

Why Does MANRS Matter?





The opinions expressed here belong solely to myself, and do not reflect the views of my employers.

DISCLAIMER

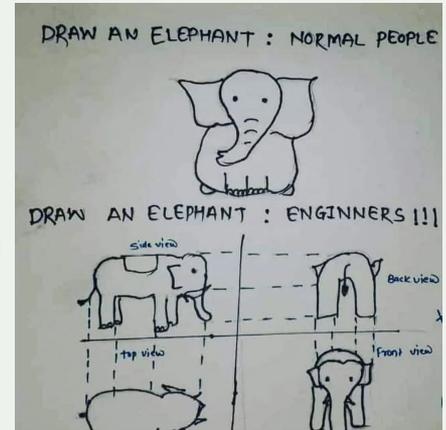


Why?

I can answer this in a simple way as an engineer, why should we improve security in internet routing?

I could mention legal, administrative, social and other aspects here... but particularly, for those who are keeping everything running, engineers also like to:

- sleep;
- go on vacations without hanging on your cell phone;
- go to a barbecue and stay until the end;
- have a nice weekend with the family without an alert;
- and many others... engineers are people too (in theory)!!!





MANRS

Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides crucial fixes to reduce the most common routing threats. MANRS offers specific actions via four programs for Network Operators, Internet Exchange Points, CDN and Cloud Providers, and Equipment Vendors.

In early 2014, a small group of network operators began working on a way to gather the wider operator community to improve the security and resilience of the global routing system. This eventually became an initiative we called the Routing Resilience Manifesto, and it produced a set of initial recommendations that we published as a draft document in July 2014 for community review and comment.

Once the community review and feedback period closed on 31 August 2014, we consolidated all the comments, updated the draft into the final version of the “Mutually Agreed Norms for Routing Security (MANRS)” document, and officially launched the MANRS site with an initial list of supporters.



Check => <https://www.youtube.com/watch?v=nJINk5p-HEE>

Source: MANRS

MANRS Programmes



Network Operators (2014)



Internet Exchange Points (2018)



Content Delivery Networks (CDNs)
and Cloud Providers (2020)



Network Equipment Vendors (2021)





Filtering

Ensure the correctness of your own announcements and of announcements from your customers to adjacent networks with prefix and AS-path granularity



Anti-Spoofing

Enable source address validation for at least single-homed stub customer networks, your own end-users, and infrastructure



Coordination

Maintain globally accessible up-to-date contact information



Global Validation

Publish your data, so others can validate routing information on a global scale



Tools

Provide monitoring and debugging tools to help others



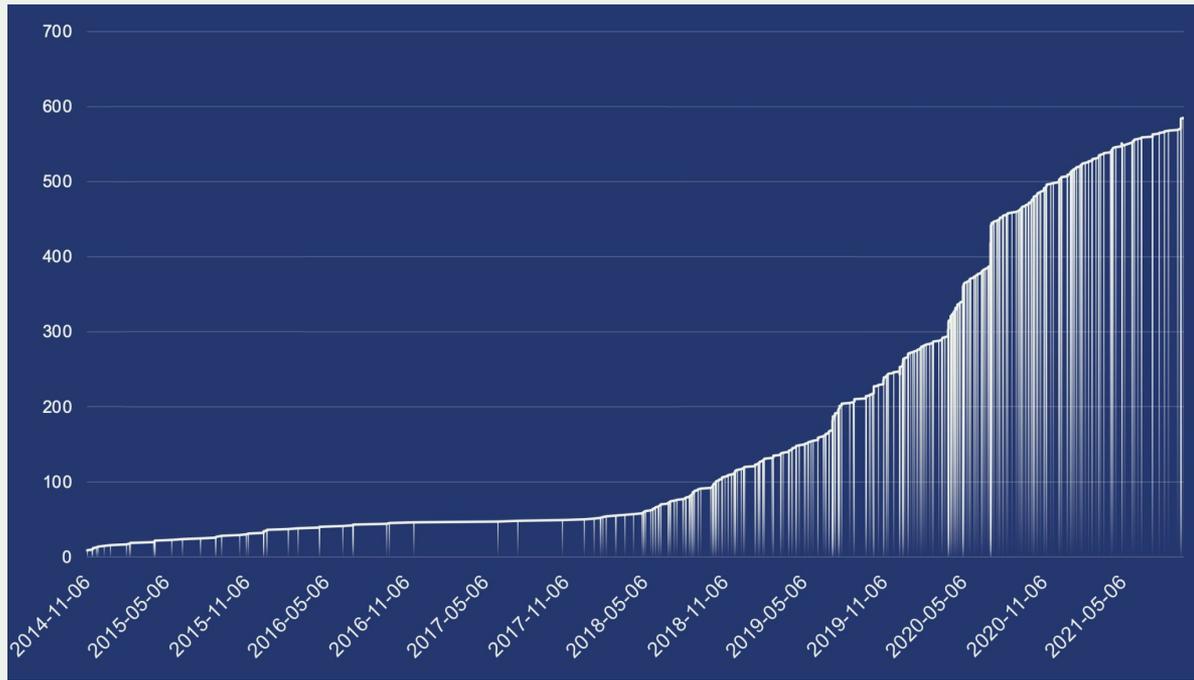
Promotion

Actively encourage MANRS adoption among peers, customers, and partners



MANRS actions

Source: MANRS



MANRS participants

22 participants

CDN and Cloud Providers

6 participants

Equipment Vendors

736 participants

Network Operators

105 participants

IXPs



Tools recommendations to help you to help all of us!





MANRS toolkit

Mutually Agreed Norms for Routing Security Tools

2 followers <https://www.manrs.org/>

- Overview
- Repositories 8
- Projects
- Packages
- People

Popular repositories

contrib Public In-development tools contributed by the community Go 10 stars 2 forks	labmgr Public ISOC Lab Manager Python 8 stars
MANRS-Implementation-Guide Public MANRS Implementation Guide 6 stars 2 forks	MANRS-validator Public A BGP Security Auditing Tool that runs locally and checks configuration the router config against the best practices as defined by MANRS RobotFramework 5 stars 1 fork
MANRS-IXP-validation-tool Public A tool that validates conformance of the IXP RS filtering policy with Action 1 of the MANRS IXP Program Python 4 stars 1 fork	GNS3-Appliances Public GNS3 Appliances for the MANRS Lab Manager 1 fork

People

This organization has no public members. You must be a member to see who's a part of this organization.

Top languages

- Python
- Go
- RobotFramework
- HTML



MANRS toolkit/repo => <https://github.com/manrs-tools>

MANRS Observatory

<https://observatory.manrs.org/>

Provides a factual state of MANRS readiness and tracks it over time

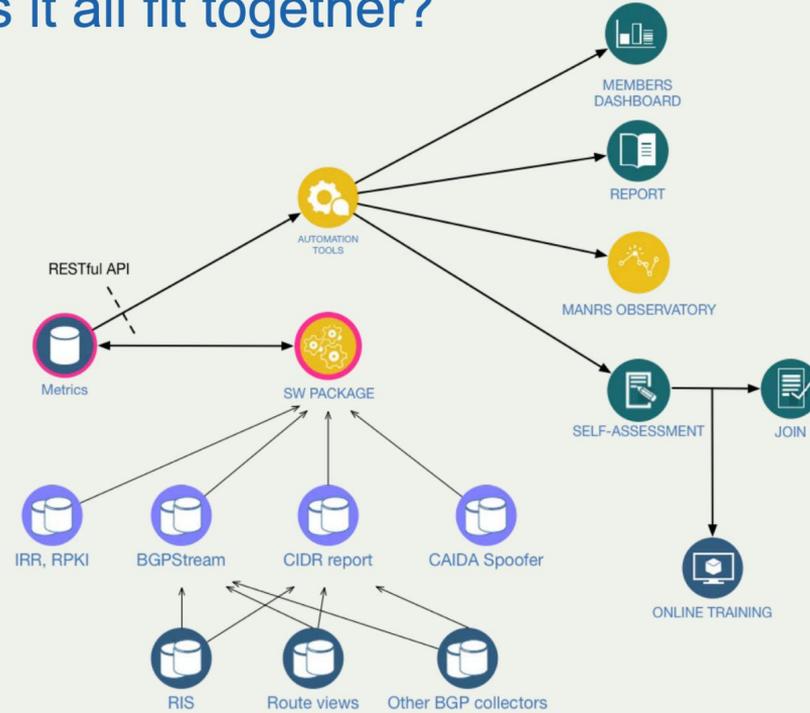
Measurements are:

- Transparent – using publicly accessible data
- Passive – no cooperation from networks required
- Evolving – MANRS community decide what gets measured and how



Source: MANRS

How does it all fit together?



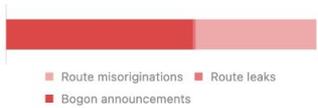
Overview

State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents

Route misoriginations	42
Route leaks	1
Bogon announcements	65
Total	108



Culprits

Culprits	76
----------	----



Routing completeness (IRR)

Unregistered	4,067	4.8%
Registered	80,244	95.2%



Routing completeness (RPKI)

Valid	22,920	27.2%
Unknown	61,147	72.5%
Invalid	244	0.3%



MANRS Readiness

Filtering



Anti-spoofing



Coordination



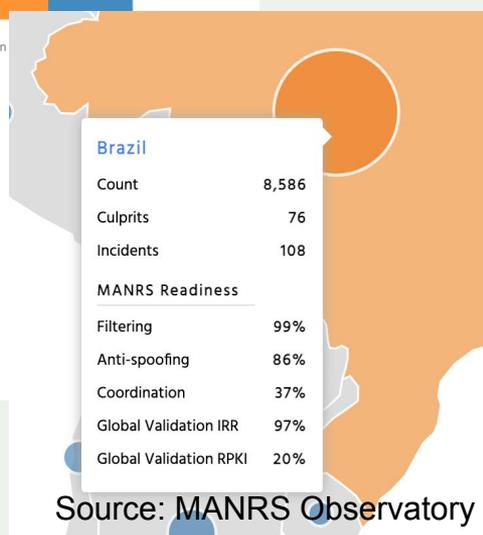
Global Validation IRR



Global Validation RPKI

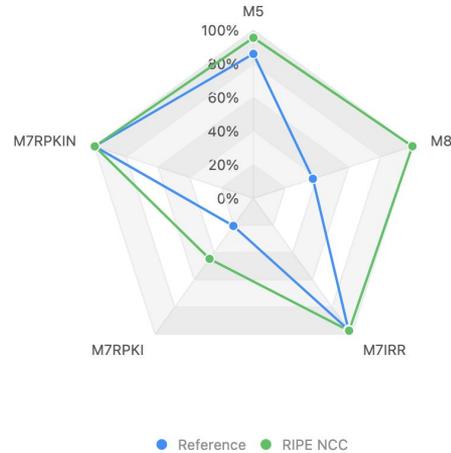
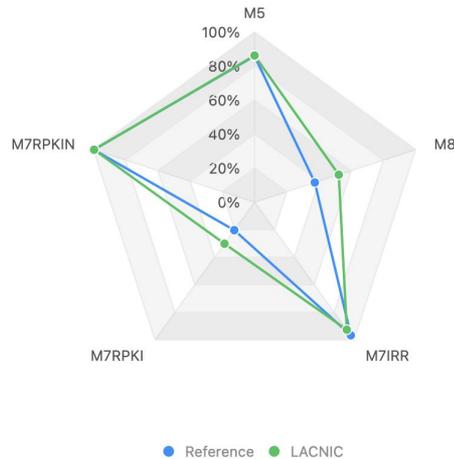
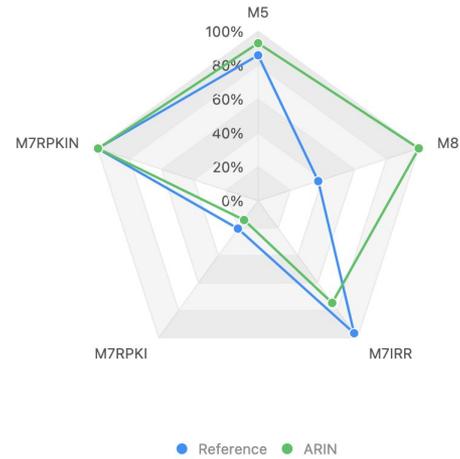
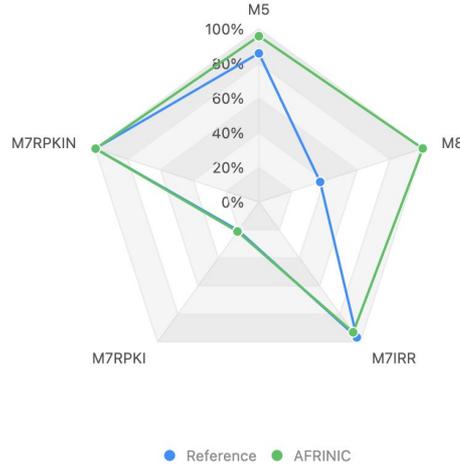
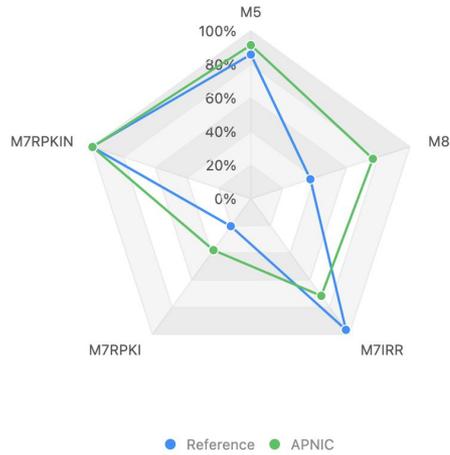


● Ready ● Aspiring ● Lagging ● No Data Available

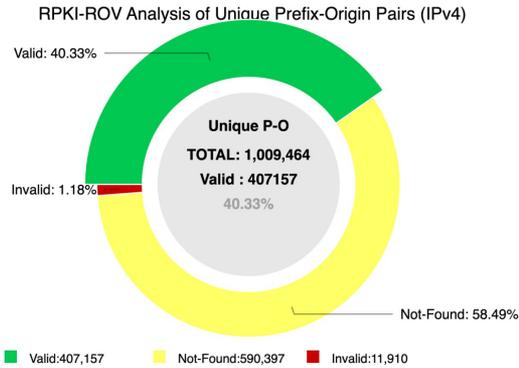


MANRS Observatory

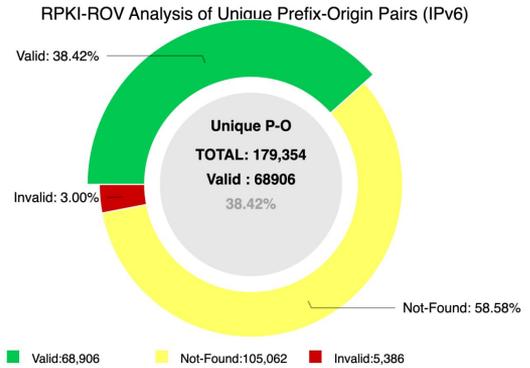
Brazil X RIRs



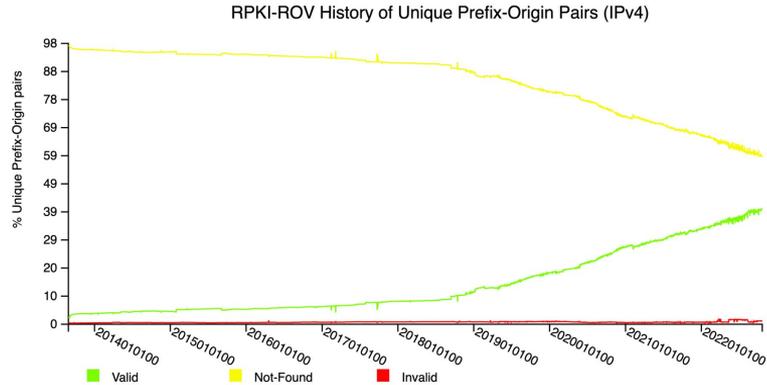
- M5 - Spoofing IP blocks**
- M7IRR - Registered routes**
- M7RPKI - Valid ROAs for routes**
- M7RPKIN - Invalid routes**
- M8 - Contact registration (RIR, IRR, PeeringDB)**



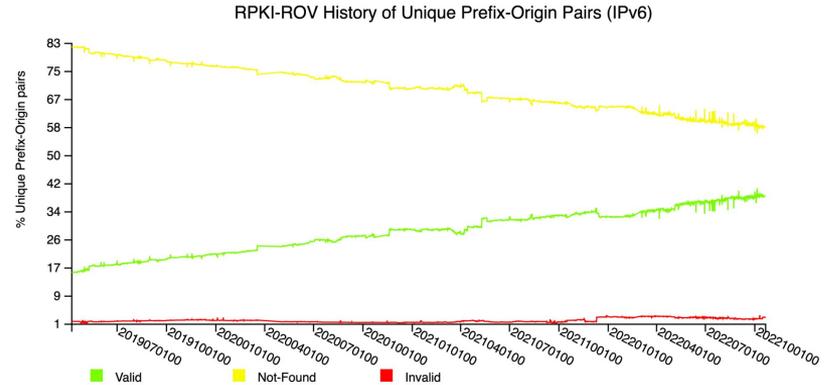
NIST RPKI Monitor: RPKI-ROV Analysis Protocol: IPv4 RIR: All Date: 2022-10-21 06:00



NIST RPKI Monitor: RPKI-ROV Analysis Protocol: IPv6 RIR: All Date: 2022-10-21 06:00



NIST RPKI Monitor: RPKI-ROV Analysis Protocol: IPv4 RIR: All



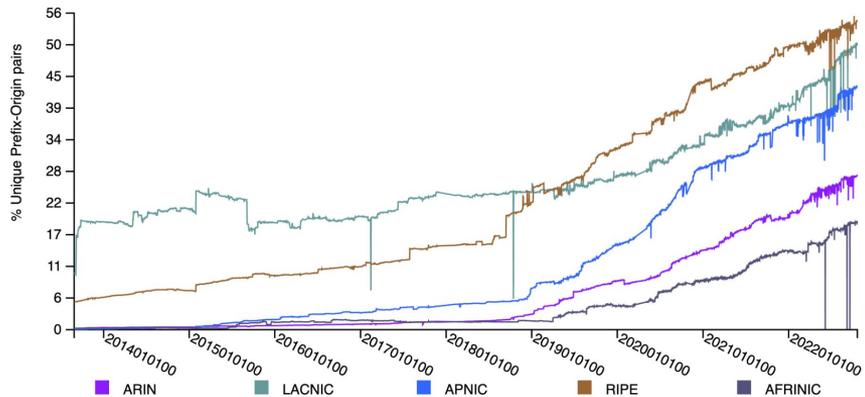
NIST RPKI Monitor: RPKI-ROV Analysis Protocol: IPv6 RIR: All



RPKI - Global status => <https://rpk-monitor.antd.nist.gov/>

Source: NIST

RPKI-ROV History of Unique Valid Prefix-Origin Pairs (IPv4) - Comparing RIR Regions

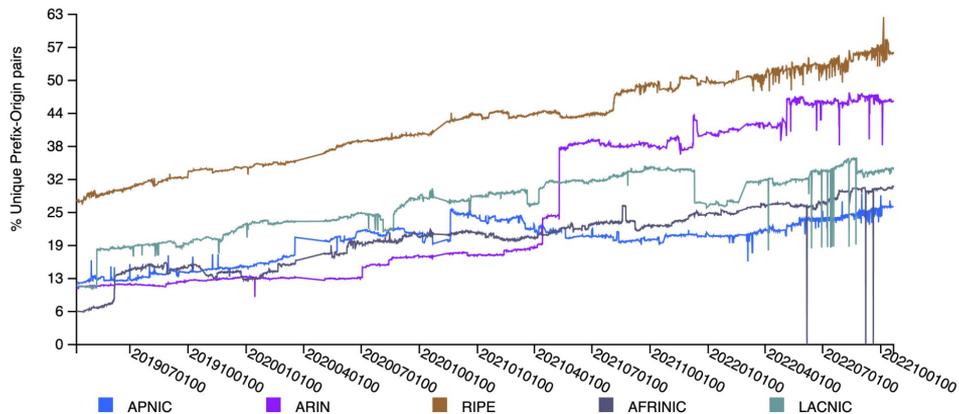


NIST RPKI Monitor: RPKI-ROV Analysis

Protocol: IPv4

RIR: All

RPKI-ROV History of Unique Valid Prefix-Origin Pairs (IPv6) - Comparing RIR Regions



NIST RPKI Monitor: RPKI-ROV Analysis

Protocol: IPv6

RIR: All



RPKI per RIR - <https://rpk-monitor.antd.nist.gov/>

Source: NIST

Global Routing Intelligence Platform

Select an event type

[All](#)
[MOAS](#)
[Sub-MOAS](#)
[New Edge](#)
[Defcon](#)

Select an event suspicion level

[All](#)
[Suspicious](#)
[Grey](#)
[Benign](#)

Select time period (UTC now: Oct 24, 2022 1:36 PM)

 Oct 23, 2022 1:35 PM - Oct 24, 2022 1:35 PM

Search for events by prefix/ASN/tags

Events List

Potential Victims	Potential Attackers	Largest (Sub)Prefix	# Prefix Events	Start Time	Duration	Suspicion	Category	Type
AS27983 Red Intercabl...J S.A.	AS266800 A. DOS S.R.L	45.234.120.0/24	1	2022-10-24 12:25	ongoing	High	Default Tr Worthy	moas
AS269827 VIGINET C.A	AS263703 NetLink Améri...a C.A.	190.97.238.0/24	6	2022-10-24 11:30	ongoing	High	Default Tr Worthy	moas
AS40 Massachusetts...nology AS268640 JSOUZANET TELECOM	AS16 Lawrence Berk...ratory	45.164.199.0/24	1	2022-10-24 11:00	0 min	High	Default Tr Worthy	moas
AS268640 JSOUZANET TELECOM	AS40 Massachusetts...nology	45.164.199.0/24	1	2022-10-24 10:55	5 min	High	Default Tr Worthy	moas
AS268640 JSOUZANET TELECOM	AS16 Lawrence Berk...ratory	45.164.198.0/24	1	2022-10-24 10:55	ongoing	High	Default Tr Worthy	moas
AS139660 OBHost LLC	AS834 IPXO LLC	104.234.220.0/24	1	2022-10-24 10:00	ongoing	High	Default Tr Worthy	moas
AS328175 Xpress Paymen...imited	AS37280 Broad Based C...imited	80.88.8.0/24	1	2022-10-24 08:35	3 hour	High	Default Tr Worthy	moas
AS47965 Signalhorn Tr...s GmbH	AS14679 Curb Mobility, LLC	64.110.153.0/24	1	2022-10-24 08:15	ongoing	High	Default Tr Worthy	moas
AS131442 Digital Netwo...vt Ltd	AS132497 DIGITAL NETWO...IMITED	103.245.68.0/24	1	2022-10-24 07:10	ongoing	High	Default Tr Worthy	moas
AS1239 Sprint	AS834 IPXO LLC	194.163.64.0/22	1	2022-10-24 07:05	ongoing	High	Default Tr Worthy	moas

 Rows per page: 10 ▾ 1-10 of 20 


GRIP - Global Routing Intelligence Platform => <https://grip.inetintel.cc.gatech.edu/>

Source: GRIP

 Reduced colour mode

Report for ASN AS1103

What does the prefix table show? ▼

Explanation of different messages ▼

Prefixes originated by AS1103

Prefix ▼	RIR ↕	BGP ↕	RPKI ↕	LEVEL3 ↕	RADB ↕	RIPE ↕	Advice ↕
129.125.0.0/16	RIPE NCC	1103	1103 1/16			1103 ✓	✓ Everything looks good
130.37.0.0/16	RIPE NCC	1103	1103 1/16			1103 ✓	✓ Everything looks good
130.89.0.0/16	RIPE NCC	1133	1133 1/16		45177 ✗	1103 ✗, 1133 ✓	✗ RPKI-invalid route objects found ⓘ Expected route object in RIPE matches BGP origin, but non-matching objects exist in other IRRs
130.112.0.0/16	RIPE NCC	1103	1103 1/16			1103 ✓	✓ Everything looks good
130.115.0.0/16	RIPE NCC	1103	1103 1/16			1103 ✓	✓ Everything looks good
131.174.0.0/16	RIPE NCC	1103	1103 1/16			1103 ✓	✓ Everything looks good
131.211.0.0/16	RIPE NCC	1103	1103 1/16			1103 ✓	✓ Everything looks good
131.224.0.0/16	RIPE NCC	1103	1103 1/16			1103 ✓	✓ Everything looks good
132.229.0.0/16	RIPE NCC	1103	1103 1/16			1103 ✓	✓ Everything looks good
134.203.0.0/16	RIPE NCC					1103	ⓘ Route objects exist, but prefix not seen in DFZ ⓘ No (covering) RPKI ROA found for route objects
134.221.0.0/16	RIPE NCC	1103	1103 1/16			1103 ✓	✓ Everything looks good



IRR explorer => <https://irrexplorer.nlnog.net/>

Source: IRR explorer

194.104.124.0/23	RIPE NCC	1103	1103 ↗/23	1103 ☑	✔ Everything looks good
194.104.240.0/20	RIPE NCC	1103		1103	❗ No (covering) RPKI ROA found for route objects
194.171.0.0/16	RIPE NCC	1103	1103 ↗/16	1103 ☑	✔ Everything looks good
194.171.72.0/24	RIPE NCC			1103 ☒	❌ RPKI-invalid route objects found ❗ Route objects exist, but prefix not seen in DFZ
194.171.96.0/21	RIPE NCC	1104	1104 ↗/21	1103 ☒, 1104 ☑	❌ RPKI-invalid route objects found ⚠ Multiple route objects exist with different origins
195.169.0.0/16	RIPE NCC	1103	1103 ↗/16	1103 ☑	✔ Everything looks good
195.169.140.0/24	RIPE NCC		288 ↗/24	1103 ☒	❌ RPKI-invalid route objects found ❗ Route objects exist, but prefix not seen in DFZ ❗ RPKI ROA exists, but prefix not seen in DFZ
2001:610::/29	RIPE NCC	1103	1103 ↗/29	1103 ☑	✔ Everything looks good
2001:610::/32	RIPE NCC		1103 ↗/48		❗ RPKI ROA exists, but prefix not seen in DFZ
2001:610:130::/48	RIPE NCC		1103 ↗/64		❗ RPKI ROA exists, but prefix not seen in DFZ
2001:67c:262c::/48	RIPE NCC	1103	1103 ↗/48	1103 ☑	✔ Everything looks good
2a0f:d980::/32	RIPE NCC	1152		1103	❌ No route objects match DFZ origin ❗ No (covering) RPKI ROA found for route objects



[Source data as JSON](#)



IRR explorer => <https://irrexplorer.nlnog.net/>

Source: IRR explorer



 Looking Glass

ROUTE SERVERS

IX.br São Paulo/SP

rs2.saopaulo.sp.ix.br (IPv4)
 multibird 2.0.8

rs2.saopaulo.sp.ix.br (IPv6)
 multibird 2.0.8

rs2.saopaulo.sp.ix.br (IPv4)

Filter by Neighbor, ASN or Description

Sort here!

Go to: **Established** Down

Last Reconfig: **Monday, October 24, 2022 6:01 AM**

Daemon is up and running

Generated **10 minutes ago**.
Next refresh in **9 minutes**.

BGP SESSIONS ESTABLISHED

Neighbor	ASN	State	Uptime	Description	Routes Recv.	Routes Filtered
187.16.221.197	6939	up	3 months	HE-v4	103855	2913
187.16.210.98	57463	up	4 months	NETIX	26631	1284
187.16.222.2	32787	up	2 months	Akamai	4893	373
187.16.218.182	16735	up	4 months	ctbc-v4	10515	211
187.16.217.48	16735	up	4 months	CTBC-2	10467	210
187.16.219.32	262589	up	7 days	Internexa	6844	178



 103.114.131.0/24
 Bogon ASN



 103.233.174.0/23
 Bogon ASN
 Invalid on RPKI



 2001:ded:8000::/48
 IX.br prefixes



 2001:df0:10c0::/48
 Never via route server

ROUTES FILTERED

Network	Next Hop	AS Path
  131.0.200.0/22 Invalid on Registro.br	187.16.218.182	16735 28284



 164.77.70.0/25
 Invalid prefix length
 Invalid on RPKI



 164.77.70.128/25
 Invalid prefix length
 Invalid on RPKI



IX.br LG it's a good start point to see what's being filtered out... if it's being sent to IX.br, probably this it's not being sent only for IX.br! :)

Source: LG IX.br

IX.br (PTT.br) São Paulo

Peers **1511** Connections **1976** Open Peers **1214** Total Speed **83.8T** % with IPv6 **94**

Organization	NIC.br
Also Known As	
Long Name	IX.br (PTT.br) São Paulo
City	São Paulo/SP
Country	BR
Continental Region	South America
Media Type	Ethernet
Service Level	Not Disclosed
Terms	Not Disclosed
Last Updated	2022-09-27T18:33:13Z
Notes 	<p>This is the Peering information for the IX.br (PTT.br) Route Servers.</p> <p>There are two route servers per IXP for redundancy purposes in Sao Paulo</p> <p>For IX.br (PTT.br) Sao Paulo we recommend a maximum-prefixes setting 370K for IPv4 and 160K for IPv6</p>

Peers at this Exchange Point

Peer Name  IPv4	ASN IPv6	Speed	Policy
(VIPLANET) E.D TELECOMUNICES 2001:12f8::217:222	266620 187.16.217.222	10G	 Open
+Net & Telecom 187.16.217.171	267554 2001:12f8::217:171	10G	Open
1 Telecom Servicos de Internet 2001:12f8::222:100	52965 187.16.222.100	100G	 Open
1 Telecom Servicos de Internet 2001:12f8::217:205	52965 187.16.217.205	5G	 Open
3E TELECOM 187.16.219.142	61924 2001:12f8::219:142	2G	 Open
3E TELECOM 187.16.221.15	61924 2001:12f8::221:15	2G	 Open



MANRS+

The purpose of the MANRS+ Working Group is to explore the idea of creating a second, elevated tier of MANRS participation for organizations that comply with more stringent requirements and auditing.

The Working Group will create a significantly higher value proposition for a subset of the MANRS participants based on a credible quality mark it will represent, recognized by customers, and used in their business decisions. This quality mark and the associated certification process assume better alignment with customer needs and more profound conformance auditing leading to better security assurance.



News!

Nominations Open for MANRS Steering Committee

Nominations for three seats on the MANRS Steering Committee are now open! The nomination period continues until 28 October 2022, 23:59 UTC.

<https://www.manrs.org/2022/10/nominations-open-for-manrs-steering-committee/>

RFC 9319

The Use of maxLength in the Resource Public Key Infrastructure (RPKI)

<https://www.rfc-editor.org/rfc/rfc9319.html>



What's next?

=> Join MANRS.

=> Help us raise awareness about routing security.

=> Contact us to get involved in elections, MANRS+ development, etc.

=> Ask your peers and providers about MANRS compliance.

**If you need help with, I'm happy to help you
(or forward you to the correct path/person)!**



Thank you.

Wait... question time!!!

Not for me (yet), this time I'll ask you!

Please join the game, and if you are in first place, a prize for relaxing a little bit! :D

