The Internet – By the numbers

South Asia – Oct 2024

Dave Phelan - APNIC

Who Am I?

- Dave Phelan
  - Network and Infrastructure engineer for a LONG time
  - Trainer at APNIC
  - Parent to 2 Human children and 3 Fur Children
  - 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?

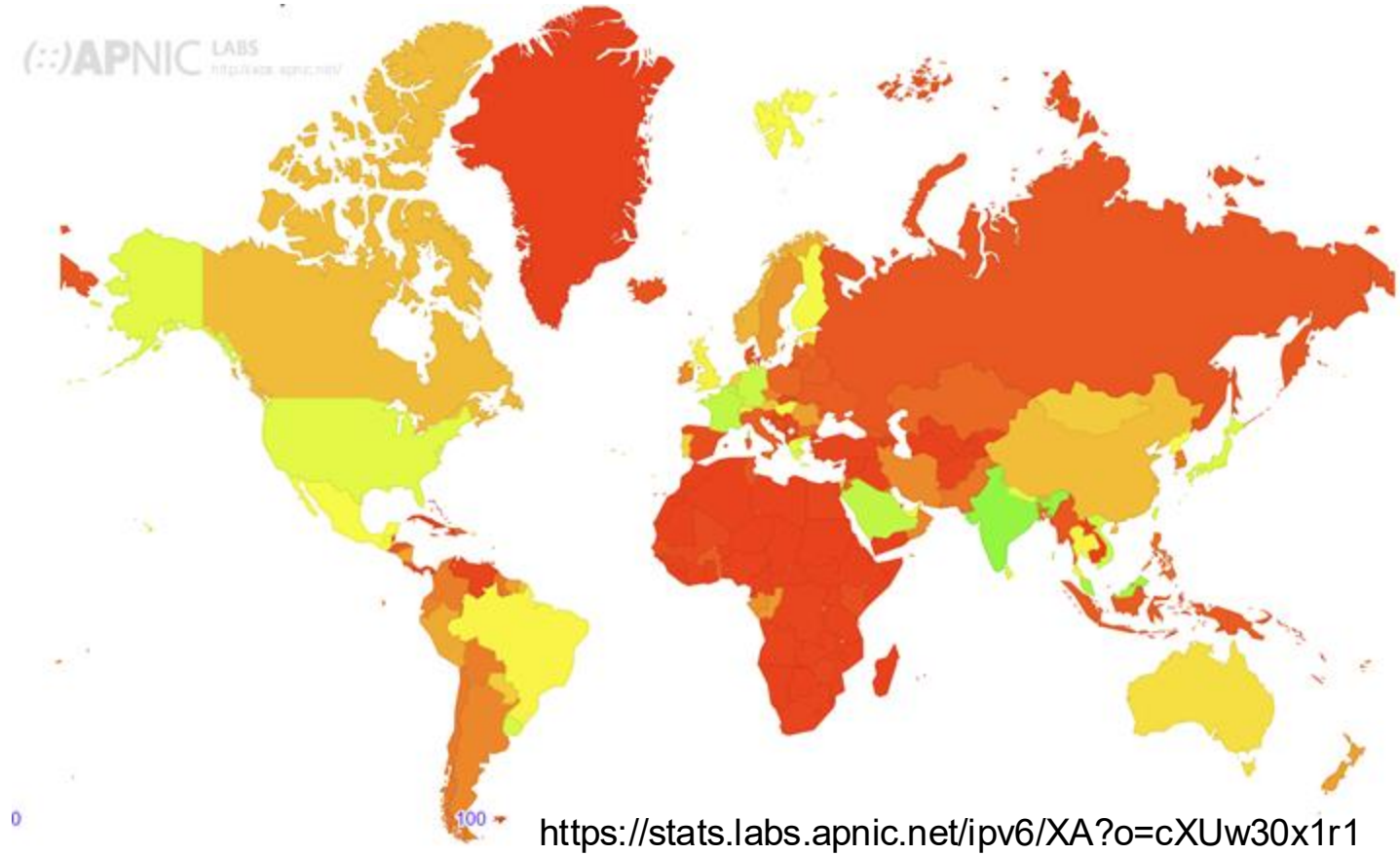
- We can use this as a benchmark
  - How are we performing
    - Network to Network
    - Economy to Economy
    - Region to Region
- What do we need to “fix”
  - Are we doing all we can within our region (see Benchmarks Above)
- Can we do better
  - For our Networks and our Users

Sources

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

IPv6

IPv6 – Global Snapshot



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

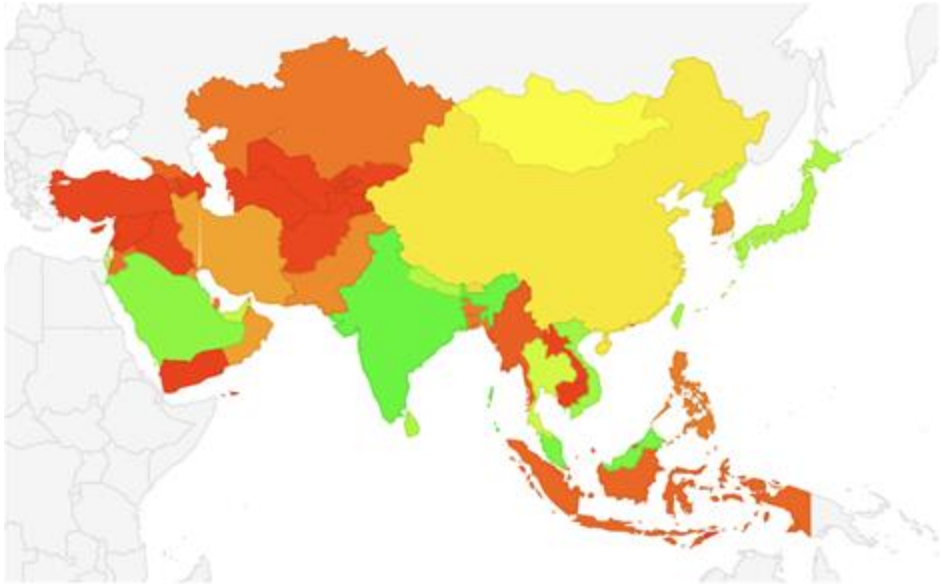
IPv6 – Global Snapshot

- 38% Global Preference
- 44.8% Asia
- 51.6% North America
- 34.8% South America
- 31.03% Europe
- 3.01% Africa
- 37.4% Oceania

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

IPv6 – Asia Sub-Region

- 3 Sub-regions
  - 69.43% South Asia
    - IN,LK,NP,BT,PK,BD,AF,MV
  - 38.5% East Asia
    - TW,JP,MN,CN,MO,KR,HK,KP
  - 31.2% South-East Asia
    - MY,VN,TH,SG,PH,ID,MM,LA,BN,KH,TL



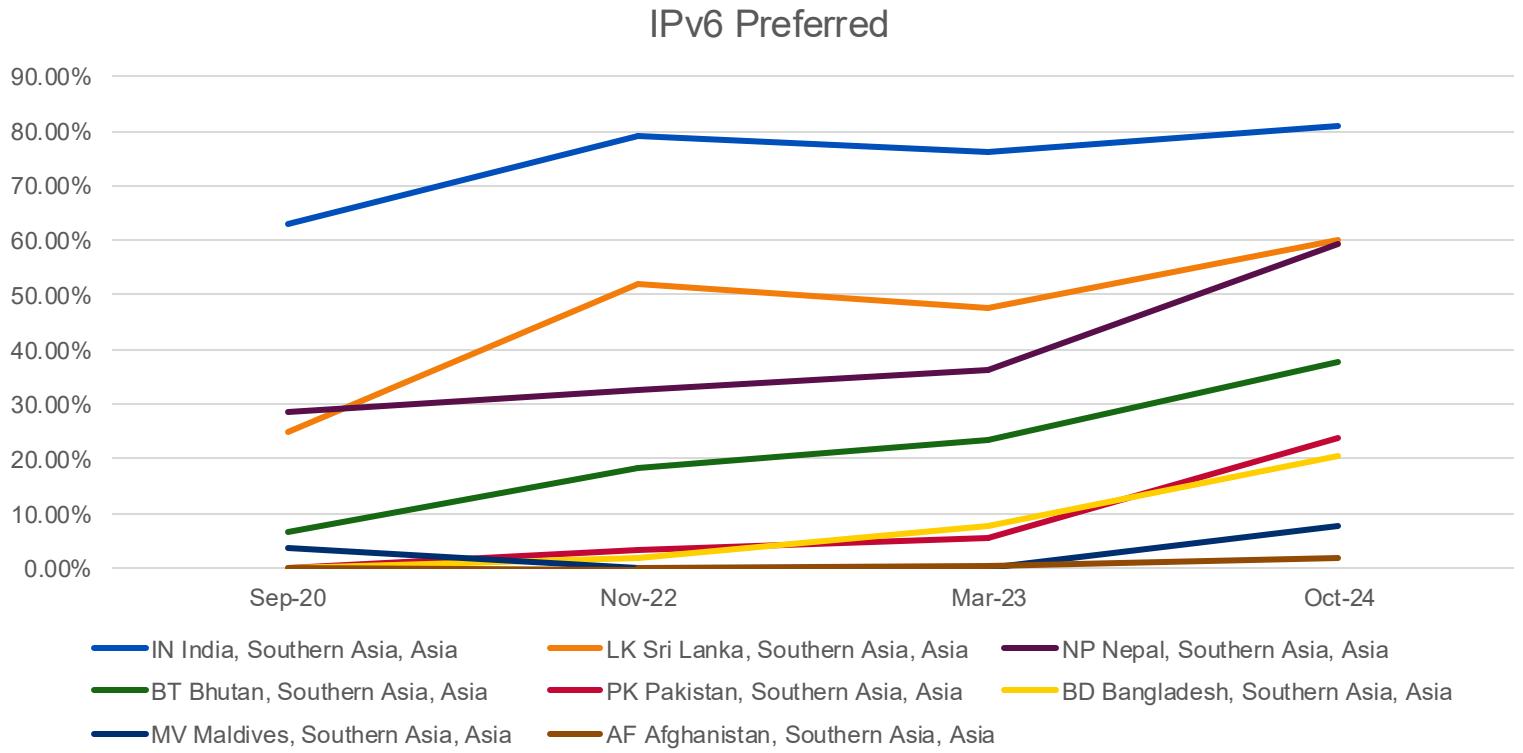
https://stats.labs.apnic.net/ipv6/XT?o=cPKw30x1r1

IPv6 – South Asia Sub-Region

CC	Country	Sep-20	Nov-22	Mar-23	Oct-24
IN	India, Southern Asia, Asia	63.07%	78.96%	76.19%	80.91%
LK	Sri Lanka, Southern Asia, Asia	25.10%	52.14%	47.67%	60.19%
NP	Nepal, Southern Asia, Asia	28.60%	32.71%	36.44%	59.43%
BT	Bhutan, Southern Asia, Asia	6.72%	18.35%	23.35%	37.65%
PK	**Pakistan, Southern Asia, Asia**	**0.03%**	**3.44%**	**5.44%**	**23.87%**
BD	Bangladesh, Southern Asia, Asia	0.03%	1.87%	7.68%	20.49%
MV	Maldives, Southern Asia, Asia	3.51%	0.08%	0.07%	7.67%
AF	Afghanistan, Southern Asia, Asia	0.11%	0.06%	0.23%	1.85%

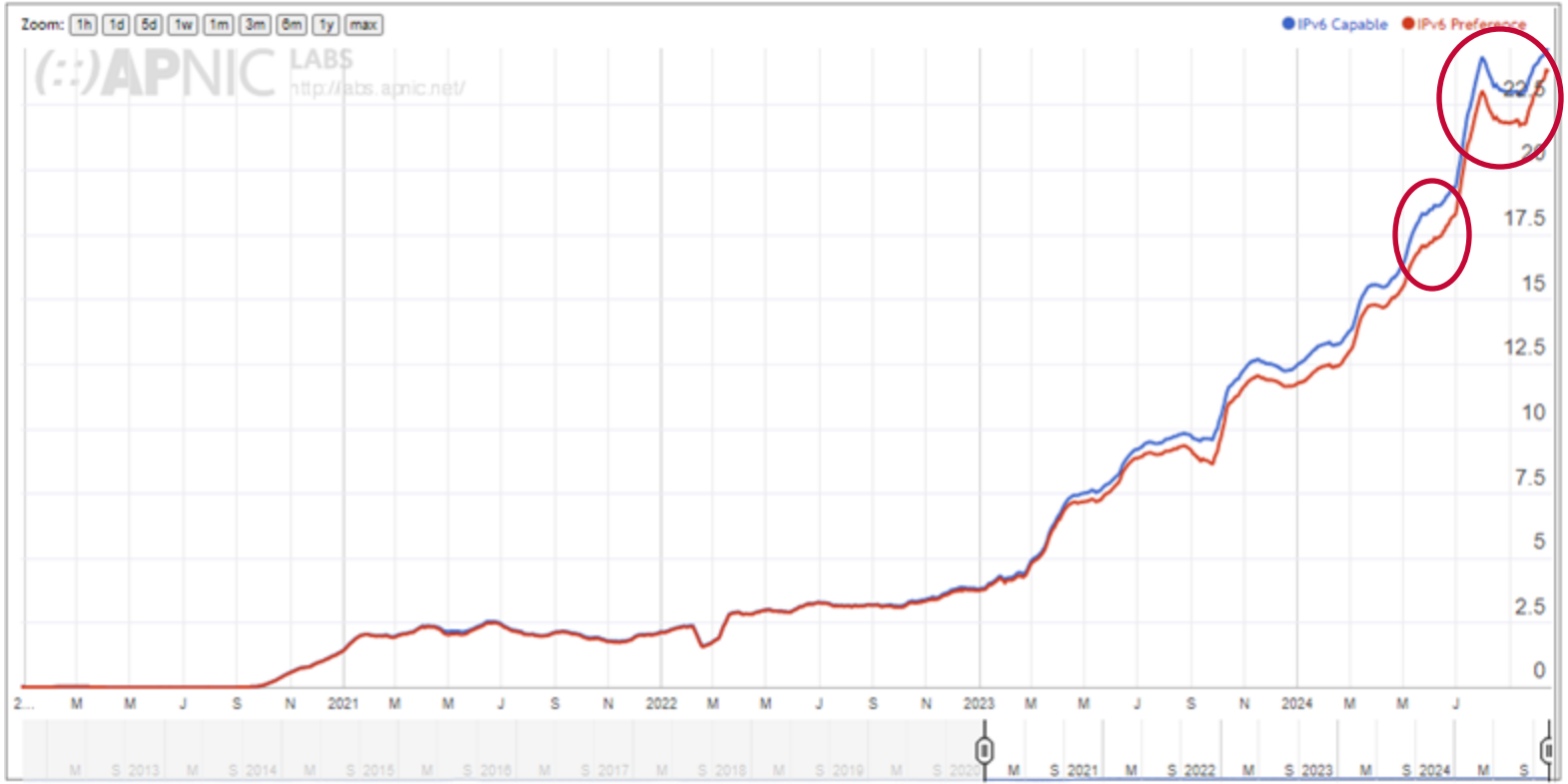
https://stats.labs.apnic.net/ipv6/XT?o=cPKw30x1r1

IPv6 – South Asia Sub-Region



https://stats.labs.apnic.net/rpki/XT?o=cXDw7v0p1x0l1

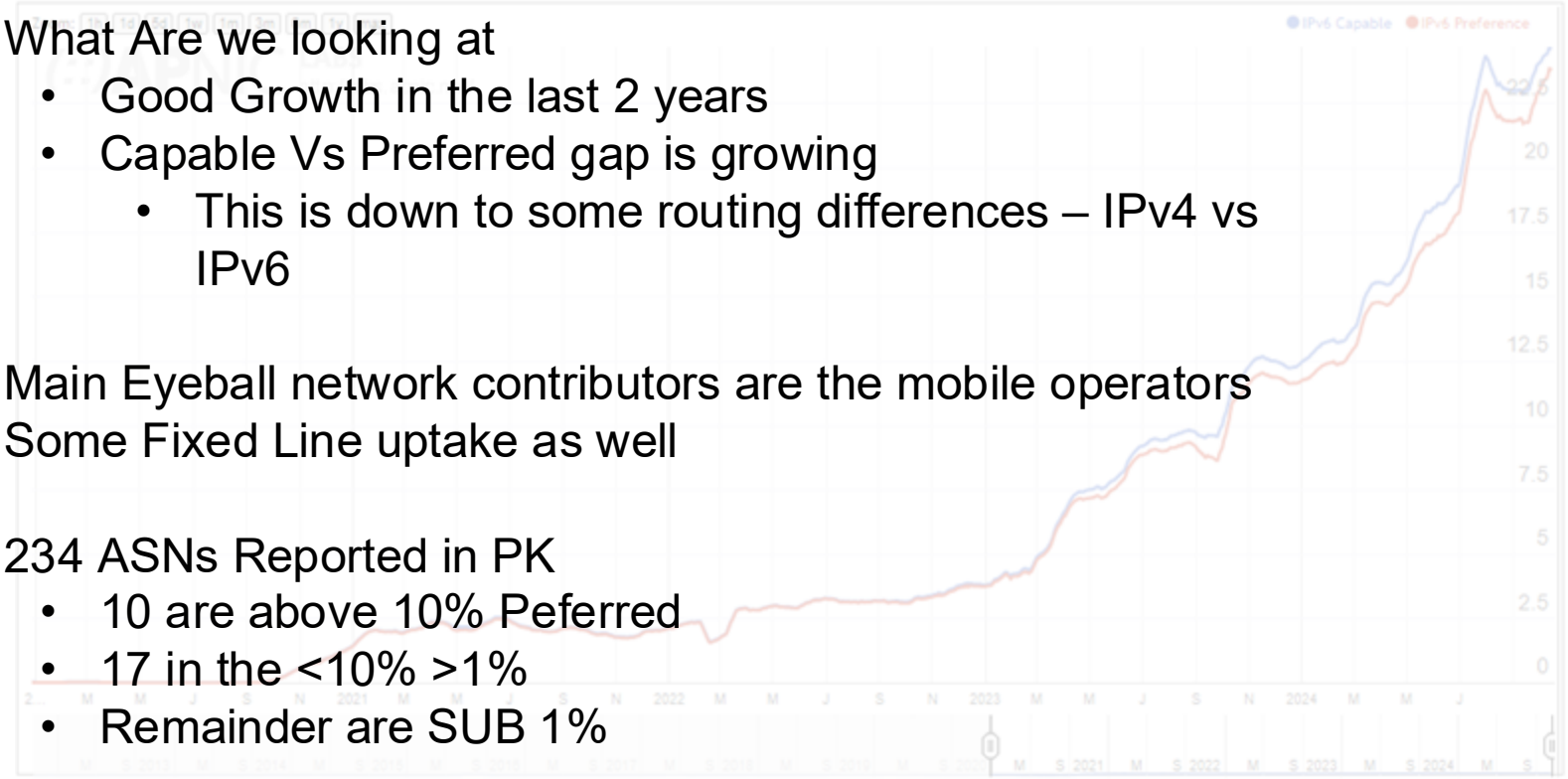
IPv6 – Pakistan



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

IPv6 – Pakistan

- What Are we looking at
  - Good Growth in the last 2 years
  - Capable Vs Preferred gap is growing
    - This is down to some routing differences – IPv4 vs IPv6



- Main Eyeball network contributors are the mobile operators
- Some Fixed Line uptake as well

- 234 ASNs Reported in PK
  - 10 are above 10% Peferred
  - 17 in the <10% >1%
  - Remainder are SUB 1%

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

Challenges

IPv6 Challenges

- End user acceptance
  - Residential and Mobile
  - Business and Enterprise
- Networks not ready
  - Older equipment
  - 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$40-50 Per IP
    - US$12,800 /24
  - Hardware
    - CGNAT is not free

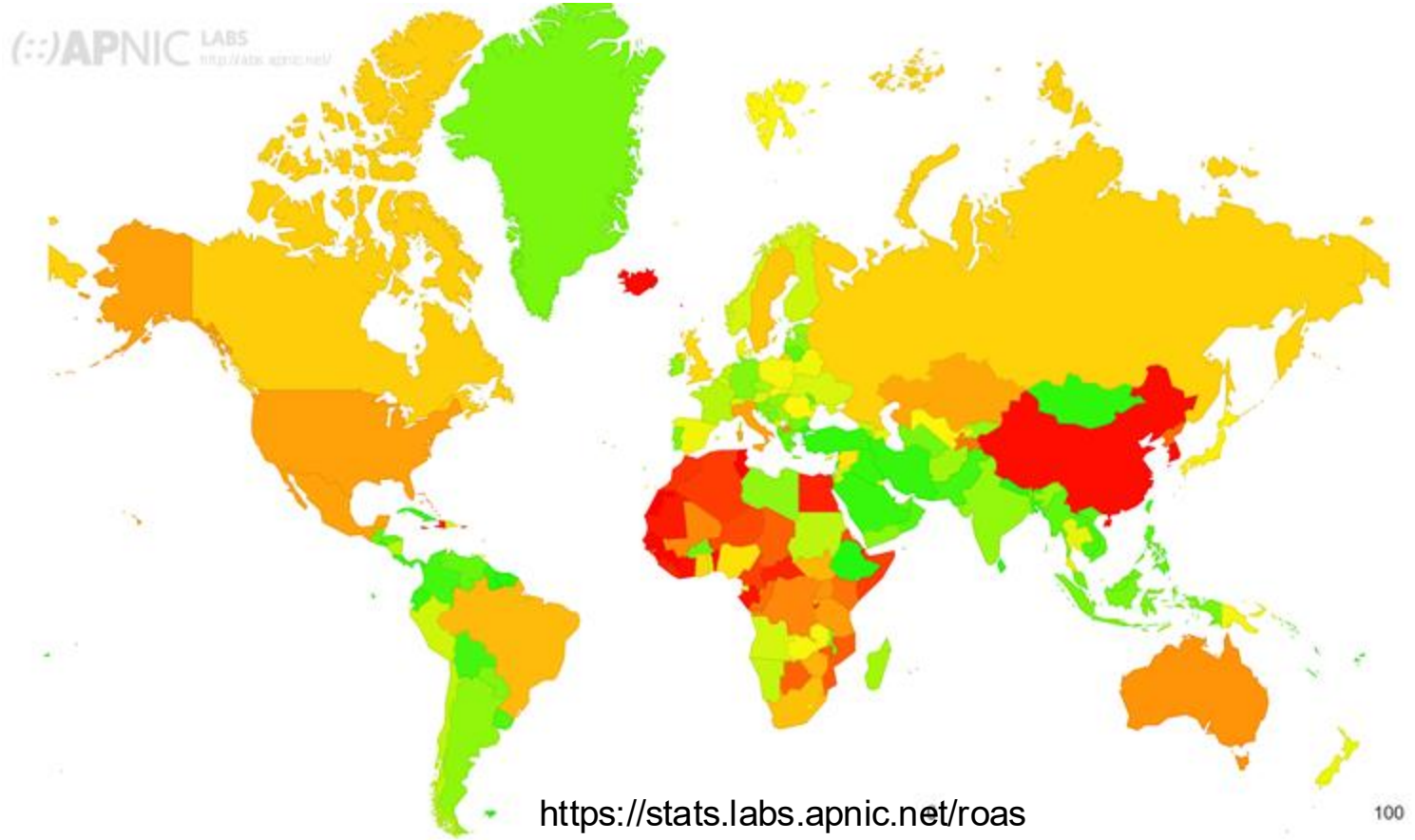
- The world is changing
  - 3 x increase/5 years
  - Hyperscalers are catching up
  - CDN Providers are ready for your IPv6 Packets
  - IPv6 is now the higher preferred Protocol in the USA

IPv6 Deployment

- Stop saying “I’ll do it tomorrow”
  - We have been saying that for 25 years
- Networks are not going to get simpler
- Grants Are available
  - https://isif.asia/infrastructure-ipv6/
    - US$30-250K
    - Open to all Industry types
- Need practical help?
  - Training: https://academy.apnic.net/
  - TA: https://academy.apnic.net/en/technical-assistance

RPKI

RPKI ROA – Global Snapshot



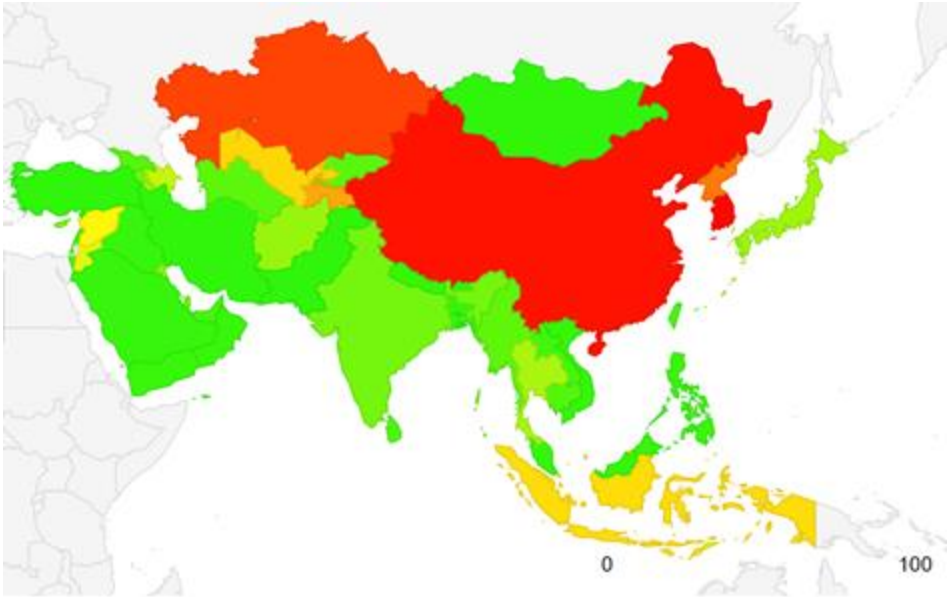
RPKI ROA – Global Snapshot

- 48.2% Global IPv4 Signed
- 54.4% Asia
- 35.7% North America
- 55.3% South America
- 55.8% Europe
- 33% Africa
- 70% Oceania

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

RPKI ROA – Asia Subregion

- 3 Sub-regions
  - 87.3% South Asia
    - IN,LK,NP,BT,PK,BD,AF,MV
  - 29.3% East Asia
    - TW,JP,MN,CN,MO,KR,HK,KP
  - 76.7% South-East Asia
    - MY,VN,TH,SG,PH,ID,MM,LA,BN,KH,TL



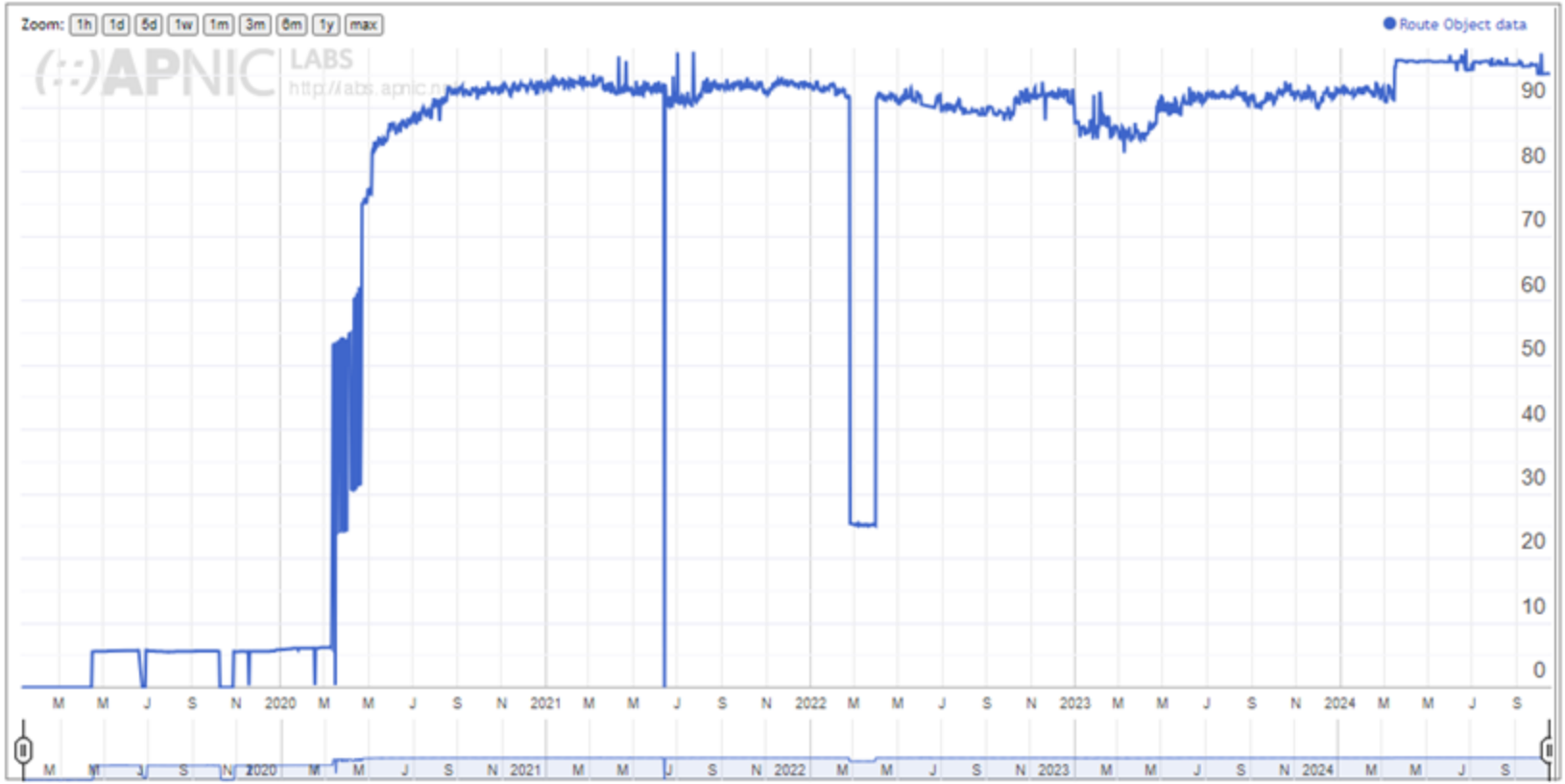
https://stats.labs.apnic.net/roa/XD

RPKI ROA – South Asia Subregion

Code	Region	V4 Valid	Pc	V4 Invalid	Pc2	V4 Unknwn	Pc3	PoT
BT	Bhutan, Southern Asia, Asia	42204	99.30%	36	0.10%	256	0.60%	0.08%
MV	Maldives, Southern Asia, Asia	95488	98.70%	0	0.00%	1280	1.30%	0.18%
PK	**Pakistan, Southern Asia, Asia**	**5111766**	**96.70%**	**47658**	**0.90%**	**127744**	**2.40%**	**9.81%**
NP	Nepal, Southern Asia, Asia	562688	96.10%	256	0.00%	22528	3.80%	1.09%
BD	Bangladesh, Southern Asia, Asia	1776332	95.70%	9780	0.50%	70912	3.80%	3.45%
LK	Sri Lanka, Southern Asia, Asia	550400	91.40%	256	0.00%	51456	8.50%	1.12%
IN	India, Southern Asia, Asia	37117115	82.00%	364613	0.80%	7790336	17.20%	84.01%
AF	Afghanistan, Southern Asia, Asia	106752	73.30%	1024	0.70%	37888	26.00%	0.27%

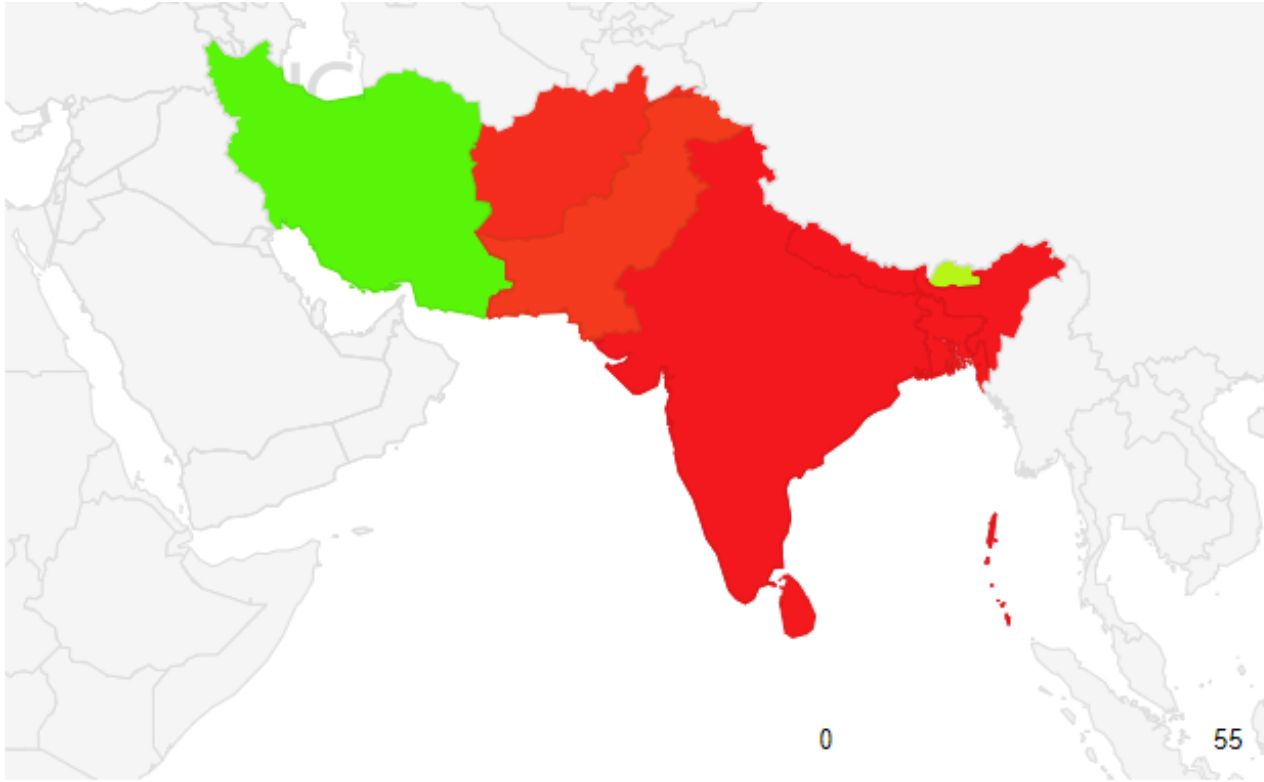
https://stats.labs.apnic.net/roa/XT

RPKI ROA – Pakistan



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

RPKI ROV – South Asia



https://stats.labs.apnic.net/rpki/XT?o=cXDw7v0p1x0l1

RPKI ROV – South Asia

Code	Region	RPKI Validates
BT	Bhutan, Southern Asia, Asia	37.55%
PK	Pakistan, Southern Asia, Asia	5.90%
AF	Afghanistan, Southern Asia, Asia	4.17%
LK	Sri Lanka, Southern Asia, Asia	1.10%
BD	Bangladesh, Southern Asia, Asia	1.01%
IN	India, Southern Asia, Asia	0.83%
NP	Nepal, Southern Asia, Asia	0.61%
MV	Maldives, Southern Asia, Asia	0.51%

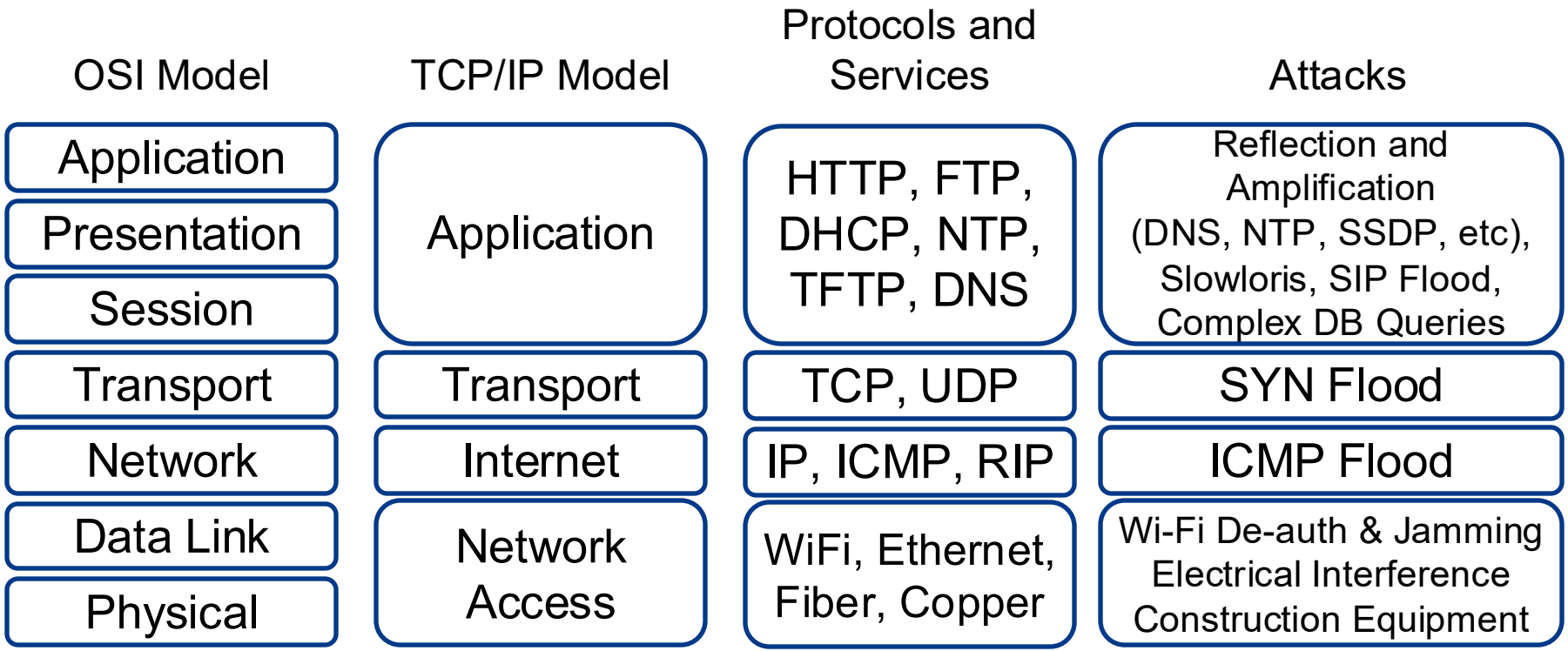
https://stats.labs.apnic.net/rpki/XT?o=cXDw7v0p1x0l1

RPKI – What do I need to do

- ROA
  - Sign your Routes
  - Make sure your ROA's 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

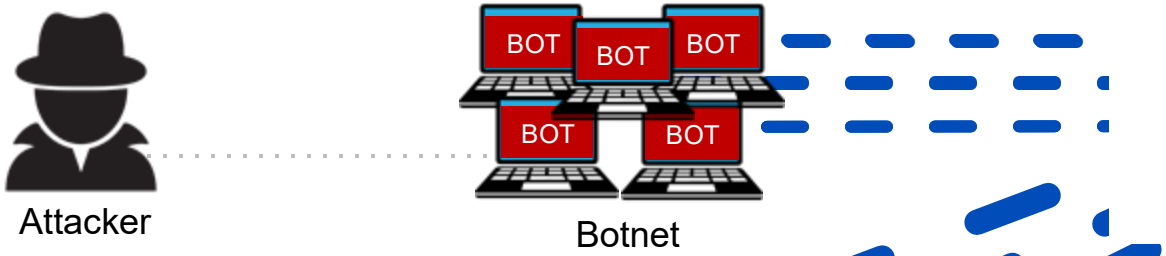


* Colour animated slide

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"



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

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

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

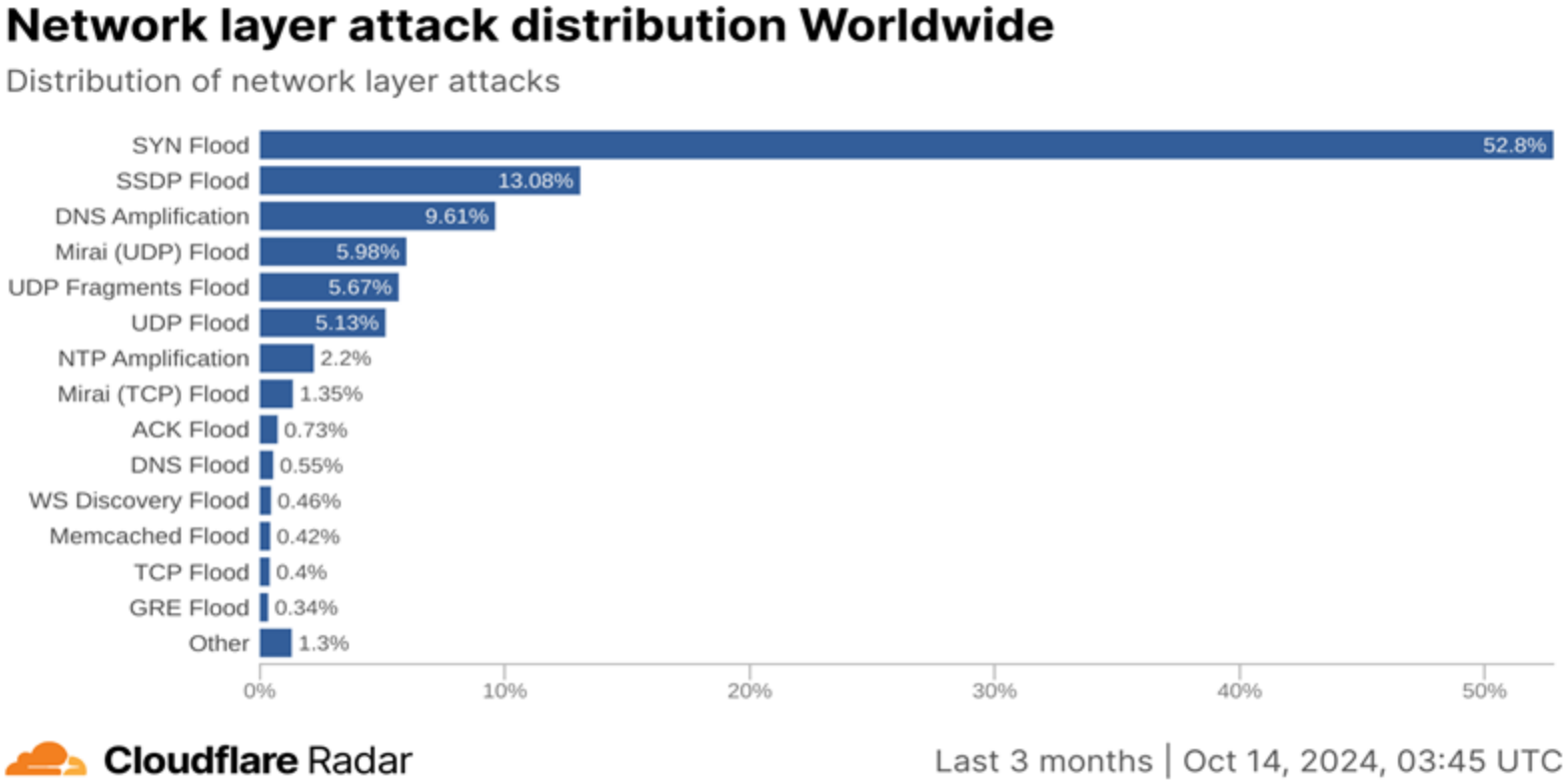
- Most data sourced from
  - Cloudflare Radar
  - Shodan.io
  - Cybergreen.net

- Top 5 Countries DDoS Sources

October 2023	April 2024	July 2024	October 2024
USA - 31% **India – 9.2%** Germany – 5.4% Brazil – 5.2% **China – 3.3%**	USA – 22.6% Germany – 6.5% **China - 5.5%** **Indonesia – 4.7%** Brazil – 4.3%	USA – 18.8% Germany – 8.45% **China = 7.49** **Pakistan – 5.9%** UK – 4.5%	USA - 20.34% Germany - 7.57% Ireland - 5.8% Brazil - 4.99% **Pakistan - 4.35%**

https://radar.cloudflare.com/security-and-attacks?dateRange=12w

Global Numbers



https://radar.cloudflare.com/security-and-attacks

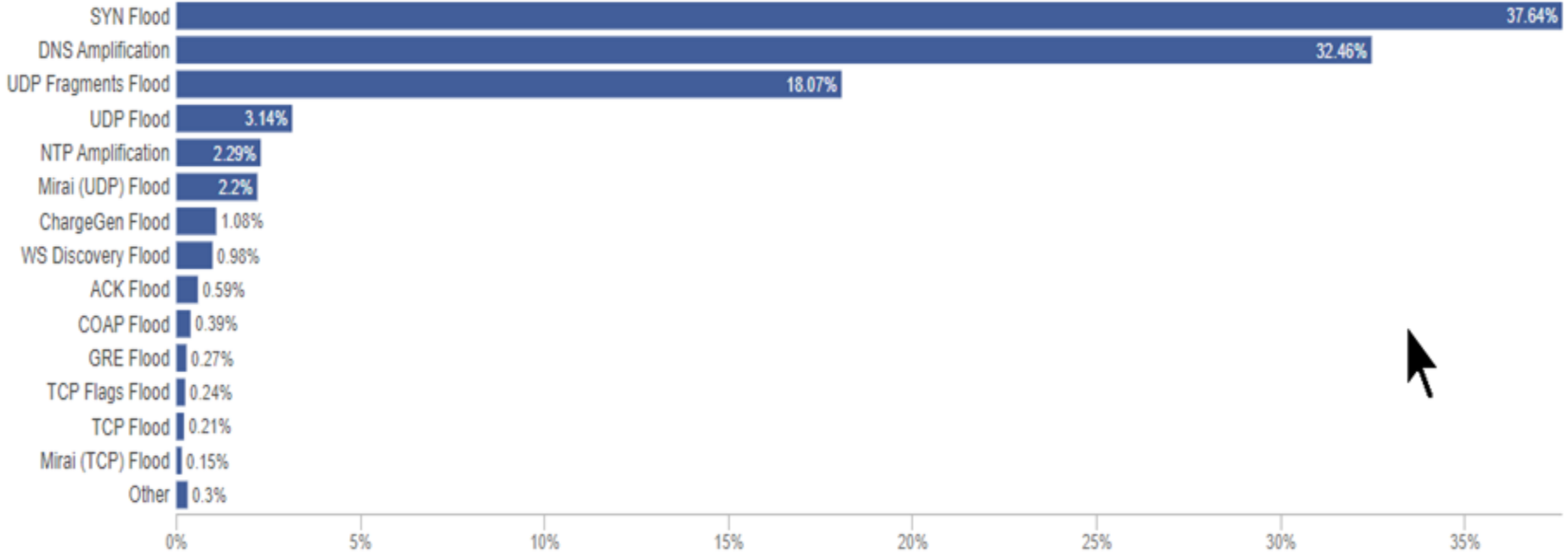
Pakistan

#	Network	Percentage
1	AS136384 - OPTIX-AS-AP Optix Pakistan Pvt. Limited	**83.90%**
2	AS9541 - CYBERNET-AP Cyber Internet Services Pvt Ltd.	2.10%
3	AS17557 - PKTELECOM-AS-PK Pakistan Telecommunication Company Limited	2.00%
4	AS9260 - MULTINET-AS-AP Multinet Pakistan Pvt. Ltd.	1.70%
5	AS136969 - KKNETWROK-AS-AP KK Networks Pvt Ltd.	1.20%

https://radar.cloudflare.com/security-and-attacks/pk?dateRange=12w

Pakistan

Attack Types



https://radar.cloudflare.com/security-and-attacks/pk?dateRange=12w

Pakistan

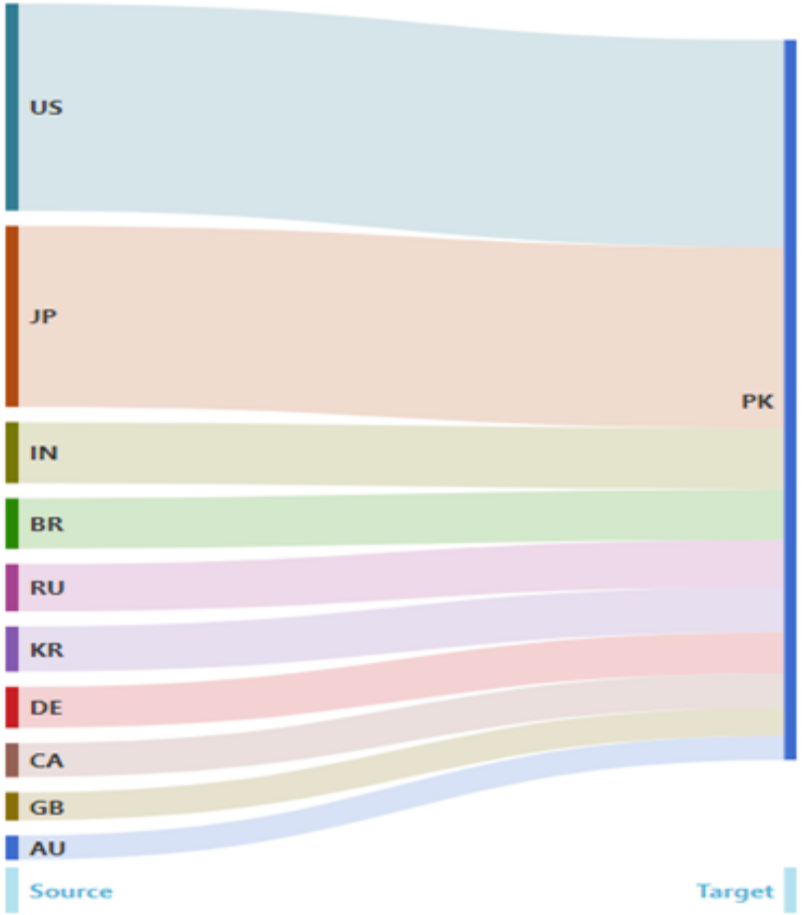
- Open Ports

DNS	139,682
NTP	14,674
SSDP	147
MemcacheD	25
Telnet	103,634
SNMP	5,000
Winbox	6,772

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

Pakistan

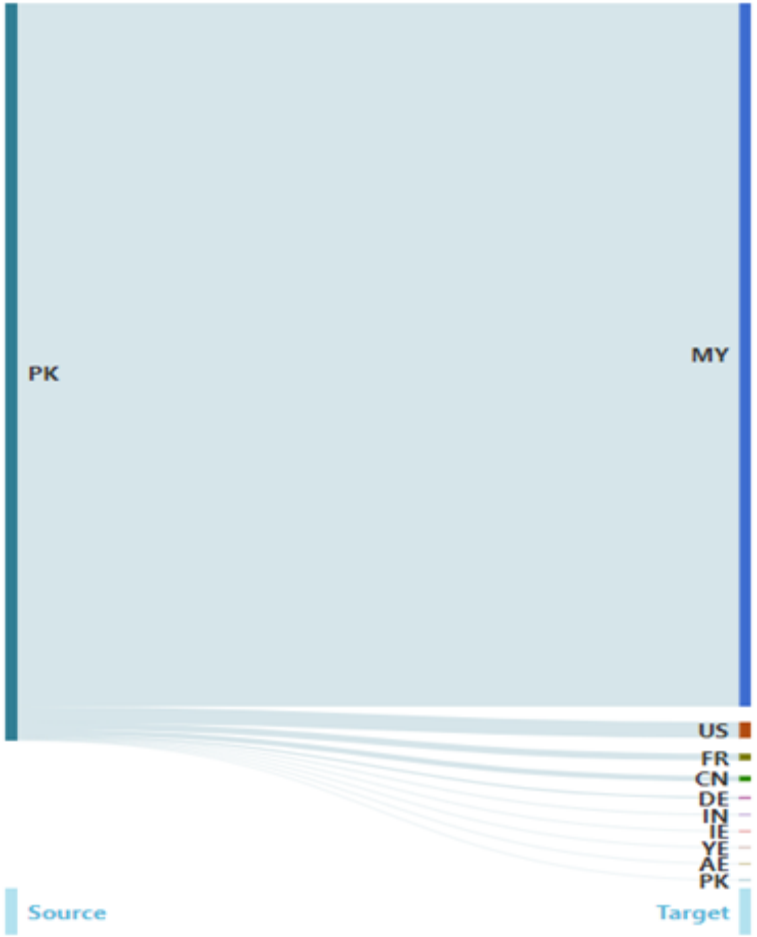
- Targets



https://radar.cloudflare.com/security-and-attacks/pk?dateRange=12w

Pakistan

- Targets



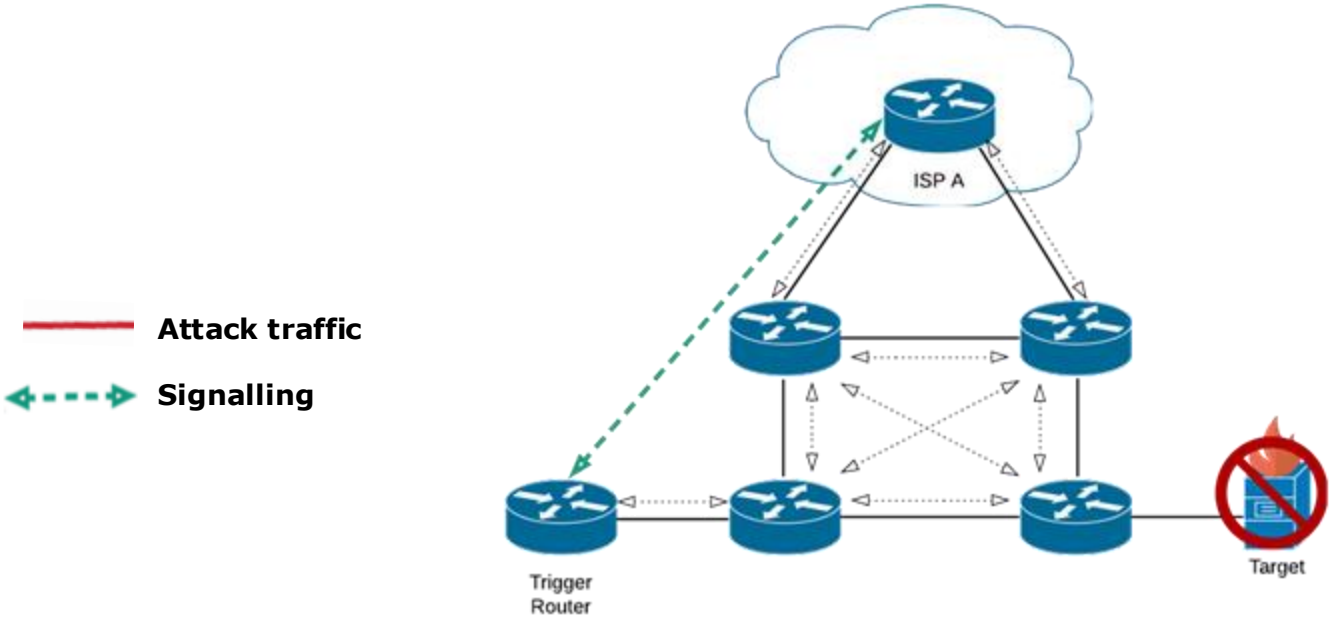
https://radar.cloudflare.com/security-and-attacks/pk?dateRange=12w

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

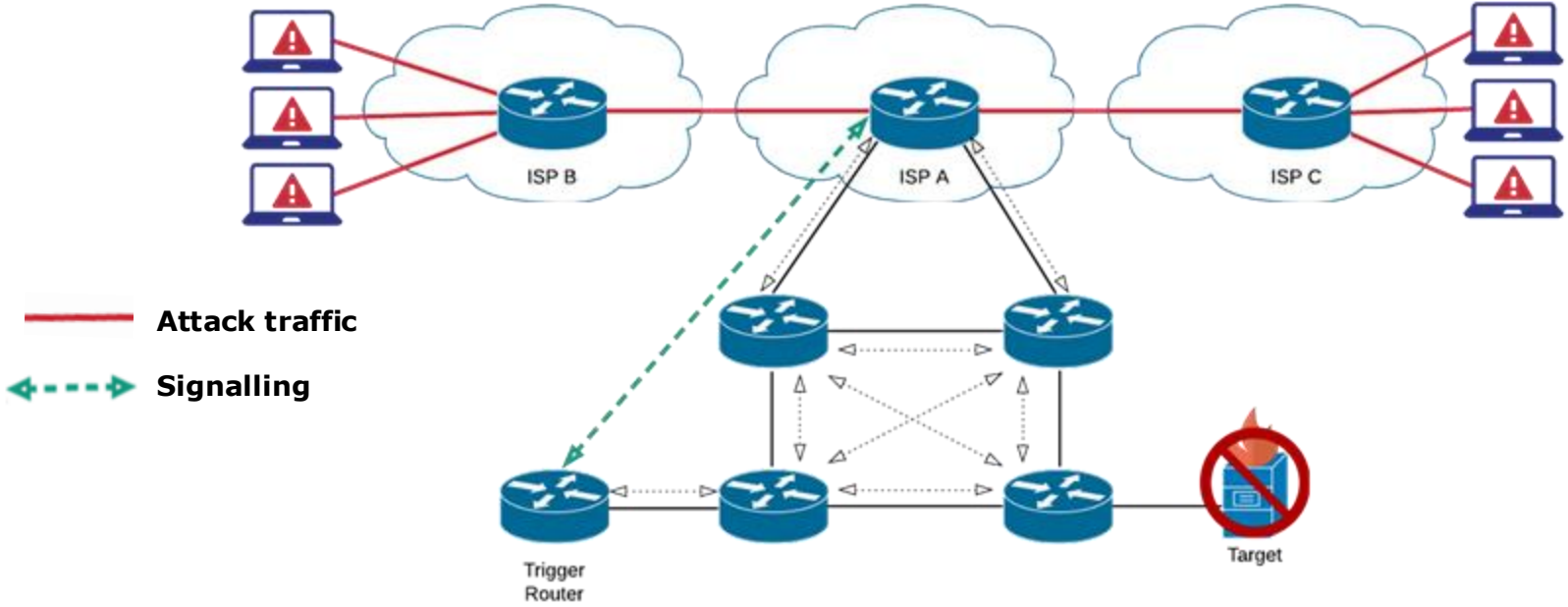
Mitigation Strategies

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



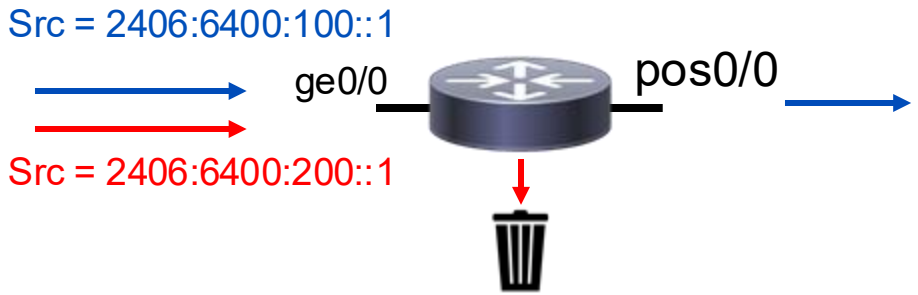
Mitigation Strategies

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

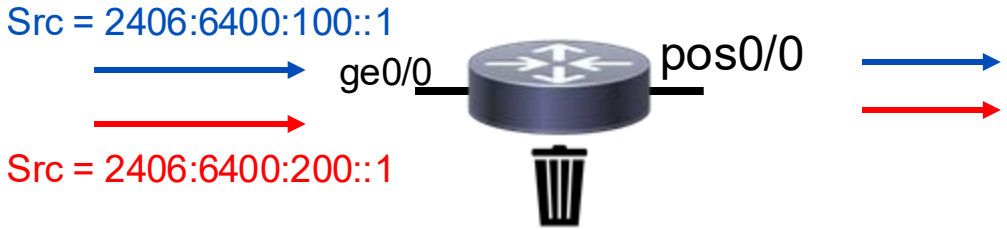


Mitigation Strategies

- 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?