MANRS

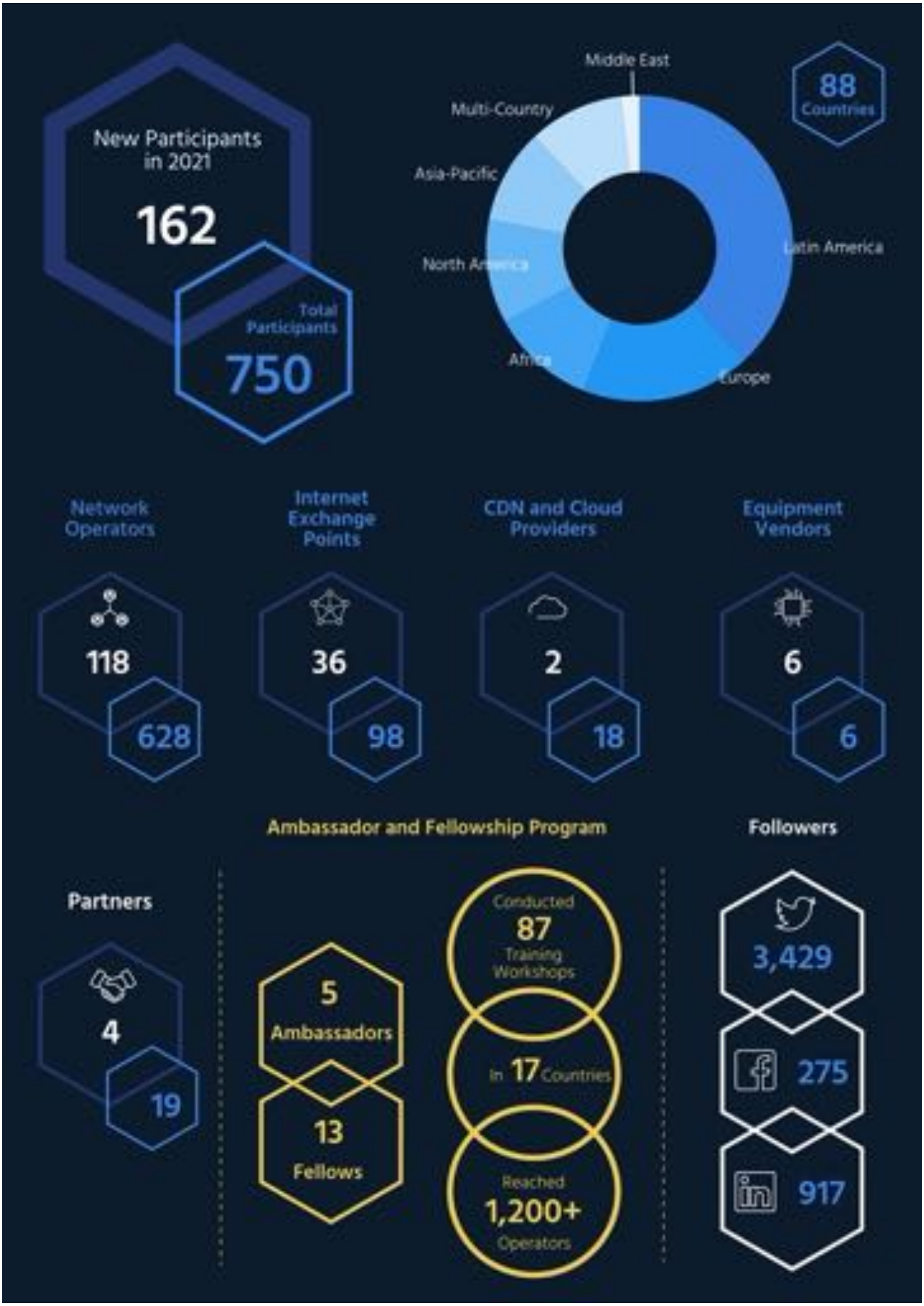
MANRS Community Report 2021

January 2022

manrs.org

Table of Contents

1. MANRS at a Glance



2. 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, and 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 network (CDN) and cloud providers,[3] and equipment vendors[4] to take MANRS actions[5] and reduce common routing threats. MANRS would have not been possible without the commitment of our community to strengthen global routing security.

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

In early 2020, the MANRS Advisory Group[11] was established to provide oversight of the MANRS application and auditing processes, enhance MANRS actions by developing conformance criteria, and participate in the selection of MANRS ambassadors and fellows. The MANRS Advisory Group worked with the MANRS community[12] to develop the MANRS Community Charter,[13] which provides guiding principles for the future governance of MANRS. The charter was accepted by the community after several rounds of consultations and came into effect on 1 November 2021.

In accordance with the MANRS Community Charter, the Advisory Group will transition to a Steering Committee comprised of individuals elected by the MANRS community. MANRS elected its first Steering Committee[14] in November 2021 to lead the community towards collective responsibility for the resilience and security of the Internet's global routing system. The first Steering Committee meeting was held in December bringing together the newly elected members.[15]

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/isps/

[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://observatory.manrs.org/#/about

[9] https://www.manrs.org/resources/training/

[10] https://www.manrs.org/ambassadors-programme/fellows/

[11] https://www.manrs.org/about/advisory-group/

[12] https://www.manrs.org/2021/04/feedback-requested-chartering-the-manrs-community/

[13] https://www.manrs.org/about/governance/community-charter/

[14] https://www.manrs.org/about/steering-committee/

[15] https://www.manrs.org/2021/11/meet-the-manrs-steering-committee/

[16] https://www.manrs.org/join/

[17] https://www.manrs.org/about/contact/

3. Our Impact in 2021

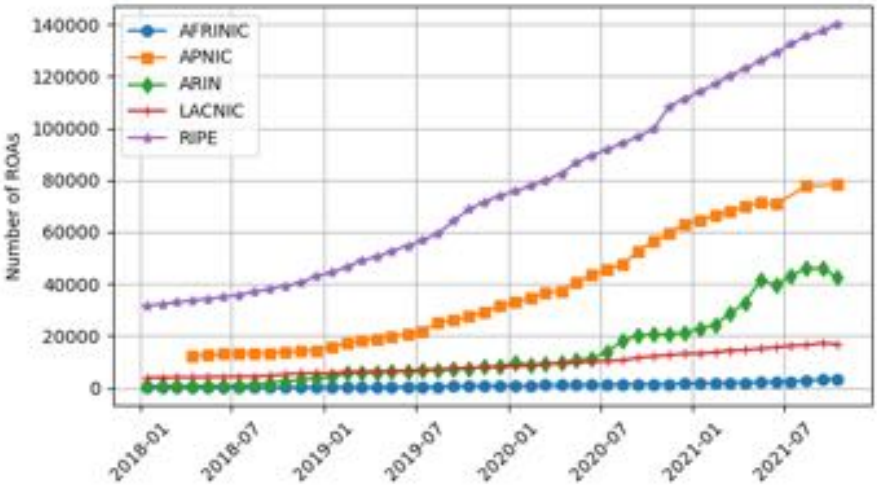
MANRS 2021 Targets Achieved

In 2021, we exceeded the set target of a 10 percent increase in route origin authorization (ROA) creation by MANRS participants, showing they support cryptographic validation of Internet Protocol (IP) address ownership. MANRS participants had a 17 percent increase in valid ROA count between January and December 2021.

We also exceeded the set target of a 5 percent increase in route origin validation (ROV) implementation by MANRS participants, showing they are checking that a given network is authorized to announce routes to a given IP address range. By the end of 2021, 68 network operators, or 9 percent of MANRS participants, were implementing ROV.

Global trend points to a substantial increase in the number of registered ROAs in the past few years, particularly in Europe, Asia-Pacific, and North America (Figure 1). This shows that resource public key infrastructure (RPKI)—a key tool in stopping route leaks and hijacks—is finally lifting off.

Figure 1. Number of ROAs, 2018-2021



MANRS' Governance Strengthened

The first election of the Steering Committee attracted 34 high-calibre and diverse candidates,[18] which enabled a successful election in November of the following seven members:

- Melchior Aelmans, Juniper Networks
- Nick Hilliard, INEX
- Flavio Luciani, NAMEX
- Arnold Nipper, DE-CIX
- Arturo Servin, Google
- Jeff Tantsura, Microsoft
- Tony Tauber, Comcast

Andrew Gallo (George Washington University) and Warrick Mitchell (Australia's Academic and Research Network), Advisory Group co-chairs, will also serve on the Steering Committee. A total of 148 participants took part in the voting process.

[18] https://www.manrs.org/about/steering-committee/nominations/

The Steering Committee members will hold quarterly meetings 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; and appoint MANRS advisors who can offer specialist advice or act as liaisons with other communities.

New MANRS Program for Network Equipment Vendors Launched

2021 added a fourth MANRS program to empower and support equipment vendors[19] to take MANRS actions and reduce common routing threats by making sure that network equipment, like routers and switches, has the right features and support. The MANRS Equipment Vendor Program has two mandatory actions and one commitment:[20]

- Action 1 – Provide relevant security features so network operators, IXPs, CDNs, and cloud providers can take MANRS actions to prevent incorrect routing information and IP address spoofing.
- Action 2 – Promote MANRS through training and technical content.
- Commitment to actively participate in the MANRS community to advise members, develop solutions, contribute to routing security resources, and promote MANRS.

The five founding participants are global leaders in network equipment—Arista, Cisco, Huawei, Juniper, and Nokia.[21] Arrcus, Inc. joined later with others expected to join soon.

Having five of the leading network equipment vendors in the world working together with the MANRS community to launch the new Equipment Vendor Program demonstrates the importance of routing security in making the Internet safe for business and consumers alike.

~ Andrei Robachevsky, Senior Director of Technology Programs, Internet Society

---

CDN and Cloud Providers Improve Routing Security with Expanded and Improved MANRS Actions

MANRS launched the CDN and Cloud Providers Program in 2020, setting a baseline for routing security actions they should take. Within months, participants realized they could raise the bar to make the program stronger and produce a bigger impact on the Internet. Participants from Akamai, Amazon, Azion, Cloudflare, Comcast, Facebook/Meta, Google, Microsoft, Netflix, Verisign, and Vultr formed a taskforce to strengthen the actions and ask more of each other and their colleagues.

In March, the MANRS community adopted the taskforce's recommendations, and the expanded actions officially became part of the MANRS CDN and Cloud Providers Program.[22] The updated actions set higher expectations for routing security

[19] https://www.manrs.org/2021/09/new-manrs-program-gathers-network-equipment-vendors-to-improve-internet-routing-security/

[20] https://www.manrs.org/equipment-vendors/

[21] https://www.internetsociety.org/news/press-releases/2021/arista-cisco-huawei-juniper-and-nokia-launch-new-manrs-equipment-vendor-program-to-improve-routing-security-worldwide/

[22] https://www.manrs.org/2021/03/cdn-cloud-providers-improve-routing-security-with-expanded-improved-manrs-program-actions/

by strengthening filtering controls and clarifying their implementation guidelines, encouraging more concrete technical and operational commitments, and facilitating coordination among participants.

The two primary enhancements are:

- Fostering RPKI as the primary technology for validation of routing information on a global scale – CDN and cloud providers commit to use ROV as part of their filtering policy for peering relationships and register all their prefixes in RPKI.

- Improving consistency of route validation based on route objects published in an Internet Routing Registry (IRR), so that peers face a consistent requirement when interconnecting with any MANRS CDN or cloud provider – This defines a standard process for collecting all necessary routing information to build an effective filtering policy. In particular, it standardizes the procedure of expanding the AS-SET object, which is used to document the downstream customers of a peer network.

To support the implementation of these commitments, the taskforce developed new guidelines for managing ROAs for operators of RPKI services.[23] It introduced best practices centered around consistent validity, consistent application programming interfaces (APIs), health metrics for RPKI infrastructure, and change integration with routing plane.

MANRS Community Reach and Engagement Broadened

To further broaden the MANRS community, four MANRS Primers[24] were developed for policymakers,[25] business executives,[26] IT executives,[27] and computer security incident response teams (CSIRTs).[28] The primers are available in three languages—English, French, and Spanish. These primers explain in simple language what routing security is, why it matters to different groups, and how MANRS can help.

In the effort to improve engagement with the MANRS community, MANRS moved the implementation guides, policy briefs, and program actions to GitHub, which allows the community to edit these documents. To streamline this process, a GitHub management tutorial was arranged that was very well attended by the community.

Continuous Improvement of the MANRS Observatory and Development of New Tools

The MANRS Observatory,[29] 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 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 Observatory dashboard is open to the public, but MANRS participants can access detailed statistics and reports for specific networks. Partner accounts are available for individuals or organizations to support efforts in promoting MANRS and routing security.

[23] https://www.manrs.org/2021/11/manrs-task-force-develops-new-guidelines-for-managing-roas/

[24] https://www.manrs.org/resources/primers/

[25] https://www.manrs.org/resources/primers/policymakers/

[26] https://www.manrs.org/resources/primers/enterprises/

[27] https://www.manrs.org/resources/primers/it-executives/

[28] https://www.manrs.org/resources/primers/csirts/

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

In 2021, MANRS continued to add new data sources[30] and features[31] to improve the Observatory based on community and user feedback. The updated version 3.1 includes:

- Addition of a new data source on routing mis-originations—the Global Routing Intelligence Platform (GRIP)—to identify Border Gateway Protocol (BGP) security incidents, including sophisticated prefix hijacking attacks and misconfigurations.
- A toggle switch allowing users to select data source for routing mis-origination incidents—BGPStream or GRIP—and a detailed report that presents information from both sources, allowing users to compare the data and get a more informative picture of how their networks operate.
- The ability to validate data and provide user feedback. For each of the routing mis-origination incidents there is a small icon with a comment box, opening a dialog to respond to that incident. Feedback allows MANRS to implement controls to reduce the number of false positives (when a legitimate BGP announcement is marked as a routing incident).
- Improvements to the public user interface, including clearer layout of the overview page, expanded contextual help, trend arrows in MANRS readiness scores, and pop-up information when hovering over the world map.
- New features for MANRS participants, including pagination and data exports, and improved partner accounts.

In addition, MANRS launched the ROA Stats Tool[32] to help network operators and researchers see the state of RPKI around the world by providing an overview of ROAs, valids, and invalids created by country or by Autonomous System Number (ASN), with data updated daily. It gives a snapshot of the current situation, but also a historical view of ROAs and validation. Complementing the ROA Stats Tool, the Internet Initiative Japan Research Lab launched a visualization tool,[33] created by MANRS fellow, Romain Fontugne,[34] for looking at ROAs, valids, and invalids, among other data.

Strategic Advocacy in Targeted Regions and Countries

The MANRS community, including ambassadors and fellows, was engaged in about 150 events during 2021 at global, regional, and local levels. MANRS' online global advocacy efforts through webinars, social media platforms, and online events, such as a series of five webinars during RPKI Week,[35] MANRS Community Meetings,[36] and Tech Talks[37] resulted in significant engagement with the community. RPKI Week was attended by more than 500 participants. MANRS also participated in global and regional events like the ENISA Telecom Security Forum, FIRST Conference on Computer Security Incident Handling, FIRST & AfricaCERT Virtual Symposium for Africa and Arab Regions, and RightsCon.

In 2021, MANRS collaborated more closely with participants, partners, and Internet Society members to organize webinars and other events. At the regional level, MANRS continued to work closely with all five Regional Internet Registries (RIRs) in Africa (AfriNIC), Asia-Pacific (APNIC), North America (ARIN), Latin American and the Caribbean (LACNIC), and Europe (RIPE NCC), as well as with regional network operator groups such as those in Africa (AfNOG), Asia-Pacific (APNOG), the Caribbean (CaribNOG), North America (NANOG), the Pacific (PacNOG), and South Asia (SANOG), and with global and regional partners like the Arab States Research and Education Network (ASREN), Cybersecurity Tech Accord, EURO-IX, NAMEX, Network Startup Resource Center (NSRC), and SAMENA Telecommunications Council.

[30] https://www.manrs.org/2021/07/new-data-source-feedback-loop-enhance-manrs-observatory/

[31] https://www.manrs.org/2021/04/manrs-observatory-update-improves-user-interface-partner-accounts/

[32] https://www.manrs.org/2021/07/introducing-manrs-roa-stats-tool/

[33] https://ihr.iijlab.net/ihr/en-us/rov

[34] https://www.manrs.org/2021/11/the-routing-game-hunting-invalid-routes/

[35] https://www.manrs.org/resources/upcoming-events/rpki-week/

[36] https://www.youtube.com/playlist?list=PL-p9v0NMlDhJC_-yLrXIKZzxdIHAgiSGF

[37] https://www.youtube.com/playlist?list=PL-p9v0NMlDhKyeHIOkp6pv97H6XefNjys

At RPKI Week, for example, MANRS partnered with all five RIRs and launched how-to videos with their help. At the 2021 OMREN Technology Summit in May, a gathering of national research and education networks (NRENs) organized by the Oman Research and Education Network (OMREN), MANRS was recognized as one of the best practices for NRENs and cited multiple times during the event. It was mentioned by David Wilde, Chief Technology Officer of Australia's Academic and Research Network, as the first recommendation for NRENs to protect themselves. Jim Ghadbane, President and Chief Executive Officer of CANARIE, Canada said that he hopes all NRENs would implement MANRS actions to help secure networks. MANRS hosted a booth at the event and received interest from regional networks and the community.

MANRS deepened engagement with the International Telecommunication Union (ITU), and contributed to capacity building in Africa for the newly approved ITU standard titled, "Framework for the operation and services of Cyber Defence Centres/CSIRTs". In Africa, MANRS also conducted workshops with UbuntuNet Alliance, the regional research and education network organization for Eastern and Southern Africa.

In Asia-Pacific, MANRS continued to engage with the Asia-Pacific Regional Internet Conference on Operational Technologies (APRICOT), Asia-Pacific Regional Internet Governance Forum (APrIGF), Asia-Pacific Telecommunity (APT), and Pacific Islands Telecommunications Association (PITA).

MANRS also targeted advocacy in specific countries such as China, India, Lao PDR, Mongolia, Nigeria, Oman, Sweden, Tuvalu, UK, Uruguay, and USA. Advocacy efforts were targeted at a diverse range of stakeholders including governmental and non-governmental organizations, the private sector, research and education networks, and the technical community. For example, in Lao PDR, Mongolia, and Tuvalu, MANRS in collaboration with APT organized high-level sessions on IXPs and routing security in August with governments. MANRS also participated in national network operator and IXP events through collaborations with bdNOG, cmNOG, HKNOG, INNOG, KeNOG, MexNOG, phNOG, RSNOG, SAFNOG, SomNOG, UKNOF, and VNIX-NOG, among others.

MANRS has actively used its website and social media in advocacy through Facebook,[38] Twitter,[39] and YouTube[40] since 2014, and in early 2021, started engagements on LinkedIn[41] garnering over 900 followers in less than a year. By the end of 2021, we had a total of 3,429 followers on Twitter (1,372 of whom joined in 2021), we posted 427 tweets and had 6,100 engagements. The MANRS Twitter account was verified (blue checked) in October 2021, gaining a mark of notability and credibility, and further strengthening MANRS' brand and following.

On the MANRS website our team, partners, ambassadors, fellows, and MANRS advocates posted a total of 38 blogs.[42] There were several major routing incidents in 2021, including in February,[43] April,[44] and October,[45] and the MANRS community took these opportunities to advocate for MANRS actions.

MANRS' Virtual Training Boosted

As travel restrictions persisted in 2021 due to COVID-19, MANRS worked with partners to strengthen our virtual training platform and delivery to help develop the next generation of routing security experts. MANRS delivered four rounds of the moderated five-week MANRS online workshop using a new learning management system with hands-on lab training. MANRS also supported global and regional training workshops on routing security, such as the annual APRICOT events that normally offer the unique combination of interacting with peers from different economies, learning from industry leaders, and sharing and resolving technical issues together. However, offering these same benefits in a virtual

[38] https://www.facebook.com/RoutingMANRS/

[39] https://twitter.com/RoutingMANRS

[40] https://www.youtube.com/channel/UC4v8wZysf5yA9HtoBBmDleg

[41] https://www.linkedin.com/company/routingmanrs

[42] https://www.manrs.org/news/

[43] https://www.manrs.org/2021/02/major-route-leak-by-as28548-another-bgp-optimizer/ and https://www.manrs.org/2021/02/did-someone-try-to-hijack-twitter-yes/

[44] https://www.manrs.org/2021/04/a-major-bgp-hijack-by-as55410-vodafone-idea-ltd/

[45] https://www.manrs.org/2021/10/facebook-has-good-manrs-mistakes-still-happen/

environment was challenging. At APRICOT 2021,[46] MANRS partnered with APNOG and NSRC to offer multiple streams of virtual tutorial setup with hands-on experience that provided a mentoring-like environment for the participants to benefit from industry experts. The training platform allowed participants to manage their own virtual machines and enable experiential learning.

In Latin America and the Caribbean, MANRS, LAC-IX, and LACNIC worked together to promote the implementation of MANRS actions for the region's IXPs through webinars and training courses. LACNIC created a training plan made up of a series of four, two-hour modules for IXPs, covering the use of BGP, RPKI, DNS, and IPv6 at IXPs.

Engagement with Internet Society Chapters and Partners in Training and Events

In 2021, a milestone was achieved when the Internet Society Sudan Chapter, which runs the country code top-level domains (ccTLDs), became the first chapter to join MANRS.[47]

MANRS collaborated with other Internet Society chapters and partners in accelerating our capacity building efforts in Benin and Cameroon. The Benin Chapter launched a routing security initiative with the goal of supporting network operators in securing Internet routing by applying MANRS actions. In Cameroon, the Cameroon Chapter organized a series of webinars on routing security, and in partnership with the Cameroon IXP (CAMIX) and the National Agency for Information and Communications Technology (ANTIC), held a training workshop for network operators on MANRS and routing security during November and December (Figure 2).[48]

In addition, awareness of MANRS was raised through the Internet Society chapters in Bolivia, Chennai (India), Mumbai (India), Honduras, Norway, Panama, and Uganda together with MANRS ambassadors and fellows.

Figure 2. Photos from the Training of Network Operators in Cameroon

[46] https://www.manrs.org/2021/02/mastering-routing-security-at-apricot-2021/

[47] https://www.manrs.org/2021/09/sudan-the-first-internet-society-chapter-to-join-manrs/

[48] https://twitter.com/Isoc_Cameroon/status/1460227510977929218

4. Community Spotlight

The MANRS community is comprised of participants, partners, ambassadors, and fellows.

As of 31 December, there were 750 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 four new partners in 2021—Nautilus Mediterranean Exchange (NAMEX), North American Network Operators Group (NANOG), Qrator Labs, and SAMENA Telecommunications Council—and a total of 162 new MANRS participants.

Here are what some of the participants and partners have said about MANRS in 2021.[49]

Equipment Vendors[50]

Ashwin Kohli, Senior Vice President of Customer Engineering, Arista Networks

> "As a global industry leader in cloud networking, we want to take part in the efforts to secure the Internet as well. MANRS is providing great guidelines to achieve that goal and Arista Networks is proud to be a founding participant of the MANRS Equipment Vendor Program.

Kevin Wollenweber, Vice President of Networking, Mass-Scale Infrastructure Group, Cisco

> "As a founding member of the MANRS Equipment Vendor Program, we look forward to collaborating with the broader community to drive network security innovation.

Shekar Ayyar, Chief Executive Officer, Arrcus

> "Creating Arrcus' ACE platform by working closely with the world's leading network providers has given us a unique perspective into how critical routing security is to protect the viability of the Internet for both businesses and consumers. We look forward to collaborating through MANRS and the Internet Society to make the Internet more secure, stable, and reliable for everyone.

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

[50] https://www.internetsociety.org/news/press-releases/2021/arista-cisco-huawei-juniper-and-nokia-launch-new-manrs-equipment-vendor-program-to-improve-routing-security-worldwide/; https://www.internetsociety.org/news/press-releases/2021/arista-cisco-huawei-juniper-and-nokia-launch-new-manrs-equipment-vendor-program-to-improve-routing-security-worldwide/; and https://www.globenewswire.com/news-release/2021/12/16/2353744/0/en/Arrcus-Joins-MANRS-to-Help-Improve-Internet-Routing-Security.html

Network Operators[51]

Mohamed Hafez, Information Security Team Lead, Internet Society Sudan Chapter

"Even though many chapters have supported MANRS in various ways, we're delighted to be the first one to be a MANRS participant. The chapter runs the ccTLDs (.sd and .سودان) of Sudan. Given the importance of our services, we decided to join MANRS to guarantee their security and reduce the possibility of routing security incidents.

Steven Xu Tan, President, China Telecom (Americas) Corporation

"All of China Telecom's backbone networks successfully implemented routing security best practices of MANRS. We deeply appreciate the efforts made by the MANRS community to advance better routing security. We are committed to playing an active role in this community and help more network operators adopt the same best practices.

Luis Arroyo, Operations Manager, Costa Rica Internet Service Provider (CRISP S.A.)

"Our company strongly believes in a secure Internet as it represents the most beneficial environment for all, it is also our most firm example for generations that will follow us.

IXPs[52]

Rafael Ibarra, Executive Director, IXSal

"IXSal, the first IXP in El Salvador, aims to get more local operators connected, and one of the key added values we offer is our adhesion to world security standards and good practices. For sure, MANRS is one of those practices that help us make Internet traffic more secure in El Salvador, and thus we are confident that, by complying with MANRS, we contribute to a better Internet for all.

Li-Heng Yu, Chief Technology Officer, Taiwan Digital Streaming

"A newly formed IXP is hard to compete with existing ones. That's why we need more modern standards and features to attract people to join. Introducing MANRS is a good feature and also enforces the security of the IXP.

Michel Lanners, Chief Information Officer, LU-CIX

"MANRS is a very worthwhile initiative that brings together in one set of guidance rules many of the industry best practices, and allows us to publicly show our support for a safer Internet.

[51] https://www.manrs.org/2021/09/sudan-the-first-internet-society-chapter-to-join-manrs/; https://www.prnewswire.com/news-releases/all-china-telecom-backbone-networks-accepted-by-manrs-301302160.html; and https://www.manrs.org/isps/participants/entry/1866/

[52] https://www.manrs.org/ixps/ixp-participants/entry/1762/; https://www.manrs.org/ixps/ixp-participants/entry/1917/; and https://www.manrs.org/ixps/ixp-participants/entry/1718/

CDN and Cloud Providers[53]

Barry Cooks, Chief Technology Officer, DigitalOcean	"We are committed to following specific MANRS guidelines as part of a broader effort to reduce leaks and other routing security issues that stem from misconfigurations.
Nathalia Nascimento, Network Engineer, GoCache	"GoCache has always been committed to implementing best practices and we strongly believe we can build a secure network if everyone contributes to this same goal. By joining the MANRS community, we reassure this commitment and encourage others to do the same.
Bikash Koley, Vice President, Google Global Networking	"To truly close the holes inherent in BGP, there is still a significant amount of engineering work required, which means small ISPs must dedicate resources to these types of initiatives, and that may be difficult to achieve quickly. That is one reason why Google has been working with MANRS to publish information about how it implements route filtering, which should make it easier for smaller networks that want to peer with Google to simply piggyback on an established approach.

Partners[54]

Qrator Labs	"It took us too long to get on track with the MANRS initiative, but this partnership will help align our efforts. Together we will make a joint effort in providing more awareness to global Internet actors and share our combined expertise on BGP routing.
Ela Yazdani, Director of Communications, CANARIE	"The partners in Canada's NREN are pleased to announce that 99 percent of organizations connected to the NREN are now connected to a MANRS-compliant network. Canada's NREN joins a number of global NREN partners, including Internet2 in the United States, GÉANT across Europe, AARNet in Australia, and SURFnet in the Netherlands, in implementing MANRS.
Steven Wallace, Internet2 Security Architect and MANRS Ambassador	"Ninety-five percent of network routes originating from US research and education institutions lack a form of hijack protection recommended by MANRS, known as RPKI. Adding this layer of security is something that the IP address owners, typically campuses in the US, will want to address. Internet2 is working to build tools, training, and outreach programs to support this need.

[53] https://securityboulevard.com/2021/01/digital-ocean-minds-its-manrs-alongside-other-service-providers/; https://www.manrs.org/cdn-cloud-providers/participants/entry/1744/; and https://cacm.acm.org/magazines/2021/8/254299-fixing-the-internet/fulltext

[54] https://blog.qrator.net/en/partnership-with-manrs_152/; https://www.canarie.ca/canadas-national-research-and-education-network-bolsters-security/; and https://www.manrs.org/2021/05/greater-manrs-alignment-will-benefit-the-us-research-and-education-community/

MANRS Ambassadors and Fellowship Program

The MANRS Ambassadors and Fellowship Program[55] that was launched in 2020 held its second edition in 2021, bringing together 5 ambassadors[56] and 13 fellows.[57] Ambassadors[58] (Figure 3) are representatives from current MANRS participants who provide mentorship, guidance, and feedback to fellows in the routing security community. In 2021, two of the ambassadors—Ram Krishna Pariyar and Zobair Khan—served as fellows in 2020.

Fellows[59] (Figure 4) 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, representing all continents, 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.

The training team of ambassadors and fellows actively raised awareness and conducted webinars, online tutorials, and training workshops in collaboration with MANRS partners and participants, Internet Society chapters, and network operator groups. In some events, fellows from the 2020 cohort also participated (Figure 5).

In 2021, MANRS launched a sponsorship program bringing on board sponsors to support the MANRS Ambassador and Fellowship Program. A total of US$26,700 was raised from APNIC, APRICOT, LACNIC, Akamai, and China Telecom to support the program.

Figure 3. Meet the 2021 MANRS Ambassadors

[55] https://www.manrs.org/ambassadors-programme/

[56] https://www.manrs.org/2021/03/meet-the-2021-manrs-ambassadors/

[57] https://www.manrs.org/2021/05/meet-the-2021-manrs-fellows/

[58] https://www.manrs.org/ambassadors-programme/ambassadors/

[59] https://www.manrs.org/ambassadors-programme/fellows/

Figure 4. Meet the 2021 MANRS Fellows

Figure 5. A Selection of Activities by MANRS Fellows

ICANN Supports MANRS

Others within the Internet ecosystem are recognizing and supporting MANRS, such as the Internet Corporation for Assigned Names and Numbers (ICANN) that is responsible for the management and oversight of the coordination of the Internet's domain name system (DNS) and its unique identifiers. For instance, in ICANN's Final Report of the DNS Security Facilitation Initiative Technical Study Group in 2021, MANRS is included as one of their recommendations:[60]

> *ICANN org should continue to participate in initiatives such as MANRS and KINDNS to measure and report on their adoption, and use those reports to create targeted educational material to improve awareness about infrastructure security. ICANN org should take the best practices coming out of those initiatives and ensure that contracted parties and the ICANN community are aware of them.*

[60] https://community.icann.org/display/DSFI/DSFI+TSG+Final+Report?preview=/176623416/176623417/DSFI-TSG-Final-Report.pdf

5. Challenges and Lessons Learned

2021 saw some major routing incidents that MANRS analyzed and drew lessons from, including the major Facebook/Meta outage[61] that affected all its platforms and billions of people, a BGP hijack by Vodafone Idea,[62] a route leak by Cablevisión,[63] and an attempt to hijack Twitter.[64] These incidents demonstrate the importance of BGP filtering and creation of ROAs that protects prefixes from hijack attempts.

Even though ROA adoption is picking up in some regions, as indicated at the start of the report (Figure 1), the adoption rate is generally very low. With only 34 percent valid ROAs across the globe, there is a need to clear misconceptions related to RPKI to increase ROA adoption. Through numerous events, training workshops, blogs, and social media posts, MANRS has emphasized the importance of implementing effective route filtering based on verifiable information about which networks are legitimately authorized to originate which number resources (AS numbers and IP prefixes), as well as the importance of having well-established and well-advertised communication channels to quickly resolve issues when they happen. MANRS participants have shown good support towards RPKI and more than 61 percent of the resources have valid ROAs, but greater efforts to strategically and collaboratively promote RPKI and accelerate ROA adoption are needed.

Within MANRS, measuring and monitoring participants' conformance with MANRS actions was a challenge. The Steering Committee has formed a working group to formalize ongoing conformance testing, which will be measured and published for all MANRS participants on a monthly basis in 2022.

6. Looking Ahead

In 2022, 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:

- A 15 percent increase in ROA creation by MANRS participants compared to 2021, showing they support cryptographic validation of IP address ownership.
- A 5 percent increase in ROV implementation by MANRS participants compared to 2021, showing they are checking that a given network is authorized to announce routes to a given IP address range.
- A 25 percent reduction in the number of MANRS participants that become nonconforming after joining.

Also in 2022, we will continue to provide ongoing support to transition MANRS to a community-designed and community-led effort. We will continue to offer leadership initiatives, such as the MANRS Ambassador and Fellowship Program, build strategic partnerships to expand our outreach and engage with different communities, and enhance capacity in routing security among network engineers around the world. Continuous improvements to the MANRS Observatory are also envisaged in 2022.

Routing security is vital to the future and stability of the Internet. Join us[65] in securing the global Internet for everyone.

[61] https://www.manrs.org/2021/10/facebook-has-good-manrs-mistakes-still-happen/

[62] https://www.manrs.org/2021/04/a-major-bgp-hijack-by-as55410-vodafone-idea-ltd/

[63] https://www.manrs.org/2021/02/major-route-leak-by-as28548-another-bgp-optimizer/

[64] https://www.manrs.org/2021/02/did-someone-try-to-hijack-twitter-yes/

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

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.org