Instituto Politécnico de Lisboa (IPL)

Instituto Superior de Engenharia de Lisboa (ISEL)

Área Departamental de Engenharia da
Eletrónica e Telecomunicações e de Computadores(ADEETC)
LEETC, LEIC, LEIM, LEIRT, MEIC

Redes de Internet (RI) – Trabalho nº 3 (BGP)

Inverno de 2020/2021- Data limite de entrega: Ver Moodle

Este trabalho tem como objetivo o aprofundamento dos conhecimentos sobre o protocolo de encaminhamento BGP e de técnicas de *Policy Based Routing* (PBR).

As 5 fases do trabalho tem um peso de cerca de 15, 15, 30, 20 e 20% respetivamente na nota final deste.

O trabalho prático é de execução por grupos de até 3 alunos, podendo na(s) aula(s) prática(s) de realização do trabalho, ou parte, existir avaliação do grupo e/ou individual sobre a realização do mesmo e o tema que envolve.

Este trabalho, tal como os seguintes, é considerado pedagogicamente fundamental ("NORMAS DE AVALIAÇAO DE CONHECIMENTOS", Conselho Pedagógico do ISEL, ponto 2.3.1).

É assumido que os alunos sabem utilizar convenientemente os comandos de configuração dos equipamentos, incluindo os de *show* e *debug*, para validar o seu trabalho e resolver os desafios que lhes vão aparecendo.

O docente decidirá conforme os relatórios entregues e as notas individuais se fará, e com que grupos fará, a discussão final dos trabalhos.

Recomenda-se o uso do GNS3, pode, no entanto, ser usado outro simulador, o PT não inclui as capacidades suficientes. O apoio ao desenvolvimento do trabalho, em caso de dúvidas, será apenas prestado usando o GNS3.

O relatório deve incluir na identificação, para além da identificação do grupo e dos alunos, os respetivos nomes e o curso. Deve incluir a justificação das escolhas efetuadas e, em anexo, os ficheiros de configuração dos *routers* nas várias fases do trabalho. Deve incluir um ***link*** para uma exportação do projeto GNS3 referente ao trabalho completo em GNS3 ("*Export Portable Project*").

Nota: Leiam TODO o enunciado antes de começar a configurar os equipamentos!

Conteúdo

Objetivo

Pretende-se com este trabalho aprofundar conhecimentos praticando com os protocolos RIPv2, OSPFv2, BGPv4 e rotas estáticas.

Existe um Internet Service Provider (ISP) que tem um AS atribuído, o AS 302. Este ISP tem clientes, estando na topologia anexa representados apenas 4 desses clientes típicos, incluindo um que possui o seu próprio AS privado (Cliente 3) e outro que possui um AS público (cliente 4).

Pretende-se que sejam configurados todos os equipamentos presentes na topologia de maneira ao ISP usar a sua rede da forma mais eficiente, tendo em consideração os equipamentos que possui, e a consiga rentabilizar prestando os melhores serviços aos seus atuais clientes assim como aos futuros.

Neste trabalho dever-se-á ter em consideração sobretudo o acesso à Internet sem preocupações com serviços como, por exemplo, redes de distribuição de conteúdos (CDN), etc.

Pretendem-se respostas precisas e concisas, não se pretende que o relatório seja um tratado sobre o que é, por exemplo, o RIPv2, o OSPFv2, etc. Pretende-se sobretudo que responda aos requisitos indicados em cada ponto de cada uma das fases, justificando as opções tomadas na configuração de maneira a serem atingidos os objetivos enunciados.

Introdução

A Internet funciona, também, graças aos protocolos de *routing* que colaboram entre si na camada de rede no controlo do tráfego constituído por pacotes IP. O conhecimento deste tipo de protocolos de *routing* permite no futuro que o estudante possa evoluir para outras tecnologias como, por exemplo, o MPLS (*Multi-Protocol Label Switching*) e o SDN (*Software Defined Networks*).

Pretende-se com este trabalho prático que o estudante aprofunde os conhecimentos dos protocolos de *routing* lecionados na UC: RIPv2, OSPFv2, BGPv4 e rotas estáticas. O trabalho divide-se em várias fases, fases estas que se vão tornando mais complexas e exigindo conhecimentos mais aprofundados conforme se vai avançando.

Para simplificar a tarefa por parte dos estudantes, em simultâneo com a disponibilização do enunciado do trabalho prático é disponibilizado também parte da configuração no GNS3. Apesar de ser disponibilizado um exemplo de uma configuração base, a qual pode ser utilizada para iniciar a realização deste trabalho, esta também pode ser ignorada se for pretendido começar do zero. Se a configuração disponibilizada for utilizada, em parte ou no seu todo, isto não elimina a necessidade da mesma dever ser percebida, testada, alterada, etc, conforme necessário ao objetivo do trabalho.

Em termos de trabalho a efetuar, apesar de ser necessário estudar e perceber este enunciado e a configuração proposta e responder às perguntas incluídas em cada ponto de cada uma das Fases, mais de metade do trabalho de configuração é disponibilizado como proposta de abordagem do mesmo, pelo menos até à Fase 3, ponto 1 (BGP básico).

Apesar do GNS3 não ter problemas com a topologia usada no trabalho, alguns computadores poderão ter características menos adequadas a correr este tipo de software e podem tornar-se mais lentos. De maneira a atenuar o peso do GNS3 no computador sugere-se que não ative sempre todos os *routers* da topologia, mas ative-os e desative-os conforme for avançando no trabalho. Ative-os a todos apenas quando isso for mesmo necessário. A afinação do idle-PC no GNS3 também ajuda a minorar a ocupação do processador.

Não se esqueça de definir o Idle-PC no GNS3 de maneira a não esgotar os recursos todos do seu processador.

Leia todo o enunciado e tente perceber bem o que é pretendido antes de realizar a primeira linha de configuração.

Aconselha-se a que este enunciado seja lido na sua totalidade, percebido e só depois deve iniciar a realização do trabalho pela Fase 1 e só após a conclusão desta fase é que deve passar à Fase 2 e assim sucessivamente. Mais tarde poderá ter de regressar a uma Fase anterior para afinar um ou outro pormenor.

Notas a ler para poupar (mesmo) tempo quando da resolução do trabalho

Nota: Quando um pacote IP é enviado, por exemplo num Ping, o endereço IP de origem que ele leva é o da interface física por onde sai do equipamento de origem. Isto, se for esquecido, pode dar azo a *debug* "demorado" dado que quando o *router* de destino tenta responder ao Ping o endereço IP de origem pode não ser conhecido se, por exemplo, a rede de origem utilizar endereços IP privados. Daí advém que os equipamentos que queremos acessíveis de fora do AS deverem estar em redes com endereços IP públicos. Quando a rede onde um *router* estiver ligado utilizar endereços IP privados, para teste pode-se usar o Ping estendido e forçar como endereço IP de origem o endereço IP do Loopback 0/RouterID do *router* (se este usar um endereço IP público) de onde se enviar o Ping.

Nota: Lembre-se que para aqueles "Ping" ou "Trace" que se arrastam existe sempre a solução do "Control Alt 6" para passar à frente.

Nota: Experimente utilizar um editor de texto tipo Notepad++ para escrever os comandos que posteriormente poderá copiar para os *routers*. Poderá assim utilizar o "copy and paste" de uma forma mais eficaz dado que alguns *routers* poderão ter uma configuração básica semelhante.

Nota: Não se esqueça de ir fazendo uns "write" / "wr" ou "do wr" ou "copy run start" para ir salvando a configuração que vai alterando nos *routers.* Nos PC do GNS3 pode ir usando "Save".

Nota: Clicar no GNS3 em cima de um *router* com o botão da direita do rato e depois na lista que aparece em "Edit config" é uma forma alternativa de poder aceder ao ficheiro de configuração de um *router*, mas … se cometer erros aqui o *router* não o avisa e pode "limpar" todos os comandos que introduzir a seguir. Deve ir sempre via CLI fazer um *show run* confirmar se as eventuais alterações aparecem quando arrancar de novo o *router* (relembra-se que o ficheiro é um *start-config* não é um *running-config*). Isto é uma "batota" que dá jeito ao configurar no GNS3, mas que deve ser bem compreendida e, se usada, deve-o ser com os devidos cuidados. [https://www.n-study.com/en/how-to-use-gns3/edit-startup-config-directly/]

Nota: Uma pergunta que deve fazer após perceber a topologia do trabalho é: Como é que neste AS os *routers* apendem as rotas para todas as redes/*routers*/PC no próprio AS/domínio e nos outros AS/domínios? Via OSPF, BGP, rotas estáticas ou ligações diretas? Será por uma rota por omissão (*default*)? Foi por redistribuição? De que tipo?

Nota: No IOS da Cisco, se uma rota para uma determinada rede não existir numa tabela de *routing* de um *router* a correr BGP, e se este receber uma rota que anuncie um *next hop* nessa rede, ele não irá incluir essa rota na sua tabela de *routing*. O BGP só pode "correr" após o IGP em uso ter atualizado as tabelas de *routing* com as rotas que o BGP vai necessitar.

Nota: A atualização das tabelas do BGP não é realizada imediatamente assim que se introduz um comando via CLI. Uma possibilidade de o conseguir de forma mais rápida é introduzindo via CLI o comando "clear ip bgp *". **Atenção**: Este comando não deve ser usado (ou se usado deve ser com muito cuidado) numa rede em produção (rede real em utilização), dado poder causar longas interrupções de tráfego.

Topologia

A topologia apresentada representa vários sistemas autónomos (AS), em 3 *tiers* [https://www.ctstelecom.com/the-three-tiers-of-isps-what-they-mean-why-theyre-important/], em que o Internet Service Provider (ISP) faz parte do *tier* 3 e possui o AS 302.

O ISP possui 4 clientes. Dois fazendo parte do seu AS, um com AS privado e outro com AS público. Apesar de na topologia o ISP ter apenas 4 clientes, deve ser assumido que o ISP pode ter, ou vir a ter, centenas ou milhares de clientes.

No *tier* 1 temos os AS 101 e 102. No *tier* 2 temos os AS 201 e 202. No *tier* 3 temos os AS 301, 302, 303 e 65005.

Nota: Para efeito de testes/documentação existem alguns números de AS definidos pelo RFC 5398 (*Autonomous System (AS) Number Reservation for Documentation*) e reservados pela IANA. Os a 2 bytes são de 64496 a 64511, existindo também outros a 4 bytes, mas neste trabalho optou-se por números de AS mais fáceis de memorizar, mas que não devem ser usados em redes reais.

Os AS utilizam entre eles o protocolo de *routing* BGPv4.

Todos os AS são geridos por entidades independentes umas das outras. Os gestores de rede de uns não podem influenciar diretamente ("mexer") nas configurações das redes dos outros (há por vezes exceções utilizando as BGP *communities* para influenciar o tráfego do lado do fornecedor do serviço, e disponibilizadas por este, mas não vamos por aí neste trabalho).

Os AS do *tier* 3 utilizam um Internet Exchange Point (IXP) para trocarem tráfego entre eles. O objetivo é tentar evitar usar para isso os AS do *tier* acima aos quais teriam de pagar pelo tráfego que por lá passe.

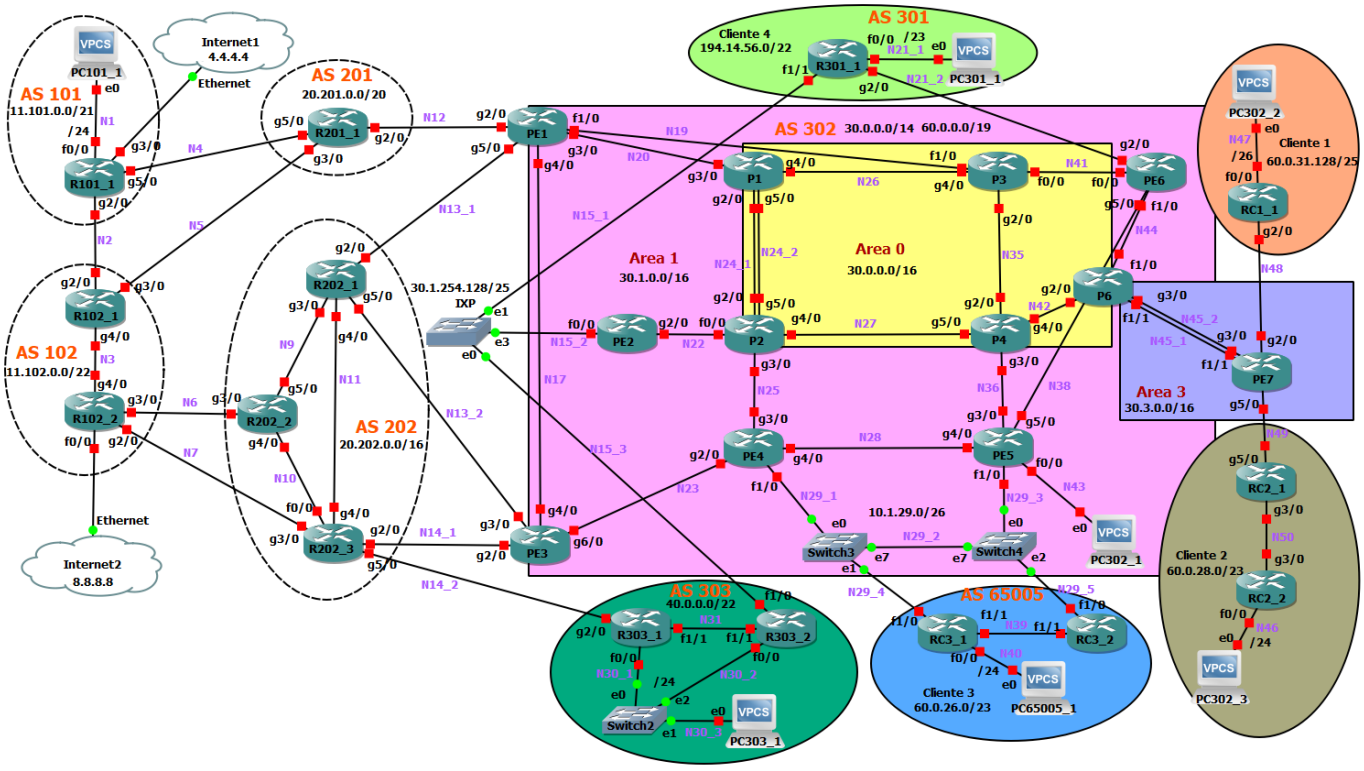
Nota: O equipamento usado como IXP (um *switch* do GNS3) possui interfaces limitadas em termos de débito, mas para o caso em questão é irrelevante. Numa rede real o IXP não deveria constituir uma limitação no débito.

Na topologia da rede do ISP, assim como na dos outros AS, não estão representadas na sua arquitetura todas as camadas *Access*, *Distribution* e *Core*, mas apenas a parte da camada *Core* necessária a este trabalho focado especialmente no BGPv4. Todas a parte referente às camadas de *Access* e de *Distribution* foi praticamente ignorada na topologia para a tornar menos complexa. Excetuam-se alguns PC para simular algumas LAN e tornar possível a realização de alguns testes. Estas LAN têm a dimensão/máscara indicada na topologia no GNS3 e, as da figura, usam a parte mais baixa do bloco de endereços IP atribuído ao Cliente.

Os AS de um *tier* não devem servir de AS de trânsito aos outros AS do mesmo *tier* ou do *tier* acima, exceptua-se o caso do outro AS do mesmo *tier* ser seu cliente. Por exemplo, o AS 201 não deve servir de AS de trânsito para o tráfego entre os AS 101 e 102. O AS 302 pode servir de AS de trânsito ao tráfego do AS 301, dado este ser seu cliente, mas não deve, no entanto, servir de AS de trânsito ao AS 303.

Dois dos clientes do ISP não possuem capacidade técnica, nem necessidade, para usarem BGPv4. Devem ser integrados no AS do ISP, mas com os devidos cuidados em termos dos protocolos de *routing* para não haver interferências por parte dos clientes na rede do ISP. Os gestores de rede dos clientes não devem poder interferir na configuração dos *routers* do operador (ISP).

Quando for necessário usar um IGP deverá ser utilizado o OSPFv2, sendo o Cliente 2 uma exceção dado pretender usar o RIPv2.



Sempre que existir mais do que um caminho possível, devem evitar-se pontos únicos de falha (redundância). Se uma rota falhar, deve passar a usar-se outra rota para o mesmo destino sempre que exista um caminho alternativo.

A ligação da topologia ao "Resto do Mundo" / Internet deve ser simulada através de interfaces tipo *Loopback* a criar nos *routers* onde na topologia se encontram ligadas as "nuvens" Internet0 e Internet1.

Internet Service Provider (ISP)

O ISP é composto por um domínio OSPFv2 (ISP), por um domínio básico/rede (Cliente 1), por um domínio/rede que usa RIPv2 como IGP (Cliente 2). Inclui também como seus clientes o AS 65005 (Cliente 3) e o AS 301 (Cliente 4). O AS 301 é um cliente com um AS público, o qual usa o ISP como AS de trânsito dado não ter dimensão para se ligar diretamente a um fornecedor do *tier* acima.

Apesar de estarem representados na topologia apenas 4 clientes, deve ser assumido que o ISP pode servir centenas ou milhares de clientes com milhares de redes distintas.

Os *routers* do ISP são designados Provider (P) e Provider Edge (PE). Os *routers* P são *routers* internos ao AS, neste caso também internos ao domínio OSPFv2 do ISP, os quais não possuem interfaces para o exterior do domínio. Os *routers* P servem, por exemplo, para interligar locais geograficamente afastados do ISP usando ligações de débito muito elevado. Os *routers* PE, para além de poderem participar no trânsito interno do ISP, possuem interfaces para ligar a clientes e a outros AS, no caso do OSPFv2 são ASBR.

A rede interna do ISP foi projetada de maneira a que os *routers* que se encontram na área 0, e as ligações entre eles, sejam robustas, eficientes e de elevada capacidade. Preferencialmente o tráfego entre os vários locais do ISP deve passar pelos *routers* P na área 0 que devem funcionar como um *backbone* no que se refere ao tráfego interno do ISP.

As áreas 0 e 1 do domínio OSPF do ISP são áreas normais. Quanto à área 3 pretende-se que, de preferência, não tenha de lidar com tabelas de *routing* pesadas em termos do suporte do endereçamento relativo a rotas externas ao domínio OSPF do ISP.

Relações com os clientes:

- As *startups*, representadas pelos Clientes 1 e 2, atingiram um nível de crescimento e maturidades tal que se tornaram independentes. Desta forma os seus *routers* não devem estar no domínio OSPF interno do ISP. Foi realizada a sua separação da rede do ISP e é necessário apoiar a sua migração.
- O Cliente 1 expressou a sua incapacidade técnica e usará *routing* estático.
- O Cliente 2 pretende usar como IGP o RIPv2.
- O Cliente 3 pretende usar BGPv4 como EGP e requereu um AS público. Este **não** lhe foi atribuído dado não ter dimensão suficiente em termos de número de redes internas. Por isso irá migrar para um AS privado, o AS 65005.
- O Cliente 4, por ser um cliente com uma rede mais complexa e com um bloco de endereçamento IP antigo/*legacy* PI, apesar de na topologia apresentada neste trabalho apenas estar presente parte da sua rede, requisitou também um AS, o qual lhe foi atribuído, o AS 301.

Relações de Trânsito/*Peering*:

- Aproveitando o crescente *know-how* dos seus quadros técnicos, o AS 302 criou um *Internet Exchange Point* (IXP) para melhorar a qualidade e rentabilizar melhor o uso da Internet entre os AS no mesmo *tier*, ligados ao IXP, criando relações de *peering* entre eles.
- O AS 201 informou o ISP que, com a ativação do BGP entre ambos, este poderá usufruir de um plano de trânsito mais favorável em relação à concorrência e poderá, inclusivamente, aceder a todas as redes dos seus *Peers* e *Content Deliver Networks* (CDN) de forma gratuita.

Endereçamento

Os endereços IP para as redes de interligação entre *routers*, são normalmente disponibilizados pelo AS que está a fornecer trânsito.

Num ISP real deveriam ser reservados para a parte da rede de *Distribution* e *Access* dos respetivos domínios, que nã aparecem neste trabalho e por isso não serem atribuídos explicitamente, como por exemplo, os endereços IP internos dos AS (servidores Web/DNS/Email/…, *Firewalls*,…, gestão de equipamentos de rede *layer* 2, etc). **Nota:** O endereçamento IP das várias redes e dos equipamentos internos poderia ser algo bem mais complexo na realidade.

De acordo com o RIPE, o qual atribuiu os seguintes blocos IPv4 públicos e AS, e o ISP que decidiu atribuir endereços IP do seu bloco público ao Cliente 3, a distribuição de blocos de endereços IPv4 pelos AS é a seguinte:

- **AS 101:** 11.101.0.0/21
- **AS 102:** 11.102.0.0/22
- **AS 201:** 20.201.0.0/20
- **AS 202:** 20.202.0.0/16
- **AS 301 (Cliente 4):** 194.14.56.0/22
- **AS 302:** 30.0.0.0/14 && 60.0.0.0/19
- **AS 303:** 40.0.0.0/22
- **AS 65005 (Cliente 3):** "Bloco IPv4 a definir pelo gestor de rede do ISP a partir do bloco do seu bloco (AS 302)", um /23

A atribuição de endereços IPv4 públicos em cada AS deve respeitar os blocos de endereços IP atribuídos a cada AS pelo RIPE ou delegados pelo respetivo ISP (caso de alguns clientes). Devem ser usados endereços IPv4 privados onde não forem necessários endereços públicos. Por exemplo, redes internas aos AS podem utilizar nas redes *point-to-point* (PTP) endereços privados.

O ISP optou por utilizar o bloco 30.0.0.0/14 para as suas redes internas e de interligação com os seus clientes. O bloco 60.0.0.0/19 é usado para delegar endereços IP aos seus clientes. Quando bloco 60.0.0.0/19 esgotar, o ISP passará a delegar aos seus clientes endereços IP do bloco 30.0.0.0/14. Conforme for progredindo em número de clientes a

intenção do ISP é aproveitar ambos os blocos de endereçamento. **Nota:** Neste trabalho, para simplificar o *debug*, assumiu-se que existe uma clara separação na finalidade de ambos os blocos.
Os endereços IP que irão servir para *routerID* dos *routers* de fronteira BGP deverão ser únicos e públicos.
Nota: A tabela de endereços incluída em anexo serve de orientação podendo o estudante alterá-la como considerar conveniente, respeitando as regras que diferenciam o uso de endereços públicos de privados.

Os clientes do ISP deverão ter os seguintes endereços públicos disponíveis:

- **Cliente 1, interno ao AS 302: 128 endereços públicos**
- **Cliente 2, interno ao AS 302: 512 endereços públicos**
- **Cliente 3 (AS 65005): 512 endereços públicos,** "Bloco IPv4 a definir pelo gestor de rede do ISP a partir do seu bloco (AS 302)"
- **Cliente 4, AS 301 (**194.14.56.0/22; Nota**:** O cliente já possuía o bloco de endereços IP): **1024 endereços públicos**

Regras de distribuição de endereços IP

Os endereços IPv4 a ser atribuídos devem seguir algum critério. Critério esse com objetivos como possibilitar a agregação de endereços, tornar mais fácil o *debug* se a atribuição de endereços seguir algum critério específico fácil de memorizar, etc. Neste trabalho segue-se em parte o critério de facilitar o *debug*, mas numa rede real podem não existir endereços suficientes para conseguir uma distribuição focada neste objetivo.

Utilizou-se uma política de nomear as redes por ordem crescente, sempre que possível, de cima para baixo e da esquerda para a direita, segundo a topologia da figura. Existem algumas exceções pontuais na regra do endereçamento como, por exemplo, o caso das interfaces dos *routers* que servem de *gateways* nas LAN onde existem outros equipamentos e que receberam quase o maior endereço IP da rede a que estão ligados, e o PC o menor endereço disponível, Se existirem vários *routers* numa rede recebem endereços no fim do bloco atribuído à LAN com ajustes para ajudar a memória, por exemplo se o bloco vai até … .255, o *router* **3** fica com o … .25**3**, o **2** com o 25**2**, etc (auxiliares de memória para ajudar quando do *debug*).

Nota: Podia-se tentar utilizar a regra de endereçamento usada no trabalho prático nº 2, mas nesta topologia os *routers* não são nomeados apenas por ordem numérica (qual seria o mais baixo por exemplo entre o P2 e o PE2?).

Atribuição de endereços IP (as regras aqui referidas não são um imperativo, são apenas regras a serem seguidas quando possível. Podem ser alteradas desde que seja justificada a razão):

ISP

- LAN c/ endereço público: 30.área.<nº rede>.m
- Redes PTP e redes de interligação que usem endereços privados: 10.área.<nº rede>.m

ISP - Clientes

- Clientes internos ao ISP (os que partilham o bloco IPv4 do ISP)
  - 60.0.<varia, sendo os endereços atribuídos a começar na parte de cima do bloco do ISP>.m
  - Numa LAN com DC ou PC, os *routers* possuem dos últimos endereços IP e os DC ou PC o menor disponível.

AS

- Redes PTP e redes de interligação entre AS: N.<nº AS menor>.<nº rede>.m (N depende do bloco IP do AS)
- Redes PTP e redes de interligação que usem endereços privados: 10.<nº AS>.<nº rede>.m

A ligação ao IXP usa endereços IPv4 públicos cedidos pelo AS 302.

Fase 1 – Endereçamento

1 - Atribuição de endereços IPv4

Cada AS tem redes que necessitam de endereços IPv4 públicos, por exemplo onde se situarem servidores de DNS, Web, *email*, etc, outras em que os endereços podem ser privados (redes internas onde o uso de NAT pode permitir poupar endereços IPv4 públicos e continuar a manter comunicação com o resto do mundo). Neste trabalho, para simplificar, devem ser ignoradas as redes internas (LAN), com equipamentos de utilizadores, necessitando de NAT.

Assuma que cada AS é gerido por uma entidade distinta dos outros AS. Os equipamentos de rede de um AS só devem ser acedidos remotamente para gestão a partir de dentro do respetivo AS.

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

Verifique e configure/altere, se necessário, o endereçamento das interfaces dos *routers* e dos restantes equipamentos na topologia. Confirme que não existem blocos de endereços IPv4 sobrepostos podendo vir a causar problemas.

Confirme as configurações em termos do endereçamento efetuado e as ligações diretas entre equipamentos vizinhos através da utilização do Ping e da verificação das respetivas tabelas de *routing*.

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"?

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, pretende-se:

- A verificação da tabela de endereçamento em ficheiro anexo ("TP3 – Endereçamento.xls") com a indicação das alterações a efetuar a esta e a razão das mesmas, se existirem.
- Uma tabela dos endereços IPv4 públicos e privados utilizados e os ainda livres no AS do ISP para poderem ser atribuídos de acordo com os critérios definidos anteriormente, por exemplo a novos clientes.
- Sugestão de uma distribuição mais "poupadinha" em termos dos endereços IPv4 públicos disponíveis inicialmente para o ISP.

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* (talvez voltar a esta questão depois de ter sido realizada a Fase 3 seja melhor).

Fase 2 – OSPFv2, RIPv2, rotas estáticas e redistribuição de rotas

1 – Configuração do protocolo OSPF

Em todos os AS onde na topologia apresentada for necessário usar um IGP deve ser usado o protocolo OSPFv2, exceto onde explicitamente for indicado outro protocolo, como é o caso do uso de RIPv2 no Cliente 2.

O domínio OSPFv2 do ISP deve utilizar 3 áreas OSPF, as indicadas na figura da topologia.

Após a configuração do OSPFv2 nos AS onde for necessário, verificar se nas tabelas de *routing* constam todas as redes dos respetivos domínios ou rotas por omissão se necessárias.

Verificar se entre equipamentos nos mesmos domínios OSPF é possível realizar Ping (**Sugestão**: Use o Ping via TCLSH para simplificar/automatizar os testes (não se esqueça das sugestões dadas no início do enunciado quando alguns dos Ping não tiverem sucesso (tipo de endereços evolvidos)).

Verifique onde faz sentido a eleição de *Designated Routers* (DR). Deve ser evitado que o OSPF os eleja desnecessariamente.

a) Na topologia do trabalho quantos DR devem existir e gerar LSA tipo 2?

Verifique se os custos das rotas OSPFv2 estão a ser calculados corretamente, incluindo se os custos apresentados nas tabelas de *routing* do PE2 e do P6 correspondem ao esperado. Assuma que na topologia em causa o débito mais elevado em qualquer interface é de **10 Gbit/s**. **Nota:** Numa situação real este débito seria baixo para ser assumido como máximo num ISP.

Configure os *routers* da área 3, se possível, para ser possível a utilização de *routers* mais simples, menos onerosos, dado ser assumido que esta área apenas foi criada para poder dar suporte a alguns, poucos, clientes naquela zona.

Como resultado deste ponto pretende-se uma descrição sucinta do que foi feito para atingir os objetivos enunciados acima, o resultado do Ping (estendido se necessário) e a parte da configuração correspondente ao OSPFv2 para atingir os objetivos indicados nos *routers* PE1, e 2, no P1 e no P6 e no *router* de fronteira com o Cliente 2 (PE7).

b) Quais os tipos de LSA que andam dentro da área 3 do domínio OSPFv2 do ISP (ver PE7, por exemplo)?
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?
d) Qual a razão do custo/métrica entre o PE1 (30.1.255.1) e o PE3 ser 6 (30.1.255.3)?
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)

Defina se se justifica, e se sim onde, o uso de rotas estáticas. Justifique devidamente a sua opção pela utilização destas.

Verifique se as rotas estáticas funcionam como esperado (se aparecem nas tabelas de *routing* e se os Ping funcionam em todos os casos).

Procure evitar, sempre que possível, a propagação de todas as rotas provenientes da Internet que poderiam, em casos reais, conter centenas de milhares de rotas, atualmente cerca de 750.000.

Como resultado deste ponto pretende-se a lista de rotas estáticas configuradas, um exemplo de configuração que seja representativo do que foi feito para o conseguir e a justificação pela opção de usar cada uma das rotas estáticas. Dado o uso de rotas estáticas se poderá apresentar como conveniente noutra fase do trabalho, o estudante poderá ter de regressar a este ponto posteriormente.

3 – Configuração do protocolo RIPv2

Configure o RIPv2 no Cliente 2.

a) As mensagens de RIPv2 não devem ser enviadas para quem não tem interesse nelas. Como proceder para que tal seja conseguido?
b) Poderia ser usado RIPv1 no cliente 2?

Tenha em consideração a forma como o Cliente 2 se liga ao ISP e o facto de que os seus *routers* internos não necessitam ter as rotas na forma explicita para tudo e mais alguma coisa fora do domínio do Cliente 2.

Como resultado deste ponto pretende-se o resultado do Ping entre equipamentos do cliente, a tabela de *routing* do RC2_1 e a parte correspondente à configuração do RIPv2 no *router* de fronteira do Cliente 2 (PE7).

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

Configure o que for necessário para que se torne possível a comunicação entre quaisquer equipamentos existentes no ISP ou nos seus clientes que não utilizem BGPv4.

a) Justifique a sua escolha de custos tipo E1 ou E2 do OSPF na redistribuição dos endereços IP.

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).

Verifique se as tabelas de *routing* incluem rotas para todos os *routers* do ISP e dos clientes e se os Ping de teste têm sucesso. Use o Ping via TCLSH para simplificar os testes, ou o Ping estendido se necessário por causa dos endereços privados.

c) No *router* PE7 será necessário incluir os dois comandos de *redistribute*?

```
router ospf 1
        redistribute static subnets
        redistribute rip subnets
        …
!
ip route 60.0.31.128 255.255.255.128 10.3.48.1
!
ip route 60.0.28.0 255.255.254.0 30.3.49.2
…
```

d) A rede N48 poderia ser um rede com endereços IP privados?

e) A rota estática para 60.0.28.0 é necessária "ip route 60.0.28.0 255.255.254.0 30.3.49.2"?

f) O que acontece se em configurações como a do *router* R102_2 o comando "*ip ospf network point-to-point*" for removido?

```
interface GigabitEthernet4/0
ip address 10.102.3.2 255.255.255.252
ip ospf network point-to-point
…
```

g) R202_1: É necessário na configuração do OSPF, no *router* 202_1, inserir tantos comandos *network*?

```
router ospf 1
log-adjacency-changes
auto-cost reference-bandwidth 1000
passive-interface default
no passive-interface GigabitEthernet3/0
no passive-interface GigabitEthernet4/0
no passive-interface GigabitEthernet5/0
network 10.0.9.0 0.0.0.3 area 0
network 10.0.11.0 0.0.0.3 area 0
network 20.202.7.251 0.0.0.0 area 0
network 20.202.0.0 0.0.7.255 area 0
network 20.202.131.0 0.0.0.3 area 0
network 20.202.132.0 0.0.0.3 area 0
```

h) Qual a necessidade de no *router* P6 se utilizar o comando seguinte e o que acontece se for substituído por *area 3 nssa* apenas?

```
router ospf 1
```

…

area 3 nssa default-information-originate

…

i) A área 3 do domínio OSPF do ISP pode ser configurada como *Totally Stub*?

No fim desta fase deve ter toda a parte do trabalho que usa ligações diretas, rotas estáticas, RIPv2 e OSPFv2 a funcionar, quer dentro do domínio do ISP, quer dentro dos outros AS, inclusive na comunicação do ISP com e entre os clientes 1 e 2.

Como resultado deste ponto pretende-se o resultado do Ping entre o PE1 e os PC dos clientes 1 e 2, a parte da configuração correspondente às várias redistribuições de endereços e respetiva explicação.

Nota: O facto de uma parte significativa do trabalho de configuração ser disponibilizada não isenta o estudante da obrigação de a ter de perceber, de a rever e de dever optar por melhores soluções quando se justifique.

Fase 3 – BGPv4, redistribuição de rotas entre o OSPFv2 e o BGP

1 - BGPv4 básico

O BGP é um protocolo muito poderoso e que permite fazer muita coisa. Para conseguir realizar a configuração de uma topologia relativamente simples com a usada neste trabalho pode implicar muito esforço de *debug*. Como tal parte da configuração é já proposta.

Nota: Neste ponto não deve existir uma preocupação especial em implementar as políticas enumeradas na Introdução, essa serão realizadas mais à frente. O objetivo aqui é apenas colocar o BGP a funcionar corretamente entre todos os AS, permitindo a realização com sucesso do Ping entre quaisquer dois equipamentos com endereços IP públicos.

Comece por configurar/verificar o BGPv4 no AS do ISP e nos AS de *tier* 1 e 2, deixe os clientes e os AS do mesmo tier do ISP para quando esta parte estiver a funcionar corretamente. Configure o BGP em todos os *routers* em que este for necessário, não descuidando quer o eBGP, quer o iBGP. No iBGP deve ser usado *full mesh*.

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?

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?

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?

d) É necessário configurar o iBGP em todos os *routers* de todos os AS? Justifique.

Realize/verifique a redistribuição de endereços IPv4 entre o BGP e o OSPF (não se esqueça que em algumas situações podem ser usadas rotas estáticas) de maneira a conseguir realizar o Ping entre todos os equipamentos com endereços IP públicos dos AS envolvidos neste ponto.

Após a configuração básica referida anteriormente configure os clientes e outros AS (301 e 303) que usam BGP e estão no mesmo *tier* do cliente. Sem preocupações de rotas específicas para este ou aquele tráfego.

Verifique se consegue realizar o Ping entre os *routers* que correm BGP.

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.?

f) Qual a razão pela qual dos *routers* P não se conseguem fazer Ping a endereços IP noutros AS?

g) Será que faz sentido a utilização de endereços IPv4 privados nas ligações ponto-a-ponto dentro dos AS? E entre os AS?

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.

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

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

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

l) Qual a rota usada entre o *router* R201_1 e o *router* R202_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"?

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.

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".

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

q) Será que se pode usar um "no syncronization" no BGP no AS do ISP?

As rotas interiores aos AS para tráfego entre dois pontos do mesmo AS, apesar da distância administrativa do OSPF ser superior à do BGP, devem ser preferidas às rotas exteriores.

Como resultado deste ponto pretende-se também o resultado do Ping, as tabelas de *routing* e do BGP (explicadas) de um dos *routers* de fronteira dos AS 101, 201, 301, 302 e do cliente 3.

2 – Implementação de políticas no iBGP no ISP

Este ponto pretende abordar a configuração do BGPv4 quando se pretendem implementar no BGP políticas um pouco mais avançadas de gestão do tráfego IPv4. Configuração esta que implica que uma abordagem do BGP, quase do tipo "*plug and play*", não seja suficiente.

Sugestão

- Cada *router* que possui BGP, tem de estar sempre a anunciar o/s bloco/s que determinada entidade possui.
- Lembrar que existem 3 formas de anunciar rotas através de BGP:
  1 – Um *router* anuncia automaticamente uma rota caso a receba por eBGP. Se a receber por iBGP anuncia apenas a *peers* eBGP.
  2 – Através da redistribuição no BGP
  3- Através do comando *network*: Mas para que consiga anunciar a rede presente no comando *network*, esta tem que estar presente na tabela de *routing*. Investigue a técnica de realizar rotas estáticas para Null 0.
- Investigue o comando "*neighbor X next-hop-self*". Decida se deverá ser usado no iBGP.
- Relembre das aulas teóricas qual deverá ser em iBGP, o endereço/interface a iniciar/estabelecer a sessão TCP.
- Para os *routers* internacionais não enviarem a tabela de *routing* inteira para os *routers* internos, deve nas sessões iBGP do PE1/3 com os restantes, colocar uma *route-map* que evite o anúncio de qualquer rota indesejada.
- A sessão iBGP entre o PE1 e PE3, deverá realizar-se pelo *link* direto entre eles. Terá de configurar o OSPF nestes dois *routers*, para que a interface de saída do PE1 para o PE3 seja a g4/0.

Verifique se é possível que os *routers* PE1 (*Provider Edge* 1) e PE3 utilizem *full routing* entre eles. Os restantes PE do ISP apenas devem possuir as redes internas (dos seus clientes) por BGP. Se for possível, configure.

Configure o iBGP, preparando os filtros para satisfazer os requisitos enunciados no início deste enunciado.

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?

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?

c) O que aconteceria se se ajustasse em todas as sessões iBGP um *keepalive* de 5 e um *hold* de 15?

Qualquer endereço do bloco do ISP que não exista/esteja atribuído/configurado no ISP, este deve ser "afundado" pelos PE que correm BGP. Quer-se com isto dizer que um pacote IP que entre para um destino (endereço IP) que não exista deve desaparecer sem deixar rasto!

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.

Como resultado deste ponto pretende-se a indicação das medidas implementadas, o resultado do Ping e as tabelas de *routing* (explicadas) de um dos *routers* de fronteira dos AS101, 202, 301, 302 e do cliente 3.

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

O ISP impõe a regra para os seus clientes em que, por questões de *Committed Access Rate* (**CAR**) / *Quality of Service* (QoS), não deve existir balanceamento de tráfego, devendo antes ser assumida uma política de redundância tipo ativo/passivo. No caso dos AS dos clientes, no caso de serem *multihomed*, não deve existir tráfego assimétrico (sair por uma das ligações e entrar por outra).

A política implementada, por exemplo quando se utiliza *Local Preference* dentro do ISP (para dar preferência a um dos *routers* de determinado cliente) para os seus clientes, deve ser escalável e genérica para poder ser usada com qualquer cliente.

O ISP origina sempre a rota *default* para os seus clientes.

O ISP relativamente aos seus clientes que usam BGP deve incluir as seguintes medidas de segurança:

- Aceitar um máximo de 50 prefixos
- Aceitar apenas tráfego das redes que lhes delegou ou que eles possuem oficialmente
- Garantir que apenas anuncia a rota *default*

Implemente, uma de cada vez, as políticas enumeradas na Introdução. Por exemplo, a preferência de locais de entrada e saída do tráfego no ISP, a garantia de tráfego simétrico.

a) Indique como configuraria o acesso do ISP ao Cliente 2 para usar eBGP. Não configure.
b) Qual a rota usada para o tráfego entre o AS do Cliente 4 e do Cliente 3?
c) Todas as rotas seguidas pelo tráfego nas questões das alíneas anteriores cumprem as restrições impostas inicialmente sobre o tráfego entre AS, *tiers*, etc?
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.

Como resultado deste ponto pretende-se a indicação de como configurou os equipamentos de rede envolvidos para conseguir atingir os objetivos enunciados.

4- *Route Refletor (RR)*

Para tornar a gestão do iBGP no ISP mais escalável e menos consumidor de recursos, optou-se por implementar um RR no P4. Explore o comando *neighbor address route-reflector-client*

A sessão de iBGP entre o PE1 e PE3 não deve utilizar o RR.

Como resultado deste ponto pretende-se a indicação de como passou de *full mesh* para RR, em termos de configuração e conhecer quais as alterações nas tabelas de *routing*, sobretudo a do P4 e na de outro *router* que use iBGP (um *router* PE) e de outro *router* P à escolha.

Fase 4 – BGPv4 avançado

Nesta fase do trabalho pretende-se influenciar o tráfego externo ao ISP (nos restantes AS) e tráfego de entrada e de saída neste.

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

Com a criação do IXP, surge o primeiro utilizador deste (AS 303).

Implemente o *peering* com os filtros que considerar necessários entre o AS 302 e o AS 303 através do IXP.

Nota: Numa relação de *peering*, apenas se anunciam os endereçamentos que se possui/próprios. Um AS não deve anunciar as redes de um *peer* seu aos AS do *tier* acima ou do mesmo *tier*, com os quais não exista *peering*. Evitam assim servir de AS de trânsito entre os AS do *tier* acima ou do mesmo *tier* que não são seus clientes.

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.

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.

Como resultado deste ponto pretende-se a indicação de como configurou os *routers* envolvidos nestas alterações para conseguir atingir os objetivos enunciados.

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

Implemente as medidas necessárias, para a proteção do ISP e dos seus clientes, em termos medidas simples de segurança como, por exemplo, a limitação do tráfego indesejável, quer de entrada, quer de saída do AS (ver sugestões). Teste com o Ping com parâmetros forçados.
Existem boas práticas que devem ser sempre seguidas:

- Deve ser seguida a política já referida antes de que um 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 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*.
- Remover os AS privados, não os anunciar.
- Garantir que não entram pacotes no seu AS com um endereço IP de origem pertencente ao seu bloco IP.

- O BGP nos AS deve ser configurado de maneira a que a implementação de boas práticas evite problemas como o *spoofing*, inclusive que se garante que apenas saem do respetivo AS pacotes com endereço de origem pertencente ao seu bloco IP oficial. Chamam-se a isto -> Filtros *anti-spoffing* e permitem negar o transporte a tráfego que tenha sido gerado ilicitamente.
- Seguir o sugerido no RFC 6890, no que à aceitação de anúncios de redes por BGP diz respeito.

Implemente estas boas práticas em todos os AS.

Como resultado deste ponto pretende-se a indicação de como configurou os *routers* envolvidos nestas alterações para conseguir atingir os objetivos enunciados.

3 - Políticas de tráfego de saída do ISP

Para além das políticas salientadas na Introdução, há que ter em atenção as seguintes:

- O AS 201 informou o ISP que, com a ativação do BGP entre ambos, este poderá usufruir de um plano de trânsito mais favorável em relação à concorrência e poderá, inclusivamente, aceder a todas as redes dos seus *Peers* e *Content Deliver Networks* (CDN) de forma gratuita. Assim, o tráfego para o "Resto do Mundo" e para os AS do *tier* 1 na topologia deve sair preferencialmente 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.
- Deve procurar garantir que o tráfego é simétrico. **Nota:** O gestor do AS 302 não tem autorização para realizar configurações no AS 202 para atingir os seus objetivos.
- 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. Este não é o caso dos representados na topologia do trabalho.

Implemente as políticas acima relacionadas com o IXP e acesso a outros AS do mesmo *tier*.

- Tráfego para o AS 303 deve sair preferencialmente pela ligação via IXP e, se esta ligação falhar, via AS 202 via PE3.

Verifique se as políticas acima relacionadas com o AS 303 se encontram todas implementadas.

Implemente as políticas acima.

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

Como resultado deste ponto pretende-se a indicação de como configurou os *routers* envolvidos nestas alterações para conseguir atingir os objetivos enunciados.

Fase 5 (Nota: Fazer 3 dos seguintes pontos à sua escolha)

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?
b) O que acontece se do R101_1 se fizer um Ping ao PE6 e não existir o *default-information originate* nos PE*n*?
c) Do P4 consegue realizar um Ping a um *router* exterior do AS?
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?
e) O comando *default-information originate* é necessário no OSPF nos *routers* PE 1 e 3?

```
router ospf 1
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 redistribute bgp 302 subnets
 passive-interface default
 no passive-interface GigabitEthernet4/0
 no passive-interface GigabitEthernet6/0
 network 10.1.17.0 0.0.0.3 area 1
```

network 10.1.23.0 0.0.0.3 area 1

network 30.1.255.3 0.0.0.0 area 1

default-information originate

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?

2 - Nova saída de tráfego internacional

O ISP passou a possuir mais uma saída internacional e ficou com o PE2 ligado ao AS101.

Configure a ligação, sabendo que esta deve ser a última preferência de saída do ISP e o tráfego deverá ser simétrico. O objetivo da nova ligação internacional é ser apenas utilizada em caso de falha da principal.

Após esta implementação, se o gestor da "equipa" verificar pelos testes efetuados que o tráfego para os seus *upstreams* está assimétrico, por exemplo que o tráfego proveniente do "Resto do Mundo" está a entrar pela nova ligação, deve solucionar o problema com o objetivo da nova ligação internacional ser apenas utilizada em caso de falha da principal e o tráfego ser sempre simétrico.

3 - Criação de um novo cliente com AS privado e ligação com redundância

Inclua na topologia outro cliente (Cliente 5) com 3 *routers* e duas LAN internas. Deve possuir duas saídas a partir do mesmo *router* (ASBR), mas com caminhos alternativo para o ISP de maneira a melhorar a redundância e realizar balanceamento de tráfego entre clientes (continuarão a ligar-se ao ISP via os *switches* existentes). Apesar de 3 routers este Cliente 5 só tem um *router* de saída com duas ligações ao exterior.

[Sugestão]

- Configure o *layer* 2 (caminhos das VLAN), de seguida o *layer* 3 PTP.

- É necessário iBGP dentro do Cliente 5. O que leva à necessidade de configurar o IGP.

- Por último ative o eBGP sem filtros. Comece por uma configuração simples e só após esta funcionar é que deve avançar com algum que considere necessário.

Reconfigure o acesso do Cliente 3: A ligação deste cliente ao ISP deverá usar BGP, tal como o novo cliente. Como o Cliente 5 pretende redundância, serão necessárias redes PTP (*point-to-point*) de interligação /30 e respetivas VLAN para dar suporte a uma possível redundância entre o ISP e o cliente.

Exemplo:

Cliente | Sessão	***Link***	**VLAN**	**Redes PTP/máscara**
C3 Sessão BGP Principal	RC3_1-PE5	35	?
C3 Sessão BGP Backup	RC3_2-PE4	34	?
C5 Sessão BGP Principal	RC5_1-PE4	54	?
C5 Sessão BGP Backup	RC5_2-PE5	55	?
…	…	…	…

Configure a política de tráfego do Cliente 5:
Tráfego de entrada no AS 65005 -> preferencialmente pelo RC3_1.

Tráfego de saída no AS 65005 -> preferencialmente pelo RC3_1.

a) Será que pode usar o *WEIGHT* para influenciar o tráfego de saída em ambos os clientes?

b) Verifique a tabela de BGP dos RC3_n e RC5_n. Qual a preferência para a 0.0.0.0 e que regra do algoritmo do fator de decisão do BGP está a contribuir para a preferência? No final, qual o *next-hop* para a 0.0.0.0?

c) Deve aplicar o *WEIGHT* em ambos os *routers* do cliente?

d) Deve usar o *Local Preference* neste caso?

Como resultado deste ponto pretende-se a configuração necessária no PE4 e 5, nos *switches* e nos *routers* dos clientes 3 e 5 necessárias para se conseguir atingir o objetivo enunciado e o resultado de testes.

4 – Eliminação do uso de um AS privado de um cliente passando a domínio privado OSPF

Suponha que o cliente que explora o AS 65005 decide deixar de usar BGP, pretendendo continuar a utilizar o seu próprio domínio OSPF internamente. Pretende igualmente continuar a usar a estrutura de rede existente que o liga ao PE4 e ao PE5 de maneira a conseguir redundância, mas sem interferência com outros eventuais clientes que se pudessem vir a ligar aos *switches* 3 e/ou 4 (sem considerar o Cliente 5). Execute as alterações necessárias a que isso seja possível continuando a resguardar a rede do ISP de possíveis erros que o cliente possa cometer na sua rede.

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

Em virtude dos recursos gastos no troço P6-PE6, o ISP pretende garantir a utilização deste caminho para o tráfego do Cliente 4 com destino o AS 65005 em detrimento da rede N38 (PE5/PE6). O PBR poderá ajudar neste objetivo.

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

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

Como resultado deste ponto pretende-se a indicação de como configurou os *routers* envolvidos com o PBR.

6 - Pedidos de rotas especiais

Chega um pedido de implementação à equipa de engenharia. O AS301 pretende que o tráfego com origem na rede 194.14.56.0/23 e destino ao "resto do mundo" saia preferencialmente pela nova ligação internacional do ISP. O tráfego deverá ser simétrico.

Simulador

A configuração básica RIP, OSPF e BGP dos *routers*, quando existente na configuração disponibilizada para este trabalho, deverá ser adaptada ao seu simulador e à forma como o configurar. Os estudantes devem estudá-la, compreendê-la, corrigi-la onde entenderem necessário (justificando as suas opções), alterá-la para atingirem os objetivos indicados e responderem às questões colocadas. Deverão complementar a configuração fornecida de maneira a conseguirem realizar a fase 4 do trabalho. Nos casos em que considere que um objetivo indicado não pode ser cumprido devido a limitações do BGP isso deverá ser justificado no relatório.

Relatório

O relatório final deve ser dividido segundo as várias fases do trabalho. Cada parte referente a uma fase deve, para além de responder às questões explicitas nas várias alíneas, descrever de forma concisa e precisa, seguindo a sugestão sobre o que é pretendido existente no final de cada ponto, o que foi feito para efetuar a respetiva fase. Deve ainda

Pretende-se como resultado deste trabalho um relatório onde conste, devidamente comentadas/justificadas:

- Em cada fase existem questões assinaladas explicitamente (alíneas) que devem ser respondidas. No fim de cada ponto existe um parágrafo que serve de orientação sobre o que se pretende como resultado do ponto ter sido configurado, incluindo para cada uma das fases do trabalho pretende-se a listagem da configuração utilizada para se atingirem os objetivos indicados para a respetiva fase.
- Indicar em cada ponto o que foi alterado relativamente às fases anteriores, se for o caso. Devem ser evitadas sobreposições de explicações sobre o mesmo tema (por exemplo: repetir na fase 2 a explicação das opções tomadas na configuração das interfaces dos *routers*), exceto se for necessário efetuar alguma alteração em relação a fases anteriores para se poder atingir o objetivo da fase atual.
- Em anexo as listagens das configurações finais de cada fase dos *routers*. Podendo ser utilizados os ficheiros obtidos nos simuladores como, por exemplo, no GNS3 com "file>Import/Export device configs".
- **Em anexo ao relatório o ficheiro do GNS3, tipo "Export Portable Project", sem imagens, correspondente ao trabalho efetuado (convém ser na forma de um *link* para uma "box/cloud").**

Bibliografia

Pode consultar qualquer bibliografia, no entanto para configurar o OSPF aconselha-se a bibliografia indicada nos trabalhos anteriores.

Para configurar a parte que respeita ao BGP aconselha-se a consultar a documentação disponibilizada, em especial na diretoria "docs_BGP". Existem lá muitos exemplos de configuração e muitos tutoriais. Dê uma vista de olhos rápida nos vários, escolha e depois conforme necessário aprofunde aqueles que precisar. Os dois "cis185" são igualmente uma boa fonte de informação:

- cis185-mod9-BGP-Part1.pdf
- cis185-mod9-BGP-Part2.pdf

O documento da Cisco "BGP tutorial" em "Cisco-BGP.pdf" é igualmente uma boa referência para começar.

Todos os outros documentos em "docs_BGP" têm uma ou outra coisa interessante, mas muito repetida entre eles. Deve no entanto "espreitá-los" e decidir por si!

A documentação do CCNA da Cisco é interessante, mas não inclui o BGP.

Links úteis

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-16/irg-xe-16-book.pdf

https://techhub.hpe.com/eginfolib/networking/docs/switches/K-KA-KB/15-18/5998-8164_mrg/content/ch15s11.html

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-3se/3850/irg-xe-3se-3850-book/irg-prefix-filter.html

http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13754-26.html

http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfbgp.html#wp1000934

https://archive.apnic.net/meetings/22/docs/tut-routing-pres-bgp-bcp.pdf

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipswitch_cef/configuration/xe-3s/isw-cef-xe-3s-book/isw-cef-load-balancing.html

https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200782-Configure-Redistributing-Internal-BGP-Ro.html

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

Anexo – Sugestões para simplificar o trabalho

- Caso necessite limpar a configuração toda de um *router* pode usar: "*delete nvram:startup-config*". Depois de executar o comando poderá executar um *reload* mas … no GNS3 o *router* "morre". Deverá realizar *stop* e *start* do *router* e ele arrancará com uma configuração limpa.
- Evite perder tempo quando se engana a escrever um commando:

  Router(config)# no ip domain-lookup

- Os *routers* que servem os IXP devem ter na sua tabela de *routing*:

  - As suas rotas
  - Rotas mais específicas para todos os seus pares no IXP
  - Um agregado para todas as rotas no seu IXP
  - Um agregado para todas as rotas noutros IXP

- *Cada AS anunciará o bloco CIDR que lhe foi atribuído via BGP:*

  router bgp n

  no synchronization
  no auto-summary
  bgp log-neighbor-changes
  network <net> mask <mask>
  !
  ip route <net> <mask> null0 250

  Don't forget the static route to Null0*. This ensures that the prefix has an entry in the routing table, and therefore will appear in the BGP table. Also, don't forget to disable synchronization and auto-summarisation – these are also mandatory requirements for ISP routers connecting to the Internet. Note that the distance of 250 applied to the static router will ensure that routing protocols announcing this exact prefix will override the static (if this is required/desired).*
- *Firstly, agree on what IP addresses should be used for the point-to-point links between the ASs. Put the /30 networks used for the DMZ links into OSPF (network statement and passive interface). Then configure eBGP between the router pairs, for example:*

  router bgp n
  neighbor <ip_addr> remote-as 200
  !neighbor <ip_addr> description eBGP with RouterXX
  neighbor <ip_addr> soft-reconfiguration in

  Use the BGP show commands to ensure that you are receiving prefixes from your neighbouring AS. Don't forget the soft-reconfiguration command – this again is mandatory on all eBGP peerings.

- Três princípios BÁSICOS:

  prefix-lists para filtrar prefixos (endereços/máscaras)
  filter-lists para filtrar ASNs
  route-maps para aplicar políticas

- Sugestão para evitar que alguns erros de configuração noutros AS afetem o AS da empresa (**RFC 6890**):

  router bgp <AS_number>
  network <ip_addr> mask <mask>
  neighbor <ip_addr> remote-as <AS_number>
  neighbor <ip_addr> prefix-list in-filter in
  !
  ip prefix-list rfc6890 deny 0.0.0.0/0 ! Block default
  ip prefix-list rfc6890 deny 0.0.0.0/8 le 32 ! "This host on this network"
  ip prefix-list rfc6890 deny 10.0.0.0/8 le 32 ! Private-Use

```
ip prefix-list rfc6890 deny 100.64.0.0/10 le 32          ! Shared Address Space
ip prefix-list rfc6890 deny 127.0.0.0/8 le 32            ! Loopback
ip prefix-list rfc6890 deny 169.254.0.0/16 le 32         ! Link Local
ip prefix-list rfc6890 deny 172.16.0.0/12 le 32          ! Private-Use
ip prefix-list rfc6890 deny 192.0.0.0/24 le 32           ! IETF Protocol Assignments
ip prefix-list rfc6890 deny 192.0.2.0/24 le 32           ! Documentation (TEST-NET-1)
ip prefix-list rfc6890 deny 192.88.99.0/24 le 32         ! 6to4 Relay Anycast
ip prefix-list rfc6890 deny 192.168.0.0/16 le 32         ! Private-Use
ip prefix-list rfc6890 deny 198.18.0.0/15 le 32          ! Benchmarking
ip prefix-list rfc6890 deny 198.51.100.0/24 le 32        ! Documentation (TEST-NET-2)
ip prefix-list rfc6890 deny 203.0.113.0/24 le 32         ! Documentation (TEST-NET-3)
ip prefix-list rfc6890 deny 224.0.0.0/3 le 32            ! Block multicast && Reserved Block
ip prefix-list rfc6890 deny 0.0.0.0/0 ge 25              ! Block prefixes >/24
ip prefix-list rfc6890 permit 0.0.0.0/0 le 32
```

- Sempre que estiver a configurar BGP pode notar que os resultados esperados face às alterações realizadas podem não aparecer imediatamente, para isso deve forçar-se o BGP.
  Para foçar o BGP deve-se limpar as suas tabelas e fazer *reset* das suas sessões usando o comando ***clear ip bgp***. A maneira mais fácil de introduzir este comando é:

  ```
  Router#clear ip bgp *
  Router#clear ip bgp <ip_addr>
  ```

  Usar este comando com muito cuidado, melhor ainda, não o usar numa rede em produção!
- O IOS da Cisco disponibiliza o comando opcional designado por ***no synchronization***. Este comando permite ao BGP ignorar a necessidade de sincronização, permitindo ao *router* anunciar rotas aprendidas via iBGP independentemente de existirem as respetivas rotas IGP.
- Reconfiguração após alterações:

  ```
  router bgp 100
  neighbor 1.1.1.1 remote-as 101
  neighbor 1.1.1.1 route-map infilter in
  neighbor 1.1.1.1 soft-reconfiguration inbound
  ! Outbound does not need to be configured!
  ```

Quando se altera a política pode-se correr o comando para a sua execução:

clear ip bgp 1.1.1.1 **soft [in | out]**

Clear ip bgp x.x.x.x in diz ao *peer* para voltar a enviar o anúncio completo do BGP.

Sugestão: Utilize um *script* tclsh nos *routers* para ajudar a automatizar o teste com múltiplos Ping entre os vários equipamentos. Para isso basta usar o *script* abaixo com os endereços IP e máscaras das interfaces que pretenda testar e fazer *copy and paste* para a linha de comandos do *router* que pretenda que seja a origem dos Ping:

```
tclsh
foreach address {
<add 1>
<add 2>
…
} { ping $address}
```

Utilize nos *routers* o **Ping estendido** para determinar o caminho que os pacotes seguem na ida e na vinda para o "resto do mundo" (simulado pela interface loopback0 no *router* do ISP_Tier1):

```
ping
Protocol [ip]:
Target IP address: <end IP destino>
Repeat count [5]: 2
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: <end IP origem>
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
```

Loose, Strict, Record, Timestamp, Verbose[none]: **record**
Number of hops [9]:
Loose, Strict, Record, Timestamp, Verbose[**RV**]:
Sweep range of sizes [n]: