Exercício 5 - Conectando-se a um PTT

Objetivo: Conectar o Sistema Autônomo a um PTT a partir do PoP-02. Serão abordados tópicos referentes as boas práticas de configuração e participação em um PTT, além de trabalharmos com políticas de roteamento de entrada e de saída.

Cenário: A rede do AS deve estar com OSPF e iBGP configurados e a sessão eBGP com a Operadora-02 deve estar ativa.

A partir deste exercício o AS passará a ter uma segunda saída para redes externas, justificando a aquisição do ASN. Essa segunda saída será a conexão ao PTT-02 feita através do roteador cisco do PoP-02. A estrutura do PTT existente no laboratório é composta por dois roteadores, um *route server*, responsável por divulgar as rotas dos participantes, e um *looking glass*. Após a conclusão do exercício, todo tráfego de entrada e saída do AS fluirá preferencialmente pelo PTT.

1. O primeiro passo para estabelecer a sessão eBGP é adicionar os endereços IPv4 e IPv6 à interface GE0/0.200 e adicionar essa interface a vlan 200, utilizada para a troca de tráfego multilateral no PTT-02.

   Para realizar essa tarefa, execute o seguinte comando no roteador cisco:

```
# configure terminal
# interface GigabitEthernet0/0.200
# encapsulation dot1Q 200
# ip address 102.222.0.XX 255.255.255.0
# ipv6 address 4D0C:222::XX/64
# exit
# exit
```

2. O passo seguinte é estabelecer a sessão eBGP entre o roteador cisco e o *looking glass*. Essa sessão não tem muitas restrições, sendo recomendado que se envie todas as informações de tabela de roteamento (*Full Routing*). Essa sessão deverá ser estabelecida com o endereço da interface física, fornecido pelo PTT.

   Para isso, execute o seguinte comando no roteador cisco:

```
# configure terminal
# router bgp 655XX
# neighbor 102.222.0.253 remote-as 64522
# neighbor 102.222.0.253 description EBGP-IPV4-LG-02
# neighbor 4D0C:222::253 remote-as 64522
# neighbor 4D0C:222::253 description EBGP-IPV6-LG-02
# address-family ipv4
# neighbor 102.222.0.253 activate
# address-family ipv6
# neighbor 4D0C:222::253 activate
# exit
# exit
# exit
```

   Para verificar se a sessão foi estabelecida execute o seguinte comando no cisco:

```
# show bgp ipv4 unicast summary
# show bgp ipv6 unicast summary
```

   Na saída do comando acima, o último campo deve indicar o número de rotas recebidas se a sessão estiver estabelecida corretamente. O *looking glass* deve anunciar algum prefixo para o seu AS? É

preciso aplicar filtros de entrada e/ou saída sobre essa sessão?

3. O passo seguinte é configurar a sessão eBGP com o *route server.* Essa sessão deverá ser fechada também através do endereço da interface física, no entanto, ela deverá ser configurada com o comando `shutdown` habilitado na configuração de vizinhança. Essa prática é recomendada para evitar que se estabeleça a sessão antes das políticas de roteamento serem aplicadas e com isso, evitar rotas indevidas acabem sendo anunciadas ao *route server*, que possui uma política de "derrubar" sessões eBGP que enviem para ele mais do que 5 prefixos.

   Os comando a serem executados no cisco são os seguintes:

```
# configure terminal
# router bgp 655XX
# no bgp enforce-first-as
# neighbor 102.222.0.254 remote-as 64502
# neighbor 102.222.0.254 shutdown
# neighbor 102.222.0.254 description EBGP-IPV4-RS-02
# neighbor 4D0C:222::254 remote-as 64502
# neighbor 4D0C:222::254 shutdown
# neighbor 4D0C:222::254 description EBGP-IPV6-RS-02
# address-family ipv4
# neighbor 102.222.0.254 activate
# neighbor 102.222.0.254 soft-reconfiguration inbound
# address-family ipv6
# neighbor 4D0C:222::254 activate
# neighbor 4D0C:222::254 soft-reconfiguration inbound
# exit
# exit
# exit
```

4. Com as configurações da sessão eBGP prontas, antes de retirar o comando `shutdown`, configure as políticas de saída no roteador cisco, aplique as rotas recebidas via PTT-02, respeitando os seguintes critérios:

   Políticas de saída:

   - Anunciar apenas dois prefixos /36 e dois prefixos /20 pelo PTT-02

   Para criar e aplicar essas políticas execute os seguintes comandos no roteador cisco:

```
# configure terminal

# ip route 102.XX.0.0 255.255.240.0 Null0
# ip route 102.XX.16.0 255.255.240.0 Null0

# ip prefix-list BGP-IPV4-OUT-PTT-02 seq 10 permit 102.XX.0.0/20
# ip prefix-list BGP-IPV4-OUT-PTT-02 seq 20 permit 102.XX.16.0/20
# route-map BGP-IPV4-OUT-PTT-02 permit 10
# match ip address prefix-list BGP-IPV4-OUT-PTT-02

# router bgp 655XX
# address-family ipv4 unicast
# network 102.XX.0.0 mask 255.255.240.0
# network 102.XX.16.0 mask 255.255.240.0
# neighbor 102.222.0.254 route-map BGP-IPV4-OUT-PTT-02 out
```

```
# ipv6 route 4d0c:XX::/36 Null0
# ipv6 route 4d0c:XX:8000::/36 Null0

# ipv6 prefix-list BGP-IPV6-OUT-PTT-02 seq 10 permit 4d0c:XX::/36
# ipv6 prefix-list BGP-IPV6-OUT-PTT-02 seq 20 permit 4d0c:XX:8000::/36
# route-map BGP-IPV6-OUT-PTT-02 permit 10
# match ipv6 address prefix-list BGP-IPV6-OUT-PTT-02

# router bgp 655xx
# address-family ipv6 unicast
# network  4d0c:XX::/36
# network  4d0c:XX:8000::/36
# neighbor 4d0c:222::254 route-map BGP-IPV6-OUT-PTT-02 out
```

5. Agora, configure políticas de entrada no roteador cisco, aplique as rotas recebidas via PTT-02, respeitando os seguintes critérios:

   Políticas de entrada:
   - Aumentar o valor do atributo LocalPref para todas as rotas IPv4 e IPv6 aprendidas via PTT-02
   - Rejeitar o recebimento de prefixos que contenham rota default, prefixos do seu próprio AS e bogons, tanto IPv4 quanto para IPv6.

   Para criar e aplicar essas políticas execute os seguintes comandos no roteador cisco:

```
# configure terminal

# ip prefix-list IPV4-BOGONS seq 10 permit 102.XX.0.0/19 le 32
# ip prefix-list IPV4-BOGONS seq 20 permit 0.0.0.0/8 le 32
# ip prefix-list IPV4-BOGONS seq 30 permit 10.0.0.0/8 le 32
# ip prefix-list IPV4-BOGONS seq 40 permit 100.64.0.0/10 le 32
# ip prefix-list IPV4-BOGONS seq 50 permit 127.0.0.0/8 le 32
# ip prefix-list IPV4-BOGONS seq 60 permit 169.254.0.0/16 le 32
# ip prefix-list IPV4-BOGONS seq 70 permit 172.16.0.0/12 le 32
# ip prefix-list IPV4-BOGONS seq 80 permit 192.0.0.0/24 le 32
# ip prefix-list IPV4-BOGONS seq 90 permit 192.0.2.0/24 le 32
# ip prefix-list IPV4-BOGONS seq 100 permit 192.168.0.0/16 le 32
# ip prefix-list IPV4-BOGONS seq 110 permit 198.18.0.0/15 le 32
# ip prefix-list IPV4-BOGONS seq 120 permit 198.51.100.0/24 le 32
# ip prefix-list IPV4-BOGONS seq 130 permit 203.0.113.0/24 le 32
# ip prefix-list IPV4-BOGONS seq 140 permit 224.0.0.0/4 le 32
# ip prefix-list IPV4-BOGONS seq 150 permit 0.0.0.0/0

# route-map BGP-IPV4-IN-PTT-02 deny 10
# match ip address prefix-list IPV4-BOGONS

# route-map BGP-IPV4-IN-PTT-02 permit 20
# set local-preference 150

# ipv6 prefix-list MEUS-PREFIXOS seq 10 permit 4d0c:XX::/32 le 128

# ipv6 prefix-list PREFIXO-DOCUMENTACAO seq 10 permit 2001:db8::/32 le 128

# ipv6 prefix-list PREFIXOS-VALIDOS seq 10 permit 2001:500::/30 le 64
# ipv6 prefix-list PREFIXOS-VALIDOS seq 20 permit 2001::/32 le 64
```

```
# ipv6 prefix-list PREFIXOS-VALIDOS seq 30 permit 2001::/16 le 64
# ipv6 prefix-list PREFIXOS-VALIDOS seq 40 permit 2001:c00::/23 le 64
# ipv6 prefix-list PREFIXOS-VALIDOS seq 50 permit 2002::/16 le 64
# ipv6 prefix-list PREFIXOS-VALIDOS seq 60 permit 2003::/16 le 64
# ipv6 prefix-list PREFIXOS-VALIDOS seq 70 permit 2400::/12 le 64
# ipv6 prefix-list PREFIXOS-VALIDOS seq 80 permit 2600::/12 le 64
# ipv6 prefix-list PREFIXOS-VALIDOS seq 90 permit 2610::/23 le 64
# ipv6 prefix-list PREFIXOS-VALIDOS seq 100 permit 2620::/23 le 64
# ipv6 prefix-list PREFIXOS-VALIDOS seq 110 permit 2800::/12 le 64
# ipv6 prefix-list PREFIXOS-VALIDOS seq 120 permit 2a00::/12 le 64
# ipv6 prefix-list PREFIXOS-VALIDOS seq 130 permit 2801::/24 le 64
# ipv6 prefix-list PREFIXOS-VALIDOS seq 140 permit 2c00::/12 le 64
# ipv6 prefix-list PREFIXOS-VALIDOS seq 150 permit 4d0c::/16 le 64

# route-map BGP-IPV6-IN-PTT-02 deny 10
# match ipv6 address prefix-list MEUS-PREFIXOS

# route-map BGP-IPV6-IN-PTT-02 deny 20
# match ipv6 address prefix-list PREFIXO-DOCUMENTACAO

# route-map BGP-IPV6-IN-PTT-02 permit 30
# match ipv6 address prefix-list PREFIXOS-VALIDOS
# set local-preference 150

# router bgp 655XX
# address-family ipv4 unicast
# neighbor 102.222.0.254 route-map BGP-IPV4-IN-PTT-02 in

# address-family ipv6 unicast
# neighbor 4d0c:222::254 route-map BGP-IPV6-IN-PTT-02 in

# exit
# exit
# exit
```

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

    - Filtrar pacotes com endereços bogons
    - Desabilitar o CDP (Cisco Discovery Protocol)
    - Desabilitar RA IPv6

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

```
# configure terminal
# interface GigabitEthernet0/0.200
# ip access-group FILTRO-BOGONS-V4 in
# ipv6 traffic-filter FILTRO-BOGONS-V6 in
# no cdp enable
# ipv6 nd ra suppress
# exit
# exit
```

7. Com políticas e filtros aplicados, habilite as sessões eBGP, IPv4 e IPv6, e salve a configuração corrente.

Para isso, execute os seguintes comandos no roteador cisco:

```
# configure terminal
# router bgp 655XX
# no neighbor 102.222.0.254 shutdown
# no neighbor 4d0c:222::254 shutdown
# exit
# exit
# copy running-config startup-config
```

8. Verifique se a sessão foi estabelecida, as rotas anunciadas e recebidas via PTT.

   Para realizar essas verificações execute os seguintes comandos no roteador cisco:

```
# show bgp ipv4 unicast summary
# show bgp ipv6 unicast summary
# show bgp ipv4 unicast neighbors 102.222.0.254 received-routes
# show bgp ipv6 unicast neighbors 4D0C:222::254 received-routes
# show bgp ipv4 unicast neighbors 102.222.0.254 advertised-routes
# show bgp ipv6 unicast neighbors 4D0C:222::254 advertised-routes
```

   - Quantos prefixos IPv4 e IPv6 estão sendo aprendidos via PTT?
   - Há diferenças entre a quantidade de prefixos IPv4 e IPv6? Por quê?
   - As políticas IPv4 e IPv6 de saída foram aplicadas corretamente?
   - O valor do atributo LocalPref foi alterado corretamente em todos os prefixos aprendidos?

Acesse os outros roteadores do AS e verifique se os prefixos aprendidos via PTT estão sendo repassados corretamente para todo o ISP via iBGP com o valor do atributo LocalPref correto.