Recommendations and Best Practices

Just as in the case of IPv4, IPv6 prefix announcements should consider a series of important security aspects. Paying attention to security when deploying eBGP4+ sessions is highly recommended. Situations resulting from misconfiguration, spoofing and DDoS attacks on edge routers, lack of validation of client prefix RPKI or IRR announcements, and other issues can compromise Internet routing security, for both IPv4 and IPv6. This is why it is important to design and deploy actions to mitigate risks and increase security.

It is also important to understand that an ISP operator's prefix announcements are part of the Global Internet Routing System. New initiatives such as the **MANRS Project** (https://www.manrs.org) and its section titled MANRS for Network Operators (https://www.manrs.org/isps/) propose concrete actions such as the implementation of best practices by ISP operators when deploying Internet routing. Similarly, in its documents BCP38 (https://tools.ietf.org/html/bcp38) and BCP84 (https://tools.ietf.org/html/bcp84), the IETF Networking Group presents best current practices for the secure control of prefixes announced and received via eBGP sessions.
The following is a summary of the most relevant best practices included in these recommendations and documents:

- Announce only the operator's and its clients' ASNs and IPv6 prefixes to upstream providers. If the ISP operator will announce end-client IPv6 prefixes, it must perform the corresponding authentication validations.
- Keep your routing information up to date with the corresponding RIR/NIR and the PeeringDB if you participate in peering.
- Document and keep your routing information up to date with the corresponding RIR and with your IRR if you are a member (both at RPKI and IRR level).
- Deploy the mechanisms required to effectively protect your network and mitigate DDoS, spoofing, and other forms of attack. Likewise, prevent spoofing traffic to the Internet.
- Deploy an adequate architecture and well-designed BGP filters to control the prefixes that are announced and received. Specifically, avoid announcing illegitimate, unauthorized, or incorrect prefixes.
- Use bogon filtering. Some public Internet providers even offer multihop eBGP sessions for announcing bogon and full bogon routes to eliminate Internet traffic from these routes.
- When designing filters, the design philosophy should be: “Deny all, accept ONLY what is needed.”
- Do not announce or accept IPv6 routes with a prefix longer than /48.
- Do not announce your default gateway to upstream providers.
- Do not accept from upstream providers the IP prefix of the ISP operators that are being published.
- Use IPv4 addresses configured in stable network interfaces and not subject to flapping as router-id addresses (example: loopback or bridge interfaces).

- Design BGP filter configurations that are scalable and make sure the system is not affected by any changes that may be required.
- Use MD5 authentication when configuring eBGP4+ sessions for added security.
- Configure eBGP4+ sessions with TTL 255 to avoid spoofing and DDoS attacks originating more than one hop away.
- Deploy TCP/179 traffic filtering and limitation techniques to deny all and accept ONLY the traffic coming from directly connected eBGP4+ peers with known connection IPv6 addresses.