Internet Society

MANRS Actions for IXPs

By Michuki Mwangi
Af-IX Meeting
21 August 2017
Abidjan, Côte d’Ivoire

MANRS

Routing Resilience Manifesto, aka MANRS

https://www.routingmanifesto.org/

https://www.manrs.org/

What are MANRS Actions for IXPs

- Proposed concrete actions that IXP operators should implement
- Complement the network operators MANRS

Action 0. Local Policy

❑ **The IXP has a published policy that reflects the implementation of MANRS actions and is obligatory for all IXP members.**

- The local policy, or set of policy documents, demonstrates the security posture of the IXP, explains how specific MANRS actions are implemented, and documents terms and conditions of related services (if applicable).

Action 1. Facilitate prevention of propagation of incorrect routing information.

❑ **The IXP implements filtering or tagging of route announcements at the Route Server based on routing information data (IRR, RPKI, etc.).**

- IXPs using a Route Server to facilitate multilateral peering can use it to validate received route announcements from a peer and subsequently filter or tag them to other peers.
- Validation is done by checking BGP announcements against IRR data (by resolving the AS-SET object) or RPKI data (ROA objects or a validated cache). It is also common to check the announcements against "bogons" or "martians" (IP prefixes as defined in RFC1918, RFC5735, and RFC6598; ASNs in the AS-PATH as defined by RFC5398, RFC6793, RFC6996, RFC7300, RFC7607).
- Based on the outcome of the validation process, the announcement is tagged as VALID, INVALID, or UNKNOWN using predefined communities or filtered in accordance with the RS published policy.

Action 2. Protect the peering platform

- ❑ **The IXP performs filtering of proprietary or other protocols not appropriate at the Ethernet platform.**

- While not strictly routing, applying hygiene on Layer 2 can ensure the smooth operation of the platform and contribute to the stability of the IXP infrastructure and routing.

- The IXP has a published policy of traffic not allowed on the peering fabric and performs filtering of such traffic. Commonly, filtering applies to:
  - ✓ ***Not allowed Ethernet frame formats***
  - ✓ ***Not allowed Ethertypes***
  - ✓ ***Link-local protocols, such as IRDP, ICMP redirects, Discovery protocols (CDP, EDP), VLAN/trunking protocols (VTP, DTP), BOOTP/DHCP, etc.***
  - ✓ ***Restricted by the MAC port security configuration***

Action 3. Assist with preventing unwanted traffic

❑ **The IXP offers telemetry data to its members.**

- By offering telemetry data based on Netflow/Jflow/Sflow/IPFIX for L2-L4 flows to its members, the IXP can assist its members in preventing unwanted traffic (e.g. traffic with spoofed source IP addresses), or mitigating a DDoS attack.
- The IXP has a published policy outlining terms and conditions of this service.

Action 4. Facilitate global operational communication and coordination between network operators.

- ❑ **The IXP facilitates communication among members by providing necessary mailing lists, and member directories.**

- The IXP and each of its members has at least one valid, active email address and one phone number that other members can use for cases of abuse, security, and operational incidents.

- Effective communication among members of an IXP is essential in mitigating network incidents such as misconfigurations, outages, or DoS attacks. Mailing lists or other means of communication and a member directory available to all members of the exchange containing up-to-date contact information play a crucial role.

Action 5. Provide monitoring and debugging tools to participants.

❑ **The IXP provides a looking glass for its members.**

- A looking glass is an important facility that can help debug routing incidents or anomalies and prevent or shorten potential outages.
- An IXP should offer a looking glass interface of its Route server to its members.

Action 6. Promote MANRS to the IXP membership.

❑ **The IXP develops and provides a demonstrable incentive for members to implement MANRS actions**

- The IXP actively promotes MANRS by encouraging its members to implement the MANRS actions in part or in full. The encouragement can take different forms, for example:

✓ Provide MANRS-related clauses in the membership/customer agreement (if the IXP has one)

✓ Offer price reductions linked to MANRS compliance. This may be a symbolic reduction with the rationale that a MANRS compliant member will less likely cause trouble to other peers and the IXP operations, easy to coordinate with, etc. therefore reducing the cost of providing the IXP service.

✓ Offer MANRS training for the members

- The offered incentives are documented in a published policy.

Action 7: Assist with the mitigation of a DDoS attack

- ❑ **The IXP provides a "sink hole" in the peering fabric that allows members to announce prefixes with the next hop setting to the sinkhole IP address,**

OR

- ❑ **The IXP facilitates signaling of blackholing requests by means of a Route Server and a specific BGP community (RFC 7999).**

- To help members mitigate the effects of a DDoS attack against their networks, the IXP offers one of two main mechanisms to terminate the unwanted traffic without overloading the peering fabric of a peer's infrastructure: a "sink hole" and a blackhole.
- With a sink hole, the IXP configures a specific MAC address and a corresponding IP address. All traffic destined to that IP address is dropped by the IXP platform. A member experiencing a volumetric DoS attack to certain prefixes of its network can announce these prefixes with the next hop setting to the sinkhole IP address. This can be done through the Route Server or bilateral peering.
- With a blackhole, a member experiencing a volumetric DoS attack signals a blackhole to the Route Server by using the BGP BLACKHOLE community. As a result, all traffic destined to these prefixes will be dropped at the IXP platform.
- The offered mechanism is documented in a published policy.

Thank you.

mwangi@isoc.org

Visit us at
www.internetsociety.org
Follow us
@internetsociety

Galerie Jean-Malbuisson 15,
CH-1204 Geneva,
Switzerland.
+41 22 807 1444

1775 Wiehle Avenue,
Suite 201, Reston, VA
20190-5108 USA.
+1 703 439 2120