DNS RESEARCH FEDERATION

RPKI Adoption and Routing Security in North America & Caribbean

Carolina Caeiro & Mark McFadden

About the Project

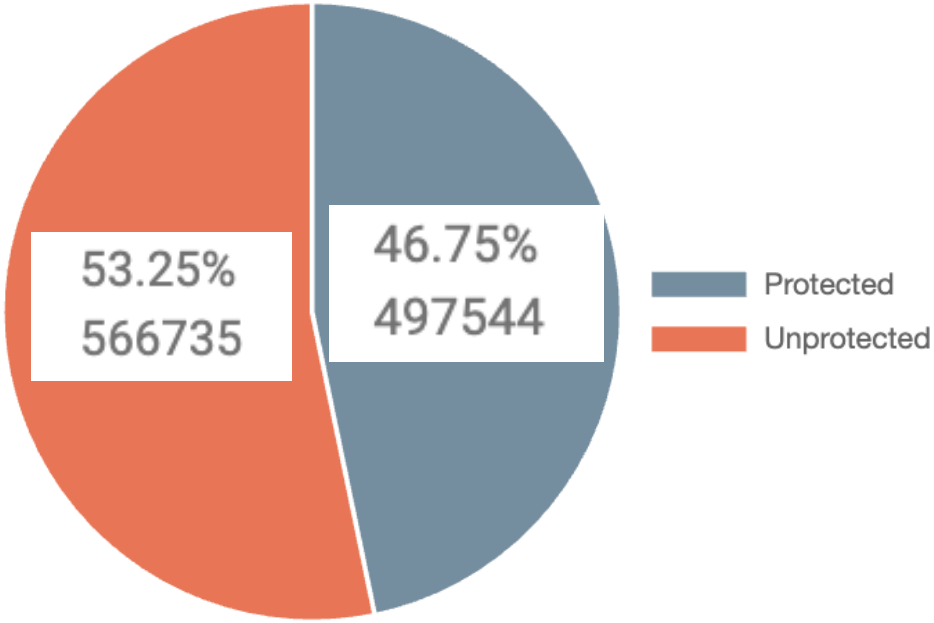
- ARIN Community Grant Program
- Showcase data on RPKI adoption in the ARIN region
- Value added:
  - Geographic data
  - Report with live indicators
  - Platform to do your own analysis

Today's Presentation

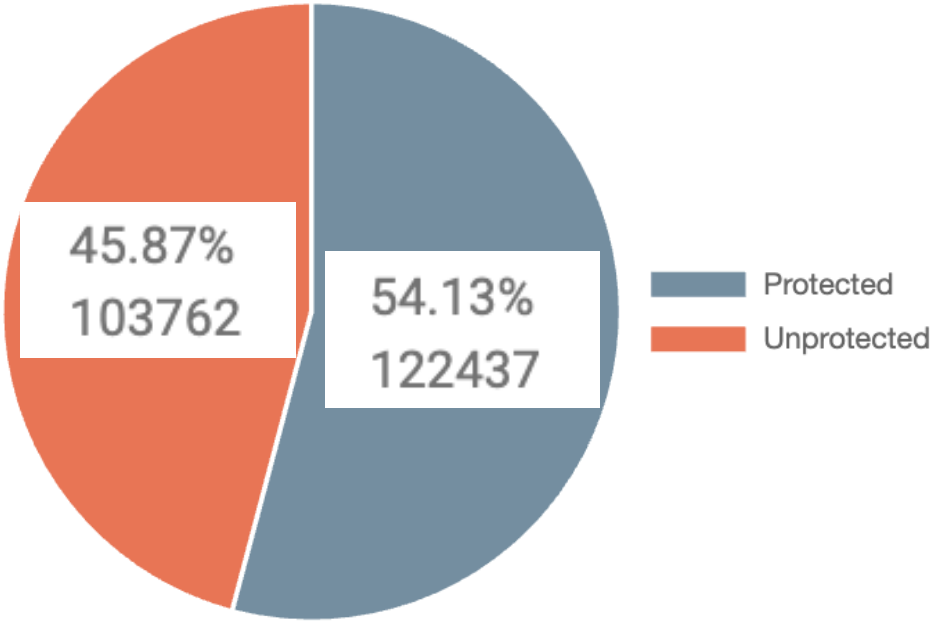
- ARIN in Context
- North American Deep Dive
- Invalids Deep Dive
- Methodology + other ways of thinking of routing security?
- Next steps

ARIN in Context: Global Coverage

IPv4 Protection



IPv6 Protection



ARIN in Context: ARIN / Global Coverage

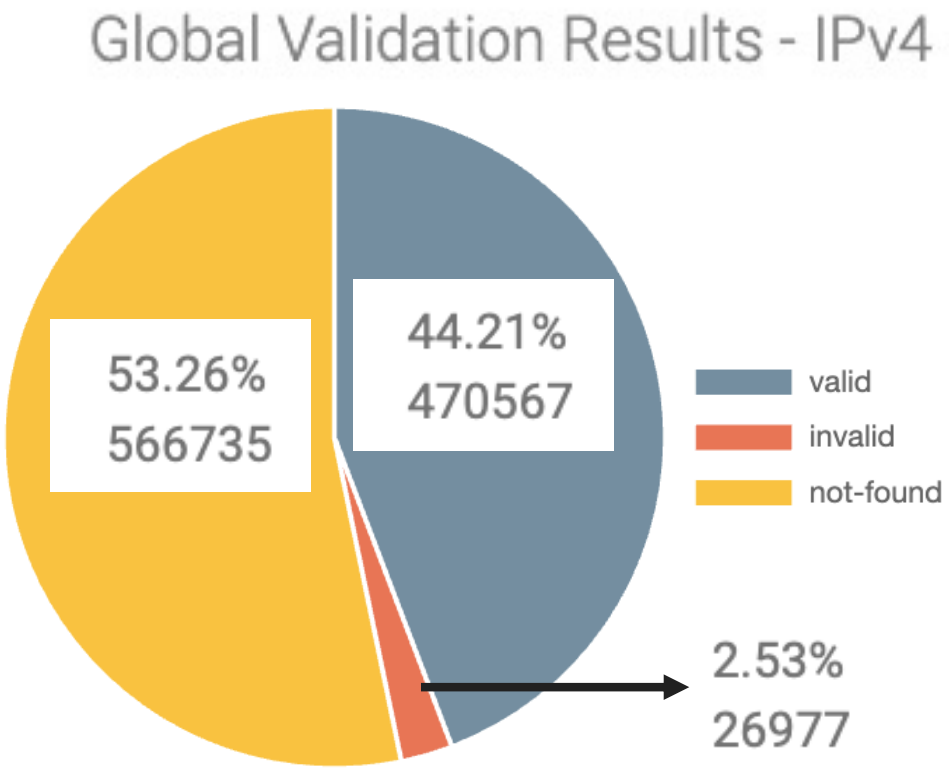
Global Coverage by RIR - IPv4

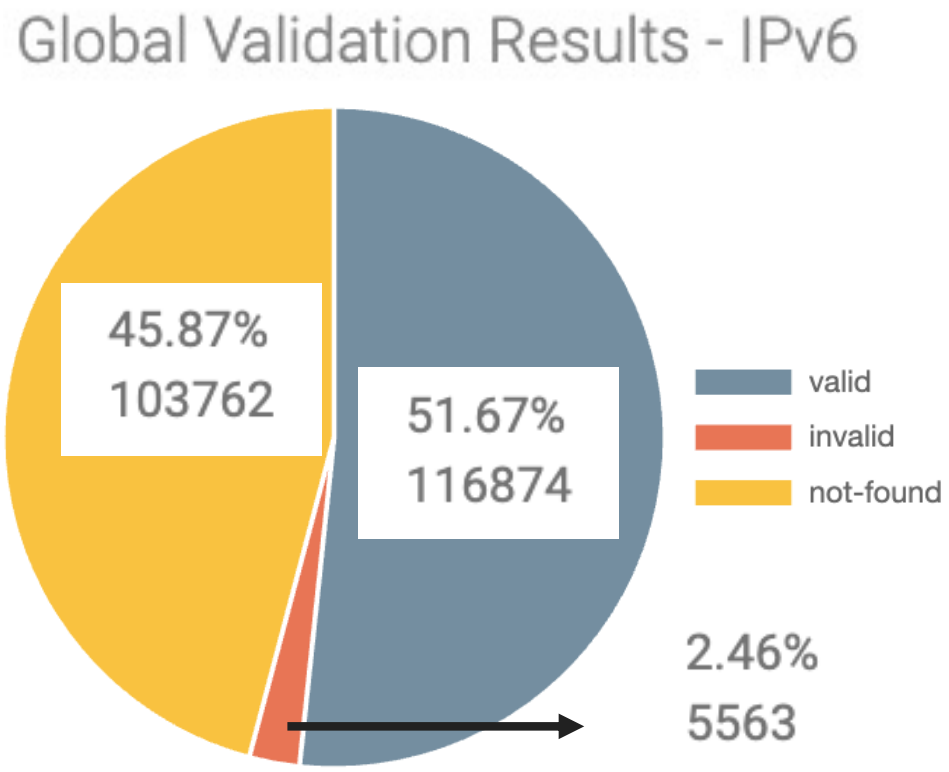
RIR	PROTECTED ↓	UNPROTECTED
arin	28.18% 86520	71.82% 220511

Global Coverage by RIR - IPv6

RIR	PROTECTED ↓	UNPROTECTED
arin	52.23% 20732	47.77% 18965

ARIN in Context: Global Validation Results





ARIN in Context: ARIN /Global Validation Results

Global Validation Results by RIR - IPv4

RIR	VALID ↓	INVALID	NOT FOUND
arin	26.41% 81082	1.77% 5438	71.82 % 220511

Global Validation Results by RIR - IPv6

RIR	VALID ↓	INVALID	NOT FOUND
arin	47.53% 18866	4.7% 1866	47.76 % 18965

Deep Dive - Results per country

2A: Coverage per Country

Ipv4 Protection

COUNTRY	NAME	PROTECTED ↓	UNPROTECTED
PM	Saint Pierre and Miquelon	100% - 18	0% - 0
VC	Saint Vincent and the Grenadines	95.83% - 23	4.17% - 1
MQ	Martinique	94.48% - 137	5.52% - 8

IPv6 Protection

COUNTRY	NAME	PROTECTED ↓	UNPROTECTED
MQ	Martinique	100% - 3	0% - 0
KN	Saint Kitts and Nevis	100% - 2	0% - 0
VC	Saint Vincent and the Grenadines	100% - 2	0% - 0

Deep Dive - Results per country

2B: Validation results per Country

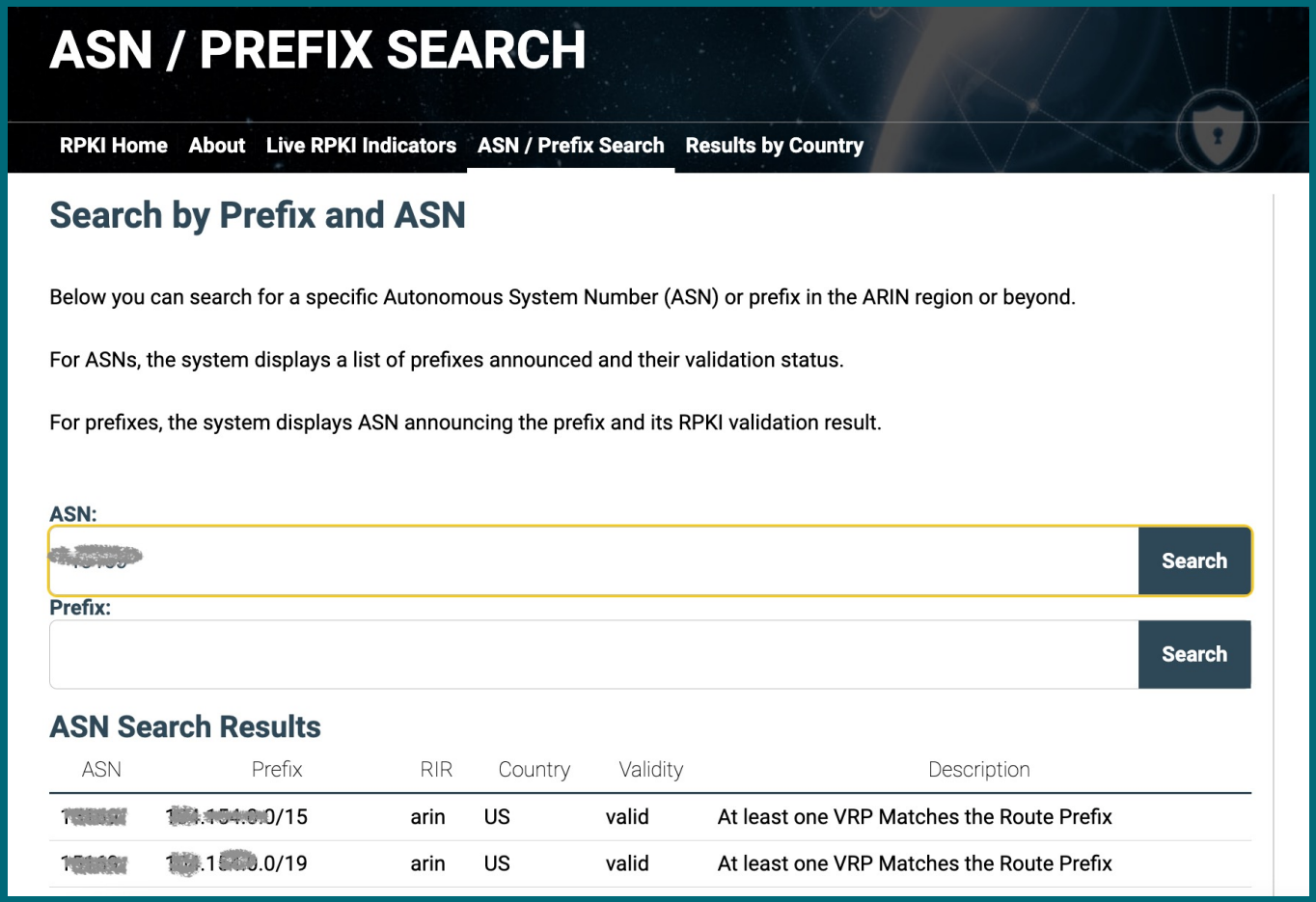
IPv4 Validity

COUNTRY	NAME	VALID ↓	INVALID	NOT FOUND
PM	Saint Pierre and Miquelon	100% - 18	0% - 0	0% - 0
VC	Saint Vincent and the Grenadines	95.83% - 23	0% - 0	4.170000000000002% -
MQ	Martinique	93.1% - 135	1.38% - 2	5.520000000000006% -

Ipv6 Validity

COUNTRY	NAME	VALID ↓	INVALID	NOT FOUND
MF	Saint Martin (French part)	100% - 1	0% - 0	0% - 0
KN	Saint Kitts and Nevis	100% - 2	0% - 0	0% - 0
VC	Saint Vincent and the Grenadines	100% - 2	0% - 0	0% - 0

Ability to perform your own personalized queries



North America Deep Dive – Canada

- 37.73% of routes have valid VRPs (validated ROA payload) (8,685) – IPv4
- 35.42% for IPv6, IPv6 takeup in not high in Canada, less IPv6 valid VRPs than US (53.42%)
- Invalids are less than 0.9% in both IPv4 and IPv6

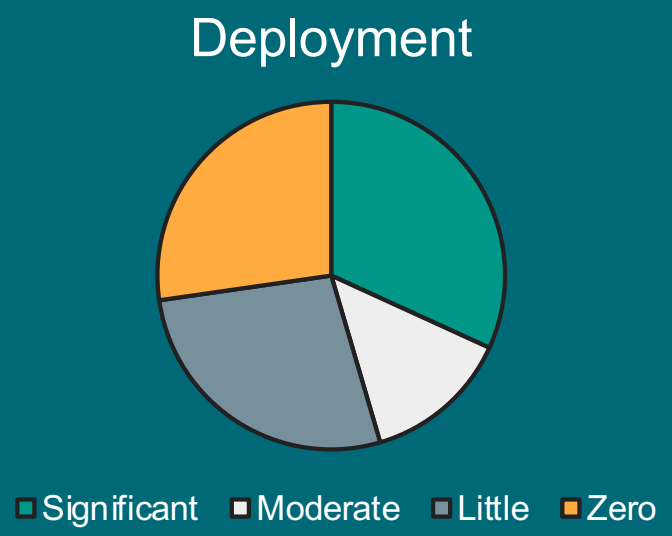
North America Deep Dive – United States

- 24.75% of routes have valid VRPs (77,531) – IPv4
- 54.42% for IPv6, which shows large deployment of IPv6 and RPKI for those prefixes
- Invalids are less than 2% in IPv4, 4.31% in IPv6
- 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

Deep Dive – Contrasting with the Caribbean (1)

In the Caribbean Region there are four distinct groups

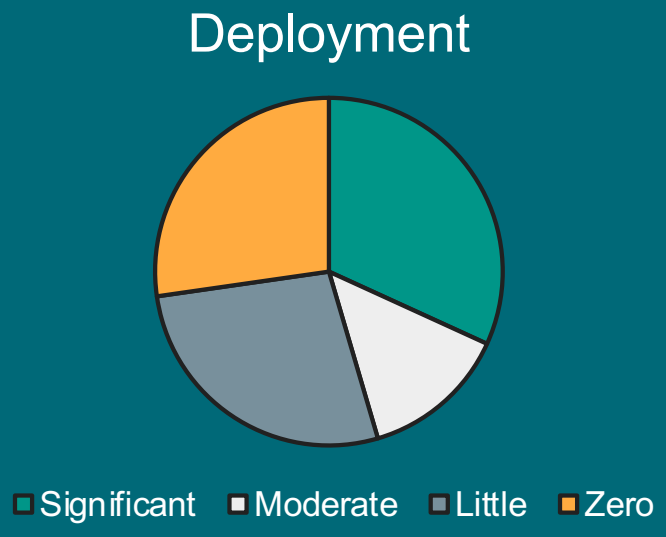
1. Those with significant deployment (>50%)
2. Those with moderate deployment (20-50%)
3. Those with little deployment (1-20%)
4. Those with no deployment



Deep Dive – Contrasting with the Caribbean (2)

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.



Deep Dive – Contrasting with the Caribbean (3)

- Invalids is almost vanishingly small. Why?
  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

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

Invalids in the ARIN region

- 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: 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 one is invalid and the other is valid
- Allocation of all three ranges is to an IP broker – configuration error?

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
- ASN: a single ASN
- However, for the first /24, one VRP Covers the Route Prefix, but no VRP ASN matches the route origin ASN
- Looks like configuration error, not abuse

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

Methodology

- 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

RPKI by end nodes protected?

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?”

Next Steps

- Online report with live indicators available: https://dnsrf.org/research/rpki/about/
- Forthcoming blog article for ARIN with some of the reflections from today

Interested in analyzing the data?

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