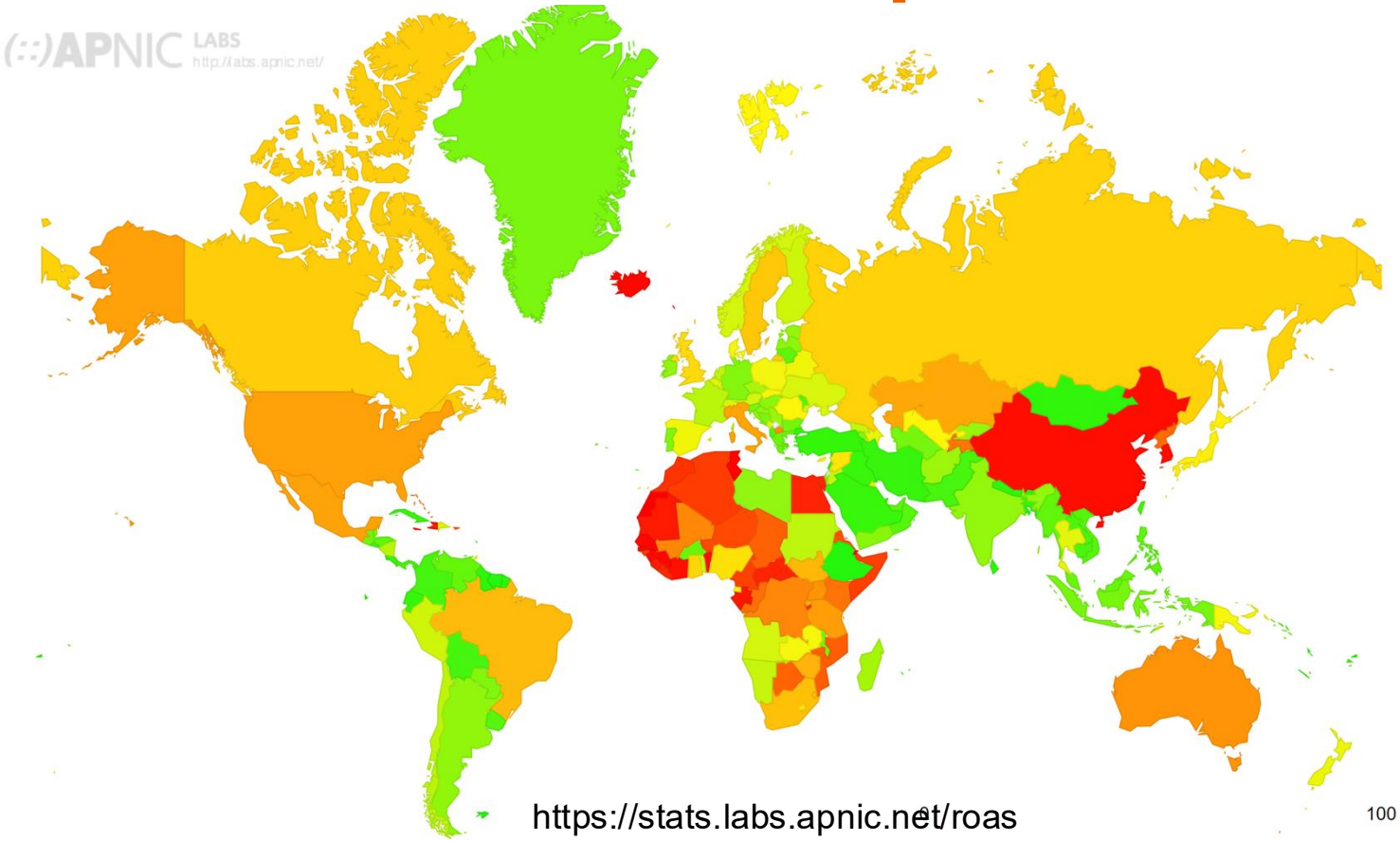
- The world is changing
  - 8 x increase/10 years
  - Hyperscalers are ready
  - CDN Providers are ready
  - IPv6 is now the higher preferred Protocol in the USA and Asia

IPv6 Deployment

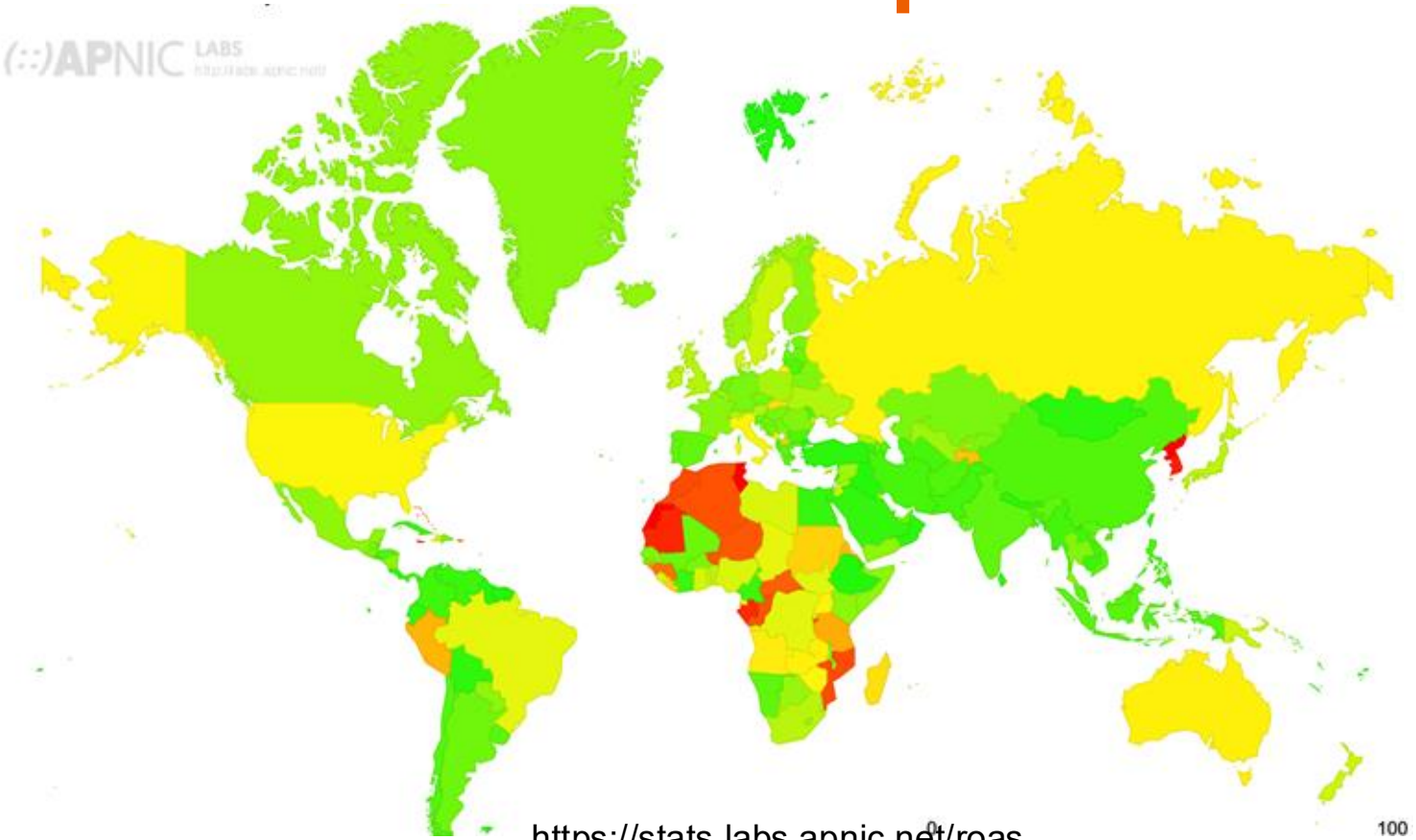
- Stop saying “I’ll do it tomorrow”
  - We have been saying that for 25 years
- Networks are not going to get simpler
- Need practical help?
  - Training: https://academy.apnic.net/
  - TA: https://academy.apnic.net/en/technical-assistance

RPKI

RPKI ROA – Global Snapshot - 2024



RPKI ROA – Global Snapshot - 2026



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

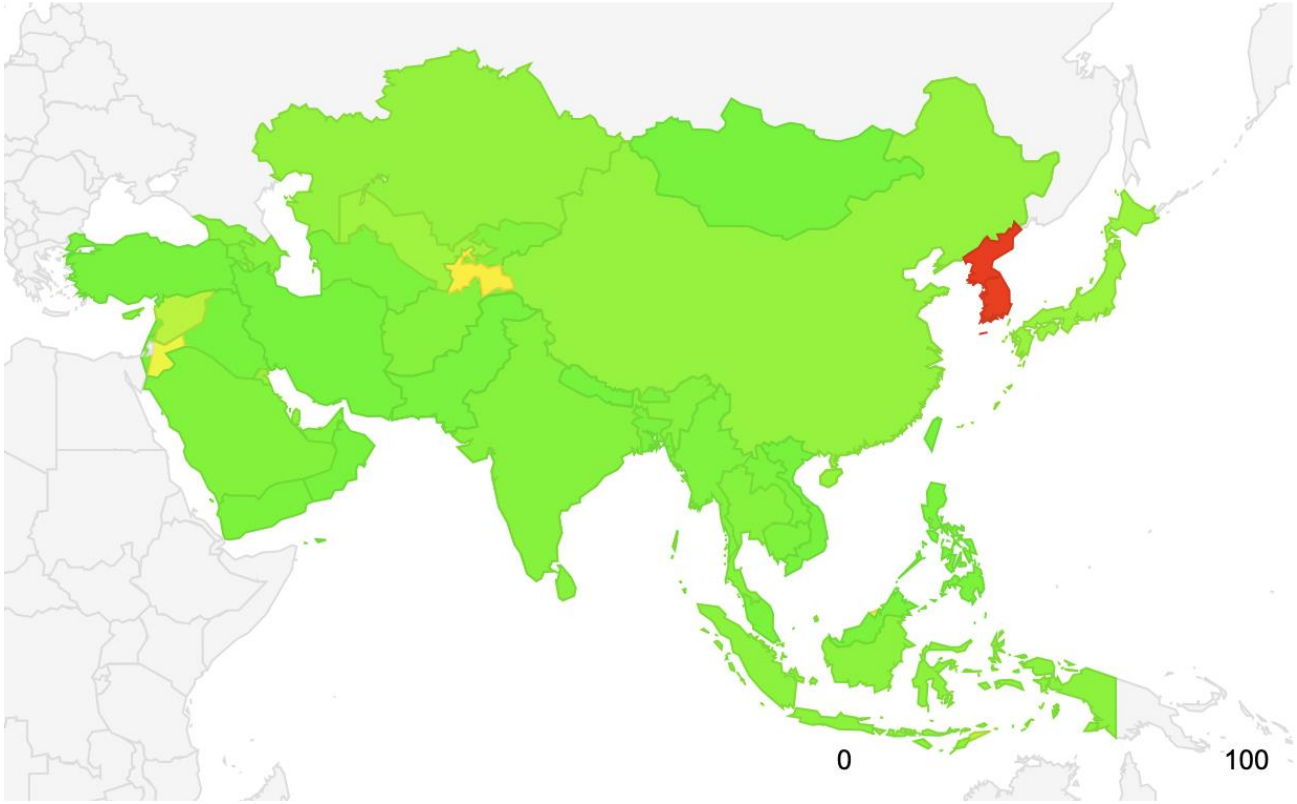
RPKI ROA – Global Snapshot - 2026

- 47.8% Global IPv4 Signed
- 57.9% Asia
- 34.6% North America
- 54.2% South America
- 53.7% Europe
- 29.7% Africa
- 69.4% Oceania



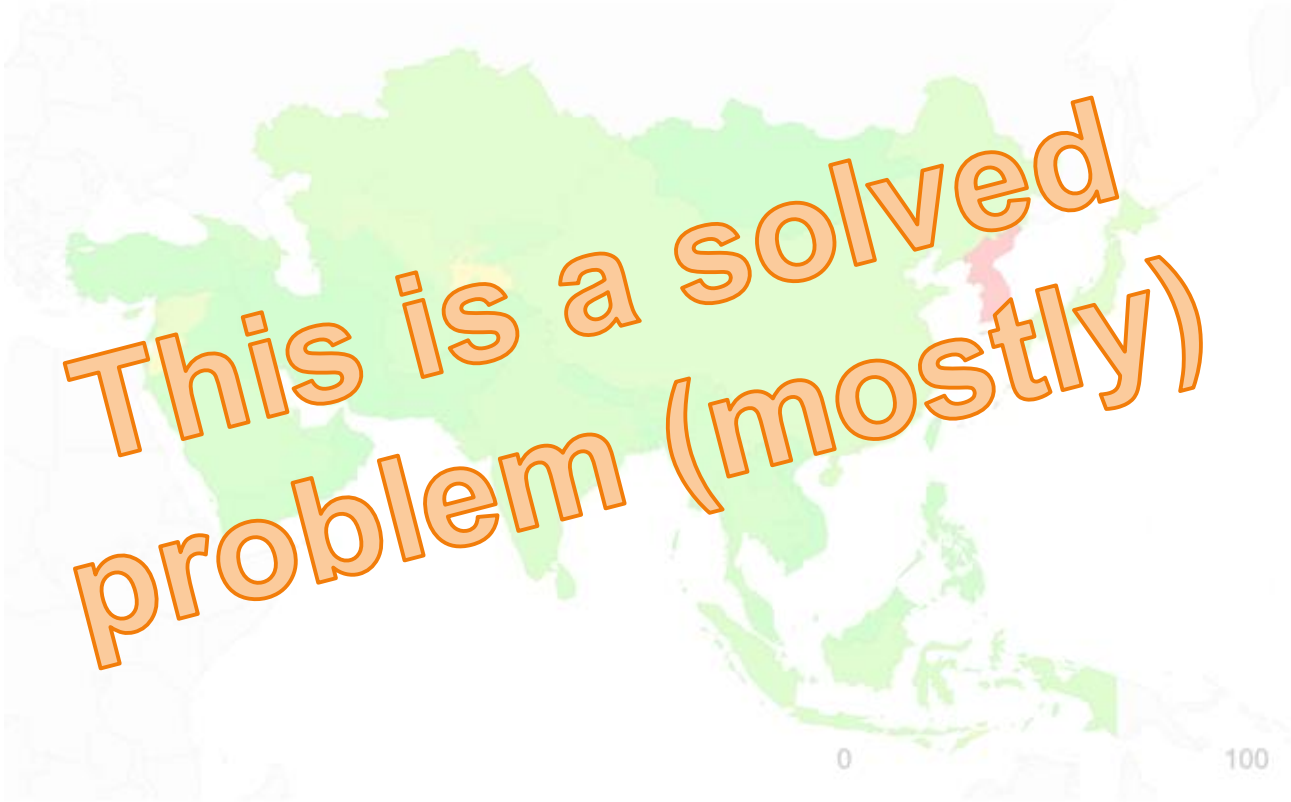
https://stats.labs.apnic.net/roas

RPKI ROA – Asia



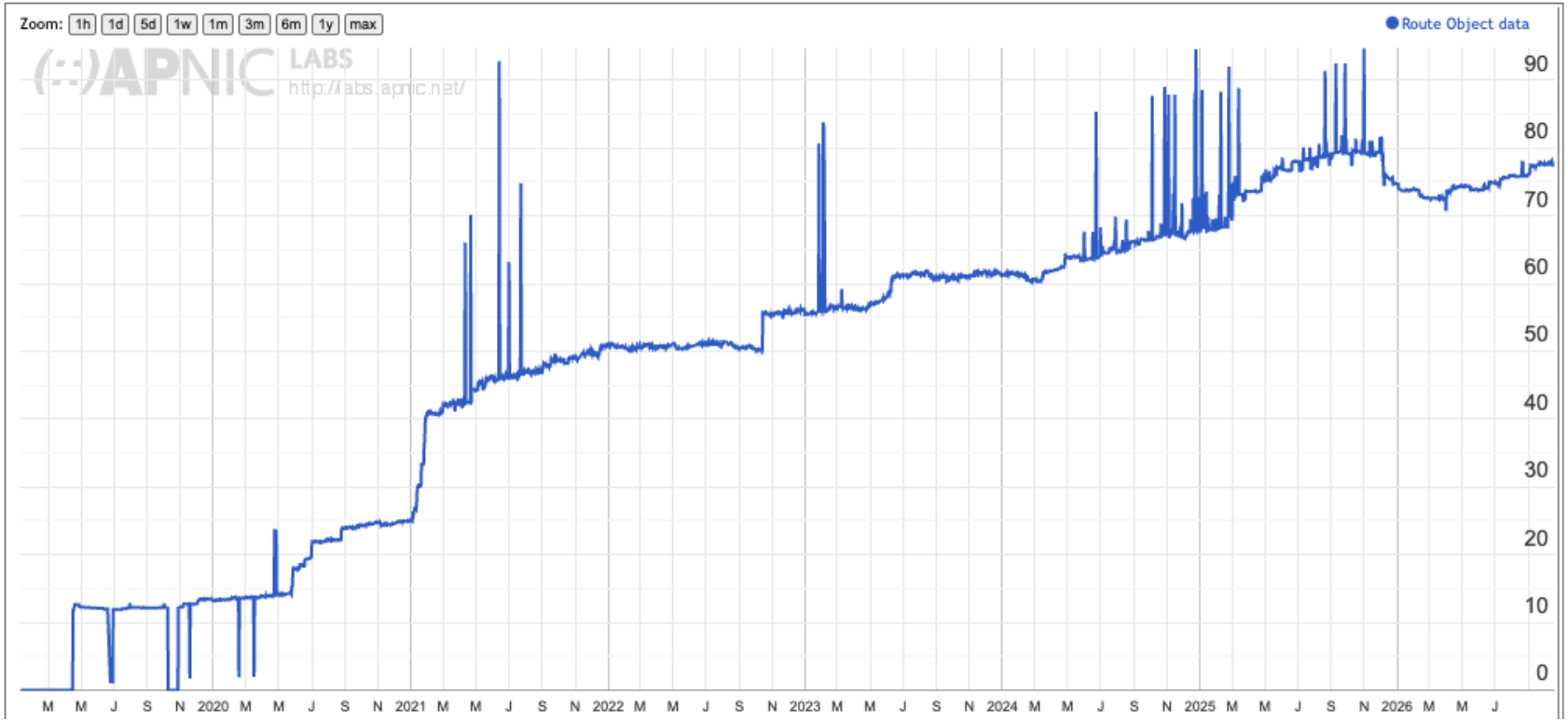
https://stats.labs.apnic.net/roa/XD

RPKI ROA – Asia



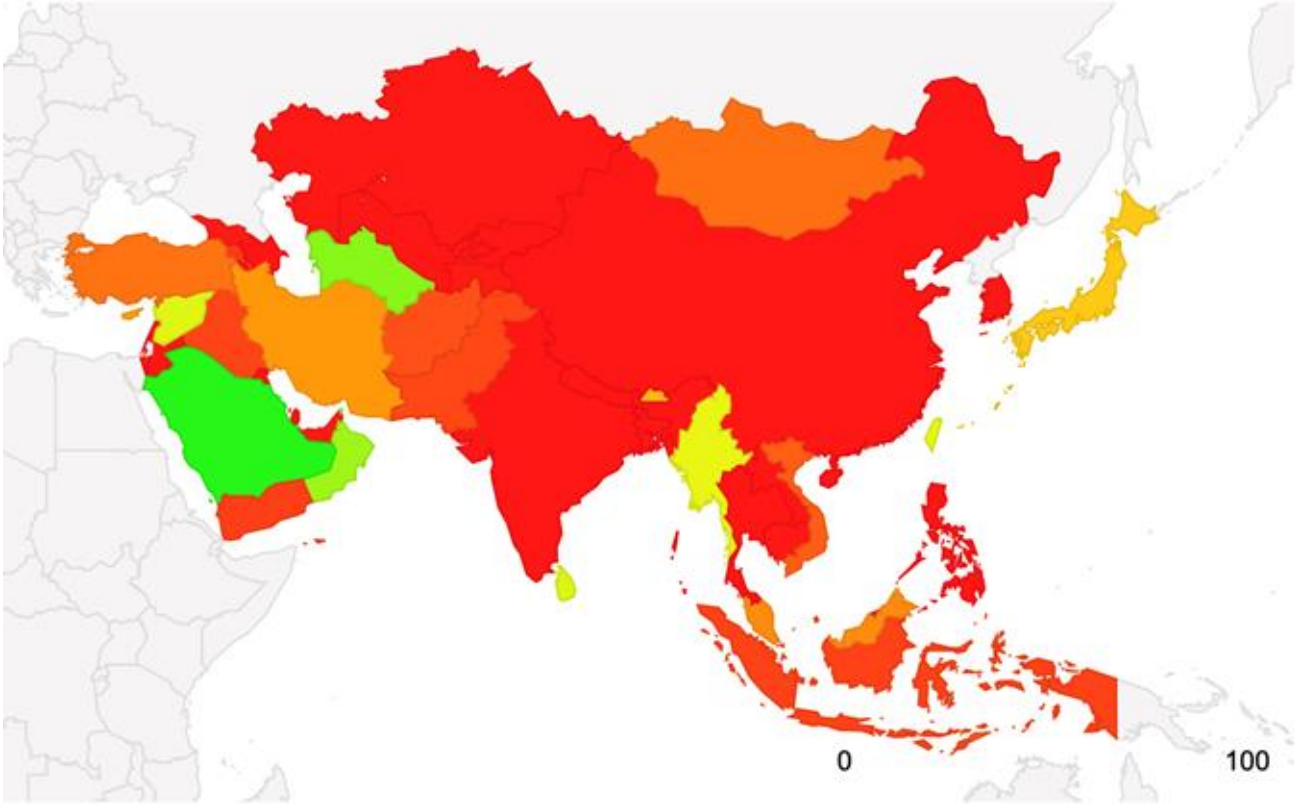
https://stats.labs.apnic.net/roa/XD

RPKI ROA – Hong Kong – IPv4



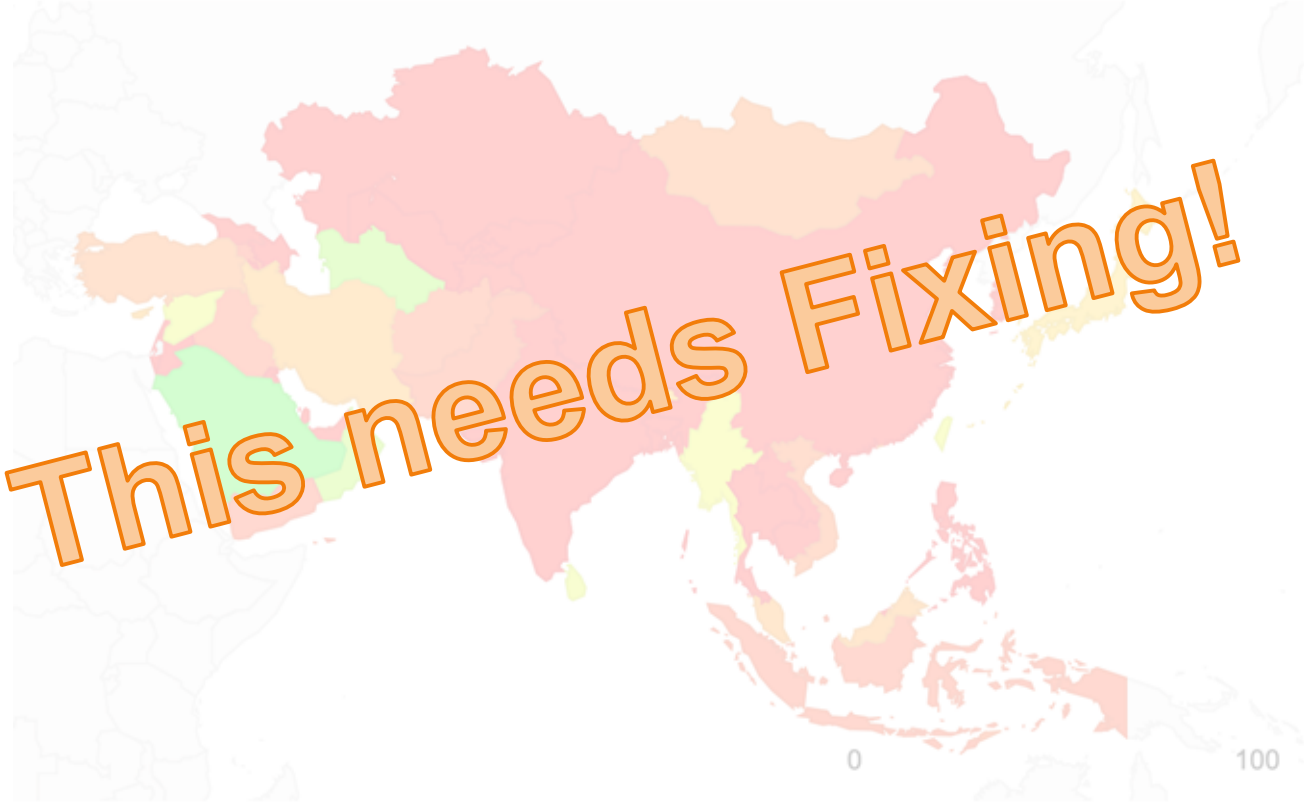
https://stats.labs.apnic.net/roa/HK

RPKI ROV – Asia



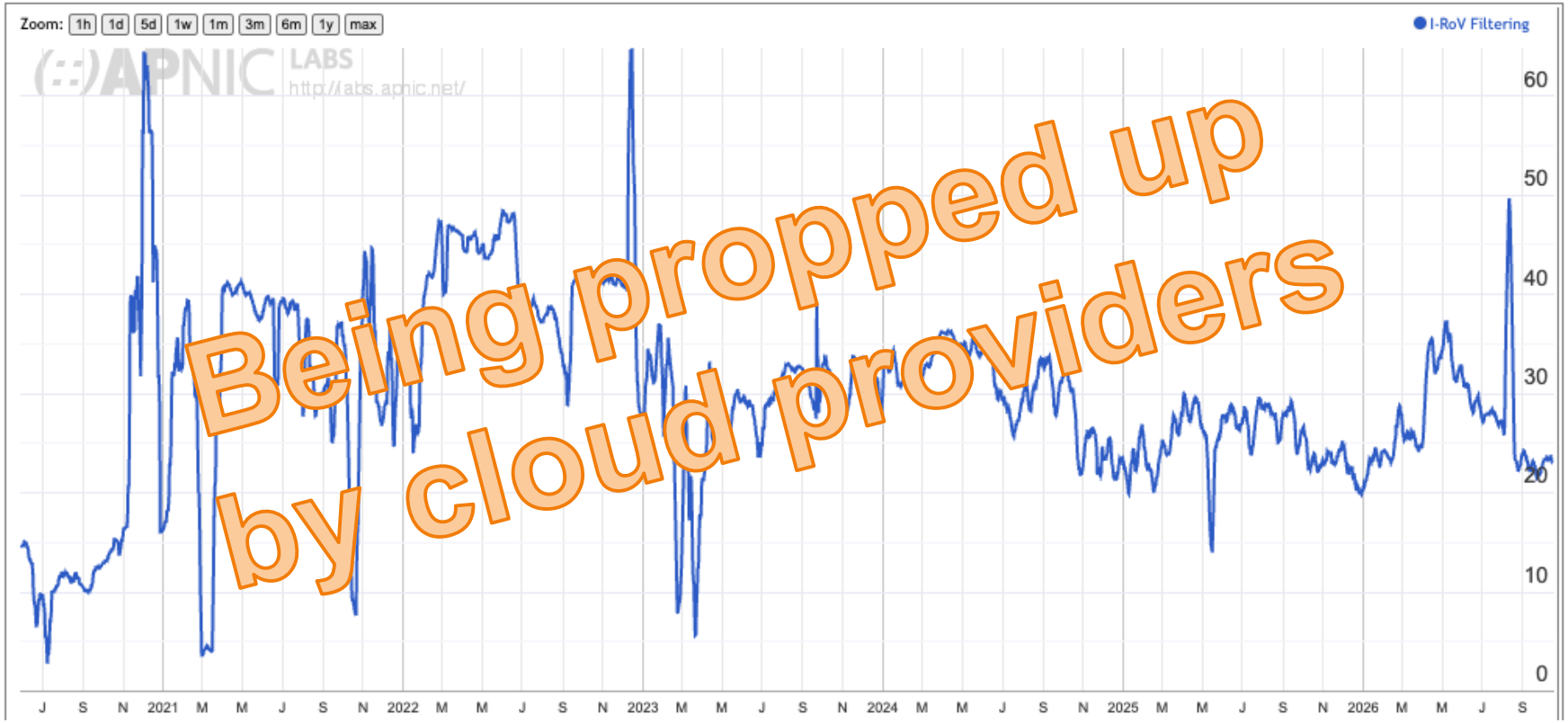
https://stats.labs.apnic.net/rpki/XD

RPKI ROV – Asia



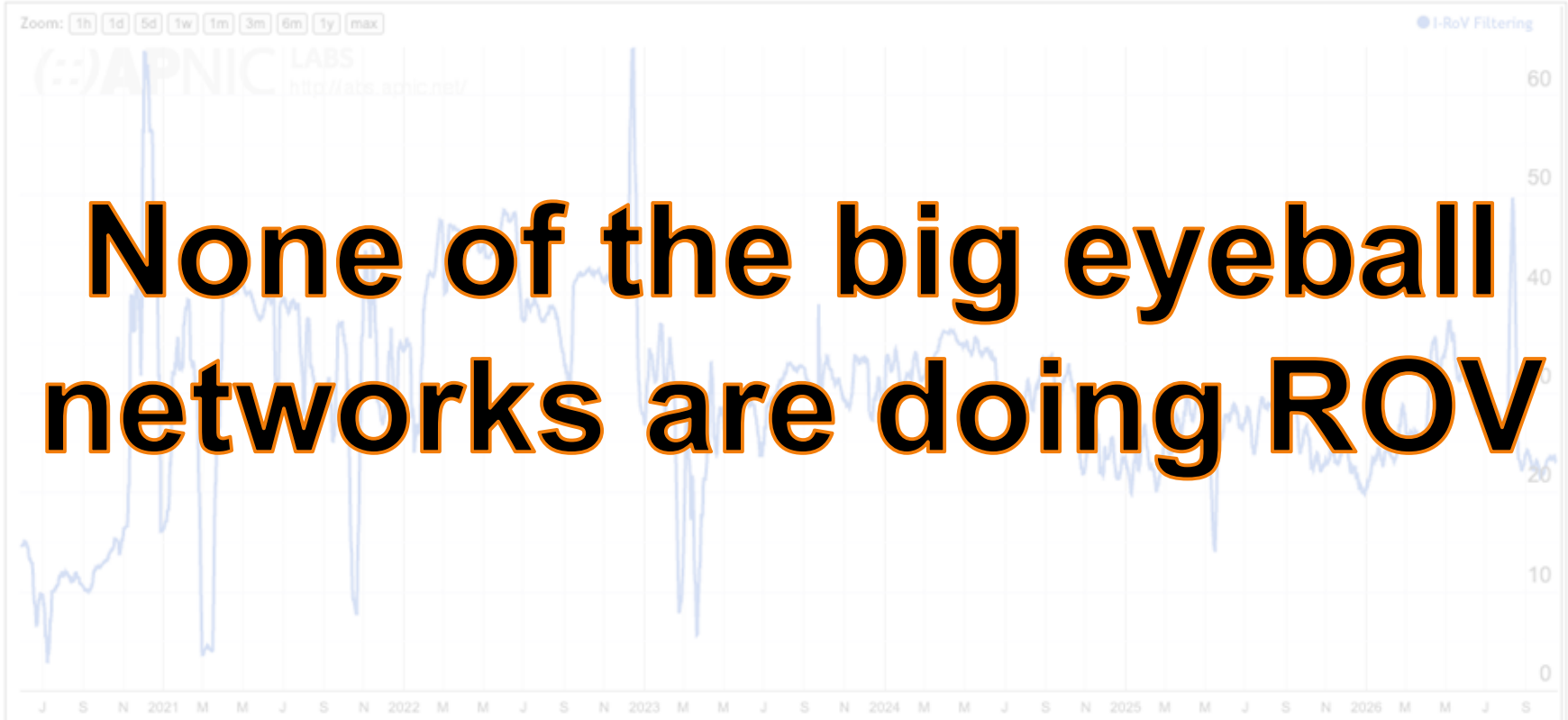
https://stats.labs.apnic.net/rpki/XD

RPKI ROV – Hong Kong



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

RPKI ROV – Hong Kong



None of the big eyeball networks are doing ROV

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

RPKI – ASPA – What is it?

- Autonomous System Provider Authorization
- Defined in two documents:
  - draft-ietf-sidrops-aspa-profile
  - draft-ietf-sidrops-aspa-verification
- The specifications provide for:
  - an ASN holder signing an object that defines its upstream ASes
  - a network operator using that data to verify the AS_PATH of a received route

RPKI – ASPA – Why is it useful?

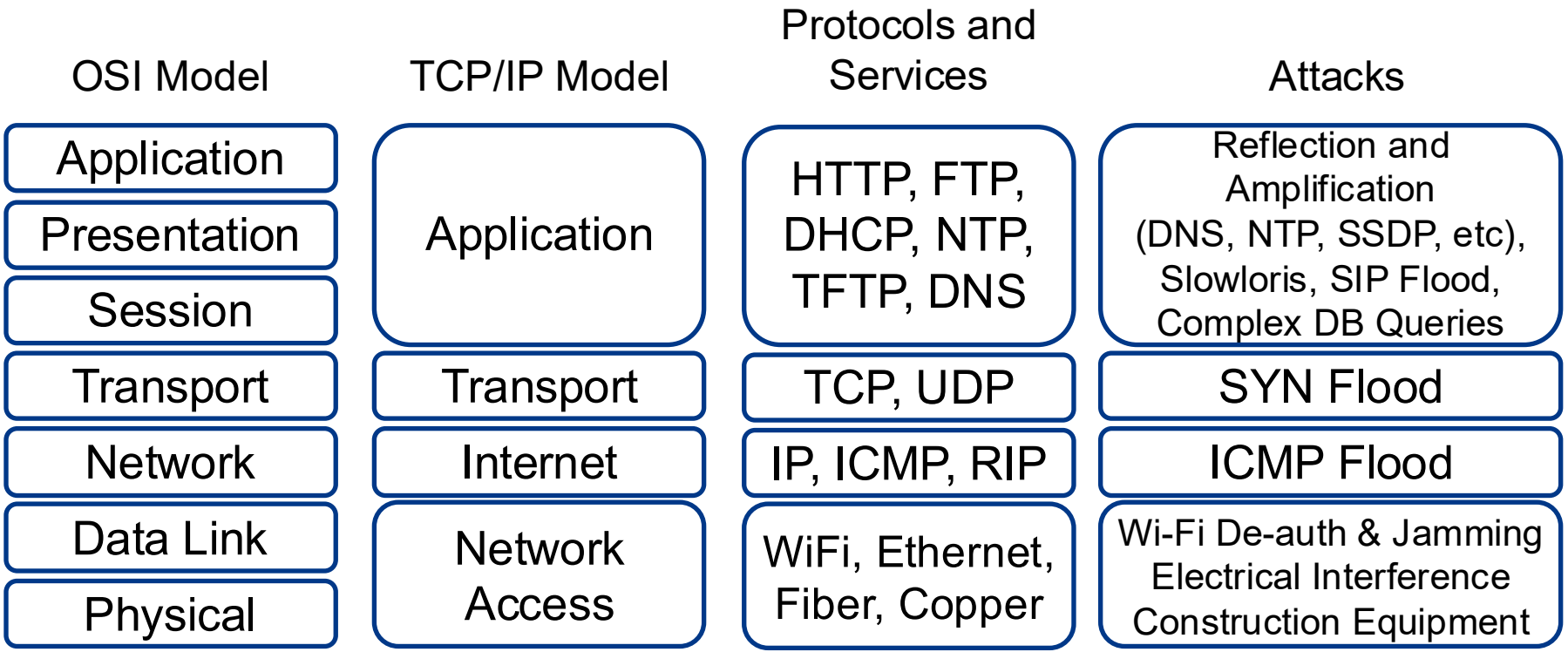
- Detect and mitigate route leaks
  - Compare ROV, which is about the origin only
- Protect against certain types of
  - forged-origin/forged-path attacks
  - Attacker must resort to longer AS paths for route to be accepted

RPKI – What do I need to do

- ROA
  - Sign your Routes (APNIC Portal)
  - ASPA – CREATE THEM! (only 15 in HK)
  - Make sure your ROA's and ASPA Match your BGP Routing
    - Check with routeviews/bgp.tools etc
- ROV
  - Full Routing Table
    - Attend some RPKI Training
    - Setup A Validator and start dropping invalid routes
  - Default/Partial Feed
    - Encourage Up-streams to Drop Invalids.

Security

DoS by Layers

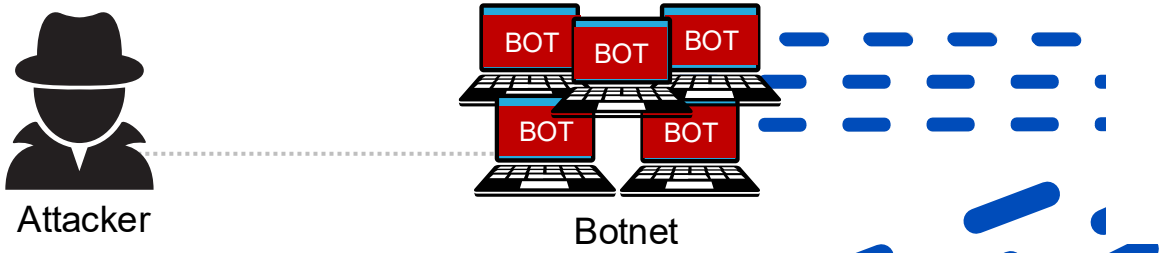


* Colour animated slide

Reflected and Amplified DDoS

1 Attacker directs bots to begin attack

2 All bots send DNS queries for the TXT record in domain “evil.com” to open recursive DNS servers and fake "my IP is 10.10.1.1"



Attacker

Botnet

3 Open resolvers ask the authoritative name server for the TXT record “evil.com”



evil.com authoritative name server

4 evil.com name server responds with 4000 byte TXT records



Victim (10.10.1.1)

5 Open resolvers cache the response and send a stream of 4000 byte DNS responses to the victim

Reflection and Amplification

- What makes for good reflection?
  - UDP
    - Spoofable / forged source IP addresses
    - Connectionless (no 3-way handshake)
- What makes for good amplification?
  - Small command results in a larger reply
    - This creates a Bandwidth Amplification Factor (BAF)
    - Reply Length / Request Length = BAF
      - Example: 3223 bytes / 64 bytes = BAF of 50.4
    - Chart on next slide created with data from https://www.us-cert.gov/ncas/alerts/TA14-017A

Amplification Factors

Protocol	Bandwidth Amplification Factor
Multicast DNS (mDNS)	2-10
BitTorrent	3.8
NetBIOS	3.8
Steam Protocol	5.5
SNMPv2	6.3
Portmap (RPCbind)	7 to 28
DNS	**28 to 54**
SSDP	**30.8**

Protocol	Bandwidth Amplification Factor
LDAP	46 to 55
TFTP	60
Quake Network Protocol	63.9
RIPv1	131.24
QOTD	140.3
CHARGEN	358.8
NTP	**556.9**
Memcached	**up to 51,000**

So why are you telling me this?

- Operators Complain about DoS/DDoS
- Do the minimum to ensure they are not contributing

- But How bad is it really?
  - (Hint: It's not good….)

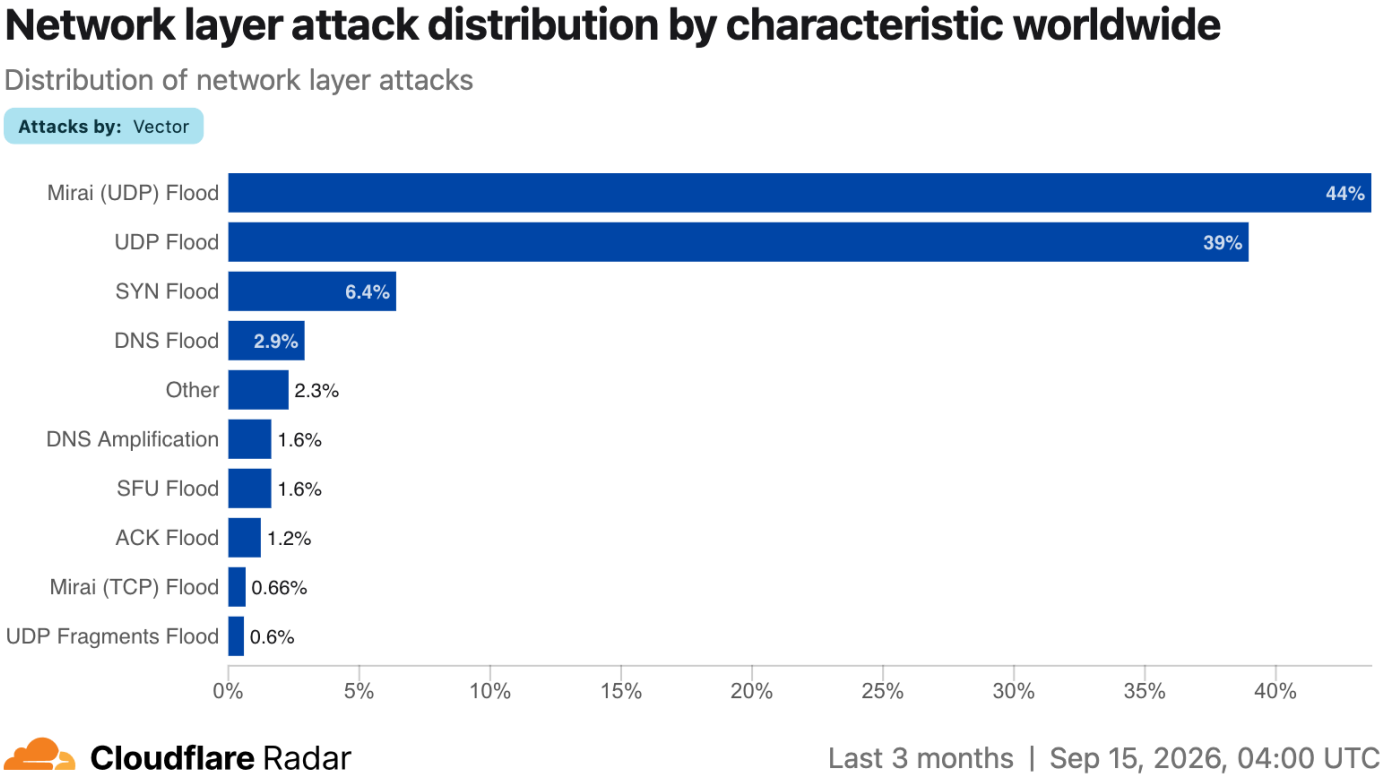
Global Numbers

- Most data sourced from
  - Cloudflare Radar
  - Shodan.io
- Top 5 Countries DDoS Sources

OCTOBER 2023	July 2024	September 2026
USA - 31%	USA – 18.8%	Brazil – 18.5%
India – 9.2%	Germany – 8.45%	USA – 12.2%
Germany – 5.4%	**China - 7.49**	Argentina – 5.4%
Brazil – 5.2%	**Pakistan – 5.9%**	Chile – 4.2%
China – 3.3%	UK – 4.5%	**India – 5.3%**

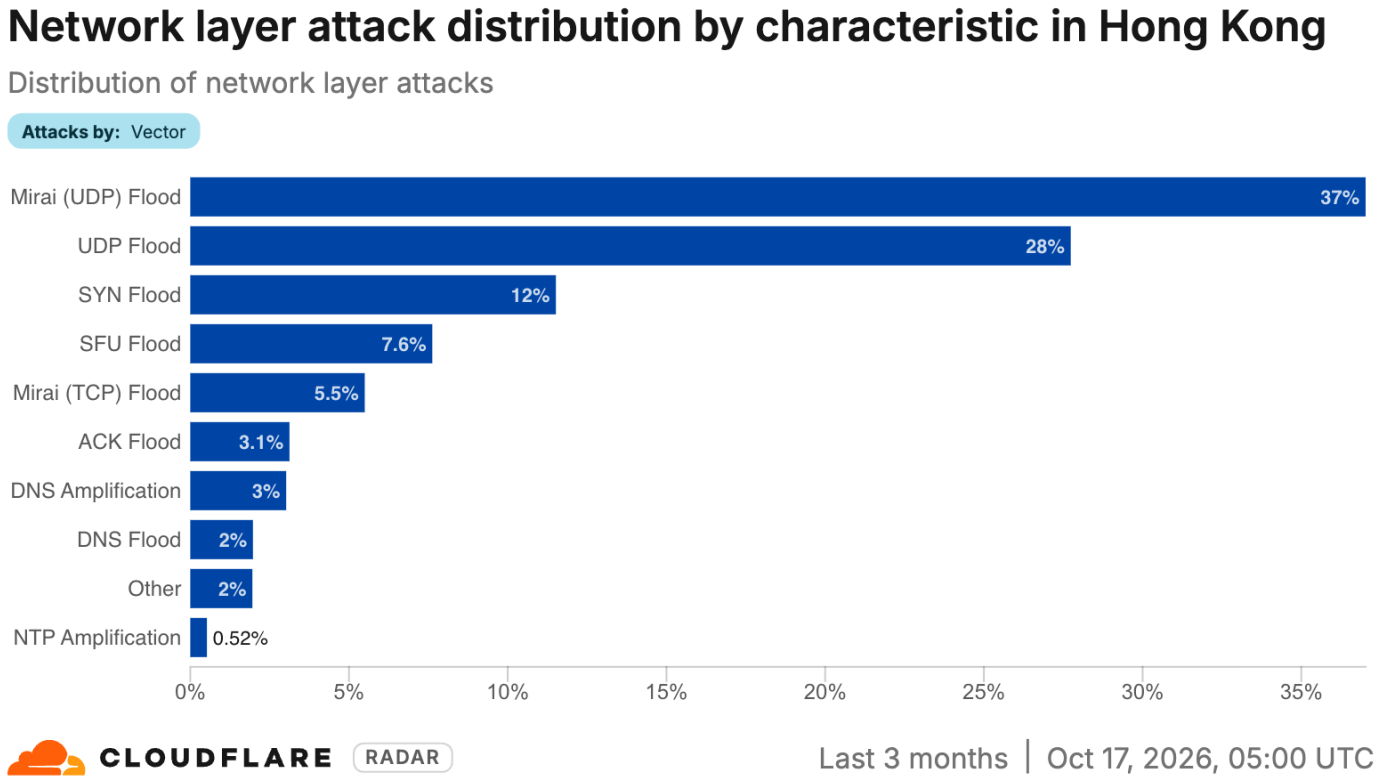
https://radar.cloudflare.com/security/network-layer

Global Numbers



https://radar.cloudflare.com/security/network-layer

Hong Kong



https://radar.cloudflare.com/security/network-layer/hk?dateRange=12w

Hong Kong

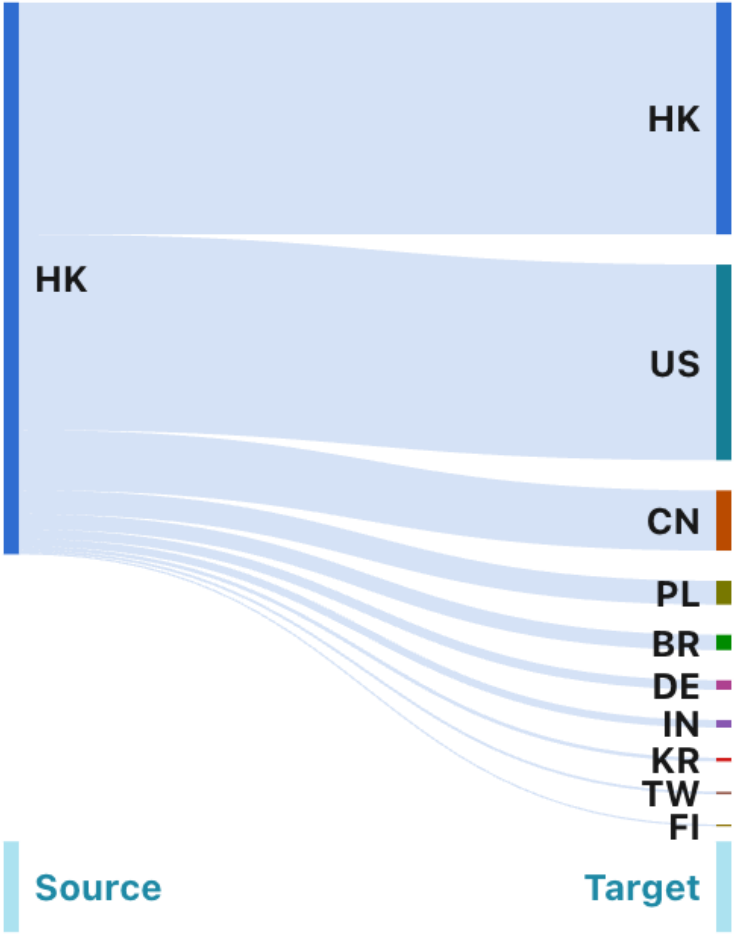
- Open Ports

DNS	17,035
NTP	70,982
SSDP	737
MemcacheD	86
Telnet	2,701
SNMP	9,729
Winbox	3,145

https://www.shodan.io/search?query=country%3Ahk

Hong Kong

- Targets



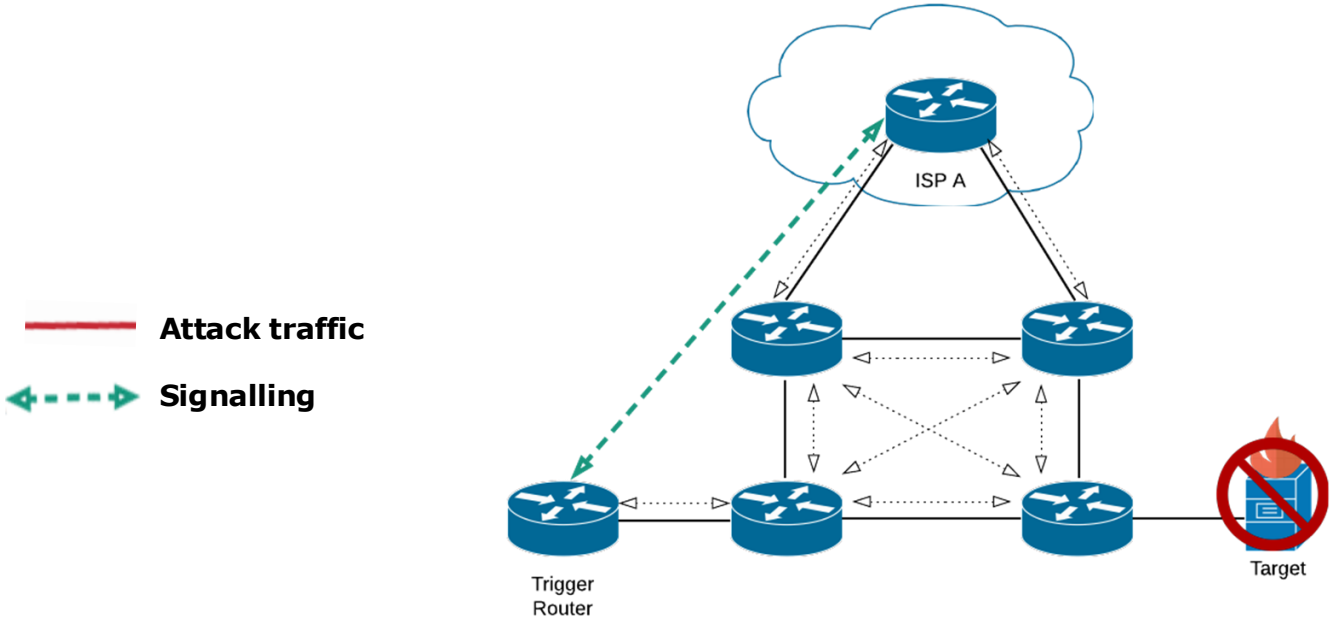
https://radar.cloudflare.com/security/network-layer/hk?dateRange=12w

Mitigation Strategies

- Protect your services from attack
  - Anycast
  - IPS / DDoS protection
  - Overall network architecture
- Protect your services from attacking others
  - Rate-limiting
  - BCP38 (outbound filtering) source address validation
  - Securely configured DNS, NTP and SNMP servers
  - No open resolvers!
    Only allow owned or authorised IP addresses to connect

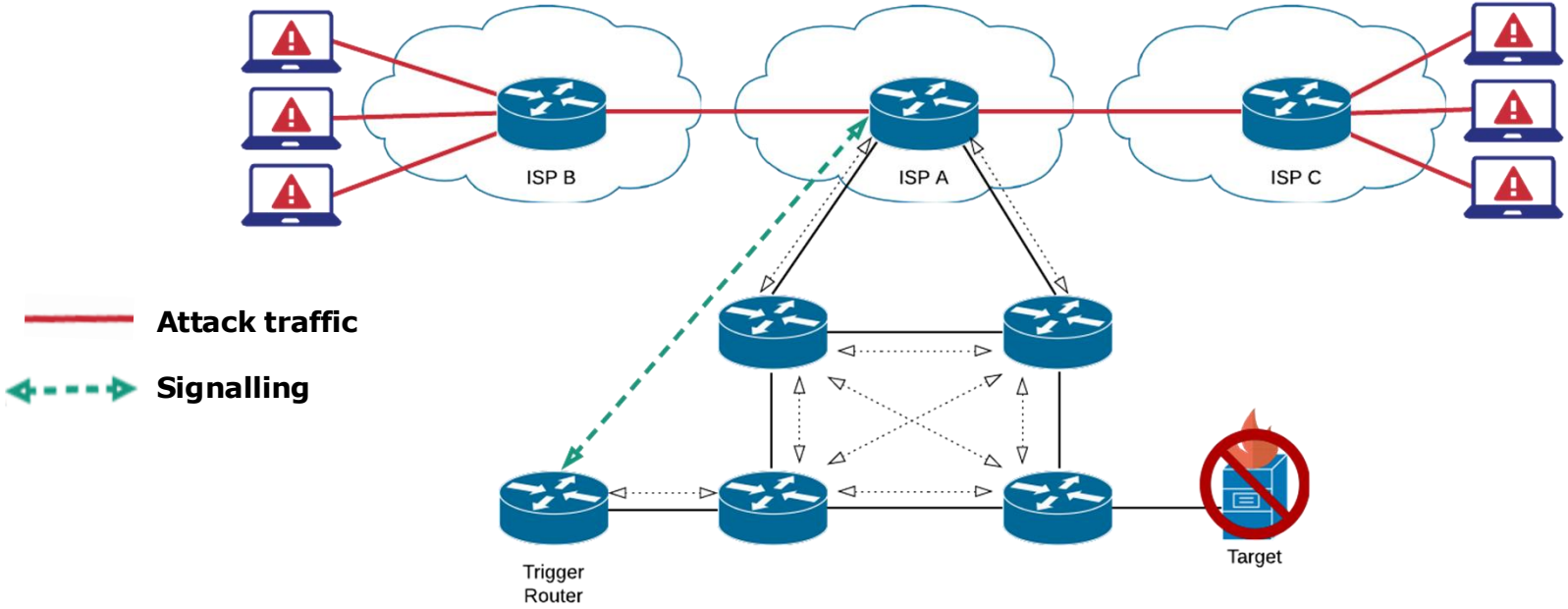
Mitigation Strategies

- Remote Triggered Black Hole (RTBH) filtering
  - With your ISP



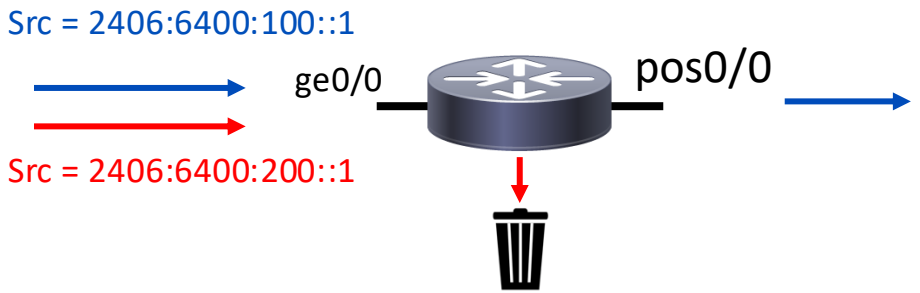
Mitigation Strategies

- Remote Triggered Black Hole (RTBH) filtering
  - With your ISP

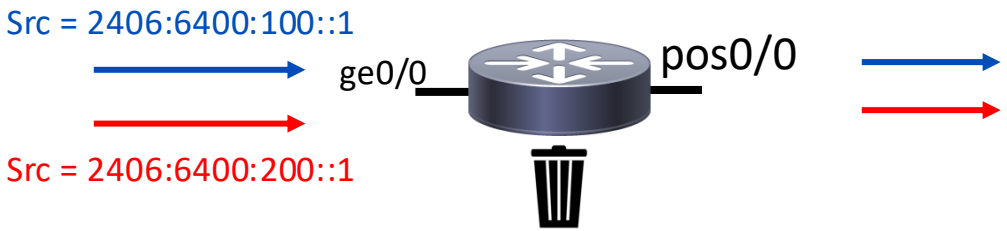


Mitigation Strategies

- uRPF
  - Strict: verifies both source address and incoming interface with entries in the forwarding table
  - Loose: verifies existence of route to source address



Forwarding Table:
2406:6400:100::/48 ge0/0
2406:6400:200::/48 fa0/0



Mitigation Strategies

- Source Remote Triggered Black Hole (sRTBH) filtering
  - RTBH with uRPF (Unicast Reverse Path Forwarding)
    - RFC5635
  - Basic Operation
    - Setup a RTBH Sinkhole (routing to a Null Interface)
    - Enable uRPF in loose mode
    - Create an appropriate community to NH traffic to your Sinkhole
    - When a source is identified
      - Tag with appropriate community to send to the Sink
      - uRPF check will fail (as it is routed to a Null)
      - Traffic Dropped

http://www.cisco.com/web/about/security/intelligence/blackhole.pdf

Questions?

