Como levantar um peering em só IPv6?

Autor: Alejandro Acosta, José G. Cotúa, Alejandro D'Egidio
Coordenação e revisão: Guillermo Cicileo
Edição: Carolina Badano, Martín Mañana
Área: Tecnología

lacnic
www.lacnic.net

Introdução

O artigo a seguir apresenta de forma ordenada as etapas a serem seguidas para levantar um peering BGP entre dois roteadores só IPv6.

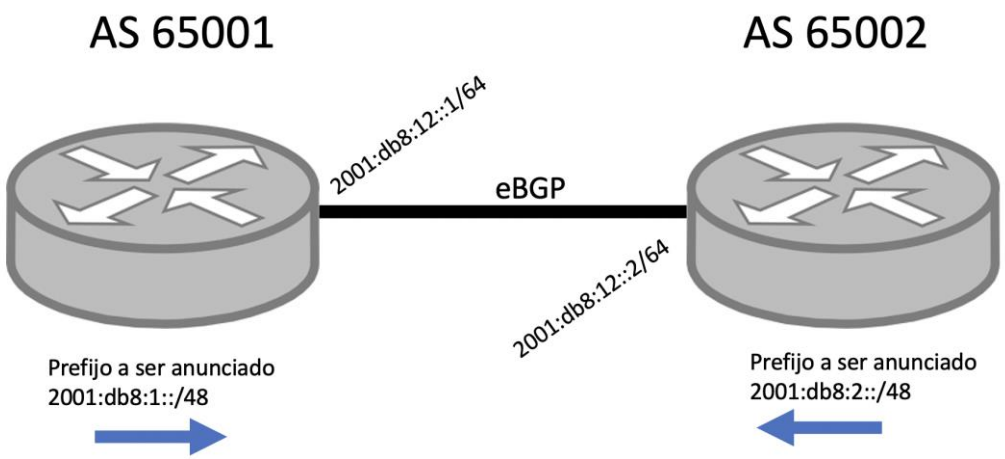
Na linguagem de BGP *peering* é conhecido como (traduzido de [1]):

"Dois roteadores que estabeleceram uma conexão para trocar informações BGP são chamados de peers BGP. Esses peers BGP trocam informações de roteamento entre si por meio de sessões BGP..."

Pré-requisitos

- Dois roteadores
- Conectividade entre os roteadores
- Suporte IPv6 em ambos os dispositivos tanto em conectividade quanto em BGP

Topologia



Para roteador R1:

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

Para roteador R2:

- IPv6 R2: 2001:db8:12::2/64
- Router-ID de R2: 10.222.222.2
- Prefixo v6 que será anunciado por R2: 2001:db8:2::/48
- IPv6 /128 de Loopback: 2001:db8:02:11::cafe/128

Passos a seguir

Passo 1 - Conectividade IPv6 entre os roteadores

Para estabelecer e testar a conectividade entre os roteadores, devemos:

1. Estabelecer a conexão física:
    - Certificar-se de que a conexão física entre as interfaces designadas de ambos os roteadores seja feita.
    - Verificar que esse link esteja UP.
2. Configurar o IPv6 nas interfaces relacionadas:
    - Designar o endereçamento IPv6 de WAN que será usado no link. Todo o endereçamento usado neste documento pertence ao segmento 2001:db8::/32 reservado para documentação.
    - Configurar o IPv6 nas interfaces relacionadas.
3. Testar conectividade IPv6:
    - Fazer um Ping IPv6 desde algum dos dois equipamentos.
    - Se não puder ser alcançado, é imprescindível corrigir essa situação antes de continuar.
    - É possível que o destino esteja filtrando os pacotes de Ping IPv6 (ICMPv6 Echo Request/Reply) e isso não significa que o BGP não vai funcionar; verificar no outro equipamento.

Nota: O BGP por padrão pensa que seu vizinho está conectado diretamente, quer dizer, o vizinho é o próximo dispositivo na rede. Se este não for o caso, configuração adicional pode ser necessária, como eBGP Multihop [2], mas este assunto não será abordado neste tutorial.

Cisco (IOS-15.4)

R1

Estado de Interface:

```
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)
```

Configuração de Interface:

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

R2

Estado de Interface:

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)

Configuração de Interface:

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

Teste de conectividade:

```
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
```

Criar a sessão BGP entre endereços Link Local (LLA) ou Global Unicast Addresses (GUA)?

As vezes teremos que tomar a decisão de como criar a sessão BGP; existem 3 possibilidades:

- Usar endereços Link Local (LLA),
- Usar endereços globais (GUA),
- Usar endereços ULA (Unique Local Address).

As duas primeiras opções são as mais usadas.

Então, o que eu uso para criar a sessão BGP?

Nós lhe daremos uma resposta direta, porém queremos fazer a explicação como deve ser. Revise estas premissas:

1. Lembremos que as mensagens BGP contêm atributos, sendo um deles o atributo NextHop [3]. Este atributo contém informações muito simples: o salto a ser usado para chegar a um destino.
2. Um roteador (um eBGP Speaker) ao aprender um prefixo de outro AS copia o atributo de NextHop para sua rede iBGP.
3. Uma rede de speakers iBGP tradicionalmente vai ter um IGP.
4. Os endereços Link Local têm escopo local, apenas o próprio barramento da rede, a LAN, o SSID, etc. Eles **não** podem ser roteados.

Talvez, agora, você já tenha respondido o que usar :-)
Nossa recomendação é criar a sessão BGP sobre GUA, e agora que revisamos as premissas fica fácil responder com uma pergunta: Como um eBGP speaker vai copiar um endereço Link Local no próximo salto para seus iBGP speaker? Simples, pode **não** (claro, existem alguns truques, mas não vamos chegar lá).

Passo 2 - Definir o Router-ID nos diferentes roteadores

Uma vez que estamos falando de equipamentos só IPv6, assumimos que os dispositivos não vão ter endereçamento IPv4. O que é que isso tem a ver?
Explicamos brevemente:

- Para que um router-id? O router-id é um campo de 32 bits que trafega na mensagem OPEN do BGP, este campo (chamado BGP Identifier) é obrigatório e é representado em um formato de endereço IPv4.
- Os roteadores têm um mecanismo para obter seus router-id.
- Se o roteador for só IPv6, o equipamento não poderá descobrir o seu router-id.
- Se o roteador não conseguir descobrir seu router-id, o administrador deverá configurar um explicitamente dentro do processo BGP.

Passo 3 - Fazer as configurações nos roteadores

Vamos mostrar dois exemplos: Mikrotik e Cisco. Podemos perceber que as informações são exatamente as mesmas, o que muda é a forma e os comandos do sistema operacional. No caso de Mikrotik usaremos a versão 6.x.

Configuração em roteadores

Mikrotik (RouterOS v6)

Roteador R1

Configuração da interface 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
```

Configuração do processo/instância BGP

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

Configuração do Peer

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

Anúncio de prefixo

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

Roteador R2

Configuração da interface loopback

```
/interface bridge add name=loopback protocol-mode=none disabled=no
/ipv6 address add address=2001:db8:02:11::cafe/128 advertise=no interface=loopback
```

Configuração do processo/instância BGP

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

Configuração do Peer

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

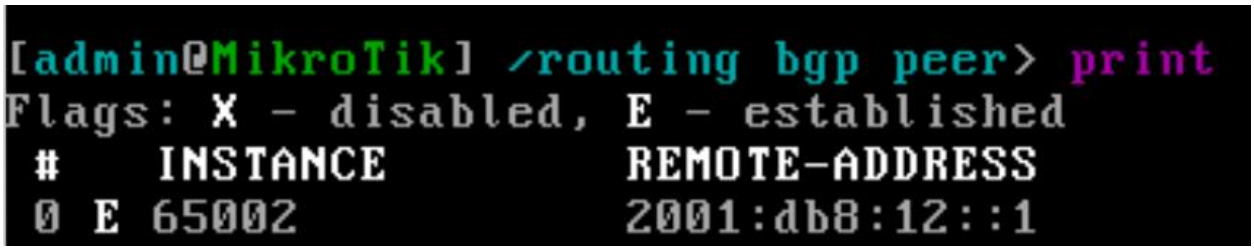
Anúncio de prefixo

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

Revisar a sessão BGP/Troubleshooting

Desde R2

É importante que a letra "E" apareça na saída, esta indica que a sessão BGP está estabelecida corretamente



Cisco (IOS-15.4)

Habilitar o IPv6

Antes de iniciar a configuração do BGP, em algumas versões do IOS, é necessário primeiro habilitar:

- **ipv6 unicast-routing**: Habilita o roteamento de pacotes IPv6.
- **ipv6 cef**: Habilita o Cisco Express Forwarding para pacotes IPv6; desta forma o processamento dos referidos pacotes é feito em Hardware, caso contrário seria feito em Software impactando diretamente na CPU do equipamento.

```
R1#configure terminal        #entramos em modo configuração
R1(config)#
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 cef
```

R1

Entramos no modo Configuração:

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

Configuramos a interface Loopback0:

```
R1(config)#interface loopback 0 #configuração da interface loopback
R1(config-if)#ipv6 address 2001:db8:1::1/128 #endereço ipv6 da interface loopback
R1(config-if)#exit
R1(config)#
```

Configuramos BGP:

```
R1(config)# router bgp 65001        #criamos o processo de BGP com o ASN
R1(config-router)# bgp router-id 10.111.111.1      #definimos o router-id
R1(config-router)# no bgp default ipv4-unicast     #desativar a configuração default de um
neighbor no AF IPv4
R1(config-router)#neighbor 2001:DB8:12::2 remote-as 65002 #definimos o neighbor
```

```
R1(config-router)# address-family ipv6      #entramos no AF do IPv6
R1(config-router-af)#  neighbor 2001:DB8:12::2 activate   #ativamos o neighbor neste AF
R1(config-router-af)#  network 2001:DB8:1::/48     #prefixo a ser anunciado
R1(config-router-af)#exit
R1(config-router)#exit
R1(config)#ipv6 route 2001:db8:1::/48 Null0 #A Cisco precisa que o prefixo a ser anunciado
esteja na tabela de roteamento.

R1(config)#exit
R1#
```

R2

Entramos no modo Configuração:

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

Configuramos a interface 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 #A Cisco precisa que o prefixo a ser anunciado
esteja na tabela de roteamento.

R2(config)#exit
R2#
```

Revisar a sessão BGP/Troubleshooting

show bgp ipv6 unicast summary

Com este comando podemos verificar os peers existentes. Um indicador de que a sessão BGP está ativa é conferir a coluna “State/PfxRcd” e verificar que ela contenha um número. Esse número indica o número de prefixos recebidos. No nosso caso, esperamos receber 1 prefixo (o IPv6 da interface loopback do 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

Com esse comando você pode ver a tabela BGP IPv6 do dispositivo e identificar em detalhe os prefixos 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         #prefixo IPv648 local
 *>  2001:DB8:1::/48  2001:DB8:12::2           0         0 65002 i       #prefixo IPv6 remoto
R1#
```

Verificar conectividade end-to-end

Depois de termos certeza de que ambos os roteadores aprenderam corretamente o prefixo do vizinho, podemos verificar a conectividade IPv6 entre os IP das Interfaces Loopback nos dois 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#
```

Verificação de conectividade PING6 de R1 a R2, no nível dos IPv6 de Loopback

Um aspecto interessante do Mikrotik é que para fazer PING (IPv4) e PING6 (IPv6) é usado o mesmo comando, e o Mikrotik identifica o IP de destino e procede à execução do PING ou PING6 de acordo com o protocolo correspondente. Em outros roteadores isso não acontece, pelo que é necessário explicitar que o PING é IPv6 usando comandos diferentes como 'ping6' (Cisco Nexus) ou '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
```

Exemplo: filtros básicos no BGP

Nesta seção vamos mostrar um exemplo básico de como fazer filtros de saída e de entrada no BGP.

Os filtros a seguir são configurados para que apenas os endereços das Interfaces Loopback0 de ambos os roteadores sejam propagados:

- Filtro de saída no R1 permitindo anunciar apenas sua Loopback0 a R2.
- Filtro de entrada no R2 permitindo receber apenas a Loopback0 de R1.
- Filtro de saída no R2 permitindo anunciar apenas sua Loopback0 a R1.
- Filtro de entrada no R1 permitindo receber apenas a Loopback0 de R2.

Conceitos prévios à configuração:

- Prefix-List:
    - As listas de prefixos são usadas para definir os prefixos a serem usados no filtro.
    - No nosso caso vamos usar:
        - PREFIXES-AS6500X: para identificar os prefixos do ASN.
        - ALL-v6: todos os prefixos IPv6. Para colocar no final e filtrar todo o resto.
- Route-map:
    - É uma sequência ordenada de instruções de permissão ou rejeição.
    - Neste caso é usada para permitir ou rejeitar o anúncio de prefixos no BGP.

Filtragem básica BGP Mikrotik

Exemplo no Mikrotik

No Mikrotik existem várias formas de programar os filtros a serem usados nas sessões de eBGP. Estas vão desde as muito simples e básicas, passando pelas de detalhes e complexidade intermediária até as mais avançadas que incluem filtragem baseada no gerenciamento e configuração de atributos avançados como MED, NEXT_HOP, AS_PATH, LOCAL_PREF, entre outros. Neste caso, para ilustrar o conceito em primeira mão, usaremos uma configuração básica e simples da filtragem BGP, e usaremos apenas os parâmetros PREFIX e PREFIX_LEN para definir os filtros.

Como em qualquer configuração de filtragem de sessões BGP, devemos configurar um filtro BGP de entrada (IN) e um filtro BGP de saída (OUT) em cada peer BGP. Ou seja, para R1 devemos configurar um filtro para IN e outro para OUT, e para R2 devemos definir um filtro para IN e outro para OUT. Dito isso, definiremos os seguintes parâmetros de configuração para cada roteador da sessão eBGP:

Roteador R1:

- **Nome do Filtro IN:** ebgp-r2-ipv6-IN
- **Nome do Filtro OUT:** ebgp-r2-ipv6-OUT
- **Prefixo IPv6 a ser anunciado:** 2001:db8:1::/48

Roteador R2:

- **Nome do Filtro IN:** ebgp-r1-ipv6-IN
- **Nome do Filtro OUT:** ebgp-r1-ipv6-OUT
- **Prefixo IPv6 a ser anunciado:** 2001:db8:2::/48

A configuração dos filtros no Mikrotik é feita na seção de configuração **'/routing filter'**. As configurações para Mikrotik RouterOS v6 seriam as seguintes:

Para Roteador 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 Roteador 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=""
```

Depois de criar os filtros IN e OUT tanto para R1 quanto para R2, devemos designar esses filtros às sessões eBGP correspondentes. A seguir, os comandos para essa configuração:

Para Roteador 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 Roteador 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: Um detalhe importante da configuração está relacionado à configuração do prefixo IPv6 a ser anunciado. A maneira mais usada é configurar o referido prefixo IPv6 na seção **'/routing bgp network'** com o atributo **'synchronize=no'**. Assim, o Mikrotik (versão 6) anunciará o prefixo IPv6 de maneira **'incondicional'** (nota: passado pelos filtros OUT correspondentes). Como alternativa, podemos colocar o prefixo IPv6 nos BGP networks do Mikrotik e colocar o atributo **'synchronize=yes'**, mas neste caso o prefixo será anunciado se e somente se estiver ativo na tabela de roteamento IPv6 do Mikrotik. Finalmente, técnicas de 'redistribute' também podem ser usadas para anunciar prefixos IPv6. Além disso, é importante mencionar que podemos anunciar via eBGP qualquer prefixo com comprimento entre /32 e /48 (ambos inclusive), tirado do nosso prefixo base designado pelo LACNIC.

******************************Aqui termina filtragem eBGP Mikrotik**
******************************Aqui termina filtragem eBGP Mikrotik**

Exemplo em 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 receber os prefixos do AS65002
 match ipv6 address prefix-list PREFIXES-AS65002
!
route-map RM-R1-R2-IN deny 20       #não permite receber nenhum outro prefixo
 match ipv6 address prefix-list ALL-v6
!
route-map RM-R1-R2-OUT permit 10    #permite anunciar os prefixos do AS65001
 match ipv6 address prefix-list PREFIXES-AS65001
!
route-map RM-R1-R2-OUT deny 20      #não permite anunciar nenhum outro prefixo
 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 #associa o route-map ao neighbor
  neighbor 2001:DB8:12::2 route-map RM-R1-R2-OUT out #associa o route-map ao 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
!
```

Verificação

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#
```

Erros comuns

Embora possa haver muitos erros no mundo das sessões BGP, quisemos listar dois casos muito típicos:

1) Sessão BGP não aparece
   Pode haver muitos motivos pelos quais uma sessão BGP não aparece entre dois peers. As mais prováveis são:
   a) Não há conectividade IP entre eles
   b) Há uma discrepância de informações entre os peers (por exemplo, endereço IP, sistema autônomo errados)

2) Meu prefixo não se encontra anunciado
   Novamente, pode haver muitos motivos pelos quais um prefixo não é anunciado, os três mais comuns são:
   a) Existe algum filtro implementado de saída na sessão BGP que proíbe o anúncio do prefixo
   b) O prefixo que você quer anunciar não está na tabela de roteamento
   c) As implementações modernas do BGP exigem implementações de políticas na sessão BGP antes que os anúncios dos prefixos sejam feitos

Conclusões

Configurar uma sessão BGP (leia-se criar um peering BGP) é muito simples, basta conhecer os parâmetros apropriados e saber como colocá-los na configuração de acordo com o dispositivo.

A parte complicada do BGP surge na hora de ter vários peers, precisar de filtros de entrada e/ou saída nas sessões BGP, e principalmente quando um sistema autônomo fizer trânsito de tráfego e prefixos de outros AS. A recomendação geral é estudar muito e ser excessivamente cauteloso ao fazer qualquer configuração.

TUDO

É sempre importante estar muito atento à segurança, anúncios, filtros e funcionamento do BGP. Sugere-se revisar o seguinte BCP BGP (Operations and Security):
https://datatracker.ietf.org/doc/html/rfc7454

Por sua vez, no LACNIC temos um grande número de vídeos sobre o BGP:
https://www.youtube.com/c/lacnicstaff/search?query=bgp

E temos um curso no nosso CAMPUS em que abordamos bastante desse tema:
https://campus.lacnic.net/mod/page/view.php?id=10647

Selecionar o Router-ID de cada roteador “sabiamente”

Referências

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