|  |  |
| --- | --- |
|  | **Instituto Superior de Engenharia de Lisboa**  Área Departamental de Engenharia de Electrónica e  Telecomunicações e de Computadores **Redes de Internet** |

**4ª Ficha de Avaliação – Prática – 17/12/2014**

**Entrega obrigatória** - **Data limite de entrega: 2015/01/14 – 8.00h**

# Introdução

Este trabalho tem como objetivo familiarizar os alunos com os protocolos de encaminhamento, com especial incidência no BGP. Com este intuito são apresentados alguns exercícios que requerem um estudo teórico prévio por parte dos alunos da bibliografia aconselhada. Os dois primeiros possuem sugestões que os alunos podem usar para atingirem os fins desejados, devendo responder de forma precisa e concisa às perguntas efetuadas. A realização do último exercício implica que os alunos realizaram com sucesso e perceberam os exercícios anteriores.

Não se assuste com o número de páginas deste enunciado, deve-se sobretudo a termos incluído sugestões de configuração para simplificar a resolução da ficha.

Estes exercícios são para serem realizados apenas após o estudo da bibliografia aconselhada. Se assim não proceder o tempo de execução do trabalho irá aumentar bastante.

Atenção que os exercícios são de dificuldade crescente pelo que devem ser realizados em sucessão. Não devem ser feios os mais avançados sem terem sido realizados os mais simples (anteriores).

Deve realizar todos os exercícios por fases:

1. Na primeira configure as interfaces e teste-as. Deve conseguir fazer *ping* entre as interfaces interligadas entre si.
2. Na segunda fase configure os protocolos de encaminhamento locais (RIP, OSPF), se for o caso, e só depois de ter os problemas resolvidos dentro de cada AS é que deve passar ao BGP e à comunicação entre AS. Poupará assim muito tempo de *debug*.

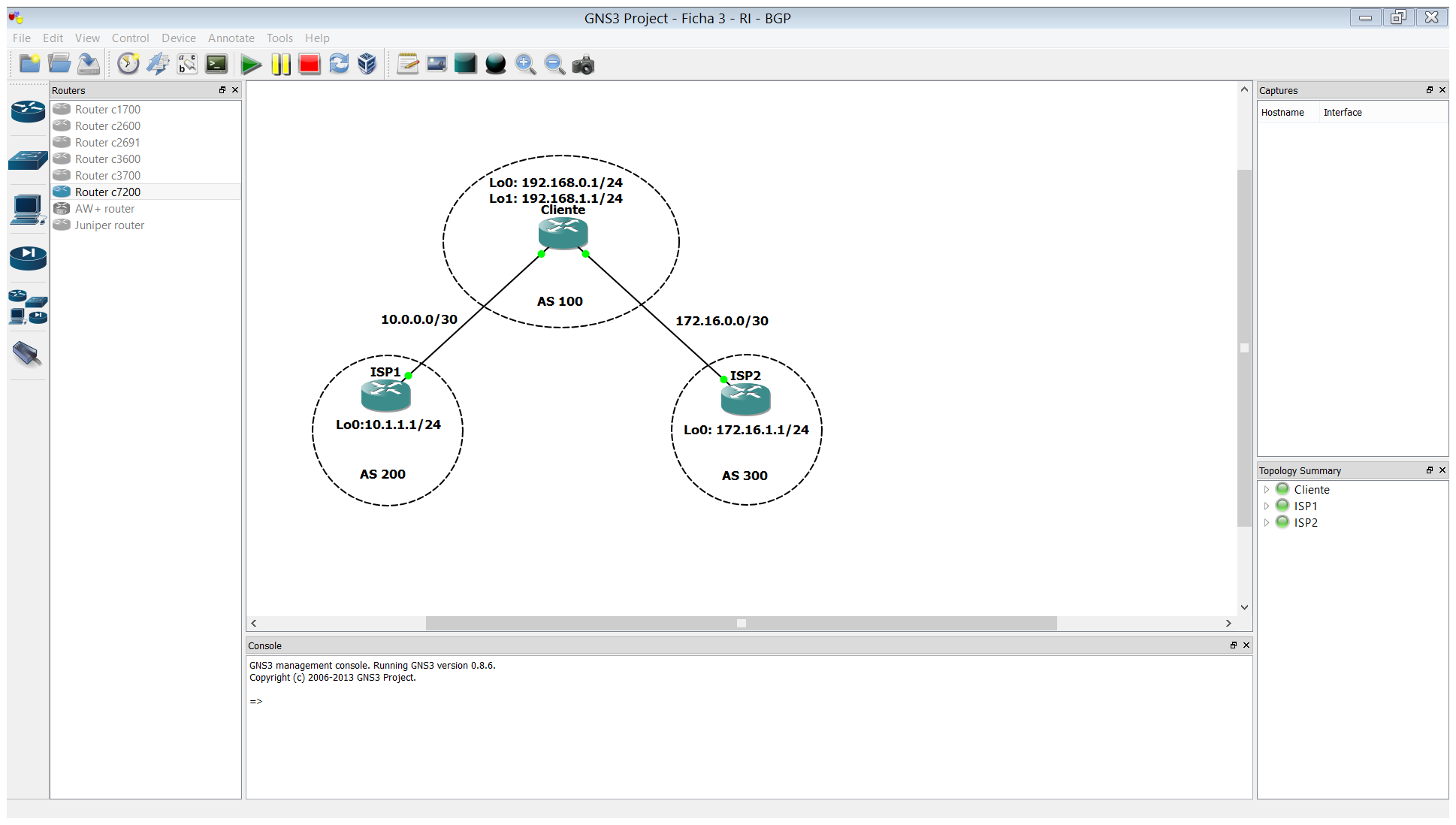
Para além da configuração final de todos os *routers*, de maneira a atingir os objetivos propostos em cada exercício, pretende-se que o relatório referente a esta ficha inclua a resposta a todas as perguntas efetuadas e a justificação do uso dos atributos, listas de acesso, etc. utilizados para se atingir os objetivos propostos no enunciado.

Para a realização destes exercícios foi usado o simulador de redes GNS3 onde foram criadas as topologias propostas nos vários exercícios. Propõem-se que os alunos façam o mesmo.

Os *routers* usados na simulação são da série 7200 com placas de duas portas FastEthernet e 4 portas série. Pode usar outros routers e outras configurações de hardware, deverá adaptar caso necessário.

**Sugestão:** Verifique se as interfaces na sua topologia condizem com as dos exemplos. Utilize um editor como o Notepad ou o Notepad++ como intermediário para ajustar os comandos antes de realizar a cópia para os *routers* no simulador. Efetue as alterações no editor e copie o resultado para o(s) *router(s)*. Isto permitir-lhe-á ter sempre todas as configurações mais recentes no editor de texto, podendo assim analisá-las detalhadamente com mais facilidade do que se tiver de estar sempre a fazer “sh ip route” nos diversos *routers* sempre que seja necessário fazer *debug*.

# Exercício 1



Pretende-se que os vá configurando os *routers* com os comandos que se seguem e que responda às questões que lhe vão sendo colocadas.

**!ISP1**

hostname ISP1

!

interface Lo0

description ISP1 Internet Network

ip address 10.1.1.1 255.255.255.0

!

interface Fa0/0

description ISP1 -> Cliente

ip address 10.0.0.1 255.255.255.252

no shutdown

!

end

**!Cliente**

hostname Cliente

!

interface Lo0

description Core router network link 1

ip address 192.168.0.1 255.255.255.0

!

interface Lo1

description Core router network link 2

ip address 192.168.1.1 255.255.255.0

!

interface Fa0/0

description Cliente -> ISP1

ip address 10.0.0.2 255.255.255.252

no shutdown

!

interface Fa0/1

description Cliente -> ISP2

ip address 172.16.0.2 255.255.255.252

no shutdown

!

end

**!ISP2**

hostname ISP2

!

interface Lo0

description ISP2 Internet Network

ip address 172.16.1.1 255.255.255.0

!

interface Fa0/1

description ISP2 -> Cliente

ip address 172.16.0.1 255.255.255.252

no shutdown

!

end

Após ter configurado as interfaces de todos os *routers* configure o BGP:

**!ISP1**

router bgp 200

neighbor 10.0.0.2 remote-as 100

network 10.1.1.0 mask 255.255.255.0

**!ISP2**

router bgp 300

neighbor 172.16.0.2 remote-as 100

network 172.16.1.0 mask 255.255.255.0

**!Cliente**

router bgp 100

neighbor 10.0.0.1 remote-as 200

neighbor 172.16.0.1 remote-as 300

network 192.168.0.0

network 192.168.1.0

Com o comando **show ip route** verifique se todos os *routers*possuem nas suas tabelas de encaminhamento todas as redes representadas na topologia? Se houver alguma que não esteja indique qual ou quais e tente justificar qual a razão.

Corra o *script* TCL nos *routers* e verifique se tem sucesso:

tclsh

foreach address {

10.0.0.1

10.0.0.2

10.1.1.1

172.16.0.1

172.16.0.2

172.16.1.1

192.168.0.1

192.168.1.1

} {

ping $address }

Usando o comando **show ip bgp** no Cliente indique qual a versão da tabela do *router* Cliente, a identificação do *router* e o porquê deste valor.

Indique qual o caminho para a rede 172.16.1.0 e o mesmo a partir do ISP1?

Qual é o estado do BGP entre o *router* Cliente e os *routers* vizinhos? (**show ip bgp neighbors**)

Como pode verificar pelas tabelas de encaminhamento do ISP1 e ISP2 ambos conseguem atingir as redes do outro ISP. Como tal, a rede Cliente (AS 100) está a ser usada como rede de trânsito. Pretende-se que tal não aconteça ou seja, a rede cliente seja *multi-homed* mas não seja de trânsito. Para evitar que o AS 100 seja uma rede de trânsito use **Cliente# access-list 1 permit 192.168.0.0 0.0.1.255** . Especifique com rigor qual a função deste comando quando usado no Cliente em conjunto com os seguintes:

router bgp 100

neighbor 10.0.0.1 distribute-list 1 out

neighbor 172.16.0.1 distribute-list 1 out

Verifique se todas as redes constam em todos os *routers*. Para que os *routers* atualizem as suas tabelas use no Cliente **clear ip bgp \*** . Qual a alteração nas tabelas dos *routers* entre antes e depois do AS Cliente ser apenas *multi-homed*?

Assumindo que os AS 200 e o 300 estavam ligados ao “resto do mundo” qual o caminho escolhido pelo Cliente para mandar tráfego para “fora”? Justifique. (sugestão: pode criar outro AS com um *router* e uma rede e verificar como ficam as tabelas de encaminhamento do Cliente para a rede nesse AS).

Configure as rotas primárias e secundárias a partir do Cliente para o resto do mundo, assumindo que a rota pelo ISP2 é a de *backup* (secundária). Pode fazê-lo usando:

ip route 0.0.0.0 0.0.0.0 10.0.0.1 210

ip route 0.0.0.0 0.0.0.0 172.16.0.1 220

Indique a razão destes comandos e qual a razão dos valores 210 e 220 no fim do comando.

Crie uma nova rede (*loopback*) no ISP1 com o endereço: **192.168.100.1**.

Verifique qual o resultado nas tabelas de encaminhamento nos *routers* dos outros AS. Justifique.

Verifique a partir do Cliente se lhe consegue fazer ping (**192.168.100.1**) a partir da rede de *loopback* (**192.168.1.1)** (sugestão: utilize o comando ping estendido do *router* - carregue no *enter* a seguir a introduzir ping). Alternativa:

ping 192.168.100.1 source 192.168.1.1

ou

ping 192.168.100.1 source Lo1

O método anterior criava rotas para o exterior do AS 100 (Cliente) usando rotas estáticas ditas flutuantes (porquê flutuantes?).

Remova ambas as rotas estáticas criadas no Cliente: **no ip route …**

Como ficou o acesso dos outros AS à rede192.168.100.0/24 criada anteriormente no ISP1?

Coloque o ISP1 a anunciar a rede usando:

router bgp 200

network 192.168.100.0

end

Esta rede (192.168.100.0) aparece nas tabelas do Cliente e do ISP2? Justifique.

Ao introduzir o comando **ip default-network 192.168.100.0** no Cliente aparece um \* a seguir a esta rede na tabela de encaminhamento do Cliente (B\* 192.168.100.0/24 [20/0] via 10.0.0.1, 00:02:33), o qual não aparecia antes. Justifique porquê.

Para criar uma rota secundária (*backup*) via ISP2 para o caso da rede 192.168.100.0 falhar poder-se-ia usar no Cliente, por exemplo:

ip route 0.0.0.0 0.0.0.0 172.16.0.1 240

ou

ip route 0.0.0.0 0.0.0.0 172.16.0.1 10

Qual seria a correta? Justifique.

Porque aparecem as seguintes duas rotas na tabela de encaminhamento do Cliente?

B\* 192.168.100.0/24 [20/0] via 10.0.0.1, 00:08:05

S\* 0.0.0.0/0 [220/0] via 172.16.0.1

Qual seria o resultado da inserção dos seguintes comandos no ISP1?

router bgp 200

neighbor 10.0.0.2 default-originate

Indique qual a configuração final de cada um dor *routers*.

Quais as alterações necessárias nos *routers* para que o AS 300 (ISP2) passe a ser um AS privado? (Nota: Embora o AS 300 continue a chamar-se ISP2 se 300 fosse na realidade o número do AS nunca poderia ser privado)

Execute as alterações.

Verifique se o AS privado é exportado para os outros AS (**show ip bgp**). Qual seria o problema do AS privado ser anunciado para a Internet?

Vai necessitar do resultado do **show ip bgp** para comparação futura, conserve-o.

Indique ao *router* Cliente para não exportar os caminhos para AS privados:

router bgp 100

neighbor 10.0.0.1 remove-private-as

Realize o comando **clear ip bgp \*** para se certificar de que os *routers* reconstroem as suas tabelas BGP.

Realize o comando **show ip bgp** nos *routers* ISP1 e Cliente. Qual a diferença em relação ao resultado obtido anteriormente? As redes do ISP2 continuam a constar nas tabelas de encaminhamento dos *routers* no ISP1 e no Cliente? Justifique.

Pretende-se que o Cliente não propague para o ISP2 rotas do AS 100 (ISP1). Assumindo que se executa no cliente os seguintes comandos:

ip as-path access-list 1 deny ^200$

ip as-path access-list 1 permit .\*

em que ^200$ e .\* representam expressões regulares em que no primeiro comando o carater ^ indica que o caminho nos AS (AS *path*) deve começar com o número 200. O carater $ indica que o atributo AS\_PATH deve também terminar com 200 (ver bibliografia aconselhada).

Essencialmente, esta expressão representa apenas caminhos que se iniciam no AS 200. Outros caminhos, os quais podem incluir o AS 200 no meio da sua lista, não estarão conformes com esta expressão.

No segundo comando o “.” (ponto) é um *wild-card* e o \* significa uma repetição do *wild-card*. Juntos, .\* , estão de acordo com qualquer valor do atributo AS\_PATH, o que tem por efeito deixar passar (permitir) qualquer valor que não tenha sido negado anteriormente na *access-list*.

No Cliente execute os comandos:

router bgp 200

neighbor 10.0.0.1 filter-list 1 out

Qual o resultado? Verifique se continua a ver todas as redes de todos os AS nas tabelas de encaminhamento dos *routers*. (Não se esqueça de fazer um **clear ip bgp \***).

O comando executado no Cliente **show ip bgp regexp ^200$** dá-nos que informação?

Execute o *scrip*:

tclsh

foreach address {

10.0.0.1

10.0.0.2

10.1.1.1

172.16.0.1

172.16.0.2

172.16.1.1

192.168.0.1

192.168.1.1

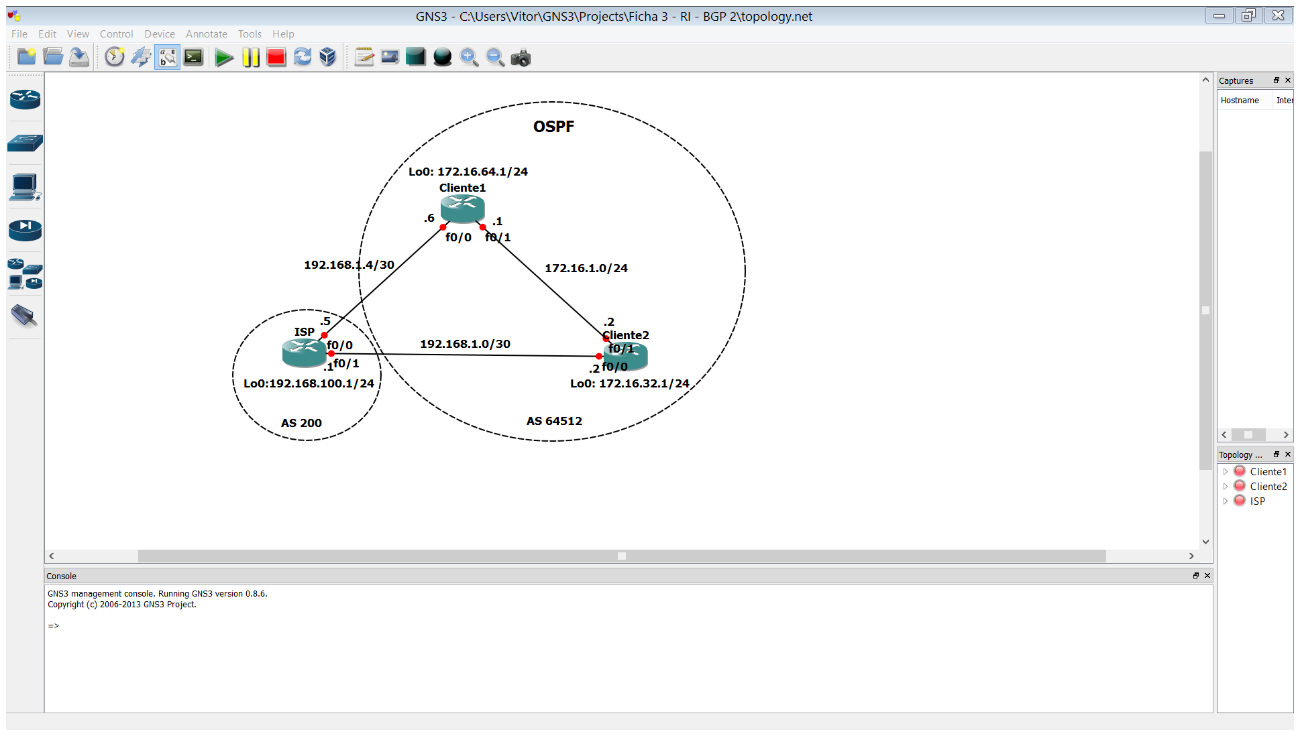
192.168.100.1

} {

ping $address }

em todos os *routers* e verifique se o resultado está de acordo com o esperado?

# Exercício 2



Utilize os comandos que se seguem para configurar as interfaces dos *routers* da figura anterior.

**!Router R1 (hostname ISP)**

hostname ISP

!

interface Loopback0

ip address 192.168.100.1 255.255.255.0

!

interface Fa0/0

ip address 192.168.1.5 255.255.255.252

no shutdown

!

interface Fa0/1

ip address 192.168.1.1 255.255.255.252

no shutdown

**!Router R2 (hostname Cliente1)**

hostname Cliente11

!

interface Loopback0

ip address 172.16.64.1 255.255.255.0

!

interface Fa0/0

ip address 192.168.1.6 255.255.255.252

no shutdown

!

interface Fa0/1

ip address 172.16.1.1 255.255.255.0

no shutdown

**!Router R3 (hostname Cliente2)**

hostname Cliente2

!

interface Loopback0

ip address 172.16.32.1 255.255.255.0

!

interface Fa0/0

ip address 192.168.1.2 255.255.255.252

no shutdown

!

interface Fa0/1

ip address 172.16.1.2 255.255.255.0

no shutdown

Teste a configuração utilizando o ping para as interfaces ligadas diretamente entre si.

Configure o OSPF no Cliente1:

router ospf 1

network 172.16.0.0

e no Cliente2:

router ospf 1

network 172.16.0.0

Configure o iBGP no Cliente1:

router bgp 64512

neighbor 172.16.32.1 remote-as 64512

neighbor 172.16.32.1 update-source lo0

Para que serve o commando **neighbor 172.16.32.1 update-source lo0** ?

Configure o iBGP no Cliente2:

router bgp 64512

neighbor 172.16.64.1 remote-as 64512

neighbor 172.16.64.1 update-source lo0

Verifique se o Cliente1 e Cliente2 se tornaram vizinhos usando o comando: **show ip bgp neighbors**

Como é que os *routers* Cliente1 e Cliente2 sabem que a ligação entre eles é iBGP e não eBGP?

Configure o eBGP no *router* ISP.

router bgp 200

neighbor 192.168.1.6 remote-as 64512

neighbor 192.168.1.2 remote-as 64512

network 192.168.100.0

Configure o Cliente1 para eBGP:

ip route 172.16.0.0 255.255.0.0 null0

router bgp 64512

neighbor 192.168.1.5 remote-as 200

network 172.16.0.0

Para que serve o comando **ip route 172.16.0.0 255.255.0.0 null0** e qual o objetivo da sua utilização?

Configure o Cliente2 para eBGP:

ip route 172.16.0.0 255.255.0.0 null0

router bgp 64512

neighbor 192.168.1.1 remote-as 200

network 172.16.0.0

Utilize o comando **show ip bgp neighbors** para verificar se todos os *routers* reconhecem os seus vizinhos.

Utilize o **show ip bgp summary** para verificar quantos atributos de caminhos BGP estão a ser usados e que memória ocupam.

Após usar **clear ip bgp \*** para reiniciar as tabelas do BGP e esperar um pouco para que estabilizem, verifique se tem acesso de todas as redes para todas as outras, nomeadamente para as redes entre o cliente1 e o ISP. Justifique.

The ping fails because Cliente1 does not have a route back to the source. The source is ISP's closest connected interface according to BGP, which in this case is the Fa0/0 link to Cliente1. The route to network 172.16.0.0 from ISP is via Cliente22, so ISP can ping the directly-connected Cliente22 interfaces but not the directly-connected Cliente1 interfaces.

Utilize o comando **show ip bgp** para verificar a tabela do router ISP.

Quantas rotas válidas para 172.16.0.0 aparecem na tabela de encaminhamento do *router* ISP? Porque é que o *router* ISP escolhe como melhor caminho via Cliente2 em vez de via Cliente1?

Because all other metrics were the same, the route advertised by the neighbor with the lower BGP router ID won the BGP route selection process.

A alteração da métrica nas ligações iria alterar o resultado nas tabelas de encaminhamento?

No, because BGP does not check link bandwidth in its route selection process. The Cliente2 router with BGP router ID 172.16.32.1 was preferred to the higher BGP router ID of the Cliente11 router (172.16.64.1).

O Cliente1 desconhece a ligação entre o ISP e o Cliente2 e o Cliente2 desconhece a ligação entre o ISP e o Cliente1. Para que o ISP consiga realizar o ping com sucesso as interfaces do lado do AS 64512, estas ligações devem ser anunciadas via BGP para o router ISP. Uma das formas de o fazer é realizar no router ISP:

router bgp 200

network 192.168.1.0 mask 255.255.255.252

network 192.168.1.4 mask 255.255.255.252

Verifique se o BGP passou a anunciar as suas próprias ligações entre AS no BGP (**show ip bgp**).

The next issue to consider is BGP policy routing between autonomous systems. The next-hop attribute of a route in a different AS is set to the IP address of the border router in the next AS toward the destination, and this attribute is not modified by default when advertising this route through IBGP. Therefore, for all IBGP peers, it is either necessary to know the route to that border router (in a different neighboring AS), or our own border router needs to advertise the foreign routes using the next-hop-self feature, overriding the next-hop address with its own IP address. The Cliente2 router is passing a policy to Cliente1 and vice versa. The policy for routing from AS 64512 to AS 200 is to forward packets to the 192.168.1.1 interface. Cliente1 has a similar yet opposite policy: it forwards requests to the 192.168.1.5 interface. If either WAN link fails, it is critical that the opposite router become a valid gateway. This is achieved if the next-hop-self command is configured on Cliente1 and Cliente2.

Verifique a tabela BGP do router Cliente2 (**show ip bgp**). Execute os comandos seguintes no Cliente1 e no Cliente2:

!Cliente1

router bgp 64512

neighbor 172.16.32.1 next-hop-self

!Cliente2

router bgp 64512

neighbor 172.16.64.1 next-hop-self

Obtenha a tabela BGP do Cliente2 e compare-a com a obtida antes. Justifique as diferenças causadas pelos comandos **next-hop-self** inseridos anteriormente.

Execute os comandos:

!Cliente1

route-map PRIMARY\_IN permit 10

set local-preference 150

exit

router bgp 64512

neighbor 192.168.1.5 route-map PRIMARY\_IN in

!Cliente2

route-map SECONDARY\_IN permit 10

set local-preference 125

exit

router bgp 64512

neighbor 192.168.1.1 route-map SECONDARY\_IN in

Utilize o comando **clear ip bgp \* soft** em ambos os routers Cliente para forçar o BGP a atualizar as tabelas.

Indique quais as alterações nas tabelas BGP (**show ip bgp**) dos *routers* Clientes, comparando-as com as obtidas antes e justifique as alterações detetadas, nomeadamente as referentes ao acesso ao segmento ISP 192.168.100.0 /24.

O tráfego do exterior (ISP) para o AS64512 é realizado via o *router* com o menor routerID, segundo o BGP. O tráfego da rede 192.168.100.0/24 irá ser enviada via?

Como é que a partir do ping estendido executado no Cliente2 consegue determinar o caminho que os pacotes seguem na ida e na vinda?

ping

Protocol [ip]:

Target IP address: 192.168.100.1

Repeat count [5]: 2

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: 172.16.32.1

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]:

Verifique o resultado obtido com o ping. Há tráfego a passar pela ligação entre o ISP e o Cliente2? Qual o atributo que permite tentar que um AS exterior, neste caso o ISP, envie preferencialmente o tráfego por uma ligação em vez de outra? Pretende-se que a ligação entre o ISP e o Cliente2 apenas seja usada em emergências. Para tal execute os seguintes comandos:

!Cliente1

route-map PRIMARY\_MED\_OUT permit 10

set Metric 50

exit

router bgp 64512

neighbor 192.168.1.5 route-map PRIMARY\_MED\_OUT out

!Cliente2

route-map SECONDARY\_MED\_OUT permit 10

exit

router bgp 64512

neighbor 192.168.1.1 route-map SECONDARY\_MED\_OUT out

Qual o objetivo dos comandos do tipo **route-map SECONDARY\_MED\_OUT permit 10**?

Qual a diferença entre o que é proposto para os *routers* Cliente1 e Cliente2? E a métrica?

Após forçar os *routers* a atualizarem as tabelas BGP (**clear ip bgp \* soft**) verifique usando o **show ip bgp** quais as alterações nas tabelas BGP.

Execute o ping estendido para 192.168.100.1 no Cliente2 e verifique as diferenças em relação aos caminhos anteriores à inserção do MED. Qual o caminho preferido pelo ISP para atingir o AS 64512?

(Nota: Tenha em atenção que numa situação real provavelmente não teríamos acesso aos *routers* do ISP pelo que os testes teriam de ser realizados do lado do “nosso AS”.)

Não existe uma rota por omissão/defeito (*defalt network*) configurada nos *routers* do AS 64512 e devia pois, num caso real, haveria “vida” para além da rede do ISP (192.168.100.0/24).

Duas formas de o fazer ou inserir no Cliente1 um comando para tal:

ip default-network 192.168.100.0

ou inserir no router ISP um comando em alternativa:

neighbor X.X.X.X default-originate

**Nota**: O primeiro funciona bem apenas para endereços *classfull.*

Utilize o comando **ip default-network 192.168.100.0** e verifique quais as alterações na tabela de encaminhamento do Cliente1. O que é que nessa tabela indica, ou não, a existência de uma rota por defeito?

Verifique se o *router* ISP tem acesso a todas as redes:

tclsh

foreach address {

192.168.100.1

172.16.64.1

172.16.32.1

192.168.1.1

192.168.1.2

192.168.1.5

192.168.1.6

172.16.1.1

172.16.1.2

} {

ping $address }

Quais foram as configurações finais de cada um dos três *routers*?

**Router ISP**

hostname ISP

!

interface Loopback0

ip address 192.168.100.1 255.255.255.0

!

interface Fa0/0

ip address 192.168.1.5 255.255.255.252

no shutdown

!

interface Fa0/1

ip address 192.168.1.1 255.255.255.252

no shutdown

!

router bgp 200

no synchronization

network 192.168.1.0 mask 255.255.255.252

network 192.168.1.4 mask 255.255.255.252

network 192.168.100.0

neighbor 192.168.1.2 remote-as 64512

neighbor 192.168.1.6 remote-as 64512

no auto-summary

!

end

**Router Cliente1**

hostname Cliente1

!

interface Loopback0

ip address 172.16.64.1 255.255.255.0

!

interface Fa0/0

ip address 192.168.1.6 255.255.255.252

no shutdown

!

interface Fa0/1

ip address 172.16.1.1 255.255.255.0

clock rate 128000

no shutdown

!

router ospf 1

network 172.16.0.0

!

router bgp 64512

no synchronization

network 172.16.0.0

neighbor 172.16.32.1 remote-as 64512

neighbor 172.16.32.1 update-source Loopback0

neighbor 172.16.32.1 next-hop-self

neighbor 192.168.1.5 remote-as 200

neighbor 192.168.1.5 route-map PRIMARY\_IN in

neighbor 192.168.1.5 route-map PRIMARY\_MED\_OUT out

no auto-summary

!

ip default-network 192.168.100.0

ip route 172.16.0.0 255.255.0.0 Null0

!

route-map PRIMARY\_IN permit 10

set local-preference 150

!

route-map PRIMARY\_MED\_OUT permit 10

set metric 50

!

end

**Router Cliente2**

hostname Cliente2

!

interface Loopback0

ip address 172.16.32.1 255.255.255.0

!

interface Fa0/0

ip address 192.168.1.2 255.255.255.252

no shutdown

!

interface Fa0/1

ip address 172.16.1.2 255.255.255.0

no shutdown

!

router ospf 1

network 172.16.0.0

!

router bgp 64512

no synchronization

network 172.16.0.0

neighbor 172.16.64.1 remote-as 64512

neighbor 172.16.64.1 update-source Loopback0

neighbor 172.16.64.1 next-hop-self

neighbor 192.168.1.1 remote-as 200

neighbor 192.168.1.1 route-map SECONDARY\_IN in

neighbor 192.168.1.1 route-map SECONDARY\_MED\_OUT out

no auto-summary

!

ip default-network 192.168.100.0

ip route 172.16.0.0 255.255.0.0 Null0

!

route-map SECONDARY\_IN permit 10

set local-preference 125

!

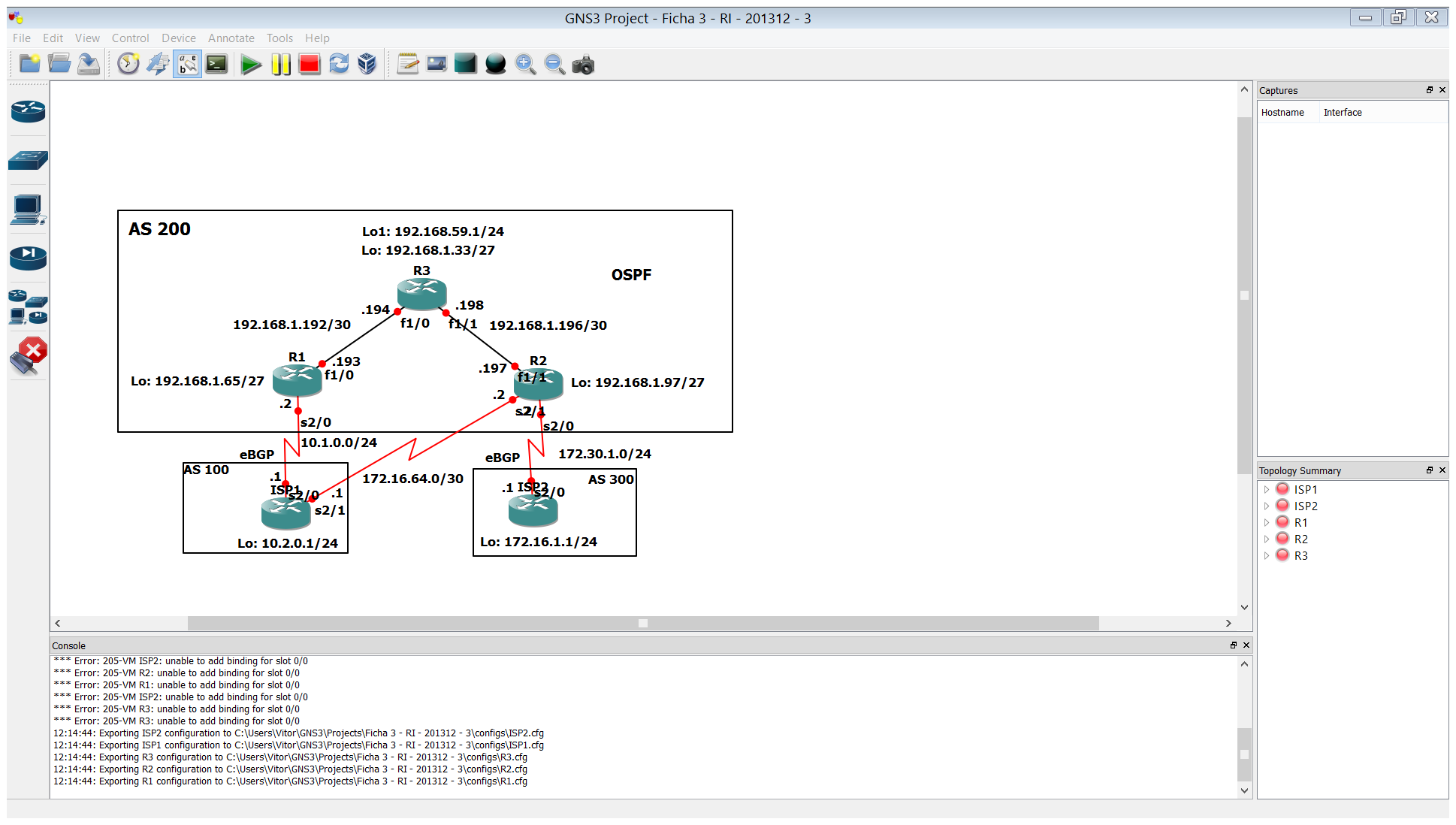
route-map SECONDARY\_MED\_OUT permit 10

set metric 75

!

End

# Exercício 3



O cenário acima representa um sistema autónomo (AS 200) com ligações a dois ISP (*multi-homed*) (AS 100 e AS 300).

Pretende-se que:

* Seja possível atingir qualquer rede a partir de qualquer rede do AS 200.
* Que as rotas externas no AS 200 sejam redistribuídas pelo OSPF.
* Não seja possível comunicar entre as redes dos sistemas autónomos do ISP1 e do ISP2 (AS 100 e AS 300). O AS 200 não é um AS de trânsito.
* A rede Lo1 do AS 200 não seja anunciada para o exterior do AS 200.
* O tráfego para o “resto do mundo” seja efetuado preferencialmente via AS 100, funcionando o AS 300 como *backup*.
* Pretende-se que o tráfego do resto do mundo para o AS 200 seja preferencialmente enviado via AS 100 e *router* R1.

Pretende-se como resultado deste exercício:

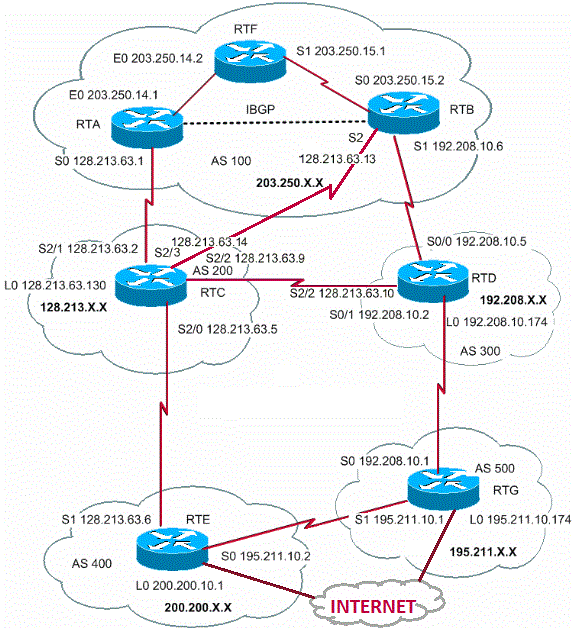
* As listagens de cada um dos *routers* devidamente comentadas, assim como um resumo de quais os atributos usados para se atingirem os resultados pedidos.
* As listagens de todas as tabelas BGP.
* As listagens de todas as tabelas de encaminhamento.
* A listagem referente ao LSA dos *routers* que correm OSPF.
* O resultados da execução do *script* que efetua ping a todas as redes da topologia usada a partir de todos os *routers*.
* Código comentado onde se justificar.
* Como referido no início da ficha, um resumo preciso e conciso sobre todas as decisões tomadas para cumprir o que foi proposto em cada ponto do enunciado do exercício.

**Responda ao seguinte questionário:**

* Quantos ABR existem no AS privado? 0
* Quantos ASBR existem no AS privado? 2
* Quantos *designated routers* existem no AS privado? 2
* Quantos LSA dos tipos 1 a 7 existem nas bases de dados de LSA dos *routers* que correm OSPF? Justifique. LSA 1: 3, LSA 2: 2, LSA 3: 0, LSA 4: 0, LSA 5: 5, LSA 6: 0, LSA 7: 0
* No BGP qual a principal finalidade do *prepending*? Influenciar as rotas de entrada no AS.
* Qual a influência que o débito das ligações tem na escolha das rotas pelo BGP? Nenhuma.
* Um AS tem de usar BGP para se poder ligar aos outros AS? Não, apenas se for multi-homed ou de trânsito.
* Num AS onde seja usado OSPF, por exemplo, para que serve o iBGP? O iBGP serva para se trocarem rotas externas entre os routers eBGP. As rotas internas ao AS são da responsabilidade do protocolo IGP, por exemplo OSPF.
* Existe o equivalente ao NAT para lidar com os números dos AS privados? Justifique.
* Porque é que nem sempre é uma boa ideia redistribuir as rotas BGP num protocolo como o OSPF? Qual a alternativa?

# Exercício 4

No cenário da figura seguinte responda às questões que se seguem com verdadeiro e falso. A todas as ligações existe associada uma sessão de BGP, por omissão são aplicados os valores seguintes aos atributos: *local-preference* (LP) = 100, métrica (MED) = 100 e WEIGHT = 100.



Não é pedido que implemente no simulador a rede da figura mas poderá faze-lo para assim poder testar as suas respostas e preparar-se para o exercício que se segue.

1. No cenário base, se os anúncios do AS100 para o AS300 forem “prepended” quatro vezes e RTD aplicar LP=200 aos anúncios recebidos de RTB, qual será o percurso do tráfego de RTG para o AS100?

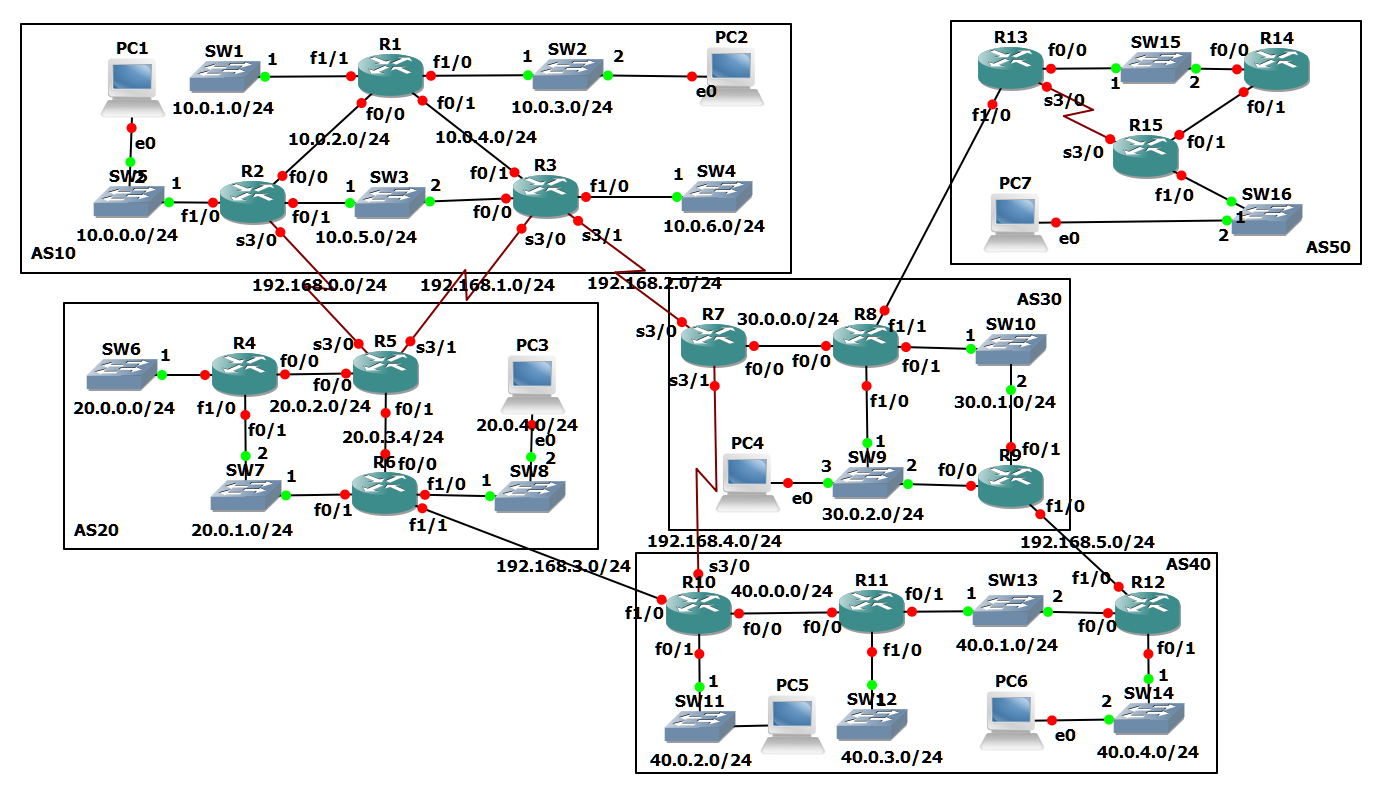
RTG, \_\_RTD\_\_,\_\_RTB \_\_,\_\_\_\_,\_\_\_\_

1. Partindo do cenário base, que atributos podem ser alterados na receção (*in*) de rotas no AS100 para que o tráfego destinado à Internet saia predominantemente por RTA?
   1. RTB marcar as rotas com LP = 80 V
   2. RTB marcar as rotas com MED = 50 F
   3. RTA marcar as rotas com *community* = internet F
   4. RTB marcar as rotas com *community* = no-export F
2. Tendo em conta o cenário acima de utilização de BGP, que soluções são possíveis realizar no AS100 de forma a influenciar o percurso de tráfego proveniente da Internet
   1. Nenhuma das outras hipóteses V
   2. Realizando *prepending* nos anúncios de rotas do RTA ao RTC F, o caminho preferido já não passava por esta ligação
   3. Colocando MED 200 nas rotas enviadas ao AS200 e de 100 às enviadas ao AS300 F
   4. Aplicando LOCAL\_PREFERENCE 200 às rotas recebidas do AS200 e 100 às recebidas do AS300 F
   5. Colocando LOCAL\_PREFERENCE 200 nas rotas enviadas ao AS200 e de 100 às enviadas ao AS300 F
3. Tendo em conta o cenário acima de utilização de BGP, que soluções são possíveis realizar no AS100 de forma a garantir que o tráfego para todos os AS exteriores passe pelo AS200
   1. Nenhuma das outras hipóteses
   2. Realizando *prepending* nos anúncios de rotas do RTA ao RTC **F**
   3. Colocando MED 200 nas rotas enviadas ao AS200 e de 100 às enviadas ao AS300 **F**
   4. Aplicando LOCAL\_PREFERENCE 200 às rotas recebidas do AS200 e 100 às recebidas do AS300 **V**
   5. Colocando LOCAL\_PREFERENCE 200 nas rotas enviadas ao AS200 e de 100 às enviadas ao AS300 **F**
4. Recorrendo à manipulação/filtragem baseada num só atributo no AS100, proponha solução para as seguintes situações:

Garantir que o tráfego proveniente do AS200 entre via RTA **Nos anúncios realizados por RTA a RTC enviando MED inferior ao de omissão (<100)**

Garantir que o tráfego sai sempre pelo RTB **Marcando as rotas recebidas do exterior pelo *router* RTA com LOCAL\_PREFERENCE inferior ao de omissão (<100)**

# Exercício 5



Configure no GNS3 a rede acima. As interfaces poderão ser outras dependendo dos *routers* que configurou no GNS3, adapte se for necessário. Os endereços IP deverão ter uma estrutura do tipo <nº AS>.<nº área OSPF>.<nº rede>.<nº *router*>. Poderá improvisar em casos como os PC, etc.

Os *routers* deverão possuir routerID que se reflitam nas interfaces *loopback* que forem configuradas em cada um, por exemplo, x.y.z.<nº *router*>.

No AS50 escolha os endereços IP a atribuir.

Num caso real a ligação ao resto da Internet seria realizada a partir do AS40. Poderá simular essa ligação se entender necessário.

Deve configurar todos os *routers* na área 0 usando como IGP o protocolo OSPF de maneira a conseguir “pingar” todas as interfaces a partir de qualquer lado. Verifique as tabelas de *routing* e use o Ping (*script*) para realizar os testes que necessitar.

Após funcionar com tudo em OSPF inicie a configuração em BGP. Siga as indicações da figura quanto aos AS. Verifique se tem acesso a todas as interfaces a partir de qualquer sítio. Não se esqueça que irá passar a ter a rede dividida em AS e que o OSPF é interior a cada um dos AS apenas.

Realize a configuração dos equipamentos tendo em atenção que se pretende que:

* Os AS20 e AS30 façam as vezes dos AS de dois ISP;
* Se um *router* não for *router* de fronteira (ASBR em OSPF) não deve correr BGP, pretendendo-se aliviar assim ao máximo as tabelas de *routing* de todos os *routers*;
* O AS 10 seja *multi-homed*, não seja de trânsito;
* O AS 50 seja um AS *stub*;
* O AS 40 seja um ISP de *tier* mais elevado do que os dos AS20 e AS 30 e que, tal como os outros ISP, seja de trânsito;
* A saída de tráfego do AS10 deve ser feita preferencialmente pela rede 198.162.1.0 (AS20);
* A entrada de tráfego no AS10, inclusive a proveniente do AS40, deve ser feita preferencialmente pela rede 198.162.0.0 (AS20);
* Se as ligações pelo AS20 falharem devem ser usadas as via 192.168.2.0 (AS30);
* A rede onde se encontra o SW16 no AS50 deve poder sempre acedida de qualquer lado de dentro do AS50 mas não deve ser acedida ou aceder para fora do respetivo AS;
* Os ISP devem proteger-se contra falsas informações que eventualmente os outros AS lhes possam transmitir e que possam levar, por exemplo, a “*black holes*”.
* [**Opcional**] Como procederia se o AS10 utilizasse RIPv2 como IGP e se pretendessem obter os resultados referidos anteriormente?

Pretende-se a configuração mais simples possível para os objetivos indicados.

No relatório a entregar, para além do equivalente ao *startup-config* dos *routers*, pretende-se uma justificação precisa e concisa das diversas opções de configuração tomadas para atingirem cada um dos objetivos anteriormente enunciados.