¿Cómo levantar un peering en IPv6 only?

Autor: Alejandro Acosta, José G. Cotúa, Alejandro D'Egidio
Coordinación/revisión: Guillermo Cicileo
Edición: Carolina Badano, Martín Mañana
Área: Tecnología

lacnic
www.lacnic.net

Introducción

El siguiente artículo presenta de manera ordenada los pasos a seguir para levantar un peering BGP entre dos routers IPv6 Only.

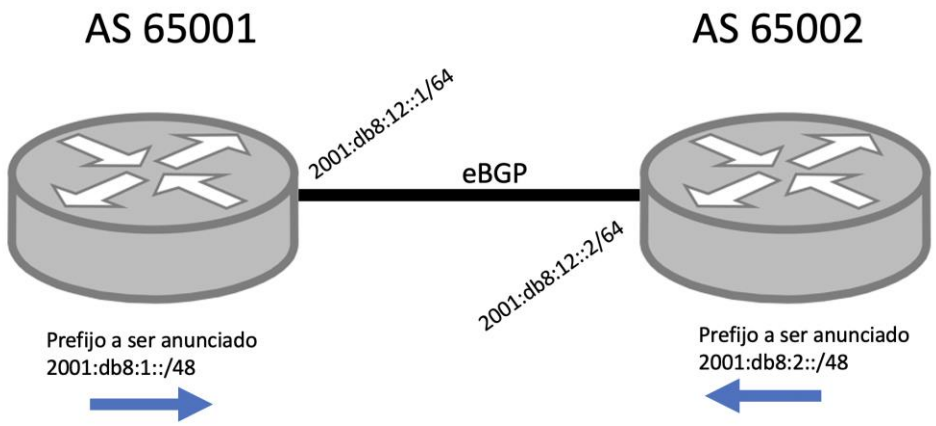
En el argot de BGP ***peering*** se conoce como (traducido de [1]):

“Dos enrutadores que han establecido una conexión para intercambiar información BGP se denominan pares BGP. Dichos pares BGP intercambian información de enrutamiento entre ellos a través de sesiones BGP ….. “

Prerrequisitos

- dos enrutadores
- conectividad entre los enrutadores
- soporte IPv6 en ambos equipos tanto en conectividad como en BGP

Topología



Para Enrutador R1:

- IPv6 de R1: 2001:db8:12::1/64
- Router-ID de R1: 10.111.111.1
- Prefijo v6 que será anunciado por R1: 2001:db8:1::/48
- IPv6 /128 de Loopback: 2001:db8:1:11::cafe/128

Para Enrutador R2:

- IPv6 R2: 2001:db8:12::2/64
- Router-ID de R2: 10.222.222.2
- Prefijo v6 que será anunciado por R2: 2001:db8:2::/48
- IPv6 /128 de Loopback: 2001:db8:2:11::cafe/128

Pasos a seguir

Paso 1 - Conectividad IPv6 entre los enrutadores

Para establecer y probar la conectividad entre los enrutadores debemos:

1. Establecer la conexión física:
    - Asegurarse que esté realizada la conexión física entre las interfaces asignadas de ambos enrutadores.
    - Verificar que dicho enlace esté UP.
2. Configurar IPv6 en las interfaces relacionadas:
    - Asignar el direccionamiento IPv6 de WAN que se utilizará en el enlace. Todo el direccionamiento utilizado en este documento pertenece al segmento 2001:db8::/32 reservado para documentación.
    - Configurar IPv6 en las interfaces relacionadas.
3. Probar conectividad IPv6:
    - Realizar un Ping IPv6 desde alguno de los dos equipos.
    - Si no se puede alcanzar es imprescindible arreglar esta situación antes de continuar.
    - Es posible que el destino esté filtrando los paquetes de Ping IPv6 (ICMPv6 Echo Request/Reply y eso no implica que no vaya a funcionar BGP; verificar en el otro equipo.

Nota: BGP por defecto piensa que su vecino se encuentra directamente conectado, es decir, el vecino es el siguiente dispositivo en la red. En caso de no ser así se puede requerir mayor configuración tal como eBGP Multihop [2], pero este tema no lo cubriremos en este how to.

Cisco (IOS-15.4)

R1

Estado de Interfaz:

```
R1#sh int et0/0
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.0100 (bia aabb.cc00.0100)
```

Configuración de Interfaz:

```
interface Ethernet0/0
 description ## R1 to R2 ##
 no ip address
 ipv6 address 2001:DB8:12::1/64
 ipv6 nd ra suppress                #recomendado, no envía mensajes de RA
```

R2
Estado de Interfaz:
R2#sh int et0/0
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.0200 (bia aabb.cc00.0200)

Configuración de Interfaz:

```
interface Ethernet0/0
 description ## R2 to R1 ##
 no ip address
 ipv6 address 2001:DB8:12::2/64
 ipv6 nd ra suppress
```

Prueba de conectividad:

```
R2#ping ipv6 2001:DB8:12::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:12::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/6 ms
R2#
R2#sh ipv6 neighbors
IPv6 Address                              Age Link-layer Addr State Interface
2001:DB8:12::1                              0 aabb.cc00.0100  REACH Et0/0
FE80::A8BB:CCFF:FE00:100                   12 aabb.cc00.0100  STALE Et0/0
```

¿Crear la sesión BGP entre direcciones Link Local (LLA) o Global Unicast Addresses (GUA)?

En algunas ocasiones tendremos que tomar la decisión de cómo crear la sesión BGP, existen 3 posibilidades:

- Utilizar direcciones Link Local (LLA),
- Utilizar direcciones globales (GUA),
- Utilizar direcciones ULA (Unique Local Address).

Las primeras dos opciones son las más comúnmente utilizadas.

Entonces, ¿qué utilizo para crear la sesión BGP?

Te daremos una respuesta directa, pero antes repasemos estas premisas:

1. Recordemos que los mensajes BGP contienen atributos, siendo uno de ellos el atributo NextHop [3]. Este atributo contiene una información muy sencilla: el salto que se debe utilizar para alcanzar un destino.
2. Un router (un eBGP Speaker) al aprender un prefijo de otro AS copia el atributo de nexthop hacia su red iBGP.
3. Una red de speakers iBGP tradicionalmente tendrá un IGP.

4. Las direcciones Link Local tienen alcance local, tan solo el propio bus de la red, la LAN, el SSID, etc. **No** pueden ser enrutadas.

Quizás ya en este momento te has respondido qué utilizar.
Nuestra recomendación es crear la sesión BGP sobre GUA, y ahora que repasamos las premisas es fácil responder con una pregunta: ¿cómo un eBGP speaker va a copiar una dirección Link Local en el nexthop hacia sus iBGP speakers? Sencillo: **no** puede (claro, existen algunos trucos pero no lleguemos hasta ello).

Paso 2 - Definir el Router-ID en los diferentes routers

Debido a que estamos hablando de equipos IPv6 Only, asumimos que los dispositivos no tendrán direccionamiento IPv4. ¿Qué tiene que ver?
Explicamos brevemente:

- ¿Para qué un router-id?. El router-id es un campo de 32 bits que viaja en el mensaje OPEN de BGP, dicho campo (llamado BGP Identifier) es obligatorio y se representa en un formato de dirección IPv4.
- Los enrutadores tienen un mecanismo para obtener su router-id.
- Si el router es IPv6 Only el equipo no podrá averiguar su router-id
- Si el router no puede averiguar su router-id el administrador debe configurar uno explícitamente dentro del proceso BGP.

Paso 3 - Realizar las configuraciones en los routers

Vamos a mostrar dos ejemplos: Mikrotik y Cisco.Podremos darnos cuenta que la información es exactamente la misma, lo que cambia es la manera y comandos del sistema operativo. En el caso de Mikrotik utilizaremos la versión 6.x.

Configuración en routers

Mikrotik (RouterOS v6)

Enrutador R1

Configuración de la interfaz loopback

```
/interface bridge add name=loopback protocol-mode=none disabled=no
/ipv6 address add address=2001:db8:1:11::cafe/128 advertise=no interface=loopback
```

Configuración del proceso/instancia BGP

```
/routing bgp instance add name=AS65001 as=65001 router-id=10.111.111.1
```

Configuración del Peer

```
/routing bgp peer add name=HACIAR2 instance=AS65001 remote-address=2001:db8:12:2 remote-
as=65002 address-families=ipv6
```

Anuncio de prefijo

```
routing bgp network add network=2001:db8:1::/48 synchronize=no
```

Enrutador R2

Configuración de la interfaz loopback

```
/interface bridge add name=loopback protocol-mode=none disabled=no
/ipv6 address add address=2001:db8:2:11::cafe/128 advertise=no interface=loopback
```

Configuración del proceso/instancia BGP

```
/routing bgp instance add name=AS65002 as=65002 router-id=10.222.222.2
```

Configuración del Peer

```
/routing bgp peer add name=HACIAR1 instance=AS65002 remote-address=2001:db8:12:1 remote-
as=65001 address-families=ipv6
```

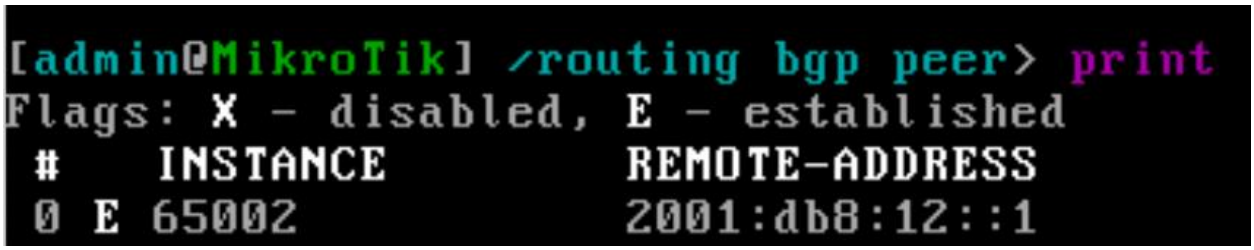
Anuncio de prefijo

```
routing bgp network add network=2001:db8:2::/48 synchronize=no
```

Revisar la sesión BGP/Troubleshooting

Desde R2

Es importante que la letra “E” aparezca en la salida; la misma indica que la sesión BGP se encuentra establecida correctamente.



Cisco (IOS-15.4)

Habilitar IPv6

Antes de comenzar con la configuración de BGP, en algunas versiones de IOS, es necesario primero habilitar lo siguiente:

- **ipv6 unicast-routing**: Habilita el enrutamiento de paquetes IPv6.
- **ipv6 cef**: Habilita Cisco Express Forwarding para paquetes IPv6 de esta manera el procesamiento de dichos paquetes se realiza en Hardware, sino se realizaría en Software impactando directamente en la CPU del equipo.

```
R1#configure terminal        #entramos en modo configuración
R1(config)#
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 cef
```

R1

Entramos en Modo Configuración:

```
R1#configure terminal
R1(config)#
```

Configuramos la interface Loopback0:

```
R1(config)#interface loopback 0 #configuración de la interfaz loopback
R1(config-if)#ipv6 address 2001:db8:1::1/128 #dirección ipv6 de la interfaz loopback
R1(config-if)#exit
R1(config)#
```

Configuramos BGP:

```
R1(config)# router bgp 65001        #creamos el proceso de BGP con el ASN
R1(config-router)# bgp router-id 10.111.111.1      #definimos el router-id
```

```
R1(config-router)# no bgp default ipv4-unicast     #desactivar la configuración default de un
neighbor en el AF IPv4
R1(config-router)#neighbor 2001:DB8:12::2 remote-as 65002 #definimos el neighbor
R1(config-router)# address-family ipv6      #entramos en el AF de IPv6
R1(config-router-af)#  neighbor 2001:DB8:12::2 activate   #activamos el neighbor en este AF
R1(config-router-af)#  network 2001:DB8:1::/48     #prefijo a ser anunciado
R1(config-router-af)#exit
R1(config-router)#exit
R1(config)#ipv6 route 2001:db8:1::/48 Null0 #Cisco necesita que el prefijo a ser anunciado se
encuentre en la tabla de enrutamiento

R1(config)#exit
R1#
```

R2

Entramos en Modo Configuración:

```
R2#configure terminal
R2(config)#
```

Configuramos la interfaz Loopback0:

```
R2(config)#interface loopback 0
R2(config-if)#ipv6 address 2001:db8:2::1/128
R2(config-if)#exit
R2(config)#
```

Configuramos BGP:

```
R2(config)#router bgp 65002
R2(config-router)# bgp router-id 10.222.222.2
R2(config-router)# no bgp default ipv4-unicast
R2(config-router)# neighbor 2001:DB8:12::1 remote-as 65001
R2(config-router)# address-family ipv6
R2(config-router-af)#  neighbor 2001:DB8:12::1 activate
R2(config-router-af)#  network 2001:DB8:2::/48
R2(config-router-af)#exit-address-family
R2(config-router)#exit
R2(config)#ipv6 route 2001:db8:2::/48 Null0 #Cisco necesita que el prefijo a ser anunciado se
encuentre en la tabla de enrutamiento

R2(config)#exit
R2#
```

Revisar la sesión BGP/Troubleshooting

show bgp ipv6 unicast summary

Con este comando podemos revisar los peers existentes. Un indicador de que la sesión BGP se encuentra levantada es revisar la columna “State/PfxRcd” y chequear que contenga un número. Dicho número indica la cantidad de prefijos recibidos. En nuestro caso esperamos recibir 1 prefijo (la IPv6 de la interfaz loopback del neighbor):

```
R1#show bgp ipv6 unicast summary
BGP router identifier 10.111.111.1, local AS number 65001
BGP table version is 3, main routing table version 3
2 network entries using 328 bytes of memory
2 path entries using 208 bytes of memory
2/2 BGP path/bestpath attribute entries using 288 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 848 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:DB8:12::2  4        65002      14      13        3    0    0 00:08:39        1
R1#
```

show bgp ipv6 unicast

Con este comando se puede observar la tabla BGP IPv6 del equipo e identificar detalladamente los prefijos aprendidos.

```
R1#show bgp ipv6 unicast
BGP table version is 3, local router ID is 10.111.111.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  2001:DB8:1::/48  ::                       0         32768 i         #prefijo IPv648 local
 *>  2001:DB8:1::/48  2001:DB8:12::2           0         0 65002 i       #prefijo IPv6 remoto
R1#
```

Verificar conectividad end-to-end

Luego de que estamos seguros de que ambos routers aprenden correctamente el prefijo del vecino, podemos verificar la conectividad IPv6 entre las IPs de las Interfaces Loopback en ambos extremos:

Ping desde R1:

```
R1#ping ipv6 2001:db8:2::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:2::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/5 ms
R1#
```

Chequeo de Conectividad PING6 de R1 a R2, a nivel de las IPv6 de Loopback

Un aspecto interesante de Mikrotik es que para hacer PING (IPv4) y PING6 (IPv6) se utiliza el mismo comando y Mikrotik identifica la IP destino y procede a realizar el PING ó PING6 de acuerdo al protocolo correspondiente. En otros routers, esto no ocurre y hay que explicitar que el PING es IPv6 usando comandos distintos como ‘ping6’ (Cisco Nexus) ó ‘ping ipv6’.

```
[admin@R1] > /ping 2001:db8:2:11::cafe src-address=2001:db8:1:11::cafe count=4
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 2001:db8:2:11::cafe                        56 123 0ms   echo reply
    1 2001:db8:2:11::cafe                        56 123 0ms   echo reply
    2 2001:db8:2:11::cafe                        56 123 0ms   echo reply
    3 2001:db8:2:11::cafe                        56 123 0ms   echo reply
    sent=4 received=4 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

Ejemplo Filtros Básicos en BGP

En esta sección mostraremos un ejemplo básico de como realizar filtros salientes y entrantes en BGP.

Se configuran los siguientes filtros para que solo se propaguen los direccionamientos de las Interfaces Loopback0 de ambos routers:

- Filtro saliente en R1 permitiendo anunciar solo su Loopback0 a R2.
- Filtro entrante en R2 permitiendo recibir solo la Loopback0 de R1.
- Filtro saliente en R2 permitiendo anunciar solo su Loopback0 a R1.
- Filtro entrante en R1 permitiendo recibir solo la Loopback0 de R2.

Conceptos previos a la configuración:

- Prefix-List:
  - Las Listas de Prefijos se utilizan para definir los prefijos a utilizar en el filtro.
  - En nuestro caso utilizaremos:
    - PREFIXES-AS6500X: Para identificar los prefijos del ASN.
    - ALL-v6: Todos los prefijos IPv6, para poner al final y filtrar todo el resto.
- Route-map:
  - Es una secuencia ordenada de sentencias de permiso o rechazo.
  - En este caso se utiliza para permitir o rechazar el anuncio de prefijos en BGP.

Filtrado Básico BGP Mikrotik

Ejemplo en Mikrotik

En Mikrotik existen varias formas de programar los filtros a ser utilizados en las sesiones eBGP. Existen desde aquellas muy sencillas y básicas, pasando por las de detalles y complejidad intermedia hasta las más avanzadas que incluyen filtrado basado en manejo y configuración de atributos avanzados como MED, NEXT_HOP, AS_PATH, LOCAL_PREF, entre otros tantos. En este caso, a objeto de ilustrar de primera mano el concepto, haremos uso de una configuración básica y sencilla del filtrado BGP, y haremos uso solamente de los parámetros PREFIX y PREFIX_LEN para la definición de los filtros.

Al igual que en toda configuración de filtrado de sesiones BGP, debemos configurar un filtro BGP de entrada (IN) y un filtro BGP de salida (OUT) en cada par BGP. Esto es, para R1 debemos configurar un filtro para IN y otro para OUT, y para R2 debemos definir un filtro para IN y otro para OUT. Dicho esto, definiremos los siguientes parámetros de configuración para cada router de la sesión eBGP:

Router R1:

- **Nombre del Filtro IN:** ebgp-r2-ipv6-IN
- **Nombre del Filtro OUT:** ebgp-r2-ipv6-OUT

- · **Prefijo IPv6 a Anunciar:** 2001:db8:1::/48

Router R2:

- · **Nombre del Filtro IN:** ebgp-r1-ipv6-IN
- · **Nombre del Filtro OUT:** ebgp-r1-ipv6-OUT
- · **Prefijo IPv6 a Anunciar:** 2001:db8:2::/48

La configuración de los filtros en Mikrotik se realiza en la sección de configuración **'/routing filter'**. Las configuraciones, para Mikrotik RouterOS v6, serían las siguientes:

Para Router R1:

```
[admin@RouterOS-v6-R1] > /routing filter

[admin@RouterOS-v6-R1] /routing filter > add chain=ebgp-r2-ipv6-IN
           prefix=2001:db8:2::/48 prefix-length=48-48 action=accept

[admin@RouterOS-v6-R1] /routing filter > add chain= ebgp-r2-ipv6-IN
           prefix=::/0 prefix-length=0-128 action=discard

[admin@RouterOS-v6-R1] /routing filter > print where
           Chain=ebgp-r2-ipv6-IN

Flags: X - disabled

 0     chain=ebgp-r2-ipv6-IN prefix=2001:db8:2::/48 prefix-length=48 invert-
match=no action=accept set-bgp-prepend-path=""

 1     chain=ebgp-r2-ipv6-IN prefix=::/0 prefix-length=0-128 invert-match=no
action=discard set-bgp-prepend-path=""

 [admin@RouterOS-v6-R1] > /routing filter

[admin@RouterOS-v6-R1] /routing filter > add chain=ebgp-r2-ipv6-OUT
prefix=2001:db8:1::/48 prefix-length=48-48 action=accept

[admin@RouterOS-v6-R1] /routing filter > add chain=ebgp-r2-ipv6-OUT
prefix=::/0 prefix-length=0-128 action=discard

[admin@RouterOS-v6-R1] /routing filter > print where chain=ebgp-r2-ipv6-OUT

Flags: X - disabled
```

```
 0    chain=ebgp-r2-ipv6-OUT prefix=2001:db8:1::/48 prefix-length=48 invert-
match=no action=accept set-bgp-prepend-path=""

 1    chain=ebgp-r2-ipv6-OUT prefix=::/0 prefix-length=0-128 invert-match=no
action=discard set-bgp-prepend-path=""
```

Para Router R2:

```
[admin@RouterOS-v6-R2] > /routing filter

[admin@RouterOS-v6-R2] /routing filter > add chain=ebgp-r1-ipv6-IN
            prefix=2001:db8:1::/48 prefix-length=48-48 action=accept

[admin@RouterOS-v6-R2] /routing filter > add chain= ebgp-r1-ipv6-IN
            prefix=::/0 prefix-length=0-128 action=discard

[admin@RouterOS-v6-R2] /routing filter > print where Chain=ebgp-r1-ipv6-IN

Flags: X - disabled

 0   chain=ebgp-r1-ipv6-IN prefix=2001:db8:1::/48 prefix-length=48 invert-
match=no action=accept set-bgp-prepend-path=""

 1   chain=ebgp-r1-ipv6-IN prefix=::/0 prefix-length=0-128 invert-match=no
action=discard set-bgp-prepend-path=""

 [admin@RouterOS-v6-R2] > /routing filter

[admin@RouterOS-v6-R2] /routing filter > add chain=ebgp-r1-ipv6-OUT
prefix=2001:db8:1::/48 prefix-length=48-48 action=accept

[admin@RouterOS-v6-R2] /routing filter > add chain=ebgp-r1-ipv6-OUT
prefix=::/0 prefix-length=0-128 action=discard

[admin@RouterOS-v6-R2] /routing filter > print where chain=ebgp-r1-ipv6-OUT

Flags: X - disabled

 0   chain=ebgp-r1-ipv6-OUT prefix=2001:db8:2::/48 prefix-length=48 invert-
match=no action=accept set-bgp-prepend-path=""

 1   chain=ebgp-r1-ipv6-OUT prefix=::/0 prefix-length=0-128 invert-match=no
action=discard set-bgp-prepend-path=""
```

Luego de crear los filtros de IN y OUT (tanto para R1 como para R2), debemos asignarlos a las sesiones eBGP correspondientes. A continuación los comandos para esta configuración:

Para Router R1:

```
[admin@RouterOS-v6-R1] > /routing bgp peer

[admin@RouterOS-v6-R1] /routing bgp peer> set [find name=HACIAR2]
            in-filter=ebgp-r2-ipv6-IN

[admin@RouterOS-v6-R1] /routing bgp peer> set [find name=HACIAR2]
            out-filter=ebgp-r2-ipv6-OUT

[admin@RouterOS-v6-R1] /routing bgp peer> print detail
```

Para Router R2:

```
[admin@RouterOS-v6-R2] > /routing bgp peer

[admin@RouterOS-v6-R2] /routing bgp peer> set [find name=HACIAR1]
            in-filter=ebgp-r1-ipv6-IN

[admin@RouterOS-v6-R2] /routing bgp peer> set [find name=HACIAR1]
            out-filter=ebgp-r1-ipv6-OUT

[admin@RouterOS-v6-R2] /routing bgp peer> print detail
```

Importante: Un detalle de configuración importante es lo relativo a la configuración del prefijo IPv6 a anunciar. La forma más comúnmente utilizada es configurar dicho prefijo IPv6 en la sección **'/routing bgp network'** con el atributo **'synchronize=no'**. De esta forma, Mikrotik (versión 6) anunciará el prefijo IPv6 de manera **'incondicional'** (atención: pasado por los correspondientes filtros de OUT) . Como forma alternativa, podemos colocar el prefijo IPv6 en los BGP networks de Mikrotik y colocando el atributo **'synchronize=yes'**, pero en este caso el prefijo será anunciado si y sólo si se encuentra activo en la tabla de rutas IPv6 de Mikrotik. Por último, también se pueden hacer uso de técnicas de 'redistribute' para anunciar prefijos IPv6. Además, es importante comentar que podemos anunciar vía eBGP cualquier prefijo con longitud entre /32 y /48 (ambos inclusive), tomado de nuestro prefijo base asignado por LACNIC.

*****************************Aquí termina Filtrado eBGP Mikrotik**
*****************************Aquí termina Filtrado eBGP Mikrotik**

Ejemplo en Cisco

R1:

```
ipv6 prefix-list ALL-v6 seq 5 permit ::/0 le 128
!
ipv6 prefix-list PREFIXES-AS65001 seq 5 permit 2001:DB8:1::/48
!
ipv6 prefix-list PREFIXES-AS65002 seq 5 permit 2001:DB8:2::/48
!
route-map RM-R1-R2-IN permit 10     #permite recibir los prefijos del AS65002
 match ipv6 address prefix-list PREFIXES-AS65002
!
route-map RM-R1-R2-IN deny 20       #no permite recibir ningún otro prefijo
 match ipv6 address prefix-list ALL-v6
!
route-map RM-R1-R2-OUT permit 10    #permite anunciar los prefijos del AS65001
 match ipv6 address prefix-list PREFIXES-AS65001
!
route-map RM-R1-R2-OUT deny 20      #no permite anunciar ningún otro prefijo
 match ipv6 address prefix-list ALL-v6
!
router bgp 65001
 address-family ipv6
  neighbor 2001:DB8:12::2 route-map RM-R1-R2-IN in #asocia el route-map al neighbor
  neighbor 2001:DB8:12::2 route-map RM-R1-R2-OUT out #asocia el route-map al neighbor
 exit-address-family
!
```

R2:

```
ipv6 prefix-list ALL-v6 seq 5 permit ::/0 le 128
!
ipv6 prefix-list PREFIXES-AS65001 seq 5 permit 2001:DB8:1::/48
!
ipv6 prefix-list PREFIXES-AS65002 seq 5 permit 2001:DB8:2::/48
!
route-map RM-R2-R1-IN permit 10
 match ipv6 address prefix-list PREFIXES-AS65001
!
route-map RM-R2-R1-IN deny 20
!
route-map RM-R2-R1-OUT permit 10
 match ipv6 address prefix-list PREFIXES-AS65002
!
route-map RM-R2-R1-OUT deny 20
 match ipv6 address prefix-list ALL-v6
!
router bgp 65002
 address-family ipv6
```

```
  neighbor 2001:DB8:12::1 route-map RM-R2-R1-IN in
  neighbor 2001:DB8:12::1 route-map RM-R2-R1-OUT out
 exit-address-family
!
```

Verificación

R1:

```
R1#show bgp ipv6 unicast
BGP table version is 9, local router ID is 10.111.111.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  2001:DB8:1::/48  ::                       0         32768 i
 *>  2001:DB8:2::/48  2001:DB8:12::2           0             0 65002 i
R1#
```

R2:

```
R2#show bgp ipv6 unicast
BGP table version is 9, local router ID is 10.222.222.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  2001:DB8:1::/48  2001:DB8:12::1           0             0 65001 i
 *>  2001:DB8:2::/48  ::                       0         32768 i
R2#
```

Errores comunes

A pesar de que pueden existir muchos errores en el mundo de sesiones BGP quisimos enumerar dos casos muy típicos:

1) La sesión BGP no levanta
   Pueden existir muchas razones por la cual una sesión BGP no levante entre dos peers. Las más probables son:
   a) No hay conectividad IP entre ellos
   b) Existe discrepancia de información entre los peers (por ejemplo, dirección IP, sistema autónomo incorrectos)

2) Mi prefijo no se encuentra anunciado
   Nuevamente pueden haber muchas razones por las cualesl no se encuentra anunciado un prefijo; las tres razones más comunes son:
   a) Existe algún filtro implementado saliente en la sesión BGP que prohíbe el anuncio del prefijo
   b) El prefijo que deseas anunciar no se encuentra en la tabla de enrutamiento
   c) Modernas implementaciones de BGP exigen implementaciones de políticas en la sesión BGP antes de realizar los anuncios de los prefijos

Conclusiones

Levantar una sesión BGP (léase crear un peering BGP) es algo muy sencillo, tan solo hay que conocer los parámetros adecuados y saber colocarlos en la configuración según el dispositivo.
La parte complicada de BGP aparece al momento de tener varios peers, necesitar filtros de entrada y/o salida en las sesiones BGP y ,sobre todo, cuando un sistema autónomo hace tránsito de tráfico y prefijos de otros ASs. La recomendación general es estudiar mucho y ser excesivamente cauteloso al momento de realizar cualquier configuración.

Todo

Siempre es importante estar muy pendiente de la seguridad, anuncios, filtros y operación de BGP. Se sugiere revisar el siguiente BCP BGP (Operations and Security):

- https://datatracker.ietf.org/doc/html/rfc7454

A su vez en LACNIC tenemos gran cantidad de videos sobre BGP:
https://www.youtube.com/c/lacnicstaff/search?query=bgp

Y tenemos un curso en nuestro CAMPUS donde cubrimos bastante esta temática:
https://campus.lacnic.net/mod/page/view.php?id=10647

Seleccionar el Router-ID de cada router “sabiamente”

Referencias

https://blog.cdemi.io/beginners-guide-to-understanding-bgp/
https://datatracker.ietf.org/doc/html/rfc7454
[2] https://networklessons.com/bgp/ebgp-multihop
[3] https://www.networkurge.com/2017/06/bgp-next-hop-attribute-and-rules.html
[4] https://blog.acostasite.com/2021/01/roles-en-bgp-reduciendo-fugas-de.html