

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**

[Introdução e Objetivos 5](#_Toc64838132)

[Fase 1 6](#_Toc64838133)

[Fase 2 7](#_Toc64838134)

[Fase 3 12](#_Toc64838135)

[Fase 4 21](#_Toc64838136)

[Fase 5 31](#_Toc64838137)

[Conclusões 35](#_Toc64838138)

[Bibliografia 36](#_Toc64838139)

[Anexo 37](#_Toc64838140)

**Índice de Figuras**

[Figura 1 - ping múltiplo 8](#_Toc64838144)

[Figura 2 - tabela de routing RC2\_1 9](file:///C:\Users\luisc\Desktop\RI_TP3_GRUPO7.docx#_Toc64838145)

[Figura 3 - configuração RIP 9](file:///C:\Users\luisc\Desktop\RI_TP3_GRUPO7.docx#_Toc64838146)

[Figura 4 - ping múltiplo 10](#_Toc64838147)

[Figura 5 - trace para o endereço da Internet 13](#_Toc64838148)

[Figura 6 - trace para o endereço 11.102.3.252 13](#_Toc64838149)

[Figura 7 - rota escolhida quando efetuado o comando trace 13](#_Toc64838150)

[Figura 8 - trace entre R\_201\_1 e R\_202\_3 14](#_Toc64838151)

[Figura 9 - Configurações do R\_202\_3 15](#_Toc64838152)

[Figura 10 – Timers BGP 16](file:///C:\Users\luisc\Desktop\RI_TP3_GRUPO7.docx#_Toc64838153)

[Figura 11 - trace efetuado 17](file:///C:\Users\luisc\Desktop\RI_TP3_GRUPO7.docx#_Toc64838154)

[Figura 12 - Configurações de routers de AS clientes 17](#_Toc64838155)

[Figura 13 - implementação do Route-Refletor no router P4 18](#_Toc64838156)

[Figura 14 implementação do Route-Refletor client 18](#_Toc64838157)

[Figura 15 - tabelas BGP router P4 19](#_Toc64838158)

[Figura 16 ping múltiplo, no router PE6 20](#_Toc64838159)

[Figura 17- Neighbors R301\_1 21](file:///C:\Users\luisc\Desktop\RI_TP3_GRUPO7.docx#_Toc64838160)

[Figura 18-Neighbors PE3 21](file:///C:\Users\luisc\Desktop\RI_TP3_GRUPO7.docx#_Toc64838161)

[Figura 19 - Exemplo da configuração da no-export community no router R\_202\_3. 22](#_Toc64838162)

[Figura 20 - Route-map configurado no R\_202\_3 de modo a impedir tráfego do router PE3. 22](#_Toc64838163)

[Figura 21 - Remover AS privados no PE3 23](#_Toc64838164)

[Figura 22 - Configuração da prefixe-list no R\_101\_1 24](#_Toc64838165)

[Figura 23 - permit 0.0.0.0/0 le 24 24](#_Toc64838166)

[Figura 24 - Configuração das passwords dos neighbors BGP no R\_101\_1. 25](#_Toc64838167)

[Figura 25 - Neighbors BGP com passwords configuradas, no R\_101\_1. 25](#_Toc64838168)

[Figura 26 - ping do pc 101\_1 pra pc 303\_1 26](#_Toc64838169)

[Figura 27 - ping do pc 302\_3 pra pc302\_2 26](#_Toc64838170)

[Figura 28 - ping do pc 301\_1 pra pc 101\_1 26](#_Toc64838171)

[Figura 29 - local preference de PE1 27](#_Toc64838172)

[Figura 30 - trace PC\_301\_1 para AS 301 27](#_Toc64838173)

[Figura 31 - configuração do atributo WEIGHT, com valor de 500 27](#_Toc64838174)

[Figura 32 - configuração do atributo WEIGHT, com valor de 32800 28](#_Toc64838175)

[Figura 33 - Trace do tráfego do cliente 4 para AS 303, e vice-versa 28](#_Toc64838176)

[Figura 34 - trace do tráfego do AS 301 para AS 101, e vice-versa 28](#_Toc64838177)

[Figura 35 - caminho pretendido para esta etapa 29](#_Toc64838178)

[Figura 36 – Mudança do weight do neighbor 30.1.254.132 29](#_Toc64838179)

[Figura 37 - trace do AS 301 para o AS 303 29](#_Toc64838180)

[Figura 38 – ping do pc 101\_1 pra pc 303\_1 30](#_Toc64838181)

[Figura 39 - ping do pc 302\_3 pra pc302\_2 30](#_Toc64838182)

[Figura 40 - ping do pc 301\_1 pra pc 101\_1 30](#_Toc64838183)

[Figura 41-Interface Router 101\_1 32](file:///C:\Users\luisc\Desktop\RI_TP3_GRUPO7.docx#_Toc64838184)

[Figura 42-Interface Router PE2 32](file:///C:\Users\luisc\Desktop\RI_TP3_GRUPO7.docx#_Toc64838185)

[Figura 43-Ping entre PC 302\_1 e PC 101\_1 32](file:///C:\Users\luisc\Desktop\RI_TP3_GRUPO7.docx#_Toc64838186)

[Figura 44 - Traceroute deste o Cliente4, sem configurações 33](#_Toc64838187)

[Figura 45 - endereço 60.0.27.252 adicionado ao router deste As 33](#_Toc64838188)

[Figura 46 - adicionado o comando "no passive-interface" 33](#_Toc64838189)

[Figura 47 - configuração do PBR no PE6 34](#_Toc64838190)

# 

# 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

1. **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.

1. **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.

1. **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.

1. **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:

* 1. Suporta de vários dispositivos NAT
  2. Aumento da segurança das informações em computadores individuais.

Desvantagens de usar endereços privados:

1. 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:

1. Mais complexa;
2. Exige constante manutenção e conservação;

# Fase 2

**1 – Configuração do protocolo OSPF**

1. **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.

1. **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.

1. **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;

1. **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;

1. **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.

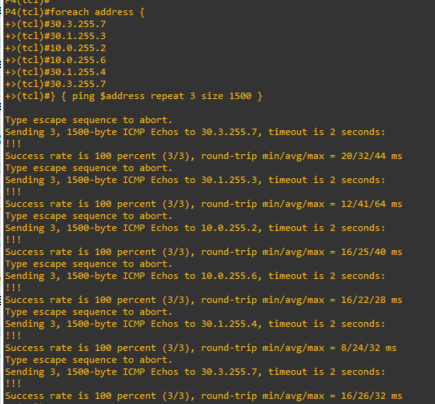


Figura 1 - ping múltiplo

**3 – Configuração do protocolo RIPv2**

1. **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.

1. **Poderia ser usado RIPv1 no cliente 2?**

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

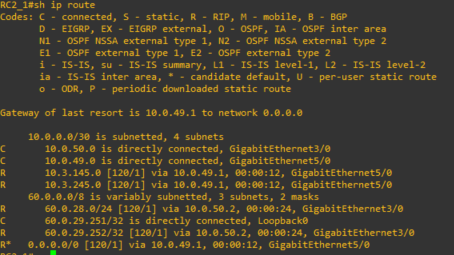


Figura 2 - tabela de routing RC2\_1

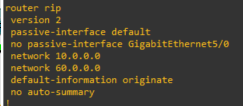


Figura 3 - configuração RIP

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

1. **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.

1. **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.

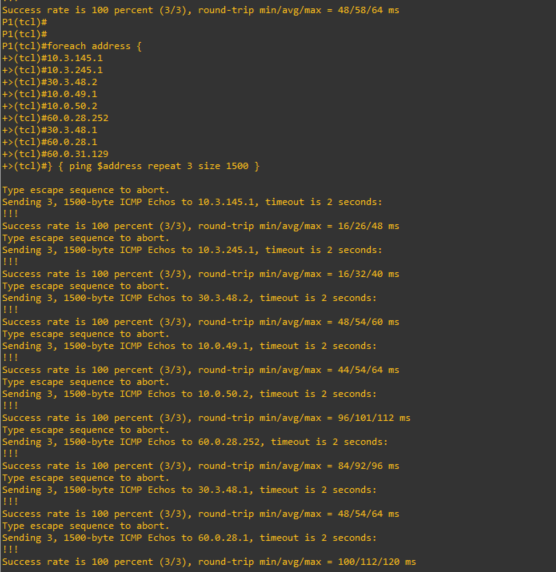


Figura 4 - ping múltiplo

1. **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.

1. **A rede N48 poderia ser uma rede com endereços IP privados?**

Não, visto que assim, o cliente 1 não conseguia ligar-se à Internet.

1. **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.

1. **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.

1. **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.

1. **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.

1. **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**

1. **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).

1. **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.

1. **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.

1. **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.

1. **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.

1. **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.

1. **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.

1. **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.

1. **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

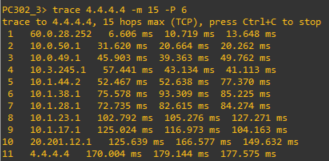


Figura 5 - trace para o endereço da Internet

1. **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)

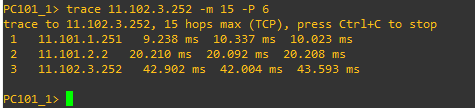


Figura 6 - trace para o endereço 11.102.3.252

1. **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.



Figura 7 - rota escolhida quando efetuado o comando trace

1. **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

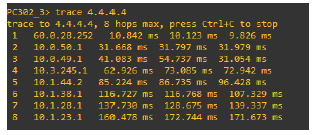


Figura 8 - trace entre R\_201\_1 e R\_202\_3

1. **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.

1. **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.

1. **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.

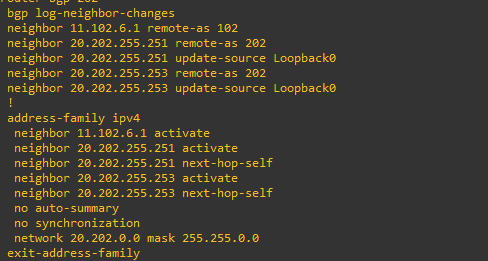


Figura 9 - Configurações do R\_202\_3

1. **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.

1. **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**

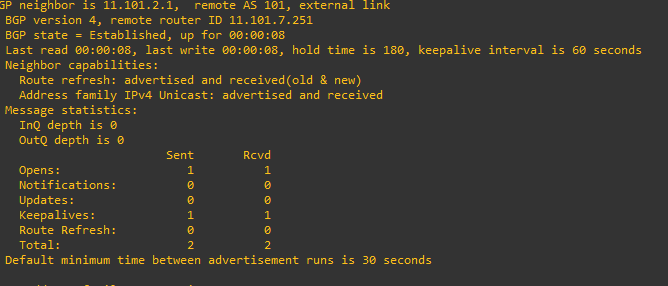
1. **Sem filtros ativos numa sessão BGP, qual o comportamento por default do Cisco IOS relativamente a anunciar/receber rotas? Quais os problemas que o comportamento por default pode causar?**

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

1. **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.

Figura 10 – Timers BGP



1. **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.

1. **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**

1. **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).

1. **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”

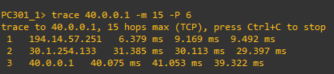


Figura 11 - trace efetuado

1. **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.

1. **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.



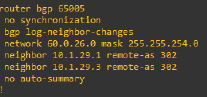
****

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:

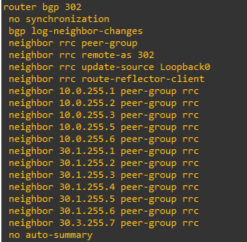


Figura 13 - implementação do Route-Refletor no router P4

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

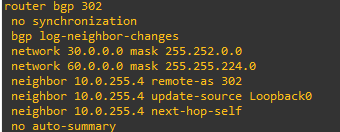


Figura 14 implementação do Route-Refletor client

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

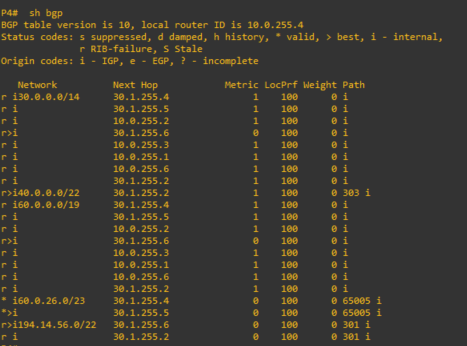


Figura 15 - tabelas BGP router P4

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.

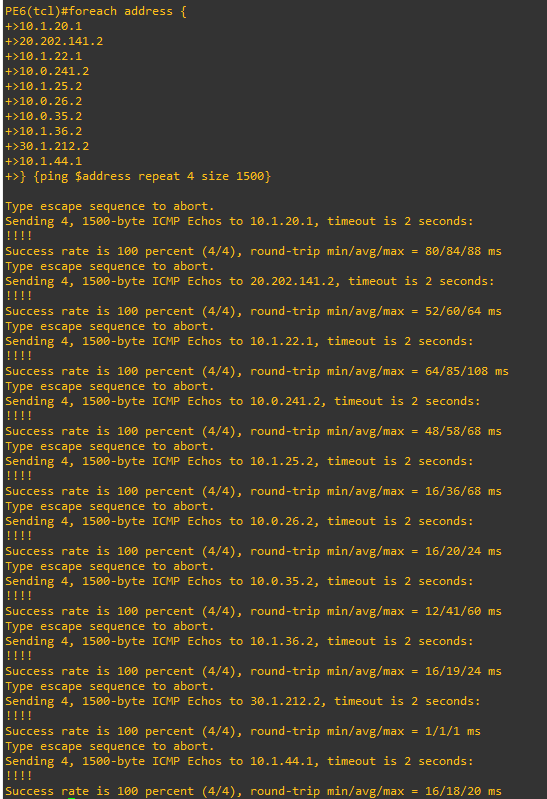


Figura 16 ping múltiplo, no router PE6

# Fase 4

**1 - Ligações eBGP de trânsito e peering do ISP**

Nesta fase foram implementas relações de peering entre os AS.

1. **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.

1. **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.

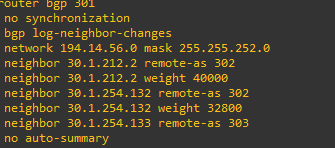


Figura 17- Neighbors R301\_1

1. **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.

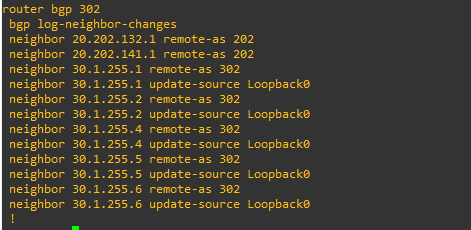


Figura 18-Neighbors PE3

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.

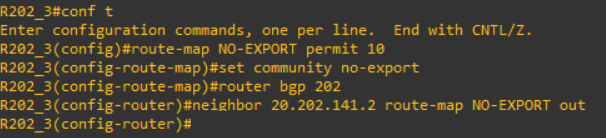


Figura 19 - Exemplo da configuração da no-export community no router R\_202\_3.

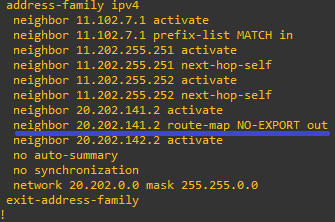


Figura 20 - Route-map configurado no R\_202\_3 de modo a impedir tráfego do router PE3.

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.

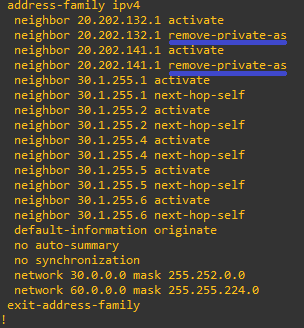


Figura 21 - Remover AS privados no PE3

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.

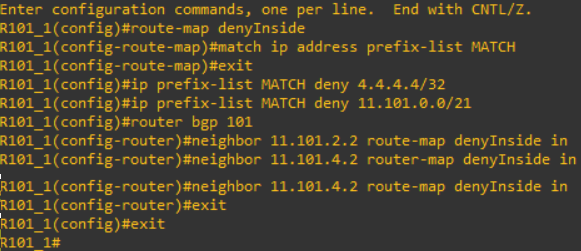
****

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.



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

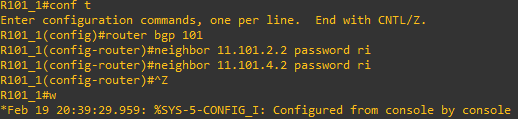


Figura 24 - Configuração das passwords dos neighbors BGP no R\_101\_1.

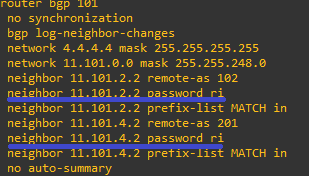


Figura 25 - Neighbors BGP com passwords configuradas, no R\_101\_1.

**Pings realizados nesta fase:**

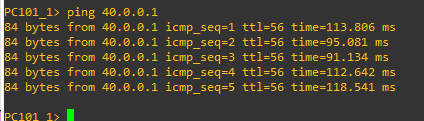


Figura 26 - ping do pc 101\_1 pra pc 303\_1

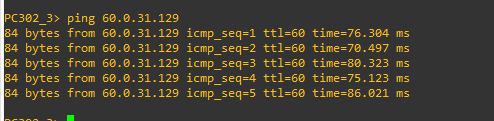


Figura 27 - ping do pc 302\_3 pra pc302\_2

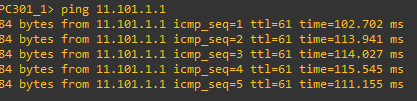


Figura 28 - ping do pc 301\_1 pra pc 101\_1

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.



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.

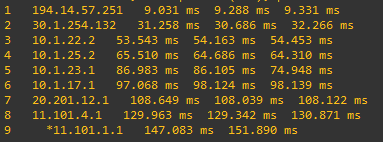
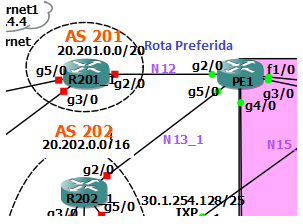


Figura 30 - trace PC\_301\_1 para AS 301

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.

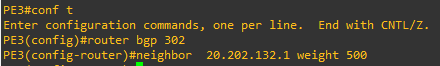


Figura 31 - configuração do atributo WEIGHT, com valor de 500

**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:

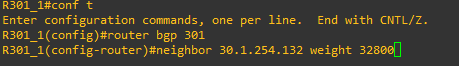
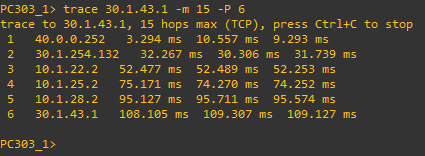


Figura 32 - configuração do atributo WEIGHT, com valor de 32800

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



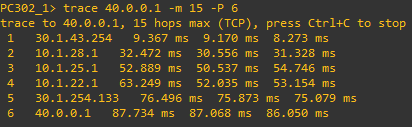
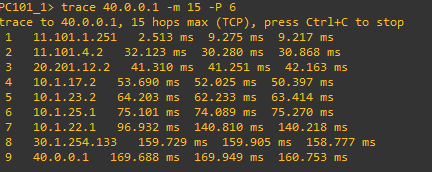


Figura 33 - Trace do tráfego do cliente 4 para AS 303, e vice-versa

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



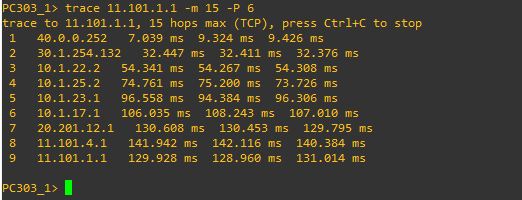


Figura 34 - trace do tráfego do AS 301 para AS 101, e vice-versa

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.

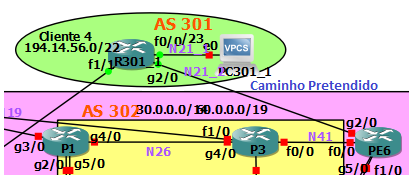
****

Figura 35 - caminho pretendido para esta etapa

Então foram realizados os seguintes comandos no r\_301\_1:

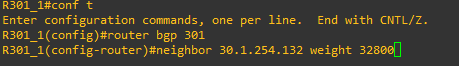


Figura 36 – Mudança do weight do neighbor 30.1.254.132

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

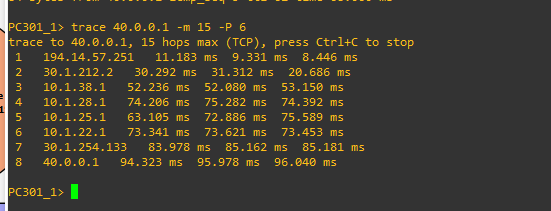


Figura 37 - trace do AS 301 para o AS 303

Tráfego está a passar pelo PE6.

1. **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:**

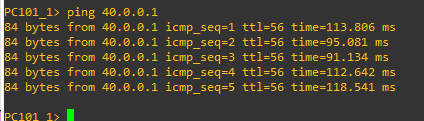


Figura 38 – ping do pc 101\_1 pra pc 303\_1

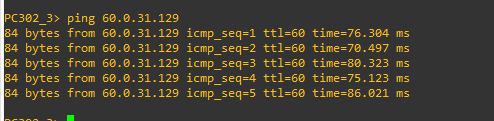


Figura 39 - ping do pc 302\_3 pra pc302\_2

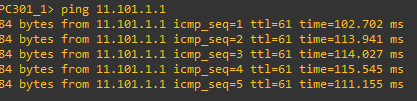


Figura 40 - ping do pc 301\_1 pra pc 101\_1

# Fase 5

**1 - Rotas internas no ISP**

1. **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.

1. **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.

1. **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.

1. **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.

1. **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.

1. **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.

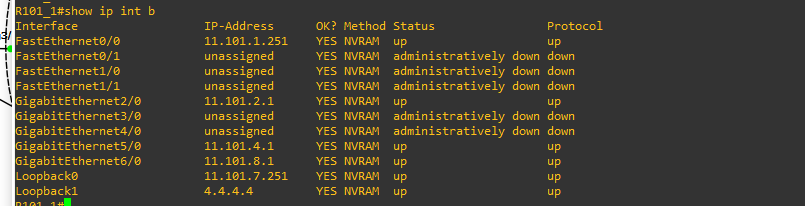


Figura 41-Interface Router 101\_1

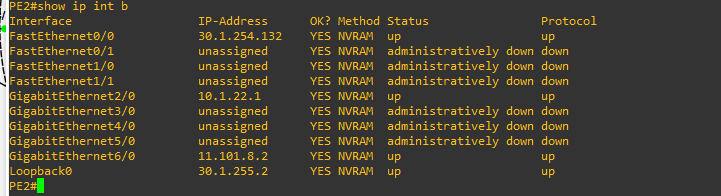


Figura 42-Interface Router PE2

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.

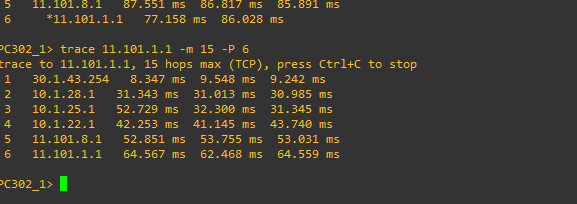


Figura 43-Ping entre PC 302\_1 e PC 101\_1

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

1. **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.

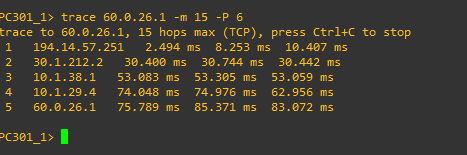


Figura 44 - Traceroute deste o Cliente4, sem configurações

1. **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.

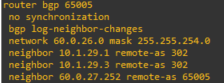


Figura 45 - endereço 60.0.27.252 adicionado ao router deste As

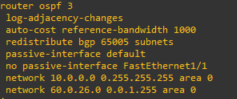
****

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”.

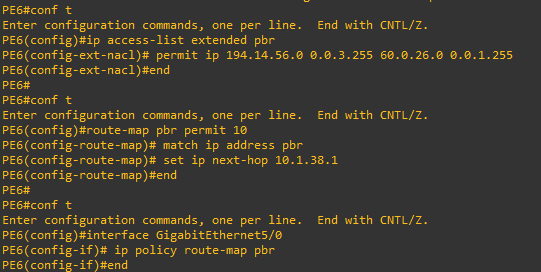


Figura 47 - configuração do PBR no PE6

# 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=-IcqbmFG4_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>