



MANRS

Mutually Agreed Norms for Routing Security

Boris Mimeur

boris.mimeur@cengn.ca

MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure.

MANRS sets a new norm for routing security.



MANRS Programmes



Network
Operators



Internet Exchange Points



Content Delivery Networks
(CDNs) and Cloud Providers



MANRS Ambassadors and Fellows Research Group initiatives



Overview

Launched in 2020, Ambassadors and Fellows make the global routing infrastructure more robust and secure.

They work in one of three categories: training, research, or policy.

Ambassadors are representatives from current MANRS participants who provide mentorship, guidance, and feedback to others in the routing security community.

Fellows are emerging leaders who believe that routing security is essential and are ready to contribute to its improvement.



MANRS Research Group 2020 initiatives

Incident review and analysis

Classify and analyze routing incidents that significantly impact the Internet

Accelerate RPKI/ROA related RFC awareness

Present a graphical representation of the interrelation of RPKI/ROA RFC's as well as summary to help consume the critical information faster and fast track the ramp up for organizations to adopt and deploy RPKI/ROA

RPKI Validators option review and assessment

Multiple validators exist today with different degree of scale being tested. Work towards a summary of the recommended option

Survey to the larger community in collaboration with Global Cyber Alliance



MANRS Research Group long term initiatives

The Observatory and tools for detection/reporting

Evolution of the MANRS Observatory, recommendation of tools for detection and mitigation including algorithm optimization to MANRS members

RPKI Ecosystem infrastructure scaling

Understand the limitations of the current scaling capability of the ecosystem available today and express the operational risks and mitigation

Beyond ROA: BGP Path validation

Review and recommend BGP path validation options



Thank you.

Boris Mimeur

boris.mimeur@cengn.ca

manrs.org



MANRS Resources



Help Is Available

If you're not ready to join yet, implementation guidance is available to help you.

- **Implementation Guide** based on Best Current Operational Practices deployed by network operators around the world
- **Tutorial modules** based on information in the Implementation Guide.

Filtering: Preventing propagation of incorrect routing information

Introduction to Filtering

The diagram illustrates a network topology. On the left, two orange circles represent customers: AS64501 (with IP ranges 2001:db8:1001::/48 and 192.0.2.0/24) and AS64502 (with IP ranges 2001:db8:2002::/48 and 198.51.100.0/24). These are connected to a central black circle representing AS64500 MANRS Participant Network. This network is connected to a blue cloud labeled 'Internet'. The Internet is connected to an orange circle representing AS B Transit Provider, which is in turn connected to a blue circle representing AS15169 Google.

Implementing prefix filters within your network can help protect against threats such as **Prefix Hijacking**, and **Route Leaks**.

Select the buttons to see examples of threats prefix filters can protect against.

[Prefix Hijacking](#) [Route Leaks](#)

Internet Society

4/33



MANRS Implementation Guide for Network Operators

If you're not ready to join yet, implementation guidance is available to help you.

- Based on Best Current Operational Practices deployed by network operators around the world
- Recognition from the RIPE community by being published as RIPE-706
- <https://www.manrs.org/bcop/>

Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

Version 1.0, BCOP series
Publication Date: 25 January 2017



MANRS

[1. What is a BCOP?](#)

[2. Summary](#)

[3. MANRS](#)

[4. Implementation guidelines for the MANRS Actions](#)

[4.1. Coordination - Facilitating global operational communication and coordination between network operators](#)

[4.1.1. Maintaining Contact Information in Regional Internet Registries \(RIRs\): AFRINIC, APNIC, RIPE](#)

[4.1.1.1. MNTNER objects](#)

[4.1.1.1.1. Creating a new maintainer in the AFRINIC IRR](#)

[4.1.1.1.2. Creating a new maintainer in the APNIC IRR](#)

[4.1.1.1.3. Creating a new maintainer in the RIPE IRR](#)

[4.1.1.2. ROLE objects](#)

[4.1.1.3. INETNUM and INET6NUM objects](#)

[4.1.1.4. AUT-NUM objects](#)

[4.1.2. Maintaining Contact Information in Regional Internet Registries \(RIRs\): LACNIC](#)

[4.1.3. Maintaining Contact Information in Regional Internet Registries \(RIRs\): ARIN](#)

[4.1.3.1. Point of Contact \(POC\) Object Example:](#)

[4.1.3.2. OrgNOCHandle in Network Object Example:](#)

[4.1.4. Maintaining Contact Information in Internet Routing Registries](#)

[4.1.5. Maintaining Contact Information in PeeringDB](#)

[4.1.6. Company Website](#)

[4.2. Global Validation - Facilitating validation of routing information on a global scale](#)

[4.2.1. Valid Origin documentation](#)

[4.2.1.1. Providing information through the IRR system](#)

[4.2.1.1.1. Registering expected announcements in the IRR](#)

[4.2.1.2. Providing information through the RPKI system](#)

[4.2.1.2.1. RIR Hosted Resource Certification service](#)

MANRS Tutorials

Tutorials based on information in the Implementation Guide

Walks through the tutorial with a test at the end of each module

Working with and looking for partners that are interested in integrating it in their curricula

<https://www.manrs.org/tutorials>

The screenshot shows a presentation slide titled "Introduction to Filtering" with a dark blue header and footer. The header text is "Filtering: Preventing propagation of incorrect routing information" and the footer includes the "Internet Society" logo and navigation icons. The main content area features a network diagram with nodes: "AS64501 Customer" (top left), "AS64500 MANRS Participant Network" (center), "AS64502 Customer" (bottom left), "AS B Transit Provider" (top right), and "AS15169 Google" (far right). A cloud labeled "Internet" is between the MANRS network and AS B. Text above the top customer node reads "2001:db8:1001::/48 | 192.0.2.0/24" and text below the bottom customer node reads "2001:db8:2002::/48 | 198.51.100.0/24". Below the diagram, text states: "Implementing prefix filters within your network can help protect against threats such as **Prefix Hijacking**, and **Route Leaks**." At the bottom of the text area are two blue buttons: "Prefix Hijacking" and "Route Leaks".

LEARN MORE:

<https://www.manrs.org>

FOLLOW US:



/RoutingMANRS

