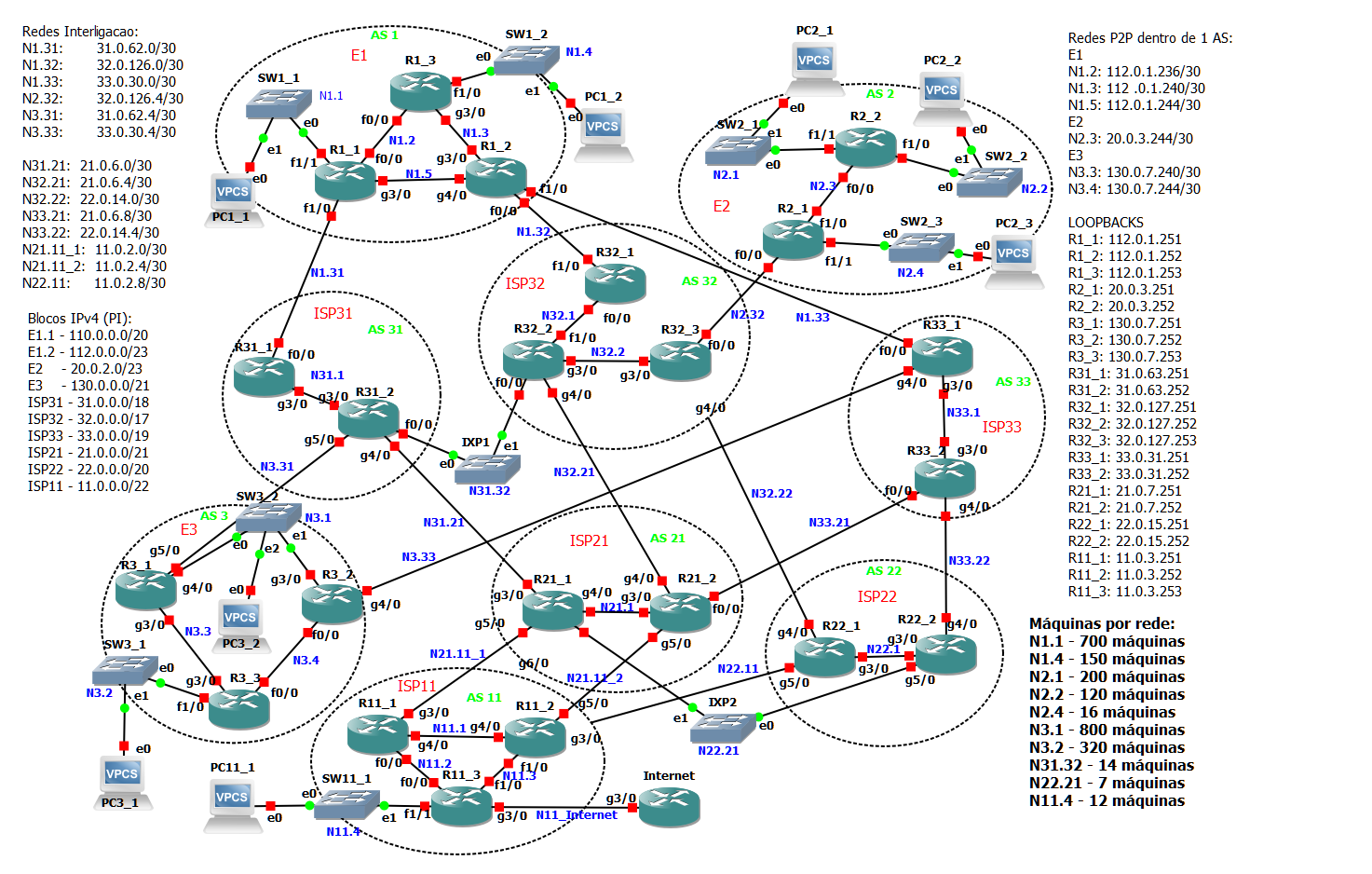
|  |  |
| --- | --- |
|  | **Instituto Superior de Engenharia de Lisboa**  Área Departamental de Engenharia de Electrónica e Telecomunicações e de Computadores (ADEETC) **Redes de Internet (RI) – 2018/2019** |

Ficha nº 4 - *BGP e IGMP*

* A resposta à ficha é individual. Para ter aprovação à disciplina deve realizar e entregar a maioria das fichas propostas.
* A bibliografia a consultar é a recomendada para a disciplina. Pode e deve procurar mais informação em outras fontes (ex: os livros da biblioteca, as normas e a Internet).
* **Deve justificar convenientemente todas as suas respostas que considerar corretas, quer das perguntas de desenvolvimento, quer das perguntas de escolha múltipla.**
* Recorra ao seu professor para esclarecer as dúvidas.
* A ficha resolvida deve ser entregue ao professor até à **data indicada no Moodle**.



1. **Na figura junta, assumindo que no AS1 é utilizado OSPFv2 como IGP, se do PC1\_2 fizer um *ping* a um dos *loopbacks* do R11\_3 qual a rota seguida pelas mensagens ICMP dentro do AS1 e o que é que influencia o caminho seguido pelos respetivos pacotes IPv4 e qual o *router* de fronteira (R1\_1 e R1\_2) que é escolhido para enviar para o exterior os pacotes IPv4 que transportam as mensagens ICMP?** **O caminho percorrido em ambos os sentidos é o mesmo?** Os caminhos dentro do domínio/rede OSPF são influenciados pelo custo das ligações. Este corresponde à soma do custo dos troços atravessados. Nos *routers* da Cisco, o custo de um troço é igual a 10^8/débito do troço. Se a rede OSPF possuir troços com débito superior a 10^8 deve-se alterar este valor em todos os *routers* do domínio OSPF para outro maior que faça sentido, por exemplo 10^10. Quando a rota inclui igualmente troços fora do domínio OSPF é necessário entrar com os custos anunciados pelo ASBR. Existem dois tipos de rotas, as do tipo 1 e as do tipo 2. Nas primeiras o custo interno é somado ao custo externo anunciado pelo ASBR para determinar o custo total. Nas do tipo 2 apenas interessa o valor anunciado pelo ASBR. Por omissão o OSPF usa as do tipo 2. O caminho percorrido em cada sentido depende das tabelas de *routing* e, neste caso, não há nada que garanta que as rotas são idênticas em ambos os sentidos dado que o router de fronteira (ASBR) a que chegam ao entrar depende do BGP.
2. **Para que nenhum gestor de outros AS fique a conhecer detalhadamente a topologia da nossa rede quais os cuidados que devemos ter**? Configurar as ligações entre o nosso AS e os outros como ligações OSPF passivas. Evita-se assim que outros obtenham informações sobre a nossa rede via OSPF.
3. **Na figura existe um IXP entre os ISP31 e ISP32 (AS31 e AS32) o qual tem como objetivo que o tráfego entre estes ISP seja realizado diretamente sem necessitar passar pelo AS do ISP do *tier* acima (AS21). Apesar do AS *path* ser menor via IXP quais os outros cuidados que é necessário ter para garantir que o tráfego IPv4 entre estes dois AS passe mesmo pelo IXP em vez de passar pelo AS acima (AS21)?** Sendo o AS\_*path* menor via IXP esta seria a rota escolhida entre os ISP31 e o ISP32. Não acontece assim se se usar atributos BGP que influenciem a rota ou se não se tiver cuidado com o anúncio dos endereços IPv4 das várias interfaces envolvidas, nomeadamente via OSPF, e na sua inclusão nas tabelas de *routing*.
4. **No AS1 existem dois *routers* de fronteira (ASBR em OSPF) com ligações aos ISP. Indique se existe uma forma, e se sim qual, para, via OSPFv2 apenas, influenciar o tráfego IPv4 de saída para o “resto do mundo” de maneira a que este saísse todo via a ligação N1.31 e se esta falhar sair em alternativa via N1.32 ou N1.33. Assuma que apenas tem o controlo do AS1.**

Anunciar, ou não, pelo OSPF as rotas externas para as redes destino no ISP; manipular, via OSPF, o custo das rotas externas anunciados pelos ASBR para atingir as redes externas ao AS1, na redistribuição de endereços do BGP para o OSPF pode-se manipular o custo anunciado pelos ASBR para que os outros *routers* prefiram uma rota de saída via R1\_1 em vez de via R1\_2.

1. **Qual a razão pela qual o iBGP necessita que as tabelas de *routing* de um AS já estejam estabilizadas antes do IBGP poder estabelecer sessões com outros *routers* do AS?** O BGP corre em cima de TCP e este de IP pelo que se as rotas não existirem (entradas nas respetivas tabelas dos *routers*) não será possível estabelecer uma rota entre os *routers* que correm iBGP pelo que a sessão TCP não poderá ser estabelecida.
2. **Como é evitado que existam *loops* internos dentro de um AS provocados por tráfego entre os routers que correm iBGP?** Todos os *routers* que correm BGPv4 (iBGP) num AS devem ter sessões estabelecidas com todos os outros *routers* do mesmo AS (*full-mesh*) e, para evitar loops internos no AS devido ao BGP, os routers internos não anunciam aos outros *routers* internos rotas aprendidas a partir de outros *routers* BGP internos ao mesmo AS.
3. **Quais as diferenças entre os AS tipo Trânsito e os do tipo *Multihomed*?** Um AS do tipo Trânsito pode-se ligar a vários AS, ISP e clientes, e pode deixar passar através dele tráfego que não tem origem nele nem a ele se destina. Um AS *multihomed* pode ligar-se a vários AS mas o AS é destino final ou de origem de todo o tráfego, não permitindo o trânsito através deles de tráfego destinado a outros AS com origem que não seja ele.
4. **Qual é o tipo de AS da Empresa 2?** *Stub*.
5. **Pode-se substituir num AS um protocolo de *routing* interno (IGP), como o OSPF, pelo iBGP?** Não.o iBGP é usado apenas para comunicar rotas entre *routers* BGP. Um *router* iBGP não ensina rotas internas a outros *routers* via iBGP.
6. **Como é que um *router* a correr BGP indica aos seus vizinhos BGP que continua “vivo”?** Existem vários mecanismos sendo que o primeiro é via TCP. Se a ligação TCP “cair” os vizinhos sabem que perderam a ligação entre eles. Se a ligação não “cair” pode acontecer que o BGP do vizinho tenha “morrido”. Para que os vizinhos tenham a certeza que os outros continuam “vivos” existe a troca periódica de mensagens de KeepAlive. Se após um intervalo de tempo (*hold time*) pré-definido não forem recebidas estas mensagens pode ser assumido que o vizinho “morreu”.
7. **Uma tabela de *routing* contem rotas para diversos destinos. Essas rotas são caracterizadas principalmente pelos seguintes elementos: Rede destino, máscara, para onde enviar (next hop), por onde enviar (interface) e custo/métrica. Descreva a forma como o BGP consegue obter, a partir da informação/atributos, como os dos tipos AS\_Path e Next Hop, as rotas com a informação necessária para a tabela de *routing* (Rede destino, Máscara, Para onde enviar (next hop), Por onde enviar (interface) e custo/métrica).** O atributo AS\_Path anuncia um prefixo (IP/máscara) e um caminho em termos dos AS a percorrer até à rede que possui o prefixo anunciado. O atributo Next-Hop indica o endereço IP da interface pertencente ao *router* BGP vizinho no próximo AS da lista de AS a percorrer. Relembre-se que um *router* para encaminhar um pacote apenas tem de saber como o entregar ao *router* seguinte na direção do destino, o próximo *router* fará o mesmo.
8. **Qual são as mensagens BGP enviadas por um *router* que detete que o caminho para uma rede/prefixo se alterou?** Uma mensagem BGP de Update com informação de Withdrawn para o prefixo em causa e a atualização com a nova rota.
9. **Se para um determinado destino/prefixo existirem várias rotas calculadas via rotas estáticas e BGP quais é que irão aparecer na tabela de *routing* de um determinado *router* que suporte ECMP?** Irão aparecer as rotas estáticas dado possuírem uma distância administrativa inferior. Neste caso só aparecerá mais do que uma rota (ECMP) se, por exemplo, existirem duas rotas estáticas com o mesmo custo. Rotas calculadas por diferentes métodos para um mesmo prefixo, usando a distâncias administrativas por omissão, nunca aparecerão na tabela em simultâneo.
10. **Em relação ao BGP, indique quais as afirmações que estão corretas:**

* O BGP é um protocolo do tipo *vector distance*
* O atributo *Weight* influencia o processo decisão de quais as rotas a colocar na tabela de *routing* #
* O atributo NEXT\_HOP é do tipo *well-known optional* podendo ou não ser incluído nos prefixos anunciados
* Um AS onde se use iBGP não necessita de outro protocolo de encaminhamento (IGP) como, por exemplo, RIPv2

1. **Em relação ao protocolo BGP**

* O atributo WEIGHT não é trocado entre *routers* do mesmo AS #
* O atributo LOCAL\_PREF é incluído em anúncios de prefixos via eBGP
* É possível garantir o percurso do tráfego de saída do AS com os atributos LOCAL\_PREF e WEIGHT #
* Para evitar tráfego de trânsito um AS deve aplicar o atributo COMMUNITY=no-export às rotas exportadas para os seus AS vizinhos
* Um AS que receba informação MULTI\_EXIT\_DISC (MED) associada a determinado prefixo deve propagá-la para todos os AS vizinhos exceto para aquele de onde o recebeu

1. **Assuma que um *router* BGP aprendeu o mesmo prefixo a partir de dois *peers* eBGP diferentes. A informação de AS\_PATH recebida do peer1 é {2345, 86, 51}, e a recebida do peer2 é {2346, 51}. Quais são os atributos que podem ser ajustados de forma a preferir a rota anunciada pelo peer1? Não se esqueça de justificar a sua resposta.**

* ORIGIN
* WEIGHT # porque se sobrepõe em termos de prioridade ao atributo AS\_Path
* LOCAL\_PREF # porque se sobrepõe em termos de prioridade ao atributo AS\_Path
* MULTI\_EXIT\_DISC
* Nenhum dos acima

1. **Acedendo remotamente a uma interface Web de “Looking Glass” foi obtida a informação abaixo acerca das rotas até à rede 192.104.48.0/24 usada por alguns servidores do campus**.

Command: show ip bgp 192.104.48.0

BGP routing table entry for 192.104.48.0/24

3356 20965 1930, via 213.242.73.73

Origin IGP, metric 0, localpref 100, valid, internal

20965 1930, via 62.40.124.21

Origin IGP, localpref 200, valid, external

20965 1930, via 62.40.124.105

Origin IGP, localpref 100, valid, external

1. Qual o AS em que se situa a rede 192.104.48.0? AS1930 - Rede Ciencia Tecnologia e Sociedade (RCTS)
2. Qual das 3 rotas será a seleccionada para o percurso entre o AS em questão e o campus do ISEL? Justifique.Não são mencionados WEIGHT, LOCAL\_PREF = 100 em 2 rotas e 200 noutra, nenhuma foi originada localmente, #2 e #3 têm o AS\_PATH mais curto, de entre estas o ORIGIN é igual (IGP), não têm informação MED, será portanto seleccionada a rota #2 por ter o Local Preference maior.
3. A quem pertencem os AS que compõem o primeiro percurso {3356 20965 1930}? (pesquise no *site* do RIPE - WHOIS)

AS3356 Level 3 Communications

AS20965 The GEANT IP Service

AS1930 Rede Ciencia Tecnologia e Sociedade (RCTS)

1. **Em relação ao IGMP, indique quais as afirmações corretas:**

* Antes de enviar uma mensagem IGMP Query é necessário fazer um pedido de ARP
* O IGMP é um protocolo que permite enviar mensagens de erro caso exista algum problema a entregar um datagrama
* No IGMP versão 1 não existem mensagens para notificar os *routers* que uma máquina já não está interessada num grupo *Multicast* #
* Quando numa rede existem vário *routers* a correr IGMPv1 e IGMPv2 é necessário configurar manualmente os *routers* para correrem IGMP v1 #

1. **Considere uma rede cujos *switches* suportam IGMPv2 onde existe o grupo *multicast* 224.1.2.9 com 10 membros ligados através de um *switch*:**

* Todos os 10 computadores podem transmitir simultaneamente para o grupo *multicast* #
* O endereço MAC destino das tramas enviadas para o endereço IP indicado é 01-00-5e-E0-02-09
* Quando o *router* envia um GROUP\_SPECIFIC\_QUERY para o endereço IP 224.1.2.9, recebe de volta 10 mensagens REPORT
* Quando o *router* não recebe nenhuma resposta às GROUP\_SPECIFIC\_QUERY enviadas para o endereço 224.1.2.9 ele pode apagar o grupo *multicast* das suas tabelas #

1. **Relativamente ao abandono de um grupo em IGMPv2:**

* A máquina envia uma mensagem de IGMP Leave #
* Ocorre de forma passiva, deixando a máquina de enviar IGMP Reports
* O router responde com uma mensagem de Group specific query, após o abandono #
* A máquina tem de enviar um IGMP Leave e esperar que o *router* confirme a receção com uma mensagem IGMP Ack enviada diretamente para o IP da máquina

1. **Qual a diferença, entre os *switches* que suportam IGMP *snooping* e os que não suportam, em termos de tráfego *multicast*?** Aplicação que corre em switches e que evita que todos os pacotes multicast sejam enviados para todas as portas do switch. Ao escutar as mensagens ICMP trocadas entre os equipamentos que correm IGMP aprende em que interfaces existem equipamentos à escuta de cada um dos grupos multicast, evitando assim enviar tráfego multicast por interfaces onde não existem nenhuns equipamentos interessados nesse tráfego. OS switches que não suportem IGMP snooping tratam os pacotes muticast como tratam os de broadcast, enviam-nos por todas as interfaces exceto aquela por onde foi recebido.