

Exercício 4a – eBGP

Objetivo: configurar a sessão eBGP entre o mikrotik-borda e o provedor de trânsito Operadora-02. Após essa configuração o ISP terá acesso a toda a estrutura montada no laboratório e aos outros grupos. O provedor de trânsito irá lhe enviar tabela BGP completa e também a rota default.

Cenário: Os endereços das interfaces físicas, o protocolo de roteamento interno e o iBGP já estão configurados.

1. Primeiro, crie uma interface de *loopback* no roteador mikrotik_borda que será utilizada para estabelecer a sessão eBGP.

No roteador mikrotik_borda utilize os seguintes comandos:

```
> interface bridge add name=lo10 auto-mac=no admin-mac=1A:B0:06:01:XX:10
> ip address add address=102.XX.0.253/32 interface=lo10 comment=EBGP
> ipv6 address add address=4D0C:XX::253/128 interface=lo10 comment=EBGP
```

2. Assim como foi feito no item 2 do exercício 2 (iBGP), adicione a interface lo10 à área zero do OSPFv2 e OSPFv3. Em seguida, a partir dos outros roteadores, teste a conectividade IPv4 e IPv6 com a *loopback* criada.
3. Também é preciso adicionar endereços IPv4 e IPv6 a interface ether1 do roteador mikrotik_borda. Essa interface é a que está diretamente conectada ao provedor de trânsito e os endereços utilizados serão fornecidos pelo provedor.

Para adicionar os endereços a interface, utilize os seguintes comandos no roteador mikrotik_borda:

```
> ip address add address=102.120.XX.1/30 interface=ether1
> ipv6 address add address=4D0C:120:0:XX::1/126 advertise=no interface=ether1
```

Por serem de uma interface externa, esse endereços NÃO DEVEM ser adicionados aos processos do OSPF.

4. Teste a conectividade com a Operadora-02 utilizando o seguinte comando no roteador mikrotik_borda:

```
> ping 102.120.XX.2
> ping 4D0C:120:0:XX::2
```

5. Como será utilizado o endereço de *loopback* para estabelecer a sessão eBGP, é preciso criar uma rota estática para alcançar a *loopback* do vizinho Operadora-02:

Para realizar essa tarefa, utilize os seguintes comandos no roteador mikrotik_borda:

```
> ip route add dst-address=102.120.255.255 gateway=102.120.XX.2
> ipv6 route add dst-address=4D0C:120:0:FFFF::255 gateway=4D0C:120:0:XX::2
```

6. Teste a conectividade com a *loopback* da Operadora-02. Caso tenha sido estabelecida, configure as sessões eBGP via IPv4 e IPv6.

Para realizar essa configuração, utilize os seguintes comandos no roteador mikrotik_borda:

```
> /routing bgp peer add address-families=ip name=EBGP-IPV4-OP02 update-
source=lo10 remote-address=102.120.255.255 remote-as=64520 multihop=yes
nexthop-choice=force-self
> /routing bgp peer add address-families=ipv6 name=EBGP-IPV6-OP02 update-
source=lo10 remote-address=4D0C:120:0:FFFF::255 remote-as=64520 multihop=yes
nexthop-choice=force-self
> /
```

7. Após o estabelecimento da sessão, verifique se rotas externas foram aprendidas pelo roteador mikrotik_borda e repassadas via iBGP aos demais roteadores do AS.

No roteador mikrotik_borda e no mikrotik_clientes execute os seguintes comandos:

```
> ip route print
> ipv6 route print
```

Todas as rotas foram aprendidas e aceitas pelo roteador mikrotik_clientes? Há alguma diferença entre as redes IPv4 e IPv6 aprendidas?

Verifique as rotas aprendidas pelo roteador cisco através dos seguintes comandos:

```
# show ip bgp
# show bgp ipv6
# show ip route
# show ipv6 route
```

No roteador juniper utilize os seguintes comandos para fazer essa verificação:

```
> show route protocol bgp
> show route
```

8. Verifique também o estado da sessão e quais prefixos estão sendo divulgados para seu provedor de trânsito.

Para isso, utilize os seguintes comandos no roteador mikrotik_borda:

```
> /routing bgp peer print detail status
> /routing bgp advertisements print peer=EBGP-IPV4-OP02
> /routing bgp advertisements print peer=EBGP-IPV6-OP02
```

O que está sendo divulgado? É preciso agregar os prefixos divulgados? Ou não há anúncios? Há alguma rede que não está sendo divulgada?

Exercício 4b – Criando Políticas de Roteamento

Para finalizar o estabelecimento da sessão BGP, configure as políticas de entrada e saída de seu AS. Não serão trabalhadas, por enquanto, questões sobre engenharia de tráfego, apenas políticas que garantam o envio dos blocos IPv6 e IPv4 agregados e políticas de entrada para filtrar o recebimento de anúncios indesejados.

1. Inicialmente, declare as redes agregadas que deverão ser anunciadas via eBGP e um filtro que permita apenas a divulgação desses prefixos.

Para realizar essa configuração, utilize os seguintes comandos no mikrotik_borda:

```
> /routing bgp network
  add disabled=no network=102.XX.0.0/19 synchronize=no
  add disabled=no network=4D0C:XX::/32 synchronize=no
> /routing filter
  add action=discard chain=BGP-OUT-IPV4 prefix=!102.XX.0.0/19
  add action=discard chain=BGP-OUT-IPV6 prefix=!4d0c:XX::/32
> /routing bgp peer set EBGP-IPV4-OP02 out-filter=BGP-OUT-IPV4
> /routing bgp peer set EBGP-IPV6-OP02 out-filter=BGP-OUT-IPV6
```

2. Verifique novamente o que está sendo anunciado à Operadora-02.

No roteador mikrotik_borda execute os seguintes comandos:

```
> /routing bgp advertisements print peer=EBGP-IPV4-OP02
> /routing bgp advertisements print peer=EBGP-IPV6-OP02
```

3. Um modo eficiente de verificar como os anúncios do AS estão sendo aprendidos por outras redes da Internet é através da utilização de um serviço chamado *looking glass*, em que alguns Sistemas Autônomos disponibilizam o acesso público a um servidor que atua como um espelho de seus roteadores de borda permitindo que se tenha a visualização da informações de suas tabelas de rotas.

Na topologia do laboratório, há um *looking glass* disponível no AS64510, da Operadora-01. Para acessá-lo, utilize os seguintes comandos a partir do servidor as_server:

```
# telnet 102.110.0.255 2605
Password: zebra
> show ip bgp 102.XX.0.0/19
> show ipv6 bgp 4d0c:XX::/32
> show ip bgp regexp 655XX$
> show ipv6 bgp regexp 655XX$
> exit
```

Por quantos caminhos diferentes o AS64510 sabe chegar a rede de seu AS? As rotas para a rede IPv4 são similares às da rede IPv6?

4. Após configurar as políticas de entrada IPv4 e IPv6 é preciso configurar políticas de entrada que protejam a rede do AS do recebimento de prefixos inválidos.

Para criar as regras IPv4 dessa política de entrada, execute os seguintes comandos no roteador mikrotik_borda:

```
> /routing filter
```

```

add action=discard chain=BGP-IN-IPV4 prefix=102.XX.0.0/19 prefix-length=19-32
add action=discard chain=BGP-IN-IPV4 prefix=0.0.0.0/8 prefix-length=8-32
add action=discard chain=BGP-IN-IPV4 prefix=10.0.0.0/8 prefix-length=8-32
add action=discard chain=BGP-IN-IPV4 prefix=100.64.0.0/10 prefix-length=10-32
add action=discard chain=BGP-IN-IPV4 prefix=127.0.0.0/8 prefix-length=8-32
add action=discard chain=BGP-IN-IPV4 prefix=169.254.0.0/16 prefix-length=16-32
add action=discard chain=BGP-IN-IPV4 prefix=172.16.0.0/12 prefix-length=12-32
add action=discard chain=BGP-IN-IPV4 prefix=192.0.0.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=192.0.2.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=192.168.0.0/16 prefix-length=16-32
add action=discard chain=BGP-IN-IPV4 prefix=198.18.0.0/15 prefix-length=15-32
add action=discard chain=BGP-IN-IPV4 prefix=198.51.100.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=203.0.113.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=224.0.0.0/4 prefix-length=4-32
add action=discard chain=BGP-IN-IPV4 prefix=0.0.0.0/0
> /

```

Crie também regras de proteção para a rede IPv6 utilizando os seguintes comandos:

```

> /routing filter
add action=discard chain=BGP-IN-IPV6 prefix=4d0c:XX::/32 prefix-length=32-128
add action=discard chain=BGP-IN-IPV6 prefix=2001:db8::/32 prefix-length=32-128
add action=accept chain=BGP-IN-IPV6 prefix=2001:500::/30 prefix-length=30-64
add action=accept chain=BGP-IN-IPV6 prefix=2001::/32 prefix-length=32-64
add action=accept chain=BGP-IN-IPV6 prefix=2001::/16 prefix-length=16-64
add action=accept chain=BGP-IN-IPV6 prefix=2001:c00::/23 prefix-length=23-64
add action=accept chain=BGP-IN-IPV6 prefix=2002::/16 prefix-length=16-64
add action=accept chain=BGP-IN-IPV6 prefix=2003::/16 prefix-length=16-64
add action=accept chain=BGP-IN-IPV6 prefix=2400::/12 prefix-length=12-64
add action=accept chain=BGP-IN-IPV6 prefix=2600::/12 prefix-length=12-64
add action=accept chain=BGP-IN-IPV6 prefix=2610::/23 prefix-length=23-64
add action=accept chain=BGP-IN-IPV6 prefix=2620::/23 prefix-length=23-64
add action=accept chain=BGP-IN-IPV6 prefix=2800::/12 prefix-length=12-64
add action=accept chain=BGP-IN-IPV6 prefix=2a00::/12 prefix-length=12-64
add action=accept chain=BGP-IN-IPV6 prefix=2801::/24 prefix-length=24-64
add action=accept chain=BGP-IN-IPV6 prefix=2c00::/12 prefix-length=12-64
add action=accept chain=BGP-IN-IPV6 prefix=4d0c::/16 prefix-length=16-64
add action=discard chain=BGP-IN-IPV6 prefix=::/0 prefix-length=0-128
> /

```

Por fim, aplique a política criada aos prefixos aprendidos através da Operadora-02. Para isso, execute os seguintes comando no roteador mikrotik_borda:

```

/routing bgp peer set EBG-IPV4-OP02 in-filter=BGP-IN-IPV4
/routing bgp peer set EBG-IPV6-OP02 in-filter=BGP-IN-IPV6

```