Trabalho TP4: Encaminhamento de Tráfego [Protocolo BGP e outros]

Beatriz Almeida[53693], Miguel Gomes[54153], and Rui Armada[50737]

Universidade do Minho, Braga 4710 - 057, Portugal
Rua da universidade, Braga, Portugal
https://www.uminho.pt/PT

Abstract. Keywords: CORE · OSPF · RIP · BGP · Routing

1 Introdução

O Trabalho Prático 4 visa estabelecer a configuração de uma simulação reduzida de uma rede complexa. São apresentados cinco sistemas autónomos, cada um com características distintas quanto à natureza do tráfego e ao uso de protocolos de roteamento específicos.

Neste relatório, destacaremos os aspetos cruciais das configurações dentro de cada sistema autónomo. Serão detalhadas todas as decisões tomadas e as modificações implementadas para assegurar que o tráfego dentro de cada sistema esteja alinhado com os critérios definidos nas diretrizes do projeto.

Incluir-se-á também uma secção dedicada aos testes realizados, descrevendo as técnicas utilizadas para verificar que os resultados obtidos estão conforme o esperado.

Prosseguiremos com uma discussão sobre a implementação realizada, iniciando com a descrição da topologia de rede adotada para este trabalho prático.

2 Definição da Topologia

Partindo da topologia, ilustrada na Figura 1, iremos focar especificamente nos elementos cruciais das configurações dos protocolos *RIP* e *OSPF*. Esses protocolos de roteamento foram o centro das análises em trabalhos práticos anteriores e serão novamente explorados neste contexto.

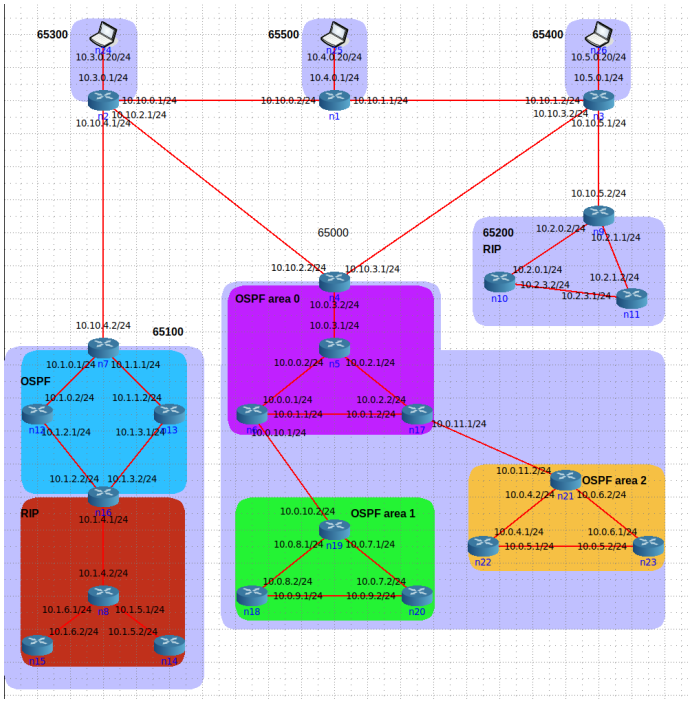

Fig. 1: Topologia utilizada

3 Configurações OSPF e RIP

3.1 AS 65200

O sistema autónomo **AS 65200**, classificado como *stub*, estabelecerá conexões *BGP* com o sistema adjacente, **AS 65400**. Além das conexões *BGP*, este sistema autónomo será composto por três *routers*. Internamente, será adotada a faixa de endereços IPv4 10.2.0.0/16, e o protocolo *RIP* será utilizado para o roteamento interno.

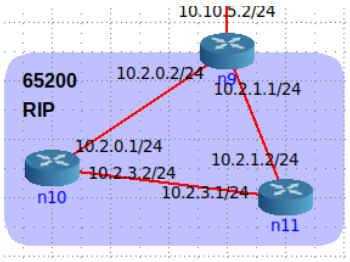

Fig. 2: AS 65200

Como foi pedido no enunciado. para além de assegurar conectividade através do protocolo *BGP* é necessário impedir o tráfego entre este sistema e o **AS 65100**. Para este efeito, é necessário impedir que o router *n9* receba rotas por *BGP* pode-se inserir um `access-list` e aplicá-la ao vizinho da rede **65400**.

```
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
```

Fig. 3: Configuração n9 (parte 1).

Como se está 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
  redistribute static
  redistribute connected
  default-information originate
  network 0.0.0.0/0
!
ip route 0.0.0.0/0 10.10.5.1
ip route 10.1.0.0/16 10.10.5.1 reject
```

Fig. 4: Configuração n9 (parte 2).

3.2 AS 65100

Este sistema autónomo, semelhante ao **AS 65200**, é um sistema autónomo de tipo *stub* que mantém relações *BGP* com um único vizinho, o **AS 65400**. Utilizará endereços IPv4 da gama 10.1.0.0/16 e adota o protocolo *OSPF*. No entanto, neste sistema ainda existem redes mais antigas que operam com o protocolo *RIP*.

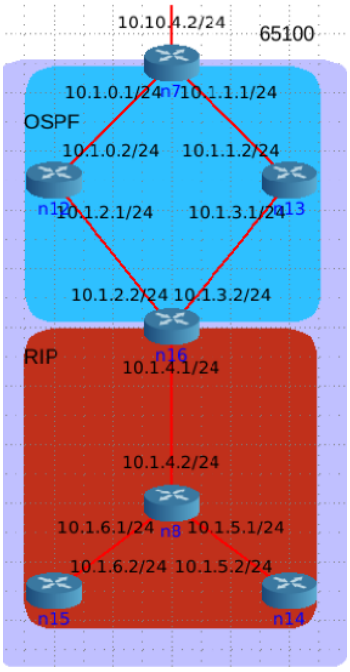

Fig. 5: AS 65100

A configuração *BGP* no *router* de entrada ao sistema, será semelhante à realizada no sistema autónomo **AS 65100**. No entanto, neste sistema, existirá um *router*, especificamente o *router n16*, que terá ativos os protocolos *RIP* e *OSPF* respetivamente. Será necessário recorrer a processos de redistribuição de rotas.

```
router ospf
  router-id 10.1.2.2
  network 10.1.2.2/24 area 0
  network 10.1.3.2/24 area 0
  network 10.1.4.1/24 area 0
  redistribute rip
!
router rip
  redistribute static
  redistribute connected
  redistribute ospf
  network 0.0.0.0/0
!
```

Fig. 6: Configuração n16.

3.3 AS 65000

Ao contrário dos sistemas **AS 65200** e **65100**, que são sistemas autónomos *stub*, este sistema é um sistema autónomo *multihomed*. Em vez de ter apenas um vizinho, terá dois, **AS 65300** e **AS 65400**. Internamente, serão utilizados endereços IPv4 da gama 10.0.0.0/16, e o protocolo de encaminhamento adotado será o *OSPF*. Existirão três áreas, e cada área contará com pelo menos três *routers*.

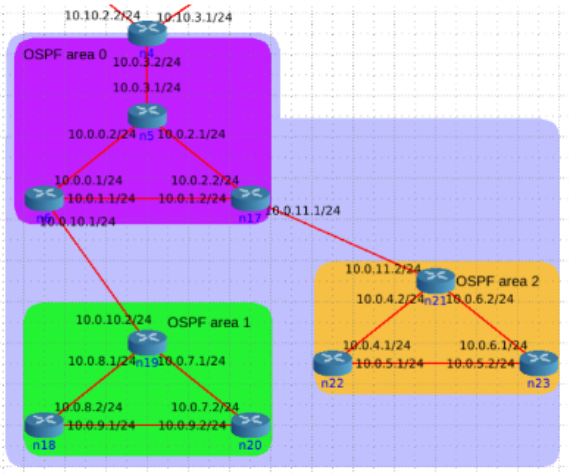

Fig. 7: AS 65000

Dado que se trata de um sistema autónomo *multihomed* com dois vizinhos, na configuração *BGP* será necessário definir ambos os vizinhos. Além de definir ambos, é crucial garantir que este é um sistema *multihomed*, mas não um sistema autónomo de trânsito. Ou seja, se as ligações entre os sistemas **AS 65300** e **AS 65400** falharem, estes não devem poder encaminhar o tráfego através deste sistema. Para tal efeito, é necessário adicionar o comando `ip as-path access-list 1 permit`. Neste sistema autónomo, existem três áreas, portanto será necessário configurar estas três áreas da mesma forma que foi realizado anteriormente.

```
.
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
!
router ospf
  router-id 10.0.3.2
  network 10.0.3.2/24 area 0
!
```

Fig. 8: Configuração n4.

3.4 AS 65300, 65400 e 65500

Estes três sistemas são sistemas autónomos de trânsito, ou seja, permitem que todo o tráfego de outros vizinhos passe por eles. Nestes sistemas, será apenas necessário configurar o protocolo BGP. O procedimento será idêntico: consiste em definir o próprio sistema e os vizinhos.

```
(n2)
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
!
(n1)
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
!
(n3)
router bgp 65400
  bgp router-id 10.10.1.2
  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
!
```

Fig. 9: Configuração n2, n1 e n3.

4 Tabelas de encaminhamento

As tabelas de encaminhamento consideradas mais importantes são as dos *routers* das áreas **65300** e **65400**, com o objetivo de provar que nenhum tráfego utiliza o **AS 65000** com um AS de trânsito, pelo que apenas se precisa de apresentar um deles.

```
Copyright 1996-2005 Kunihiro Ishiguro, et al.

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, 00:01:14
B>* 10.1.0.0/16 [20/0] via 10.10.4.2, eth2, 00:01:16
B>* 10.1.0.0/24 [20/1] via 10.10.4.2, eth2, 00:01:16
B>* 10.1.1.0/24 [20/1] via 10.10.4.2, eth2, 00:01:16
B>* 10.2.0.0/16 [20/0] via 10.10.0.2, eth0, 00:00:47
B>* 10.2.0.0/24 [20/0] via 10.10.0.2, eth0, 00:00:47
B>* 10.2.1.0/24 [20/0] via 10.10.0.2, eth0, 00:00:47
C>* 10.3.0.0/24 is directly connected, eth3
B>* 10.4.0.0/16 [20/0] via 10.10.0.2, eth0, 00:01:17
B>* 10.4.0.0/24 [20/1] via 10.10.0.2, eth0, 00:01:17
B>* 10.5.0.0/16 [20/0] via 10.10.0.2, eth0, 00:00:47
B>* 10.5.0.0/24 [20/0] via 10.10.0.2, eth0, 00:00:47
C>* 10.10.0.0/24 is directly connected, eth0
B>* 10.10.1.0/24 [20/1] via 10.10.0.2, eth0, 00:01:17
C>* 10.10.2.0/24 is directly connected, eth1
B>* 10.10.3.0/24 [20/0] via 10.10.0.2, eth0, 00:00:47
C>* 10.10.4.0/24 is directly connected, eth2
B>* 10.10.5.0/24 [20/0] via 10.10.0.2, eth0, 00:00:47
C>* 127.0.0.0/8 is directly connected, lo
n2#
```

Fig. 10: Tabela de encaminhamento de n2.

5 Testes de conectividade

Primeiro teste: Por exemplo, *n10* não consegue dar *ping* para 10.1.0.1, mas consegue mandar *ping*, por exemplo, para 10.0.8.2.

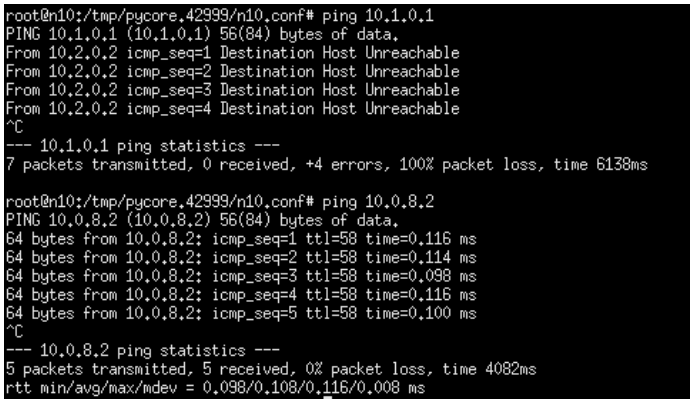

Fig. 11: Ping realizado em n10.

Segundo teste: O Host n25 consegue dar ping para o endereço do router n10, por exemplo.

Fig. 12: Ping realizado em n25.

6 Ataques Históricos ao Protocolo BGP e suas Implicações

6.1 Ataque ao Protocolo BGP: O Caso do Redirecionamento do Tráfego do YouTube em 2008

Um dos incidentes mais notórios relacionados à segurança do protocolo BGP ocorreu em fevereiro de 2008, envolvendo a Pakistan Telecom e o YouTube. Este evento é particularmente ilustrativo das vulnerabilidades inerentes ao design e à operação do BGP, um protocolo essencial para a funcionalidade da internet global.

Contexto do Incidente O Border Gateway Protocol (BGP) é utilizado para rotear o tráfego de dados na internet, determinando as rotas mais eficientes que os pacotes de dados devem seguir entre sistemas autónomos (AS). No entanto, o BGP baseia-se na confiança entre os operadores dos sistemas autónomos, assumindo que as rotas anunciadas são corretas e legítimas. Esta premissa de confiança foi explorada de forma acidental pela Pakistan Telecom quando anunciou para a Internet Routing Table uma rota para os endereços IP do YouTube.

Descrição Técnica do Ataque A Pakistan Telecom, com a intenção de bloquear localmente o acesso ao YouTube, inadvertidamente anunciou ao BGP que possuía a rota mais curta para os servidores do YouTube. Devido ao BGP não validar a origem dos anúncios de rota, esta informação foi aceita por outros ISPs e propagada globalmente. Como resultado, uma quantidade significativa do tráfego destinado ao YouTube foi redirecionada para a Pakistan Telecom, sobrecarregando sua infraestrutura limitada e tornando o YouTube inacessível para usuários em várias partes do mundo.

Outros Ataques Notáveis ao BGP

- **China Telecom Hijack (2010):** A China Telecom erroneamente anunciou a posse de 15% das rotas da internet global, redirecionando grandes volumes de tráfego internacional para dentro da China por aproximadamente 18 minutos.
- **Indosat Hijack (2014):** A operadora indonésia Indosat acidentalmente assumiu o controle de mais de 320.000 rotas da internet, afetando diversos serviços e operadoras ao redor do mundo.
- **Vazamento de Telecomunicações Russo (2017):** Uma má configuração em um ISP russo redirecionou tráfego de importantes redes de entrega de conteúdo e serviços financeiros através de servidores na Rússia, impactando significativamente o desempenho da internet global.
- **Sequestro de IP através de BGP no DEFCON 22 (2014):** Demonstração prática de como redirecionar tráfego destinado a um endereço IP específico para um servidor sob controle dos atacantes, ilustrando a possibilidade de interceptação e análise de dados.

Impacto e Resolução O incidente não só demonstrou a fragilidade do YouTube e de outros serviços de grande escala dependentes do BGP, mas também evidenciou uma falha crítica na segurança da infraestrutura global da internet. O problema foi eventualmente resolvido quando o anúncio falso foi identificado e removido, restaurando o roteamento normal após intervenção manual dos administradores de rede e operadores de backbone.

Implicações para a Segurança do BGP Este incidente sublinha a necessidade de implementações de segurança robustas no BGP, como a utilização do BGPSEC, que propõe a adição de assinaturas digitais aos anúncios de rotas para validar sua origem e integridade. No entanto, a adoção do BGPSEC tem sido lenta devido à sua complexidade operacional e ao aumento de custos associados.

Referência Principal Para uma análise mais profunda sobre os desafios de segurança do BGP e possíveis soluções, recomenda-se a consulta ao estudo "*A survey of BGP security*" por K Butler et al., 2004, disponível em: `http://vglab.cse.iitd.ac.in/~sbansal/csl865/readings/BGP-security.pdf`.

7 Conclusão

Nos projetos anteriores, explorámos diversos protocolos que se revelaram fundamentais para o desenvolvimento deste trabalho prático. Neste projeto, contudo, ocorreu uma integração única de diferentes protocolos, o que representou um desafio significativo. Inicialmente, custou-nos a perceber como o protocolo BGP funcionava, o que inicialmente impediu a conectividade adequada.

Ao concluir este trabalho, percebemos uma aproximação prática do funcionamento da Internet no contexto real e reconhecemos que a área de *routing* é intrinsecamente complexa e desafiadora. Apesar dos desafios, estamos confiantes de que todos os objetivos delineados foram atingidos com sucesso.

References

1. Configure RIP Route Metric (n.d.) Retrieved March 19, 2024, from https://www.geeksforgeeks.org/configuring-rip-route-metric-offset-lists-in-cisco/