Material de descarga - Módulo 6
Recomendaciones y mejores prácticas

Introducción:

Bienvenidos al sexto módulo del curso “Fundamentos de BGP e introducción a RPKI” de LACNIC. En esta oportunidad se podrá aprender acerca de la selección del mejor camino a seguir para alcanzar un destino. Más adelante se verá cuáles son las prácticas recomendadas y para finalizar se verá un resumen de los temas tratados.

.

TEMA 1 - Selección del mejor camino

Como se ha mencionado desde el principio, BGP es un protocolo de ruteo que basa sus decisiones en los atributos de los prefijos. ¿Pero cómo es que los evalúa? Sigue lo que se llama un algoritmo de decisión. BGP irá evaluando sentencias del algoritmo una a una, en forma secuencial y respetando el orden, y cuando una de sentencias pueda marcar la diferencia entre las rutas, la decisión sobre la mejor ruta estará tomada y el algoritmo se detendrá.

Se verá ahora cómo es la selección del mejor camino, cuando se tienen varias alternativas para alcanzar un destino.

Lo primero que evaluará BGP es naturalmente si el *next-hop* indicado en la ruta es accesible a través de IP, pues si no lo es, la ruta automáticamente se descarta.

Si se tienen varias rutas a un mismo destino y todas son con *next-hop* alcanzables, entonces BGP evaluará si alguna de las rutas fue aprendida por iBGP, la opción de “synchronization” está habilitada, y la ruta no está en la tabla de alguno de los protocolos de ruteo interno. En esos casos la ruta es descartada. Vale la pena aclarar que hoy en día, y desde hace bastante tiempo ya, la opción de synchronization viene deshabilitada por default en la mayoría de los sistemas operativos de los *router*, por lo que se ha decidido no incluirlo en este curso. No obstante, merece atención sobre todo debido a que tiene alta precedencia en el algoritmo de decisión, por lo que se aconseja su lectura en bibliografías de referencia.

Si las rutas no son descartadas en el paso anterior, entonces BGP continuará con el proceso de evaluación.

Si estuviera configurado el atributo **Weight**, seguiría por éste y elegirá la ruta con mayor peso.

Si el atributo Weight no logra decidir, entonces BGP evaluará nuevamente y elegirá la ruta de mayor **Local_Preference**.

Si el Local_Preference es el mismo, entonces BGP preferirá la ruta que haya sido originada en el *router*, ya sea por el comando *network* o con *redistribution*.

Si ninguno de los pasos anteriores se cumple, BGP evaluará cuál es el AS_Path más corto. Notar que recién aquí BGP tiene en cuenta la longitud del AS_Path, que da una idea de la distancia a la que se encuentra el destino (los AS por los que hay que pasar). En muchos casos este es el criterio por el cual se definirá la mejor ruta, si no se ha hecho uso de Weight o Local_Preference.

Si aún así no puede decidirse la mejor ruta, entonces se evaluará el código de origen y se elegirá el de menor valor, teniendo en cuenta que IGP tiene menor valor que EGP, y a su vez éste es preferido antes que una ruta de origen desconocido o “incomplete”.

Si el origen de las rutas es el mismo, ha llegado la hora de que BGP evalúe el atributo MED. Es importante aclarar que para que este atributo sea evaluado, los *neighbors* desde donde se aprendieron las rutas deben pertenecer al mismo sistema autónomo, a no ser que se especifique lo contrario en la configuración de BGP con el comando “bgp always-compare-med”. El menor valor de MED es preferido.

Llegada esta instancia de decisión, se preferirán las rutas que se aprendan por eBGP, a las aprendidas por iBGP.

Si aún no se ha podido tomar una decisión, BGP preferirá la ruta cuyo *Next-Hop* tenga la menor métrica en el IGP.

Es difícil que se tenga que llegar a este punto de decisión porque en general en cualquiera de las instancias anteriores se puede decidir cuál es la mejor ruta. No obstante, si se llegara hasta acá, BGP decidiría en base a la ruta que tuviera menor “router-ID”, que es la mayor IP de las interfaces de un *router*.

Gráficamente se puede sintetizar de la siguiente manera:

1. Evaluación del NH

El NH es alcanzable?

SÍ → Evalúa synchronization

NO → Ruta se descarta

2. Evaluación de synchronization

- iBGP
- Synch habilitado
- No hay entrada en la tabla de ruteo

SÍ → Ruta se descarta

NO → Continúa el proceso de evaluación

3. Evaluación del Weight

Weight ≠

SÍ → Elige ruta > Weight

NO → Evalúa Local_Pref

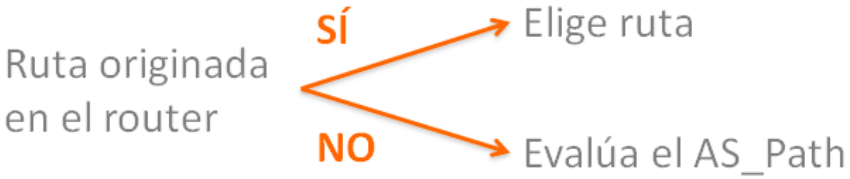
4. Evaluación del Local_Pref

Local_Pref ≠

SÍ → Elige ruta > Local_Pref

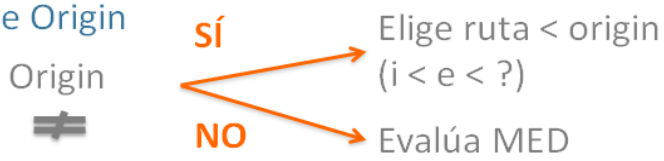
NO → Evalúa si la ruta fue originada en ese router

5. Origin de la ruta

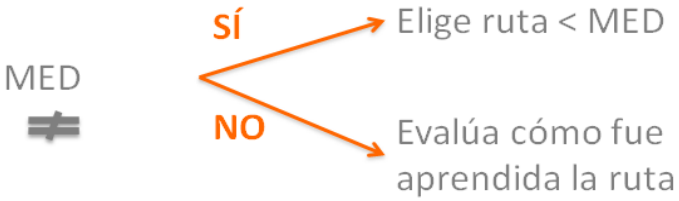


6. Evaluación del AS_Path

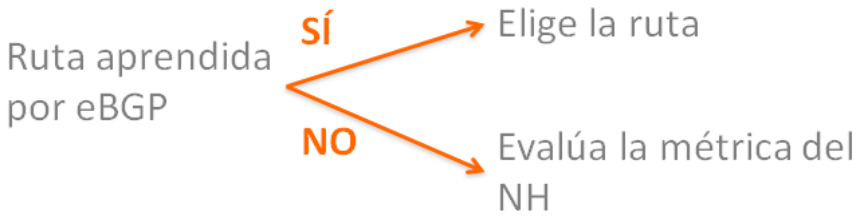
7. Evaluación de Origin



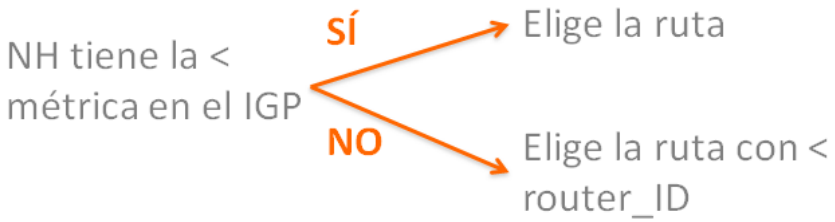
8. Evaluación del MED



9. Evaluación de cómo fue aprendida la ruta



10. Evaluación de la métrica del NH



Tema 2 - BCP (Best Current Practices)

Llegada esta instancia del curso, ya se ha tomado conocimiento de cómo realizar configuraciones básicas en BGP.

No obstante, más allá de que hagamos una configuración básica, no deja de ser crítica, y anunciar y recibir prefijos de Internet es una responsabilidad grande para cualquier administrador de red.

Por este motivo, considerar algunas recomendaciones y buenas prácticas ayudará mucho a realizar una buena gestión de la red. Se verán algunas de éstas.

En primer lugar, es muy importante considerar los roles de los IGPs y el del BGP. La recomendación es que siempre se utilice un IGP para llevar información de las rutas de infraestructura de la organización, y que se utilice BGP para las rutas de Internet y las de clientes, discriminando entre iBGP y eBGP de la siguiente manera:

- **eBGP** naturalmente para las sesiones con *neighbors* pertenecientes a otros AS.
- **iBGP** utilizarlo para transportar:
  - Los prefijos de Internet a través del *backbone*
  - Los prefijos de los clientes

Es importante también tener en cuenta la sumarización de prefijos y no desagregar más de lo necesario. Hacia afuera de nuestro sistema autónomo sólo se debería mostrar la información de prefijos sumarizada, no desagregando las redes a menos que haya alguna razón realmente válida.

Otra buena práctica consiste en utilizar direcciones /32 para las interfaces de *loopbacks* y levantar las sesiones de iBGP con ellas.

El uso de "Peer Groups", para agrupar vecinos con las mismas características de ruteo, por ejemplo: clientes, proveedores, tránsito, etc.

Para mitigar el robo de prefijos, algo que se puede hacer fácilmente es utilizar passwords en la sesiones de BGP.

Entre lo que se recomienda como buena práctica NO hacer, está:

- Redistribuir BGP dentro de un IGP.
- Redistribuir prefijos IGP dentro del BGP.
- Usar IGP para transportar prefijos de clientes o redes externas.

Finalmente, se verán qué prefijos no se debería aceptar recibir de ningún *neighbor*, ni anunciarlos:

- Prefijos definidos en el RFC1918. Ver cuáles son en la URL: https://tools.ietf.org/html/rfc1918
- Los prefijos propios de la organización (para evitar *loops*).
- La ruta por defecto, a no ser que se requiera.
- Prefijos mayores a /24 (o sea, bloques de redes pequeñas como /25, /26, etc.).

A continuación, se muestra un ejemplo de un filtro implementado con prefix-list para ser implementado a la entrada de una sesión BGP:

```
ip prefix-list in-filter deny 0.0.0.0/0     ! Block default
ip prefix-list in-filter deny 0.0.0.0/8 le 32
ip prefix-list in-filter deny 10.0.0.0/8 le 32
ip prefix-list in-filter deny 101.10.0.0/19 le 32  ! Block local prefix
ip prefix-list in-filter deny 127.0.0.0/8 le 32
ip prefix-list in-filter deny 169.254.0.0/16 le 32
ip prefix-list in-filter deny 172.16.0.0/12 le 32
ip prefix-list in-filter deny 192.0.2.0/24 le 32
ip prefix-list in-filter deny 192.168.0.0/16 le 32
ip prefix-list in-filter deny 224.0.0.0/3 le 32   ! Block multicast
ip prefix-list in-filter deny 0.0.0.0/0 ge 25     ! Block prefixes >/24
ip prefix-list in-filter permit 0.0.0.0/0 le 32
```

También, en el caso de ISP es importante aplicar las reglas de la BCP38 (RFC 2827), a fin de no permitir *spoofing* de direcciones. Para ver una introducción al tema referirse a: www.bcp38.info

Como nota final en este tema, para quienes estén interesados en contribuir a la mejora del ruteo global, pueden ver en https://www.routingmanifesto.org el documento MANRS: *Mutually Agreed Norms for Routing Security*, que es una iniciativa para despertar conciencia y promover acciones en los ISPs y otras organizaciones para un ruteo más seguro y estable en Internet.

Tema 3 - Resumen de lo visto

Llegando al tercer tema del sexto módulo, se resumirán los principales conceptos que se han visto en este curso de BGP.

BGP es un protocolo de ruteo externo o EGP que se utiliza para la comunicación de sistemas autónomos en Internet.

Fue concebido para llevar información de las rutas externas a nuestro AS, ya sea dentro o fuera del mismo (iBGP o eBGP).

Trabaja aprendiendo y anunciando rutas a través de sesiones con *routers* que se denominan "*neighbors*", que se deben configurar explícitamente.

Para saber cuál es la mejor ruta utiliza un algoritmo de decisión basado en atributos.

Una administración controlada de los prefijos que se anuncian y reciben a través de BGP supone la implementación de políticas en las sesiones, tanto en la entrada como en la salida de las mismas. Para eso se vieron los filtros por IP y por AS_Path, los route-maps y una gran cantidad de atributos.

BGP se despliega en toda la Internet gracias a una gran cadena de confianza entre los administradores de las redes. No obstante, diferentes formas de ataques pueden producir caminos indeseados del tráfico de Internet, como el secuestro de rutas o los *route leaks*.

Para mitigar esto existen diferentes medidas que se pueden tomar, pero la principal de ellas, por aportar la garantía del origen de las rutas, es RPKI.

Finalmente existe documentación y RFCs que ayudan a llevar adelante implementaciones de BGP con buenas prácticas y recomendaciones para que nuestra organización también sea parte la

comunidad que vela por el buen crecimiento de Internet.

Ahora sí, se ha llegado al final del curso “Fundamentos de BGP e Introducción a RPKI”. Esperamos hayan sacado provecho de este material y las prácticas.

Volver a compartir con ustedes estos cursos, es un deseo de **Campus LACNIC**.