Interligação de Redes IP
Encaminhamento de Tráfego [Protocolo BGP]

Luís Magalhães[1,2], Luís Sousa[1,3], and Hugo Marques[1,4]

[1] University of Minho, Braga, Portugal
[2] pg47415@alunos.uminho.pt
[3] a89597@alunos.uminho.pt
[4] pg47848@alunos.uminho.pt

Abstract. Keywords: router · host · RIP · OSPF · vtysh · BGP

1 Introdução

Este trabalho surge no âmbito da Unidade Curricular de Interligação de Redes IP, do Mestrado em Engenharia Informática da Universidade do Minho e visa demonstrar os resultados que foram obtidos neste mesmo último trabalho prático. Foi proposto ao grupo, o uso da ferramenta *CORE* com intuito de trabalhar com encaminhamento entre diversos sistemas autónomos. O objetivo é implementar um sistema global que utilize o protocolo *Border Gateway Protocol* (BGP) entre sistemas autónomos, mas também protocolos como *Open Shortest Path First* (OSPF) e *Routing Information Protocol* (RIP) para encaminhamento interno em alguns destes.

A intensa pesquisa para antigir o objetivo proposto será uma forma de fundamentar o conhecimento dos protocolos de encaminhamento apresentados ao longos das atividades letivas bem como a configuração dos mesmos.

2 Topologia inicial

Primeiramente, foi necessário implementar uma topologia, tendo por base a topologia do enunciado. Para isso, no *CORE*, recriaram-se os routers existentes e respetivas ligações observáveis na figura 1.

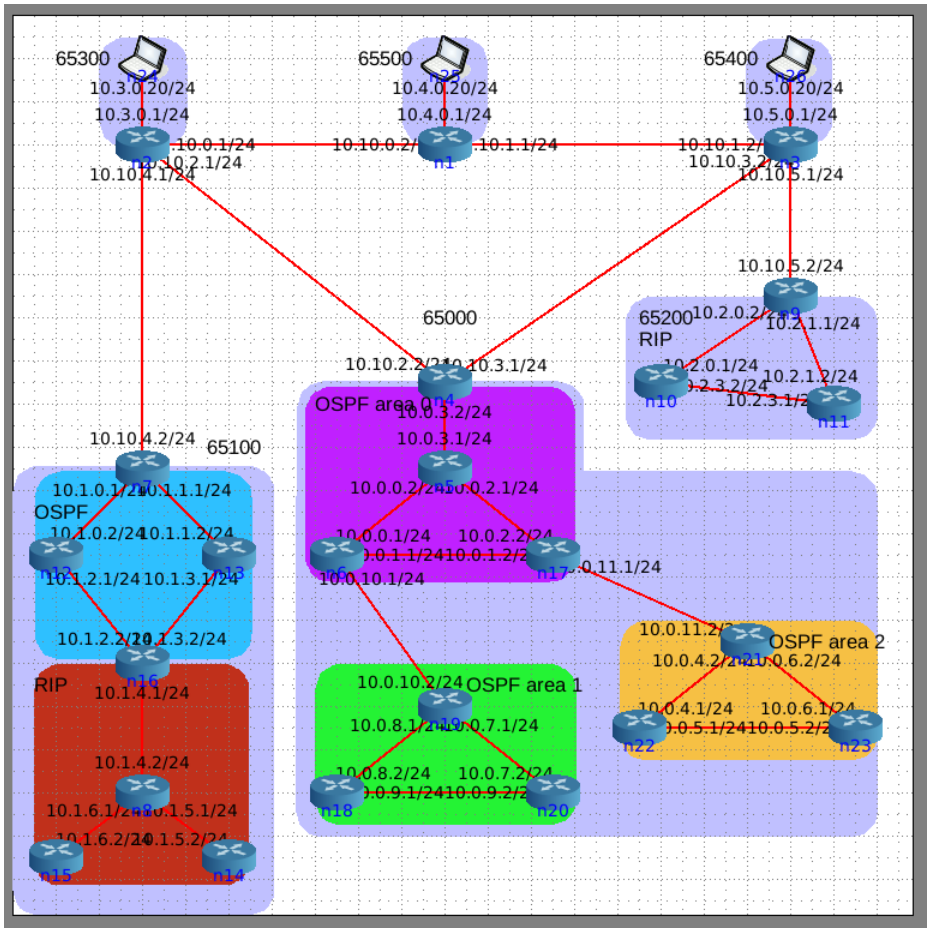

Fig. 1. Topologia Inicial

3 Sistema Autónomo 65200

3.1 Definição do Protocolo Interno - OSPF

O AS 65200 utiliza os endereços IPv4 da gama 10.2.0.0/16, RIP como protocolo interno e uma rota por defeito para comunicar com os sistemas externos, o que, após a realização dos trabalhos anteriores, é trivialmente alcançado.

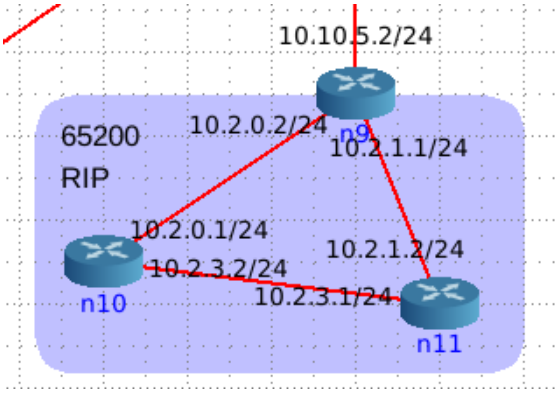

Fig. 2. Sistema Autónomo AS65200

3.2 Definição do Protocolo Externo - *BGP*

Como requisito deste trabalho, para além de assegurar conectividade através do protocolo BGP é necessário impedir o tráfego entre este sistema e o AS65100. Para impedir que o router n9 receba rotas por BGP podemos inserir um access-list a aplica-la ao vizinho da rede 65400. Segue-se a configuração usada para esse fim.

```
router bgp 65200
  bgp router-id 10.10.5.2
  redistribute connected
  network 10.2.0.0 mask 255.255.0.0
  neighbor 10.10.5.1 remote-as 65400
  neighbor 10.10.5.1 distribute-list 1 in
!
access-list 1 deny 10.1.0.0 0.0.255.255
access-list 1 permit any
```

Como estamos a utilizar rotas estáticas do género "ip route 0.0.0.0" também é necessário criar um filtro dentro da rede que descarte todos os pacotes para a rede desejada.

```
router rip
  (...)
  default-information originate
!
ip route 0.0.0.0/0 10.10.5.1
ip route 10.1.0.0/16 10.10.5.1 reject
```

4 Sistema Autónomo 65100

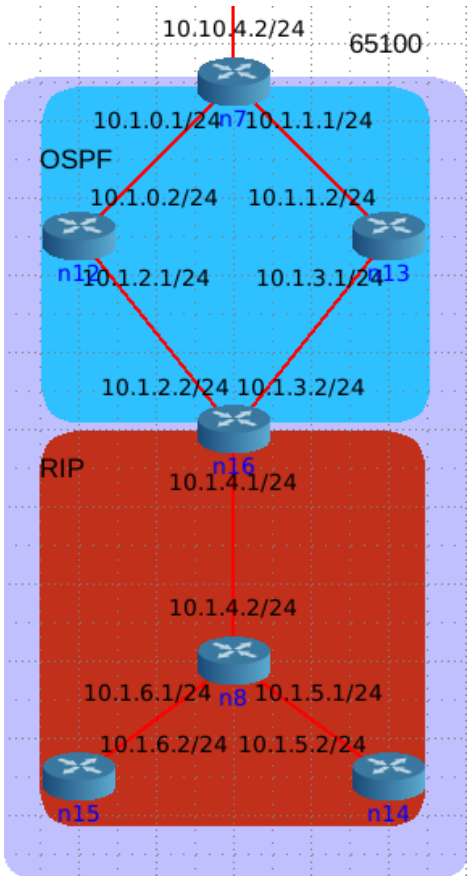

Fig. 3. Sistema Autónomo AS65200

4.1 Definição do Protocolo Interno - *RIP e OSPF*

Para configurar os protocolos RIP e OSPF é necessário que um router possua os dois protocolos em simultâneo. Este router é o n16, o qual necessita de realizar partilha de rotas entre os dois protocolos. Para tal, apenas necessitamos de adicionar a seguinte configuração.

```
router rip
  (...)
  redistribute ospf
!
router ospf
  (...)
  redistribute rip
!
```

4.2 Definição do Protocolo Externo - *BGP*

A comunicação com as redes exteriores com rota estática bem como o processo de bloquear a comunicação com a AS65200 foi realizada de um modo análogo á AS65200.

5 Sistema Autónomo 65000

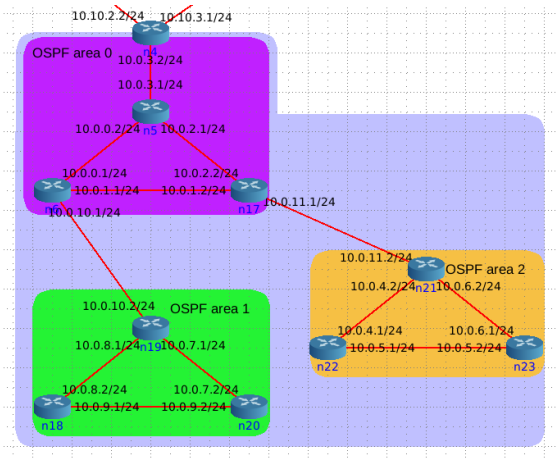

Fig. 4. Sistema Autónomo AS65000

5.1 Definição do Protocolo Interno - OSPF

A configuração do OSPF e das 3 áreas necessárias e com ips da gama 10.0.0.0/16 já foi realizado num trabalho anterior, pelo que não apresenta grande dificuldade.

5.2 Definição do Protocolo Externo - *BGP*

De modo a garantir a conectividade global ás redes inserimos uma configuração semelhante á utilizada em anteriores.
Como requisito adicional desta AS, o router bgp não deve receber pacotes de transito. Para tal, basta desativar a divulgação de rotas aprendidas apagando "redistribute connected", a qual vem por defeito na configuração do zebra criada pelo CORE.

A configuração final é a que se segue:

```
router bgp 65000
  bgp router-id 10.10.2.2
  network 10.0.0.0/16
  neighbor 10.10.3.2 remote-as 65400
  neighbor 10.10.2.1 remote-as 65300
!
```

6 Sistemas Autónomos 65300, 65400 e 65500

Neste capítulo encontram-se os três sistemas autónomos restantes que possuem a mesma natureza. Todos estes são sistemas autónomos de trânsito, i.e, permitem que tráfego de outros vizinhos passem por estes. Para tal, estes anunciam todos os prefixos que conhecem aos seus vizinhos de modo a que nas tabelas de encaminhamento existam rotas possíveis que passem pelo sistema de tráfego em questão.

Os 3 sistemas são analisados em conjunto, visto que são idênticos, e portanto iremos apenas demonstrar as políticas implementadas e respetivas configurações para alguns deles.

6.1 Definição do Protocolo Interno

Estas áreas não possuem protocolos de encaminhamento interno.

6.2 Definição do Protocolo Externo - *BGP*

As configurações destes routers resumem-se à configuração do protocolo BGP, que passa pela criação da sua área das ligações com áreas adjacentes. As suas ligações EBGP permitem que se anuncie prefixos aos sistemas autónomos vizinhos.

Segue-se como exemplo a configurações dos routers de fronteira da AS 65300, AS 65400 e AS 65500, na qual primeiramente é definido o *border* router juntamente com o seu id, é usado o comando *network* de modo a indicar qual o prefixo que vai anunciar aos seus vizinhos como sendo a sua rede interna e após isso são definidas as configurações dos vizinhos através do comando *neighbor*. As configurações são semelhantes para os três AS.

```
router bgp 65300
  bgp router-id 10.0.0.1
  redistribute connected
  network 10.3.0.0 mask 255.255.0.0
  neighbor 10.10.0.2 remote-as 65500
  neighbor 10.10.2.2 remote-as 65000
  neighbor 10.10.4.2 remote-as 65100
!

router bgp 65400
  bgp router-id 10.0.1.2
  redistribute connected
  network 10.5.0.0 mask 255.255.0.0
  neighbor 10.10.5.2 remote-as 65200
  neighbor 10.10.3.1 remote-as 65000
  neighbor 10.10.1.1 remote-as 65500
!
```

```
router bgp 65500
  bgp router-id 10.10.0.2
  redistribute connected
  network 10.4.0.0 mask 255.255.0.0
  neighbor 10.10.0.1 remote-as 65300
  neighbor 10.10.1.2 remote-as 65400
!
```

7 Tabelas de encaminhamento

As tabelas de encaminhamento que consideramos mais relevantes são dos router das áreas 65300 e 65400, com o objetivo de provar que nenhum tráfego utiliza o AS65000 como um AS de transito, pelo que apenas precisamos de apresentar um deles.

```
n2# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, o - OSPF6, I - IS-IS, B - BGP, A - Babel,
       > - selected route, * - FIB route

B>* 10.0.0.0/16 [20/0] via 10.10.2.2, eth1, 00:00:58
B>* 10.1.0.0/16 [20/0] via 10.10.4.2, eth2, 00:00:54
B>* 10.1.0.0/24 [20/1] via 10.10.4.2, eth2, 00:00:54
B>* 10.1.1.0/24 [20/1] via 10.10.4.2, eth2, 00:00:54
B>* 10.2.0.0/16 [20/0] via 10.10.0.2, eth0, 00:00:26
B>* 10.2.0.0/24 [20/0] via 10.10.0.2, eth0, 00:00:26
B>* 10.2.1.0/24 [20/0] via 10.10.0.2, eth0, 00:00:26
C>* 10.3.0.0/24 is directly connected, eth3
B>* 10.4.0.0/16 [20/0] via 10.10.0.2, eth0, 00:00:56
B>* 10.4.0.0/24 [20/1] via 10.10.0.2, eth0, 00:00:56
B>* 10.5.0.0/16 [20/0] via 10.10.2.2, eth1, 00:00:28
B>* 10.5.0.0/24 [20/0] via 10.10.2.2, eth1, 00:00:28
C>* 10.10.0.0/24 is directly connected, eth0
B>* 10.10.1.0/24 [20/1] via 10.10.0.2, eth0, 00:00:56
C>* 10.10.2.0/24 is directly connected, eth1
B>* 10.10.3.0/24 [20/0] via 10.10.2.2, eth1, 00:00:28
C>* 10.10.4.0/24 is directly connected, eth2
B>* 10.10.5.0/24 [20/0] via 10.10.2.2, eth1, 00:00:28
C>* 127.0.0.0/8 is directly connected, lo
n2#
```

Fig. 5. Tabela de encaminhamento do router n2

8 Conclusão

Com este trabalho prático tivemos oportunidade de desenvolver as configurações dos protocolos de encaminhamento BGP, OSPF e RIP. Os processos de configuração de protocolos RIP e OSPF já tinham sido explorados em trabalhos anteriores, mas a implementação deste em conjunto com o BGP expandiu a nossa visão sobre a complexidade de um sistema autónomo. Foi possível, no decorrer deste trabalho, explorar as várias políticas de encaminhamento que podiam ser aplicadas nas várias situações e com isto escolher qual a abordagem que melhor se aplicava. O controlo de rotas com políticas como *access list* e *permit/deny* revelaram-se essenciais para a elaboração deste trabalho. Por último, retiramos daqui diferentes técnicas e comandos que nos permitiram diagnosticar todos os problemas de encaminhamento intra e inter-domínio com que nos deparamos. Podemos assim concluir que todo o enunciado proposto foi realizado com sucesso.