Exercício 6 – Engenharia de Tráfego

Objetivo: Configurar as sessões eBGP entre o roteador mikrotik_borda e os roteadores do PTT-01 e entre o roteador cisco e o roteador da Operadora-03. Essa segunda sessão simulará a contratação de um *link* através da estrutura do PTT-02. Serão abordadas boas práticas no estabelecimento de sessões eBGP e de participação em um PTT.

Cenário inicial: O Sistema Autônomo deverá estar com os protocolos OSPF e iBGP configurados e com as sessões eBGP estabelecidas com o PTT-02 e com a Operadora-02.

Inicialmente serão apresentados os comandos para a configuração do mikrotik_borda para conectá-lo ao PTT-01. As configurações do roteador cisco estão listadas a partir do item 11.

1. O primeiro passo é configurar endereçamento IPv4 e IPv6 na interface ether5 do mikrotik_borda e adiciona-los à vlan 400, utilizada para a troca de tráfego multilateral no PTT-01

   Utilize os seguintes comandos no mikrotik_borda para realizar esse passo:

```
> ip address add address=102.111.0.XX netmask=255.255.255.0 interface=ether5 \
comment=EBGP-PTT-01
> ipv6 address add address=4d0c:111::XX/64 interface=ether5 \
comment=EBGP-PTT-01
> interface vlan add name=VLAN-ATM-PTT-01 vlan-id=400 interface=ether5
```

2. Teste a conectividade da interface criada “pingando” as interfaces do *route server* e do *looking glass* do PTT-01

3. Se houver conectividade, configure as sessões eBGP IPv4 e IPv6 entre o roteador mikrotik_borda e o roteador do *looking glass*.

   Utilize os seguintes comandos no mikrotik_borda para estabelecer essa sessão:

```
> /routing bgp peer add address-families=ip name=EBGP-IPV4-LG-PTT01 \
remote-address=102.111.0.253 remote-as=64511 nexthop-choice=force-self
> /routing bgp peer add address-families=ipv6 name=EBGP-IPV6-LG-PTT01 \
remote-address=4D0C:111::253 remote-as=64511 nexthop-choice=force-self
> /
```

   Para verificar se a sessão foi estabelecida utilize o seguinte comando:

```
> routing bgp peer print brief
```

4. Agora, estabeleça as sessões eBGP IPv4 e IPv6 entre o mikrotik_borda e o *route server*. Lembre-se de colocar a sessão no estado “*disable*” e só habilita-la após a configuração das políticas de roteamento.

   No roteador mikrotik_borda, execute os seguintes comandos para configurar as sessões eBGP IPv4 e IPv6:

```
> /routing bgp peer add address-families=ip name=EBGP-IPV4-RS-PTT01 \
remote-address=102.111.0.254    remote-as=64501    nexthop-choice=force-self
disable=yes

> /routing bgp peer add address-families=ipv6 name=EBGP-IPV6-RS-PTT01 \
remote-address=4D0C:111::254    remote-as=64501    nexthop-choice=force-self
disable=yes

> /
```

5. A política de saída a ser configurada no mikrotik_borda deve seguir os seguintes critérios:

   - O tráfego de entrada do AS, IPv4 e IPv6, deve vir preferencialmente pelo PTT-01 em relação à Operadora-02
   - O tráfego de entrada com destino aos IPs do PoP-01 deve vir preferencialmente pelo PTT-01 em relação às Operadoras e ao PTT-02
   - O tráfego de entrada do AS que não vier pelos PTTs deve vir preferencialmente pela Operadora-02 em relação a Operadora-03

6. Existem diversas formas de se atender os critérios acima. Uma solução possível é estabelecer uma política de saída no roteador mikrotik_borda que anuncie os seguintes prefixos através do *route server* do PTT-01:

   - 102.XX.0.0/21 - (1º /21 do PoP-01)
   - 102.XX.8.0/21 - (2º /21 do PoP-01)
   - 102.XX.0.0/20 - (/20 do PoP-01)
   - 102.XX.16.0/20 - (/20 do PoP-02)
   - 4D0C:XX::/37 - (1º /37 do PoP-01)
   - 4D0C:XX:0800::/37 - (2º /37 do PoP-01)
   - 4D0C:XX::/36 - (/36 do PoP-01)
   - 4D0C:XX:8000::/36 - (/36 do PoP-02)

   Esses prefixos são mais específicos que os já anunciados para a Operadora-02 e para divulgá-los, execute os seguintes comandos:

```
> /routing bgp network
  add disabled=no network=102.XX.0.0/21 synchronize=no
  add disabled=no network=102.XX.8.0/21 synchronize=no
  add disabled=no network=102.XX.0.0/20 synchronize=no
  add disabled=no network=102.XX.16.0/20 synchronize=no
  add disabled=no network=4D0C:XX::/37 synchronize=no
  add disabled=no network=4D0C:XX:800::/37 synchronize=no
  add disabled=no network=4D0C:XX::/36 synchronize=no
  add disabled=no network=4D0C:XX:8000::/36 synchronize=no
> /routing filter
  add action=accept chain=BGP-OUT-PTT01-IPV4 prefix=102.XX.0.0/21
  add action=accept chain=BGP-OUT-PTT01-IPV4 prefix=102.XX.8.0/21
  add action=accept chain=BGP-OUT-PTT01-IPV4 prefix=102.XX.0.0/20
  add action=accept chain=BGP-OUT-PTT01-IPV4 prefix=102.XX.16.0/20
  add action=discard chain=BGP-OUT-PTT01-IPV4 prefix=0.0.0.0/0 prefix-length=0-32
  add action=accept chain=BGP-OUT-PTT01-IPV6 prefix=4D0C:XX::/37
  add action=accept chain=BGP-OUT-PTT01-IPV6 prefix=4D0C:XX:800::/37
  add action=accept chain=BGP-OUT-PTT01-IPV6 prefix=4D0C:XX::/36
  add action=accept chain=BGP-OUT-PTT01-IPV6 prefix=4D0C:XX:8000::/36
  add action=discard chain=BGP-OUT-PTT01-IPV6 prefix=::/0 prefix-length=0-128
> /routing bgp peer set EBGP-IPV4-RS-PTT01 out-filter=BGP-OUT-PTT01-IPV4
> /routing bgp peer set EBGP-IPV6-RS-PTT01 out-filter=BGP-OUT-PTT01-IPV6
```

7. Como política de entrada no mikrotik_borda, é preciso rejeitar o recebimento dos anúncios vindos do *route server* do PTT-01 que contenham: prefixos do seu próprio AS, prefixos da Operadora-02, *bogons* e rota *default;* tanto IPv4 quanto para IPv6. Nos prefixos restantes, aumente o valor do atributo LocalPref, influenciando para que o tráfego de saída do AS saia preferencialmente pelo PTT-01.

   Para aplicar essas regras sobre os anúncios IPv4 recebidos, execute os seguintes comandos no roteador mikrotik_borda:

```
> /routing filter
 add action=discard chain=BGP-IN-PTT01-IPV4 prefix=102.XX.0.0/19 prefix-length=19-32
 add action=discard chain=BGP-IN-PTT01-IPV4 prefix=102.120.0.0/16 prefix-length=16-32
 add action=discard chain=BGP-IN-PTT01-IPV4 prefix=0.0.0.0/8 prefix-length=8-32
 add action=discard chain=BGP-IN-PTT01-IPV4 prefix=10.0.0.0/8 prefix-length=8-32
 add action=discard chain=BGP-IN-PTT01-IPV4 prefix=100.64.0.0/10 prefix-length=10-32
 add action=discard chain=BGP-IN-PTT01-IPV4 prefix=127.0.0.0/8 prefix-length=8-32
 add action=discard chain=BGP-IN-PTT01-IPV4 prefix=169.254.0.0/16 prefix-length=16-32
 add action=discard chain=BGP-IN-PTT01-IPV4 prefix=172.16.0.0/12 prefix-length=12-32
 add action=discard chain=BGP-IN-PTT01-IPV4 prefix=192.0.0.0/24 prefix-length=24-32
 add action=discard chain=BGP-IN-PTT01-IPV4 prefix=192.0.2.0/24 prefix-length=24-32
 add action=discard chain=BGP-IN-PTT01-IPV4 prefix=192.168.0.0/16 prefix-length=16-32
 add action=discard chain=BGP-IN-PTT01-IPV4 prefix=198.18.0.0/15 prefix-length=15-32
 add action=discard chain=BGP-IN-PTT01-IPV4 prefix=198.51.100.0/24 prefix-length=24-32
 add action=discard chain=BGP-IN-PTT01-IPV4 prefix=203.0.113.0/24 prefix-length=24-32
 add action=discard chain=BGP-IN-PTT01-IPV4 prefix=224.0.0.0/4 prefix-length=4-32
 add action=discard chain=BGP-IN-PTT01-IPV4 prefix=0.0.0.0/0
 add action=accept chain=BGP-IN-PTT01-IPV4 set-bgp-local-pref=150
> /
```

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

```
> /routing filter
  add action=discard chain=BGP-IN-PTT01-IPV6 prefix=4d0c:XX::/32 prefix-length=32-128
  add action=discard chain=BGP-IN-PTT01-IPV6 prefix=4d0c:120::/32 prefix-length=32-128
  add action=discard chain=BGP-IN-PTT01-IPV6 prefix=2001:db8::/32 prefix-length=32-128
  add action=accept chain=BGP-IN-PTT01-IPV6 prefix=2001:500::/30 prefix-length=30-64 \
set-bgp-local-pref=150
  add action=accept chain=BGP-IN-PTT01-IPV6 prefix=2001::/32 prefix-length=32-64 \
set-bgp-local-pref=150
  add action=accept chain=BGP-IN-PTT01-IPV6 prefix=2001::/16 prefix-length=16-64 \
set-bgp-local-pref=150
  add action=accept chain=BGP-IN-PTT01-IPV6 prefix=2001:c00::/23 prefix-length=23-64 \
set-bgp-local-pref=150
  add action=accept chain=BGP-IN-PTT01-IPV6 prefix=2002::/16 prefix-length=16-64 \
set-bgp-local-pref=150
  add action=accept chain=BGP-IN-PTT01-IPV6 prefix=2003::/16 prefix-length=16-64 \
set-bgp-local-pref=150
  add action=accept chain=BGP-IN-PTT01-IPV6 prefix=2400::/12 prefix-length=12-64 \
set-bgp-local-pref=150
  add action=accept chain=BGP-IN-PTT01-IPV6 prefix=2600::/12 prefix-length=12-64 \
set-bgp-local-pref=150
  add action=accept chain=BGP-IN-PTT01-IPV6 prefix=2610::/23 prefix-length=23-64 \
set-bgp-local-pref=150
  add action=accept chain=BGP-IN-PTT01-IPV6 prefix=2620::/23 prefix-length=23-64 \
set-bgp-local-pref=150
  add action=accept chain=BGP-IN-PTT01-IPV6 prefix=2800::/12 prefix-length=12-64 \
set-bgp-local-pref=150
  add action=accept chain=BGP-IN-PTT01-IPV6 prefix=2a00::/12 prefix-length=12-64 \
set-bgp-local-pref=150
  add action=accept chain=BGP-IN-PTT01-IPV6 prefix=2801::/24 prefix-length=24-64 \
set-bgp-local-pref=150
  add action=accept chain=BGP-IN-PTT01-IPV6 prefix=2c00::/12 prefix-length=12-64 \
set-bgp-local-pref=150
  add action=accept chain=BGP-IN-PTT01-IPV6 prefix=4d0c::/16 prefix-length=16-64 \
set-bgp-local-pref=150
  add action=discard chain=BGP-IN-PTT01-IPV6 prefix=::/0 prefix-length=0-128
> /
```

Por fim, aplique as políticas criadas. Para isso, execute os seguintes comando no roteador mikrotik_borda:

```
/routing bgp peer set EBGP-IPV4-RS-PTT01 in-filter=BGP-IN-PTT01-IPV4
/routing bgp peer set EBGP-IPV6-RS-PTT01 in-filter=BGP-IN-PTT01-IPV6
```

8. Outras boas práticas devem ser aplicadas para evitar o tráfego de pacotes indesejados, como:

- Filtrar pacotes com endereços *bogons*
- Desabilitar o MNDP (*Mikrotik Neighbor Discovery Protocol*)
- Desabilitar RA IPv6

Para realizar esses passos, execute os seguintes comandos no roteador mikrotik_borda:

```
> /ip firewall filter
  add action=drop chain=forward in-interface=ether5 src-address-list=FILTRO-BOGONS-V4

> /ipv6 firewall filter
  add action=drop chain=forward in-interface=ether5 src-address=2001:db8::/32
  add action=accept chain=forward in-interface=ether5 src-address-list=FILTRO-BOGONS-V6
  add action=drop chain=forward in-interface=ether5

> /ip neighbor discovery
  set ether5 discover=no

> /ipv6 nd print
> /ipv6 nd set 0 disabled=yes
```

9. Por fim, com todas as políticas de entrada e saída e todos os filtros configurados, habilite a sessão eBGP com o *route server*

```
> /routing bgp peer set EBGP-IPV4-RS-PTT01 disable=no

> /routing bgp peer set EBGP-IPV6-RS-PTT01 disable=no
```

10. Verifique no *looking glass* da Operadora-01 e no *looking glass* do PTT-01 os prefixo anunciados e compare-os. Utilize o seguinte comando para verificar quais rotas são geradas a partir do seu ASN:

```
> sh ip bgp regexp 655XX$
> sh ipv6 bgp regexp 655XX$
```

11. Para estabelecer a sessão eBGP entre o roteador cisco e o roteador da Operadora-03, o primeiro passo é adicionar os endereços IPv4 e IPv6 à interface GE0/0.2XX e adicionar essa interface a vlan 2XX. Essa vlan foi provisionada pela equipe do PTT e reservada para o acordo bi-lateral entre o AS655XX e a Operadora-03 para a contratação de um *link* Internet.

    Para realizar essa tarefa, execute os seguintes comandos no roteador cisco:

```
# configure terminal
# interface GigabitEthernet0/0.2XX
# encapsulation dot1Q 2XX
# ip address 102.130.XX.1 255.255.255.254
# ipv6 address 4D0C:130:0:XX::1/127
# exit
# exit
```

12. Também é necessário configurar endereçamento IPv4 e IPv6 na interface Loopback10, que será utilizada para estabelecer a sessão eBGP com a Operadora-03, e adiconar esta interface aos processos do OSPF.

    Execute no roteador cisco os seguintes comandos:

```
# configure terminal
# interface Loopback10
# description EBGP
# ip address 102.XX.16.253 255.255.255.255
# ipv6 address 4D0C:XX:8000::253:1/112
# ip ospf 100 area 0
# ipv6 ospf 200 area 0
# ipv6 ospf network point-to-point
# router ospf 100
# passive-interface Loopback10
# ipv6 router ospf 200
# passive-interface Loopback10
# exit
# exit
```

13. Teste a conectividade com a interface Loopback10 criada, tanto em IPv4 quanto em IPv6, realizando testes de “ping” e “traceroute” a partir dos demais equipamentos do AS. É importante garantir que a configuração da interface esteja correta antes de utiliza-la para estabelecer a sessão eBGP.

14. Crie rotas estáticas para os endereços IPv4 e IPv6 da interface loopback da Operadora-03 no roteador cisco, para garantir que haja conectividade entre os dois roteadores. Após essa configuração, teste a conectividade com a interface loopback da Operadora-03.

    Para criar essas rotas, execute os seguintes comandos:

```
# configure terminal
# ip route 102.130.255.255 255.255.255.255 102.130.XX.0
# ipv6 route 4D0C:130:0:FFFF::255/128 4D0C:130:0:XX::
# exit
```

15. Com as interfaces e rotas estáticas configuradas, configure as sessões eBGP IPv4 e IPv6 entre o roteador cisco e o roteador da Operadora-03. Lembre-se de deixar o estado das sessões em “*shutdown*” até configurar as políticas de roteamento, e lembre-se também de configurar o parâmetro “ebgp-multi-hop” com o valor 2, pois as sessões serão estabelecidas utilizando os endereços IPs da interface Loopback10.

Para realizar essas configurações, execute os seguintes comandos no roteador cisco:

```
# configure terminal
# router bgp 655XX
# neighbor 102.130.255.255 remote-as 64530
# neighbor 102.130.255.255 shutdown
# neighbor 102.130.255.255 ebgp-multihop 2
# neighbor 102.130.255.255 description EBGP-IPV4-OP03
# neighbor 4D0C:130:0:FFFF::255 remote-as 64530
# neighbor 4D0C:130:0:FFFF::255 shutdown
# neighbor 4D0C:130:0:FFFF::255 ebgp-multihop 2
# neighbor 4D0C:130:0:FFFF::255 description EBGP-IPV6-OP03
# address-family ipv4
# neighbor 102.130.255.255 activate
# neighbor 102.130.255.255 soft-reconfiguration inbound
# address-family ipv6
# neighbor 4D0C:130:0:FFFF::255 activate
# neighbor 4D0C:130:0:FFFF::255 soft-reconfiguration inbound
# exit
# exit
# exit
```

16. Com as sessões configuradas, é preciso agora criar políticas de saída. Essas políticas devem seguir os seguintes critérios:

    - O tráfego de entrada com destino aos IPs do PoP-02 deve vir preferencialmente pelo PTT-02 em relação às Operadoras e ao PTT-01

        - Um modo possível de respeitar esse critério é adicionando à política de saída já existente com o PTT-02, os anúncios dos 2 prefixos /37 IPv6 e dos 2 prefixos /21 IPv4 do POP02. Isso pode ser feito executando os seguintes comandos no roteador cisco:

```
# configure terminal
# ip route 102.XX.16.0 255.255.248.0 Null0
# ip route 102.XX.24.0 255.255.248.0 Null0
# ip prefix-list BGP-IPV4-OUT-PTT-02 seq 30 permit 102.XX.16.0/21
# ip prefix-list BGP-IPV4-OUT-PTT-02 seq 40 permit 102.XX.24.0/21

# ipv6 route 4D0C:XX:8000::/37 Null0
# ipv6 route 4D0C:XX:8800::/37 Null0
# ipv6 prefix-list BGP-IPV6-OUT-PTT-02 seq 30 permit 4D0C:XX:8000::/37
# ipv6 prefix-list BGP-IPV6-OUT-PTT-02 seq 40 permit 4D0C:XX:8800::/37

# router bgp 655XX
# address-family ipv4 unicast
# network 102.XX.16.0 mask 255.255.248.0
# network 102.XX.24.0 mask 255.255.248.0
# address-family ipv6 unicast
# network 4D0C:XX:8000::/37
# network 4D0C:XX:8800::/37
# exit
# exit
# exit
```

- O *link* contratado com a Operadora-03 deve ser utilizado apenas como *backup*

    - Um modo possível de respeitar esse critério é criando uma política de saída que anuncie os prefixos /32 IPv6 e /19 IPv4, através da Operadora-03 com *prepends*. Isso pode ser feito executando os seguintes comandos no roteador cisco:

```
# configure terminal
# ip route 102.XX.0.0 255.255.224.0 Null0
# ip prefix-list BGP-IPV4-OUT-OP03 seq 10 permit 102.XX.0.0/19
# route-map BGP-IPV4-OUT-OP03 permit 10
# match ip address prefix-list BGP-IPV4-OUT-OP03
# set as-path prepend 655XX 655XX 655XX
# router bgp 655XX
# address-family ipv4 unicast
# network 102.XX.0.0 mask 255.255.224.0
# neighbor 102.130.255.255 route-map BGP-IPV4-OUT-OP03 out

# ipv6 route 4D0C:XX::/32 Null0
# ipv6 prefix-list BGP-IPV6-OUT-OP03 seq 10 permit 4D0C:XX::/32
# route-map BGP-IPV6-OUT-OP03 permit 10
# match ipv6 address prefix-list BGP-IPV6-OUT-OP03
# set as-path prepend 655XX 655XX 655XX
# router bgp 655XX
# address-family ipv6 unicast
# network 4D0C:XX::/32
# neighbor 4D0C:130:0:FFFF::255 route-map BGP-IPV6-OUT-OP03 out
# exit
# exit
# exit
```

17. Crie também, uma política de entrada no roteador cisco rejeitando o recebimento de prefixos que contenham rota *default*, prefixos do seu próprio AS, e endereços *bogons*, tanto IPv4 quanto para IPv6. Como esses filtros já foram criados anteriormente, basta associá-los a um “route-map” de entrada.

    Para isso, execute os seguintes comandos no roteador cisco:

```
# configure terminal
# ip as-path access-list 100 permit .*
# route-map BGP-IPV4-IN-OP03 deny 10
# match ip address prefix-list IPV4-BOGONS
# route-map BGP-IPV4-IN-OP03 permit 20
# match as-path 100
# router bgp 655XX
# address-family ipv4 unicast
# neighbor 102.130.255.255 route-map BGP-IPV4-IN-OP03 in

# route-map BGP-IPV6-IN-OP03 deny 10
# match ipv6 address prefix-list MEUS-PREFIXOS
# route-map BGP-IPV6-IN-OP03 deny 20
# match ipv6 address prefix-list PREFIXO-DOCUMENTACAO
# route-map BGP-IPV6-IN-OP03 permit 30
# match ipv6 address prefix-list PREFIXOS-VALIDOS
# router bgp 655XX
# address-family ipv6 unicast
```

```
# neighbor 4D0C:130:0:FFFF::255 route-map BGP-IPV6-IN-OP03 in
# exit
# exit
# exit
```

18. Para aplicar as novas políticas aos prefixos anunciados e recebidos através do PTT-02, é preciso “limpar” essas informações na tabela de roteamento BGP.

    Execute o seguinte comando:

```
# clear bgp all 64502 soft
```

19. Com todas as políticas configuradas, habilite a sessão eBGP com a Operadora-03.

    Para isso execute os seguintes comandos:

```
# configure terminal
# router bgp 655XX
# no neighbor 102.130.255.255 shutdown
# no neighbor 4D0C:130:0:FFFF::255 shutdown
# exit
# exit
```

20. Verifique no servidor de *looking glass* da Operadora-01 e no servidor de *looking glass* do PTT-02 os prefixo anunciados e compare-os

21. Teste conectividade com os outros ASes