Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

Authors: David Freedman, Brian Foust, Barry Greene, Ben Maddison, Andrei Robachevsky, Job Snijders, Sander Steffann
Document ID: ripe-706
Date: June 2018

---

1. What is a BCOP?

A Best Current Operational Practices (BCOP) document describes best current operational practice on a particular topic, as agreed by subject matter experts and periodically reviewed by the Internet community.

2. Summary

The "Mutually Agreed Norms for Routing Security" (MANRS, https://www.manrs.org) BCOP provides guidance to ease deployment of measures required by MANRS and is targeted at stub networks and small providers. The document should also assist in checking if the network setup is compliant with MANRS.

3. MANRS

Throughout the history of the Internet, collaboration amongst participants and shared responsibility for its smooth operation have been two of the pillars supporting the tremendous growth and success of the Internet, as well as its security and resilience. Technology solutions are an essential element here, but technology alone is not sufficient. To stimulate visible improvements in this area, a greater change toward a culture of collective responsibility is needed.

With this goal in mind an industry driven initiative called the "Mutually Agreed Norms for Routing Security (MANRS)" was launched in November 2014. The initiative has four objectives:

- Raise awareness and encourage actions by demonstrating commitment of the growing group of supporters
- Promote the culture of collective responsibility for resilience and security of the Internet's global routing system
- Demonstrate the ability of the industry to address issues of resilience and security of the Internet's global routing system in the spirit of collective responsibility
- Provide a framework for ISPs to better understand and help address issues related to resilience and security of the Internet's global routing system

3.1 The MANRS Principles

- We (the ISP/network operator) recognise the interdependent nature of the global routing system and our own role in contributing to a secure and resilient Internet.
- We will integrate best current practices related to routing security and resilience in our network management processes in line with the Actions.
- We are committed to preventing, detecting and mitigating routing incidents through collaboration and coordination with peers and other ISPs in line with the Actions.
- We encourage our customers and peers to adopt these Principles and Actions.

3.2 The MANRS Actions

Many different recommendations exist to improve the security and resilience of the inter-domain routing system. Some of the advice can even appear somewhat contradictory and often the key decision can come down to understanding what is most important or appropriate for a given network considering its size and resources, the number of external connections, customers and end users it has, the size and expertise of its staff, and so forth.

The MANRS Actions underline a set of recommendations that are definitely valuable to the overall security and resilience of the global routing system, as well as to the network operator itself. They address three main classes of problems:

- Problems related to incorrect routing information;
- Problems related to traffic with spoofed source IP addresses; and
- Problems related to coordination and collaboration between network operators.

The Actions are:

1. Filtering - Preventing propagation of incorrect routing information.
    - Network operator defines a clear routing policy and implements a system that ensures correctness of their own announcements and announcements from their customers to adjacent networks with prefix and AS-path granularity.
    - Network operator is able to communicate to their adjacent networks which announcements are correct.
    - Network operator applies due diligence when checking the correctness of their customer’s announcements, specifically that the customer legitimately holds the ASN and the address space it announces.
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 an incorrect source IP address from entering and leaving the network.
3. Coordination - Facilitating global operational communication and coordination between network operators.
    - Network operator maintains globally accessible up-to-date contact information.

4. Global Validation - Facilitating validation of routing information on a global scale.
    - Network operator has publicly documented routing policy, ASNs and prefixes that are intended to be advertised to external parties.

3.3 Becoming a MANRS Participant

Network operators who agree to the Principles and implement at least one of the Actions (though not solely the Coordination Action) can become a MANRS Participant. This entitles you to use of the MANRS badge, you will be listed on the routingmanifesto.org website, and you can contribute to this document and others like it.

The proposed recommendations, referred to as Actions in the MANRS document and in this BCOP, address the most common cases and are designed to incur minimum cost and risk when implementing them. Any particular Action is not a comprehensive solution to the outlined problems.

4. Implementation guidelines for the MANRS Actions

The selection of actions was based on an assessment of the balance between small, incremental individual costs and the potential common benefit. They define a minimal security baseline. Any particular Action is not a comprehensive solution to the outlined problems.

In order to facilitate the implementation of MANRS Actions a set of guidelines has been developed in the framework of the BCOP activity. The full guidelines are provided here: https://www.manrs.org/bcop/

5. Information checklist

Effective implementation of routing security relies on the availability of up-to-date information, such as contact information, routing policies and specifically networks that are being originated by a network operator. Being a responsible network operator requires both publishing contact and routing policy information, and using the information published by others to validate the routing announcements received from others.

5.1. Publishing information - checklist

There are many places where information can be published. This summary can be used as a checklist when publishing and updating information, and can be included in your organisation's processes and procedures.

- For the AFRINIC, APNIC and RIPE NCC service regions:
    - Publish contact information for roles/departments as ROLE objects
      Optionally: create PERSON objects for staff members and link from the ROLE
    - Create IRR objects and refer to the correct POCs from those objects and document your routing policy:
        - INETNUM and INET6NUM
            - admin-c: refer to your IPAM administrators

                - tech-c: refer to the administrators of the systems on this network
            - AUT-NUM
                - admin-c: refer to your peering coordinators
                - tech-c: refer to your NOC
                - mp-import/mp-export: document your BGP connections
            - ROUTE and ROUTE6
                - remarks: document contacts for your NOC, abuse desk, etc.
                - ping-hdl: refer to your NOC
    - Create RPKI ROAs for all prefixes that you announce from your ASNs
    - Publish your peering locations, policy and contacts in PeeringDB
    - Publish your peering locations, policy and contacts on your website
    - Publish your NOC and abuse contacts on your website

- For the LACNIC service region:
    - Publish contact information for roles/departments as POC objects
    - Publish contact information for the Organisations holding resources (directly allocated by LACNIC or re-allocated by a LIR)
    - Publish the DNS that provides the reverse resolution for IP blocks
    - Refer to the correct POCs for your resources:
        - tech-c: refer to your IPAM administrators
        - abuse-c: refer to your network abuse desk
    - Create RPKI ROAs for all prefixes that you announce from your ASNs
    - Publish your peering locations, policy and contacts in PeeringDB
    - Publish your peering locations, policy and contacts on your website
    - Publish your NOC and abuse contacts on your website

- For the ARIN service region:
    - Publish contact information for roles/departments as POC objects
    - Refer to the correct POCs from your resources
        - NET
            - NOC POC: refer to your NOC and optionally sysadmins
            - Tech POC: refer to your IPAM administrators
            - Abuse POC: refer to your systems abuse desk
        - ASN
            - NOC POC: refer to your NOC and peering coordinators
            - Tech POC: refer to your IPAM administrators
            - Abuse POC: refer to your network abuse desk
    - Create IRR objects and refer to the correct POCs from those objects and document your routing policy:
        - INETNUM and INET6NUM
            - admin-c: refer to your IPAM administrators
            - tech-c: refer to the administrators of the systems on this network
        - AUT-NUM
            - admin-c: refer to your peering coordinators

        - tech-c: refer to your NOC
        - mp-import/mp-export: document your BGP connections
    - ROUTE and ROUTE6
        - remarks: document contacts for your NOC, abuse desk, etc.
- Create RPKI ROAs for all prefixes that you announce from your ASNs
- Publish your peering locations, policy and contacts in PeeringDB
- Publish your peering locations, policy and contacts on your website
- Publish your NOC and abuse contacts on your website

5.2. Validating information - checklist

Operating a network in a responsible way requires the validation of the traffic you and your customers send to the rest of the Internet, and validation of the routes that your upstreams, peers and customers announce to you. Failing to validate any of this makes your network vulnerable to route hijacks and a potential source of DDoS attack traffic.

- Apply ACLs and/or uRPF filtering to your customers' connections
- Apply ACLs, uRPF and/or SAVI filtering to your own networks
- Use the information in the IRRs to filter routes that your customers announce to you
- Validate the announcements from your customers against the RPKI ROAs

6. Acknowledgements

The main authors of this document are David Freedman, Brian Foust, Barry Greene, Ben Maddison, Andrei Robachevsky, Job Snijders and Sander Steffann. We also thank Will van Gulik, Jakob Heitz, Aris Lambrianidis, Kevin Meynell and Massimiliano Stucchi for their review and contributions to this document.