# 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
  - 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)

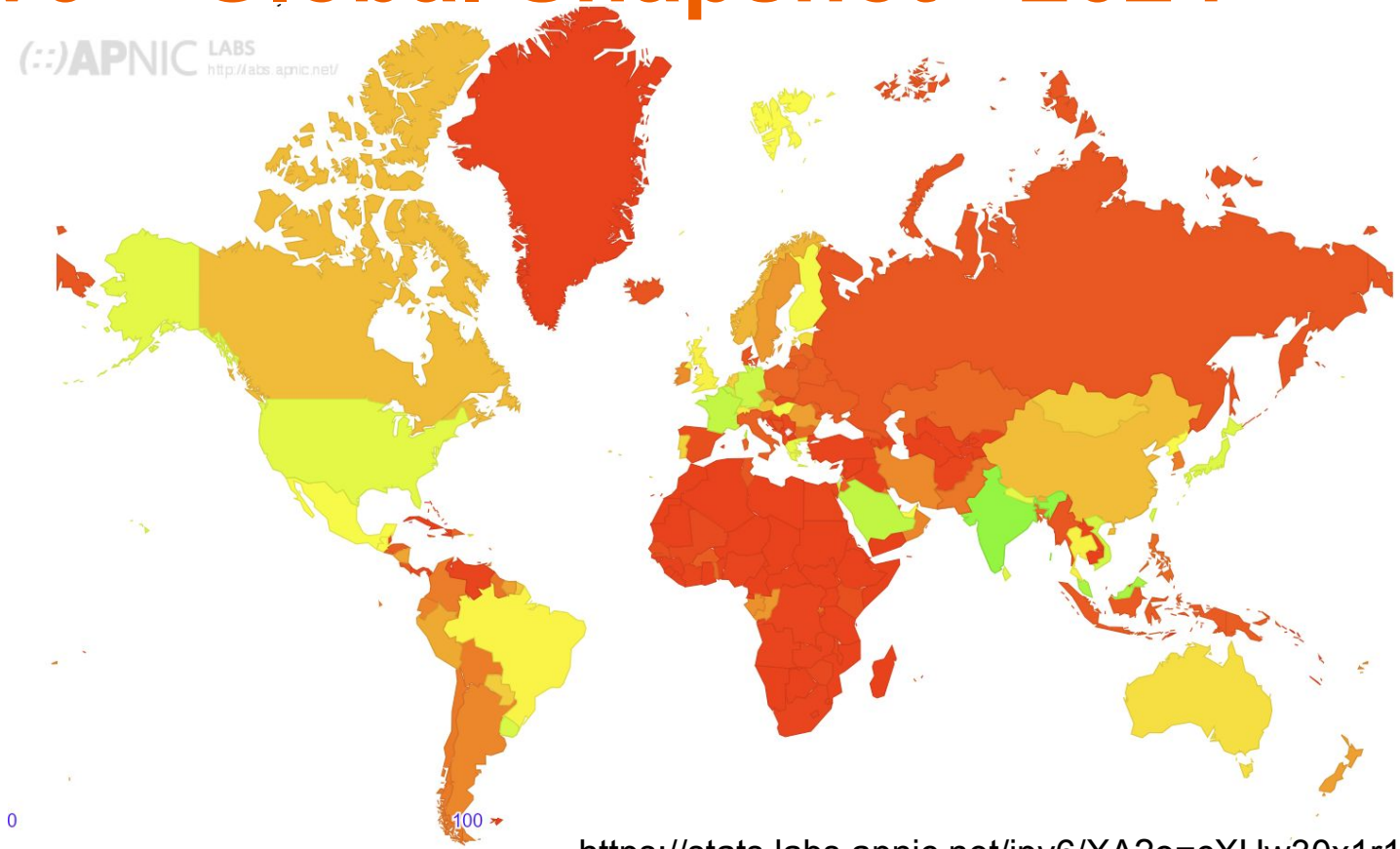
# Why do we care about the numbers?

- 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

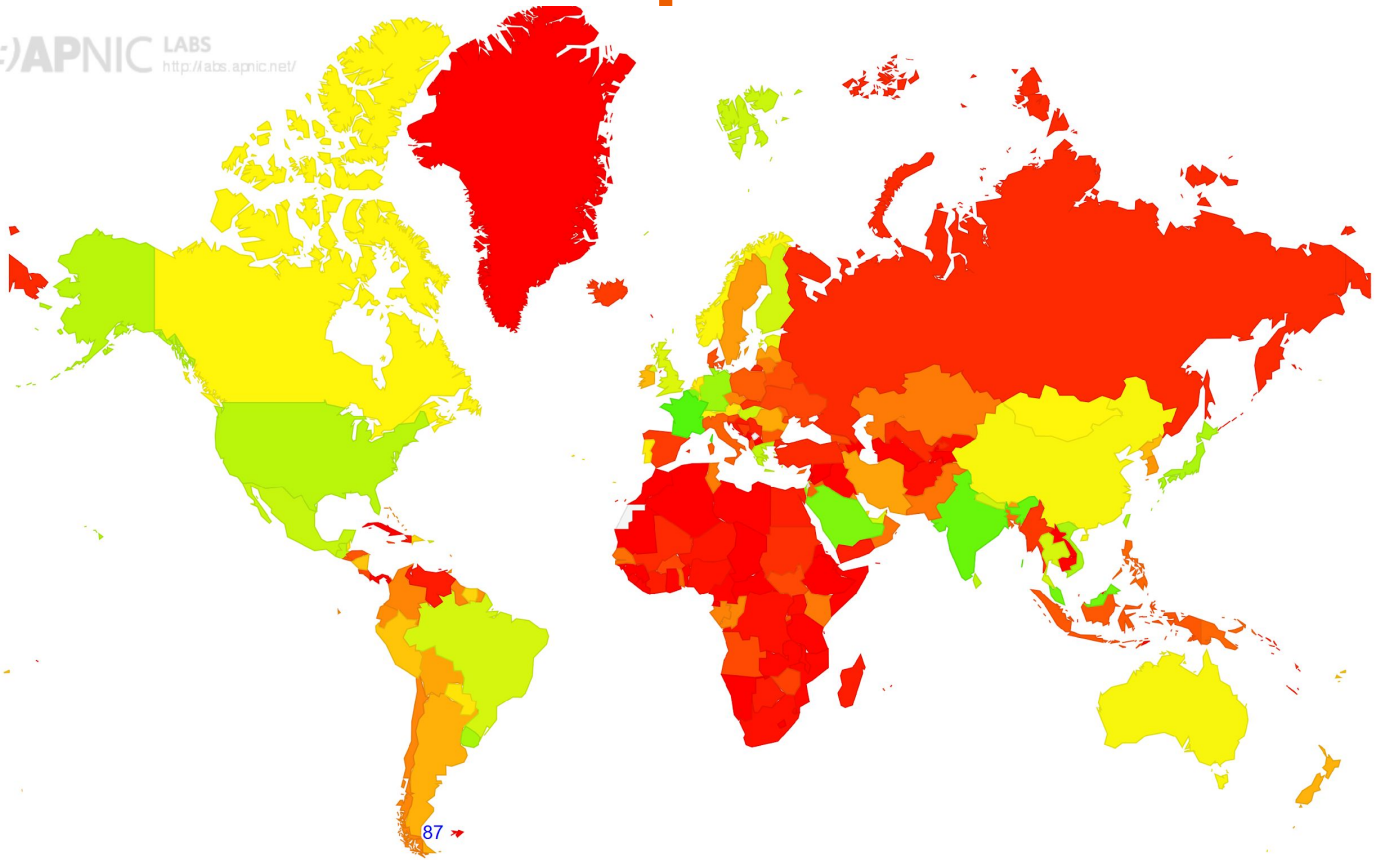
- Data for this presentation have come from numerous sources
  - https://stats.labs.apnic.net
  - https://radar.cloudflare.com
  - https://shodan.io
  - My own collection of stats

# IPv6 – Global Snapshot - 2024



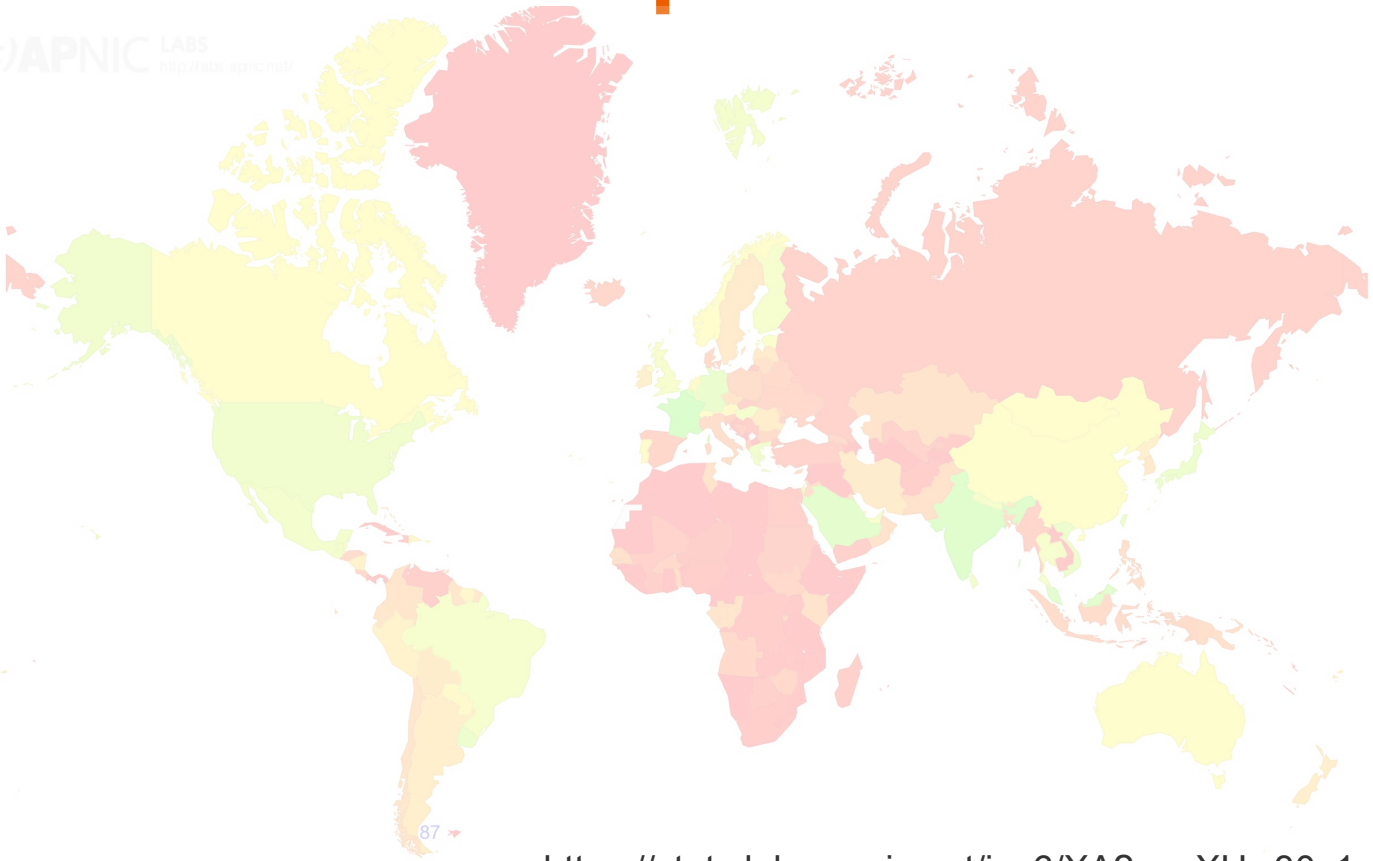

https://stats.labs.apnic.net/ipv6/XA?o=cXUw30x1r1

# IPv6 – Global Snapshot - 2025




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

# IPv6 – Global Snapshot - 2025



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

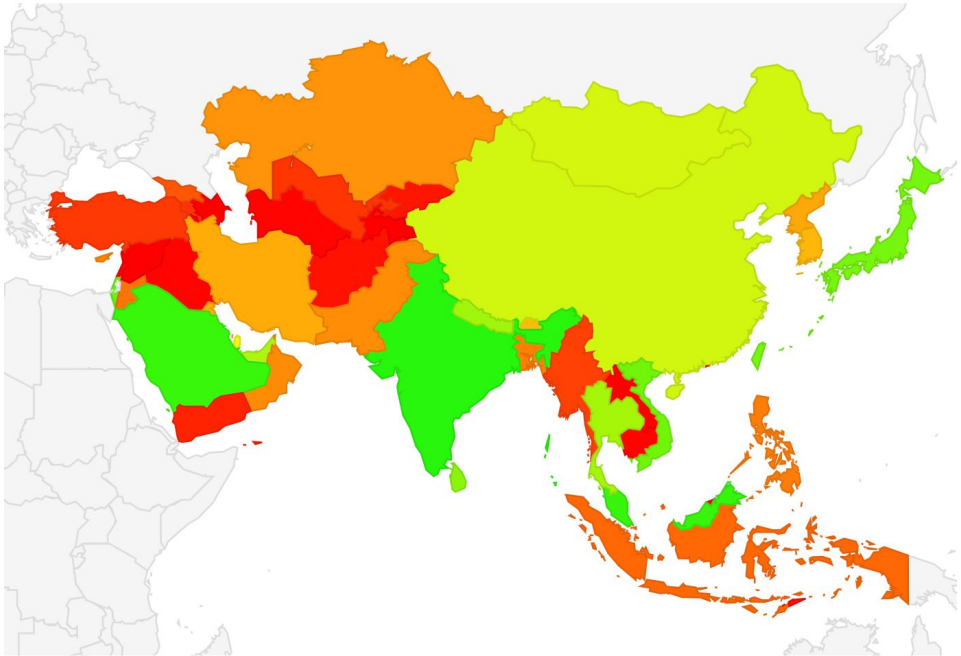
# IPv6 – Global Snapshot

- Global Preference 38% (2024 – 38%)
- Asia 43.4% (2024 - 43.14%)
- North America 46.8% (2024 - 53%)
- South America 38.6% (2024 - 36%)
- Europe 31.1% (2024 - 30%)
- Africa 3.8% (2024 - 2.4%)
- Oceania 35.4% (2024 - 35.8%)

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

# IPv6 – Asia Sub-Region

- 3 Sub-regions
  - 57.7% South Asia
    - IN,LK,NP,BT,PK,BD,AF,MV
  - 45.2% 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



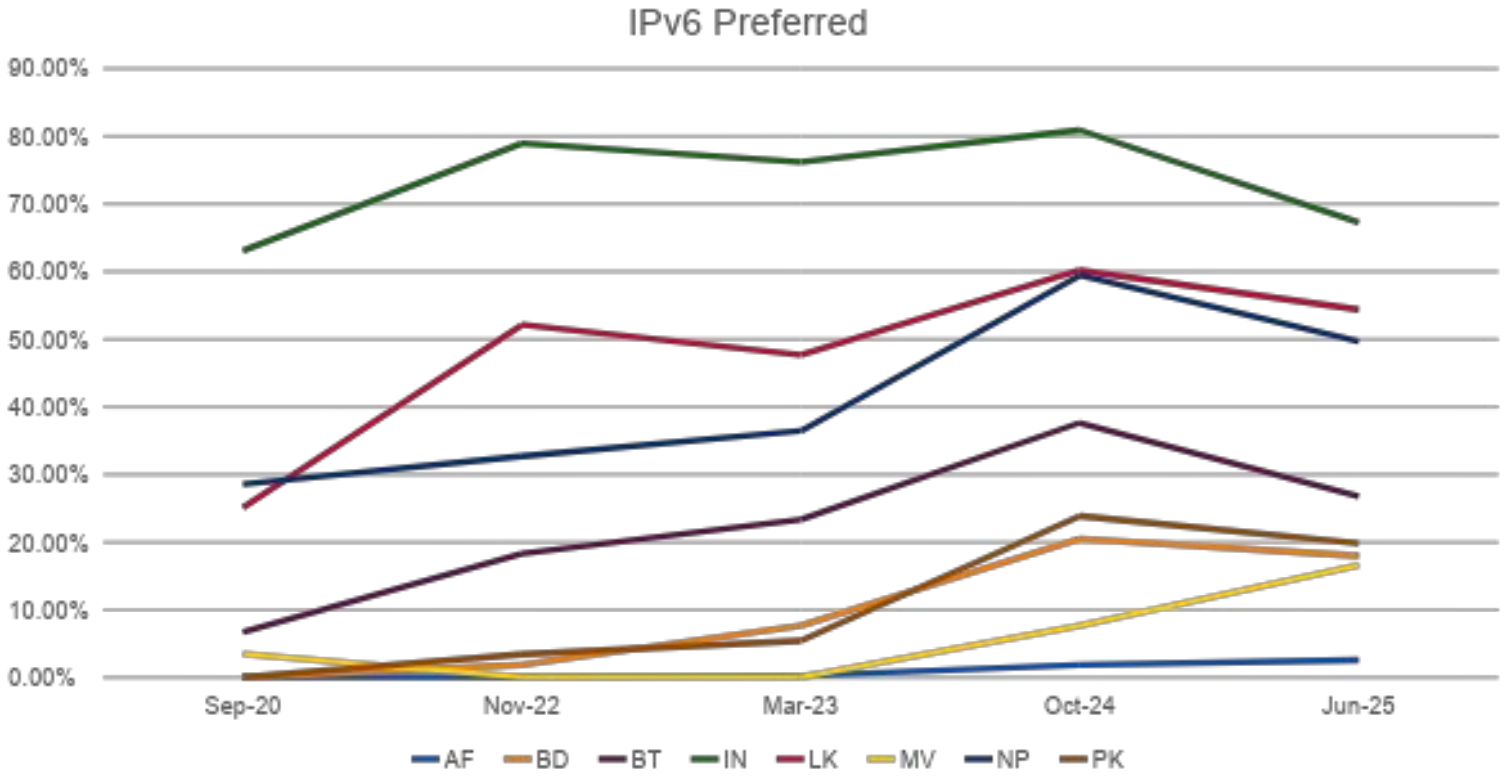
https://stats.labs.apnic.net/ipv6/XD?o=cXAw30x1r1

# IPv6 – South Asia Sub-Region

| CC | Country | 2020-09 | 2022-11 | 202303 | 202411 | 202506 |
|---|---|---|---|---|---|---|
| AF | Afghanistan | 0.11% | 0.06% | 0.23% | 1.85% | 2.60% |
| BD | Bangladesh | 0.03% | 1.87% | 7.68% | 20.49% | 17.99% |
| BT | Bhutan | 6.72% | 18.35% | 23.35% | 37.65% | 26.77% |
| IN | India | 63.07% | 78.96% | 76.19% | 80.91% | 67.23% |
| LK | Sri Lanka | 25.10% | 52.14% | 47.67% | 60.19% | 54.38% |
| MV | Maldives | 3.51% | 0.08% | 0.07% | 7.67% | 16.62% |
| **NP** | **Nepal** | **28.60%** | **32.71%** | **36.44%** | **59.43%** | **49.70%** |
| PK | Pakistan | 0.03% | 3.44% | 5.44% | 23.87% | 19.82% |

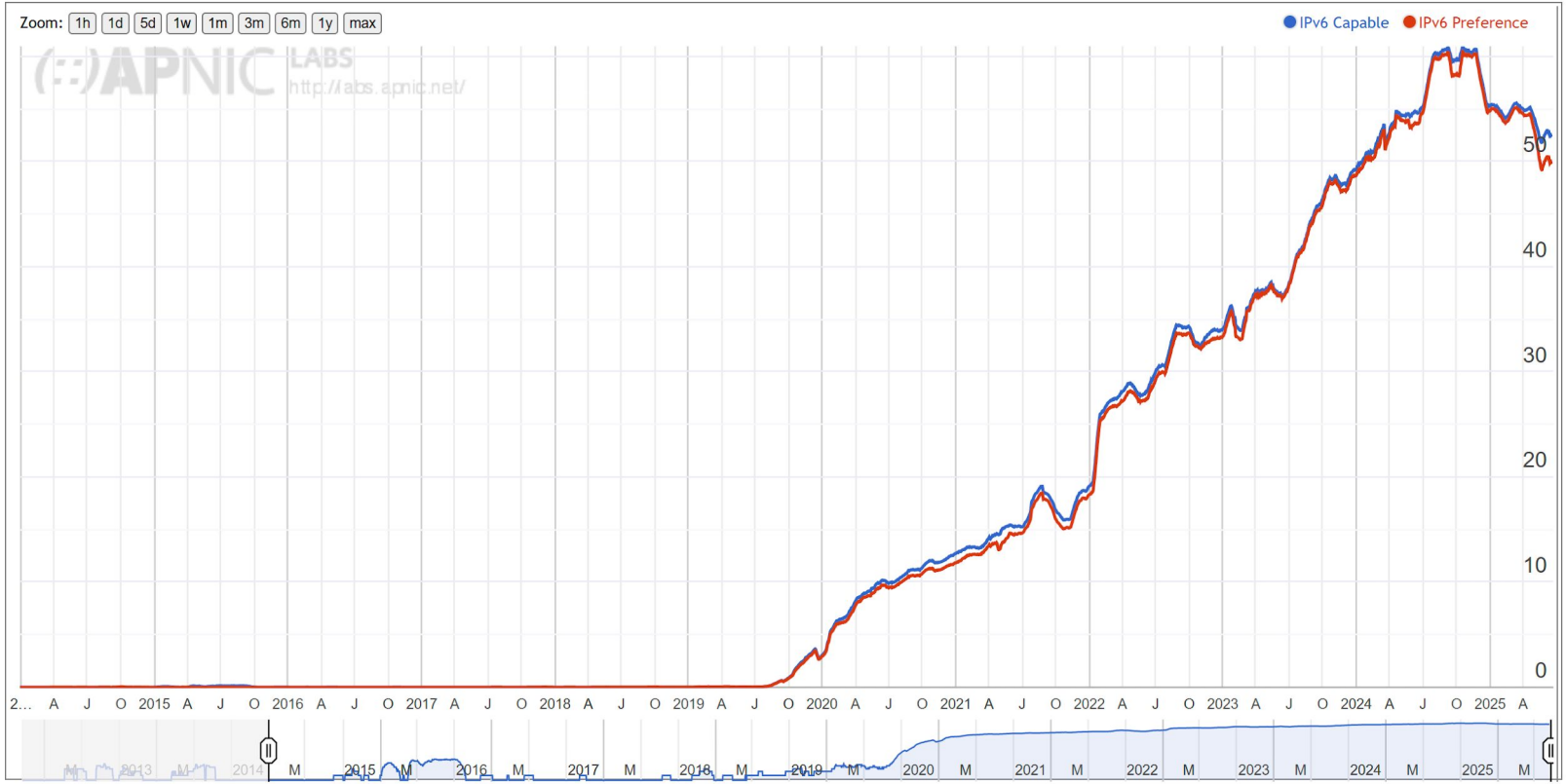
https://stats.labs.apnic.net/ipv6/XD?o=cXAw30x1r1

# IPv6 – South Asia Sub-Region




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

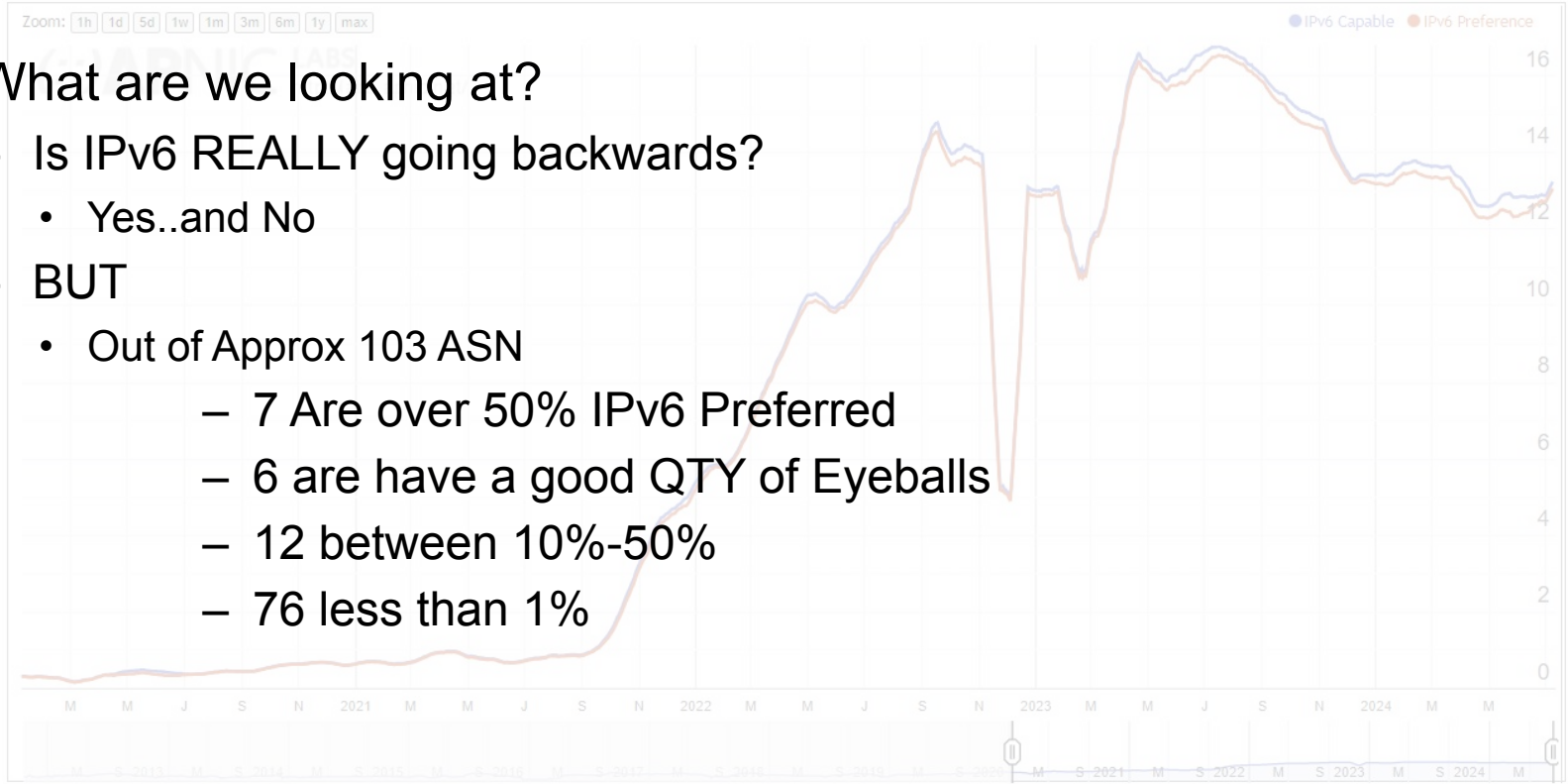
# IPv6 – Nepal




https://stats.labs.apnic.net/ipv6/NP?o=cXTw30x1r1

# IPv6 – Nepal

- What are we looking at?
  - Is IPv6 REALLY going backwards?
    - Yes..and No
  - BUT
    - Out of Approx 103 ASN
      - 7 Are over 50% IPv6 Preferred
      - 6 are have a good QTY of Eyeballs
      - 12 between 10%-50%
      - 76 less than 1%




https://stats.labs.apnic.net/ipv6/AS17501?c=NP&p=1&v=1&w=30&x=1

# 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

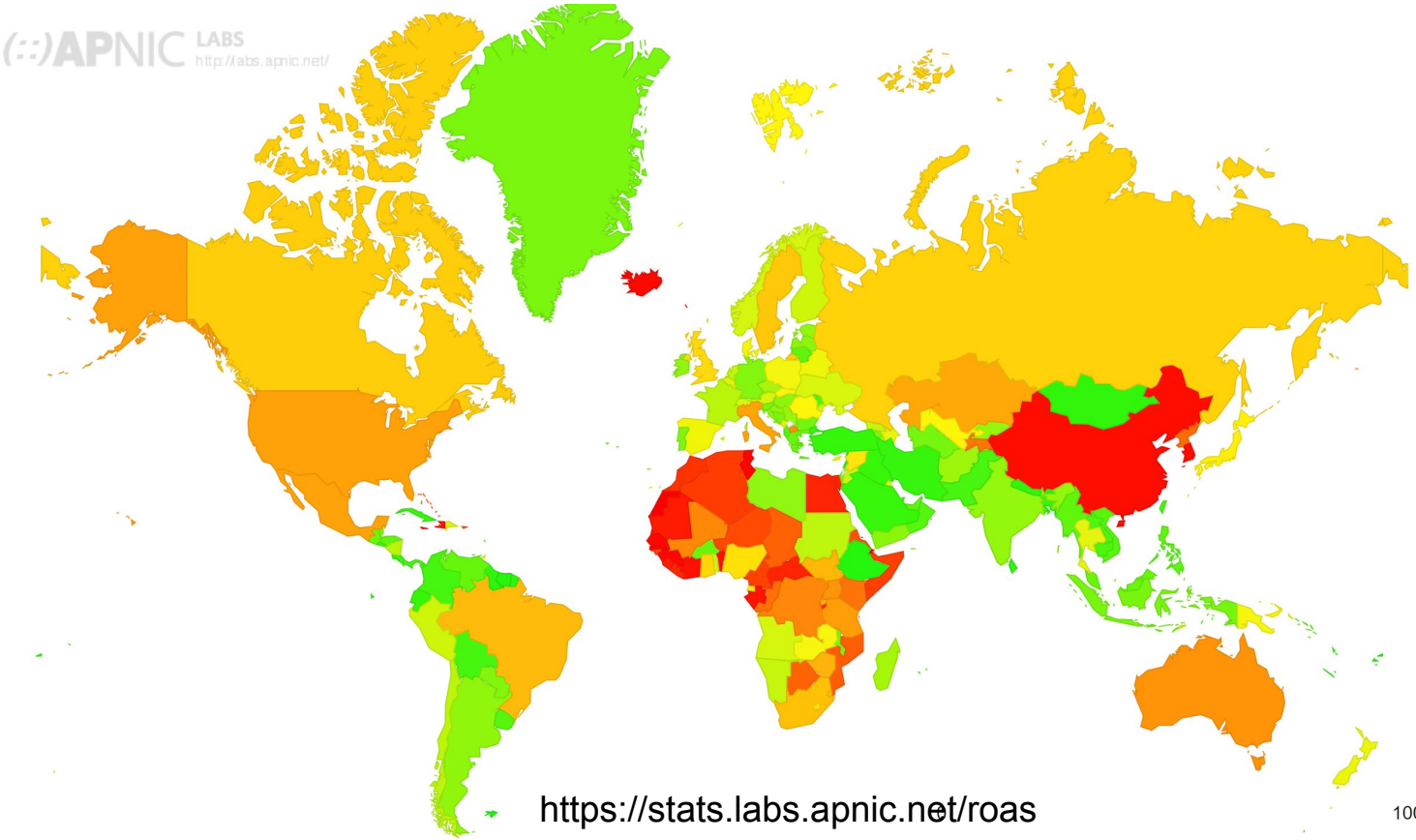

- The world is changing
  - 3 x increase/5 years
  - Hyperscalers are catching up
  - CDN Providers are ready for your IPv6 Packets
  - IPv6 Tipped over the 50% mark in Asia this year

# IPv6 Deployment

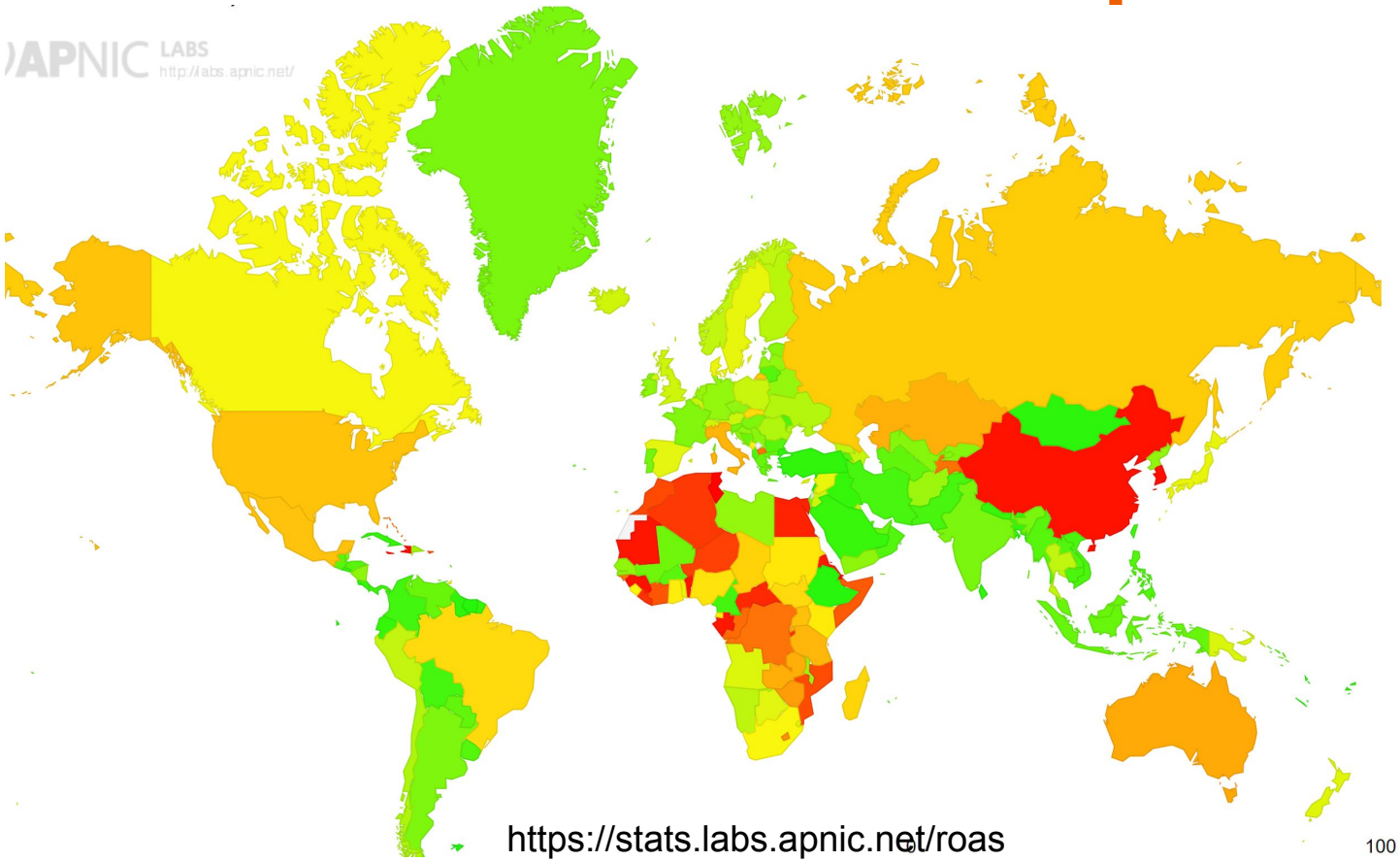
- Stop saying “I’ll do it tomorrow”
  - We have been saying that for 25 years
- Networks are not going to get simpler
- Grants Are available
  - https://isif.asia/infrastructure-ipv6/
    - US$30-250K
    - Open to all Industry types
- Need practical help?
  - Training: https://academy.apnic.net/
  -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

# RPKI

# RPKI ROA – 2024 Global Snapshot



# RPKI ROA – 2025 Global Snapshot



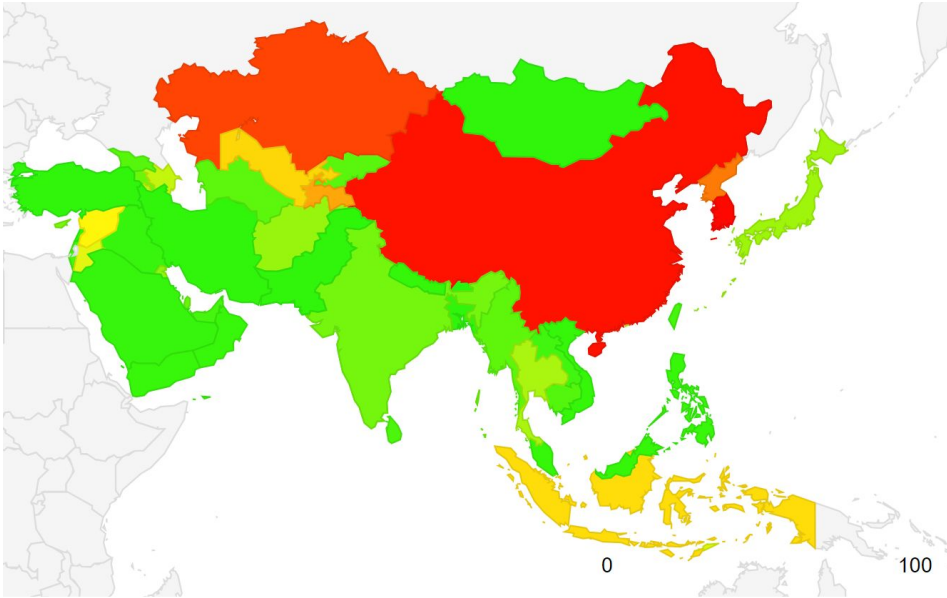
# RPKI ROA – Global Snapshot

- Global IPv4 Signed 54% (2024 - 47.8%)
- Asia 62.1% (2024 - 57.9%)
- North America 43.2 (2024 - 34.6%)
- South America 58.9 (2024 - 54.2%)
- Europe 61.4% (2024 - 53.7%)
- Africa 36.5% (2024 - 29.7%)
- Oceania 71.1% (2024 - 69.4%)

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

# RPKI ROA – Asia Subregion

- 3 Sub-regions
  - 88.8% South Asia
    - IN,LK,NP,BT,PK,BD,AF,MV
  - 29.7% East Asia
    - TW,JP,MN,CN,MO,KR,HK,KP
  - 83.3% South-East Asia
    - MY,VN,TH,SG,PH,ID,MM,LA,BN,KH,TL



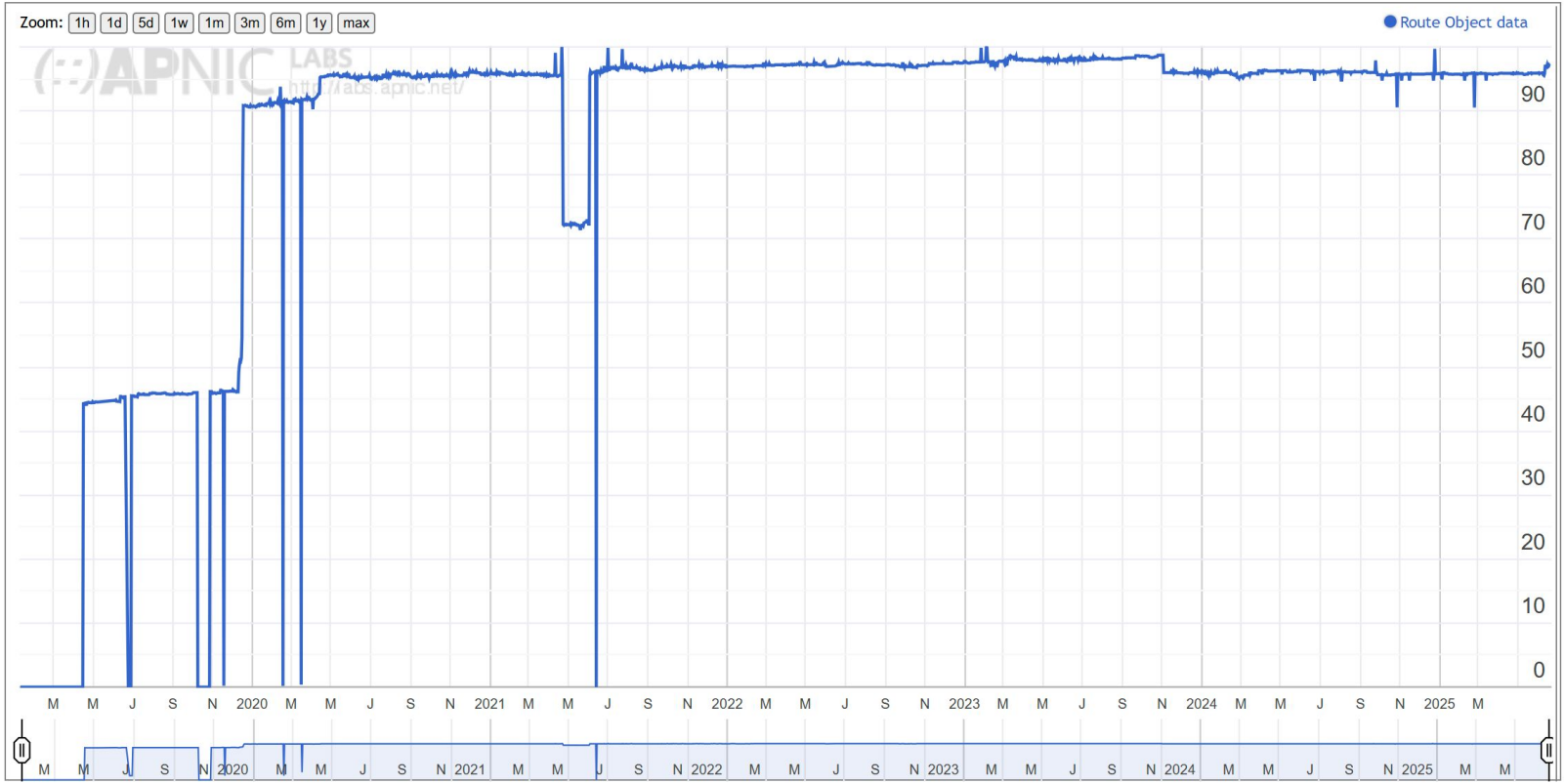

https://stats.labs.apnic.net/roa/XD

# RPKI ROA – South Asia Subregion

| Code | Region | V4 Valid | Pc | V4 Invalid | Pc | V4 Unknwn | Pc | V4 Total Addrs | PoT |
|---|---|---|---|---|---|---|---|---|---|
| AF | Afghanistan | 111360 | 73.4% | 768 | 0.5% | 39680 | 26.1% | 151808 | 0.28% |
| BD | Bangladesh | 1866919 | 98.4% | 4441 | 0.2% | 26368 | 1.4% | 1897728 | 3.51% |
| BT | Bhutan | 44544 | 98.3% | 0 | 0.0% | 768 | 1.7% | 45312 | 0.08% |
| IN | India | 38537323 | 85.0% | 167829 | 0.4% | 6616577 | 14.6% | 45321729 | 83.94% |
| LK | Sri Lanka | 538624 | 91.2% | 256 | 0.0% | 51456 | 8.7% | 590336 | 1.09% |
| MV | Maldives | 93184 | 98.6% | 0 | 0.0% | 1280 | 1.4% | 94464 | 0.17% |
| **NP** | **Nepal** | **569088** | **97.4%** | **0** | **0.0%** | **15104** | **2.6%** | **584192** | **1.08%** |
| PK | Pakistan | 5160654 | 97.3% | 6963 | 0.1% | 138496 | 2.6% | 5306113 | 9.83% |

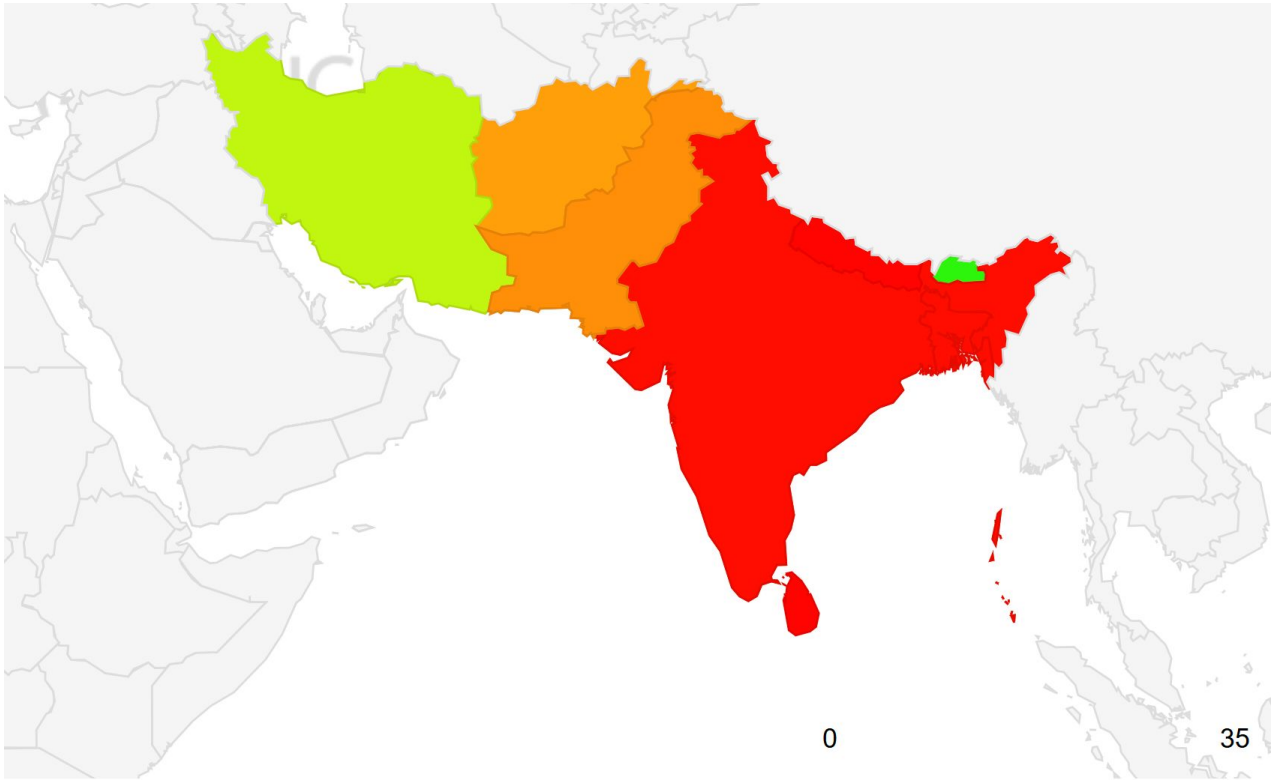
https://stats.labs.apnic.net/roa/NP

# RPKI ROA – Nepal




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

# RPKI ROV – South Asia




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

# RPKI ROV – South-East Asia

| Code | Region | RPKI Validates |
|---|---|---|
| AF | Afghanistan | 11.38% |
| BD | Bangladesh | 0.77% |
| BT | Bhutan | 34.49% |
| IN | India | 0.95% |
| LK | Sri Lanka | 0.32% |
| MV | Maldives | 0.28% |
| NP | Nepal | 0.38% |
| PK | Pakistan | 10.14% |

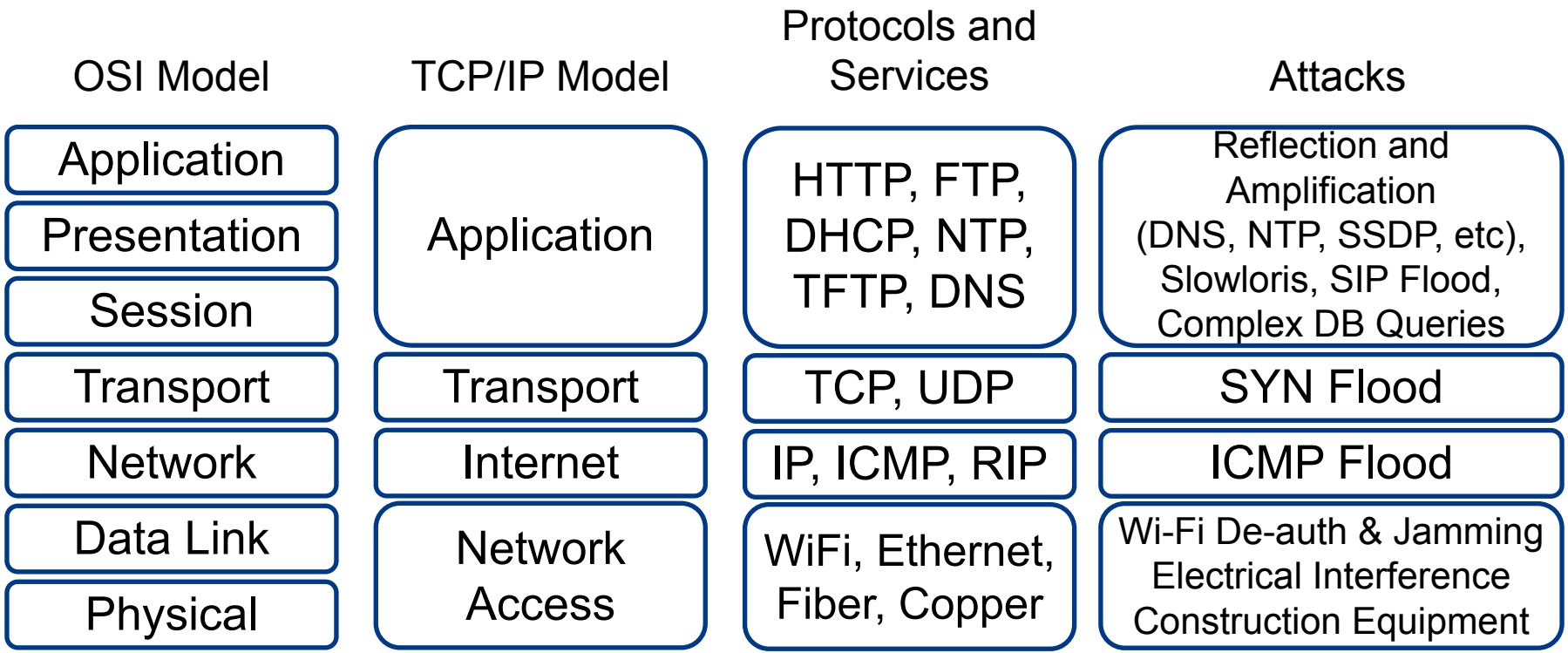
https://stats.labs.apnic.net/rpki/XU?o=cXDw7v0p1x0l1

# RPKI – What do I need to do

- ROA
  - Sign your Routes (APNIC Portal)
  - 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

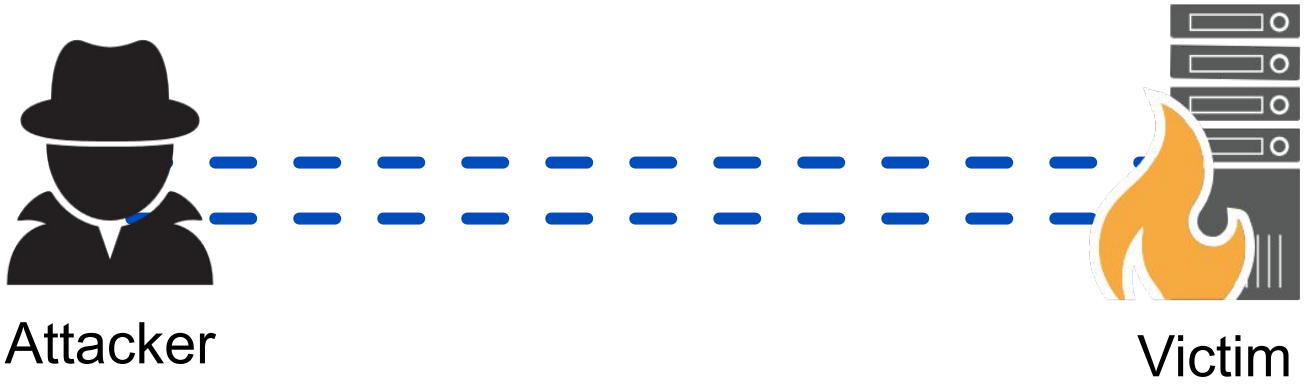
# DoS by Layers




* Colour animated slide

# Simple DoS

1 Attacker sends any valid or invalid traffic to the victim

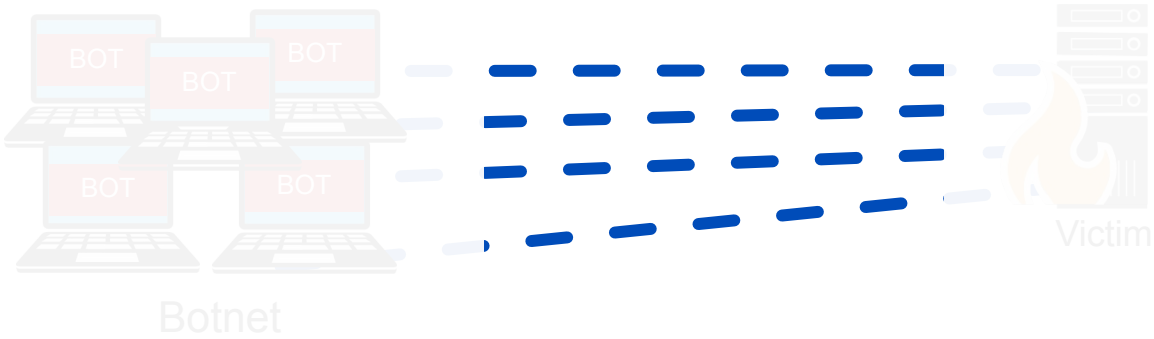


# Simple DDoS

1 Attacker directs bots to begin attack

2 All bots send any valid or invalid traffic to the victim

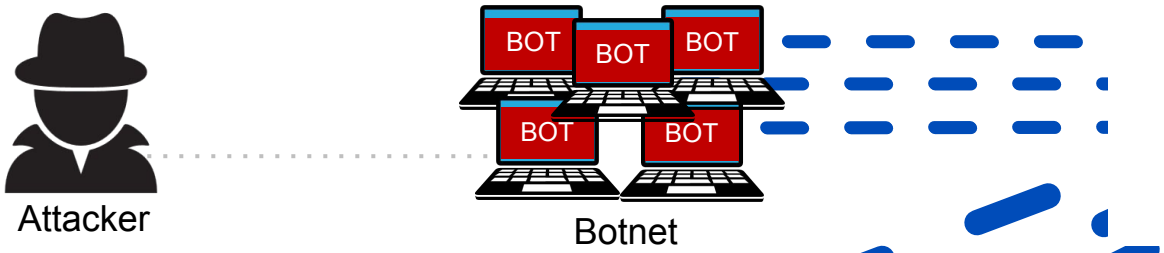
Attacker



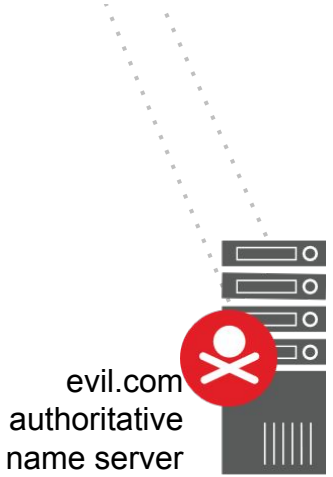
# Reflected and Amplified DDoS

**1** Attacker directs bots to begin attack

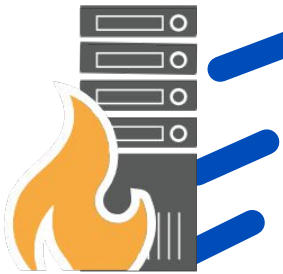
**2** All bots send DNS queries for the TXT record in domain “evil.com” to open recursive DNS servers and fake "my IP is 10.10.1.1"




**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….)

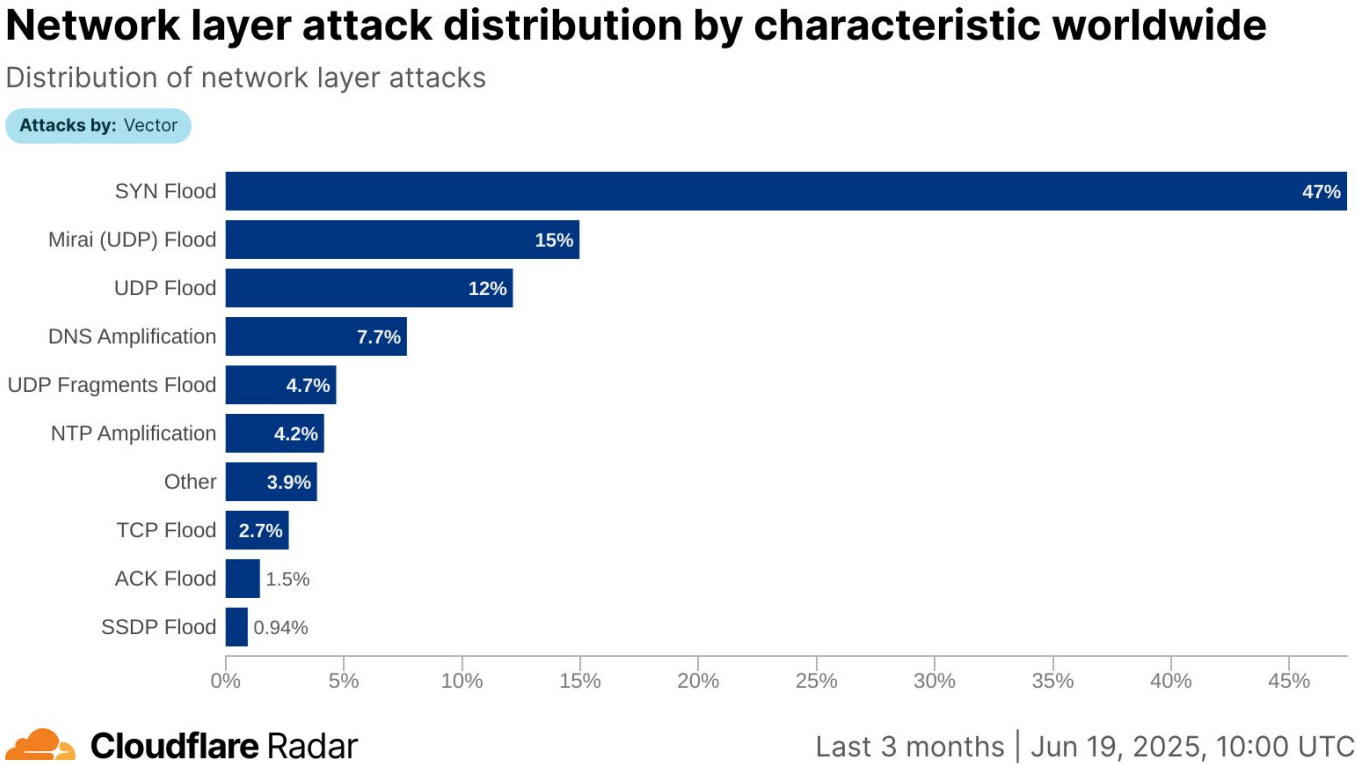
# Global Numbers

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

| APRIL 2024 | July 2024 | June 2025 |
|---|---|---|
| USA – 22.6% | USA – 18.8% | USA - 20.1% |
| Germany – 6.5% | Germany – 8.45% | **Hong Kong - 6.7%** |
| **China - 5.5%** | **China = 7.49** | Brazil - 4.8% |
| **Indonesia – 4.7%** | **Pakistan – 5.9%** | **Japan - 4.6%** |
| Brazil – 4.3% | UK – 4.5% | Germany 4.2% |

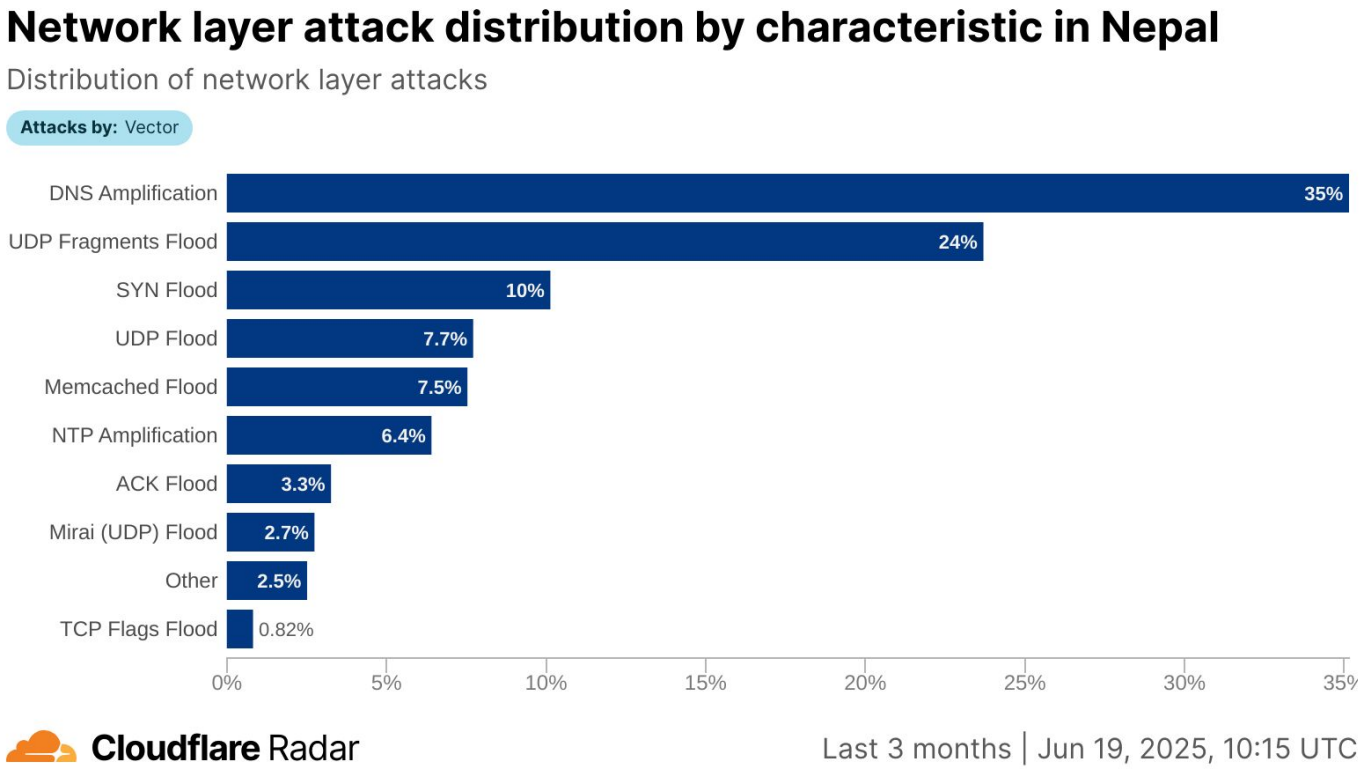
https://radar.cloudflare.com/security-and-attacks

# Global Numbers




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

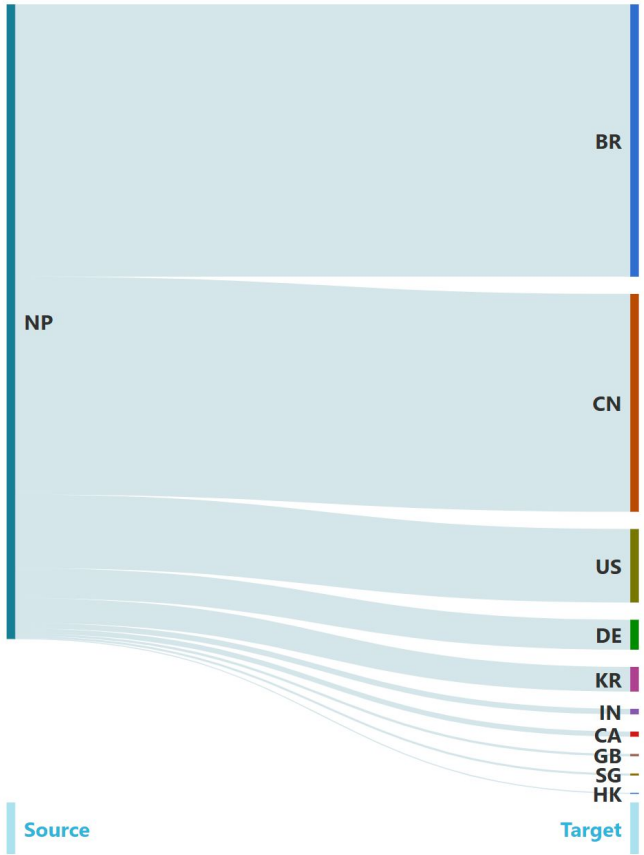
# Nepal




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

# Nepal

- Targets




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

# Indonesia

- Open Ports

| | |
|---|---|
| DNS | 934 |
| NTP | 4,151 |
| SSDP | 9 |
| MemcacheD | 11 |
| Telnet | 830 |
| SNMP | 889 |
| Winbox | 3,117 |

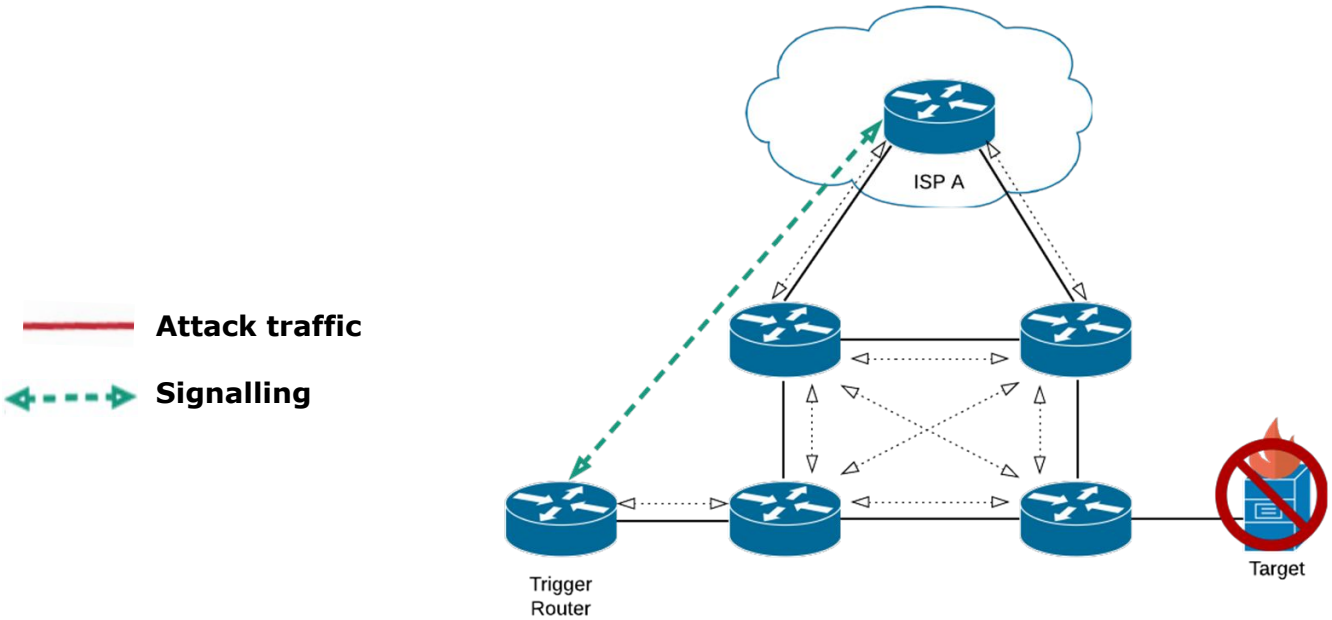
https://www.shodan.io/search?query=country%3Anp

# 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

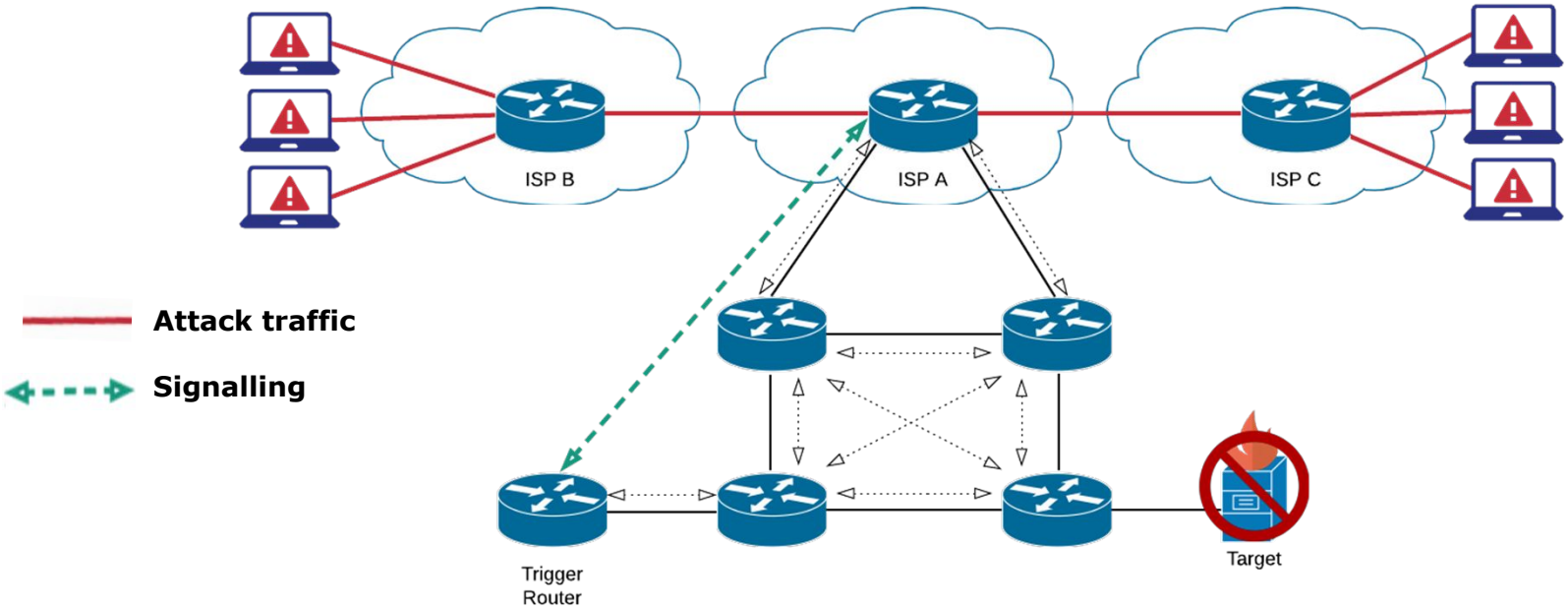
# Mitigation Strategies

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



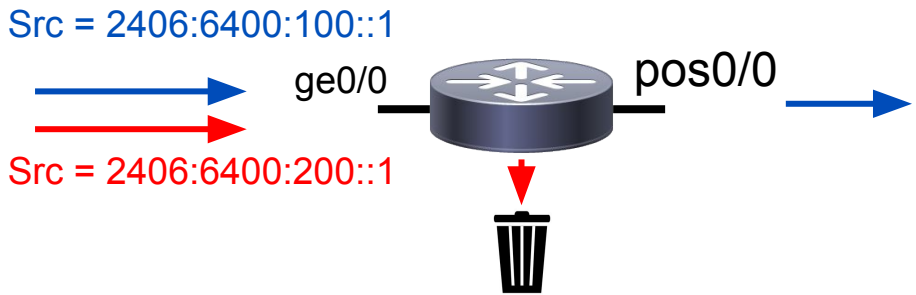
# Mitigation Strategies

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



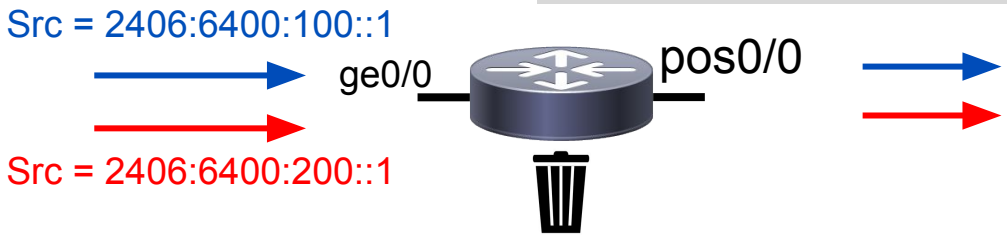
# Mitigation Strategies

- uRPF
  - Strict: verifies both source address and incoming interface with entries in the forwarding table




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

  - Loose: verifies existence of route to source address



# 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?