**Universidade do Minho**

Relatório do Trabalho Prático - 2016/17

****

Redes de Computadores 2

Docente: Maria João Mesquita Rodrigues Cunha Nicolau Pinto

Mestrado Integrado de Engenharia de Telecomunicações e Informática – 3ºAno

11 de junho de 2017

# Constituição do Grupo



Francisco Peixoto Silva, A68491

[a68491@alunos.uminho.pt](mailto:a68491@alunos.uminho.pt)



Luís Pedro Lobo de Araújo, A73232

[a73232@alunos.uminho.pt](mailto:a73232@alunos.uminho.pt)



Nuno Frederico Oliveira Tavares, A73985

[a73985@alunos.uminho.pt](mailto:a73985@alunos.uminho.pt)

Índice

[Constituição do Grupo 2](#_Toc484943832)

[Índice de Figuras 3](#_Toc484943833)

[Índice de Tabelas 4](#_Toc484943834)

[Lista de Siglas/Acrónimos 5](#_Toc484943835)

[1. Introdução 5](#_Toc484943836)

[2. Estudo do problema 5](#_Toc484943837)

[3. Projeto 7](#_Toc484943838)

[3.1. Ligações entre AS 7](#_Toc484943839)

[3.2. Sistemas autónomos 7](#_Toc484943840)

[AS 65000 8](#_Toc484943841)

[AS 65100 8](#_Toc484943842)

[AS 65200, AS 65300 e AS65400 9](#_Toc484943843)

[4. Configuração e Testes 9](#_Toc484943844)

[4.1. Topologia da rede 9](#_Toc484943845)

[4.2. Encaminhamento estático 10](#_Toc484943846)

[4.3. OSPF 10](#_Toc484943847)

[4.4. RIP 13](#_Toc484943848)

[4.5. BGP e Políticas de Encaminhamento 14](#_Toc484943849)

[AS 65000 15](#_Toc484943850)

[AS 65100 17](#_Toc484943851)

[AS 65200 20](#_Toc484943852)

[AS 65300 20](#_Toc484943853)

[AS 65400 22](#_Toc484943854)

[5. Conclusão 22](#_Toc484943855)

# Índice de Figuras

[Figura 1 - Cenário experimental sugerido no enunciado do problema 6](#_Toc484943856)

[Figura 2 - Topologia da rede emulada no CORE 9](#_Toc484943857)

[Figura 3 - Resultado da execução dos comandos ping e traceroute entre os terminais n17 e n16 10](#_Toc484943858)

[Figura 4 - Áreas OSPF do AS65100 11](#_Toc484943859)

[Figura 5 - Configuração de um router (OSPF1-1) com o protocolo OSPF 11](#_Toc484943860)

[Figura 6 - Configuração de uma interface (eth2 do OSPF1-1) de um router com autenticação MD5 12](#_Toc484943861)

[Figura 7 - Tabela de encaminhamento de R4 12](#_Toc484943862)

[Figura 8 - Resultado da execução do comando ping entre os terminais n19 e n33 12](#_Toc484943863)

[Figura 9 - Configuração de um router (R1) com o protocolo RIP 13](#_Toc484943864)

[Figura 10 - Tabela de encaminhamento do router n12 14](#_Toc484943865)

[Figura 11 - Resultado da execução do comando ping entre os terminais n45 e n46 14](#_Toc484943866)

[Figura 12 - Serviços ativos num router (R8) do AS 65400 15](#_Toc484943867)

[Figura 13 - Configuração de routers com os protocolos EBGP e IBGP 15](#_Toc484943868)

[Figura 14 - Topologia do AS 65000 16](#_Toc484943869)

[Figura 15 - Configuração do router R1 16](#_Toc484943870)

[Figura 16 – Tabelas BGP dos routers R2 do AS 65100 (esquerda) e do R7 do AS 65200 (direita) 17](#_Toc484943871)

[Figura 17 - Topologia do AS 65100 17](#_Toc484943872)

[Figura 18 - Configuração do router R2 do AS 65100 18](#_Toc484943873)

[Figura 19 - Tabelas BGP dos routers R1 do AS 65000 (esquerda), R2 do AS 65100 (direita) e do R7 do AS 65200 (centro) 18](#_Toc484943874)

[Figura 20 - Configuração do router R3 do AS 65100 19](#_Toc484943875)

[Figura 21 - Tabela BGP dos routers R3 do AS 65100 (esquerda) e R5 do AS 65300 (direita) 19](#_Toc484943876)

[Figura 22 - Configuração do router R4 do AS65100 19](#_Toc484943877)

[Figura 23 - Tabela BGP dos routers R4 do AS 65100 (esquerda) e R6 do AS 65300 (direita). 20](#_Toc484943878)

[Figura 24 - Configuração do router R7 do AS 65200 20](#_Toc484943879)

[Figura 25 - Tabela BGP do router R7 do AS 65200 20](#_Toc484943880)

[Figura 26 - Configuração do router R5 do AS 65300 21](#_Toc484943881)

[Figura 27 - Configuração do router R6 do AS 65300 21](#_Toc484943882)

[Figura 28 - Tabela BGP do router R8 do AS 65400 21](#_Toc484943883)

[Figura 29 - Configuração do router R8 do AS 65400 22](#_Toc484943884)

# Índice de Tabelas

[Tabela 1 - Endereçamento privado nas ligações entre AS 7](#_Toc484905434)

[Tabela 2 - Tabela de endereçamento do AS65000 8](#_Toc484905435)

[Tabela 3 - Tabela de endereçamento do AS 65100 8](#_Toc484905436)

[Tabela 4 - Tabela de endereçamento dos AS 65200, AS 65300 e AS 65400 9](#_Toc484905437)

# Lista de Siglas/Acrónimos

ABR – *Area Border Router*

AS – *Autonomous System*

BGPv4 – *Border Gateway Protocol* *version 4*

CORE – *Common Open Research Emulator*

EBGP – *External Border Gateway Protocol*

IBGP – *Internal Border Gateway Protocol*

IP – *Internet Protocol*

LSA – *Link State Advertisement*

MD5 – *Message-Digest algorithm 5*

OSPF – *Open Shortest Path First*

RIP – *Routing Information Protocol*

SPF – *Shortest Path First*

UC – Unidade Curricular

# Introdução

Este relatório documenta todo o trabalho desenvolvido para resolver um problema proposto no âmbito da Unidade Curricular de Redes de Computadores 2.

O projeto consiste no desenvolvimento de soluções que permitam o encaminhamento intra e inter-domínio entre os vários terminais associados à topologia utilizada.

Com este projeto pretende-se que sejam aplicados conceitos de configuração de encaminhamento interno através de Encaminhamento Estático, RIP (*Routing Information Protocol*) e OSPF (*Open Shortest Path First*). Também se pretende que sejam aplicados os conceitos de encaminhamento externo utilizando o protocolo BGPv4 (*Border Gateway Protocol* *version 4*).

Serão ainda definidas políticas de encaminhamento que definem como o tráfego deverá circular sobre a topologia configurada quando um terminal pretende comunicar com outro que não pertence à sua sub-rede.

# Estudo do problema

Pretende-se emular uma topologia no *software* CORE (*Common Open Research* *Emulator*) que estabeleça as seguintes relações entre os vários ASs (*Autonomous System* – Sistemas Autónomos) como podemos visualizar na Figura 1.

Como podemos verificar pela imagem temos que implementar 5 ASs (AS 65000, AS 65100, AS 65200, AS 65300 e AS 65400), estes deverão ser configurados de maneira a que o protocolo utilizado entre diferentes ASs seja o e-BGP e entre vizinhos que pertençam ao mesmo AS seja o i-BGP.

É pedido que os sistemas autónomos AS 65200, AS 65300 e AS65400 sejam configurados a nível de encaminhamento intra-domínio com encaminhamento estático, enquanto o AS 65000 e o AS 65100 o encaminhamento seja dinâmico utilizando os protocolos OSPF e RIP, respetivamente.

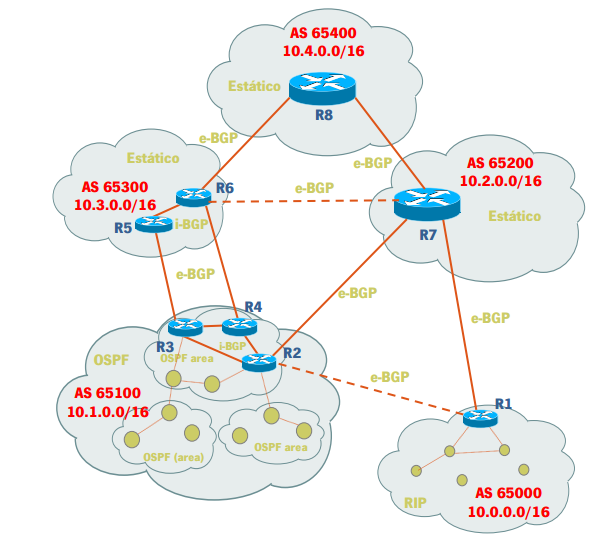


Figura - Cenário experimental sugerido no enunciado do problema

Existem ainda alguns requisitos que o sistema deverá implementar, para isso é necessário definir políticas de encaminhamento que garantam que o fluxo de informação circule da maneira que é pedido no enunciado.

De seguida são apresentados esses mesmos requisitos que o sistema deverá assegurar:

* o AS 65000 tem um contrato de parceria com o AS 65100 que lhe permite encaminhar diretamente o tráfego interno para ele. Esta ligação deverá ser a preferida;
* para atingir o AS 65200, o AS 65000 deverá utilizar a ligação direta preferencialmente. No entanto, se esta ligação falhar poderá encaminhar o tráfego para o AS 65200 através do AS 65100;
* o AS 65100 é um sistema *multihomed* e seletivamente de trânsito já que aceita encaminhar tráfego entre os AS 65200 e 65000 (mas apenas entre estes). Ou seja, o AS 65300 não deve ter possibilidade de encaminhar tráfego através deste sistema autónomo;
* para atingir o sistema autónomo AS 65400 deverá ser preferida a rota via sistema autónomo AS 65300 em detrimento da rota via sistema autónomo AS 65200 (no caso de estarem disponíveis as duas ligações de saída). No entanto para as redes do sistema autónomo AS 65200, a ligação direta deve ser a preferida. Da mesma forma, para as redes do sistema autónomo AS 65300, a ligação direta deve ser a preferida;
* se a ligação direta para o AS 65000 não estiver disponível, o AS 65200 pode usar o AS 65100 como *backup* para chegar ao AS 65000. Se estiverem as duas ligações disponíveis, a ligação direta deverá ser a preferida;
* o AS 65300 não é ISP do AS 65000 e por esse motivo não deverá divulgar ao AS 65400, a rota para o AS 65000. Desta forma o AS 65400 não pode usar o AS 65300 para atingir o AS 65000, em nenhuma circunstância;
* o AS 65400 tem duas rotas alternativas como o mesmo AS\_PATH Len para atingir o 65100, e prefere usar a rota via AS 65300.

Por fim é importante que o encaminhamento interno seja imune a falsos anúncios de falsos encaminhadores, para combater tal será necessário implementar medidas de segurança tais como autenticação entre interfaces de *routers* utilizando o algoritmo MD5 (*Message-Digest algorithm 5*).

# Projeto

## Ligações entre AS

Em baixo na Tabela 1 podemos encontrar a tabela de endereçamento privado das ligações entre sistemas autónomos. A estas ligações foram atribuídos endereços IP (*Internet Protocol*) na gama de endereços privados 192.168.1.0/24.

Tabela - Endereçamento privado nas ligações entre AS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Endereço de rede | Endereço de difusão | Máscara de rede | Gama de endereços | Ligação |
| 192.168.1.0 | 192.168.1.3 | /30 | 192.168.1.1-2 | AS65300 e AS65400 |
| 192.168.1.4 | 192.168.1.7 | /30 | 192.168.1.5-6 | AS65400 e AS65200 |
| 192.168.1.8 | 192.168.1.11 | /30 | 192.168.1.9-10 | AS65300 |
| 192.168.1.12 | 192.168.1.15 | /30 | 192.168.1.13-14 | AS65100 e AS65300 |
| 192.168.1.16 | 192.168.1.19 | /30 | 192.168.1.17-18 | AS65100 e AS65300 |
| 192.168.1.20 | 192.168.1.23 | /30 | 192.168.1.21-22 | AS65100 |
| 192.168.1.24 | 192.168.1.27 | /30 | 192.168.1.25-26 | AS65100 |
| 192.168.1.28 | 192.168.1.31 | /30 | 192.168.1.29-30 | AS65100 |
| 192.168.1.32 | 192.168.1.35 | /30 | 192.168.1.33-34 | AS65100 e AS65200 |
| 192.168.1.36 | 192.168.1.39 | /30 | 192.168.1.37-38 | AS65000 e AS65200 |
| 192.168.1.40 | 192.168.1.43 | /30 | 192.168.1.41-42 | AS65300 e AS65200 |
| 192.168.1.44 | 192.168.1.47 | /30 | 192.168.1.45-46 | AS65000 e AS65100 |

## Sistemas autónomos

Para cada AS foi definida uma tabela de endereçamento que permitisse que as várias ligações entre *routers* e terminais fossem possíveis dentro de cada sistema autónomo. Podemos reparar que nos sistemas autónomos AS 65200, AS 65300 e AS 65400 temos pequenas sub-redes com poucos terminais somente para efeitos de teste.

### AS 65000

Neste AS é pedido que o protocolo de encaminhamento dinâmico utilizado seja o RIP, em baixo na Tabela 2 podemos visualizar a tabela de endereçamento das várias redes presentes no AS 65000.

Tabela - Tabela de endereçamento do AS65000

|  |  |  |  |
| --- | --- | --- | --- |
| Endereço de rede | Endereço de difusão | Máscara de rede | Gama de endereços |
| 10.0.0.0 | 10.0.0.3 | /30 | 10.0.0.1-2 |
| 10.0.0.4 | 10.0.0.7 | /30 | 10.0.0.5-6 |
| 10.0.0.8 | 10.0.0.11 | /30 | 10.0.0.9-10 |
| 10.0.0.12 | 10.0.0.15 | /30 | 10.0.0.13-14 |
| 10.0.0.16 | 10.0.0.19 | /30 | 10.0.0.17-18 |
| 10.0.1.0 | 10.0.1.255 | /24 | 10.0.1.1-254 |
| 10.0.2.0 | 10.0.2.255 | /24 | 10.0.2.1-254 |
| 10.0.3.0 | 10.0.3.255 | /24 | 10.0.3.1-254 |

### AS 65100

O OSPF é o protocolo eleito para lidar com o encaminhamento dinâmico neste AS, a Tabela 3 apresenta a tabela de endereçamento para as redes existentes no AS 65100.

Tabela - Tabela de endereçamento do AS 65100

|  |  |  |  |
| --- | --- | --- | --- |
| Endereço de rede | Endereço de difusão | Máscara de rede | Gama de endereços |
| 10.1.0.0 | 10.1.0.3 | /30 | 10.1.0.1-2 |
| 10.1.0.4 | 10.1.0.7 | /30 | 10.1.0.5-6 |
| 10.1.0.8 | 10.1.0.11 | /30 | 10.1.0.9-10 |
| 10.1.0.12 | 10.1.0.15 | /30 | 10.1.0.13-14 |
| 10.1.0.16 | 10.1.0.19 | /30 | 10.1.0.17-18 |
| 10.1.0.20 | 10.1.0.23 | /30 | 10.1.0.21-22 |
| 10.1.0.24 | 10.1.0.27 | /30 | 10.1.0.25-26 |
| 10.1.0.28 | 10.1.0.31 | /30 | 10.1.0.29-30 |
| 10.1.0.32 | 10.1.0.35 | /30 | 10.1.0.33-34 |
| 10.1.0.36 | 10.1.0.39 | /30 | 10.1.0.37-38 |
| 10.1.0.40 | 10.1.0.43 | /30 | 10.1.0.41-42 |
| 10.1.0.44 | 10.1.0.47 | /30 | 10.1.0.45-46 |
| 10.1.0.48 | 10.1.0.51 | /30 | 10.1.0.49-50 |
| 10.1.0.52 | 10.1.0.55 | /30 | 10.1.0.53-54 |
| 10.1.0.56 | 10.1.0.59 | /30 | 10.1.0.57-58 |
| 10.1.0.60 | 10.1.0.63 | /30 | 10.1.0.61-62 |
| 10.1.0.64 | 10.1.0.67 | /30 | 10.1.0.65-66 |
| 10.1.0.68 | 10.1.0.71 | /30 | 10.1.0.69-70 |

### AS 65200, AS 65300 e AS65400

Dentro destes sistemas autónomos o encaminhamento será estático, ou seja, o administrador da rede (neste caso o grupo) tem que definir as rotas e configurá-las em cada *router*. A Tabela 4 apresenta a tabela de endereçamento para estes ASs.

Tabela - Tabela de endereçamento dos AS 65200, AS 65300 e AS 65400

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Endereço de rede | Endereço de difusão | Máscara de rede | Gama de endereços | Sistema Autónomo |
| 10.2.0.0 | 10.2.255.255 | /16 | 10.2.0.1-10.2.255.254 | AS 65200 |
| 10.4.0.0 | 10.4.255.255 | /16 | 10.4.0.1-10.4.255.254 | AS 65400 |
| 10.3.0.0 | 10.3.0.255 | /24 | 10.3.0.1-255 | AS65300 |
| 10.3.1.0 | 10.3.1.255 | /24 | 10.3.1.1-255 |

# Configuração e Testes

Nesta secção iremos abordar todos os *scripts*, comandos e serviços utilizados pelo grupo de forma a configurar os vários equipamentos emulados no *software* CORE.

## Topologia da rede

O grupo utilizou o modo de edição do CORE para desenhar a topologia da rede que irá ser emulada neste *software*, a Figura 2 demonstra a topologia desenvolvida pelo grupo tendo em conta as tabelas de endereçamento apresentadas na secção anterior.

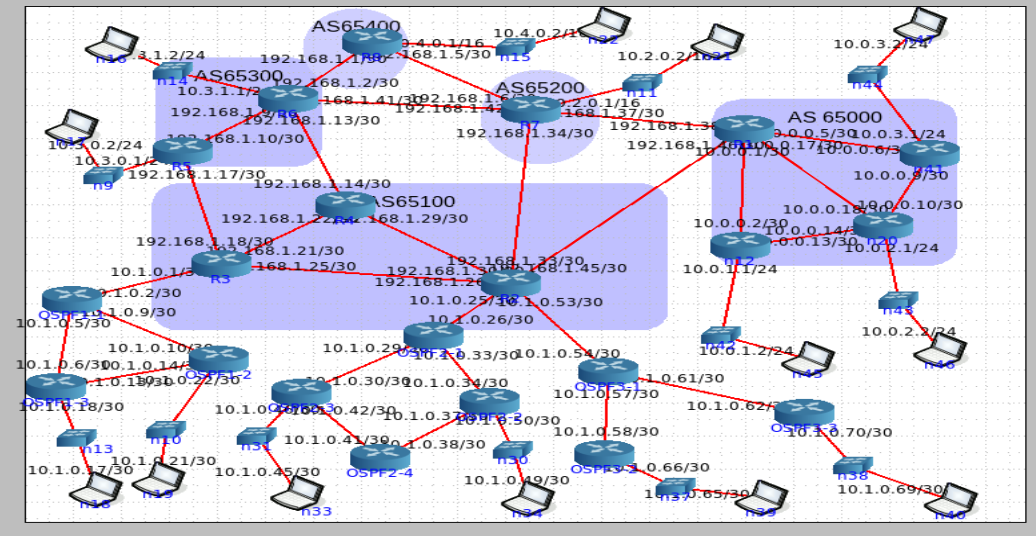


Figura - Topologia da rede emulada no CORE

## Encaminhamento estático

Para configurar o encaminhamento estático entre dois *routers* vamos utilizar o exemplo dos equipamentos associados ao AS 65300. Como podemos ver temos dois *routers* (R5 e R6) ligados entre si com endereços IP pertencentes à rede privada 192.168.1.8/30. De forma a que seja possível a comunicação entre eles em R5 e R6 configuramos com os seguintes comandos respetivamente, utilizando o Quagga (*software* de encaminhamento de redes):

* *ip route* 10.3.1.0/24 192.168.1.9
* *ip route* 10.3.0.0/24 192.168.1.10

Nestes comandos podemos reparar que o primeiro endereço IP é o endereço da rede para a qual se pretende comunicar e o segundo endereço relaciona-se com o endereço do próximo nó para o qual os pacotes que pretendam tomar rumo até à rede anteriormente definida deverão dirigir-se.

Para testar o encaminhamento estático utilizamos dois terminais (n16 e n17) do AS 65300. Primeiramente executamos o comando *ping* para testar a conectividade entre os terminais e de seguida o comando *traceroute* para analisar se o caminho que as mensagens tomam é o esperado. A Figura 3 apresenta os resultados deste mesmo teste, podendo confirmar-se o bom funcionamento das configurações anteriormente realizadas.

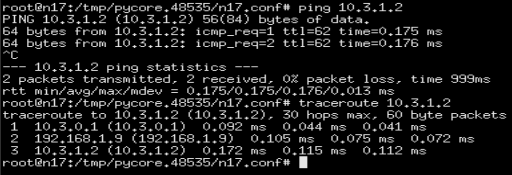


Figura - Resultado da execução dos comandos *ping* e *traceroute* entre os terminais n17 e n16

## OSPF

Neste caso vamos configurar os *routers* que pertencem ao AS 65100 para funcionar com o protocolo de encaminhamento dinâmico OSPF. Vamos dividir este sistema autónomo em várias áreas como é possível visualizar na Figura 4.

O protocolo OSPF é baseado no algoritmo *Shortest Path First* (SPF, também conhecido como algoritmo de Dijkstra). O funcionamento deste protocolo dá-se através de mensagens de aviso do estado das ligações entre os vários *routers* da rede em questão, a estas mensagens são dadas o nome de *Link State Advertisement*. Com estas mensagens cada *router* sabe o estado de toda a topologia da rede e consegue calcular, através do algoritmo SPF, as rotas com custos menores para qualquer outro *router* da rede.

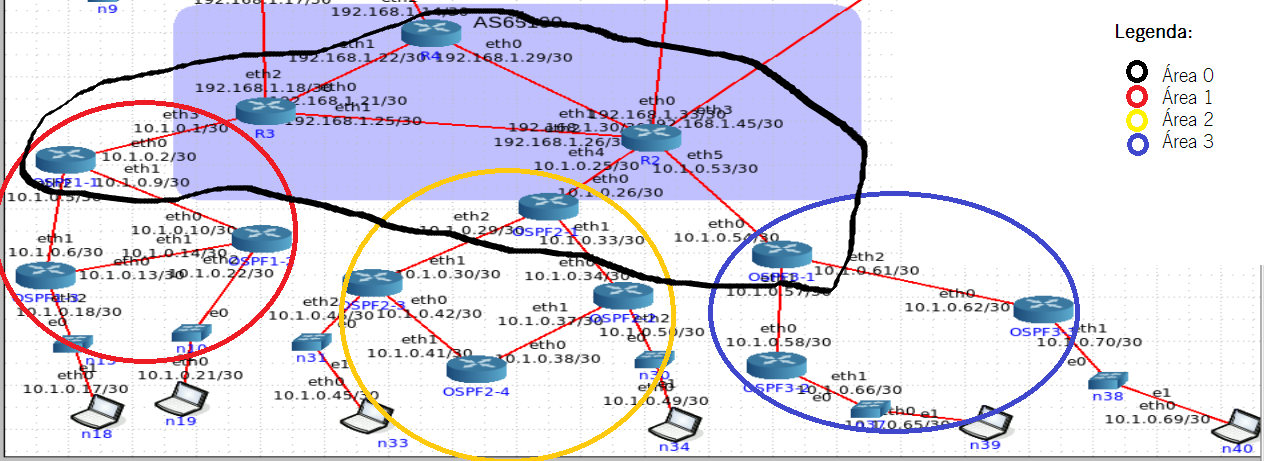


Figura - Áreas OSPF do AS65100

Uma rede OSPF pode ser dividida em vários subdomínios denominados por áreas. Uma área é uma coleção lógica de redes OSPF, *routers* e ligações que têm a mesma identificação de área. Um *router* dentro de uma área deverá manter uma base de dados topológica para a área à qual pertence. Um *router* não tem informação detalhada sobre a topologia da rede fora da sua área, isto permite que o tamanho da base de dados do *router* seja menor.

Para configurar os *routers* do AS 65100 de forma a trabalharem com o protocolo OSPF foram utilizados os seguintes comandos:

* *configure terminal* – para configurar o terminal em questão;
* *router* ospf – para configurar um *router* com o protocolo OSPF;
* *network* [endereço IP da rede vizinha] *area* [identificação da área] – serve para definir quais as redes vizinhas e a quais áreas OSPF pertencem;
* *area* [identificação da área] *authentication message–digest* – define que a área em questão utiliza autenticação nas suas interfaces de saída;
* *redistribute bgp* – para redistribuir as rotas provenientes do protocolo BGP.

Adicionalmente foi necessário configurar também as interfaces dos *routers* de cada área para que pudessem utilizar autenticação MD5 como medida de segurança, apenas foram configuradas as interfaces que pertencem a áreas OSPF:

* *ip ospf authentication message-digest* – para ativar o serviço de autenticação;
* *ip ospf message-digest-key* [nº de identificação da chave] md5 [chave] – serve para especificar o nº de identificação da chave e a chave que serão utilizados na autenticação entre interfaces.

No nosso caso utilizamos uma única chave utilizando o “1” como nº identificador e “rc2fln” como chave. Podemos visualizar um exemplo de configuração na Figura 7.

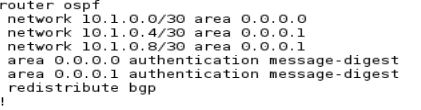


Figura - Configuração de um router (OSPF1-1) com o protocolo OSPF

Na Figura 6 vemos as configurações de uma interface para que esta funcione corretamente com autenticação MD5.

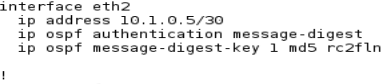


Figura - Configuração de uma interface (eth2 do OSPF1-1) de um *router* com autenticação MD5

De forma a verificar que os *routers* do AS 65100 estão a funcionar devidamente com o protocolo OSPF foram verificadas as suas tabelas de encaminhamento através do seguinte comando:

* *show ip ospf route*

Na Figura 7 vemos os resultados deste comando executado num *router* (R4) que integra a área 0 do AS 65100, confirmamos que ele está a aprender corretamente as rotas de OSPF. O mesmo processo foi realizado para os restantes *routers* deste AS.

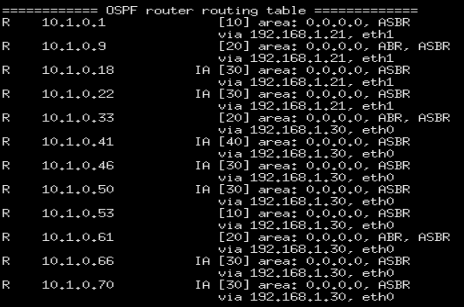


Figura - Tabela de encaminhamento de R4

Para confirmar que o OSPF estava configurado devidamente executamos o comando *ping* entre terminais deste AS. A Figura 8 apresenta um exemplo da execução deste teste entre os terminais n19 e n33. O mesmo processo foi realizado entre os vários terminais deste AS.

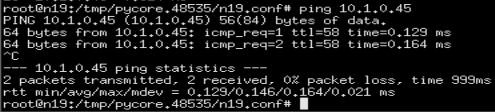


Figura - Resultado da execução do comando *ping* entre os terminais n19 e n33

## RIP

No Sistema Autónomo 65000 configuraram-se os seus *routers* para atuarem segundo o protocolo encaminhamento dinâmico RIP, que é baseado nos algoritmos de Bellman-Ford.

Este protocolo é baseado em trocas de mensagens, onde cada mensagem tem no seu conteúdo informações sobre as rotas que o *router* conhece e a distância do *router* para cada uma delas. O que recebe as mensagens calcula a distância para as outras redes e guarda toda a informação na sua tabela de roteamento. A distância da rota é medida pela quantidade de saltos entre *routers* (cada salto denominado por *hop*) e é calculada com base no número de *routers* existentes num determinado caminho numa determinada rota. O máximo número de *hops* permitidos pelo RIP é 15, a partir deste número em diante as distâncias são consideradas infinitas.

Estas informações são trocadas em intervalos regulares, mal o *router* é ligado, ou quando o *router* recebe atualizações na sua tabela.

Para configurar os routers do AS 65000 de forma a trabalharem com o protocolo RIP, utilizou-se os seguintes comandos:

* *configure terminal* – para configurar o terminal em questão;
* *router rip* – ativa no router em questão o protocolo RIP;
* *redistribute BGP* – para redistribuir as rotas provenientes do protocolo BGP;
* *network* [endereço IP de uma rede] – Especifica que esta rede deverá estar ativa para o protocolo RIP.

O grupo decidiu utilizar o protocolo RIP v2 porque este permite que os *routers* habilitados com este protocolo atuem como um grupo *multicast*, pode ser utilizado em redes que utilizam *subnetting* pois envia informações sobre a máscara de rede nos anúncios e por ser possível implementar um mecanismo de autenticação.

Como medida de segurança, de forma a que os *routers* aceitem somente os anúncios de routers autenticados, configurou-se as interfaces dos routers para utilizarem autenticação MD5, como já anteriormente configurado para o AS 65100. Os comandos utilizados para a autenticação entre interfaces dos *routers* deste AS:

* *ip rip authentication mode* md5 – para ativar o serviço de autenticação
* *ip rip authentication key-chan* [chave] – serve para especificar a chave que será utilizado na autenticação.

Na figura abaixo (Figura 9) podemos visualizar um exemplo de configuração do *router* R1.

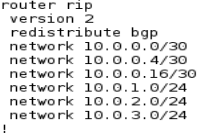


Figura - Configuração de um *router* (R1) com o protocolo RIP

Para as interfaces dos *routers* que pertencem ao AS 65000 utilizou-se a chave “teste”, na figura abaixo está ilustrado as configurações necessárias para que a interface funcione corretamente com a autenticação MD5.

Com o intuito de analisar se as configurações foram bem realizadas, foram analisadas as tabelas de encaminhamento dos vários *routers* pertencentes a este AS com o seguinte comando:

* *show ip rip.*

A Figura 10 demonstra o resultado de um destes testes, neste caso no *router* n12. Podemos verificar que ele é capaz de aprender as rotas para todos os nodos da rede deste AS 65000.

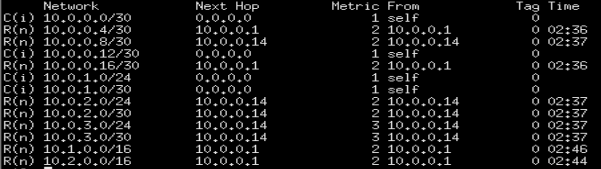


Figura - Tabela de encaminhamento do *router* n12

Para garantir que a conetividade entre terminais é estabelecida com sucesso, foram feitos testes utilizando o comando *ping* entre os vários terminais deste AS, na Figura 11 podemos ver os resultados de um exemplo deste mesmo teste entre os terminais n45 e n46. Analisando a figura concluímos que a conetividade entre estes terminais é possível.

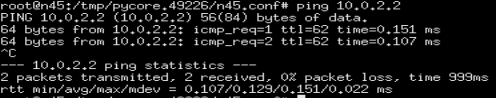


Figura - Resultado da execução do comando *ping* entre os terminais n45 e n46

## BGP e Políticas de Encaminhamento

O encaminhamento inter-domínio foi realizado através do protocolo BGP com o objetivo de estabelecer as rotas entre os vários sistemas autónomos presentes na rede. Entre AS distintos foi utilizado o protocolo EBGP (*External Border Gateway Protocol*) que é uma extensão do BGP e ligações dentro do mesmo AS (como é o caso da ligação nos AS 65300 e AS 65100) utilizam o protocolo IBGP (*Internal Border Gateway Protocol*) que também é uma extensão do BGP. Neste caso sempre que queiramos configurar um *router* para utilizar o protocolo BGP devemos ativar o serviço BGP como podemos verificar na Figura 12.



Figura - Serviços ativos num *router* (R8) do AS 65400

Para configurar um *router* que atue com o EBGP devemos utilizar os seguintes comandos:

* *configure terminal* – para configurar o terminal em questão;
* *router bgp* [nº do AS que pertence] – para configurar um *router* com o protocolo BGP;
* *network* [endereço IP de rede] – serve para definir a qual rede pertence o *router*;
* *neighbor* [endereço IP da interface de saída do vizinho] [nº do AS que pertence] – serve para definir quais são os vizinhos que lhe estão diretamente conectados.

Em relação ao IBGP o comando que diferencia a configuração do EBGP é o seguinte:

* *neighbor* [endereço IP da interface de saída do vizinho] *next-hop-self* – força o BGP a utilizar o endereço IP como próximo salto.

A Figura 13 demonstra as configurações utilizadas para um router com EBGP e as configurações de um router com IBGP.

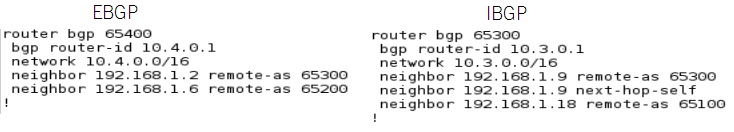
**

Figura - Configuração de *routers* com os protocolos EBGP e IBGP

No caso do BGP, como é um protocolo interdomínio, temos que configurar os *Border Routers* de cada AS para definir as políticas que estes pretendem implementar. Como tal, iremos começar pelo AS 65000.

### AS 65000

Estamos perante um AS *stub*, este apenas acede ao exterior através do AS 65200, no entanto também mantém uma ligação de parceria com o AS 65100. A Figura 14 demonstra a topologia de rede deste AS.

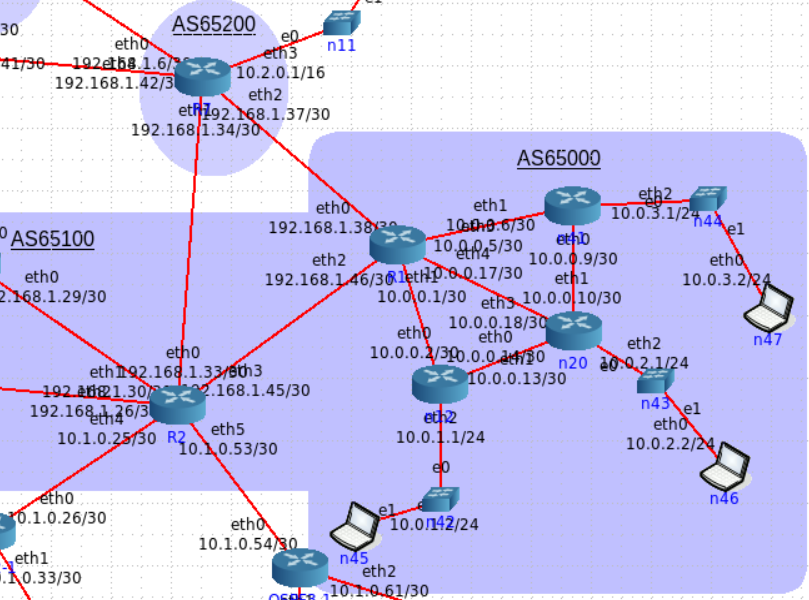


Figura - Topologia do AS 65000

Como podemos ver na Figura 15, além da configuração geral do BGP, já explicada acima, contamos com um *route-map* de saída anunciado ao AS 65100 e 65200. A sua função é filtrar e anunciar aos respetivos ASs, através de uma *access-list*, apenas a rota diretamente conectada.

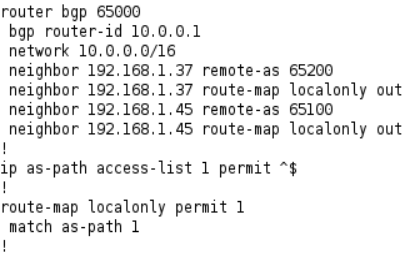


Figura - Configuração do *router* R1

Na Figura 16, podemos constatar que as rotas recebidas pelos *Area* *Border Routers* (ABR) do AS 65100 e 65200 são as esperadas, contendo apenas a rota diretamente conectada para o AS 65000.

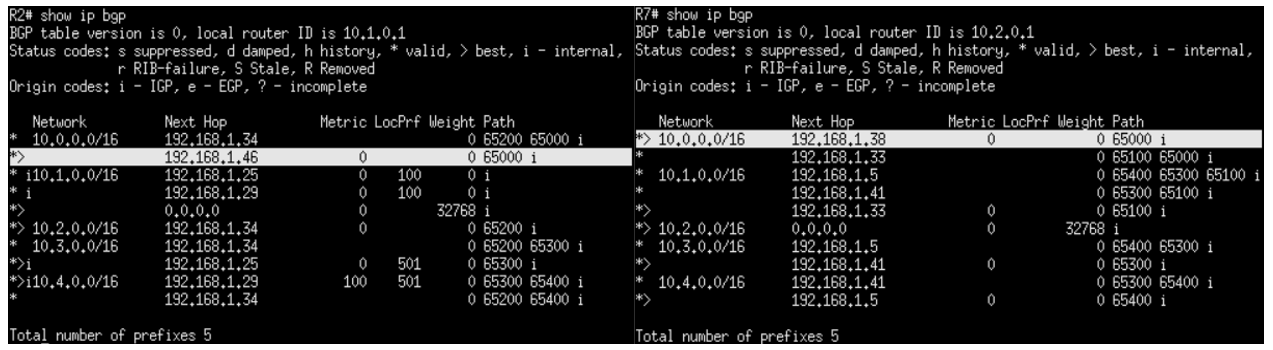


Figura – Tabelas BGP dos *routers* R2 do AS 65100 (esquerda) e do R7 do AS 65200 (direita)

### AS 65100

Neste AS contamos com dois vizinhos que nos garantem acesso ao exterior: o AS 65200 e o 65300, por essa razão este AS é *multihomed.* Para além disso, o AS 65100 tem uma ligação de parceria com o AS 65000, que permite que este e o AS 65200 comuniquem através dele, caso a ligação AS 65000 - AS 65200 falhe. A Figura 17 apresenta a topologia de rede deste AS.

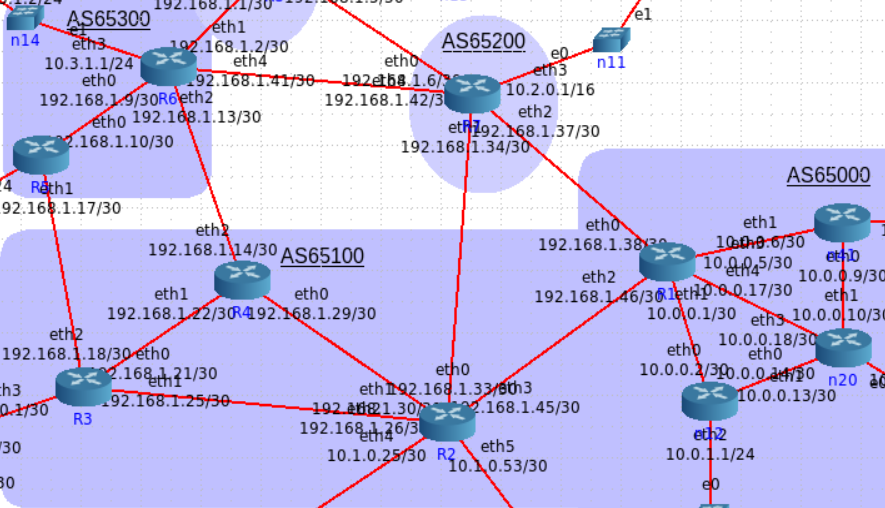


Figura - Topologia do AS 65100

Com a configuração presente na Figura 18 podemos ver várias das políticas implementadas. Usamos o *route-map* “RMtransit” para anunciar ao AS 65000 as redes do AS 65200 e vice-versa. Através do *route-map* “rm3” e “rm4”, definimos as preferências do tráfego destinado ao AS 65300 seguir via router R3, e do tráfego destinado ao AS 65400 via R4, através de um *local-preference* mais elevado.

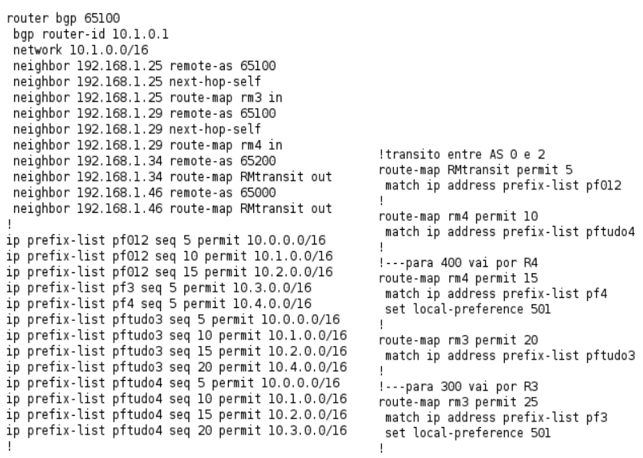


Figura - Configuração do *router* R2 do AS 65100

Através das tabelas da figura 19 podemos ver as rotas apresentadas e escolhidas por meio das políticas descritas acima.

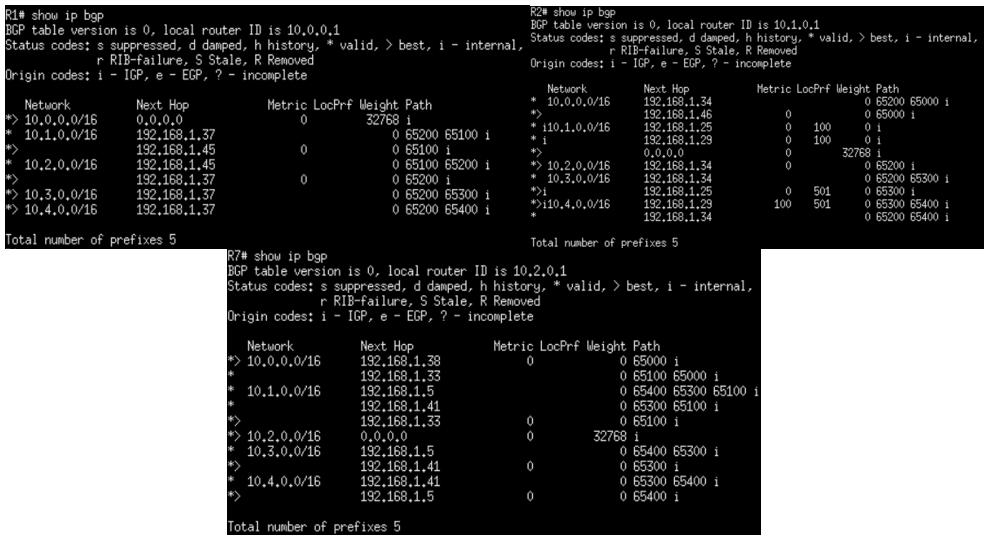


Figura - Tabelas BGP dos *routers* R1 do AS 65000 (esquerda), R2 do AS 65100 (direita) e do R7 do AS 65200 (centro)

Na Figura 20 encontramos os *route-map* associados ao anúncio das rotas aos vizinhos, mais concretamente o *route-map* “directonly” onde apenas anuncia a rede local, visto não se tratar de um *router* de trânsito. O *route-map* “rm3” e “rm4” assim como no router R2 (acima descrito), dá preferência ao tráfego destinado ao AS 65300 a seguir por R3, e ao destinado ao AS 65400 seguir por R4.

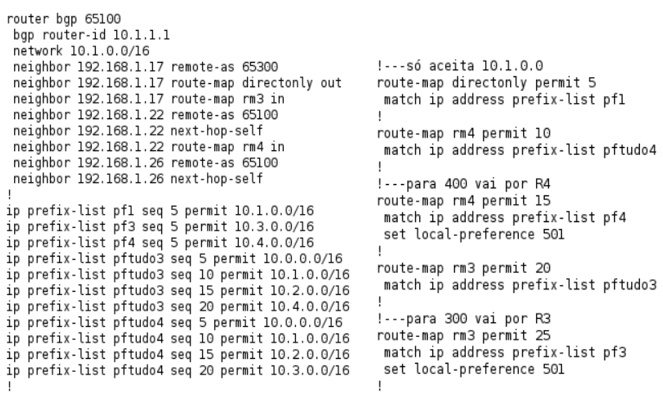


Figura - Configuração do *router* R3 do AS 65100

Através das tabelas apresentadas na Figura 21 podemos ver as rotas apresentadas e escolhidas por meio das políticas descritas acima.

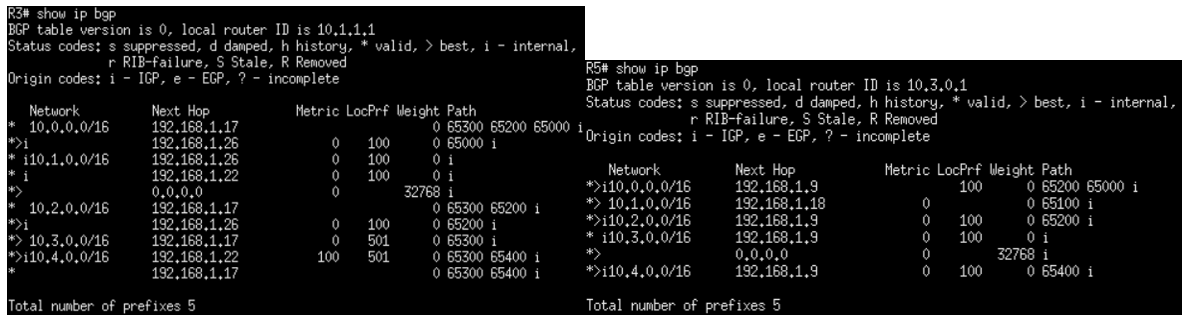


Figura - Tabela BGP dos *routers* R3 do AS 65100 (esquerda) e R5 do AS 65300 (direita)

As configurações do router R4 vão de encontro às configurações já apresentadas do router R3, como se pode ver na Figura 22.

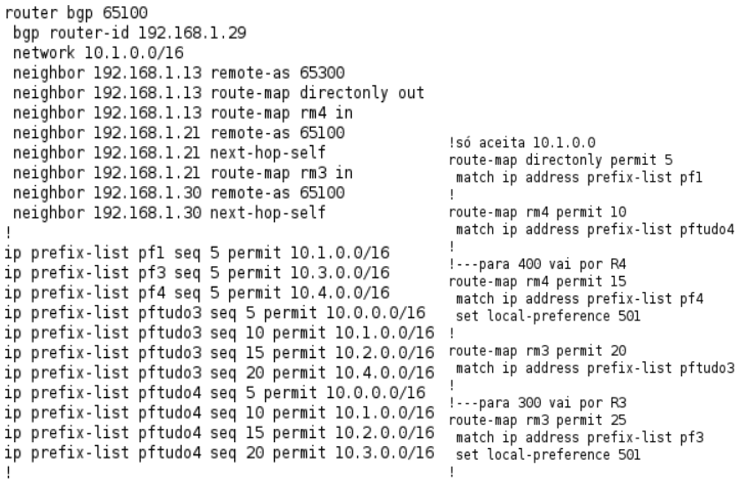


Figura - Configuração do *router* R4 do AS65100

Na Figura 23 podemos ver as tabelas obtidas através das políticas aplicadas.

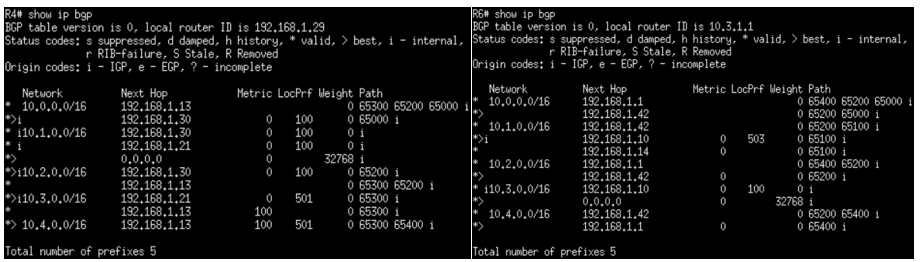


Figura - Tabela BGP dos *routers* R4 do AS 65100 (esquerda) e R6 do AS 65300 (direita).

### AS 65200

O AS 65200 é apenas um sistema autónomo de trânsito, portanto a sua configuração é relativamente simples. Este apenas anuncia aos seus vários vizinhos todas as suas redes e as redes anunciadas por estes, como demonstrado na Figura 24. Na Figura 25 encontra-se a tabela resultante desta configuração.

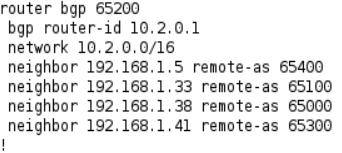


Figura - Configuração do *router* R7 do AS 65200

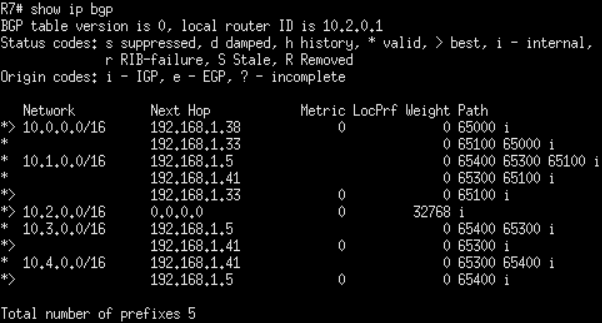


Figura - Tabela BGP do *router* R7 do AS 65200

### AS 65300

Na configuração do *router* R5, presente na Figura 26, apenas utilizamos a configuração geral do BGP pois todas as políticas necessárias ao AS 65300 estão presentes na configuração do *router* R6 (Figura 27). Nesta utilizamos o *route-map* “deny65000” juntamente com uma *access-list* para não anunciar ao AS 65400 a rota para o 65000. O *route-map* “rm1” é utilizado para encaminhar o tráfego direcionado ao AS 65100 a seguir pelo *router* R5. Para influenciar o AS 65100 a usar o router R5 para atingir o AS 65300 e 65400, foi utilizado o *route-map* “rm34”, que anuncia ao AS 65100 as rotas com uma métrica de 100, para estas serem refutadas quando comparadas com a métrica 0 das rotas enviadas pelo *router* R5.

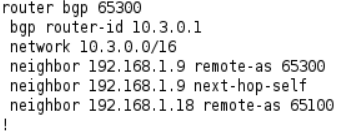


Figura - Configuração do *router* R5 do AS 65300

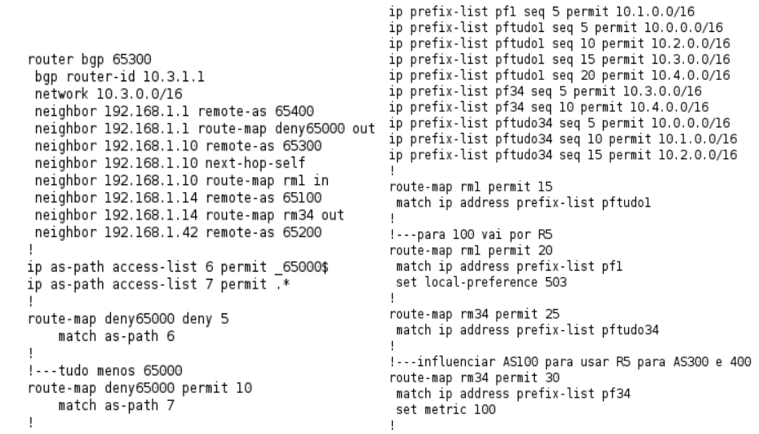


Figura - Configuração do *router* R6 do AS 65300

Com as tabelas BGP apresentadas nas figuras 28, 21 (*router* R5) e 23 (*router* R6), demonstradas na secção do AS 65100, podemos verificar a escolha das rotas anunciadas e selecionadas através das políticas descritas acima.

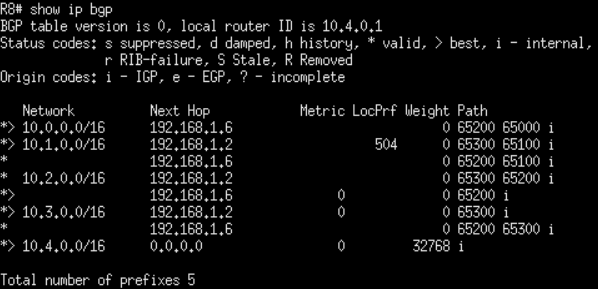


Figura - Tabela BGP do *router* R8 do AS 65400

### AS 65400

O AS 65400 é um sistema autónomo de trânsito, como tal anuncia a todos os seus vizinhos todas as suas redes e as redes anunciadas por estes. No entanto é pedido que, para atingir o AS 65100 dê preferência à rota via AS 65300, para tal foi usado o *route-map* “rm1” presente na figura 29, atribuindo um *local-preference* maior a esta rota.

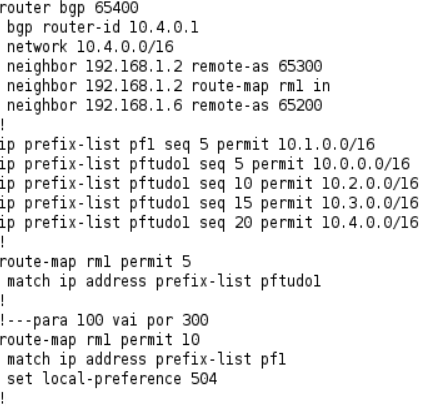


Figura - Configuração do *router* R8 do AS 65400

A tabela resultante destas políticas está presente na figura 28, na secção do AS 65300.

# Conclusão

Este relatório serviu o propósito de desenvolver uma solução, com base nos conhecimentos adquiridos na UC de Redes de Computadores 2, capaz de simular uma topologia de rede que envolve a comunicação entre sistemas autónomos.

Foram utilizados mecanismos provenientes de vários protocolos durante a configuração dos equipamentos emulados no *software* CORE. Para o encaminhamento dinâmico entre ABRs de ASs diferentes foi utilizado o protocolo BGP. Estes ABR são responsáveis por encaminhar o tráfego entre AS, foi utilizado o protocolo EBGP para ligações entre ABRs que pertencem a AS diferentes e o protocolo IBGP para ligações entre ABRs que pertencem ao mesmo AS.

Para cada AS foi estabelecido um protocolo de encaminhamento dinâmico intra-domínio. Seguindo a topologia apresentada na secção “[4.1. Topologia da rede](#_Topologia_da_rede)”, no AS 65000 foram utilizados mecanismos do protocolo RIP na configuração dos seus *routers*. No AS 65100 foram utilizados mecanismos do protocolo OSPF na configuração dos seus routers. Os *routers* dos restantes ASs foram configurados utilizando mecanismos de encaminhamento estático os quais o administrador da rede é que tem responsabilidade de manter atualizados e operacionais.

Devido ao enunciado do problema estabelecer algumas regras relativamente ao anúncio de rotas entre ABRs e como estes devem encaminhar o tráfego entre ASs foram estabelecidas configurações adicionais para que estas regras se cumprissem na topologia de rede emulada. Para tal foram aplicados os conceitos de *route-maps* para restringir o encaminhamento do tráfego para certas situações e permitir para outras.

Com este trabalho o grupo aprendeu como diferenciar sistemas autónomos quanto ao seu tipo, ou seja, ficaram aprendidos de como funcionam sistemas *multi-homed*, stub e de trânsito.

A solução apresentada pelo grupo neste relatório cumpre todos os objetivos definidos no início deste e respeita todas as restrições que o enunciado do problema especifica. É importante frisar que a solução é dotada de segurança e apresenta bons níveis de fiabilidade e estabilidade. Esta poderá vir a ser melhorada no futuro pelo grupo quando existirem condições de maior disponibilidade.