MANRS

MANRS Community Report 2022

March 2023

manrs.org

Table of Contents

Executive Summary

Mutually Agreed Norms for Routing Security (MANRS) continued to grow in 2022, adding 136 participants for a total of 886 participants across its four programs. It also continued to encourage the adoption of Resource Public Key Infrastructure (RPKI) and Route Origin Validation (ROV), with over 66% of MANRS participants having valid ROAs compared with 34% globally, and 11% now implementing ROV, which is ultimately what MANRS is trying to encourage.

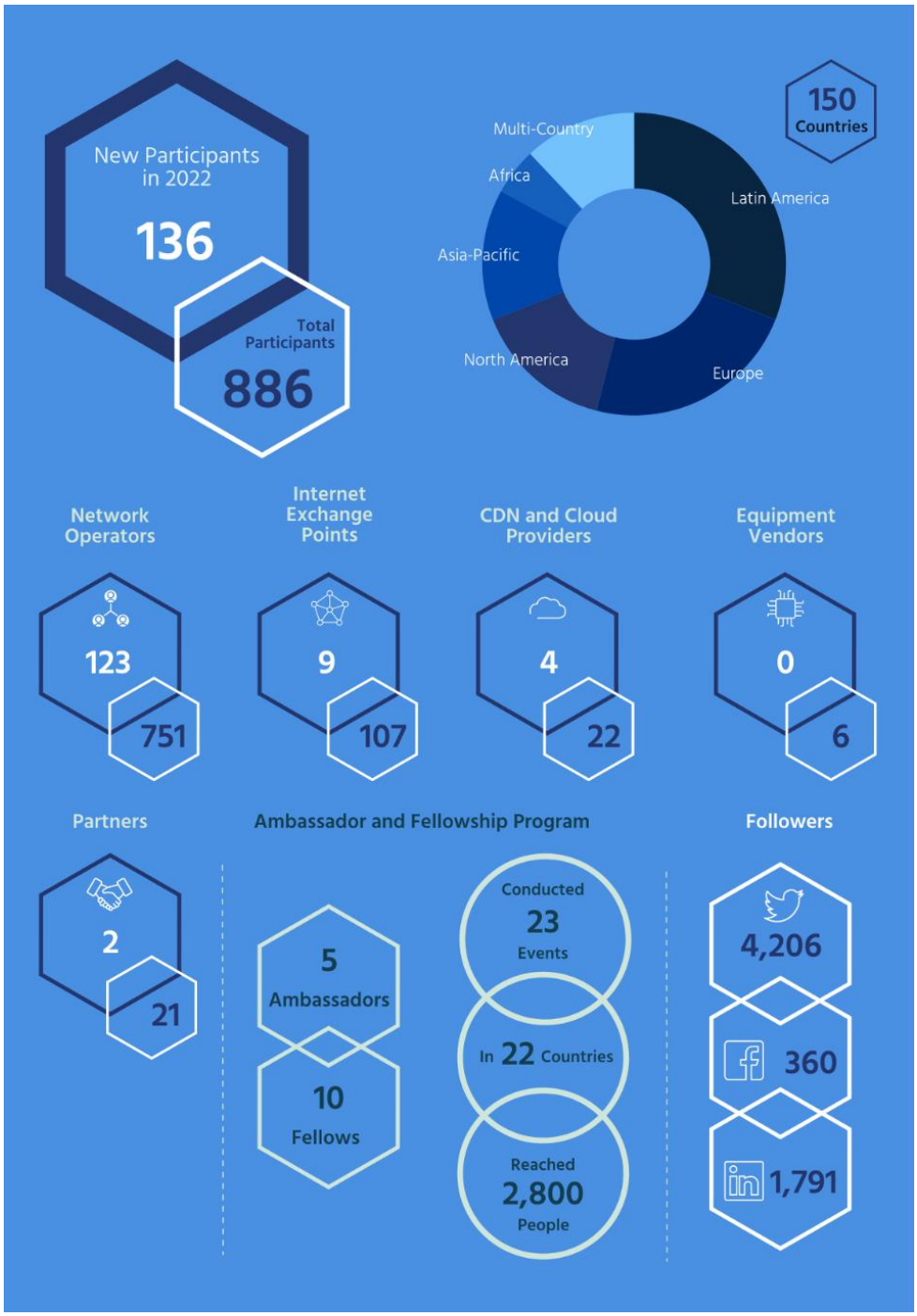
MANRS also responded to enterprise customer demand by establishing MANRS+, which aims to establish an elevated tier of participation for organizations that require greater security assurances and can comply with more stringent requirements. The MANRS+ Working Group was chartered to identify use cases and their requirements to develop an industry-recognized quality mark that can be understood by customers and used in their business decisions. This working group involves enterprises, network operators, and certification agencies both from within and outside of the MANRS community.

MANRS responded to the United States Federal Communications Commission (US FCC) Notice of Inquiry on Routing Security along with 45 other organizations and individuals, of whom 70% referenced MANRS. The European Union (EU) also adopted the MANRS Readiness Framework as a set of key Internet standards and has committed to biannual updates of MANRS readiness in member countries to improve Internet security across the EU. In addition, the Organisation for Economic Co-operation and Development (OECD) published a report for policymakers on "Routing security: BGP incidents, mitigation techniques, and policy actions" that referenced MANRS as an information source.

MANRS has been developing a relationship with the Forum of Incident Response and Security Teams (FIRST) community over the past three years and organized a full-day MANRS tutorial at the FIRST Conference 2022, which led to the creation of the Network Security Special Interest Group (NetSec SIG). This will help MANRS bring more routing security knowledge to 640 Computer Security and Incident Response Teams (CSIRTs) in 101 countries, who can bring this to their constituencies.

Reaching more people and encouraging more networks to become MANRS compliant means we all benefit from a more secure Internet. The MANRS team and Internet Society will work with the SIG to organize training and tutorials, and guide its participants on how to join MANRS.

MANRS at a Glance



About Us

Mutually Agreed Norms for Routing Security (MANRS) is a global, community-driven initiative. In 2014, a small group of network operators recognized the need to join forces to improve the security and resilience of the Internet's global routing system. With support from the Internet Society, MANRS was born.

Since then, the MANRS community has grown and expanded to empower and support not only network operators,[1] but also Internet Exchange Points (IXPs),[2] Content Delivery Networks (CDNs) and Cloud providers,[3] and equipment vendors[4] to implement the MANRS Actions[5] and reduce common routing threats. MANRS would not have been possible without the commitment of our community to strengthen global routing security.

By 2025, MANRS aims to become a self-governing community of participants and partner organizations[6] that drives global adoption of MANRS actions and improvements in routing security. Efforts toward achieving this goal include providing reliable tools[7] for compliance and measurement, such as the MANRS Observatory,[8] building capacity of network engineers and policymakers through training,[9] and the Ambassadors[10] and Fellows[11] program, and advocating for policies that strengthen routing security.

Per the MANRS Community Charter,[12] the MANRS Steering Committee[13] was established. It is comprised of individuals elected by MANRS participants to lead the community toward collective responsibility for the resilience and security of the Internet's global routing system. The first election[14] was held in November 2021, and the second election[15] for three seats was held in November 2022.

If you would like to learn about how your organization can support MANRS, please visit our website[16] or contact us.[17]

[1] https://www.manrs.org/netops/
[2] https://www.manrs.org/ixps/
[3] https://www.manrs.org/cdn-cloud-providers/
[4] https://www.manrs.org/equipment-vendors/
[5] MANRS actions are the compulsory and recommend actions that MANRS participants should be taking to improve the security and resilience of the Internet global routing system. There are defined actions for network operators, IXPs, CDN and cloud providers, and equipment vendors.
[6] Partner organizations do not operate a network but actively support MANRS goals. https://www.manrs.org/about/partners/
[7] https://www.manrs.org/resources/
[8] https://www.manrs.org/manrs-observatory/
[9] https://www.manrs.org/resources/training/
[10] https://www.manrs.org/ambassadors/
[11] https://www.manrs.org/fellows/
[12] https://www.manrs.org/about/governance/community-charter/
[13] https://www.manrs.org/about/steering-committee/
[14] https://www.manrs.org/2021/11/meet-the-manrs-steering-committee/
[15] https://www.manrs.org/2022/11/new-manrs-steering-committee-members/
[16] https://www.manrs.org/join/
[17] https://www.manrs.org/about/contact/

Our Impact in 2022

A Significant Milestone for Routing Security Reached

Globally in 2022, efforts to improve the security and resilience of the Internet's routing system passed a significant milestone[18] with more than 50 percent of advertised Internet Protocol version 6 (IPv6) address space having valid route origin authorizations (ROAs). This means that, for the first time, the majority of announced IPv6 address space is secured with Resource Public Key Infrastructure (RPKI)—a key tool in stopping route leaks and hijacks (Figure 1). While we cannot claim that this milestone is a direct result of MANRS, it demonstrates a growing sense of shared responsibility for improving routing security.

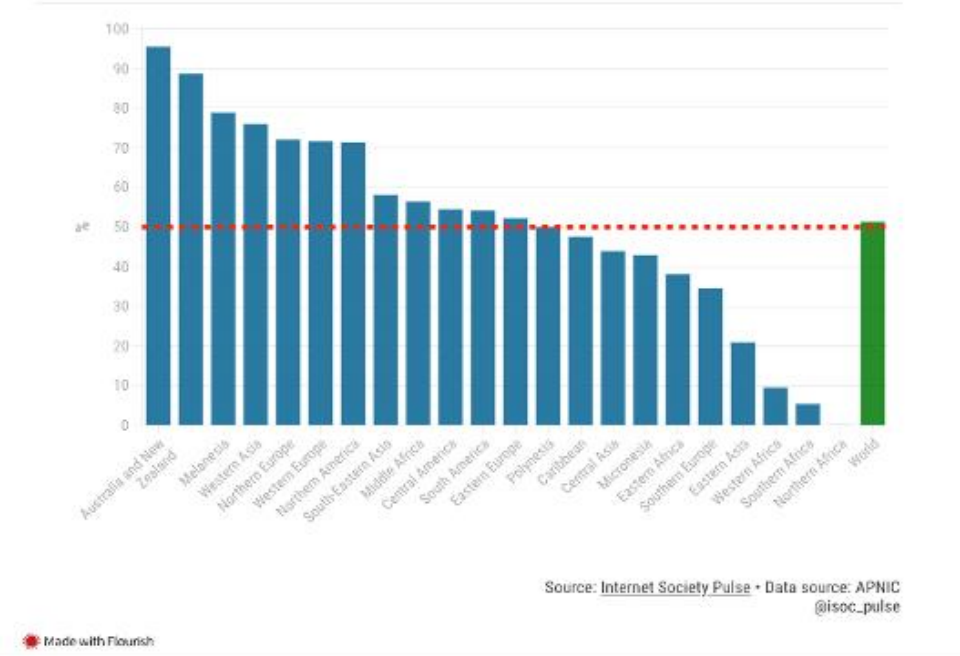


Figure 1. The regional variation in routing security: announced IPv6 address space covered by ROA, April 2022.

The overall figure, however, masks regional disparities—it is worth noting that Africa, Eastern and Central Asia, and Southern Europe are all still some way away from reaching this threshold. The IPv4 Internet is also several years behind IPv6 as only 33 percent of announced IPv4 address space is secured by an accompanying ROA.

[18] https://www.manrs.org/2022/04/majority-of-announced-ipv6-address-space-now-secured-by-roas/

ROA Creation by MANRS Participants Increased

At the end of 2021, 60.8 percent of MANRS' 750 participants had valid ROAs. By the end of 2022, this figure rose to 66.3 percent of 886 participants (Figure 2).

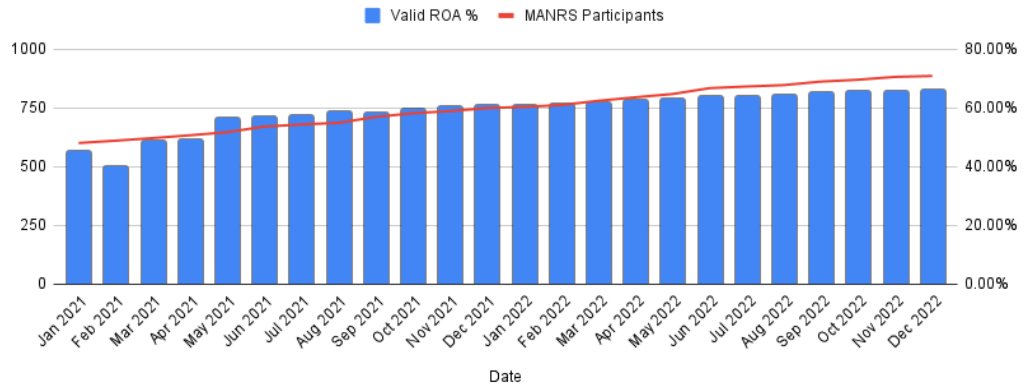


Figure 2. The percentage of MANRS Participants with Valid ROA, 2021-2022.

Working Group Established to Create MANRS+, an Elevated Tier of MANRS Participation

MANRS has traditionally focused on peer-to-peer relationships—forming a community of operators to make the Internet better and do the right thing for everyone. The strategy has been successful, as there are now nearly 900 MANRS participants across four programs. However, there are over 70,000 networks or autonomous system numbers (ASNs) on the Internet. While not every ASN must participate, as many of them are small networks with no major impact on the Internet, we need significantly more networks implementing MANRS actions to stop routing security incidents in their tracks.

We believe customer demand can be a driving force in increasing routing security. If we can enhance the business case for MANRS, customers will demand better routing security of their network connectivity providers and providers will ensure they are complying with the MANRS actions that mitigate routing security risks.

To this end, the community formed the MANRS+ Working Group[19] to discuss creating a second, elevated tier of MANRS participation for organizations that comply with more stringent requirements and auditing. Its charter[20] describes the working group's intention to create a significantly higher value proposition for a subset of the existing MANRS participants based on a credible quality mark it will represent, recognized by customers, and used in their business decisions. This quality mark and its implementation and conformance requirements assume better alignment with customer needs, leading to better security assurance. The MANRS+ Working Group is tasked with developing the requirements for MANRS+.

The MANRS+ Working Group is co-chaired by Matt Davies (Visa) and Andrei Robachevsky (Internet Society). Membership in the working group is open to everyone—MANRS participation is not required.

[19] https://www.manrs.org/about/manrs-working-group/

[20] https://www.manrs.org/about/manrs-working-group-charter/

MANRS' Governance Strengthened

The second election of the Steering Committee for three seats attracted eight high-caliber and diverse candidates,[21] which enabled a successful election in November of the following three members:

- Melchior Aelmans, Juniper Networks
- Musa Stephen Honlue, AFRINIC Ltd.
- Tony Tauber, Comcast

Together, they join six other Steering Committee members[22] to:

- Make recommendations on MANRS actions and minimum conformance criteria
- Supervise the auditing process for new applicants
- Handle the appeals process from applicants that have been refused approval
- Make recommendations on the suspension and termination of organizations from MANRS participation that fail to meet the minimum conformance criteria
- Supervise the incident-handling processes
- Appoint MANRS advisors who can offer specialist advice or act as liaisons with other communities

Monthly Conformance Reports Issued to All MANRS Participants

Starting from early 2022, monthly conformance reports[23] have been sent to MANRS participants providing their MANRS Readiness Scores[24] and potential non-compliance routing security incidents. We have been encouraging participants to send us feedback on the reports and verify incidents that the MANRS Observatory has detected to help us improve the quality of incident reporting. Some participants have used these reports to demonstrate their commitment to routing security (Figure 3).

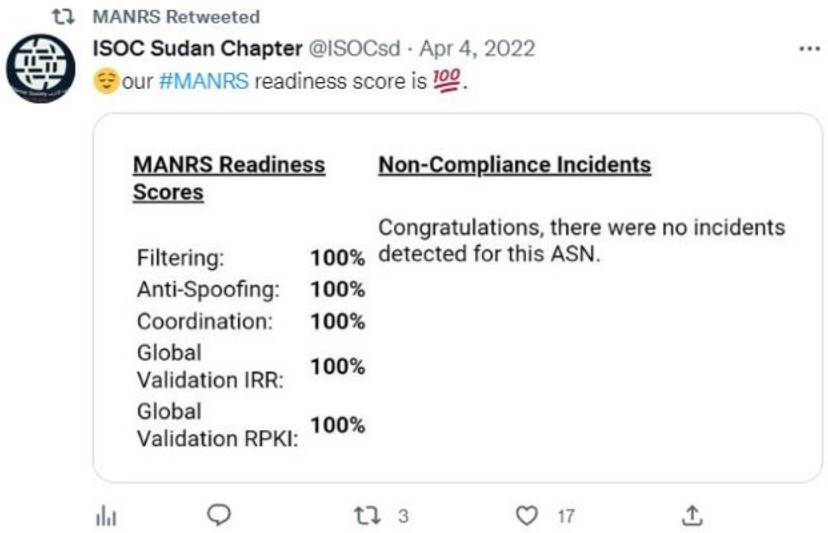


Figure 3. The Internet Society Sudan Chapter published its conformance report on Twitter.

[21] https://www.manrs.org/2022/10/meet-the-manrs-steering-committee-candidates/

[22] https://www.manrs.org/about/governance/steering-committee/steering-committee-members/

[23] https://www.manrs.org/2022/05/youve-got-mail-manrs-conformance-reports-and-incident-reporting/

[24] https://observatory.manrs.org/#/about

MANRS Community Reach and Engagement Broadened

The MANRS community is continuously reaching out to new audiences to create more awareness around MANRS, explain the steps to implement its actions, and convince more people running networks that routing security is an important aspect that deserves top consideration.

Over the years, we have developed a close relationship with the Forum of Incident Response and Security Teams (FIRST)[25] community. FIRST brings together security experts to exchange information and cooperate on issues of mutual interest, such as new vulnerabilities or attacks.

In June 2022, we held a full-day MANRS tutorial at the FIRST Conference in Ireland. The tutorial helped participants understand the basics of Border Gateway Protocol (BGP), how to implement the MANRS actions for network operators on different platforms, details of how RPKI works, and associated demos and exercises. By the end of the day, participants recognized the importance of routing security and discussed creating a Special Interest Group (SIG) inside FIRST. The day after the tutorial, participants gathered with other interested parties to submit a draft charter for the SIG to FIRST's Board for approval.

By August, the FIRST Board approved the creation of the Network Security Special Interest Group (NetSec SIG). This new SIG helps the MANRS community bring more routing security knowledge to a new audience, currently composed of 640 teams in 101 countries. Reaching more people and encouraging more networks to become MANRS compliant means we all benefit from a more secure Internet. The MANRS team and Internet Society will work with the SIG to organize training and tutorials, and guide its participants on how to join MANRS.

The EU Includes MANRS as a Key Internet Standard

The European Union (EU) has adopted the MANRS Readiness Framework,[26] based on five actions—filtering, anti-spoofing, coordination, validation with Internet Routing Registry (IRR), and validation with RPKI—as a set of key Internet standards. The EU has committed to half-yearly updates on member countries' MANRS readiness on an online dashboard[27] to encourage the uptake of MANRS actions and increase Internet security across the EU.

MANRS Contributed to the US FCC Notice of Inquiry on Routing Security

MANRS submitted comments[28] in response to the United States Federal Communications Commission (US FCC) Notice of Inquiry on Routing Security. As part of the process, a survey was conducted among MANRS participants. We also conducted an analysis[29] of all the submissions to the US FCC. Forty-five organizations or individuals filed 49 comments. Respondents included Internet service providers, trade associations, academics/researchers, and individuals.

Nearly 70 percent of the responses mentioned MANRS, some relying heavily on MANRS for recommendations (e.g., Microsoft), and many using MANRS articles and data as citations and references.

---

[25] https://www.manrs.org/2022/09/welcoming-the-new-first-netsec-special-interest-group/

[26] https://ec.europa.eu/internet-standards/manrs.html

[27] https://ec.europa.eu/internet-standards/

[28] https://www.manrs.org/2022/04/the-us-fcc-asked-about-routing-security-heres-what-manrs-participants-had-to-say/

[29] https://www.manrs.org/2022/10/manrs-and-the-us-fcc-notice-of-intent-on-routing-security/

"Microsoft encourages the FCC to highlight and support industry guidelines defined as part of the MANRS routing security program and advises the FCC to collaborate with the MANRS organization, which can provide the FCC with industry-tested leading practices, insights into the current risk-landscape, and future collaboration on Internet routing security."

An OECD Report for Policymakers Cites MANRS as an Important Resource

In a 2022 report for policymakers published by the Organisation for Economic Co-operation and Development (OECD) on "Routing security: BGP incidents, mitigation techniques and policy actions",[30] MANRS has been repeatedly listed as an information source.

In one of its recommendations, the report calls for governments to work with industry and technical experts on a framework that would establish targeted actions to improve routing security within a set time frame. It is a call for a multistakeholder approach, using MANRS as an example.

We encourage policymakers to work with network and infrastructure operators, critical infrastructure protection agencies, and standards bodies, among others, to improve global routing security while also preserving vital aspects of the system that have allowed the Internet to be open and universal.

Strategic Advocacy in Targeted Regions and Countries

As travel restrictions eased in 2022, we could physically participate in regional events and had our first face-to-face MANRS Community Meeting in 2.5 years at RIPE85 in Serbia in October. At RIPE85, we also organized a Best Current Operational Practices (BCOP) Task Force session.[31]

[30] https://www.manrs.org/2022/11/new-oecd-report-on-routing-security-for-policymakers/

[31] https://ripe85.ripe.net/programme/meeting-plan/bcop-tf/

Figure 4. The MANRS community participating at RIPE85 and SGNOG9.

The MANRS community continued to tirelessly advocate for MANRS across different regions throughout 2022. For example, in the Asia-Pacific region, at the Asia-Pacific Regional Internet Conference on Operational Technologies (APRICOT) 2022, REANNZ,[32] the first network operator in New Zealand to join MANRS, presented MANRS' work. Australia's Academic and Research Network (AARNet),[33] a MANRS participant, showcased MANRS at TNC22, the largest global research and education networking conference, held in Italy. MANRS Fellow, Indra Raj Basnet, raised awareness about MANRS at the South Asian Network Operators Group Conference (SANOG38).[34] Aftab Siddiqui, MANRS Project Lead, was invited to present the outlook of routing security in Singapore[35] at SGNOG9, using data from the MANRS Observatory.

In North America, MANRS participant Digital Ocean[36] shared its experience participating in MANRS at the North American Network Operators' Group Conference (NANOG86). Internet2,[37] a MANRS partner, introduced MANRS at a webinar organized by Research and Education Networks Information Sharing and Analysis Center (REN-ISAC), reaching out to the US research and education network community. In Latin America, the Internet Exchange Services Yucatán (IXSY), the

[32] https://2022.apricot.net/program/schedule-conference/#/day/10/securing-routing

[33] https://www.aarnet.edu.au/tnc22

[34] https://www.sanog.org/sanog38/program.html

[35] https://blog.apnic.net/2022/10/04/routing-security-in-singapore/

[36] https://www.youtube.com/watch?v=9MMz9t-BG5Y&list=PLO8DR5ZGla8jtquZaIDizi3q-GnoUgrQQ&index=20

[37] https://events.iu.edu/ren-isac/event/587453-webinar-introduction-to-manrs-mutually-agreed

National Association of Wireless Internet Providers (WISP MX), and various other organizations continued to engage with MANRS current and former fellows in training their community of network operators (Figure 5).

Figure 5. MANRS Fellows engaged in training network operators in Latin America.

In June, MANRS published a report on the status of RPKI in Australia and New Zealand.[38] The report finds that despite progress in the two countries, routing security remains in a poor state, exposing everyone to risks of data loss, theft, or interrupted critical services. The findings reiterate the urgency to accelerate the adoption of MANRS actions. As more network operators work together, the fewer incidents there will be and the less damage they can do.

Advancing Our Global Engagement

We stepped up our online global engagement efforts through a series of online tutorials, panels, and presentations during RPKI Week[39] in July (Figure 6), the MANRS Community Meetings,[40] and various webinars and meetings, such as those organized by Azion,[41] Health Information Sharing and Analysis Center (Health-ISAC),[42] and the Roma Internet Exchange Point (NAMEX).[43] This enabled us to engage diverse stakeholders in the community, including not only MANRS participants but also key infrastructure groups that knew little about routing security.

[38] https://www.manrs.org/2022/06/routing-security-a-work-in-progress-in-australia-new-zealand/

[39] https://www.manrs.org/event/rpki-week-2022/

[40] https://www.manrs.org/event/manrs-community-meeting-april-2022/

[41] https://www.azion.com/en/lp/webinar-secure-edge-networks/

[42] https://twitter.com/HealthISAC/status/1583467913599627264?cxt=HHwWgMCt9bDrzfkrAAAA

[43] https://nam2022.namex.it/

Figure 6. RPKI Week.

MANRS has actively used its website and social media in advocacy through Facebook,[44] Twitter,[45] and YouTube[46] since 2014, and in early 2021, started engagements on LinkedIn.[47] By the end of 2022, we had 4,206 followers on Twitter (777 joined in 2022), and we posted 125 tweets that generated about 1,500 likes. On LinkedIn, we had 1,791 followers (874 joined in 2022), and our 79 posts generated about 1,900 reactions. On Facebook, we had 360 followers (85 joined in 2022), and our 88 posts resulted in 418 reactions.

On the MANRS website, our team, partners, ambassadors, fellows, and MANRS advocates published 25 blog posts[48] in 2022. Every year, we investigate incidents that emphasize the vulnerability of the Internet routing ecosystem and how most of these incidents could be avoided. There were several major routing incidents in 2022 and the MANRS community took these opportunities to advocate for MANRS actions. For instance, in February, cryptocurrency platform KLAYswap[49] had a routing security incident that allowed hackers to steal about $1.9 million USD of digital assets. The MANRS blog[50] dug into the technical details and explained how MANRS actions can help us all. MANRS also looked into the attacks on Ukraine's services[51] and Apple.[52] However, it was not all gloom and doom as we also featured how Twitter's creation of ROAs for its IP resources guarded against a BGP hijack attempt in March.[53]

[44] https://www.facebook.com/RoutingMANRS/
[45] https://twitter.com/RoutingMANRS
[46] https://www.youtube.com/@RoutingMANRS/featured
[47] https://www.linkedin.com/company/routingmanrs
[48] https://www.manrs.org/blog/
[49] https://medium.com/klayswap/klayswap-incident-report-feb-03-2022-70ff124aed6b
[50] https://www.manrs.org/2022/02/klayswap-another-bgp-hijack-targeting-crypto-wallets/
[51] https://www.manrs.org/2022/03/did-ukraine-suffer-a-bgp-hijack-and-how-can-networks-protect-themselves/
[52] https://www.manrs.org/2022/07/for-12-hours-was-part-of-apple-engineerings-network-hijacked-by-russias-rostelecom/
[53] https://www.manrs.org/2022/03/lesson-learned-twitter-shored-up-its-routing-security/

MANRS Virtual Training

In addition to the self-paced online tutorials on MANRS[54] available in English, Spanish, and French, a virtual four-week, instructor-led MANRS course[55] in English, Spanish, and French was organized during the last quarter of 2022. The next course is planned for January 2023.

MANRS-sponsored Research Paper Published by Passive and Active Measurement Conference 2023

A research study entitled, "RPKI Time-of-Flight: Tracking Delays in the Management, Control, and Data Planes," was accepted by the Passive and Active Measurement Conference 2023.[56] This is the first comprehensive study to measure: (1) the entire ecosystem of ROA manipulation by all five Regional Internet Registries, propagation on the management plane to Relying Parties and to routers; (2) the effects on BGP as seen by global control plane monitors; and (3) the effects on data plane latency and reachability.

MANRS' research agenda is largely driven by the Ambassadors and Fellows program. In 2022, the research team focused on building tools and data pipelines to gain better insights into the state of routing security globally. They include:

1. The study of the lifecycle of blackhole prefixes and how they are protected by RPKI, and the use of BGP blackholing at IXPs to mitigate distributed denial-of-service attacks.
2. The study of RPKI validation cycles of widely-used Relying Party software to understand how they operate and identify possible bottlenecks that degrade overall validation time.
3. The development of a novel technique to measure the deployment rate of route origin validation (ROV) globally.

Continuous Improvement of the MANRS Website and Observatory

The MANRS Observatory,[57] launched in August 2019, is an online tool that monitors Internet routing security by aggregating data from trusted sources into a user-friendly dashboard for viewing routing incidents and checking general routing health. The MANRS Observatory brings increased transparency to routing operations and sheds light on trends in routing security globally, regionally, and for individual networks so that improvements are made based on evidence.

The MANRS Observatory dashboard gives a high-level overview of the state of routing security, MANRS readiness, and statistics for specific regions and economies. MANRS readiness indicates how well MANRS actions are implemented and is calculated using a set of metrics for each action, computed from different data sources. The MANRS Observatory dashboard is open to the public, but MANRS participants can access detailed statistics and conformance reports for their specific networks. Partner accounts are available for individuals or organizations to support research on routing security and efforts in promoting MANRS.

[54] https://www.manrs.org/resources/training/tutorials/

[55] https://www.internetsociety.org/learning/manrs/

[56] https://pam2023.networks.imdea.org/accepted/

[57] https://observatory.manrs.org/#/about

In 2022, MANRS continued to improve conformance measurements[58] and the data quality and tools[59] to assess the health of the global routing table. We have been working with researchers and network operators to facilitate the development of improved data quality and tools. They include:

- A tool to help detect Type-1 BGP hijacks (AS path manipulation).
- PyBGPKIT API, an API backend that provides RESTful API access to BGPKIT software and data offerings using PyBGPKIT. This tool is useful when investigating the causes of routing incidents.
- ROA History is a tool that collects historical RPKI data from RIPE Network Coordination Centre's RPKI repository. It provides an API that allows users to check whether a prefix was covered by a ROA in the past.
- The Shutdown and Hijack Measurement and Identification Tool (SHMIT) offers better insight into when and how anomalies in BGP happen.

Moreover, MANRS added new features[60] to its website to better highlight community contributions to routing security and streamline access to MANRS resources. One key change is the live MANRS Observatory dashboard on the MANRS homepage, showing the state of global routing security in real time. Another new feature is the total number of participants right on the homepage. Under the new Community tab, you can find information about Ambassadors and Fellows, training, and events. The Resources tab carries links to our reports, tools, and promotional materials.

[58] https://www.manrs.org/2022/06/configuration-issue-penalizing-single-digit-asns/

[59] https://www.manrs.org/2022/04/rfc-7911-what-happens-when-routers-do-not-speak-the-same-language/

[60] https://www.manrs.org/2022/06/new-features-on-the-manrs-website/

Community Spotlight

The MANRS community comprises participants, partners, ambassadors, and fellows.

As of 31 December 2022, there were 886 MANRS participants made up of network operators, IXPs, CDNs, cloud providers, and equipment vendors implementing MANRS actions. The network operators secure customer-provider interconnections, equipment vendors ensure network equipment has the right features and support, while IXPs, CDNs, and cloud providers create a secure network peering environment and encourage good routing practices from their members, customers, and partners. MANRS partners do not necessarily operate networks but actively support MANRS goals. We are pleased to welcome two new partners in 2022—Code BGP and Cyber Security Agency of Singapore—and a total of 136 new MANRS participants.

Here are what some of the participants and partners have said about MANRS.[61]

Danny McPherson, Executive Vice President and Chief Security Officer, Verisign

> "MANRS aims to reduce the most common routing system vulnerabilities by creating a culture of collective responsibility toward the security, stability, and resiliency of the global routing system. MANRS is continuing to gain traction, guiding Internet operators on what they can do to make the routing system more reliable.

Luis Fiallo, Global Growth Technology Executive and Board Member, China Telecom Americas

> "I'm very pleased that we recently celebrated one year of having all of our global affiliates' backbone networks validated by MANRS. We're proud to say that our participation in MANRS has resulted in more secure networks with no major routing issues for our customers.

Sebastian Becker, Global Peering Manager and Principal Engineer, Deutsche Telekom

> "Being MANRS compliant not only improves our own routing security capabilities, but has the potential to help others improve theirs. This is an opportunity for us to make a significant contribution to global routing and securing a reliable and scalable Internet ecosystem for generations to come.

Geoff Houston, Chief Scientist, APNIC

> "MANRS offers a well-structured and carefully thought through approach to best current practices in routing security and is clearly the best program in the industry today in this area.

Stefan Gulinck, Network Architect, BNIX

> "The importance of MANRS can not be understated because of the critical challenges the routing on the Internet faces. Being the biggest Internet exchange in Belgium, it is crucial that we contribute to a stronger route security and evangelize this to our community.

[61] For more testimonials, see https://www.manrs.org/about/testimonials/

Zhang Gao Yi,Project Leader, Huize Network

"MANRS is an organization that promotes a more secure Internet infrastructure. As a research organization with a broad membership, including students, researchers, and practitioners, our goals are broadly aligned with those of MANRS.

Walisson Gois, Network Engineer, Brasil Digital

"Nosso objetivo é alcançar uma internet segura e estável. As recomendações do MANRS nos ajudam a alcançar esse objetivo e também manter nossa organização segura. Garanto que se todos seguissem essas recomendações já estaríamos em uma internet de exelência.

MANRS Ambassadors and Fellows Program

In 2022, five ambassadors[62] and 10 fellows[63] completed the third cohort of the MANRS Ambassadors and Fellows program.

Ambassadors[64] (Figure 7) are representatives from current MANRS participants who provide mentorship, guidance, and feedback to fellows in the routing security community. In 2022, two fellows from 2021—Musa Stephen and Romain Fontugne—returned as ambassadors.

Figure 7. Meet the 2022 MANRS Ambassadors.

[62] https://www.manrs.org/ambassadors/2022-manrs-ambassadors/

[63] https://www.manrs.org/2022/04/announcing-2022-manrs-fellows/

[64] https://www.manrs.org/ambassadors/

Fellows[65] are emerging leaders who believe that routing security is essential and are ready to contribute to its improvement. The fellowship allows individuals to bring new perspectives, innovative ideas, and research experience into the MANRS work to improve routing security. Ambassadors and fellows from different countries work together in three areas—training, research, and policy—to train diverse communities on good routing practices, research ways to secure routing, and survey the global policy landscape, respectively.

Together, they carried out 23 interventions, including training, meetings, and presentations on MANRS and routing security. They reached at least 2,800 people from 22 countries in Africa, the Asia-Pacific, Europe, and Latin America. In some events, fellows from the 2021 cohort also participated (Figure 8).

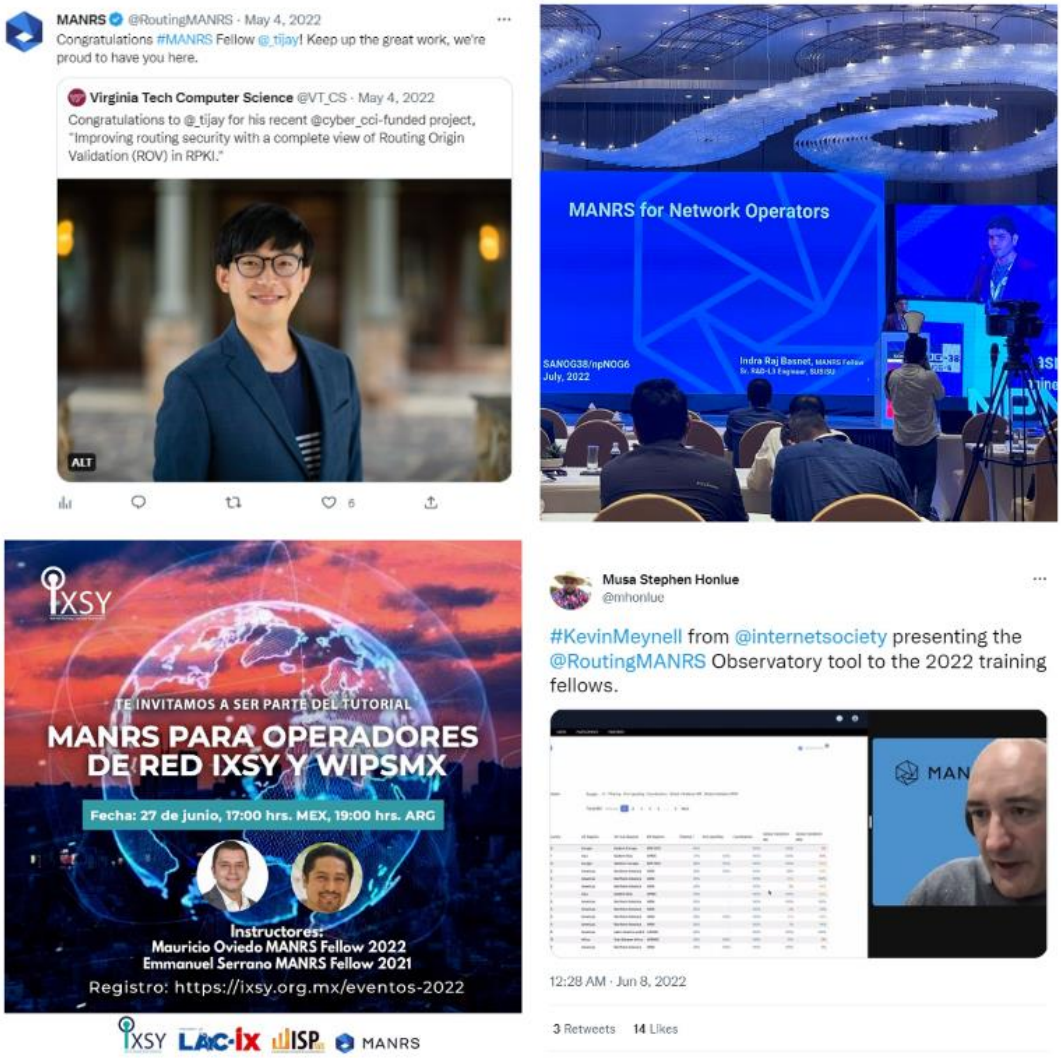


Figure 8. A selection of activities under the Ambassadors and Fellows program.

[65] https://www.manrs.org/fellows/

Challenges and Lessons Learned

Even though ROA adoption is picking up in some regions, as indicated at the start of the report (Figures 1 and 2), the adoption rate is generally low. While the global valid ROA count increased by about seven percentage points from 35 percent in December 2021 to 42 percent in December 2022, it is not good enough yet to secure global routing.

Convincing people to implement basic routing security measures is challenging. Often it is not technology that is the impediment, but more of a mental or psychological barrier to understanding why one would want to secure a network. It is easy to assume if a network isn't broken, there is nothing to fix—but, in fact, routing still has major problems that are not always visible or predictable based on one network's behavior, and it is every operator's responsibility to contribute to the solution. Action requires behavioral change, which comes from acknowledging the consequences of not putting in responsible routing security measures. The MANRS community is driving this behavioral change toward more secure routing.

Looking Ahead

MANRS is now established as the leading routing security program, recognized by the Internet industry and policymakers, and increasingly by enterprises relying on Internet services. We develop best practices in collaboration with the Internet industry, develop and maintain the MANRS Observatory to monitor the state of global routing security, and provide information sharing and capacity building to encourage the implementation of good routing security practices.

In 2023, we are excited to develop MANRS+ with the community. MANRS will continue to advocate participation among network operators, IXPs, CDNs, cloud providers, and equipment vendors, and their uptake in implementing routing security measures with the following targets:

- Increase conformance of MANRS participants by 10 percent.
- Encourage five MANRS participants to join the Internet Society as organization members.
- Grow the MANRS community with the addition of 10 organization members and 10 IXPs.

Over the coming year, MANRS will strengthen and add to its best practices, including developing these into recognized standards. As routing security has gained the attention of policymakers, MANRS will also be monitoring and providing inputs where appropriate to regulatory developments as these happen.

We will continue to transition to a self-governed community of network operators, IXPs, CDNs, cloud providers, equipment vendors, and partner organizations that drives global adoption of MANRS actions and improvements in routing security. We will also continue to offer leadership initiatives, such as the MANRS Ambassadors and Fellows program (which will be renamed as the MANRS Mentors and Ambassadors program in 2023), build strategic partnerships to expand our outreach and engagement, and improve data quality and tools on the MANRS Observatory to guide decision-making. We recently launched the MANRS API in February 2023.

The Internet Society has funded the MANRS initiative since its inception, but now it needs your support to continue to grow and strengthen the routing security community. We are therefore looking for industry sponsors who are interested in supporting the MANRS Observatory, the Mentors and Ambassadors program, and its community events, including the Routing Security Summit.

If you are a MANRS participant, please consider becoming an Organization Member of the Internet Society[66] to help us continue to secure the global Internet for everyone.

[66] https://www.internetsociety.org/about-internet-society/organization-members/