Recomendaciones y buenas prácticas

El anuncio de los Prefijos IPv6, al igual que los bloques IPv4, debe ser realizado tomando en cuenta aspectos importantes de seguridad. Es muy recomendable prestarle atención a los aspectos de seguridad en el despliegue de las sesiones eBGP4+. Situaciones provenientes de configuraciones erróneas, ataques de tipo spoofing y DDOS a enrutadores de borde, no validación RPKI o IRR de anuncio de prefijos de clientes, entre otros, comprometen la seguridad del enrutamiento de Internet, tanto para IPv4 como para IPv6. Es importante entonces que se diseñen y desplieguen acciones para mitigar los riesgos y aumentar la seguridad.

También, es importante entender que el anuncio de los prefijos de un operador ISP es parte del Sistema Global de Enrutamiento de Internet. Nuevas iniciativas como la del Proyecto **MANRS 'https://www.manrs.org/'**, en su apartado de MANRS para Operadores de Red **'https://www.manrs.org/isps/'** proponen acciones muy concretas como buenas prácticas a seguir en el despliegue del Enrutamiento de Internet por parte de los operadores ISP. De la misma forma, el Grupo de Networking de la IETF presenta en sus documentos BCP38 (https://tools.ietf.org/html/bcp38) y BCP84 (https://tools.ietf.org/html/bcp84), buenas prácticas para control seguro de los prefijos anunciados y recibidos en las sesiones eBGP.
A continuación, el resumen de las buenas prácticas mas resaltantes provenientes de estas recomendaciones y documentos:

- Anunciar a los Upstream Providers SOLO el ASN y los Prefijos IPv6 del operador y los de sus clientes. Si el operador ISP va a anunciar los Prefijos IPv6 de Clientes FInales debe hacer las validaciones de autenticaciópn correspondientes.
- Mantener la información de enrutamiento actualizada en el RIR/NIR correspondiente y en PeeringDB si hace Peering.
- Documentar y mantener actualizada la información de enrutamiento ante el RIR correspondiente, y ante el IRR si está asociado. Esto, a nivel de RPKI y IRR.
- Desplegar los mecanismos necesarios para una efectiva protección de red y mitigar ataques DDOS, Spoofing, entre otros. De igual manera, prevenir el tráfico 'spoofing' hacia Internet.
- Desplegar una adecuada arquitectura y un buen diseño de Filtros BGP a objeto de controlar los prefijos que se anuncian y se reciben. Específicamente, evitar el anuncio de prefijos ilegítimos, no autorizados y erróneos.
- Uso de Filtrado Bogons. Hay incluso proveedores públicos de Internet que ofrecen sesiones eBGP Multihop para el anuncio de Rutas Bogons y Full Bogons a objeto de suprimir el tráfico hacia la Internet de estas rutas.
- Para el diseño de los filtros: filosofía de diseño 'denegar todo y aceptar SOLO lo conveniente'.
- No anunciar ni aceptar Rutas IPv6 con Longitud de Prefijo mayor a /48.
- No anunciarle a los Upstream Providers el Default Gateway.
- No aceptar de los Upstream Providers los Prefijos IPv6 del operador ISP que se están publicando.
- Utilizar como router-id direcciones IPv4 configuradas en interfaces de red estables y sin posibilidad de flapping. Por ejemplo, interfaces loopback o interfaces bridge.

- Diseñar la configuración de los Filtros BGP que sean escalables y que el sistema no se impacte ante cambios requeridos.
- Utilizar autenticación MD5 en la configuración de sesiones eBGP4+ para mayor seguridad.
- Configurar las sesiones eBGP4+ con TTL 255 para evitar Spoofing y DDOS provenientes de más allá de un salto.
- Desplegar técnicas de Filtrado y Limitación de Tráfico TCP/179 a objeto de denegar todo y aceptar SOLO el tráfico proveniente de los Peers eBGP4+ directamente conectado, conciendo sus IPv6 de conexión.