THE IMPOSSILE MANRS

Hanna Kreitem
KREITEM@ISOC.ORG

Why Does MANRS Matter?

Quick Overview of MANRS

Border Gateway Protocol (BGP) is based entirely on trust between networks.

Prone to Prefix and Route Hijacks, Route Leaks, and IP Spoofing.

Mutually Agreed Norms for Routing Security (MANRS) offers crucial fixes to reduce the most common routing threats. Relies on collective responsibility to ensure a globally robust and secure routing infrastructure.

MANRS Programs defines the minimum steps networks, CDNs, vendors, and IXPs should take to ensure the security and resilience of the Internet's global routing system.

MANRS Programs and Actions

Network Operators	CDN and Cloud Providers	IXP	Vendor
Action1: Filtering *	Filtering	Filtering	Provide solutions for the implementation of specific MANRS Actions by other participants
Action 2: Anti-spoofing	Anti-spoofing	Promotion	Promote MANRS through training and technical content
Action 3: Coordination *	Coordination	Protect the peering platform	Commit to ongoing MANRS activities
Action 4: Global Validation *	Global Validation	Coordination	
	Promotion	Tools	
	Tools		

Conforming with MANRS

Or is MANRS impossible to conform with?

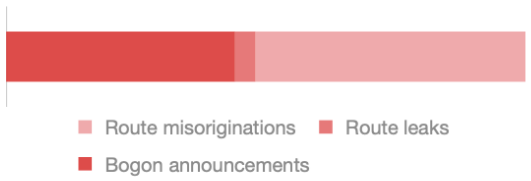
MANRS Readiness, Global

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

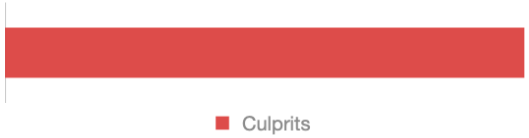
Incidents

Route misoriginations	**939**
Route leaks	**71**
Bogon announcements	**794**
Total	**1,804**



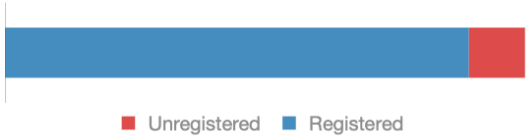
Culprits

Culprits	**1,236**



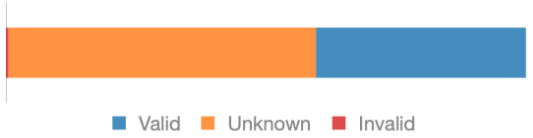
Routing completeness (IRR)

Unregistered	122,277	**10.8%**
Registered	1,008,528	**89.2%**



Routing completeness (RPKI)

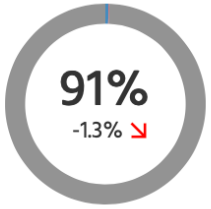
Valid	456,387	**40.4%**
Unknown	668,526	**59.1%**
Invalid	5,892	**0.5%**



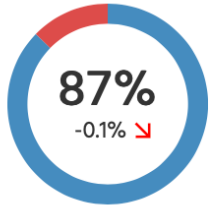
MANRS Readiness

Filtering

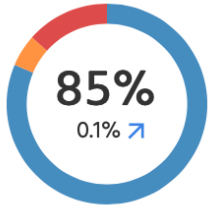
Anti-spoofing



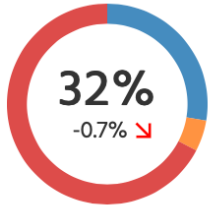
Coordination



Global Validation IRR



Global Validation RPKI



Ready Aspiring Lagging No Data Available

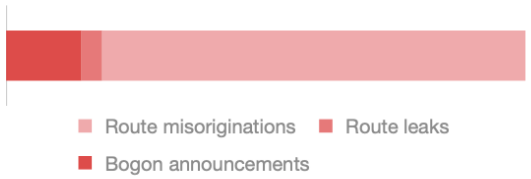
MANRS Readiness, Middle East

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	62
Route leaks	3
Bogon announcements	11
Total	76

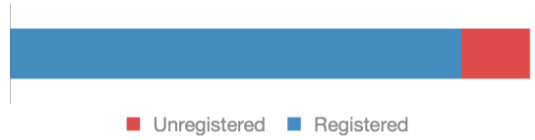


Culprits

Culprits	46

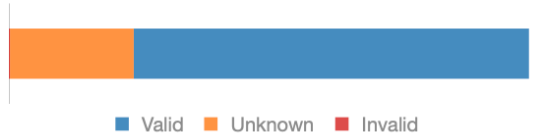
Routing completeness (IRR)

Unregistered	7,814	13.2%
Registered	51,553	86.8%



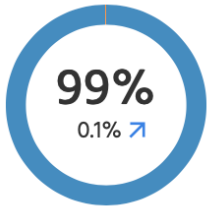
Routing completeness (RPKI)

Valid	45,105	76.0%
Unknown	14,110	23.8%
Invalid	152	0.2%



MANRS Readiness

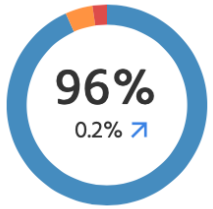
Filtering



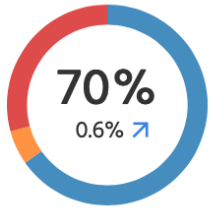
Anti-spoofing

Coordination

Global Validation IRR



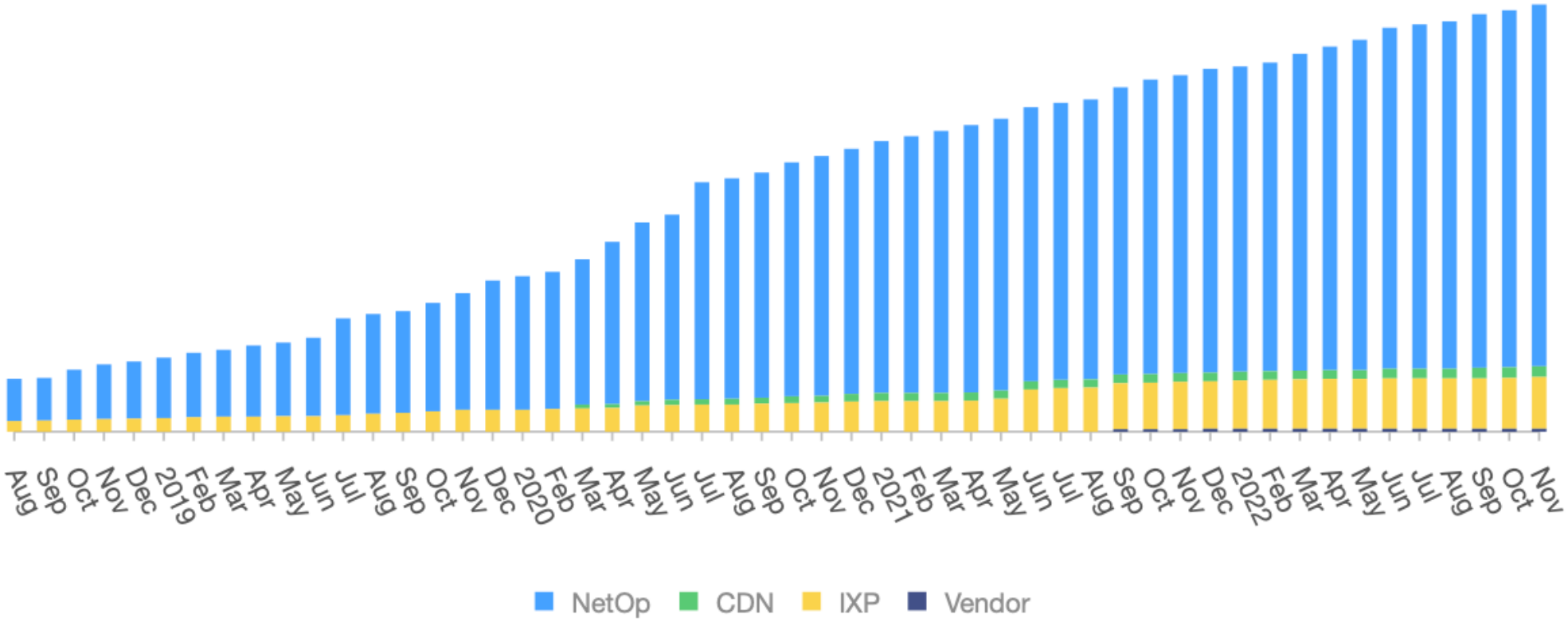
Global Validation RPKI



Ready Aspiring Lagging No Data Available

MANRS Participants Global

Participants by program by month



Network Operators	747
CDN and Cloud Providers	22
IXP	107
Vendors	6

November 2022

MANRS Participants ME

Network Operators	18
CDN and Cloud Providers	-
IXP	3 (UAE-IX, SAIX, DE-CIX IST)
Vendors	-
November 2022	

What does it take to become a MANRS participant?

TIME

KNOW-HOW

ACCESS TO RESOURCES

MANRS Actions and Implementation (NetOps)

Action 1, Filtering
Preventing propagation of incorrect routing information.
There are several ways to build these filters: 1. Use Internet Routing Registries (IRRs) and require the customers to register route objects 2. Use Resource Public Key Infrastructure (RPKI) and require the customers to create Route Origin Authorizations (ROAs) 3. Use an internal database with the information provided as part of the provisioning process This document will only focus on the first two cases, since case 3 is proprietary.

More details and sample configurations available at the MANRS Implementation Guide:
https://www.manrs.org/netops/guide/

MANRS Actions and Implementation (NetOps)

Action 2, Anti-spoofing
Preventing traffic with spoofed source IP addresses
Network operator implements a system that enables source address validation for at least single-homed stub customer networks, their own end-users and infrastructure. Network operator implements anti-spoofing filtering to prevent packets with incorrect source IP address from entering and leaving the network.
For most smaller and simpler network architectures the easiest way to prevent spoofing is by using Unicast RPF (uRPF) in Strict Mode.

More details and sample configurations available at the MANRS Implementation Guide:
https://www.manrs.org/netops/guide/

MANRS Actions and Implementation (NetOps)

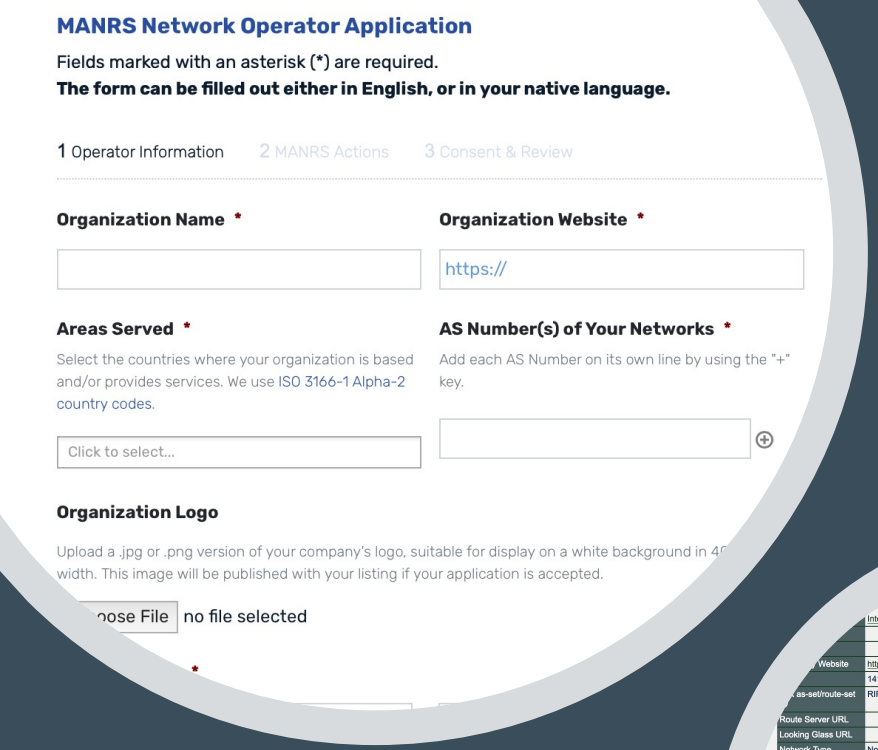
Action 3, Coordination
Facilitating global operational communication and coordination between network operators
• At a minimum, a network operator should register and maintain 24/7 contact information in at least one of RADB, AfriNIC, APNIC, ARIN, LACNIC and RIPE, and also on their public website.

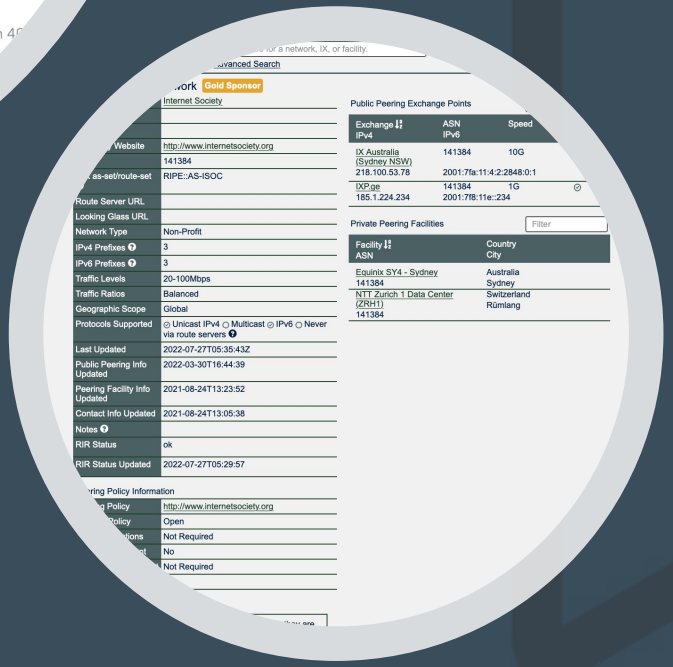
More details and sample configurations available at the MANRS Implementation Guide:
https://www.manrs.org/netops/guide/

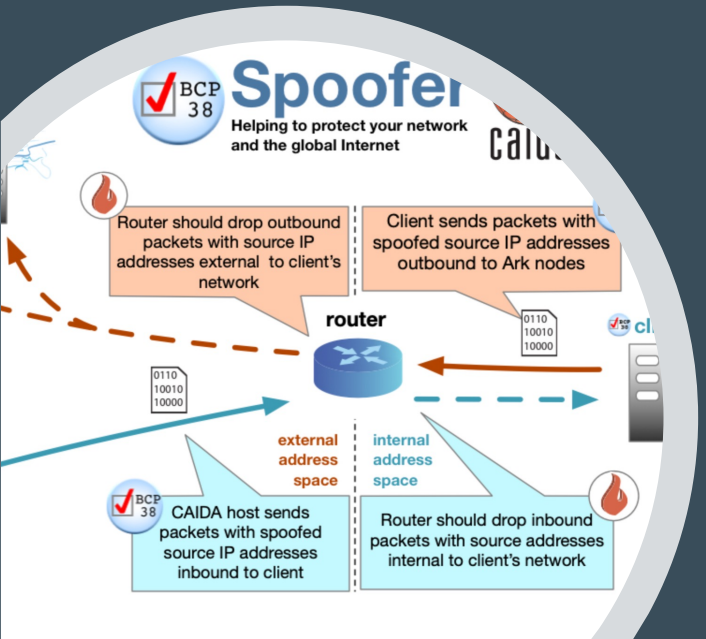
MANRS Actions and Implementation (NetOps)

Action 4, Global Validation
Facilitating validation of routing information on a global scale.
• Network operator is able to communicate to their adjacent networks which announcements are correct; • Network operator has publicly documented routing policy, ASNs and prefixes that are intended to be advertised to external parties.
route/route6 objects registered in one of the IRR databases; and ROAs published in the RPKI system

More details and sample configurations available at the MANRS Implementation Guide:
https://www.manrs.org/netops/guide/







Common Issues When Joining MANRS

1. Applying
2. Anti-spoofing data
3. For the region: Action 3

We usually aim to respond to your application within 2-3 days, can take up to a week.

Next?

Implement the actions and apply to become a participant

Thank you.

Hanna Kreitem

KREITEM@ISOC.ORG

LEARN MORE:
https://www.manrs.org

FOLLOW US:


/RoutingMANRS