



UNIVERSIDADE DO MINHO | 2020/2021

GESTÃO DO ENCAMINHAMENTO EM SISTEMAS AUTÓNOMOS

ENCAMINHAMENTO DE TRÁFEGO EM REDES IP

GRUPO 1:

André Gonçalo Ribeiro da Silva Lopes.....A75363

Jorge Manuel de Almeida e Sousa.....A74230

Leandro Henrique Dantas Alves.....A82157

1 Etapa 1: Familiarização com o hardware e o software

Esta etapa, numa primeira fase, teve como objetivo a familiarização com os equipamentos reais e, para tal, foram configurados dois desses equipamentos, *routers*, para a possível comunicação entre dois *hosts*. No primeiro *router* foi atribuída a gama da rede **10.4.0.0/16**, como rede interna. Já para o segundo foi atribuída a gama **10.5.0.0/16**. Para a interligação entre ambos, foram escolhidos endereços IP na gama da rede **192.168.0.0/24**.

Numa segunda fase, foi criada uma pequena topologia no simulador de redes GNS3 (*Graphical Network Simulator-3*), presente na Figura 1, para a adaptação a este novo simulador. Esta topologia, é constituída por 3 redes locais, com as seguintes gamas de rede: **10.4.0.0/16**, **10.5.0.0/16** e **10.1.0.0/16**. Por último, foi feita a ligação da uma das redes da topologia simulada, no nosso caso, a rede **10.1.0.0/16**, com os equipamentos reais através do uso de um nó *Cloud*, presente no simulador, que usa a interface *ethernet* da máquina para a comunicação com o exterior, como está representado na Figura 2.

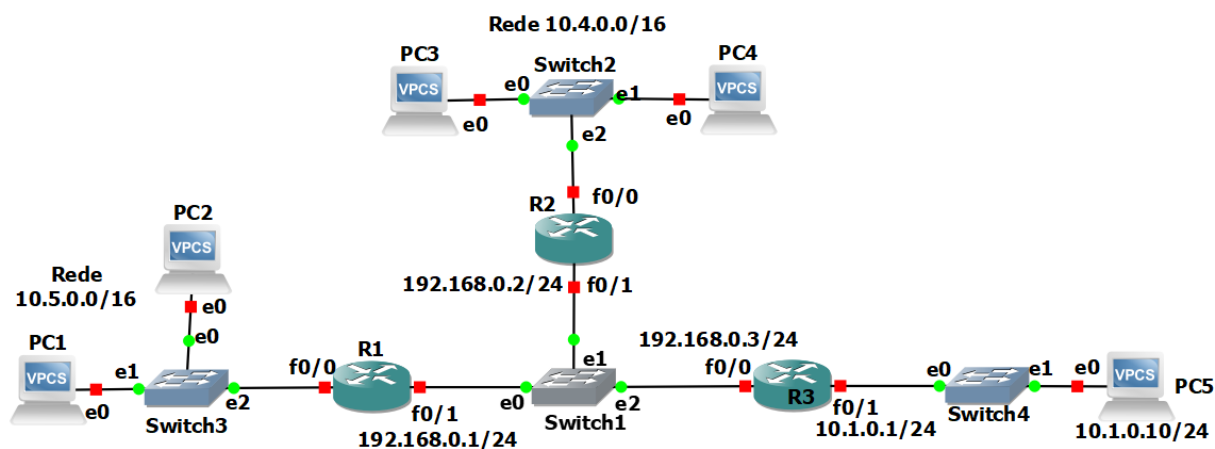


Figura 1 - Topologia simulada

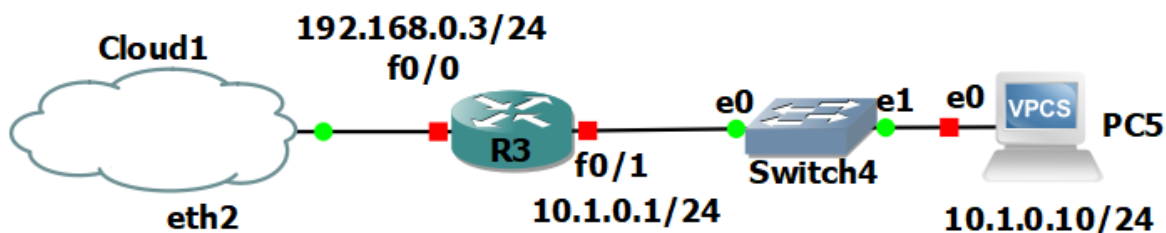


Figura 2 - Topologia simulada para ligação ao exterior

2 Etapa 2: Configuração de um sistema autónomo emulado

Nesta etapa, foi criado, no simulador GNS3, um Sistema Autónomo (SA) com o número de Sistema Autónomo AS65100, presente na **Erro! A origem da referência não foi encontrada..** Este SA usa internamente uma rede na gama **10.1.0.0/16** para endereços IPv4.

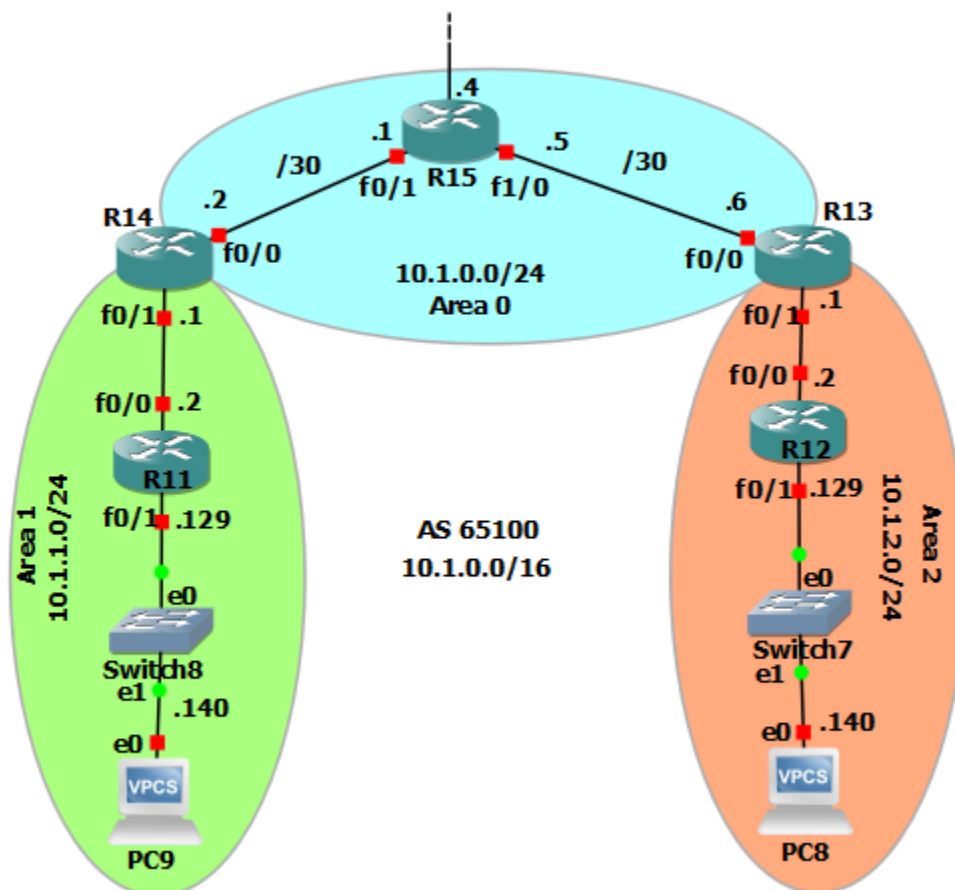


Figura 3 - Sistema Autónomo AS65100 simulado

Internamente, este SA utiliza o protocolo de encaminhamento OSPF (*Open Shortest Path First*), dividido por áreas, para a atribuição dinâmica das rotas internas. Para cada área, foi atribuída uma sub-rede com máscara /24 da rede **10.1.0.0/16**, como podemos ver através da figura acima, sendo a área 0 (área *backbone*) pintada a azul, a área 1 a verde e a área 2 a laranja.

Ainda no encaminhamento interno, foi aplicado um sistema de autenticação no protocolo OSPF para proibir a partilha de falsos anúncios de falsos encaminhadores através dos seguintes comandos:

- `ip ospf message-digest-key key md5 password`
- `area area-number authentication message-digest`

Todos os comandos usados relativos ao protocolo OSPF estão presentes nas figuras que se seguem, Figura 4 e Figura 5.

Em cada área existe um *router* interno, *router* R11 e R12, à exceção da área 0 que não tem nenhum. Estes *routers* tem a seguinte configuração, apresentada na Figura 4.

```
router ospf 1
log-adjacency-changes
area 1 authentication message-digest
area 1 range 10.1.1.0 255.255.255.0
network 10.1.1.0 0.0.0.127 area 1
network 10.1.1.128 0.0.0.127 area 1
!
```

Figura 4 - Configuração OSPF para *router* da área

Cada *router* ABR (*Area Border Router*), *router* R14 e R13, tem a configuração apresentada em Figura 5.

```
router ospf 1
log-adjacency-changes
area 0 authentication message-digest
area 0 range 10.1.0.0 255.255.255.0
area 1 authentication message-digest
area 1 range 10.1.1.0 255.255.255.0
network 10.1.0.0 0.0.0.255 area 0
network 10.1.1.0 0.0.0.255 area 1
!
```

Figura 5 - Configuração OSPF para *router* entre áreas

De notar que estas configurações podem mudar ligeiramente dependendo da área onde os *routers* estão incluídos.

Para a comunicação com outros Sistemas Autónomos, o nosso SA utiliza o protocolo BGP (*Border Gateway Protocol*) que foi ativado no *router* R15, com a configuração que está apresentada na Figura 6.

```
router bgp 65100
no synchronization
bgp router-id 192.168.0.1
bgp log-neighbor-changes
network 10.1.0.0 mask 255.255.0.0
redistribute ospf 1
neighbor 192.168.0.5 remote-as 500
neighbor 192.168.0.5 next-hop-self
neighbor 192.168.0.5 filter-list 1 out
neighbor 192.168.0.2 remote-as 65200
neighbor 192.168.0.2 next-hop-self
neighbor 192.168.0.2 soft-reconfiguration inbound
neighbor 192.168.0.2 filter-list 1 out
no auto-summary
!
ip forward-protocol nd
!
ip as-path access-list 1 permit ^$
!
```

Figura 6 - Configuração BGP

3 Etapa 3: Implementação de uma política de encaminhamento inter-domínio

O Sistema Autônomo **AS65100** tem como vizinhos 2 outros Sistemas Autônomos, representados como **AS65200** e **AS500** (AS65500), como podemos ver na configuração apresentada na Figura 6 através do comando **neighbor neighbor_IP_address remote-as AS_number**. Para cada um destes vizinhos foram aplicadas algumas regras nos anúncios de rede através da criação da regra com o comando **ip as-path access-list number { permit | deny } regexp^[1]** e, consequentemente, a aplicação desta com o seguinte comando **neighbor neighbor_IP_address filter-list acc_lst_number out**, para filtrar todos os anúncios que o AS65100 anuncia aos seus vizinhos. No comando **[1]** foi utilizado a expressão regular **^\$**, que corresponde a todos os prefixos do AS local.

Devido às políticas apresentadas nesta etapa, o *router* de borda do Sistema Autônomo **AS65500** teve também de ser configurado com algumas regras que suportassem tais políticas. Na Figura 7 estão apresentadas as configurações que se implementaram.

```
router bgp 500
no synchronization
bgp router-id 192.168.0.5
bgp log-neighbor-changes
network 10.5.0.0 mask 255.255.0.0
neighbor 192.168.0.6 remote-as 600
neighbor 192.168.0.6 next-hop-self
neighbor 192.168.0.4 remote-as 65400
neighbor 192.168.0.4 next-hop-self
neighbor 192.168.0.4 soft-reconfiguration inbound
neighbor 192.168.0.4 route-map AS400IN-LP in
neighbor 192.168.0.4 filter-list 5 out
neighbor 192.168.0.1 remote-as 65100
neighbor 192.168.0.1 next-hop-self
neighbor 192.168.0.2 remote-as 65200
neighbor 192.168.0.2 next-hop-self
neighbor 192.168.0.2 route-map AS65200IN-LP in
no auto-summary
!
ip forward-protocol nd
!
ip as-path access-list 5 permit ^$
ip as-path access-list 5 permit _65100$
!
route-map AS400IN-LP permit 10
set local-preference 150
!
route-map AS65200IN-LP permit 10
set local-preference 200
!
```

Figura 7 - Configuração BGP do *border router* do AS65500

Através dos comandos **route-map name permit sequence_number** e **set local-preference number** definimos quais as rotas que devem ter mais preferência sendo essas as escolhidas pelo *router*. Neste *router* teve de ser implementada uma regra extra com o comando **[1]**,

onde a expressão regular escolhida foi **_65100\$**, que corresponde aos prefixos originados no **AS65100**, pois o Sistema Autônomo 65500 é um ISP (*Internet Service Provider*) do Sistema Autônomo 65100.

4 Testes e Resultados

Após a configuração do *router* real para a comunicação entre os Sistemas Autônomos emulados no GNS3 dos restantes grupos, verificou-se que as regras aplicadas ao protocolo BGP estavam a funcionar corretamente, como apresentado na Figura 8.

```
BGP table version is 9, local router ID is 192.168.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop           Metric LocPrf Weight Path
*> 10.1.0.0/30     0.0.0.0              0         32768 ?
*> 10.1.0.4/30     0.0.0.0              0         32768 ?
*> 10.1.1.0/24     10.1.0.2             20        32768 ?
* 10.2.0.0/16     192.168.0.5           0          500 65200 i
*>                192.168.0.2           0          65200 i
*> 10.3.0.0/16     192.168.0.5           0          500 600 65400 65300 i
*> 10.4.0.0/16     192.168.0.5           0          500 65400 i
*> 10.5.0.0/16     192.168.0.5           0          500 i
*> 10.6.0.0/16     192.168.0.5           0          500 600 i
```

Figura 8 - Tabela BGP do *router* de borda do AS 65100