ISEL
INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

Licenciatura em Engenharia Informática e Multimédia

Redes de Informação

Ano Letivo 2020/21

5º Semestre

Trabalho3

22 fevereiro

Grupo 7:

Luís Fonseca (A45125)

Miguel Silvestre (A45101)

Duarte Domingues (A45140)

Docente: Eng. Vítor Almeida

Índice de Conteúdos

Índice de Figuras

Introdução e Objetivos

Para este último projeto proposto na disciplina de Redes de Informação, pretendia-se a implementação do protocolo BGP, sendo dada a configuração do protocolo OSPF e RIP em certa área.

Neste contexto, deveríamos inserir o protocolo BGP no Core do ISP, assim como na migração quer dos acessos dos seus clientes quer no peering externo para este novo protocolo. Devemos ter em conta:
Relações com os clientes:

Semelhante ao que efetuámos no trabalho anterior, começámos por configurar todos os endereços IP dos vários dispositivos, e os endereços IP (redes) de cada interface, tendo em conta quais dos dispositivos deveriam ser configurados com encaminhamento estático. Seguimos o enunciado para configurar os vários AS, de acordo os endereços explícitos lá.

Posto isto, passámos à implementação das várias restrições no que toca à comunicação entre AS. Todas as questões relevantes relativas a esta topologia serão abordadas no presente relatório, assim como a listagem de comandos usados nas várias etapas da configuração.

Fase 1

a) Indique se, no domínio OSPF do ISP, utilizar blocos de endereçamento IPv4 distintos em cada uma das áreas faz sentido.

O uso de diferentes blocos IPv4 faz sentido, para que seja necessário conseguir distinguir os diferentes AS. A área de backbone(área 0) como tem de receber todos os LSAs das diferentes áreas, faz sentido usar diferentes endereços, sendo mais fácil de verificar onde estão a ser recebidos os diferentes endereços das áreas existentes.

b) Quais os problemas que adviriam de uma distribuição de endereços como a utilizada se a topologia representasse uma rede real e não existissem endereços IPv4 com "fartura"?

Redução dos endereços IP, visto que em IPv4 existe um número limitado de endereços.

A expansão da tabela de encaminhamento, visto que o número de servidores pode vir a aumentar, também crescem o número de rotas na rede.

Falha na conetividade: visto que caso, estejamos a configurar mais do que um endereço IPv4 publico, o host da rede esta oculto.

c) Como procederia se o acesso para controlo/gestão dos equipamentos do ISP, ou outro AS, não devesse poder ser realizado de fora do respetivo AS. Como resultado deste ponto, para além da resposta a questões evidenciadas nas alíneas anteriores.

Criação de endereços privados para cada uma das áreas, facilitando a informação contida em cada um dos AS, não permitindo que os outros AS conheçam as outras rotas.

d) Indique alguns prós e contras da utilização de endereços IP privados e públicos nas redes interiores do ISP, assim como nos Loopbacks utilizados para se obter os routerID.

Vantagens de usar endereços privados:

a. Suporta de vários dispositivos NAT
b. Aumento da segurança das informações em computadores individuais.

Desvantagens de usar endereços privados:

a. NAT diminui a velocidade sob alta demanda na troca de dados;

Vantagens de usar endereços públicos:

a. Mais segura
b. Capacidade de controlar o acesso à Internet dos funcionários

Desvantagens de usar endereços públicos:

a. Mais complexa;
b. Exige constante manutenção e conservação;

Fase 2

1 – Configuração do protocolo OSPF

a) **Na topologia do trabalho quantos DR devem existir e gerar LSA tipo 2?**
Efetuando o comando “sh ip ospf”, não foram encontrados DRs, pelo que não existem DRs na topologia.

b) **Quais os tipos de LSA que andam dentro da área 3 do domínio OSPFv2 do ISP (ver PE7, por exemplo)?**
Os tipos de LSA que andam dentro da área 3 do domínio OSPFv2 do ISP são LSA do tipo 1, 3 e 7.

c) **Para procurar garantir que a ligação escolhida entre o PE1 e o PE3 é a N17 e não outra, mesmo que houvesse uma ao lado, em paralelo, como 1Gbit/s também, como procederia?**
Baixava o custo da ligação, neste caso para 1mb;

d) **Qual a razão do custo/métrica entre o PE1 (30.1.255.1) e o PE3 ser 6 (30.1.255.3)?**
O custo desta ligação no início era 10, mas teve de ser alterada para 6;

e) **Suponha que pretendia colocar as duas redes entre os routers P6 e o PE7 (N45_1 e N45_2) a balancearem tráfego entre os dois routers. Como procederia?**
Alteraria o custo métrica OSPF das ligações, igualando-a.

2 – Configuração de rotas estáticas de interligação entre domínios (ISP e alguns clientes)

Na lista abaixo, foi necessário criar rotas estáticas para os seguintes routers:

- O router PE6 e R301;
- O router PE7 e o AS302;
- O router PE3 e o R202;
- O router PE1 e o R201:
- O router PE4 e o RC3_1;
- O router PE5 e o RC3_2:

Sendo necessário criar estas rotas estáticas, para que seja necessário a área de backbone conheça as outras áreas.
Efetuando um ping múltiplo, verificamos o correto funcionamento dessas rotas estáticas, e o significado de terem sido feitas rotas estáticas para os routers mencionados acima.

```
P4(tcl)#foreach address {
+>(tcl)#30.3.255.7
+>(tcl)#30.1.255.3
+>(tcl)#10.0.255.2
+>(tcl)#10.0.255.6
+>(tcl)#30.1.255.4
+>(tcl)#30.3.255.7
+>(tcl)#} { ping $address repeat 3 size 1500 }

Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 30.3.255.7, timeout is 2 seconds:
!!!
Success rate is 100 percent (3/3), round-trip min/avg/max = 20/32/44 ms
Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 30.1.255.3, timeout is 2 seconds:
!!!
Success rate is 100 percent (3/3), round-trip min/avg/max = 12/41/64 ms
Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 10.0.255.2, timeout is 2 seconds:
!!!
Success rate is 100 percent (3/3), round-trip min/avg/max = 16/25/40 ms
Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 10.0.255.6, timeout is 2 seconds:
!!!
Success rate is 100 percent (3/3), round-trip min/avg/max = 16/22/28 ms
Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 30.1.255.4, timeout is 2 seconds:
!!!
Success rate is 100 percent (3/3), round-trip min/avg/max = 8/24/32 ms
Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 30.3.255.7, timeout is 2 seconds:
!!!
Success rate is 100 percent (3/3), round-trip min/avg/max = 16/26/32 ms
```

Figura 1 - ping múltiplo

3 – Configuração do protocolo RIPv2

a) As mensagens de RIPv2 não devem ser enviadas para quem não tem interesse nelas. Como proceder para que tal seja conseguido?

Colocando o comando "passive-interface". Assim cada router que não quer receber as informações do router configurado com RIP, não recebe os updates desse mesmo router, configurado com RIP.

b) Poderia ser usado RIPv1 no cliente 2?

Não, visto que o RIPv1 não aceita classless, ou seja, não aceita mascaras.

```
RC2_1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.49.1 to network 0.0.0.0

     10.0.0.0/30 is subnetted, 4 subnets
C       10.0.50.0 is directly connected, GigabitEthernet3/0
C       10.0.49.0 is directly connected, GigabitEthernet5/0
R       10.3.145.0 [120/1] via 10.0.49.1, 00:00:12, GigabitEthernet5/0
R       10.3.245.0 [120/1] via 10.0.49.1, 00:00:12, GigabitEthernet5/0
     60.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       60.0.28.0/24 [120/1] via 10.0.50.2, 00:00:24, GigabitEthernet3/0
C       60.0.29.251/32 is directly connected, Loopback0
R       60.0.29.252/32 [120/1] via 10.0.50.2, 00:00:24, GigabitEthernet3/0
R*   0.0.0.0/0 [120/1] via 10.0.49.1, 00:00:12, GigabitEthernet5/0
```

Figura 2 - tabela de routing RC2_1

```
router rip
 version 2
 passive-interface default
 no passive-interface GigabitEthernet5/0
 network 10.0.0.0
 network 60.0.0.0
 default-information originate
 no auto-summary
```

Figura 3 - configuração RIP

4 - Redistribuição de rotas no AS do ISP entre os protocolos de routing IGP

a) **Justifique a sua escolha de custos tipo E1 ou E2 do OSPF na redistribuição dos endereços IP**
Foi escolhido a rota E2, visto que é aquela que terá sempre uma métrica externa.

b) **Indique a razão da escolha do tipo de redistribuição que utilizou, por exemplo entre o ISP e os clientes 1 e 2 (por exemplo: redistribuição de OSPF no RIP e vice-versa; redistribuição do RIP no OSPF e rotas estáticas no outro sentido; redistribuição mútua, mas usando filtros; rotas estáticas em ambos os sentidos).**
Visto que o router P6 funciona como um ABR, ele irá conhecer as rotas de todo as outras áreas. No router PE7 usamos RIP e rotas estáticas, visto que precisamos que o cliente 1 e 2 espalhe o seu endereço para as outras áreas, sendo mais fácil fazer o ping entre elas.

```
Success rate is 100 percent (3/3), round-trip min/avg/max = 48/58/64 ms
P1(tcl)#
P1(tcl)#
P1(tcl)#foreach address {
+>(tcl)#10.3.145.1
+>(tcl)#10.3.245.1
+>(tcl)#30.3.48.2
+>(tcl)#10.0.49.1
+>(tcl)#10.0.50.2
+>(tcl)#60.0.28.252
+>(tcl)#30.3.48.1
+>(tcl)#60.0.28.1
+>(tcl)#60.0.31.129
+>(tcl)#} { ping $address repeat 3 size 1500 }

Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 10.3.145.1, timeout is 2 seconds:
!!!
Success rate is 100 percent (3/3), round-trip min/avg/max = 16/26/48 ms
Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 10.3.245.1, timeout is 2 seconds:
!!!
Success rate is 100 percent (3/3), round-trip min/avg/max = 16/32/40 ms
Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 30.3.48.2, timeout is 2 seconds:
!!!
Success rate is 100 percent (3/3), round-trip min/avg/max = 48/54/60 ms
Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 10.0.49.1, timeout is 2 seconds:
!!!
Success rate is 100 percent (3/3), round-trip min/avg/max = 44/54/64 ms
Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 10.0.50.2, timeout is 2 seconds:
!!!
Success rate is 100 percent (3/3), round-trip min/avg/max = 96/101/112 ms
Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 60.0.28.252, timeout is 2 seconds:
!!!
Success rate is 100 percent (3/3), round-trip min/avg/max = 84/92/96 ms
Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 30.3.48.1, timeout is 2 seconds:
!!!
Success rate is 100 percent (3/3), round-trip min/avg/max = 48/54/64 ms
Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 60.0.28.1, timeout is 2 seconds:
!!!
Success rate is 100 percent (3/3), round-trip min/avg/max = 100/112/120 ms
```

Figura 4 - ping múltiplo

c) **No router PE7 será necessário incluir os dois comandos de redistribute?**
Sim visto que precisamos de redistribuir a sua rota RIP como a sua rota estática, para todos os AS conheceram as rotas do lado do cliente 1.

d) **A rede N48 poderia ser uma rede com endereços IP privados?**
Não, visto que assim, o cliente 1 não conseguia ligar-se à Internet.

e) **A rede N48 poderia ser uma rede com endereços IP privados?**
Não, visto que como o cliente 2 esta a correr sobre RIP, ele não envia updates das suas rotas para os outros routers.

f) **O que acontece se em configurações como a do router R102_2 o comando "ip ospf network point-to-point" for removido?**
Deixa de propagar a rede, como sendo em point-to-point. O ospf, por defeito, anuncia a rota com /32. Ao fazer override, é necessário usar ligação point-to-point.

g) **R202_1: É necessário na configuração do OSPF, no router 202_1, inserir tantos comandos network?**
Sim, visto que é necessário que todas as rotas sejam conhecidas na área de backbone.

h) **Qual a necessidade de no router P6 se utilizar o comando seguinte e o que acontece se for substituído por área 3 nssa apenas?**
Serve para injetar uma rota por defeito do tipo 7 para a área 3 NSSA. Caso apenas usemos "área 3 nssa", não anuncia nenhuma rota.

i) **A área 3 do domínio OSPF do ISP pode ser configurada como Totally Stub?**
Não, porque a área 3 tem um ASBR, e numa área totally stub, não existem ASBR.

Fase 3

1 - BGPv4 básico

a) **Quando sai uma mensagem BGP de um router qual é o endereço IP de origem que essa mensagem leva? E se o router BGP tiver uma interface loopback 0, por exemplo, configurada qual é o endereço IP de origem que essa mensagem indica? Como resolve a questão de que se existir mais do que um caminho para um router, o facto de uma interface física "morrer" não dever implicar a perda de vizinhança numa relação iBGP?**
O endereço de origem do router que enviou essa mensagem. Aquele que contem a do loopback 0. Olhando para os atributos., aquele que o melhor MED (aquele que tiver um valor mais baixo).

b) **E se um router receber uma mensagem BGP de Update com um Next-hop que não consta na sua tabela de routing, o que acontece?**
A mensagem é ignorada, pois é necessário conhecer o endereço IP do router do próximo hop.
Se um router receber uma mensagem BGP de Update com um Next-hop que não consta na sua tabela de routing ele não irá incluir essa rota na sua tabela de routing. No BGP é necessário ter atualizado as tabelas de routing com as rotas que o BGP vai necessitar antes de correr BGP.

c) **Investigue o comando "no bgp default ipv4-unicast". Será necessário usar este comando ("no bgp default ipv4- unicast") neste trabalho? E se fosse na rede de um ISP real?**
Permite ao router funcionar como multicast IPv4, em vez de únicast (por defeito). Sim, visto que o BGP funciona apenas em multicast.

d) **É necessário configurar o iBGP em todos os routers de todos os AS? Justifique.**
Não, dentro de alguns AS podem estar a correr outros protocolos IGP, não tendo necessidade de usar IBGP para destribuir rotas exteriores dentro do AS.

e) **As tabelas de routing de todos os routers que correm BGP incluem todas as redes existentes na topologia do trabalho, incluindo as 4.4.4.4 e 8.8.8.8.?**
Não, não há a necessidade de os routers incluírem nas tabelas de routing todas as redes existentes na topologia, routers quando querem enviar tráfego para fora confiam noutros routers para desatribuírem a informação para as rotas destino.

f) **Qual a razão pela qual dos routers P não se conseguem fazer Ping a endereços IP noutros AS?**
Não conseguem aceder aos routers fora do AS, visto que não esta configurado BGP neste tipo de router, apenas OSPF.

g) **Será que faz sentido a utilização de endereços IPv4 privados nas ligações ponto-a-ponto dentro dos AS? E entre os AS?**
Não, visto que endereços privados são usados por ISPs e redes de clientes para conservar números de AS exclusivas. Não podem ser usados para aceder a Internet global porque não são exclusivos.

h) Quais são as rotas preferenciais do AS 302 (PE7) até à Internet (simulada pelo 4.4.4.4 e 8.8.8.8)? Alguma surpresa? Justifique

Visto que o router fronteira não tem BGP implementado, não conseguem efetuar o ping para a internet.

i) O tráfego interno do Cliente 2 segue que rota até à saída do ISP para, por exemplo, 4.4.4.4?

Sim, efetuando um "trace" conseguimos chegar a internet com o endereço 4.4.4.4

```
PC302_3> trace 4.4.4.4 -m 15 -P 6
trace to 4.4.4.4, 15 hops max (TCP), press Ctrl+C to stop
 1   60.0.28.252   6.606 ms  10.719 ms  13.648 ms
 2   10.0.50.1   31.620 ms  20.664 ms  20.262 ms
 3   10.0.49.1   45.903 ms  39.363 ms  49.762 ms
 4   10.3.245.1   57.441 ms  43.134 ms  41.113 ms
 5   10.1.44.2   52.467 ms  52.638 ms  77.370 ms
 6   10.1.38.1   75.578 ms  93.309 ms  85.225 ms
 7   10.1.28.1   72.735 ms  82.615 ms  84.274 ms
 8   10.1.23.1   102.792 ms  105.276 ms  127.271 ms
 9   10.1.17.1   125.024 ms  116.973 ms  104.163 ms
10   20.201.12.1   125.639 ms  166.577 ms  149.632 ms
11   4.4.4.4   170.004 ms  179.144 ms  177.575 ms
```

Figura 5 - trace para o endereço da Internet

j) Qual a rota usada entre o PC101_1 e o router R102_2?

Escolhe a rota pela qual apresenta o melhor caminho (neste caso aquele que tiver um MED mais baixo)

```
PC101_1> trace 11.102.3.252 -m 15 -P 6
trace to 11.102.3.252, 15 hops max (TCP), press Ctrl+C to stop
 1   11.101.1.251   9.238 ms  10.337 ms  10.023 ms
 2   11.101.2.2   20.210 ms  20.092 ms  20.208 ms
 3   11.102.3.252   42.902 ms  42.004 ms  43.593 ms

PC101_1>
```

Figura 6 - trace para o endereço 11.102.3.252

k) Qual a rota usada entre o PC101_1 e o router R202_3?

Efetuando um trace, podemos verificar qual a rota que ele escolhe, ou seja, a rota com o caminho mais curto.

```
 1 20.201.12.2 8 msec 20 msec 24 msec
 2 20.202.131.1 [AS 202] 48 msec 12 msec 20 msec
 3 20.202.131.1 [AS 202] !H  !H  !H
```

Figura 7 - rota escolhida quando efetuado o comando trace

l) Qual a rota usada entre o router R201_1 e o router R202_3?

Foi efetuado um trace entre R_201_1 e R_202_3

```
PC302_3> trace 4.4.4.4
trace to 4.4.4.4, 8 hops max, press Ctrl+C to stop
 1   60.0.28.252   10.842 ms  10.123 ms  9.826 ms
 2   10.0.50.1     31.668 ms  31.797 ms  31.979 ms
 3   10.0.49.1     41.083 ms  54.737 ms  31.054 ms
 4   10.3.245.1    62.926 ms  73.085 ms  72.942 ms
 5   10.1.44.2     85.224 ms  86.735 ms  96.428 ms
 6   10.1.38.1    116.727 ms  116.768 ms  107.329 ms
 7   10.1.28.1    137.730 ms  128.675 ms  139.337 ms
 8   10.1.23.1    160.478 ms  172.744 ms  171.673 ms
```

Figura 8 - trace entre R_201_1 e R_202_3

m) Qual a necessidade ao configurar o BGP de introduzir comandos como: "ip route 20.201.0.0 255.255.240.0 Null0 250"?

O uso do comando como "ip route 20.201.0.0 255.255.240.0 Null0 250" é para garantir que descarta todo o tráfego que não tem uma rota mais especifica e é usado para prevenir loops. A distância de 250 aplicada ao router estático assegura que os protocolos de routing a anunciar este prefixo iram dar overide na rota estática.

n) Faz mais sentido utilizar como endereço IP de um vizinho (neighbor) iBGP o endereço de uma das interfaces físicas desse vizinho ou o endereço da interface de loopback utilizada como router ID nesse vizinho? Atualize a configuração dos routers de acordo com o que considerar mais correto.

Faz mais sentido utilizar como endereço IP de um vizinho (neighbor) iBGP a interface loopback, pois é usada para estabelecer conexão entre peers IBGP, a interface loopback permite prevenir tolerância a erros no caso da interface física ou link for abaixo, o que não acontece no caso de usar endereço de uma das interfaces físicas desse vizinho.

o) Verifique se as configurações do BGP nos vários AS estão conforme o que considera correto no que se refere ao uso dos comandos "Update-source" e "Next-hop-self".

O comando é utilizado para formar uma relação de vizinhança com um endereço diferente (o de loopback) do que aquele que está diretamente conectado ao router, permitindo assim ao router em BGP saber que se trata de iBGP devido à utilização de uma interface de loopback. O comando Next-hop-self permite alterar o atributo next-hop das rotas recebidas por si. Observou-se que a maior parte dos routers tinham estas configurações de forma correta, porém, no router 202_3 reparou-se que não se tinha configurado estes comandos, então configurou-se next-hop-self nos vizinhos do mesmo AS e update source corretamente.

```
bgp log-neighbor-changes
neighbor 11.102.6.1 remote-as 102
neighbor 20.202.255.251 remote-as 202
neighbor 20.202.255.251 update-source Loopback0
neighbor 20.202.255.253 remote-as 202
neighbor 20.202.255.253 update-source Loopback0
!
address-family ipv4
 neighbor 11.102.6.1 activate
 neighbor 20.202.255.251 activate
 neighbor 20.202.255.251 next-hop-self
 neighbor 20.202.255.253 activate
 neighbor 20.202.255.253 next-hop-self
 no auto-summary
 no synchronization
 network 20.202.0.0 mask 255.255.0.0
exit-address-family
```

Figura 9 - Configurações do R_202_3

p) Os AS 102 e 202 necessitam de redistribuição de endereços entre BGP e OSPF?

Não é necessária redistribuição de endereços entre BGP e OSPF, pois nos AS 102 e 202, não utilizam OSPF para comunicar entre eles, mas sim BGP, logo não há necessidade de redistribuição.

q) Será que se pode usar um "no syncronization" no BGP no AS do ISP?
Sim, visto que quando corremos BGP em dois ou mais routers, necessitamos de correr iBGP entre todos eles. Este comando permite que não se faça nenhuma "sincronização" iBGP e outro protocolo interno, como por exemplo OSPF, permitindo ao router anunciar rotas aprendidas via iBGP independentemente de existirem as respetivas rotas IGP.

2 – Implementação de políticas no iBGP no ISP

a) **Sem filtros ativos numa sessão BGP, qual o comportamento por default do Cisco IOS relativamente a anunciar/receber rotas? Quais os problemas que o comportamento por default pode causar?**
Por default o Cisco IOS recebe todas as rotas presentes no BGP sem realizar qualquer tipo de filtração, anuncia as rotas para todos os vizinhos da AS

b) **Execute o comando "show bgp neighbors" num router. Quais os timers por default de keepalive e hold? O que significam? Qual o motivo de serem tão longos?**
Os timers por default de keepalive(60s) e hold(180s) por default são longos, pois hold timers muito curtos podem levar a sessões de BGP desconetadas. Isto acontece se pacotes BGP forem buffered por mais tempo que esperado ou se o router estiver demasiado ocupado para gerar mensagens keep alive em tempos muito curtos.

```
GP neighbor is 11.101.2.1,  remote AS 101, external link
 BGP version 4, remote router ID 11.101.7.251
 BGP state = Established, up for 00:00:08
 Last read 00:00:08, last write 00:00:08, hold time is 180, keepalive interval is 60 seconds
 Neighbor capabilities:
   Route refresh: advertised and received(old & new)
   Address family IPv4 Unicast: advertised and received
 Message statistics:
   InQ depth is 0
   OutQ depth is 0
                        Sent       Rcvd
   Opens:                  1          1
   Notifications:          0          0
   Updates:                0          0
   Keepalives:             1          1
   Route Refresh:          0          0
   Total:                  2          2
 Default minimum time between advertisement runs is 30 seconds
```

Figura 10 – Timers BGP

c) **O que aconteceria se se ajustasse em todas as sessões iBGP um keepalive de 5 e um hold de 15?**
Os timers por default de keepalive e hold por default são longos, pois hold timers muito curtos podem levar a sessões de BGP desconetadas. Isto acontece se pacotes BGP forem buffered por mais tempo que esperado ou se o router estiver demasiado ocupado para gerar mensagens keep alive em tempos muito curtos.

d) **Qual o ajuste da configuração necessária nos routers que correm iBGP para permitir que, se em qualquer router falhar qualquer uma das suas interfaces, as mensagens iBGP possam continuar a chegar a esse router desde que exista pelo menos uma rota para ele.**
O ajuste seria configurar uma interface de loopback , enquanto o dispositivo estiver a operar a interface de loopback estará sempre ligada. Caso se use uma interface física a sessão iBGP irá se ligar/desligar conforme a interface se ligue/desligue.

3 - Políticas de eBGP, entre o ISP e os seus clientes

a) Indique como configuraria o acesso do ISP ao Cliente 2 para usar eBGP. Não configure

- Configurar BGP nos routers da topologia
- Definir o router ID para os diferentes routers utilizando endereço de loopback para atribuir uma identificação ao router no BGP.
- Indicar os vizinhos do router através do comando “neighbor remote as” indicando os endereços de loopback de cada um e a que AS pertencem
- A vizinhança deve ser criada utilizando o endereço do loopback (neighbor <endereço IPv4> update-source lo0).

b) Qual a rota usada para o tráfego entre o AS do Cliente 4 e do Cliente 3?
Na figura a seguir, podes ver qual a rota que o pc do cliente 4 efetua, através do comando “trace”

```
PC301_1> trace 40.0.0.1 -m 15 -P 6
trace to 40.0.0.1, 15 hops max (TCP), press Ctrl+C to stop
 1   194.14.57.251   6.379 ms  9.169 ms  9.492 ms
 2   30.1.254.133   31.385 ms  30.113 ms  29.397 ms
 3   40.0.0.1   40.075 ms  41.053 ms  39.322 ms
```

Figura 11 - trace efetuado

c) Todas as rotas seguidas pelo tráfego nas questões das alíneas anteriores cumprem as restrições impostas inicialmente sobre o tráfego entre AS, tiers, etc?
A restrição de não poder ser enviado tráfego para um AS privado , e a restrição dos AS não serem de tráfego para outros clientes estão a ser cumpridas.

d) Num ISP real qual seria o problema de existir um número elevado de ligações entre o ISP e outros AS? Reveja as configurações e verifique se estão de acordo com as políticas requeridas na Introdução. Altere se necessário.
O problema de existir um número elevado de ligações entre o ISP e outros AS, seria, como num contexto real um ISP teria que se ligar a um número muito elevado de AS, iria provocar que houvesse ume excesso da memória possível dos routers do ISP, devido a um número muito elevado de entradas na tabela BGP, e iria demorar muito tempo a encaminhar informação.

Nas configurações configuraram-se os routers do cliente para aceitarem um **máximo de 50 prefixos**, foi realizado com o seguinte comando: maximum-prefix.

```
R301_1(config)#router bgp 301
R301_1(config-router)#neighbor 30.1.212.2 maximum-prefix 50
```

```
router bgp 65005
 no synchronization
 bgp log-neighbor-changes
 network 60.0.26.0 mask 255.255.254.0
 neighbor 10.1.29.1 remote-as 302
 neighbor 10.1.29.3 remote-as 302
 no auto-summary
!
```

Figura 12 - Configurações de routers de AS clientes

4 – Route Refletor

Para tornar a gestão do iBGP mais escalável e menos consumidor de recursos, optou-se por implementar um Route-Reflector no P4. Explorámos então o comando “neighbor address route-reflector-client”. Tivemos em conta que a sessão de iBGP entre o PE1 e PE4 não utiliza o Route-Reflector.

Explicando um pouco mais acerca deste novo conceito, Route-Reflector, esta é uma técnica que quebra a regra de que o iBGP não anuncia/ensina rotas aprendidas por iBGP, tornando mais escalável o iBGP e a sua gestão mais simples. Usa-se o comando “route-reflector-client” para configurar o router local como refletor de rotas e o vizinho especificado como um dos seus clientes. Todos os vizinhos configuras neste comando serão membros do grupo de clientes e os demais peers BGP serão membros do grupo “não cliente” do refletor de rotas local.

Para o route-refletor, efetuamos os comandos que se podem ver na figura abaixo:

```
router bgp 302
 no synchronization
 bgp log-neighbor-changes
 neighbor rrc peer-group
 neighbor rrc remote-as 302
 neighbor rrc update-source Loopback0
 neighbor rrc route-reflector-client
 neighbor 10.0.255.1 peer-group rrc
 neighbor 10.0.255.2 peer-group rrc
 neighbor 10.0.255.3 peer-group rrc
 neighbor 10.0.255.5 peer-group rrc
 neighbor 10.0.255.6 peer-group rrc
 neighbor 30.1.255.1 peer-group rrc
 neighbor 30.1.255.2 peer-group rrc
 neighbor 30.1.255.3 peer-group rrc
 neighbor 30.1.255.4 peer-group rrc
 neighbor 30.1.255.5 peer-group rrc
 neighbor 30.1.255.6 peer-group rrc
 neighbor 30.3.255.7 peer-group rrc
 no auto-summary
```

Figura 13 - implementação do Route-Refletor no router P4

Para o route-refletor client, efetuamos os comandos que podem ser vistos abaixo:

```
router bgp 302
 no synchronization
 bgp log-neighbor-changes
 network 30.0.0.0 mask 255.252.0.0
 network 60.0.0.0 mask 255.255.224.0
 neighbor 10.0.255.4 remote-as 302
 neighbor 10.0.255.4 update-source Loopback0
 neighbor 10.0.255.4 next-hop-self
 no auto-summary
```

Figura 14 implementação do Route-Refletor client

Para comprovar o correto funcionamento, usamos o comando “sh bgp” no router P4, para verificar os endereços BGG que são recebidos, e “sh ip route” para verificar que os endereços configurados como BGP constam das tabelas de routing

```
P4#  sh bgp
BGP table version is 10, local router ID is 10.0.255.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
r i30.0.0.0/14      30.1.255.4               1    100      0 i
r i                 30.1.255.5               1    100      0 i
r i                 10.0.255.2               1    100      0 i
r>i                 30.1.255.6               0    100      0 i
r i                 10.0.255.3               1    100      0 i
r i                 10.0.255.1               1    100      0 i
r i                 10.0.255.6               1    100      0 i
r i                 30.1.255.2               1    100      0 i
r>i40.0.0.0/22      30.1.255.2               1    100      0 303 i
r i60.0.0.0/19      30.1.255.4               1    100      0 i
r i                 30.1.255.5               1    100      0 i
r i                 10.0.255.2               1    100      0 i
r>i                 30.1.255.6               0    100      0 i
r i                 10.0.255.3               1    100      0 i
r i                 10.0.255.1               1    100      0 i
r i                 10.0.255.6               1    100      0 i
r i                 30.1.255.2               1    100      0 i
* i60.0.26.0/23     30.1.255.4               0    100      0 65005 i
*>i                 30.1.255.5               0    100      0 65005 i
r>i194.14.56.0/22   30.1.255.6               0    100      0 301 i
r i                 30.1.255.2               0    100      0 301 i
```

Figura 15 - tabelas BGP router P4

Foi também feito um ping múltiplo, para verificar o correto funcionamento destes routes, vendo assim se todos os endereços configurados neste AS são “pingados” com sucesso.

```
PE6(tcl)#foreach address {
+>10.1.20.1
+>20.202.141.2
+>10.1.22.1
+>10.0.241.2
+>10.1.25.2
+>10.0.26.2
+>10.0.35.2
+>10.1.36.2
+>30.1.212.2
+>10.1.44.1
+>} {ping $address repeat 4 size 1500}

Type escape sequence to abort.
Sending 4, 1500-byte ICMP Echos to 10.1.20.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (4/4), round-trip min/avg/max = 80/84/88 ms
Type escape sequence to abort.
Sending 4, 1500-byte ICMP Echos to 20.202.141.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (4/4), round-trip min/avg/max = 52/60/64 ms
Type escape sequence to abort.
Sending 4, 1500-byte ICMP Echos to 10.1.22.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (4/4), round-trip min/avg/max = 64/85/108 ms
Type escape sequence to abort.
Sending 4, 1500-byte ICMP Echos to 10.0.241.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (4/4), round-trip min/avg/max = 48/58/68 ms
Type escape sequence to abort.
Sending 4, 1500-byte ICMP Echos to 10.1.25.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (4/4), round-trip min/avg/max = 16/36/68 ms
Type escape sequence to abort.
Sending 4, 1500-byte ICMP Echos to 10.0.26.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (4/4), round-trip min/avg/max = 16/20/24 ms
Type escape sequence to abort.
Sending 4, 1500-byte ICMP Echos to 10.0.35.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (4/4), round-trip min/avg/max = 12/41/60 ms
Type escape sequence to abort.
Sending 4, 1500-byte ICMP Echos to 10.1.36.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (4/4), round-trip min/avg/max = 16/19/24 ms
Type escape sequence to abort.
Sending 4, 1500-byte ICMP Echos to 30.1.212.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (4/4), round-trip min/avg/max = 1/1/1 ms
Type escape sequence to abort.
Sending 4, 1500-byte ICMP Echos to 10.1.44.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (4/4), round-trip min/avg/max = 16/18/20 ms
```

Figura 16 ping múltiplo, no router PE6

Fase 4

1 - Ligações eBGP de trânsito e peering do ISP

Nesta fase foram implementas relações de peering entre os AS.

a) **Implemente o peering com os filtros que considerar necessários entre o AS 302 e o AS 303 através do IXP.**
Foram estabelecidas ligações de peer entre o AS302 e o AS303 usando IXP. Não foram usados filtros adicionais para estabelecer a relação de peering.

b) **Dado o AS 301 ser um cliente de longa data do ISP, existe uma relação de peering do ISP com este, uma direta e outra via IXP. Implemente este peering tendo em consideração que o ISP propaga as redes do AS 301 para os seus routers internos.**

Foi estabelecido peering entre o AS 301 e o A303 pelo IXP e pelos routers R301_1 e PE6.

```
router bgp 301
no synchronization
bgp log-neighbor-changes
network 194.14.56.0 mask 255.255.252.0
neighbor 30.1.212.2 remote-as 302
neighbor 30.1.212.2 weight 40000
neighbor 30.1.254.132 remote-as 302
neighbor 30.1.254.132 weight 32800
neighbor 30.1.254.133 remote-as 303
no auto-summary
```

Figura 17- Neighbors R301_1

c) **Reconfigure as ligações entre o AS 202 e AS 302. As redes de interligação mantiveram-se, mas é necessário eliminar o routing estático, se existir, e criar duas sessões BGP.**

Foi criada duas sessões BGP entre o AS 302 e o AS 202. Para tal foram usados os routers R201_1, R202_3 e PE3.

```
router bgp 302
 bgp log-neighbor-changes
 neighbor 20.202.132.1 remote-as 202
 neighbor 20.202.141.1 remote-as 202
 neighbor 30.1.255.1 remote-as 302
 neighbor 30.1.255.1 update-source Loopback0
 neighbor 30.1.255.2 remote-as 302
 neighbor 30.1.255.2 update-source Loopback0
 neighbor 30.1.255.4 remote-as 302
 neighbor 30.1.255.4 update-source Loopback0
 neighbor 30.1.255.5 remote-as 302
 neighbor 30.1.255.5 update-source Loopback0
 neighbor 30.1.255.6 remote-as 302
 neighbor 30.1.255.6 update-source Loopback0
 !
```

Figura 18-Neighbors PE3

Nesta etapa foram implementadas diversas medidas, para proteção do ISP e dos seus clientes, como por exemplo, garantir que não entram pacotes no seu AS com um endereço IP de origem pertencente ao seu bloco IP.

2 - Políticas de segurança do ISP relativas aos AS dos tiers superiores

Nesta etapa foram implementadas diversas medidas, para proteção do ISP e dos seus clientes, como por exemplo, garantir que não entram pacotes no seu AS com um endereço IP de origem pertencente ao seu bloco IP.

AS não deve servir de AS de trânsito aos AS do *tier* acima ou do mesmo *tier*, exceto se for seu cliente / Um AS que não seja de trânsito só deve anunciar as redes que possui e as redes dos seus clientes (os AS a que fornece trânsito).

Um AS serve de AS de trânsito quando este permite tráfego de trânsito, tráfego que não se inicia ou termina em si mesmo.
Foi necessário impedir que que um AS servisse de AS de trânsito aos AS do *tier* acima, exceto no caso de ser seu cliente. De modo a impedir os AS de servirem de AS de trânsito iremos configurar os AS de forma a recusarem a passagem de tráfego de trânsito, não anunciado rotas diferentes das suas.
Recorremos ao uso de **No-Export Community**, iremos configurar os routers de forma aos prefixos não desejados de outros routers sejam marcados com no-export community. Isto permite que prefixos de outros routers sejam conhecidos dentro do AS, mas não sejam anunciados para outros routers.
Foi criado um **route-map** denominado NO-EXPORT, os route-map permitem verificar certas condições, e se estas condições forem cumpridas atribuir um certo valor. Foi também criada uma community no-export de forma que, os vizinhos que não queremos que informação seja exportada, sejam marcados com no-export community.

```
R202_3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R202_3(config)#route-map NO-EXPORT permit 10
R202_3(config-route-map)#set community no-export
R202_3(config-route-map)#router bgp 202
R202_3(config-router)#neighbor 20.202.141.2 route-map NO-EXPORT out
R202_3(config-router)#
```

Figura 19 - Exemplo da configuração da no-export community no router R_202_3.

```
address-family ipv4
 neighbor 11.102.7.1 activate
 neighbor 11.102.7.1 prefix-list MATCH in
 neighbor 11.202.255.251 activate
 neighbor 11.202.255.251 next-hop-self
 neighbor 11.202.255.252 activate
 neighbor 11.202.255.252 next-hop-self
 neighbor 20.202.141.2 activate
 neighbor 20.202.141.2 route-map NO-EXPORT out
 neighbor 20.202.142.2 activate
 no auto-summary
 no synchronization
 network 20.202.0.0 mask 255.255.0.0
exit-address-family
!
```

Figura 20 - Route-map configurado no R_202_3 de modo a impedir tráfego do router PE3.

Este procedimento foi elaborado para o router R_201_1 e R_202_3.

Um AS não deve anunciar as redes de um peer aos AS do tier acima ou do mesmo tier, mas com os quais não haja peering. Evitaram assim servir de AS de trânsito entre os AS do tier acima ou do mesmo tier.

Semelhantemente ao realizado anteriormente, de modo a impedir um AS de anunciar redes, redes que não possui foi usado no-Export Community.

Remover os AS privados, não os anunciar.

Em ordem a múltiplos AS poderem interagir, cada um necessita de ter um identificador único, números de sistemas autónomos (ASN) podem ser públicos ou privados. ASN públicos são necessários para sistemas autónomos poderem trocar informação pela internet, um ASN privado pode ser usado se um AS estiver a comunicar apenas com um único fornecedor via BGP.
Na topologia da rede, o único AS privado é o AS 65005 (cliente 3), a gama de endereços privados é (64512 – 65535).
De forma a remover os AS privados é necessário utilizar o comando: **remove-private-as.** Este comando irá remover números de AS privados do AS PATH.

```
address-family ipv4
 neighbor 20.202.132.1 activate
 neighbor 20.202.132.1 remove-private-as
 neighbor 20.202.141.1 activate
 neighbor 20.202.141.1 remove-private-as
 neighbor 30.1.255.1 activate
 neighbor 30.1.255.1 next-hop-self
 neighbor 30.1.255.2 activate
 neighbor 30.1.255.2 next-hop-self
 neighbor 30.1.255.4 activate
 neighbor 30.1.255.4 next-hop-self
 neighbor 30.1.255.5 activate
 neighbor 30.1.255.5 next-hop-self
 neighbor 30.1.255.6 activate
 neighbor 30.1.255.6 next-hop-self
 default-information originate
 no auto-summary
 no synchronization
 network 30.0.0.0 mask 255.252.0.0
 network 60.0.0.0 mask 255.255.224.0
exit-address-family
!
```

Figura 21 - Remover AS privados no PE3

No router PE3, PE6, PE1, foi usado o remove-private-as em relação aos seus vizinhos do AS, de forma a remover o número destes AS do seu AS PATH.

Garantir que não entram pacotes no seu AS com um endereço IP de origem pertencente ao seu bloco IP.

De modo a garantir que não encontram pacotes no AS com um endereço IP de origem pertencente ao seu bloco IP, recorreu-se ao uso de prefix-list. Criou-se uma prefix-list denominada denyInside que faz “deny” de prefixos com endereço IP de origem pertencente ao seu bloco IP, para impedir que estes entrem no AS.

```
Enter configuration commands, one per line.  End with CNTL/Z.
R101_1(config)#route-map denyInside
R101_1(config-route-map)#match ip address prefix-list MATCH
R101_1(config-route-map)#exit
R101_1(config)#ip prefix-list MATCH deny 4.4.4.4/32
R101_1(config)#ip prefix-list MATCH deny 11.101.0.0/21
R101_1(config)#router bgp 101
R101_1(config-router)#neighbor 11.101.2.2 route-map denyInside in
R101_1(config-router)#neighbor 11.101.4.2 router-map denyInside in
R101_1(config-router)#neighbor 11.101.4.2 route-map denyInside in
R101_1(config-router)#exit
R101_1(config)#exit
R101_1#
```

Figura 22 - Configuração da prefixe-list no R_101_1

Como se pode observar no seguinte exemplo, no router R_101_1, é criado uma prefix-list que impede a entrada do prefixo 11.101.0.0/21, que é o prefixo com endereço IP de origem pertencente ao seu bloco IP.

```
ip prefix-list MATCH seq 5 deny 11.101.0.0/21
ip prefix-list MATCH seq 10 permit 0.0.0.0/0 le 24
no cdp log mismatch duplex
```

Figura 23 - permit 0.0.0.0/0 le 24

De seguida é necessário realizar um **permit 0.0.0.0/0 le 24** para permitir os outros prefixos com *length* menor ou igual a 24.
Este procedimento foi elaborado para os diversos routers pertencentes às tiers superiores.

Autentificação entre peers BGP / anti spoffing

Foi configurada autenticação MD5 entre peers BGP das tiers superiores, para cada segmento enviado na conexão TCP ser verificado. A autentificação tem que ser configurada com a mesma password em ambos os peers BGP.

Foram configuradas passwords iguais nos routers R_101_1, R_102_2, R_201_1, R_202_2

```
R101_1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R101_1(config)#router bgp 101
R101_1(config-router)#neighbor 11.101.2.2 password ri
R101_1(config-router)#neighbor 11.101.4.2 password ri
R101_1(config-router)#^Z
R101_1#w
*Feb 19 20:39:29.959: %SYS-5-CONFIG_I: Configured from console by console
```

Figura 24 - Configuração das passwords dos neighbors BGP no R_101_1.

```
router bgp 101
 no synchronization
 bgp log-neighbor-changes
 network 4.4.4.4 mask 255.255.255.255
 network 11.101.0.0 mask 255.255.248.0
 neighbor 11.101.2.2 remote-as 102
 neighbor 11.101.2.2 password ri
 neighbor 11.101.2.2 prefix-list MATCH in
 neighbor 11.101.4.2 remote-as 201
 neighbor 11.101.4.2 password ri
 neighbor 11.101.4.2 prefix-list MATCH in
 no auto-summary
```

Figura 25 - Neighbors BGP com passwords configuradas, no R_101_1.

Pings realizados nesta fase:

```
PC101_1> ping 40.0.0.1
84 bytes from 40.0.0.1 icmp_seq=1 ttl=56 time=113.806 ms
84 bytes from 40.0.0.1 icmp_seq=2 ttl=56 time=95.081 ms
84 bytes from 40.0.0.1 icmp_seq=3 ttl=56 time=91.134 ms
84 bytes from 40.0.0.1 icmp_seq=4 ttl=56 time=112.642 ms
84 bytes from 40.0.0.1 icmp_seq=5 ttl=56 time=118.541 ms

PC101_1>
```

Figura 26 - ping do pc 101_1 pra pc 303_1

```
PC302_3> ping 60.0.31.129
84 bytes from 60.0.31.129 icmp_seq=1 ttl=60 time=76.304 ms
84 bytes from 60.0.31.129 icmp_seq=2 ttl=60 time=70.497 ms
84 bytes from 60.0.31.129 icmp_seq=3 ttl=60 time=80.323 ms
84 bytes from 60.0.31.129 icmp_seq=4 ttl=60 time=75.123 ms
84 bytes from 60.0.31.129 icmp_seq=5 ttl=60 time=86.021 ms
```

Figura 27 - ping do pc 302_3 pra pc302_2

```
PC301_1> ping 11.101.1.1
84 bytes from 11.101.1.1 icmp_seq=1 ttl=61 time=102.702 ms
84 bytes from 11.101.1.1 icmp_seq=2 ttl=61 time=113.941 ms
84 bytes from 11.101.1.1 icmp_seq=3 ttl=61 time=114.027 ms
84 bytes from 11.101.1.1 icmp_seq=4 ttl=61 time=115.545 ms
84 bytes from 11.101.1.1 icmp_seq=5 ttl=61 time=111.155 ms
```

Figura 28 - ping do pc 301_1 pra pc 101_1

Como se pode observar, as ligações continuam a funcionar.

3 - Políticas de tráfego de saída do ISP

Nesta etapa foram elaboradas um conjunto de políticas de forma a influenciar o tráfego de saída do ISP.

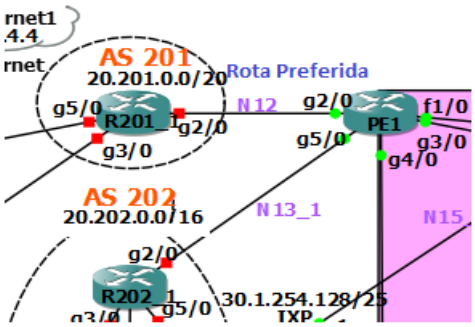
O tráfego para o "Resto do Mundo" e para os AS do tier 1 na topologia deve sair preferencialmente pelo AS 201.

Tráfego para AS do tier 1 tem que sair pelo AS 201. Inicialmente de forma ao tráfego de saída ser feito preferivelmente pelo router PE1, foi aumentado o seu valor de local preference.

```
router bgp 302
 bgp default local-preference 600
```

Figura 29 - local preference de PE1

De seguida de forma a ser preferido o R_201_1 em relação ao R_202_2 foi atribuído um valor maior para o WEIGHT no AS 201, em relação ao AS 202.




```
1   194.14.57.251   9.031 ms  9.288 ms  9.331 ms
2   30.1.254.132   31.258 ms  30.686 ms  32.266 ms
3   10.1.22.2   53.543 ms  54.163 ms  54.453 ms
4   10.1.25.2   65.510 ms  64.686 ms  64.310 ms
5   10.1.23.1   86.983 ms  86.105 ms  74.948 ms
6   10.1.17.1   97.068 ms  98.124 ms  98.139 ms
7   20.201.12.1   108.649 ms  108.039 ms  108.122 ms
8   11.101.4.1   129.963 ms  129.342 ms  130.871 ms
9     *11.101.1.1   147.083 ms  151.890 ms
```

Figura 30 - trace PC_301_1 para AS 301

Ao realizar um trace do PC_301_1 para o AS 301, pode-se observar que o tráfego de saída para a internet está a passar pelo router PE1 e pelo AS 201.

Tráfego para o AS 202 deve sair preferencialmente pela PE1(R202_1), se esta ligação falhar pelo PE3 para o R202_1 e, se ambas falharem via R202_3.

Nas configurações anteriores, o tráfego já passa preferencialmente pela PE1, de forma a priorizar o router R_202_1 em relação ao R_202_3 configurou-se o peso do R_202_1 como maior do que o R_202_3.

```
PE3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE3(config)#router bgp 302
PE3(config-router)#neighbor  20.202.132.1 weight 500
```

Figura 31 - configuração do atributo WEIGHT, com valor de 500

Deve procurar garantir que o tráfego é simétrico.

O tráfego deve ser simétrico, ou seja, as rotas de saída devem ser semelhantes às rotas de entrada. Foram realizadas as seguintes configurações no router R_301_1:

```
R301_1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R301_1(config)#router bgp 301
R301_1(config-router)#neighbor 30.1.254.132 weight 32800
```

Figura 32 - configuração do atributo WEIGHT, com valor de 32800

Foram realizados testes de forma a verificar a simetria do tráfego.

```
PC303_1> trace 30.1.43.1 -m 15 -P 6
trace to 30.1.43.1, 15 hops max (TCP), press Ctrl+C to stop
 1   40.0.0.252   3.294 ms  10.557 ms  9.293 ms
 2   30.1.254.132   32.267 ms  30.306 ms  31.739 ms
 3   10.1.22.2   52.477 ms  52.489 ms  52.253 ms
 4   10.1.25.2   75.171 ms  74.270 ms  74.252 ms
 5   10.1.28.2   95.127 ms  95.711 ms  95.574 ms
 6   30.1.43.1   108.105 ms  109.307 ms  109.127 ms

PC303_1>
```

```
PC302_1> trace 40.0.0.1 -m 15 -P 6
trace to 40.0.0.1, 15 hops max (TCP), press Ctrl+C to stop
 1   30.1.43.254   9.367 ms  9.170 ms  8.273 ms
 2   10.1.28.1   32.472 ms  30.556 ms  31.328 ms
 3   10.1.25.1   52.889 ms  50.537 ms  54.746 ms
 4   10.1.22.1   63.249 ms  52.035 ms  53.154 ms
 5   30.1.254.133   76.496 ms  75.873 ms  75.079 ms
 6   40.0.0.1   87.734 ms  87.068 ms  86.050 ms
```

Figura 33 - Trace do tráfego do cliente 4 para AS 303, e vice-versa

No trace do tráfego do cliente 4 para AS 303, e vice-versa, como se pode observar, tráfego é simétrico.

```
PC101_1> trace 40.0.0.1 -m 15 -P 6
trace to 40.0.0.1, 15 hops max (TCP), press Ctrl+C to stop
 1   11.101.1.251   2.513 ms  9.275 ms  9.217 ms
 2   11.101.4.2   32.123 ms  30.280 ms  30.868 ms
 3   20.201.12.2   41.310 ms  41.251 ms  42.163 ms
 4   10.1.17.2   53.690 ms  52.025 ms  50.397 ms
 5   10.1.23.2   64.203 ms  62.233 ms  63.414 ms
 6   10.1.25.1   75.101 ms  74.089 ms  75.270 ms
 7   10.1.22.1   96.932 ms  140.810 ms  140.218 ms
 8   30.1.254.133   159.729 ms  159.905 ms  158.777 ms
 9   40.0.0.1   169.688 ms  169.949 ms  160.753 ms
```

```
PC303_1> trace 11.101.1.1 -m 15 -P 6
trace to 11.101.1.1, 15 hops max (TCP), press Ctrl+C to stop
 1   40.0.0.252   7.039 ms  9.324 ms  9.426 ms
 2   30.1.254.132   32.447 ms  32.411 ms  32.376 ms
 3   10.1.22.2   54.341 ms  54.267 ms  54.308 ms
 4   10.1.25.2   74.761 ms  75.200 ms  73.726 ms
 5   10.1.23.1   96.558 ms  94.384 ms  96.306 ms
 6   10.1.17.1   106.035 ms  108.243 ms  107.010 ms
 7   20.201.12.1   130.608 ms  130.453 ms  129.795 ms
 8   11.101.4.1   141.942 ms  142.116 ms  140.384 ms
 9   11.101.1.1   129.928 ms  128.960 ms  131.014 ms

PC303_1>
```

Figura 34 - trace do tráfego do AS 301 para AS 101, e vice-versa

No trace do tráfego do AS 301 para AS 101, e vice-versa, como se pode observar, tráfego é simétrico.

Tráfego para os AS do mesmo tier o tráfego deve sair preferencialmente por ligações diretas e, quando estas não existam, via IXP como seria o caso de AS do mesmo tier que não tivessem ligações diretas.

O caminho entre o R301_1 deve ser preferencialmente R_301_1 para PE6 , em relação a , R_301_1 para R_303_2, de modo a preferenciar ligação direta.

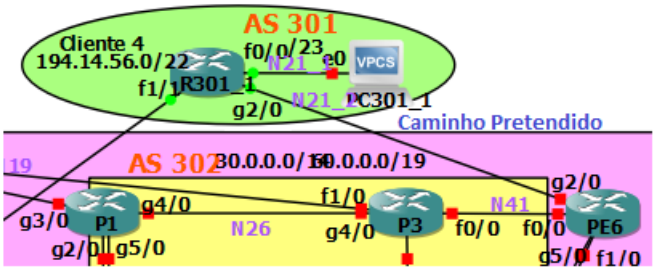


Figura 35 - caminho pretendido para esta etapa

Então foram realizados os seguintes comandos no r_301_1:

```
R301_1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R301_1(config)#router bgp 301
R301_1(config-router)#neighbor 30.1.254.132 weight 32800
```

Figura 36 – Mudança do weight do neighbor 30.1.254.132

Foi feito um trace do AS 301 para o AS 303, de forma a averiguar se está a funcionar bem.

```
PC301_1> trace 40.0.0.1 -m 15 -P 6
trace to 40.0.0.1, 15 hops max (TCP), press Ctrl+C to stop
 1   194.14.57.251   11.183 ms  9.331 ms  8.446 ms
 2   30.1.212.2   30.292 ms  31.312 ms  20.686 ms
 3   10.1.38.1   52.236 ms  52.080 ms  53.150 ms
 4   10.1.28.1   74.206 ms  75.282 ms  74.392 ms
 5   10.1.25.1   63.105 ms  72.886 ms  75.589 ms
 6   10.1.22.1   73.341 ms  73.621 ms  73.453 ms
 7   30.1.254.133   83.978 ms  85.162 ms  85.181 ms
 8   40.0.0.1   94.323 ms  95.978 ms  96.040 ms

PC301_1>
```

Figura 37 - trace do AS 301 para o AS 303

Tráfego está a passar pelo PE6.

a) Poder-se-ia realizar agregação de endereços IPv4 nesta topologia de maneira a tornar as tabelas de routing menores?

Pode-se agregar endereços, mas podia causar possíveis problemas, pois ia ter muitas redes pertencentes ao mesmo sítios.

Pings realizados nesta fase:

```
PC101_1> ping 40.0.0.1
84 bytes from 40.0.0.1 icmp_seq=1 ttl=56 time=113.806 ms
84 bytes from 40.0.0.1 icmp_seq=2 ttl=56 time=95.081 ms
84 bytes from 40.0.0.1 icmp_seq=3 ttl=56 time=91.134 ms
84 bytes from 40.0.0.1 icmp_seq=4 ttl=56 time=112.642 ms
84 bytes from 40.0.0.1 icmp_seq=5 ttl=56 time=118.541 ms

PC101_1>
```

Figura 38 – ping do pc 101_1 pra pc 303_1

```
PC302_3> ping 60.0.31.129
84 bytes from 60.0.31.129 icmp_seq=1 ttl=60 time=76.304 ms
84 bytes from 60.0.31.129 icmp_seq=2 ttl=60 time=70.497 ms
84 bytes from 60.0.31.129 icmp_seq=3 ttl=60 time=80.323 ms
84 bytes from 60.0.31.129 icmp_seq=4 ttl=60 time=75.123 ms
84 bytes from 60.0.31.129 icmp_seq=5 ttl=60 time=86.021 ms
```

Figura 39 - ping do pc 302_3 pra pc302_2

```
PC301_1> ping 11.101.1.1
84 bytes from 11.101.1.1 icmp_seq=1 ttl=61 time=102.702 ms
84 bytes from 11.101.1.1 icmp_seq=2 ttl=61 time=113.941 ms
84 bytes from 11.101.1.1 icmp_seq=3 ttl=61 time=114.027 ms
84 bytes from 11.101.1.1 icmp_seq=4 ttl=61 time=115.545 ms
84 bytes from 11.101.1.1 icmp_seq=5 ttl=61 time=111.155 ms
```

Figura 40 - ping do pc 301_1 pra pc 101_1

Fase 5

1 - Rotas internas no ISP

a) **Se a rede N41 (P3/PE6) passar a gigabit Ethernet (pode apenas baixar o custo com ip ospf cost n) a rota entre o router PE1 e o PE6 será alterada face à atual?**
Se a rede N41 (P3/PE6) passar a gigabit Ethernet a rota entre o router PE1 e o PE6 será alterada. Caso seja escolhido um custo mais baixo, o OSPF ira preferir a rota com o custo mais baixo.

b) **O que acontece se do R101_1 se fizer um Ping ao PE6 e não existir o default-information originate nos PEn?**
Este comando permite propagar uma rota default no OSPF. Caso este comando não esteja em algum dos comandos, o default-information originate nos PEn as rotas default no OSPF não são advertised, então o ping não tem sucesso.

c) **Do P4 consegue realizar um Ping a um router exterior do AS?**
Não é possível realizar um ping do P4 a um router exterior, pois não possui nenhuma rota para o "resto do mundo" pois foi utilizado o comando "default-information originate always", que permite criar uma rota default, que por sua vez, é passada ao P4 em vez da tabela de routing completa.

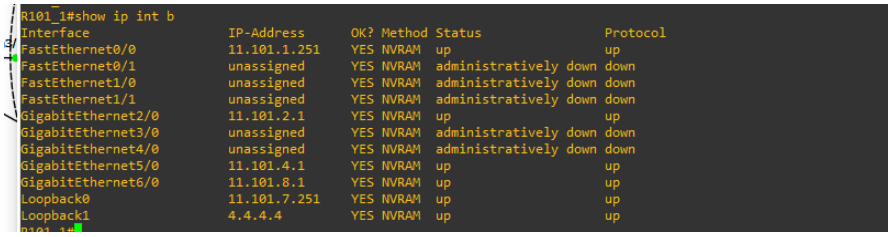
d) **Sendo o ISP um AS de trânsito como evitar ter de realizar redistribuição de todas as rotas do BGP no OSPF para que, por exemplo, os routers P conheçam as redes externas e saibam encaminhar o tráfego de pacotes IP para elas?1**
Visto que, como os routers em BGP estão a propagar as suas rotas, o IGP esta desativado. Para evitar que estas rotas sejam redistribuídas no OSPF, é necessário ligar o IGP, através do comando "**bgp redistribute-internal**", permitindo aplicar restrições na redistribuição das rotas iBGP.

e) **O comando default-information originate é necessário no OSPF nos routers PE 1 e 3?**
Sim, ao usar este comando nos routers PE1 e PE3, no OSPF, ele não propaga as suas rotas, até ser criada uma rota "default", e constar da tabela de routing destes dois routers. Caso existisse a rota por defeito, era adicionada a palavra "always", dizendo aos routers para propagar a rota "default" para os outros routers, mesmo não tendo a rota "default" na tabela de routing.

f) **Os routers que correm iBGP, com exceção do PE1 e 3, não conhecem as redes de interligação do PE1 e do PE3 para os outros AS, não constam nas suas tabelas de routing. Como é que os routers internos conseguem colocar nas suas tabelas de routing as rotas anunciadas pelo BGP?**
Usando o comando "network", associando o endereço, e criar uma rota estática que ira colocar esses endereços nos routers internos que correm BGP. No entanto, este comando não garante que a network colocado no router é adicionado com sucesso, visto que o BGP ignora este comando. O BGP apenas propaga essa rota por BGP se constar na tabela de routing desse router. Para ter a garantia que colocamos esta network, adicionamos no final do comando "null0". Assim, quando criarmos uma rota estática, ele recebe tráfego por qualquer endereço IP.

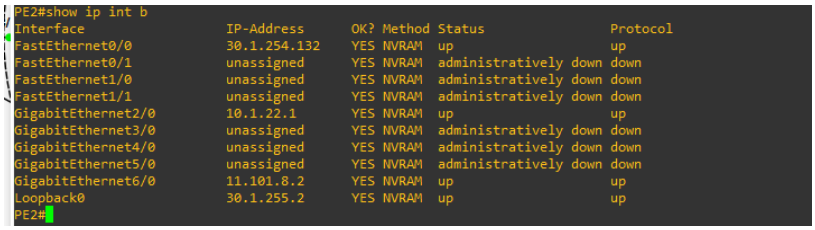
2- Nova saída de tráfego internacional

Para efetuar este ponto foi preciso fazer uma ligação entre os routers R101_1 e PE2. Usou-se a interface g0/6 para fazer a ligação. Atribui-se os seguintes endereços às interfaces.



```
R101_1#show ip int b
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            11.101.1.251    YES NVRAM  up                    up
FastEthernet0/1            unassigned      YES NVRAM  administratively down down
FastEthernet1/0            unassigned      YES NVRAM  administratively down down
FastEthernet1/1            unassigned      YES NVRAM  administratively down down
GigabitEthernet2/0         11.101.2.1      YES NVRAM  up                    up
GigabitEthernet3/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet4/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet5/0         11.101.4.1      YES NVRAM  up                    up
GigabitEthernet6/0         11.101.8.1      YES NVRAM  up                    up
Loopback0                  11.101.7.251    YES NVRAM  up                    up
Loopback1                  4.4.4.4         YES NVRAM  up                    up
```

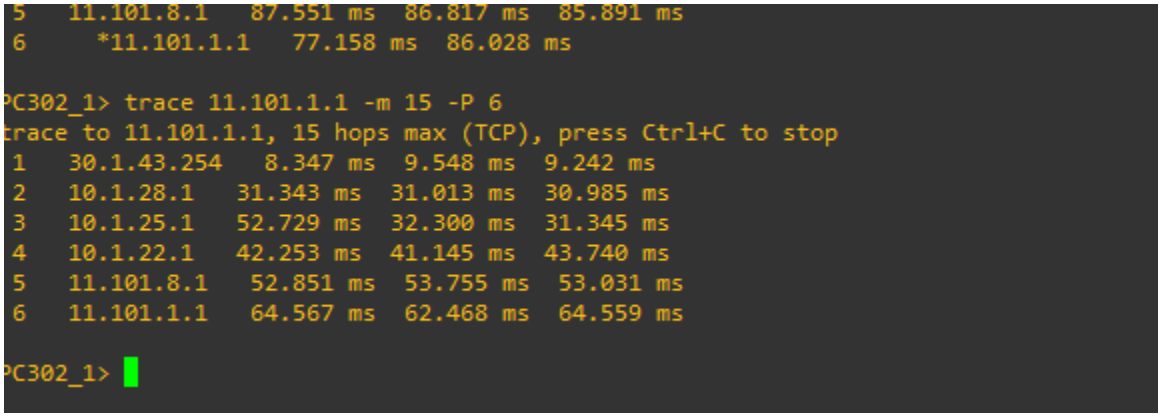
Figura 41-Interface Router 101_1



```
PE2#show ip int b
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            30.1.254.132    YES NVRAM  up                    up
FastEthernet0/1            unassigned      YES NVRAM  administratively down down
FastEthernet1/0            unassigned      YES NVRAM  administratively down down
FastEthernet1/1            unassigned      YES NVRAM  administratively down down
GigabitEthernet2/0         10.1.22.1       YES NVRAM  up                    up
GigabitEthernet3/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet4/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet5/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet6/0         11.101.8.2      YES NVRAM  up                    up
Loopback0                  30.1.255.2      YES NVRAM  up                    up
PE2#
```

Figura 42-Interface Router PE2

Após atribuídos os endereços foi feito um route-map de modo a alterar o local preference para preferir esta rota para verificar que a ligação estava a funcionar. Por fim feito um trace entre o PC 302_1 e o PC 101_1 e apagou-se o route-map.



```
5   11.101.8.1   87.551 ms  86.817 ms  85.891 ms
6     *11.101.1.1   77.158 ms  86.028 ms

PC302_1> trace 11.101.1.1 -m 15 -P 6
trace to 11.101.1.1, 15 hops max (TCP), press Ctrl+C to stop
1   30.1.43.254   8.347 ms  9.548 ms  9.242 ms
2   10.1.28.1   31.343 ms  31.013 ms  30.985 ms
3   10.1.25.1   52.729 ms  32.300 ms  31.345 ms
4   10.1.22.1   42.253 ms  41.145 ms  43.740 ms
5   11.101.8.1   52.851 ms  53.755 ms  53.031 ms
6   11.101.1.1   64.567 ms  62.468 ms  64.559 ms

PC302_1>
```

Figura 43-Ping entre PC 302_1 e PC 101_1

5 - Engenharia de tráfego usando Policy Based Routing (PBR)

a) Sem qualquer mudança na configuração, qual é o caminho utilizado?

De modo a observar todos os saltos do caminho, sem qualquer mudança nas configurações, efetuámos um traceroute desde o PC301_1 ao PC65005_1.

```
PC301_1> trace 60.0.26.1 -m 15 -P 6
trace to 60.0.26.1, 15 hops max (TCP), press Ctrl+C to stop
 1   194.14.57.251   2.494 ms  8.253 ms  10.407 ms
 2   30.1.212.2   30.400 ms  30.744 ms  30.442 ms
 3   10.1.38.1   53.083 ms  53.305 ms  53.059 ms
 4   10.1.29.4   74.048 ms  74.976 ms  62.956 ms
 5   60.0.26.1   75.789 ms  85.371 ms  83.072 ms

PC301_1>
```

Figura 44 - Traceroute deste o Cliente4, sem configurações

b) Execute as configurações para executar o pretendido. Indique quais são as rotas utilizadas.

Antes de passar para a configuração do PBR, foi necessário efetuar algumas alterações no AS65005. Em ambos os routers foram adicionados as seguintes instruções, permitindo que o cliente 4 consiga efetuar o ping para este AS.

```
router bgp 65005
 no synchronization
 bgp log-neighbor-changes
 network 60.0.26.0 mask 255.255.254.0
 neighbor 10.1.29.1 remote-as 302
 neighbor 10.1.29.3 remote-as 302
 neighbor 60.0.27.252 remote-as 65005
```

Figura 45 - endereço 60.0.27.252 adicionado ao router deste As

```
router ospf 3
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute bgp 65005 subnets
 passive-interface default
 no passive-interface FastEthernet1/1
 network 10.0.0.0 0.255.255.255 area 0
 network 60.0.26.0 0.0.1.255 area 0
```

Figura 46 - adicionado o comando "no passive-interface"

As políticas de tráfego (PBR – Policy Based Routing) são técnicas que se usam para fazer decisões de roteamento pelo administrador da rede. Quando um router recebe um pacote, normalmente decide o próximo salto com base no IP de destino, procurando uma entrada na tabela de roteamento. No caso das políticas, pretende-se um “match” com alguma condição e decide-se o próximo salto com base neste match. Portanto, há uma escolha seletiva dos pacotes a redirecionar, e para caminhos diferentes. As várias condições podem ter a ver com o tamanho dos pacotes, o endereço de origem, entre outros…

Usam-se listas de filtros de prefixos às rotas importadas ou exportadas (entradas e saídas), havendo um número máximo de prefixos. A alteração aos atributos destas rotas faz-se através de um “set” e estas alterações podem ser aplicadas condicionalmente “match”.

```
PE6#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE6(config)#ip access-list extended pbr
PE6(config-ext-nacl)# permit ip 194.14.56.0 0.0.3.255 60.0.26.0 0.0.1.255
PE6(config-ext-nacl)#end
PE6#
PE6#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE6(config)#route-map pbr permit 10
PE6(config-route-map)# match ip address pbr
PE6(config-route-map)# set ip next-hop 10.1.38.1
PE6(config-route-map)#end
PE6#
PE6#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE6(config)#interface GigabitEthernet5/0
PE6(config-if)# ip policy route-map pbr
PE6(config-if)#end
```

Figura 47 - configuração do PBR no PE6

Conclusões

Para terminar, pensamos ter cumprido com sucesso a maioria dos objetivos deste trabalho. Ficámos familiarizados com o mundo dos protocolos routing internos (RIP, OSPF…), conexões entre peers eBGP, peers iBGP, quais as especificações para haver ligações ISP, ou seja, acesso à Internet, entre vários outros tópicos. Revemos e implementámos várias condições para importação e exportação de rotas – atributos BGP, outros métodos (prepeending, comunidades…). Nesta mesma medida, aplicámos listas de prefixos, de forma a garantir que regras de entrada/saída fossem aplicadas apenas a rotas cujo IP se inserisse nessas listas…

Contudo este foi um projeto bastante complexo, contendo vários passos intermédios, e neste relatório pensamos ter varrido todas as decisões tomadas, ou pelo menos aquelas que considerámos mais relevantes para cumprir todas as especificações. Completámos a configuração dos endereços IP aos novos links da topologia, modificámos algumas coisas nos diferentes AS, e nos respetivos tiers, ativámos iBGP no ISP e o acesso dos Clientes 1, 2 e 3, ativámos o Route-Reflector, para otimizar as ligações iBGP e a gestão de recursose, por fim, configurámos o eBGP de toda a topologia, sem filtros. Garantimos a concretização das Políticas de Tráfego de Upstream do ISP, igualmente, através de filtros com listas de prefixos.

Fazendo um balanço do nosso próprio trabalho, pensamos ter conseguido atingir a maioria dos requisitos, tendo comprovado a implementação das políticas e as várias condições de entrada e saída nas AS, de acordo as especificações do enunciado, e compreender todos os conteúdos lecionados durante o semestre relacionados ao tema.

Bibliografia

https://www.cisco.com/c/en/us/support/docs/ip/ip-routed-protocols/14956-route-to-null-interface.html

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13759-37.html

https://books.google.pt/books?id=-IcgbmFG4_UC&pg=PA107&lpg=PA107&dq=isp+peer+group&source=bl&ots=NiG0C_Mbir&sig=ACfU3U2rF8eT0lQEDyo8MV-mkTemqKPJVA&hl=pt-PT&sa=X&ved=2ahUKEwiM9PLE7q3nAhUN-hQKHWgzBdIQ6AEwCnoECAoQAQ#v=onepage&q=isp%20peer%20group&f=false

https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/bgp/set-local-preference.html

https://community.cisco.com/t5/networking-documents/how-to-configure-pbr/ta-p/3122774

https://community.cisco.com/t5/switching/access-list-for-policy-based-routing-for-2nd-gateway/td-p/3179531

https://www.noction.com/blog/bgp-med-attribute

https://ipcisco.com/lesson/bgp-weight-attribute/

https://networklessons.com/bgp/how-to-configure-bgp-weight-attribute

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13759-37.html#exampleone

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/command/irg-cr-book/bgp-n1.html

https://en.wikipedia.org/wiki/Policy-based_routing

Anexo

Link download do projeto, com todas as configurações:

https://iselpt-my.sharepoint.com/:u:/g/personal/a45125_alunos_isel_pt/EYot5lOpGFVImcq5ubUH1TEBcf3_oIGHmNU7kl4IA5XN2Q?e=0ISWH6