Protocolos de Comunicação
2018-2019

Ficha prática 5 – Border Gateway Protocol

Objetivos e organização

A presente ficha prática tem por objetivo explorar a configuração e utilização do protocolo *Border Gateway Protocolo* (BGP). Este protocolo é um dos mais complexos protocolos de encaminhamento e será aqui abordado nas suas vertentes mais essenciais. Trata-se de um protocolo de encaminhamento exterior, ou seja, um protocolo destinado ao encaminhamento de tráfego entre sistemas autónomos distintos. A sua utilização principal é como protocolo de encaminhamento no *backbone* da Internet (entre ISPs) e, por isso, não é utilizado na maioria das redes periféricas, a não ser que estas tenham ligações a mais do que um ISP.

Esta ficha de trabalho deve ser executada em duas aulas. Na primeira, a ficha deve ser cuidadosamente estudada e preparada, antes de ser executada em ambiente laboratorial na segunda aula. O total de tempo estimado para a resolução da ficha, incluindo o estudo extra-aula, é de 8 horas. A ficha é composta por exercícios guiados, para os quais se indicam os comandos a executar, e por exercícios abertos, isto é, exercícios cuja resolução exigirá pesquisa e concretização autónomas.

Nesta ficha serão abordados os seguintes tópicos

- Configuração básica e utilização do protocolo Border Gareway Protocol version 4 (BGP-4) em redes com *routers* Cisco
- Utilização do iBGP e eBGP
- Filtragem de rotas
- Definição de preferências de encaminhamento

Ao longo da execução da ficha deverão ser guardados os resultados dos comandos digitados e os ficheiros de configuração elaborados, de forma a possibilitar a sua análise pelo docente. Para além desses resultados, deverá dar especial atenção à interpretação e análise decorrentes não só do trabalho realizado nas aulas como do estudo extra-aula subjacente a esta ficha.

Deve ter em atenção que a execução das fichas práticas pode exigir a colaboração entre grupos de trabalho, de modo a serem construídos cenários com dimensão e funcionalidades adequadas ao estudo das questões em análise. Mais importante do que a simples configuração individual dos *routers* dos diversos cenários é a interpretação dos resultados obtidos, quer no(s) *router*(s) sob direta responsabilidade do seu grupo quer no conjunto das redes, interpretação essa que constitui um fator fundamental na avaliação.

A avaliação da ficha terá em conta as seguintes componentes e pesos:
- Preparação prévia da ficha – 10%
- Conhecimento da matéria – 30%
- Execução dos exercícios – 50%
- Autonomia – 10%

1. Exemplos de configuração básica do *Border Gateway Protocol*

A presente secção contém uma série de exemplos, de forma a introduzir e explicar brevemente os comandos para configuração básica de BGP em *routers* Cisco. A sua compreensão é fundamental para a execução dos exercícios desta ficha prática, que se encontram na secção 2.

A configuração do protocolo BGP inicia-se com o comando 'router bgp' seguido do número do sistema autónomo ao qual o *router* pertence. Ao contrário do que acontece no OSPF, onde o número que se segue ao comando 'router ospf' é um número de processo, com significado local, no caso do comando 'router bgp' o número de sistema autónomo é um número com significado global, atribuido por um 'Internet Registry'.
A seguir ao comando 'router bgp' seguem-se comandos 'network', que indicam as redes a anunciar por BGP. Se não for indicada uma máscara de rede, o *router* assume o esquema de endereçamento 'classful':

```
router bgp 200
 network 10.50.0.0 mask 255.255.0.0
```

Os vizinhos BGP (BGP peers) são especificados através do comando 'neighbor'. Se for especificado o mesmo número de sistema autónomo parar o *router* vizinho, então é utilizado o protocolo iBGP. Se o número de sistema autónomo for distinto é utilizado o eBGP:

```
router bgp 200
 network 10.50.0.0 mask 255.255.0.0
 neighbor 172.18.1.1 remote-as 300
```

A sincronização de *routers* BGP é um dos mecanismos que permite controlar a difusão de rotas. Se for utilizada sincronização, os *routers* BGP não podem anunciar rotas a outros *routers* BGP antes de estas lhe serem dadas a conhecer por um protocolo de encaminhamento interior. É um mecanismo pouco utilizado que, normalmente, é desactivado. No caso do iBGP este mecanismo tem sempre que ser desactivado. A desactivação é feita com o comando 'no synchronization':

```
router bgp 200
 no synchronization
 network 10.50.0.0 mask 255.255.0.0
 neighbor 172.18.1.1 remote-as 300
```

Por defeito, o BGP faz sumarização de rotas com base no esquema de endereçamento 'classful'. Com o incremento da utilização do esquema de endereçamento CIDR, tal é, normalmente, indesejável. A desactivação da sumarização de rotas 'classful' pode ser feita utilizando o comando 'no auto-summary':

```
router bgp 200
 no synchronization
 network 10.50.0.0 mask 255.255.0.0
 neighbor 172.18.1.1 remote-as 300
 no auto-summary
```

A palavra chave 'default-originate' é adicionada ao comando 'neighbor' para indicar a um *router* vizinho que o presente *router* anuncia uma rota de defeito. Por exemplo, esta palavra chave pode ser utilizada para anunciar a routers iBGP vizinhos que um dado *router* do sistema autónomo anuncia a rota de defeito:

```
router bgp 200
```

```
 no synchronization
 network 10.50.0.0 mask 255.255.0.0
!
! Vizinho eBGP
 neighbor 172.18.1.1 remote-as 300
!
! Vizinho iBGP
 neighbor 10.50.1.2 remote-as 200
 neighbor 10.50.1.2 default-originate
 no auto-summary
!
! Definir rota de defeito
ip route 0.0.0.0 0.0.0.0 172.18.1.1
```

Por defeito, quando um *router* iBGP anuncia uma rota a um vizinho iBGP anuncia-a tal como a recebeu, não se colocando como próximo salto. Caso se pretenda que o router iBGP que anuncia a rota seja utilizado como próximo passo, esse *router* deve ser configurado com a palavra chave 'next-hop-self' associada ao comando 'neighbor', tal como no exemplo seguinte:

```
router bgp 200
 no synchronization
 network 10.50.0.0 mask 255.255.0.0
!
! Vizinho eBGP
 neighbor 172.18.1.1 remote-as 300
!
! Vizinho iBGP
! Anunciamos rota de defeito
! Somos utilizados como próximo passo
 neighbor 10.50.1.2 remote-as 200
 neighbor 10.50.1.2 next-hop-self
 neighbor 10.50.1.2 default-originate
 no auto-summary
!
! Definir rota de defeito
ip route 0.0.0.0 0.0.0.0 172.18.1.1
```

Em certas condições anómalas podem ocorrer situações de instabilidade das redes, que levem a que certas rotas estejam a alternar entre os estados 'up' e 'down' de forma cíclica e com uma frequência relativamente elevada. O comando 'bgp dampening' tem por objectivo assegurar a estabilidade de rotas. Quando este comando é utilizado, o *router* só permite um determinado número de alterações do estado de uma rota num dado período de tempo. Se esse número for ultrapassado, a rota é colocada no estado 'hold-down', não sendo utilizada durante um determinado intervalo de tempo. Findo esse intervalo a rota é activada de novo:

```
router bgp 200
 no synchronization
 bgp dampening
 network 10.50.0.0 mask 255.255.0.0
 … …
```

Num cenário misto envolvendo BGP e OSPF, no caso de se pretender redistribuir as rotas anunciadas por OSPF no ambiente BGP, poderá ser utilizado o comando 'redistribute ospf nnn', sendo nnn o número do processo OSPF. No exemplo seguinte, as rotas do processo OSPF 90 serão redistribuídas no sistema autónomo 200:

```
router bgp 200
 no synchronization
```

```
 bgp dampening
 redistribute ospf 90
 … …
```

A filtragem de rotas é uma das funcionalidades mais importantes do protocolo BGP, já que em ambiente de encaminhamento exterior é fundamental efectuar 'policy routing'. Existem variadas formas para definir quais as rotas que são anunciadas e quais as que são filtradas em BGP. Uma dessas formas consiste na especificação de filtros a aplicar à sequência de sistemas autónomos a anunciar.

No exemplo seguinte o *router* BGP apenas anuncia ao seu vizinho as rotas que contenham os sistemas autónomos 400, 500 ou 600:

```
router bgp 200
 no synchronization
 bgp dampening
 redistribute ospf 90
 network 10.50.0.0 mask 255.255.0.0
!
! Vizinho eBGP
! Define-se uma filter-list de saída, a especificar por uma
! access list com o mesmo número
 neighbor 172.18.1.1 remote-as 300
 neighbor 172.18.1.1 filter-list 1 out
!
! Vizinho iBGP
! Anunciamos rota de defeito
! Somos utilizados como próximo passo
 neighbor 10.50.1.2 remote-as 200
 neighbor 10.50.1.2 next-hop-self
 neighbor 10.50.1.2 default-originate
 no auto-summary
!
! Definir rota de defeito
ip route 0.0.0.0 0.0.0.0 172.18.1.1
!
! Access list a usar pela filter list.
! Permite apenas rotas que contenham os AS 400, 500 ou 600
ip as-path access-list 1 permit _(400|500|600)_
```

Os 'AS paths' podem ser definidos com base numa série de expressões regulares. A tabela seguinte identifica os formatos possíveis:

Tabela 1 – Expressões regulares utilizáveis na especificação de 'AS path'

Expressão regular	**Significado**
.*	Qualquer AS path
^$	AS path vazio, ou seja, AS path originado no próprio sistema autónomo
^250$	AS path apenas composto pelo sistema autónomo 250.
^(150|250|350)$	AS path apenas composto por um sistema autónomo, que pode ser o 150, o 250 ou o 350
^150_	Todos os AS paths que comecem no AS 150

_150_	Todos os AS paths que contenham o AS 150
_150$	Todos os AS paths que terminem no AS 150

2. Exercícios de configuração básica do Border Gateway Protocol

---

Exercício 1 - Com base nos exemplos apresentados na secção 1, configure o cenário BGP da Figura 1. Na última página desta ficha encontrará uma reprodução do cenário da figura. Utilize essa página para elaborar o plano de ligações e de endereçamento. Use as gamas de endereços privados indicadas na figura. Solicite ao docente o valor da variável X a utilizar.

- Cada router deve anunciar as redes às quais se encontra ligado;
- Os *routers* R1 e R2 correm OSPF e BGP;
- As rotas anunciadas por OSPF devem ser redistribuídas para BGP;
- Não deverá ser efectuada sincronização entre os *routers* BGP do AS 3000;
- Deverá ser utilizado 'route dampening';
- O *router* R1 deve colocar-se como 'próximo salto' das rotas que anuncia ao *router* R2;
- O *router* R2 deve colocar-se como 'próximo salto' das rotas que anuncia ao *router* R1;
- Não deverá ser efectuada sumarização de rotas BGP;
- Neste cenário não defina quaisquer rotas de defeito;

- Depois de montado o cenário da Figura 1, execute o seguinte:
  - Verifique a conectividade entre as diversas redes dos diferentes AS, recorrendo ao comando 'ping'.
  - Obtenha a tabela de BGP nos *routers* R1, R2, ISP1 e ISP2, através da execução do comando 'show ip bgp' em cada um desses *routers*.
  - Obtenha a tabela de routing nos *routers* R1, R2, ISP1 e ISP2, através da execução do comando 'show ip route' em cada um desses *routers*, e compare-a com a tabela de BGP;
  - Analise e interprete todos os resultados obtidos.

Dado que o cenário da Figura 1 inclui a ligação do AS 3000 à Internet através de dois ISPs distintos, poderemos utilizar este cenário para estabelecer uma preferência, definindo qual dos dois ISPs deve ser usado em situações normais.

Para tal, recorre-se ao parâmetro 'local preference' do BGP, que é trocado entre *routers* BGP do mesmo sistema autónomo de forma que estes determinem qual deve ser utilizado para acesso ao exterior. O valor de defeito deste parâmetro é 100. Valores menores indicam menores preferências.

No exemplo seguinte, um *router* BGP do sistema autónomo 150 atribui uma preferência 50 (isto é, menor que a preferência de defeito) à ligação com o seu vizinho de um outro sistema autónomo. Ou seja, o tráfego que se destina ao exterior do sistema autónomo 150 deverá sair, preferencialmente, por outro *router* BGP que não este.

Para tal, é utilizado um 'route-map'. Os route-maps permitem influenciar o tráfego por alteração dos atributos de uma rota.

```
! Adicionar o route-map que altera a preferência para o vizinho
router bgp 150
 neighbor 10.10.1.1 route-map PREF in
```

```
!
! Criar o route-map
route-map PREF permit 10
  set local-preference 50
```

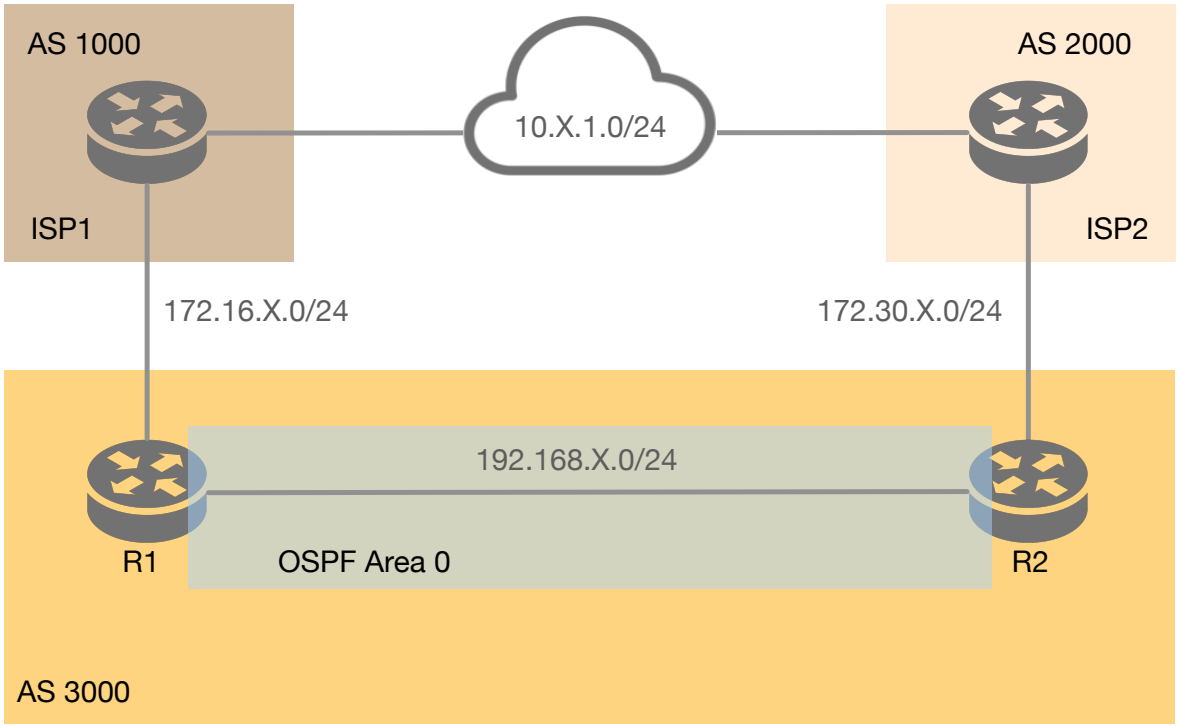
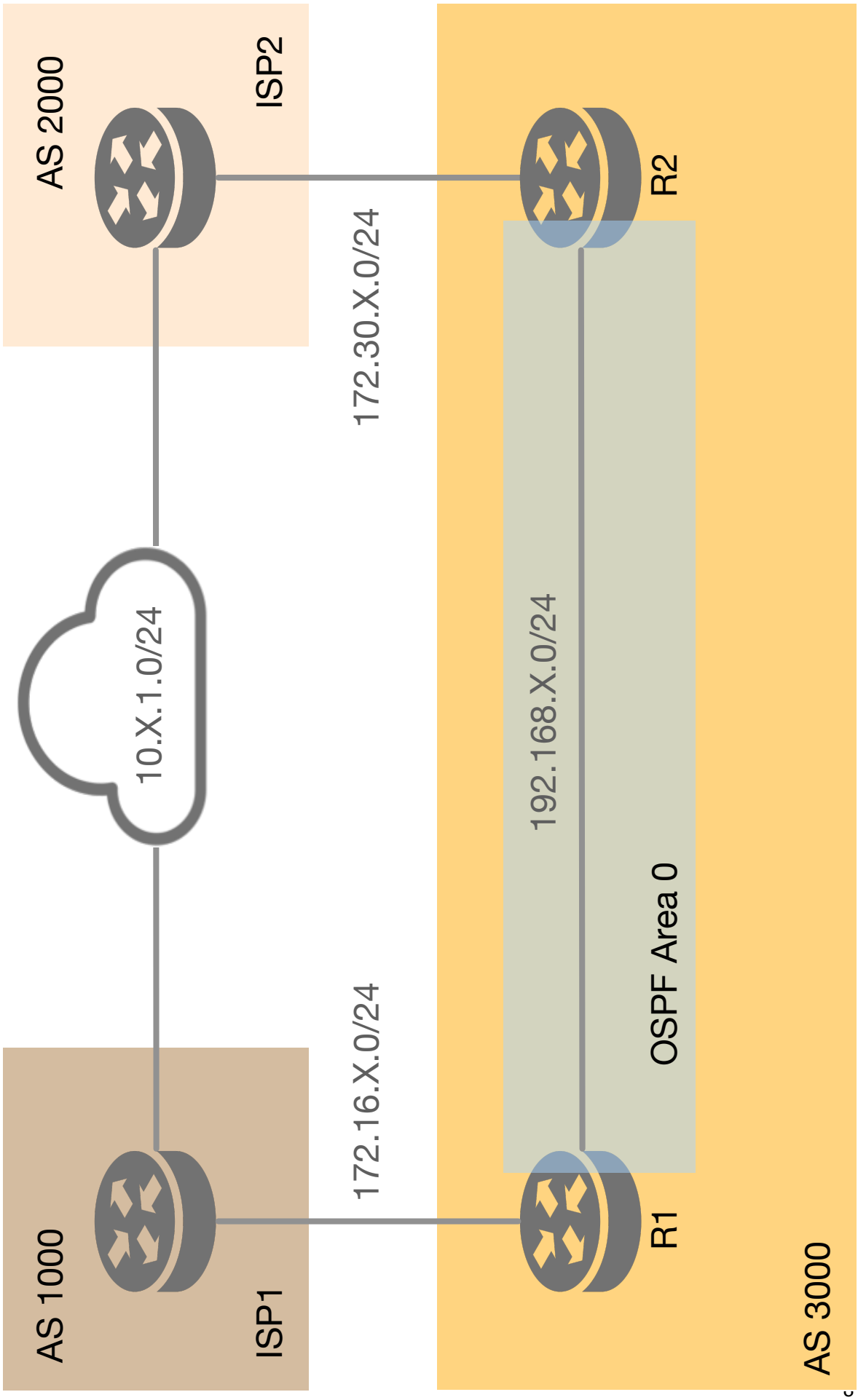


Figura 1 – Rede BGP com dois Internet Service Providers

Exercício 2 - Com base no exemplo apresentado acima, e para o cenário da Figura 1, execute o seguinte (NOTA: os grupos de cada cenário devem colaborar, discutindo e definindo as soluções de configuração de todos os *routers*):

- Estabeleça uma preferência pelo ISP1, no que diz respeito ao tráfego de saída do AS 3000.
- Depois de configurada a preferência, execute o seguinte:
  - Verifique a conectividade entre as diversas redes dos diferentes AS, recorrendo ao comando 'ping'.
  - Obtenha a tabela de BGP nos *routers* R1, R2, ISP1 e ISP2, através da execução do comando 'show ip bgp' em cada um desses routers.
  - Obtenha a tabela de *routing* nos *routers* R1, R2, ISP1 e ISP2, através da execução do comando 'show ip route' em cada um desses *routers*, e compare-a com a tabela de BGP;
  - Analise e interprete todos os resultados obtidos.
- Desative a ligação entre os *routers* R1 e ISP1.
  - Verifique a conectividade entre as diversas redes dos diferentes AS, recorrendo ao comando 'ping'.
  - Verifique as alterações nas tabelas de BGP e de routing dos diversos *routers*.
  - Analise e interprete os resultados.
- Reponha a ligação entre os *routers* R1 e ISP1, e desative agora a ligação entre o router R2 e o router ISP2.

- Verifique a conectividade entre as diversas redes dos diferentes AS, recorrendo ao comando 'ping'.
- Verifique as alterações nas tabelas de BGP e de routing dos diversos *routers*.
- Analise e interprete os resultados.


AS 2000
ISP2
AS 1000
ISP1
AS 3000
R1
R2
OSPF Area 0
10.X.1.0/24
172.16.X.0/24
172.30.X.0/24
192.168.X.0/24