LAC-IX
LATIN AMERICA AND CARIBBEAN IXPs

MEJORES PRÁCTICAS BGP PARA PARTICIPANTES DE IXP

Guía para Gestión de Sesiones de Peering

Versión: 1.2
Fecha: Mayo 2026
Audiencia: Miembros de Internet Exchange Points en LAC
Nivel: Fundamental a Intermedio

Table of Contents

1. Introducción

1.1 Propósito del Documento

Esta guía establece los principios fundamentales y mejores prácticas para la configuración y gestión de sesiones BGP en Internet Exchange Points (IXPs). El objetivo es garantizar una operación eficiente, segura y conforme a los estándares de la industria, proporcionando a los participantes del IXP las herramientas y conocimientos necesarios para una integración exitosa.

1.2 Alcance

El presente documento está diseñado para cubrir los aspectos esenciales de la operación BGP en un entorno de IXP. Comenzaremos con los principios básicos que rigen las sesiones BGP en estos puntos de intercambio, seguidos por las reglas fundamentales de anuncio de prefijos que todo participante debe conocer y respetar. También exploraremos las configuraciones de seguridad esenciales que protegen tanto su red como el ecosistema completo del IXP.

Las políticas de routing recomendadas se presentan con ejemplos prácticos que ilustran escenarios reales encontrados en la operación diaria de IXPs en América Latina y el Caribe. Cada sección incluye casos de uso específicos que ayudarán a los operadores de red a comprender no solo el "qué" sino también el "por qué" detrás de cada recomendación.

1.3 Importancia del BGP Correcto en IXPs

La configuración correcta de BGP en un IXP no es simplemente una cuestión técnica, sino un compromiso fundamental con toda la comunidad de Internet. Cuando un participante configura incorrectamente sus sesiones BGP, las consecuencias pueden extenderse mucho más allá de su propia red.

- Los anuncios de rutas incorrectas pueden propagarse rápidamente a través del IXP, afectando a docenas o incluso cientos de otras redes que confían en la precisión de la información de routing compartida. Este tipo de error puede causar pérdida de tráfico significativa o routing subóptimo que degrada la calidad del servicio para usuarios finales en toda la región.

- Desde una perspectiva de seguridad, las configuraciones inadecuadas crean vulnerabilidades que pueden ser explotadas por actores maliciosos. El secuestro de prefijos (prefix hijacking) y otras formas de manipulación de routing se ven facilitadas cuando los participantes no implementan los filtros y validaciones apropiadas. Además, una configuración deficiente puede impactar negativamente la reputación de su red dentro de la comunidad técnica, afectando futuras oportunidades de peering y colaboración.

- Finalmente, es importante recordar que cada IXP tiene políticas específicas que deben ser respetadas. Las violaciones de estas políticas, ya sean intencionales o accidentales, pueden resultar en consecuencias que van desde advertencias hasta la desconexión del IXP. Por todo esto, invertir tiempo en comprender y aplicar correctamente estas mejores prácticas es fundamental para el éxito de su participación en el IXP.

2. Principios Fundamentales

2.1 Regla de Oro: Separación de Tráfico

El principio más importante que debe guiar toda configuración BGP en un IXP puede expresarse de manera simple pero crucial: el tráfico aprendido en el IXP nunca debe ser anunciado a proveedores de tránsito, y el tráfico aprendido de proveedores de tránsito nunca debe ser anunciado en el IXP.

Esta regla fundamental existe por razones tanto técnicas como económicas. Cuando se participa en un IXP, el objetivo es intercambiar tráfico directamente con otros participantes sin intermediarios, aprovechando la proximidad física y las relaciones de peering sin costo. Si comenzara a anunciar rutas aprendidas en el IXP hacia sus proveedores de tránsito, estaría esencialmente convirtiéndose en un punto de tránsito entre el IXP y esas redes upstream, algo que típicamente viola los términos de servicio de su proveedor y puede resultar en costos inesperados.

De manera similar, anunciar rutas de tránsito en el IXP significa que está ofreciendo acceso a Internet completo a través de su red, lo cual no solo es técnicamente problemático sino que también puede exponerlo a tráfico no deseado y potenciales abusos. Esta práctica es la base de una operación correcta en un IXP y protege tanto a su red como a la comunidad completa del punto de intercambio.

2.1 Conceptos Básicos

2.2.1 Tipos de Relaciones BGP

Para comprender adecuadamente cómo configurar BGP en un IXP, primero debemos entender los diferentes tipos de relaciones que existen en el ecosistema de Internet. En el contexto de un IXP, encontramos principalmente tres tipos de relaciones que determinan cómo fluye el tráfico y qué prefijos deben ser anunciados.

- El peering en IXP representa el intercambio de tráfico sin costo entre pares que se encuentran conectados al mismo punto de intercambio. Esta es la relación fundamental que justifica la existencia del IXP. Cuando dos redes establecen peering en un IXP, acuerdan intercambiar tráfico destinado a sus respectivas redes y las de sus clientes, pero no actúan como tránsito una para la otra.

- El tránsito o upstream es la relación donde un proveedor le proporciona acceso completo a Internet. Esta es típicamente una relación comercial donde usted paga por el servicio. Su proveedor de tránsito anuncia todas las rutas de Internet hacia usted y espera recibir únicamente sus prefijos propios y los de sus clientes. Esta asimetría es fundamental: usted recibe "todo" pero solo debe anunciar "lo suyo".

- Finalmente, la relación de cliente o downstream es donde usted proporciona servicios de conectividad a Internet a otras redes. En este caso, usted es quien anuncia todas las rutas de Internet hacia sus clientes y recibe únicamente los prefijos que ellos originan. Esta relación es el espejo de la relación con su tránsito.

2.2.2 Flujo de Tráfico Correcto

Para visualizar cómo debe fluir correctamente el tráfico en su red, imagine una jerarquía simple. En la parte superior está Internet global, accesible a través de sus proveedores de tránsito. Su red se encuentra en el medio, actuando como punto de convergencia. Por un lado, se conecta hacia arriba con proveedores de tránsito, recibiendo rutas completas de Internet pero anunciando únicamente sus prefijos propios y los de sus clientes.

Por otro lado, su red se conecta lateralmente al IXP, donde la relación es de igual a igual con otros participantes. Aquí también anuncia solo sus prefijos propios y los de sus clientes, nunca las rutas que aprendió de sus proveedores de tránsito. Esta separación es lo que mantiene la integridad del ecosistema de peering.

3. Reglas Esenciales de Anuncio de Prefijos

3.1 Qué Anunciar en el IXP

La decisión sobre qué prefijos anunciar en el IXP debe basarse en un principio simple: solo debe anunciar aquellas redes que están bajo su control directo o autorización explícita. Esto incluye principalmente sus propios prefijos, aquellos que han sido asignados directamente a su ASN por el registro regional correspondiente (como LACNIC en nuestra región). Estos son los prefijos que representan su infraestructura y sus servicios.

Adicionalmente, tiene permitido y es esperado que anuncie los prefijos de sus clientes downstream. Estas son las redes a las cuales usted proporciona conectividad a Internet como proveedor de servicios. Al anunciar estos prefijos en el IXP, está permitiendo que sus clientes se beneficien del peering directo con otros participantes del punto de intercambio, mejorando su latencia y calidad de servicio.

Por otro lado, existe una lista clara de lo que nunca debe anunciar en el IXP. Los prefijos aprendidos de sus proveedores de tránsito están absolutamente prohibidos, ya que esto convertiría su red en un punto de tránsito no autorizado.
De igual manera, los prefijos que aprende de otros peers en el mismo IXP o en otros IXPs no deben ser re-anunciados. La ruta por defecto (0.0.0.0/0 o ::/0) nunca debe aparecer en un IXP, ya que esto indicaría que está ofreciendo acceso completo a Internet, algo que no corresponde a la naturaleza del peering. Finalmente, anunciar la tabla completa de rutas de Internet en el IXP es una violación grave que afectaría a todos los participantes.

3.2 Qué NO Anunciar a Proveedores de Tránsito

La relación con sus proveedores de tránsito también requiere disciplina en los anuncios. Hacia estos proveedores, su responsabilidad es anunciar únicamente las redes bajo su control. Esto significa sus propios prefijos y los de sus clientes, exactamente igual que en el IXP, pero por razones diferentes.

Lo crítico aquí es nunca anunciar los prefijos que ha aprendido a través del IXP. Si lo hiciera, estaría intentando atraer tráfico hacia esas redes a través de su proveedor de tránsito, lo cual generaría varios problemas. Primero, estaría violando probablemente los términos de servicio de su proveedor, quien espera transportar solo su tráfico legítimo. Segundo, podría generar costos inesperados si su tránsito tiene límites de volumen o cobra por el tráfico entrante. Tercero, y más importante, estaría actuando como tránsito no autorizado para esas redes, lo cual puede resultar en serios problemas legales y técnicos.

Tampoco debe anunciar prefijos aprendidos de otros peers fuera del IXP o de otros IXPs donde participe. Cada relación de peering es independiente y los prefijos aprendidos en una no deben propagarse a otras sin autorización explícita.

3.3 Ejemplo Práctico

Para ilustrar estos conceptos, consideremos un escenario real. Imagine que su red opera como AS65001 y tiene asignados los prefijos 198.51.100.0/24 para IPv4 y 2001:db8:1000::/48 para IPv6. Además, tiene un cliente que le ha delegado el anuncio de 203.0.113.0/24. Su red está conectada tanto al IXP-LAC como a un proveedor de tránsito (AS174).

En este escenario, la configuración correcta implica anunciar en IXP-LAC exactamente tres prefijos: su propio 198.51.100.0/24, su propio 2001:db8:1000::/48, y el de su cliente 203.0.113.0/24. A su proveedor de tránsito AS174, anuncia exactamente los mismos tres prefijos. La simetría aquí no es coincidencia sino el resultado de aplicar correctamente el principio fundamental.

Lo que definitivamente no debe hacer es anunciar en el IXP las rutas que aprendió de AS174, que probablemente incluyen cientos de miles de prefijos representando Internet completo. Tampoco debe anunciar la tabla completa o la ruta por defecto. En dirección inversa, no debe anunciar a AS174 ninguna de las rutas que aprendió de los peers en IXP-LAC, por más tentador que pueda parecer para "mejorar" la conectividad.

4. Configuración de Políticas BGP

4.1 Uso de BGP Communities

Las BGP Communities son una herramienta poderosa que funciona como etiquetas o marcadores que pueden adjuntarse a las rutas BGP. Estas etiquetas viajan con los anuncios de prefijos y permiten implementar políticas complejas de routing de manera elegante y escalable. Piense en ellas como "post-it notes" digitales que viajan con cada ruta, indicando información sobre su origen, propósito o tratamiento deseado.

La estrategia recomendada implica crear un esquema interno de communities que le permita identificar rápidamente el origen de cada prefijo en su red. Por ejemplo, puede usar la community 65001:1000 para marcar todos sus prefijos propios, aquellos que origina directamente. Los prefijos de sus clientes pueden llevar la community 65001:2000, permitiendo distinguirlos de sus propias rutas.
Para los prefijos aprendidos de tránsito, una community como 65001:3000 actúa como una señal de alarma: estas rutas nunca deben ser re-anunciadas en el IXP. De manera similar, los prefijos aprendidos en el IXP pueden marcarse con 65001:4000, recordándole a su sistema que estas rutas no deben propagarse a sus proveedores de tránsito.

Este sistema de marcado permite crear políticas de exportación muy específicas. Cuando configura una sesión BGP hacia el IXP, puede simplemente decir "anuncia todas las rutas que tengan community 65001:1000 o 65001:2000, pero rechaza cualquier cosa con 65001:3000 o 65001:4000". Esta abstracción hace que su configuración sea más fácil de mantener y menos propensa a errores.

4.2 Políticas de Importación y Exportación

Para las sesiones en el IXP, su política de exportación debe funcionar como un filtro muy selectivo. Primero, debe permitir explícitamente los prefijos marcados con las communities que identifican sus rutas propias y las de sus clientes. Estos son los únicos prefijos que tienen lugar en el IXP.

Simultáneamente, debe denegar activamente los prefijos que llevan las communities de tránsito. Esta denegación explícita es importante porque previene accidentes: incluso si por algún error de configuración esos prefijos llegaran hasta este punto, serían bloqueados.

Finalmente, cualquier prefijo que no coincida con ninguna regla anterior debe ser denegado por defecto. Esta es la práctica de "denegar implícito" que es fundamental en seguridad de red.

La política de importación desde el IXP también requiere atención cuidadosa. Cada prefijo que recibe del IXP debe ser inmediatamente marcado con la community correspondiente, por ejemplo 65001:4000. Esta marca es su primera línea de defensa contra la re-exportación accidental de estas rutas hacia tránsito.

Además de marcar, debe validar la longitud de los prefijos recibidos. Para IPv4, generalmente se aceptan prefijos entre /8 y /24, rechazando cualquier cosa más específica que /24 a menos que haya un acuerdo explícito. Para IPv6, el rango típico es /16 a /48. Prefijos fuera de estos rangos son generalmente sospechosos y deben ser rechazados.

La validación del AS_PATH también es crítica. Su propio ASN nunca debe aparecer en el path de rutas que está recibiendo, ya que esto indicaría un loop de routing. Si su sistema de validación RPKI está funcionando, también debe aplicar estas verificaciones en este punto, dando preferencia a rutas con estado "valid" y rechazando aquellas con estado "invalid".
Para las sesiones con proveedores de tránsito, el patrón es similar pero invertido. Al exportar hacia tránsito, permite sus prefijos propios (65001:1000) y los de clientes (65001:2000), pero niega explícitamente cualquier cosa con la marca de IXP (65001:4000).

Al importar de tránsito, todos los prefijos recibidos deben marcarse con 65001:3000 y se les debe asignar una local-preference baja, típicamente 80. Esta preferencia baja asegura que su router siempre preferirá rutas aprendidas directamente en el IXP (que tendrán preferencia más alta, como 150) sobre las rutas de tránsito. Esto optimiza sus costos al maximizar el uso del peering sin costo y minimizar el tráfico por enlaces de tránsito pagados.

5. Filtros de Seguridad

5.1 Filtros de Prefijos Esenciales

La implementación de filtros de seguridad robustos es una responsabilidad fundamental de cualquier operador de red. Existen rangos de direcciones IP que, por diseño o por convención, nunca deben aparecer en el routing público de Internet. Estos rangos, comúnmente llamados "bogons", deben ser filtrados tanto en la importación como en la exportación de rutas.

Los prefijos privados definidos en RFC1918 para IPv4 y RFC4193 para IPv6 son el primer grupo que debe filtrar. Estos incluyen los bien conocidos 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16 para IPv4, y fc00::/7 para IPv6. Estos rangos están reservados explícitamente para uso privado y su aparición en Internet público es siempre un error o un intento malicioso.

Los prefijos de documentación también deben ser filtrados sin excepción. Estos incluyen 192.0.2.0/24, 198.51.100.0/24 y 203.0.113.0/24 para IPv4, junto con 2001:db8::/32 para IPv6. Estos rangos existen únicamente para ser usados en documentación y ejemplos, como este mismo documento, y nunca deben ser ruteados.

Otros rangos problemáticos incluyen las direcciones de loopback (127.0.0.0/8 y ::1/128), las direcciones link-local (169.254.0.0/16 y fe80::/10), y los rangos reservados para multicast (224.0.0.0/4 y ff00::/8). La presencia de cualquiera de estos en anuncios BGP indica un problema serio que debe ser rechazado inmediatamente.

Finalmente, la ruta por defecto (0.0.0.0/0 y ::/0) merece mención especial. En un IXP, nunca debe recibir ni anunciar la ruta por defecto. Su presencia indica que alguien está intentando anunciar acceso completo a Internet a través del IXP, lo cual es inadecuado y potencialmente peligroso.

5.2 Filtros de Longitud de Prefijo

Más allá de filtrar rangos específicos, también debe implementar filtros basados en la longitud de los prefijos. Para IPv4, el rango generalmente aceptado va desde /8 hasta /24. Los prefijos más pequeños que /8 son extremadamente raros y generalmente representan errores. Los prefijos más específicos que /24 también son problemáticos porque fragmentan excesivamente el espacio de direcciones y pueden ser usados en ataques de secuestro de prefijos.

Para IPv6, los parámetros son diferentes debido a la naturaleza distinta del protocolo. El rango típicamente aceptado va desde /16 hasta /48. Los registros regionales generalmente asignan bloques /32 o mayores a operadores, quienes luego pueden subdividirlos en /48s para propósitos específicos.
La razón para estos límites es tanto práctica como de seguridad. Prefijos excesivamente específicos aumentan el tamaño de las tablas de routing globales sin proporcionar beneficios proporcionales. Además, pueden ser usados en ataques donde un atacante anuncia un prefijo más específico que el legítimo para secuestrar tráfico.

5.3 Validación de AS_PATH

El AS_PATH es uno de los atributos más importantes de BGP y su validación es crucial para prevenir loops y detectar anomalías. La verificación más básica pero esencial es asegurarse de que su propio ASN no aparezca en el path de las rutas que está recibiendo. Si aparece, significa que la ruta ha pasado por su red antes, creando un loop que debe ser rechazado inmediatamente.

También es prudente implementar un límite en la longitud del AS_PATH. En un Internet bien conectado, las rutas generalmente tienen paths cortos. Un path que contiene más de 10 o 15 ASNs es sospechoso y puede indicar varias cosas: una cadena excesivamente larga de relaciones de tránsito, AS_PATH prepending excesivo usado para manipular routing, o posiblemente un intento de ocultar el verdadero origen de una ruta.

Los números de AS privados, que existen en el rango 64512-65534 para ASNs de 16 bits, nunca deben aparecer en el routing público de Internet. Estos números son análogos a los rangos de IP privados y su presencia en un path público indica un error de configuración grave. Si ve estos números en rutas recibidas, debe rechazarlas inmediatamente.

6. Errores Comunes a Evitar

6.1 Los Nueve Errores Más Frecuentes

1. Anunciar full table en IXP: Esto ocurre cuando un operador configura erróneamente su política de exportación y termina anunciando todas las rutas que aprendió de sus proveedores de tránsito hacia el IXP. Este error puede causar problemas masivos, saturando las tablas de routing de otros participantes y creando confusión generalizada en el routing. La ruta por defecto nunca debe aparecer en un IXP, y mucho menos la tabla completa de Internet.
2. Anunciar rutas de IXP a tránsito: Cuando un operador anuncia a sus proveedores de tránsito las rutas que aprendió en el IXP, está convirtiendo su red en tránsito no autorizado. Esto no solo viola los términos de servicio típicos del tránsito, sino que puede generar costos inesperados y problemas legales. Imagine recibir una factura enorme porque estuvo transportando tráfico entre el IXP y su proveedor upstream sin saberlo.
3. No configurar max-prefixes: Sin este límite, si un peer comienza a anunciar rutas incorrectas masivamente, su router las aceptará todas, potencialmente causando problemas de memoria y procesamiento. El límite de prefijos actúa como un fusible: si algo va mal, la sesión se cae antes de que cause daño real a su sistema.
4. Aceptar prefijos muy específicos: Un atacante puede anunciar un prefijo más específico que el legítimo para atraer tráfico hacia su red. Sin filtros de longitud apropiados, su red podría ayudar inadvertidamente en este ataque.
5. No filtrar prefijos privados: Los rangos RFC1918 y otros prefijos reservados nunca deben aparecer en routing público, y permitir su paso indica una configuración descuidada que probablemente tiene otros problemas.
6. No validar AS_PATH: Si su propio ASN aparece en el path de una ruta recibida, indica un loop que debe ser detectado y rechazado inmediatamente. Sin esta validación, puede terminar con routing circular que nunca converge correctamente.
7. No implementar RPKI: Sin validación RPKI, su red es vulnerable a aceptar anuncios fraudulentos de prefijos, lo que puede llevar a tráfico mal dirigido o interceptado.
8. Ignorar las políticas del IXP: No leer y seguir estas políticas puede resultar en problemas técnicos o incluso en desconexión.

9. No documentar la configuración: Cuando ocurre un problema a las 3 AM, tener documentación clara sobre qué se configuró y por qué es invaluable. Más aún, cuando se necesita transferir conocimiento a nuevos miembros del equipo o cuando se debe revisar decisiones pasadas, la documentación ausente convierte cada tarea en arqueología de configuraciones.

6.2 Señales de Configuración Incorrecta

Existen varios indicadores que pueden alertarle sobre problemas en su configuración BGP. Estar atento a estas señales puede ayudarle a detectar y corregir problemas antes de que escalen.

Si está recibiendo más de un millón de rutas en su sesión con el IXP, es casi seguro que algo está mal. Los IXPs típicamente no tienen tantas rutas únicas entre sus participantes. Esta situación probablemente indica que alguien está anunciando la tabla completa, posiblemente usted mismo si la alarma viene de un peer que se queja.

Un AS_PATH excesivamente largo, digamos más de 10 hops, es otra señal de alerta. Las rutas en un IXP típicamente tienen paths cortos porque representan conexiones directas o casi directas. Paths largos pueden indicar problemas de configuración, AS_PATH prepending excesivo, o rutas que no deberían estar en el IXP.

Si su sesión BGP está en constante flapping, estableciéndose y cayéndose repetidamente, busque problemas con timers BGP, problemas de capa 2 o 3, o posiblemente límites de prefijos que se están excediendo regularmente. El flapping no solo afecta su conectividad sino que crea inestabilidad para todos los participantes que tienen rutas a través de usted.

Cuando RPKI marca sus prefijos o los que está recibiendo como "Invalid", debe investigar inmediatamente. Esto puede indicar que sus ROAs están mal configurados, que está originando prefijos sin autorización, o que está aceptando anuncios fraudulentos.

Si el tráfico no está fluyendo como esperaba, con patrones asimétricos o rutas subóptimas evidentes, revise sus políticas de local-preference y sus filtros. A menudo, el tráfico "sorpresivo" indica que las rutas no están siendo preferidas o rechazadas como se planeó.

Las quejas de otros participantes del IXP nunca deben ser ignoradas. Si el NOC del IXP o un peer le contacta con preocupaciones sobre sus anuncios, tómelo seriamente. La comunidad técnica es generalmente muy profesional y estas comunicaciones casi siempre indican problemas reales.

Finalmente, si ve rutas duplicadas con diferentes AS_PATHs que apuntan al mismo destino pero con características muy diferentes, investigue. Esto puede indicar problemas de convergencia, anuncios incorrectos, o intentos de manipulación de tráfico.

6.3 Ejemplo de matriz de revisión

Origen del prefijo	Tag de Community Interna	¿Exporta a IXP?	¿Exporta a Tránsito Upstream?
Infraestructura propia	65017:40:00	Sí	Sí
Clientes Downstream	65034:20:00	Sí	Sí
Aprendido de Tránsito	65051:00:00	NO (Bloqueo Crítico)	NO
Aprendido de IXP	65067:40:00	-	NO (Evita filtrado de tránsito)

7. Checklist de Implementación

7.1 Antes de Conectar al IXP

- □ Obtener información del IXP:
- □ Rango de IPs asignado
- □ ASN del Route Server (si aplica)
- □ Políticas específicas del IXP
- □ BGP Communities soportadas
- □ Contactos técnicos
- □ Preparar su red:
- □ Crear ROAs en RPKI para sus prefijos
- □ Registrar prefijos en IRR (LACNIC, etc.)
- □ Documentar sus prefijos a anunciar
- □ Preparar filtros de exportación
- □ Preparar filtros de importación
- □ Configurar equipos:
- □ Configurar interfaz física hacia IXP
- □ Configurar direcciones IP del IXP
- □ Preparar configuración BGP
- □ Configurar políticas de routing

- □ Configurar filtros de seguridad

7.2 Durante la Configuración

- □ Configuración BGP:
- □ Configurar sesión con Route Server
- □ Aplicar filtros de exportación
- □ Aplicar filtros de importación
- □ Configurar max-prefixes apropiado
- □ Configurar MD5 password (si aplica)
- □ Configurar timers BGP
- □ Configurar local-preference

- □ Validación:
- □ Verificar sesión BGP establecida
- □ Verificar prefijos anunciados correctos
- □ Verificar prefijos recibidos razonables
- □ Verificar no se están anunciando rutas de tránsito
- □ Verificar RPKI validation funcionando
- □ Probar conectividad con peers

7.3 Después de Conectar

- □ Monitoreo:
- □ Configurar alertas para sesión down
- □ Configurar alertas para cambios de prefijos
- □ Monitorear tráfico
- □ Revisar logs regularmente
- □ Verificar en Looking Glass del IXP
- □ Documentación:
- □ Documentar configuración implementada
- □ Actualizar PeeringDB
- □ Actualizar documentación interna
- □ Compartir con equipo
- □ Programar revisión periódica
- □ Optimización:
- □ Establecer sesiones directas con peers clave
- □ Optimizar políticas según tráfico observado
- □ Participar en comunidad del IXP
- □ Asistir a eventos técnicos

8. Recursos y Referencias

8.1 Documentación Estándar

- RFCs Relevantes:
- RFC 4271 - BGP-4
- RFC 7454 - BGP Operations and Security
- RFC 8212 - Default External BGP (EBGP) Route Propagation
- RFC 6811 - BGP Prefix Origin Validation
- RFC 8205 - BGPsec Protocol
- RFC 1997 - BGP Communities
- RFC 7999 - BLACKHOLE Community
- BCPs (Best Current Practices):
- BCP 194 (RFC 7454) - BGP Operations and Security
- BCP 38 (RFC 2827) - Ingress Filtering
- MANRS - Mutually Agreed Norms for Routing Security

8.2 Herramientas Online

Validación y Testing

- bgp.tools - Información de ASN/prefijos
- stat.ripe.net - Estadísticas y validación
- peeringdb.com - Base de datos de peering
- bgp.he.net - Hurricane Electric BGP Toolkit
- irrexplorer.nlnog.net - Validación de IRR
- query.milacnic.lacnic.net - Información de ASN/prefijos LACNIC

RPKI

- - rpki.cloudflare.com - Validador público
- - rpki-validator.ripe.net – Validador público

Monitoreo

- - bgpstream.com - Eventos BGP globales
- - bgpmon.net - Monitoreo de prefijos

9. Glosario de Términos

ASN (Autonomous System Number): Identificador único para un sistema autónomo en Internet.

BGP (Border Gateway Protocol): Protocolo de routing usado entre sistemas autónomos.

IRR (Internet Routing Registry): Base de datos de políticas de routing.

IXP (Internet Exchange Point): Infraestructura que permite el intercambio de tráfico entre redes.

Local Preference: Atributo BGP que indica preferencia de rutas dentro de un AS.

MED (Multi-Exit Discriminator): Métrica BGP para influenciar entrada de tráfico.

Peering: Interconexión entre redes para intercambiar tráfico.

ROA (Route Origin Authorization): Registro RPKI que autoriza a un AS a anunciar un prefijo.

RPKI (Resource PKI): Infraestructura de validación de origen de rutas.

Route Server: Servidor del IXP que facilita sesiones BGP multilaterales.

Tránsito: Servicio de conectividad completa a Internet provisto por un upstream.

10. Ejemplos de Configuración

10.1 Cisco IOS/IOS-XE

! Definir prefijos propios

- ip prefix-list OWN-PREFIXES seq 5 permit 198.51.100.0/24
- ip prefix-list OWN-PREFIXES seq 10 permit 203.0.113.0/24

! Filtrar prefijos inválidos (ejemplo parcial)

- ip prefix-list BOGONS deny 0.0.0.0/8 le 32
- ip prefix-list BOGONS deny 10.0.0.0/8 le 32
- ip prefix-list BOGONS deny 172.16.0.0/12 le 32
- ip prefix-list BOGONS deny 192.168.0.0/16 le 32
- ip prefix-list BOGONS deny 192.0.2.0/24 le 32

! ... continuar con otros bogons

! Filtrar longitud de prefijos

- ip prefix-list PREFIX-LENGTH permit 0.0.0.0/0 ge 8 le 24

! Route-map para exportar al IXP
route-map IXP-OUT permit 10
match ip address prefix-list OWN-PREFIXES
set community 65001:1000

! Route-map para importar del IXP
route-map IXP-IN deny 10
match ip address prefix-list BOGONS
!
route-map IXP-IN deny 20
match ip address prefix-list PREFIX-LENGTH

match as-path 1
!
route-map IXP-IN permit 100
set local-preference 150
set community 65001:4000 additive

```
! Configuración del neighbor (Route Server)
router bgp 65001
neighbor 192.0.2.1 remote-as 65500
neighbor 192.0.2.1 description IXP-RouteServer
neighbor 192.0.2.1 password 7 [encrypted-password]
!
address-family ipv4
neighbor 192.0.2.1 activate
neighbor 192.0.2.1 route-map IXP-OUT out
neighbor 192.0.2.1 route-map IXP-IN in
neighbor 192.0.2.1 maximum-prefix 50000 90
```

10.2 Juniper JunOS

```
# Definir prefijos propios
policy-options {
prefix-list own-prefixes {
198.51.100.0/24;
203.0.113.0/24;
}

# Prefijos bogons (ejemplo parcial)
prefix-list bogons {
0.0.0.0/8;
10.0.0.0/8;
172.16.0.0/12;
192.168.0.0/16;
192.0.2.0/24;
# ... continuar
}
}
```

```
# Policy para exportar al IXP
policy-options {
policy-statement ixp-export {
term own-prefixes {
from {
prefix-list own-prefixes;
}
then {
community add own-routes;
accept;
}
}
term reject-all {
then reject;
}
}

# Policy para importar del IXP
policy-statement ixp-import {
term reject-bogons {
from {
prefix-list bogons;
}
then reject;
}
term reject-long-prefixes {
from {
route-filter 0.0.0.0/0 prefix-length-range /25-/32;
}
then reject;
}
term accept-all {
then {
local-preference 150;
community add learned-from-ixp;
accept;
}
}
}
```

```
# Communities
community own-routes members 65001:1000;
community learned-from-ixp members 65001:4000;
}

# Configuración del neighbor
protocols {
bgp {
group ixp-peers {
type external;
peer-as 65500;
neighbor 192.0.2.1 {
description "IXP Route Server";
authentication-key "[encrypted-key]";
import ixp-import;
export ixp-export;
family inet {
unicast {
prefix-limit {
maximum 50000;
teardown 90;
}
}
}
}
}
}
}
```

10.3 BIRD

```
# /etc/bird/bird.conf

# Definir ASN y Router ID
router id 198.51.100.1;

# Prefijos propios
define OWN_PREFIXES = [
198.51.100.0/24,
203.0.113.0/24
];

# Prefijos bogons (ejemplo parcial)
define BOGONS = [
0.0.0.0/8+,
10.0.0.0/8+,
172.16.0.0/12+,
192.168.0.0/16+,
192.0.2.0/24+,
# ... continuar
0.0.0.0/0{25,32}, # Rechazar más específicos que /24
0.0.0.0/0{0,7}  # Rechazar menos específicos que /8
];

# Función para validar prefijos
function is_valid_prefix()

{
if net ~ BOGONS then return false;
if net ~ OWN_PREFIXES then return true;
return false;
}

# Función para marcar rutas propias
function mark_own_routes()
{
bgp_community.add((65001,1000));
}
```

```
# Función para marcar rutas de IXP
function mark_ixp_routes()
{
bgp_local_pref = 150;
bgp_community.add((65001,4000));
}

# Filtro de exportación al IXP
filter ixp_export
{
if net ~ OWN_PREFIXES then {
mark_own_routes();
accept;
}
reject;
}

# Filtro de importación del IXP
filter ixp_import
{
if net ~ BOGONS then reject;
if bgp_path.len > 10 then reject;

mark_ixp_routes();
accept;
}

# Protocolo BGP para Route Server del IXP
protocol bgp ixp_rs {
description "IXP Route Server";
local as 65001;
neighbor 192.0.2.1 as 65500;
password "your-bgp-password";

ipv4 {
import filter ixp_import;
export filter ixp_export;
import limit 50000 action restart;
};
```

```
# No modificar next-hop en IXP
next hop self no;
}
```

10.4 ARISTA

```
! Definir prefijos propios
ip prefix-list OWN-PREFIXES seq 5 permit 198.51.100.0/24
ip prefix-list OWN-PREFIXES seq 10 permit 203.0.113.0/24

! Filtrar prefijos inválidos / bogons
ip prefix-list BOGONS seq 5 deny 0.0.0.0/8 le 32
ip prefix-list BOGONS seq 10 deny 10.0.0.0/8 le 32
ip prefix-list BOGONS seq 15 deny 172.16.0.0/12 le 32
ip prefix-list BOGONS seq 20 deny 192.168.0.0/16 le 32
ip prefix-list BOGONS seq 25 deny 192.0.2.0/24 le 32
ip prefix-list BOGONS seq 100 permit 0.0.0.0/0 le 32

! Filtrar longitud de prefijos aceptables desde el IXP
ip prefix-list PREFIX-LENGTH seq 10 permit 0.0.0.0/0 ge 8 le 24

! AS-PATH demasiado largo, ejemplo: más de 10 ASNs
ip as-path access-list AS-PATH-LONG permit ^([0-9]+_){10,}

! Route-map para exportar al IXP
route-map IXP-OUT permit 10
match ip address prefix-list OWN-PREFIXES

set community 65001:1000 additive
!
route-map IXP-OUT deny 100

! Route-map para importar del IXP
route-map IXP-IN deny 10
match ip address prefix-list BOGONS
!
route-map IXP-IN deny 20
match invert-result ip address prefix-list PREFIX-LENGTH
```

```
!
route-map IXP-IN deny 30
match as-path AS-PATH-LONG
!
route-map IXP-IN permit 100
set local-preference 150
set community 65001:4000 additive

! Configuración del neighbor Route Server
router bgp 65001
router-id 198.51.100.1
neighbor 192.0.2.1 remote-as 65500
neighbor 192.0.2.1 description IXP-RouteServer
neighbor 192.0.2.1 password 7 [encrypted-password]
neighbor 192.0.2.1 send-community
neighbor 192.0.2.1 route-map IXP-OUT out
neighbor 192.0.2.1 route-map IXP-IN in
neighbor 192.0.2.1 maximum-routes 50000 warning-limit 90
!
address-family ipv4
neighbor 192.0.2.1 activate
```

Feedback: Agradecemos sus comentarios y sugerencias para mejorar este documento. Envíe sus aportes a: lacixtech@socium.cr