DNS RESEARCH FEDERATION

RPKI adoption and Routing Security in the ARIN region

Carolina Caeiro and Mark McFadden

About the Project

- Produced with support from ARIN Community Grant Program
- Goals:
  - Showcase data on RPKI adoption and routing incidents in the ARIN region
  - Encourage greater academic and industry scrutiny over routing security practices
- Value added:
  - Geographic data by country in ARIN region
  - Report with live indicators
  - Access to our data analytics platform to do your own analysis

DNS RESEARCH FEDERATION

About DNS Research Federation

- The DNSRF a new centre of excellence to advance the understanding of the Domain Name System's impact on cybersecurity, policy and technical standards
- A not for profit organisation based in the UK
- Areas of activity:
  - Education and research
  - Access to data
  - Engagement in technical standards

DNS RESEARCH FEDERATION

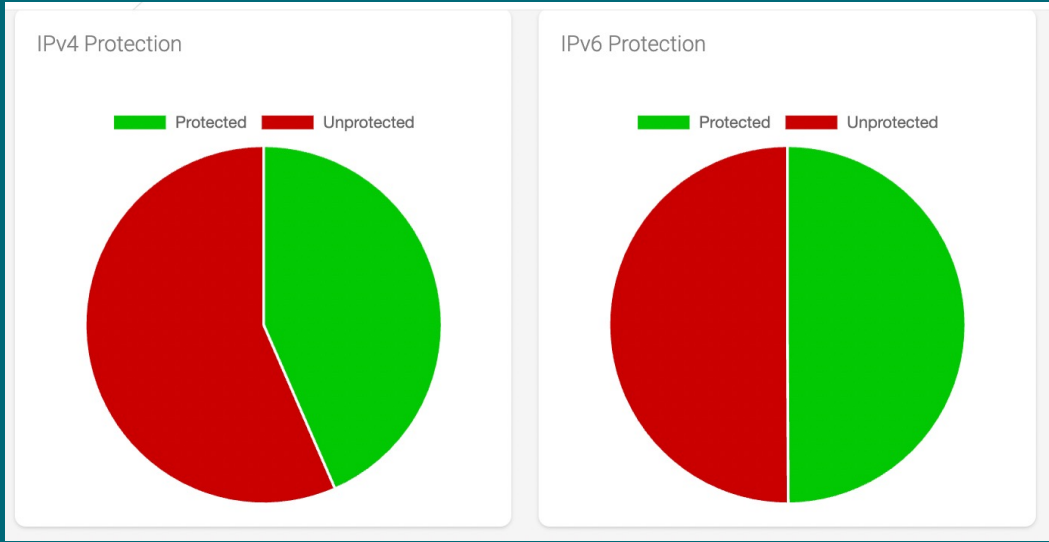
Today's Presentation

- ARIN in Context: Global/ARIN Adoption and Validation Results
- ARIN Deep Dive: Adoption and Validation Results Per Country and subregional trends.
- Invalids in the ARIN region
- Methodology
- Other ways of thinking of routing security? → RPKI adoption per IP address
- Next steps

ARIN in Context: Global Coverage

Global Coverage by % and number of Prefix-ASN Pairs

DERIVED TYPE	PROTECTED	UNPROTECTED
IPv4	43.44% 440255	56.56% 573215
IPv6	49.92% 100993	50.08% 101309



DNS RESEARCH FEDERATION

ARIN in Context: ARIN / Global Coverage

Global Coverage by % and number of Prefix-ASN Pairs

DERIVED TYPE	PROTECTED	UNPROTECTED
IPv4	43.44% 440255	56.56% 573215
IPv6	49.92% 100993	50.08% 101309

Global Coverage by RIR - IPv4

RIR	PROTECTED ↓	UNPROTECTED
arin	25.65% 75985	74.35% 220287

Global Coverage by RIR - IPv6

RIR	PROTECTED ↓	UNPROTECTED
arin	50.50% 17930	49.50% 17572

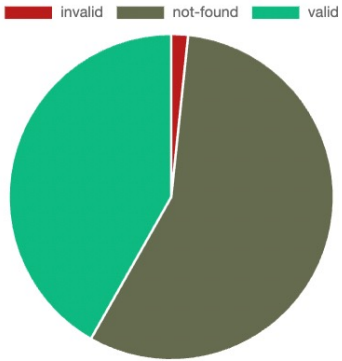
DNS RESEARCH FEDERATION

ARIN in Context: Global Validation Results

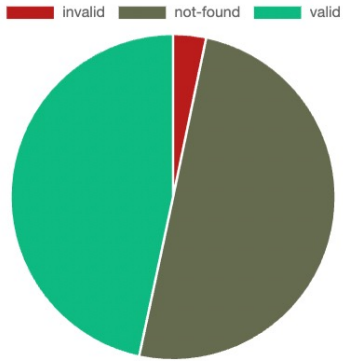
Global Validation Results and Prefix-ASN Pairs

DERIVED TYPE	VALID	INVALID	NOT FOUND
IPv4	41.77% 423357	1.67% 16898	56.56% 573215
IPv6	46.65% 94364	3.28% 6629	50.07% 101309

Global Validation Results - IPv4



Global Validation Results - IPv6



DNS RESEARCH FEDERATION

ARIN in Context: ARIN /Global Validation Results

Global Validation Results and Prefix-ASN Pairs

DERIVED TYPE	VALID	INVALID	NOT FOUND
IPv4	41.77% 423357	1.67% 16898	56.56% 573215
IPv6	46.65% 94364	3.28% 6629	50.07% 101309

Global Validation Results by RIR - IPv4

RIR	VALID ↓	INVALID	NOT FOUND
arin	23.97% 71012	1.68% 4973	74.35% 220287

Global Validation Results by RIR - IPv6

RIR	VALID ↓	INVALID	NOT FOUND
arin	47.33% 16802	3.18% 1128	49.49% 17572

DNS RESEARCH FEDERATION

ARIN Deep Dive - Results per country

2A: Coverage per Country

Ipv4 Protection

COUNTRY	NAME	PROTECTED	UNPROTECTED
VC	Saint Vincent and the Grenadines	95.83% - 23	4.17% - 1
GD	Grenada	68.00% - 17	32.00% - 8
KY	Cayman Islands	63.89% - 23	36.11% - 13
TC	Turks and Caicos Islands	51.72% - 15	48.28% - 14
KN	Saint Kitts and Nevis	50.00% - 6	50.00% - 6
VG	Virgin Islands (British)	41.60% - 104	58.40% - 146
GP	Guadeloupe	33.33% - 13	66.67% - 26
CA	Canada	31.12% - 7109	68.88% - 15737
US	United States of America	26.45% - 73764	73.55% - 205066
AG	Antigua and Barbuda	21.41% - 79	78.59% - 290

IPv6 Protection

COUNTRY	NAME	PROTECTED	UNPROTECTED
KN	Saint Kitts and Nevis	100.00% - 2	0.00% - 0
VC	Saint Vincent and the Grenadines	100.00% - 2	0.00% - 0
KY	Cayman Islands	80.00% - 16	20.00% - 4
GP	Guadeloupe	75.00% - 12	25.00% - 4
DM	Dominica	75.00% - 3	25.00% - 1
GD	Grenada	65.38% - 17	34.62% - 9
US	United States of America	56.27% - 22216	43.73% - 17263

2B: Validation results per Country

IPv4 Validity

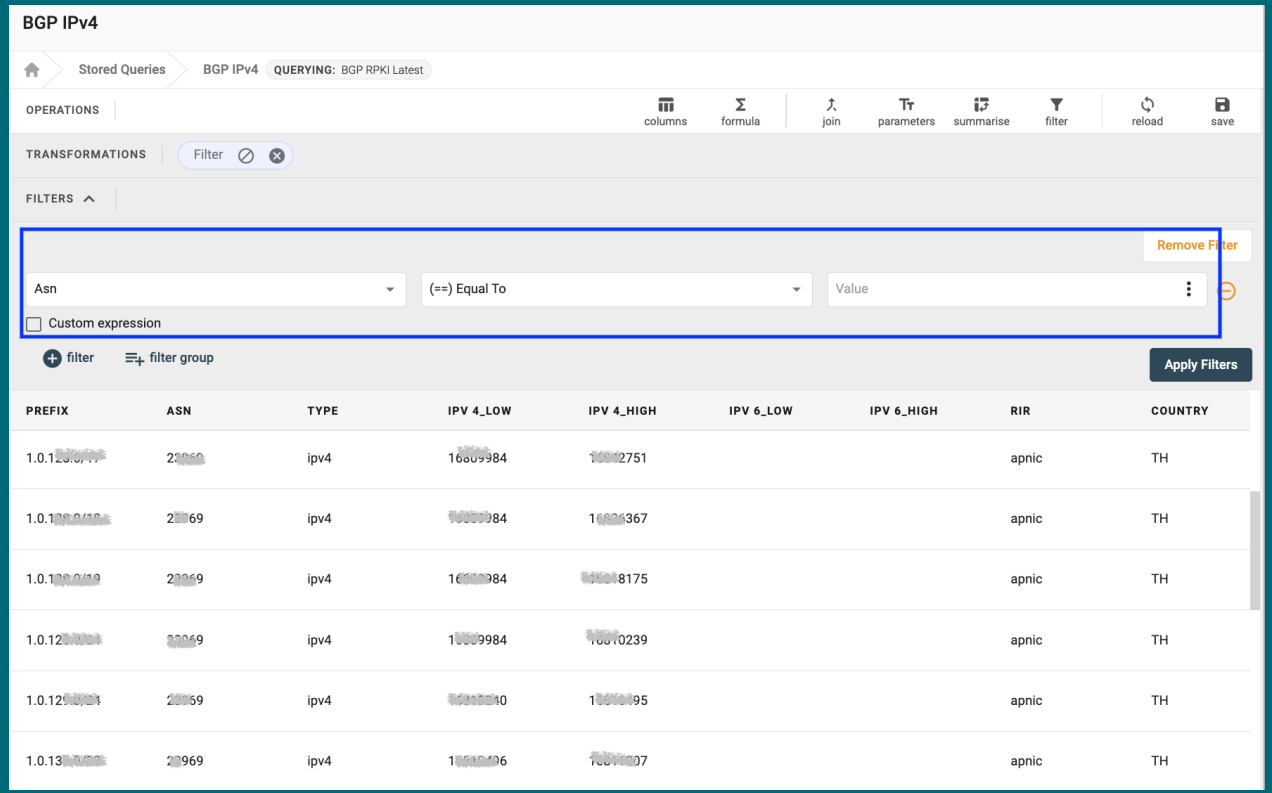
COUNTRY	NAME	VALID	INVALID	NOT FOUND
VC	Saint Vincent and the Grenadines	95.83% - 23	0.00% - 0	4.17% - 1
GD	Grenada	68.00% - 17	0.00% - 0	32.00% - 8
KY	Cayman Islands	63.89% - 23	0.00% - 0	36.11% - 13
TC	Turks and Caicos Islands	51.72% - 15	0.00% - 0	48.28% - 14
KN	Saint Kitts and Nevis	50.00% - 6	0.00% - 0	50.00% - 6
VG	Virgin Islands (British)	39.60% - 99	2.00% - 5	58.40% - 146
GP	Guadeloupe	33.33% - 13	0.00% - 0	66.67% - 26
CA	Canada	30.29% - 6920	0.83% - 189	68.88% - 1573
US	United States of America	24.66% - 68757	1.80% - 5007	73.54% - 2050
AG	Antigua and Barbuda	21.41% - 79	0.00% - 0	78.59% - 290

Ipv6 Validity

COUNTRY	NAME	VALID	INVALID	NOT FOUND
VC	Saint Vincent and the Grenadines	100.00% - 2	0.00% - 0	0.00% - 0
KN	Saint Kitts and Nevis	100.00% - 2	0.00% - 0	0.00% - 0
KY	Cayman Islands	80.00% - 16	0.00% - 0	20.00% - 4
GP	Guadeloupe	75.00% - 12	0.00% - 0	25.00% - 4
DM	Dominica	75.00% - 3	0.00% - 0	25.00% - 1
GD	Grenada	65.38% - 17	0.00% - 0	34.62% - 9

DNS RESEARCH FEDERATION

DAP – Ability to perform queries

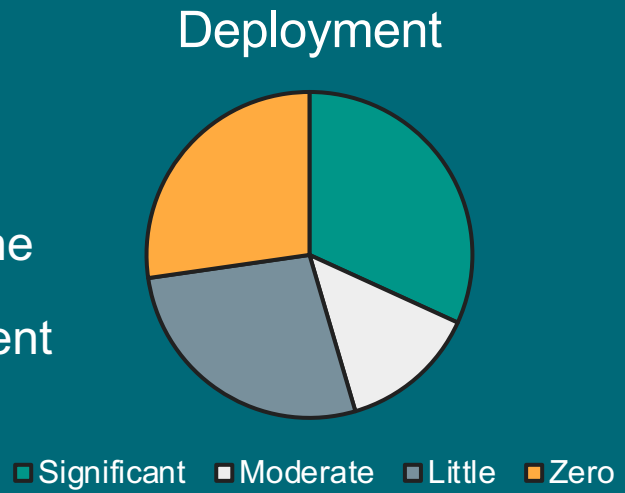


DNS RESEARCH FEDERATION

ARIN Deep Dive - Subregional Trends 1

- In the Caribbean Region there are four distinct groups
- 1. Those with significant deployment (>50%)
- 2. Those with moderate deployment (20-50%)
- 3. Those with little deployment (1-20%)
- 4. Those with no deployment

- Is this IPv4 specific?
- Intriguingly, the only difference is that ALL of the IPv6 deployment in those who are in the “little deployment” group for IPv4 have NO deployment for IPv6.



DNS RESEARCH FEDERATION

ARIN Deep Dive - Subregional Trends 2

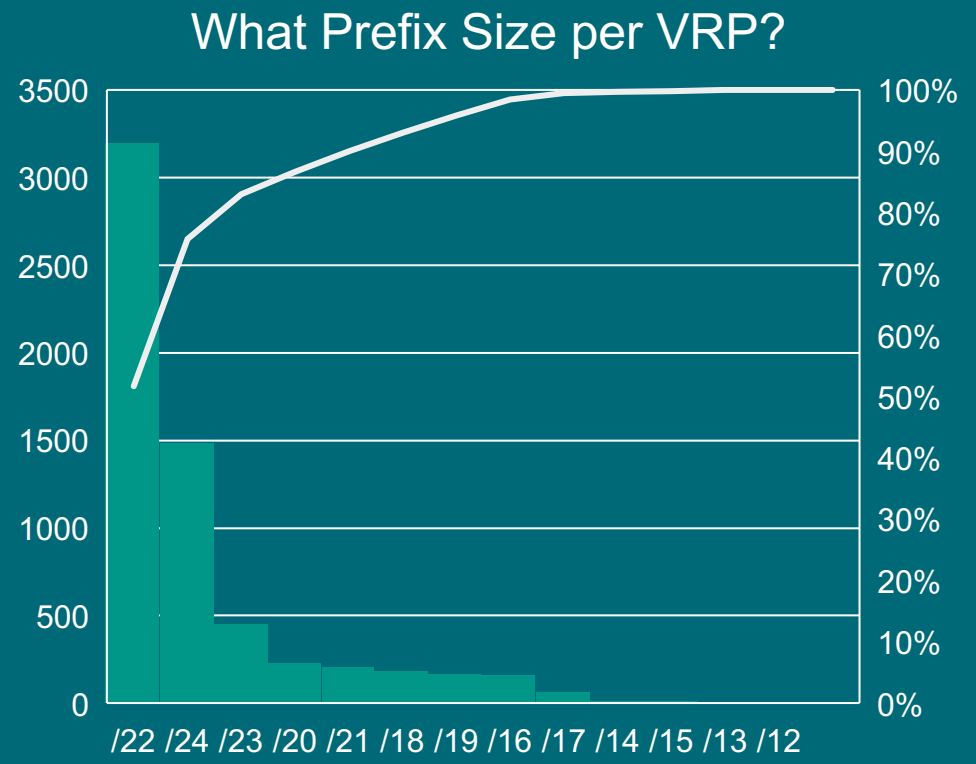
- In the Caribbean Region the number of invalids is almost vanishingly small
- There are two reasons for this:
- 1. The number of routes covered is naturally small compared to larger North American countries
- 2. The pattern of deployment is specific to individual ISPs and the data suggests that some ISPs make configuration errors

- Caribbean Region nations served by multiple ISPs see invalids for isolated routes served by individual ISPs

ARIN Deep Dive - Subregional Trends 3

- Canada
- 30.29% of routes have valid VRPs (6,920) – IPv4
- 50% for IPv6, but that appears to be because IPv6 takeup in not high in Canada
- Invalids are less than 0.9%
- /22s make up a large majority of the protected prefix size

- Protected prefix sizes range from /24s to /12s



DNS RESEARCH FEDERATION

ARIN Deep Dive - Subregional Trends 4

- United States
- 24.66% of routes have valid VRPs (68,757) – IPv4
- >53% for IPv6, which shows large deployment of IPv6 and RPKI for those prefixes
- Invalids are less than 2%
- Impressive given the number of VRPs
- Much more common in the US to have multiple invalids for a single AS

- Protected prefix sizes range from /24s to /12s

Invalids in the ARIN region

- What About Invalids?
- Are these configuration problems or actual abuse
- Pattern 1:
- *A number of ASes are covered per prefix, but something goes wrong with one of the prefixes in the AS*
- *We see this pattern often in the data*
- Pattern 2:
- *Isolated invalids: where a single AS is covered per prefix but something goes wrong with a single, isolated prefix*
- Pattern 3:
- *Duplicated records: more than one AS allocated to a unique prefix*

Case Study: British Virgin Islands

- ISP configuring one VRP for every /24
- 10.1.145.0/24
- 10.1.146.0/24
- 10.1.147.0/24 (obviously, these are examples . . ._
- ASN: a single ASN
- However:
- For the first /24, one VRP Covers the Route Prefix, but no VRP ASN matches the route origin ASN
- This looks like a configuration error to us, not abuse
- We see the same pattern applied to other ASes

Case Study: Puerto Rico

- ISP also configuring one VRP for every /24
- 10.1.224.0/24
- 10.1.225.0/24
- 10.1.226.0/24
- 10.1.227.0/24
- ASN: various, different for every prefix
- However:
- For the third /24, one VRP Covers the Route Prefix, but once again, no VRP ASN matches the route origin ASN
- In this case, the allocation of all four ranges is to an IP broker – configuration error? Leftover configuration?

Case Study: Canada

- ISP also configuring one VRP for every /24
- 10.1.102.0/24
- 10.1.234.103.0/24
- 10.1.234.104.0/24
- However:
- For the first /24, multiple VRPs Cover the same Route Prefix, but in this case one is invalid and the other is valid
- This is a different problem, but, once again, the allocation of all three ranges is to an IP broker – configuration error?

Methodology

- RPKI Validity Status of BGP announcements
- Unit of study: unique Prefix/Origin AS
- Data Sources and Validation
  - RouteViews for raw BGP Data – 6 vantage points, 94% coverage
  - Routinator for Route Origin Validation
  - RIR Public Stats Files for geoinformation
- Cross referencing with NIST and MANRS data to assess results → continuing to finesse algorithms

Rethinking Methodologies: RPKI adoption per IP address

Consider size of ranges.

The unit of measure for this presentation is “Source/Destination Address Pairs protected by a VRP.” That is consistent with other studies and with the work at NIST.

Would another interesting metric be the “total number of IP addresses served in routes protected by a VRP?” Instead of examining the number of routes successfully protected, look at the number of end nodes being protected? The data collected in this project supports that sort of analysis.

Next Steps

- Finalizing our data analysis and presenting indicators in an online report with live indicators
- Blog article for ARIN with some of the reflections from today
- Get the word out: presentations at NANOG, CARIBNOG

Interested in analyzing the data?

- Sign up for an account with DAP.LIVE: https://dnsrf.org/

DNS RESEARCH FEDERATION