UNIVERSIDADE DA BEIRA INTERIOR

Engenharia

Estudo de Convergência do Protocolo *Open Shortest Path First* Numa Rede Institucional Usando o Cisco Packet Tracer

Nuno Ricardo da Conceição Rosa Marques

Dissertação para obtenção do Grau de Mestre em

Engenharia Informática

(2º Ciclo de Estudos)

Orientador: Prof. Doutor Mário Marques Freire

Covilhã, outubro de 2012

Dedicatória

À minha mamã com muito amor

Agradecimentos

Um especial agradecimento em forma de abraço ao meu orientador Professor Mário Marques Freire pela constante ajuda e suporte a qualquer hora do dia e da noite!

Aos meus pais e irmã que desde que me conheço não me têm faltado com absolutamente nada, a eles um bem-haja.

À minha mais que tudo na vida – Guida - obrigado por estares ao meu lado.

Resumo

O Open Shortest Path First (OSPF) é um *Interior Gateway Protocol* (IGP) de encaminhamento dinâmico baseado em *Link States*. Conheceu as suas raízes em 1987 e foi amplamente implementado em todo o mundo. Ao longo dos anos até à atualidade, foi alvo de várias contribuições devido à evolução das exigências das redes que culminou num protocolo bastante robusto e sólido. Os novos domínios de encaminhamento não param de crescer e requerem serviços de rede cada vez mais redundantes mantendo a alta disponibilidade. O crescimento do tamanho de um domínio de encaminhamento está diretamente ligado à velocidade de convergência da rede. Nesta dissertação descrevem-se aspetos de funcionamento e de configuração do protocolo OSPF numa rede institucional, a rede de todo o *campus* da Universidade da Beira Interior. Foi proposta, implementada e testada uma configuração que proporciona redundância e alta disponibilidade de forma dinâmica e com tempos mínimos de convergência.

Palavras Chave

Autonomous Border *Router*, Autonomous System Border *Router*, Backup Domain *Router*, Border Gateway Protocol, Data Base Description, Domain *Router*, Enhanced Interior Gateway, Routing Protocol, *Link* State Advertise, *Link* State Acknowledgement, *Link* State Request, *Link* State Update, Not So Stubby Area, Open Shortest Path First, Routing Information Protocol, Stub Area.

Abstract

Open Shortest Path First (OSPF) is an Interior Gateway Routing Protocol (IGRP) based on dynamic Link States. Created in 1987 and was widely implemented throughout the world. Over the years up to the present has been the target of several contributions due to the changing requirements of network protocol which culminated in a very robust and solid protocol. The new routing domains do not stop growing and require increasingly redundant network services maintaining high availability. The growing size of a routing domain is directly linked to the speed of network convergence. This dissertation will describe some aspects of the operation and configuration of the OSPF protocol and make a proposal to reduce convergence time of a network. It was proposed, implemented and tested a network configuration which provides dynamic redundancy and high availability with minimum convergence times to the network of an Institution, Beira Interior University.

Keywords

Autonomous Border *Router*, Autonomous System Border *Router*, Backup Domain *Router*, Border Gateway Protocol, Data Base Description, Domain *Router*, Enhanced Interior Gateway, Routing Protocol, *Link* State Advertise, *Link* State Acknowledgement, *Link* State Request, *Link* State Update, Not So Stubby Area, Open Shortest Path First, Routing Information Protocol, Stub Area.

Índice

Lista de Figuras

Lista de Tabelas

Lista de Acrónimos

ABR Autonomous Border *Router*

ASBR Autonomous System Border *Router*

BDR Backup Domain *Router*

BGP Border Gateway Protocol

DBD Data Base Description

DR Domain *Router*

EIGRP Enhanced Interior Gateway Routing Protocol

EL External *Link*

IP Internet Protocol

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

LSA *Link* State Advertise

LSAck *Link* State Acknowledgement

LSR *Link* State Request

LSU *Link* State Update

NBMA Non-Broadcast Multiple Acess

NL Network *Link*

NSSA Not So Stubby Area

OSPF Open Shortest Path First

RIP Routing Information Protocol

RL *Router Link*

SA Stub Area

SFP Shortest Path First

SL Summary *Link*

VLSM Variable Length Subnet Masking

Capítulo 1

Introdução

1.1 Enquadramento da Dissertação

Na perspetiva em que poderá ser impossível evitar catástrofes naturais ou de origem humana, torna-se imperativa a existência de resiliência e alta disponibilidade em redes informáticas, como forma de contribuir para o desempenho de uma instituição. Para isto, torna-se necessária a eliminação de pontos de falha numa rede recorrendo, nomeadamente, a replicação de *routers* e de ligações proporcionando resiliência de forma transparente e comutação de ligações impercetível aos diferentes serviços e utilizadores da rede. Dados críticos que não são comunicados derivado à falta de caminhos alternativos da rede (ou na procura destes) podem levar a custos superiores ao do próprio valor da implementação de uma solução que forneça serviços de rede redundantes e de alta disponibilidade.

Nesta dissertação pretende-se expor, de forma bastante completa, aspetos sobre o funcionamento e configuração do protocolo *Open Shortest Path First* (OSPF) [1] - [2], com o objetivo de identificar os principais atores que influenciam os tempos de convergência de uma rede OSPF. Identificados estes atores, pretende-se encontrar uma configuração que contribua para a redução dos tempos de convergência de uma rede com várias ligações redundantes maximizando a disponibilidade da rede. No fim será feito um estudo e uma proposta de configuração para uma rede institucional, a rede de todo o *campus* da Universidade da Beira Interior, com o âmbito de garantir a máxima redundância e alta disponibilidade possíveis com a infraestrutura de rede existente.

1.2 Conceitos subjacentes ao OSPF

1.2.1 Resenha Histórica sobre o OSPF

O desenvolvimento inicial do OSPF começou em 1987 pelo Grupo de Trabalho do OSPF da Internet Engineering Task Force (IETF). Naquele tempo, a Internet era predominantemente uma rede académica e de investigação fundada pelo governo norte-americano.

Em 1989, a especificação para o OSPFv1 foi publicada na RFC 1131 [3]. Havia duas implementações escritas: uma para executar em *routers* e outra para executar em estações de trabalho UNIX. A última implementação tornou-se mais tarde um processo UNIX difundido conhecido como GATED. O OSPFv1 foi um protocolo de encaminhamento experimental e nunca foi implantado.

Em 1991, o OSPFv2 foi introduzido na RFC 1247 [4] por John Moy. O OSPFv2 ofereceu melhorias técnicas significativas sobre o OSPFv1. Ao mesmo tempo, a ISO trabalhava num protocolo de encaminhamento *Link-state* próprio chamado *Intermediate System-to-Intermediate System* (IS-IS). Conforme o esperado, a IETF escolheu o OSPF como seu IGP recomendado (Protocolo IGP).

Em 1998, a especificação do OSPFv2 foi atualizada na RFC 2328 e é a RFC atual para OSPF.

Em 1999, OSPFv3 para IPv6 foi publicado na RFC 2740 [5] o qual foi elaborado por John Moy, Rob Coltun e Dennis Ferguson.

São vários os trabalhos relacionados com este tema nomeadamente:

Ogier [6] propôs uma otimização na transferência da lista sumária da base de dados, uma extensão para OSPFv2/v3 de modo a acelerar essa transferência minimizando o tamanho dos pacotes.

Venkatesh [7] propôs uma extensão da operação do OSPF em redes convencionais onde estabelecimento de adjacência via troca de base de dados ocorre somente ao longo das ligações de spanning tree mantidas de forma dinâmica pelos *routers* da rede.

1.2.2 Classificação dos Protocolos de Encaminhamento

Existem dois tipos de protocolos de encaminhamento: estático e dinâmico. Os protocolos de encaminhamento dinâmico dividem-se em dois grupos: *Interior Gateway Protocols* (IGP) e *Exterior Gateway Protocol* (EGP). Os IGPs dividem-se em dois tipos: *Distant Vector Routing Protocols* e *Link State Routing Protocols*. No caso dos EGPs são do tipo *Path Vector*. Na tabela 1 pode-se observar a distribuição da classificação de cada um dos protocolos de encaminhamento.

Tabela 1 - Classificação dos protocolos de encaminhamento [8].

Tipo	**Interior Gateway Protocols**				**Exterior Gateway Protocols**
	Distance Vector Routing Protocols		*Link* State Routing Protocols		Path Vector
Classful	RIP	IGRP			EGP
Classless	RIPv2	EIGRP	OSPFv2	IS-IS	BGPv4
IPv6	RIPng	EIGRP	OSPFv3	IS-IS	BGP

1.2.3 Cisco Packet Tracer

O *Cisco Packet Tracer* [9] detém uma tecnologia de rede abrangente, dotado para fins de ensino e investigação na área das redes que oferece uma combinação única de simulação em tempo real, visualização, avaliação, recursos de criação de atividades e de colaboração multiutilizador. Permite a criação de topologias de redes físicas e lógicas atravessando ao ínfimo detalhe todos os níveis da pilha OSI. Inclui um *packet sniffer* embutido que permite analisar todos os pacotes que participaram na experiência laboratorial. Facilita a partilha de conhecimento e informação, devido à sua natureza aberta.

O *Cisco Packet Tracer* fornece dois modos de operação para visualizar o comportamento de uma rede: modo de tempo real e o modo de simulação. No modo em tempo real, a rede comporta-se como dispositivos reais, com resposta em tempo real de todas as atividades da rede. No modo de simulação podemos ver e controlar os intervalos de tempo, o funcionamento interno de transferência de dados e a propagação de dados através de uma rede. Os protocolos suportados por esta plataforma ao nível da aplicação são: *File Transfer Protocol, Simple Mail Transfer Protocol, Post Office Protocol v3, HyperText Transport Protocol, Trivial File Transfer Protocol, Telnet, Secure Shell, Domain Name Server, Dynamic Host Configuration Protocol, Network Time Protocol, Simple Network Management Protocol, Authentication Authorization Accounting, Integrated Services Router Voice over Internet Protocol,* Skinny Client Control Protocol, *config* e *calls Integrated Services Router, command support, Call Manager Express*; Ao nível do transporte: *Transmission Control Protocol, User Datagram Protocol, Nagle Algorithm, IP Fragmentation, Real Time Protocol; ao nível da rede: Border Gateway Protocol, Internet Protocol v4, Internet Control Message Protocol, Address Resolution Protocol, Internet Protocol v6, Internet Control Message Protocol v6, Internet Protocol Security, Routing Information Protocol v1/v2/ng, Multi-Area Open Shortest Path First, Enhanced Interior Gateway Routing Protocol, Static Routing, Route Redistribution,*

Multilayer Switching, Layer 3 Quality of Service, Network Address Translation, Zone-based policy firewall e *Intrusion Protection System o*n the ISR, *Generic Route Encapsulation Virtual Private Network (VPN), Internet Protocol Security VPN*; ao nível da interface de rede: *Ethernet (802.3), 802.11, High-Level Data Link Control, Frame Relay, Point to Point Protocol, PPPoE, Spanning Tree Protocol, Rapid Spanning Tree Protocol, Virtual Trunking Protocol, Dynamic Trunking Protocol, Cisco Discovery Protocol, 802.1q, Layer 2 Quality of Service, Simple Wireless Encryption Protocol, Wi-Fi Protected Access, Extensible Authentication Protocol*.

1.2.4 Alta Disponibilidade e Convergência de Protocolos

Por alta disponibilidade entende-se por um sistema resiliente a falhas cujo objetivo é manter os serviços disponibilizados o máximo de tempo possível. Cada vez mais é necessário garantir a disponibilidade de um serviço, especialmente quando essa rede dá suporte a aplicações de tempo real ou transporta dados críticos/vitais. A convergência de um protocolo é atingida quando todas as bases de dados de todos os *routers* da mesma área estão idênticas. As atualizações destas bases de dados são feitas por métodos específicos, no caso do OSPF via *Link State Advertises*.

1.3 Definição do Problema e Objetivos

Mesmo com a presença de encaminhamento estático é possível criar redundância nas ligações recorrendo às métricas com igual destino em interfaces de saída diferentes. Esta implementação prima pelos tempos mínimos de convergência e é impercetível à maioria das aplicações mais exigentes nomeadamente fluxos de voz, vídeo de tempo real ou *online gaming*. No entanto, a implementação resulta mal quando a conetividade IP se perde apesar da interface de saída continuar operacionalmente ativa e o *router* não tem maneira de validar essa perda de conetividade pois não estabelece adjacências com os seus vizinhos. Como resultado, este fica a enviar (descartar) pacotes por essa interface. Neste panorama, poderíamos pensar no nível da camada da ligação dos dados do modelo OSI onde temos protocolos que fornecem serviços de redundância tais como o *Rapid Spanning Tree* (RSTP, IEEE 802.3w). Habilitar estes protocolos num *router* (caso o suporte) é de todo

desaconselhado e, caso se faça, muitas situações terão de ser previstas e acauteladas. É possível ter STP a atribuir o estado de *backup* a uma interface, desabilitando-a e, por outro lado, um protocolo de camada 3 a entregar nessa interface sem sucesso resultando numa nova convergência da rede pelo fato de ter havido uma mudança de topologia de rede. *Chia-Tai et al*, [10] sugere uma solução de dois routers em *hot-stanby* com tempos de convergência de 166 ms em caso de falha de hardware e 360 ms em caso de falha no software.

A heterogeneidade de equipamentos existentes nesta instituição limita em muito a escolha de um protocolo de encaminhamento dinâmico. Uma análise detalhada das caraterísticas e protocolos suportados pelos *routers* resultou na seleção de dois possíveis protocolos de encaminhamento: RIP (*Routing Information Protocol*) [11] e OSPF (*Open Shortest Path First*). No entanto, esta rede detém redes descontínuas o que inviabiliza o uso de RIP pois é um protocolo *classfull* e, mesmo na sua versão 2, estaríamos limitados pelo número de saltos suportados. Por outro lado, o crescimento de domínios de encaminhamento tornam os tempos de convergência elevados podendo chegar ao ponto de todo o domínio colapsar. Assim o primeiro problema a abordar consiste em expor aspetos sobre o funcionamento e configuração do protocolo OSPF de forma aprofundada com o objetivo de identificar os atores que contribuem para o atraso na convergência de uma rede OSPF e propor uma configuração para reduzir esses tempos na rede institucional considerada, a rede da Universidade da Beira Interior.

Associado a este problema, existe um segundo problema que reside na escassez de ligações redundantes na rede da Universidade da Beira Interior, e na inexistência de um protocolo de encaminhamento dinâmico. De modo a ultrapassar este problema, pretende-se ativar troços existentes nas ligações de *backbone* entre *routers* e propor uma configuração que acolha de forma dinâmica os novos troços de modo a garantir resiliência e alta disponibilidade à rede desta instituição.

1.4 Estratégia Adotada para Resolução do Problema

O protocolo OSPF está munido de mecanismos internos para deteção de falhas baseadas em *hello* e *dead timers* que estão diretamente ligados aos tempos de convergência de uma rede aquando uma mudança de topologia. Através do Cisco Packet Tracer pretende-se testar estas convergências e encontrar uma relação entre largura de banda e os valores de *hello* e *dead* de modo a minimizar os tempos de convergência. Típicamente os routers mais recentes estão munidos de (*Application Specific Integrated Circuits*) ASICs para o encaminhamento de pacotes

e CPU para o plano de controlo com a finalidade de efetuar cálculos para o protocolo OSPF. Não existe o problema do router sofrer um *meltdown* por não ter tempo de processador por estar demasiado ocupado a despachar pacotes. Assim vão ser efetuados diversos testes com diferentes combinações de *hello* e *dead timers* na plataforma *Cisco Packet Tracer*. Serão construídas duas topologias de rede diferentes, ambas envolvendo três *routers* com ligações ponto-a-ponto e a outra topologia com dois *switches* adicionais. Serão criadas disrupções de rede e registados os tempos de convergência para os diferentes valores de *hello* e *dead timers*.

Em relação à proposta de reconfiguração da rede da Universidade da Beira Interior serão executados os seguintes passos:

- Recolha da topologia de rede existente
- Recolha do número de troços de fibra escura
- Recolha do número de portas livres nos organizadores de fibra
- Efetuar novas ligações físicas aos equipamentos
- Determinar o número de áreas a serem usadas
- Definir portas de *upLink* e portas de acesso
- Autenticação encriptada entre routers da mesma área
- Atribuição de endereçamento IP às interfaces lógicas
- Distribuição das redes diretamente ligadas no processo OSPF

1.5 Organização da Dissertação

O corpo desta dissertação é composto por cinco capítulos: Introdução, *Open Shortest Path First*, Proposta de configuração de rede e Conclusão incluindo trabalho futuro. Existe também um Anexo. As referências estão após o capítulo 6. A seguir apresenta-se um resumo dos conteúdos de cada capítulo.

O Capítulo 1 elucida o contexto do assunto abordado nesta dissertação, identifica o problema a ser resolvido e os principais objetivos.

O Capítulo 2 descreve um estudo e exposição aprofundada do protocolo OSPF com o principal objetivo de identificar variáveis que afetem os tempos de convergência.

O Capítulo 3 descreve uma verificação de configurações OSPF e uma proposta de configuração para uma rede institucional, a rede de todo o *campus* Universidade da Beira Interior

garantindo um máximo de redundância e minimizando os tempos de convergência, ficando limitado à infraestrutura de rede existente.

O Capítulo 4 resume as principais conclusões desta dissertação além de fornecer algumas orientações para futuras pesquisas e trabalhos.

O Anexo A contempla as configurações de uma rede.

O Anexo B contempla uma proposta de configuração para a rede da Universidade da Beira Interior.

Capítulo 2

Aspetos Sobre o Funcionamento e Configuração do OSPF

Introdução

O *Open Shortest Path First* (OSPF) é um *Interior Gateway Protocol* usado para distribuir informações de rotas dentro de um único sistema autónomo. É um protocolo de encaminhamento dinâmico baseado na técnica *Link-state* que foi desenvolvido como uma substituição para o protocolo de encaminhamento do vetor de distância RIP. O RIP foi um protocolo de encaminhamento bastante aceite no início da Internet, mas a sua confiabilidade baseada somente na contagem de saltos como a única medida para escolher a melhor rota rapidamente tornou-se inaceitável em redes maiores que necessitavam de uma solução de encaminhamento mais robusta.

O OSPF é um protocolo de encaminhamento *classless* que usa o conceito de áreas para escalabilidade. A métrica do OSPF é um valor arbitrário chamado custo definido pelo RFC 2328. Neste capítulo pretende-se apresentar de forma aprofundada o modo de funcionamento do protocolo OSPF e identificar as variáveis que contribuem para os tempos de convergência de uma rede OSPF.

Este capítulo tem como objetivo:

i) Descrever os recursos do OSPF, identificar a abrangência dos comandos de configuração;

ii) Descrever, modificar e calcular métricas utilizadas pelo OSPF;

iii) Descrever o processo de eleição do Router em redes multiacesso.

2.1 Descrição da Base de Dados *Link*-State

O pacote *Database Descriptor* (DBD) contém uma lista abreviada da base de dados *Link-state* do *router* que o envia, os *routers* que o recebem e comparam com a base de dados *Link-state* local. A figura 1 representa uma topologia de rede onde existem duas áreas (Area 0 e Area 1) e também o *router* RTE que está a executar dois protocolos de encaminhamento ao mesmo tempo, OSPF e RIP. Nas figuras 2 a 4 podem ver-se as configurações dos *routers* RTA, RTE e RTC.

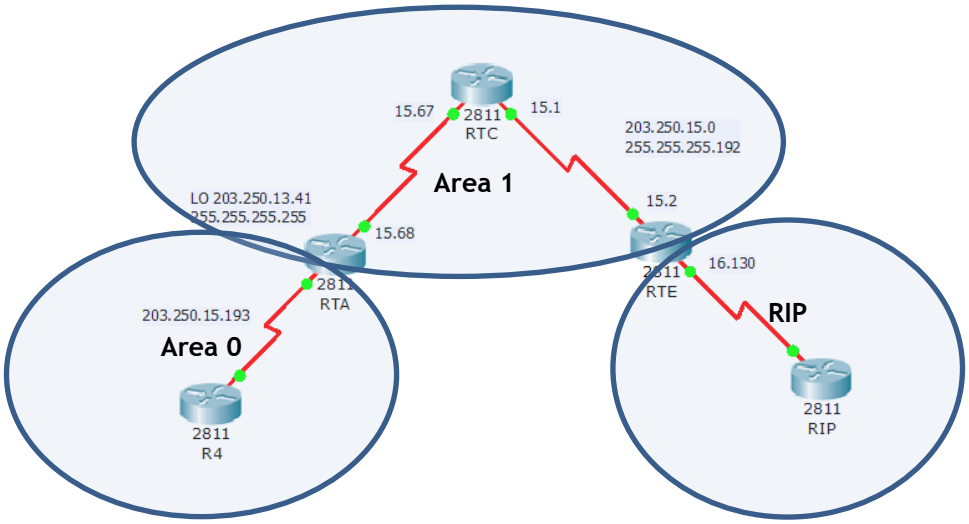

Figura 1 - Topologia de rede com *routers* em modo ABR (*Area Border Router*) [12].

```
interface Loopback0
  ip address 203.250.13.41 255.255.255.255
 interface Ethernet0
  ip address 203.250.15.68 255.255.255.192
 interface Ethernet1
  ip address 203.250.15.193 255.255.255.192

 router ospf 10
  network 203.250.0.0 0.0.255.255 area 0

 RTA#show ip route
 Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default

 Gateway of last resort is 203.250.15.67 to network 0.0.0.0

      203.250.16.0 255.255.255.192 is subnetted, 1 subnets
 O E2    203.250.16.128 [110/10] via 203.250.15.67, 00:00:50, Ethernet0
      203.250.13.0 255.255.255.255 is subnetted, 1 subnets
 C       203.250.13.41 is directly connected, Loopback0
      203.250.15.0 255.255.255.192 is subnetted, 3 subnets
 O IA    203.250.15.0 [110/74] via 203.250.15.67, 00:00:50, Ethernet0
 C       203.250.15.64 is directly connected, Ethernet0
 C       203.250.15.192 is directly connected, Ethernet1
 O*E2 0.0.0.0 0.0.0.0 [110/10] via 203.250.15.67, 00:00:50, Ethernet0
```

Figura 2 - Configuração do RTA

```
RTE#
 ip subnet-zero

 interface Ethernet0
  ip address 203.250.16.130 255.255.255.192

 interface Serial0
  ip address 203.250.15.2 255.255.255.192

 router ospf 10
  redistribute rip metric 10 subnets
  network 203.250.15.0 0.0.0.63 area 1
  default-information originate metric 10

 router rip
  network 203.250.16.0

 ip route 0.0.0.0 0.0.0.0 Ethernet0

RTE#show ip route
*output omitido*
 Gateway of last resort is 0.0.0.0 to network 0.0.0.0

      203.250.16.0 255.255.255.192 is subnetted, 1 subnets
 C       203.250.16.128 is directly connected, Ethernet0
      203.250.13.0 is variably subnetted, 2 subnets, 2 masks
 O IA    203.250.13.41 255.255.255.255
            [110/75] via 203.250.15.1, 00:16:31, Serial0
      203.250.15.0 255.255.255.192 is subnetted, 3 subnets
 C       203.250.15.0 is directly connected, Serial0
 O IA    203.250.15.64 [110/74] via 203.250.15.1, 00:16:31, Serial0
 O IA    203.250.15.192 [110/84] via 203.250.15.1, 00:16:31, Serial0
 S*   0.0.0.0 0.0.0.0 is directly connected, Ethernet0
```

Figura 3 - Configuração do RTE

```
RTC#
 ip subnet-zero

 interface Ethernet0
  ip address 203.250.15.67 255.255.255.192

 interface Serial1
  ip address 203.250.15.1 255.255.255.192

 router ospf 10
  network 203.250.15.64 0.0.0.63 area 0
  network 203.250.15.0 0.0.0.63 area 1

RTF#show ip route
*output omitido*
 Gateway of last resort is 203.250.15.2 to network 0.0.0.0

      203.250.16.0 255.255.255.192 is subnetted, 1 subnets
 O E2    203.250.16.128 [110/10] via 203.250.15.2, 04:49:05, Serial1
      203.250.13.0 255.255.255.255 is subnetted, 1 subnets
 O       203.250.13.41 [110/11] via 203.250.15.68, 04:49:06, Ethernet0
      203.250.15.0 255.255.255.192 is subnetted, 3 subnets
 C       203.250.15.0 is directly connected, Serial1
 C       203.250.15.64 is directly connected, Ethernet0
 O       203.250.15.192 [110/20] via 203.250.15.68, 04:49:06, Ethernet0
 O*E2 0.0.0.0 0.0.0.0 [110/10] via 203.250.15.2, 04:49:06, Serial1
```

Figura 4 - Configuração do *router* RTC.

Na figura 5 temos o resultado do comando *show ip ospf database* que dá uma visão geral de toda a base de dados OSPF ordenada por áreas do *router* RTC. Este *router* tem o papel de ABR (*Area Border Router*) dado que tem mais que uma área na sua base de dados. A área 1 é composta por *router Links* e *Summary Links*. Não existem *network Links* porque não existem *Domnain Routers* em qualquer dos segmentos de rede da Area 1. Também não existem *Autonomous System Border Routers* (ASBR*) Links* pois a única ASBR está na Area 0. Os *Link*s externos não pertencem a uma área específica pois estas são inundadas por todo o lado. É de fazer notar que todos os *Link*s são uma acumulação de *Link*s de todos os *routers* nessa área. O *Link-ID* é, de fato, o *Link-State ID*, esta informação representa um *router* e não apenas um *Link* em particular. Um *router* que tenha todas as suas interfaces na mesma área é denominada *Internal Router* (IR). Um *router* que tenha várias interfaces em diferentes áreas é denominado de *Area Border Router* (ABR). Um *router* que tenha a função de *gateway* e sirva de ponte entre OSPF e outros protocolos de encaminhamento tais como: EIGRP, IS-IS, RIP, BGP, *Static* ou outras instâncias de OSPF é denominado de *Autonomous System Boundary Router* (ASBR).

```
RTC#show ip ospf database
       OSPF Router with ID (203.250.15.67) (Process ID 10)
                Router Link States (Area 1)

Link ID         ADV Router      Age    Seq#       Checksum Link count
203.250.15.67   203.250.15.67   48     0x80000008 0xB112   2
203.250.16.130  203.250.16.130  212    0x80000006 0x3F44   2

                Summary Net Link States (Area 1)
Link ID         ADV Router      Age    Seq#       Checksum
203.250.13.41   203.250.15.67   602    0x80000002 0x90AA
203.250.15.64   203.250.15.67   620    0x800000E9 0x3E3C
203.250.15.192  203.250.15.67   638    0x800000E5 0xA54E

                Router Link States (Area 0)
Link ID         ADV Router      Age    Seq#       Checksum Link count
203.250.13.41   203.250.13.41   179    0x80000029 0x9ADA   3
203.250.15.67   203.250.15.67   675    0x800001E2 0xDD23   1

                Net Link States (Area 0)
Link ID         ADV Router      Age    Seq#       Checksum
203.250.15.68   203.250.13.41   334    0x80000001 0xB6B5

                Summary Net Link States (Area 0)

Link ID         ADV Router      Age    Seq#       Checksum
203.250.15.0    203.250.15.67   792    0x80000002 0xAEBD

                Summary ASB Link States (Area 0)
Link ID         ADV Router      Age    Seq#       Checksum
203.250.16.130  203.250.15.67   579    0x80000001 0xF9AF

                AS External Link States
Link ID         ADV Router      Age    Seq#       Checksum Tag
0.0.0.0         203.250.16.130  1787   0x80000001 0x98CE   10
203.250.16.128  203.250.16.130  5      0x80000002 0x93C4   0
```

Figura 5 - Base de dados *Link-state* de um *router* OSPF.

Link State Request

Os pacotes do tipo *Link-state* são enviados aos *routers* vizinhos a solicitar mais informações sobre qualquer entrada na DBD, enviando um *Link-State Request* (LSR). Cada *router* constrói uma lista de LSA (*Link State Advertisements*) necessários de modo a manter a sua adjacência atualizada. A lista retransmitida é mantida de modo a verificar que todas as LSA enviadas são efetivamente recebidas. Para especificar o número de segundos entre retransmissões de LSA usa-se o comando: *ip ospf retransmit-interval*.

Link State Update

Os pacotes de *Link-State Update* (LSU) são utilizados para responder às LSRs, bem como anunciar novas informações. Os LSUs contêm onze tipos diferentes de *Link-State Advertise* (LSAs) tal como mostra a tabela 2.

Link-State Acknowledgement

Quando um LSU é recebido, o *router* envia um *Link-State Acknowledgement* (LSAck) para confirmar a receção do LSU.

2.2 Protocolo *Hello*

2.2.1 Introdução

Um pacote OSPF do tipo 1 é um pacote *Hello* do OSPF e tem como função detetar vizinhos de OSPF estabelecendo adjacências de vizinho. Esta adjacência obedece aquando da comparação de igualdade dos valores anunciados pelos dois *routers* a fim de se tornarem vizinhos. Os pacotes *Hello* colaboram na eleição do DR e do BDR em redes multiacesso nomeadamente *Ethernet* e *Frame Relay*.

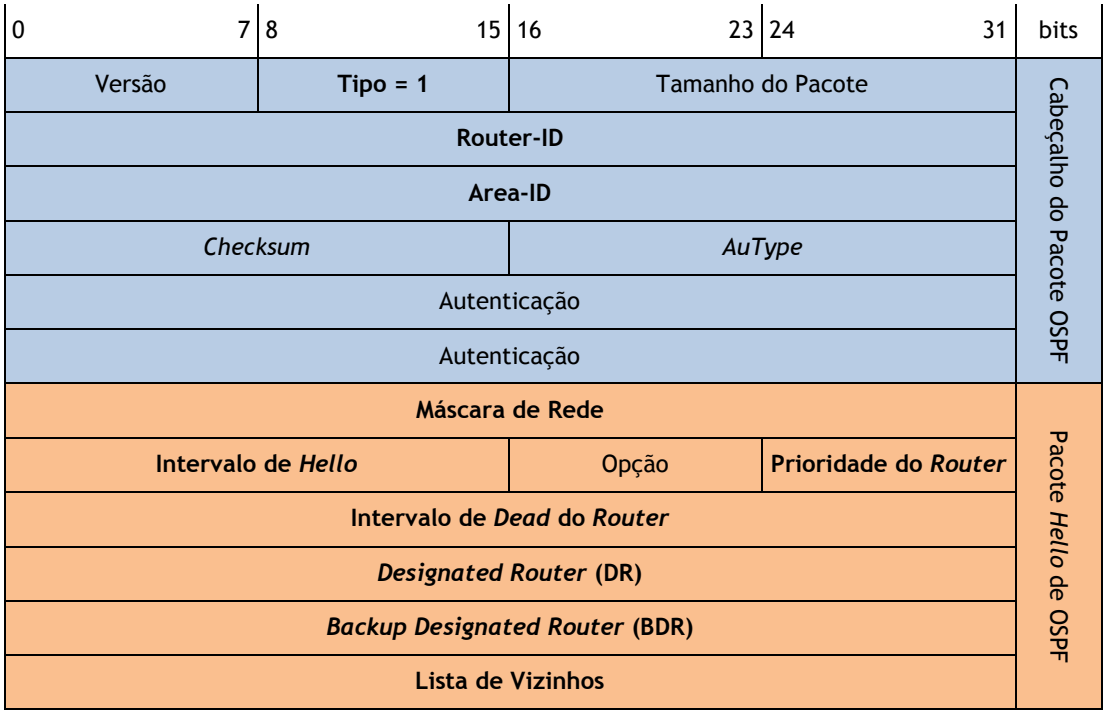

Figura 6 – Representação esquemática do formato do pacote OSPF *Hello* do tipo 1 [13].

A figura 6 mostra uma representação esquemática do formato do pacote OSPF *Hello* do tipo 1. O campo tipo de 8 bits pode tomar os valores de 1 a 5: *Hello*, DD, LS *Request*, LS *Update*, LS ACK, respetivamente. O campo ID do *Router* indica o *router* de origem e ID da Área indica a área a partir da qual o pacote foi originado. O campo Máscara de Rede de 32 bits contém a máscara da sub-rede associada com a interface de envio. O intervalo em segundos entre os *Hellos* do *router* que envia é definido pelo campo Intervalo de *Hello*. O campo Prioridade do *Router* é utilizado na eleição do DR (*Domain Router*) e do BDR (*Backup Domain Router*). Os campos Designated *Router* e Backup Designated *Router*, de 32 bits cada, tomam o valor 0 se não estiverem numa rede multiacesso, caso contrário estes campos acomodam valores das *OSPF ID* (endereços IP) dos *routers* eleitos para tais funções. A lista de vizinhos contém uma lista de *routers* aos quais o *router* de envio estabeleceu uma relação de adjacência, sendo esta informação guardada no campo Lista de Vizinhos com um tamanho de 32 *bits*.

2.2.2 Processo de Vizinhança

Antes de um *router* OSPF poder enviar os seus *Link-states* a outros *routers*, ele deverá determinar se existem outros vizinhos OSPF em algum dos seus *Link*s. Na figura 7, os *routers* OSPF estão a enviar pacotes *Hello* em todas as interfaces habilitadas por OSPF para determinar se existem vizinhos nesses *Link*s. As informações no OSPF *Hello* incluem a ID do

router OSPF que envia o pacote *Hello*. Receber um pacote *Hello* de OSPF numa interface confirma para um *router* que há outro *router* OSPF neste *Link*. O OSPF estabelece então uma adjacência com o vizinho. Por exemplo, na figura 7, o *router* R1 estabelecerá adjacências com os *routers* R2 e R3. Mas para que esta relação de vizinhança OSPF aconteça, eles deverão concordar nos valores de cinco campos: Intervalo de *Hello*, intervalo de *Dead*, tipo de rede (*Area-ID*), Autenticação e *Stub Area Flag*.

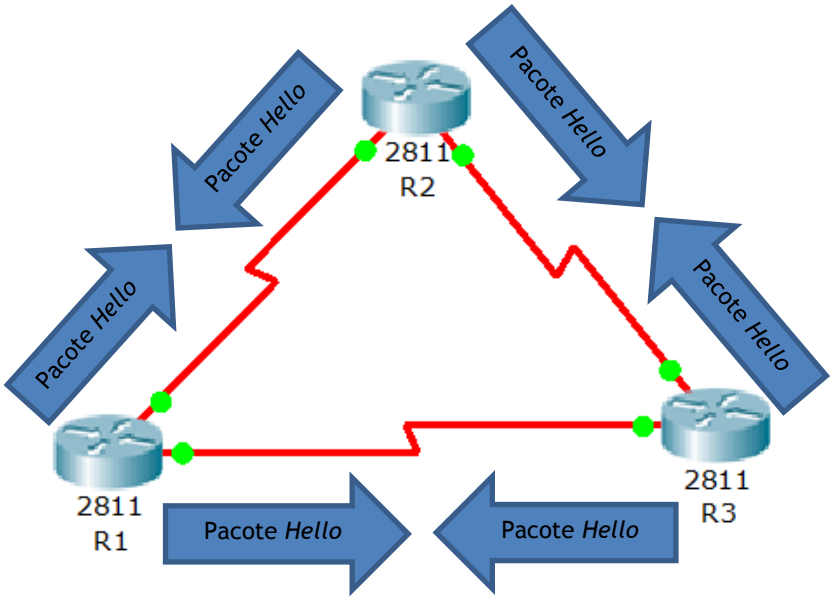

Figura 7 - Propagação de Pacotes OSPF *Hello*.

2.2.3 Intervalos de *Hello* e *Dead*

O intervalo de *Hello* do OSPF indica com que frequência o *router* OSPF transmite os seus pacotes *Hello*. Por norma, os pacotes *Hello* de OSPF são enviados a cada 10 segundos em segmentos multiacesso e ponto-a-ponto e a cada 30 segundos em segmentos de rede ponto-a-multiponto do tipo Frame Relay, X.25 e ATM.

Na maioria dos casos, os pacotes *Hello* do OSPF são enviados como *multicast* para um endereço reservado para *ALLSPFRouters* em 224.0.0.5. A utilização de um endereço *multicast* permite que um dispositivo ignore o pacote se a sua interface não estiver habilitada para aceitar pacotes OSPF ou que mesmo estando habilitada, não pertença a essa sessão de *multicast*, evitando assim um consumo adicional de tempo de processador de dispositivos que não participam nesta sessão.

O intervalo de *Dead* é o período, em segundos, que o *router* esperará para receber um pacote *Hello* antes de declarar o vizinho inativo. No caso da Cisco, este intervalo assume o valor padrão de quatro vezes o intervalo de *Hello*. Para segmentos multiacesso e ponto-a-ponto, este período é de 40 segundos. Para redes (*Non-Broadcast Multi-Access*) NBMA, o intervalo de *Dead* é de 120 segundos. Se o intervalo de *Dead* expirar antes de os *routers* receber num pacote *Hello*, o OSPF removerá aquele vizinho da sua base de dados *Link-state* e enviará as informações *Link-state* sobre o vizinho "inativo" para todas as interfaces OSPF habilitadas.

2.2.4 Identificação da Área, Autenticação e *Stub Area Flag*

Também é pré-condição de vizinhança que a identificação da área, a autenticação e a *Stub Area Flag* sejam verificadas e sejam idênticas. Portanto, para além dos valores de *Hello* e *Dead*, dois *routers* não formam uma vizinhança se não forem verificados os seguintes pontos:

- Dois *routers* com um segmento comum; as suas interfaces têm de pertencer à mesma área nesse segmento. Naturalmente, as interfaces devem pertencer à mesma sub-rede e ter máscara semelhante.

- A Autenticação OSPF permite a configuração de uma senha para uma área específica. Os *Routers* que se querem tornar vizinhos têm de trocar a mesma senha num determinado segmento.

- De forma similar, dois *routers* também têm que concordar com o valor da *Stub Area Flag* nos pacotes de *Hello*, de modo a se tornarem vizinhos.

2.2.5 Atualização de OSPF *Link-state*

As atualizações de *Link-State* (LSUs) são pacotes utilizados para atualizações de encaminhamento OSPF. Um pacote LSU pode conter 11 tipos diferentes de Anúncios *Link*-State (LSAs), como mostrado na tabela 2. A diferença entre os termos Atualização *Link*-State (LSU) e Anúncio *Link*-State (LSA) pode, às vezes, ser confusa. De vez em quando, estes termos

são utilizados um no lugar do outro. Um LSU contém um ou mais LSAs e ambos os termos podem ser utilizados para referir-se a informações de *Link-state* propagadas por *routers* OSPF.

Tabela 2 - Diferentes tipos de LSAs [14].

Tipo de LSA	Descrição
1	LSAs de *router*
2	LSAs de rede
3 ou 4	LSAs de resumo
5	LSAs externos de sistema autónomo
6	LSAs de OSPF *multicast*
7	Definido para *áreas not-so-stubby*
8	Atributos LSA externos para Protocolo de Encaminhamento de Borda (BGP)
9,10 ou11	LSAs opacos

Os *Router Links* (RL) são gerados por cada um dos *routers para as áreas a que pertencem e descrevem* o estado das interfaces do *router*.

Os *Links* de Rede (NL) são gerados por um DR de um segmento específico; Estes são uma indicação de *routers* conectados a esse segmento.

Os Links Resumo (SL) são as ligações entre áreas (tipo 3); estes *Links* listam as redes dentro de outras áreas, mas ainda pertencentes ao sistema autónomo. Os *Links* de Resumo são injetados pelo ABR do *backbone* para outras áreas e de outras áreas para o *backbone*. Estes *Links* são usados para a agregação entre as áreas. Outros tipos de *Links* de Resumo são os *Links* ASBR-Summary. Estas são as ligações do tipo 4 que apontam para o ASBR que certifica que todos os *routers* sabem o caminho para sair do sistema autónomo.

Os *Links* externos (EL), do tipo 5 são injetados por ASBR para o domínio.

A figura 8 mostra os diferentes tipos de *Link*. *Router* R1 gera um *router Link* (RL) e um *Link* de rede na área 1 (NL) uma vez que é *Domain Router* nesse específico segmento de rede

dessa área. O *router* R2 é um ABR, gera RL e *Links* de resumo nas áreas 0 e 1. Estes *Link*s de resumo pertencem a uma lista de redes que são trocadas entre as duas áreas.

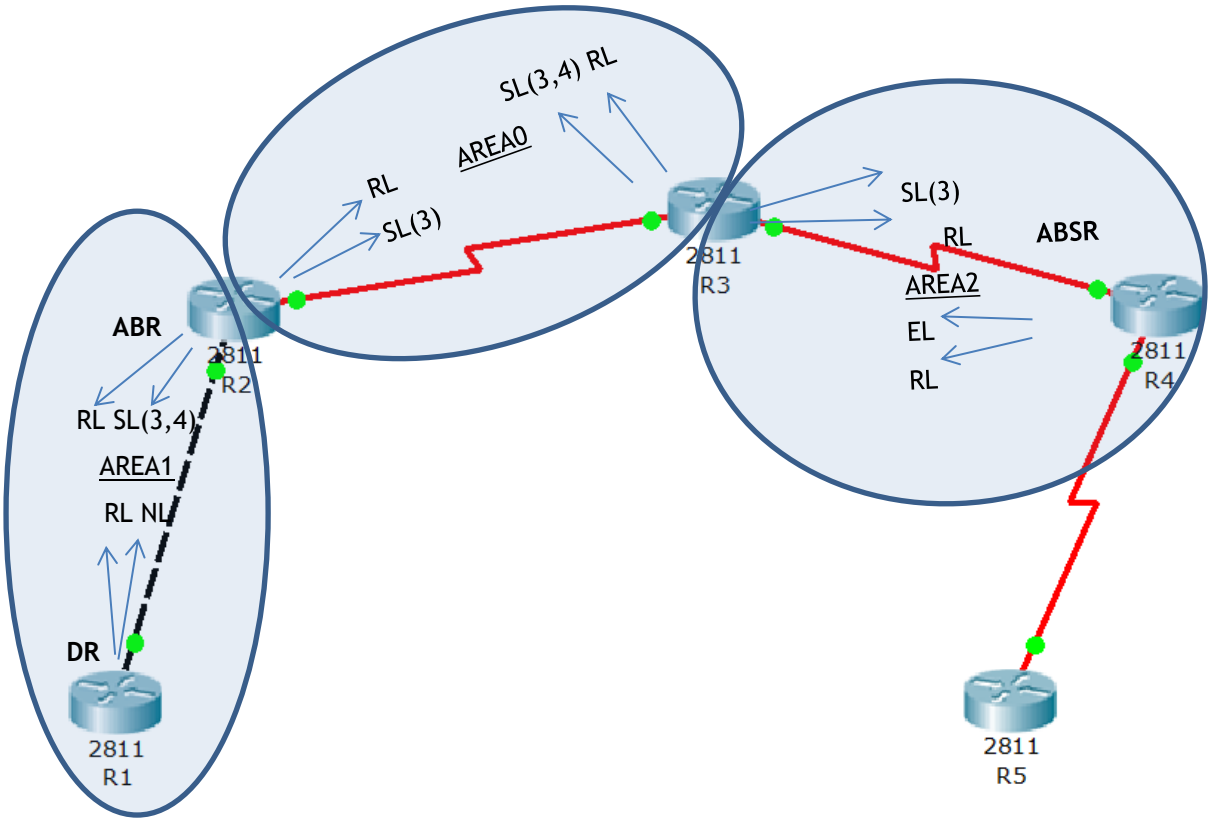

Figura 8 – Representação Esquemática ilustrando diferentes tipos de LSAs [15].

Um *Link* de resumo ASBR é também injetado pelo *router* R2 na área 1. Esta é uma indicação da existência de um ASBR, ou seja, R4.

Da mesma forma o *router* R3, que é outro ABR, gera um RL para as áreas 0 e 2, um SL(3) para a área 2 (dado que não está a anunciar qualquer ASBR) e um SL(3,4) para a área 0 anunciando R4. O *router* R4 gera um RL para a área 2 e gera um RL para as rotas externas aprendidas via BGP. As rotas externas serão inundadas por todo o domínio.

2.3 Algoritmo OSPF

2.3.1 Introdução

Cada *router* de OSPF mantém um base de dados *Link-state* contendo os LSAs recebidos de todos os outros *routers*. Quando um *router* recebe todos os LSAs e constrói a sua base de dados *Link-state* local, o OSPF utiliza o algoritmo *Shortest Path First* (SPF) de *Dijkstra* para criar uma árvore SPF. A árvore SPF é então utilizada para preencher a tabela de encaminhamento IP com os melhores caminhos para cada rede. Este algoritmo tem as seguintes fases:

1. Após a iniciação ou devido a qualquer alteração de informações de rotas, um *router* gera um anúncio de estado de *Link*. Este anúncio representa uma coleção de todos os estados de *Link* sobre nesse *router*.

2. Todos os *routers* trocam estados de *Link* através de *flooding*. Cada *router* que recebe uma atualização de estado de *Link* armazena uma cópia na sua base de dados de estado de *Link*s e somente depois propaga essas atualizações para outros *routers*.

3. Após concluída a atualização da base de dados de todos *routers*, cada *router* calcula uma árvore de caminho mais curto para todos os destinos. O algoritmo de Dijkstra é usado para calcular a árvore do caminho mais curto. Os destinos, o custo associado e o próximo salto para chegar a esses destinos formam a tabela de encaminhamento IP.

4. No caso de não ocorrer nenhuma alteração na rede OSPF, tais como o custo de um *Link* ou uma rede que está sendo adicionada ou excluída, não serão feitas alterações ou cálculos enquanto estas condições se verificarem. Quando existirem de alterações ou atualizações, estas serão comunicadas por meio de pacotes de estado de *Link* e o algoritmo de Dijkstra é recalculado para encontrar novamente o caminho mais curto.

O algoritmo coloca cada *router* na raiz da árvore e calcula o caminho mais curto para cada destino baseado em custos acumulados necessários para chegar a um determinado destino. Apesar de todos os *routers* terem efetuado os seus cálculos sobre a base de dados de estados dos *Link*s, estes têm uma vista única da topologia da rede.

2.3.2 Distâncias Administrativas

A distância administrativa (AD, *administrative distance*) define a preferência de uma origem de encaminhamento. Cada origem de encaminhamento, incluindo protocolos de encaminhamento específicos, rotas estáticas e até mesmo redes diretamente conectadas, tomam um valor no parâmetro AD consoante o protocolo em causa. Os *routers* usam o recurso AD para selecionar o melhor caminho quando recebem dois destinos idênticos por interfaces diferentes.

A distância administrativa é um valor inteiro de 0 a 255. Quanto menor o valor, melhor será a origem da rota. A melhor distância administrativa é a de 0. Só uma rede diretamente conectada tem uma distância administrativa de 0. Essa distância não pode ser alterada.

É possível modificar a distância administrativa de rotas estáticas e de protocolos de encaminhamento dinâmico. Uma distância administrativa de 255 significa que o *router* não confia na origem dessa rota e não será instalada na tabela de encaminhamento. A tabela 3 mostra distâncias administrativas de vários protocolos de encaminhamento.

Tabela 3 - Distâncias administrativas de protocolos de encaminhamento.

Protocolo	Distância Administrativa
Diretamente conectado	0
Rota estática	1
EIGRP Rota sumarizada	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externo	170
BGP interno	200
Desconhecida	255

2.4 Autenticação

2.4.1 Introdução

É possível autenticar os pacotes OSPF de modo a que os *routers* possam participar num domínio pré-definido *passwords*. Por omissão a password usada é *null* o que leva a que as trocas de tabelas de encaminhamentos não sejam autenticadas. Existem dois métodos de autenticação: *Simple password authentication* que autentica mediante a apresentação de uma chave que é definida por área e *Message Digest Authentication* (MD-5) que é uma autenticação criptográfica onde, ao invés de transmitir uma chave, este envia uma *message digest* gerada internamente. A seguir apresenta-se uma breve descrição sobre estes dois métodos de autenticação.

2.4.2 Simple Password Authentication

Este modo de autenticação permite que uma chave seja definida por área. Os *routers* que se encontram na mesma área e que queiram participar nesse domínio de encaminhamento deverão usar a mesma chave. Os comandos necessários para configurar este tipo de autenticação são: i*p ospf authentication-key* (a ser efetuado sobre uma interface) e a*rea* <*area-id*> *authentication* (a ser efetuado no *process-id* da instancia de OSPF). Na figura 9 temos um exemplo de como configurar a *Simple Password Authentication*.

```
configure terminal
interface fa0/0
ip address 10.10.10.10 255.255.255.0
ip ospf authentication-key mypassword
exit
router ospf 5
network 10.10.0.0 0.0.255.255 area 10
area 10 authentication
```

Figura 9 – Configuração de Simple Password Authentication.

2.4.3 Message Digest Authentication

A Message Digest Authentication é uma autenticação criptográfica. São configuradas em cada *router* uma chave e uma chave-id. O *router* usa um algoritmo baseado no pacote OSPF, na chave e na chave-id para gerar uma *message digest* que fica anexada a esse pacote. Ao contrário da autenticação simples, a chave não é trocada sobre a ligação. Um número de sequência não-decrescente é incluído em cada pacote OSPF para proteger contra ataques de replicação. Este método também permite transições ininterruptas entre chaves. Esta funcionalidade é muito útil para administradores de redes que desejam mudar a senha do OSPF sem interromper as comunicações.

Se uma interface é configurada com uma nova chave, o *router* irá enviar várias cópias do mesmo pacote, cada um autenticado por chaves diferentes. O *router* irá parar de enviar estes pacotes duplicados assim que detete que todos seus vizinhos adotaram a nova chave. Na figura 10 é apresentado um exemplo dos comandos necessários para configurar a *message digest authentication*.

```
configure terminal
interface fa0/0
ip address 10.10.10.10 255.255.255.0
ip ospf message-digest-key 10 md5 mypassword
exit
router ospf 5
network 10.10.0.0 0.0.255.255 area 0
area 0 authentication message-digest
```

Figura 10 - Configuração de Message Digest Authentication.

2.5 Configurar o OSPF

O OSPF está habilitado com o comando de configuração global *router* ospf process-id, conforme se mostra na figura 11. O process-id é um número entre 1 e 65535 escolhido pelo administrador de redes. O process-id tem apenas significado local, isto é, não tem que corresponder a outros *routers* OSPF para estabelecer adjacências com outros *routers*. Isto

difere do EIGRP, o ID do processo EIGRP ou o número do sistema autónomo precisa ser idêntico para que dois vizinhos EIGRP se tornem adjacentes.

```
Configure terminal
Router ospf 10
```

Figura 11 - Configuração para habilitar OSPF.

O comando *network* utilizado com o OSPF tem a mesma função que tem quando utilizado por outros protocolos de encaminhamento IGP:

- As interfaces de um *router* que corresponderem ao endereço de rede do comando *network* serão habilitadas para enviar e receber pacotes OSPF.
- Esta rede (ou sub-rede) será incluída nas atualizações de encaminhamento OSPF.
- O comando network é utilizado no modo de configuração de encaminhamento.

```
Configure terminal
Router ospf 10
network 192.168.0.0 0.0.255.255 area 10
```

Figura 12 - Configuração para adicionar redes

às atualizações de encaminhamento OSPF.

Na figura 12, o comando *network* do OSPF utiliza uma combinação de endereço de rede (192.168.0.0) e *wildcard mask* (0.0.255.255) semelhantes àquela que pode ser utilizada pelo EIGRP. Porém, ao contrário do EIGRP que usa máscaras, o OSPF exige uma *wildcard mask*. O endereço de rede, juntamente com a *wildcard mask*, é utilizado para especificar a interface ou conjunto de interfaces que serão habilitadas para OSPF através do comando *network*.

No caso do EIGRP, a máscara do tipo *wildcard* pode ser configurada como o inverso de uma máscara de sub-rede. Por exemplo, a interface *FastEthernet* 0/0 de um *router* está na rede 192.168.1.16/28. A máscara de sub-rede para esta interface é /28 ou 255.255.255.240. O inverso da máscara de sub-rede resulta numa *wildcard mask*. Na figura 13 é mostrada uma conversão de uma máscara para uma *wildcard mask*.

```
   255.255.255.255
 - 255.255.255.240 (Máscara)
     0.  0.  0. 15 (wildcard mask)
```

Figura 13 - Cálculo para converter máscaras em *wildcard masks*.

A área *area-id* refere-se à área OSPF. Uma área OSPF é um grupo de *routers* que partilham informações *Link-state*. Todos os *routers* OSPF na mesma área devem ter as mesmas informações *Link-state* nas suas bases de dados *Link-state*. Isto é realizado por *routers* que enviam os seus *Link-states* individuais a todos os outros *routers* na área.

Uma rede OSPF também pode ser configurada como áreas múltiplas. Existem várias vantagens de se configurarem redes OSPF como múltiplas áreas e, consequentemente, bases de dados *Link-state* menores e uma maior capacidade de isolar problemas de rede instáveis dentro de uma área. De certa forma, esta abordagem faz lembrar aquando a introdução de VLANs (*Virtual Local Area Network*), que veio reduzir a congestão das redes ao nível do desempenho devido ao tamanho dos domínios de *broadcast*.

Quando todos os *routers* estiverem dentro da mesma área OSPF, os comandos de rede devem ser configurados com a mesma area-id em todos os *routers*. Embora qualquer area-id possa ser utilizada, é recomendado utilizar uma area-id de 0 com o OSPF de área única. Esta convenção facilitará o processo no caso de a rede ser posteriormente configurada como OSPF com múltiplas áreas, onde a área 0 torna-se a área de *backbone*.

A figura 14 consiste numa configuração dos três *routers* da figura 7, habilitando o OSPF em todas as interfaces. Neste ponto, e após a convergência da rede, todos os *routers* conseguirão enviar *pings* de e para todas as interfaces lógicas.

```
R1(config-router)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 192.168.2.0 0.0.0.255 area 0
R1(config-router)#network 192.168.3.0 0.0.0.255 area 0
R2(config-router)#router ospf 2
R2(config-router)#network 192.168.4.0 0.0.0.255 area 0
R2(config-router)#network 192.168.5.0 0.0.0.255 area 0
R2(config-router)#network 192.168.6.0 0.0.0.255 area 0
R3(config-router)#router ospf 3
R3(config-router)#network 192.168.7.0 0.0.0.255 area 0
R3(config-router)#network 192.168.8.0 0.0.0.255 area 0
R3(config-router)#network 192.168.9.0 0.0.0.255 area 0
```

Figura 14 - Configuração de três *routers* de modo a habilitar

a partilha de tabelas de encaminhamento numa área única.

2.6 Determinação da ID do Router

A ID do *Router* OSPF é utilizada para identificar unicamente cada *router* no domínio de encaminhamento OSPF. Uma ID de *Router* é simplesmente um endereço IP. Os *routers* produzem a sua ID com base em três critérios e com a seguinte precedência:

1. Utilizam o endereço IP configurado com o comando *router*-id de OSPF.

2. Se o *router*-id não estiver configurado, o *router* escolherá o endereço IP mais alto de qualquer uma das suas interfaces de *loopback*.

3. Se nenhuma interface de *loopback* estiver configurada, o *router* escolherá o endereço IP ativo mais alto das suas interfaces físicas.

A figura 15 ilustra uma configuração de interfaces lógicas e o parâmetro *router-id* onde endereço IP escolhido na eleição do *router*-id foi 1.1.1.1. Este resultado foi estaticamente

configurado no processo de OSPF 5 e prevalece sobre qualquer outra configuração de IP nas interfaces físicas ou de *loopback*.

```
configure terminal
Interface l0
ip address 192.168.100.1 255.255.255.252
interface s0/0/1
ip address 192.168.2.1 255.255.255.240
no shutdown
exit
router ospf 5
router-id 1.1.1.1
…
Router#show ip ospf
Routing Process "ospf 5" with ID 1.1.1.1
<resto do resultado omitido>
```

Figura 15 - Eleição de *router*-id onde a configuração do *router*-id prevalece.

Na figura 16 podemos verificar que o endereço IP escolhido para *router*-id foi 192.168.100.1, dado que não existindo uma configuração explícita do *router*-id no processo OSPF, a escolha recaiu numa interface de *loopback* 0 com o IP mais alto.

```
configure terminal
Interface l0
ip address 192.168.100.1 255.255.255.252
Interface l1
ip address 192.168.10.1 255.255.255.252
interface s0/0/1
ip address 192.168.200.1 255.255.255.240
no shutdown
…
Router#show ip ospf
Routing Process "ospf 5" with ID 192.168.100.1
<resto do resultado omitido>
```

Figura 16 - Eleição de *router*-id onde o endereço IP da interface de loopback prevalece.

Na figura 17 podemos verificar que o IP escolhido para *router*-id foi 192.168.2.1, dado que não existindo uma configuração explícita do *router*-id no processo OSPF nem interfaces de *loopback*, a escolha recaiu no IP mais alto entre todas as interfaces físicas ativas.

```
configure terminal
Interface s0/0/0
ip address 192.168.100.1 255.255.255.252
interface s0/0/1
ip address 192.168.2.1 255.255.255.240
no shutdown
…
Router#show ip ospf
Routing Process "ospf 5" with ID 192.168.2.1
<resto do resultado omitido>
```

Figura 17 - Eleição de *router*-id onde o endereço IP da interface prevalece.

2.6.1 Endereços de Loopback

Se o comando *router*-id do OSPF não for utilizado e as interfaces de *loopback* estiverem configuradas, o OSPF escolherá o endereço IP mais alto de qualquer uma das suas interfaces de *loopback*. Um endereço de *loopback* é uma interface virtual e está automaticamente no estado *up* quando configurado. Na figura 18, podemos ver uma sucessão de comandos para configurar um interface de *loopback*. Estas interfaces não precisam do comando *no shutdown* dado que quando entramos em modo de configuração dessa interface de loopback, esta e o *line protocol* ficam com o seu estado de operacionalidade em cima.

```
Router(config)#interface loopback 1
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
Router(config-if)#ip address 192.168.100.1 255.255.255.0
Router(config-if)#interface loopback 2
%LINK-5-CHANGED: Interface Loopback2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback2, changed state to up
Router(config-if)#ip address 192.168.99.1 255.255.255.240
```

Figura 18 - Configuração de interfaces de *loopback*.

Na figura 19, todos os três *routers* foram configurados com endereços de *loopback* para representar as IDs do *router* OSPF. A vantagem de utilizar uma interface de *loopback* é que – diferente das interfaces físicas – ela não pode falhar. Não há nenhum cabo ou dispositivo adjacente real dos quais a interface de *loopback* dependa para estar no estado up. Portanto, utilizar um endereço de *loopback* para a ID do *router* fornece estabilidade ao processo OSPF.

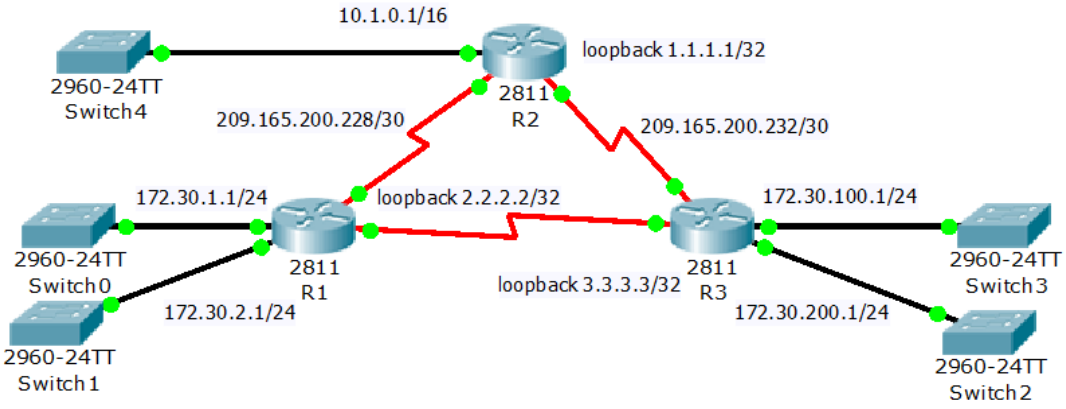

Figura 19 - Topologia de rede com interfaces de *loopback* configuradas.

2.6.2 O Comando Router-id do OSPF

O comando *router*-id do OSPF tem prioridade sobre os endereços IP de interface de *loopback* e física para determinar a ID do *router*. Um exemplo da utilização deste comando pode ser observado na figura 20:

```
Router(config)#router ospf process-id
Router(config-router)#router-id ip-address
```

Figura 20 - Sintaxe do comando *router*-id do OSPF.

2.6.3 Modificar a ID do Router

A ID do *router* é selecionada quando o OSPF é configurado através do seu primeiro comando *network* de OSPF. Se o comando *router*-id de OSPF ou o endereço de loopback for configurado depois do comando *network* do OSPF, a ID do *router* será derivada da interface com o endereço IP ativo mais alto.

A ID do *router* pode ser modificada com o endereço IP através do comando *router*-id de OSPF e seguidamente, reiniciar o *router* (com o comando *reload*) ou, preferencialmente, utilizar o comando clear *ip ospf process* tal como indicado na figura 21.

```
Router#clear ip ospf process
```

Figura 21 - Comando para forçar uma nova eleição de *router*-id.

2.7.4 IDs de Router duplicadas

Quando dois *routers* tiverem a mesma ID de *router* num domínio OSPF, o encaminhamento poderá não funcionar corretamente. Se a ID do *router* for a mesma em dois *routers* vizinhos, o estabelecimento da vizinhança pode não ocorrer. Quando ocorrerem IDs de *router* OSPF duplicadas, o IOS exibirá uma mensagem semelhante à da figura 22.

```
%OSPF-4-DUP_RTRID1: Detected router with duplicate router ID
```

Figura 22 - Mensagem de erro quando são detetadas duas *routers*-id idênticas.

2.7 Métrica do Open Shortest Path First

A métrica do OSPF é chamada de custo. Da RFC 2328: "Um custo está associado com o lado de saída de cada interface do *router*. Este custo é configurável pelo administrador do sistema. Quanto menor o custo, mais provável será o uso da interface para encaminhar o tráfego de dados."

2.7.1 Definição

Note-se que o RFC 2328 não especifica que valores devem ser utilizados para determinar o custo. Este valor do custo está associado às larguras de banda cumulativas das interfaces de saída do *router* para a rede de destino. Em cada *router*, o custo para uma interface é calculado como 10^8 dividido pela largura de banda em *bps*. Isto é conhecido como largura de banda de referência. Divide-se 10^8 pela largura de banda da interface de modo que as interfaces com os valores de largura de banda mais altos tenham um menor custo calculado.

No entanto, nas métricas de encaminhamento, a rota de custo mais baixo é a rota preferida (por exemplo, com RIP, 3 saltos é melhor que 10). A tabela 4 mostra os custos de OSPF por omissão para vários tipos de interfaces.

Tabela 4 - Custo OSPF associado à velocidade das interfaces de um *router* [16].

Tipos de Interface	10^8/bps = Custo
Fast Ethernet e mais rápida	10^8 / 100.000.000 bps = 1
Ethernet	10^8 / 10.000.000 bps = 10
E1	10^8 / 2.048.000 bps = 48
T1	10^8 / 1.544.000 bps = 64
128 Kbps	10^8 / 128.000 bps = 781
64 Kbps	10^8 / 64.000 bps = 1562
56 kbps	10^8 / 56.000 bps = 1785

A métrica de uma interface OSPF é uma indicação do custo associado ao envio de pacotes por uma determinada interface. Este custo é inversamente proporcional à largura de banda dessa interface, isto é, a uma elevada largura de banda está associado a um custo baixo ou, quanto maior for o custo, menor será a largura de banda disponível. Por omissão, o custo de uma interface é calculado com base na sua largura de banda. No entanto este valor poder ser alterado recorrendo ao comando: ip ospf cost no modo global de configuração de interface.

2.7.2 Largura de Banda de Referência

A largura de banda de referência é padronizada em 10^8, isto é, 100.000.000 bps ou 100 Mbps. Isto resulta em interfaces com uma largura de banda de 100 Mbps ou maiores tendo o mesmo custo de OSPF de 1. A largura de banda de referência pode ser modificada para acomodar redes com *Link*s mais rápidos de 100.000.000 bps (100 Mbps), usando o comando OSPF *auto-cost reference-bandwidth*. Quando este comando for necessário, recomenda-se que ele seja utilizado em todos os *routers* de modo que a métrica de encaminhamento OSPF permaneça consistente.

2.7.3 Largura de Banda Padrão das Interfaces

O comando *show interface* permite visualizar várias caraterísticas de uma interface, nomeadamente a largura de banda. Este valor em muitas interfaces série toma um valor por omissão de T1 (1.544 Mbps). Porém, algumas interfaces serie podem padronizar-se a 128 kbps. Portanto, nunca se deve supor que o OSPF está a utilizar um valor de largura de banda específico. Deve sempre ser verificado o valor por omissão com o comando *show interface*. Este valor de largura de banda não afeta realmente a velocidade do *Link*. É utilizado por alguns protocolos de encaminhamento para calcular a métrica do encaminhamento. Em interfaces série, a velocidade real do *Link* é diferente da largura de banda padrão. Assim, torna-se importante que o valor da largura de banda reflita a velocidade real do *Link* de forma que a tabela de encaminhamento tenha informações precisas sobre o melhor caminho.

Por exemplo, um fornecedor de serviços de rede fornece um *Link* a 128kbps. No entanto as portas negoceiam a 100 mbps. Esta situação requer que o custo dessa interface seja manualmente alterada para refletir a velocidade contratada e não a velocidade em que as portas negociaram. Esta situação leva a que os custos calculados nessa interface não reflitam a realidade e inclusive pode acontecer que certos pacotes sejam encaminhados para esta interface em detrimento de interfaces mais rápidas.

Atualmente temos velocidades de *Link* que são muito mais rápidas do que as velocidades da Fast Ethernet, nomeadamente Gigabit Ethernet, 10GigE e 40GigE. Utilizar uma largura de banda de referência de 100.000.000 resulta em interfaces com valores de largura de banda de 100 Mbps e mais altos, tendo o mesmo custo de OSPF de 1.

Para obter cálculos de custo mais precisos, é necessário ajustar o valor de largura de banda de referência. A largura de banda de referência pode ser modificada para acomodar estes *Link*s mais rápidos utilizando o comando *auto-cost reference-bandwidth* <*speed*> do OSPF. Esta configuração tem de ser replicada em todos os *routers* para que os custos calculados sejam consistentes.

2.8 Redes Multiacesso

2.8.1 Introdução

Uma rede multiacesso é uma rede com mais de dois dispositivos que partilham o mesmo meio. As redes locais *Ethernet* são um exemplo de uma rede multiacesso no mesmo domínio de *broadcast*. Denominam-se redes multiacesso porque pode haver vários *hosts*, impressoras,

routers e outros dispositivos que são todos membros da mesma rede ou VLAN (*Virtual Local Area Network*). Por outro lado, numa rede ponto-a-ponto existem apenas dois dispositivos em rede, um em cada ponta. As figuras 23 a 27 ilustram exemplos de redes ponto-a-ponto, multiacesso com *broadcast*, sem *broadcast* multiacesso (NBMA), ponto-a-multiponto e com *Link*s virtuais, respetivamente.

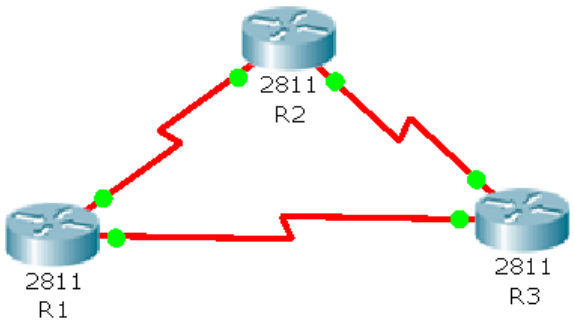

Figura 23 - Rede ponto-a-ponto.

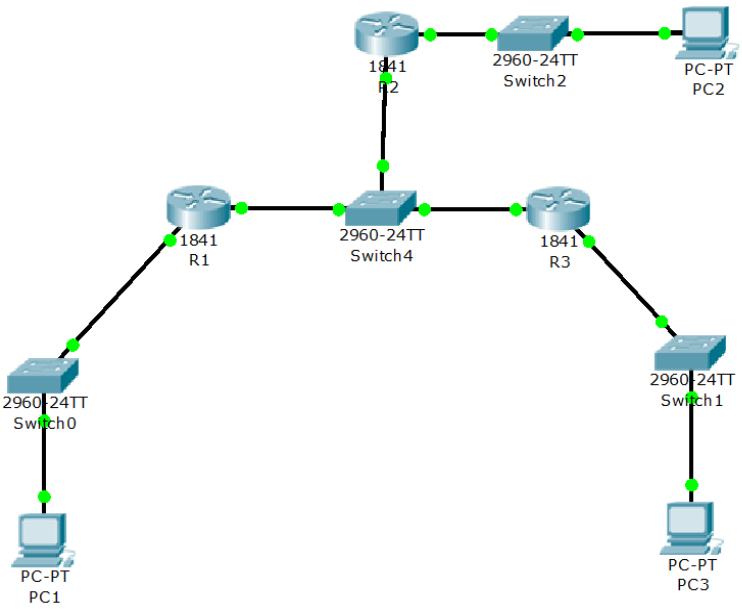

Figura 24 - Rede multiacesso com *broadcast*.

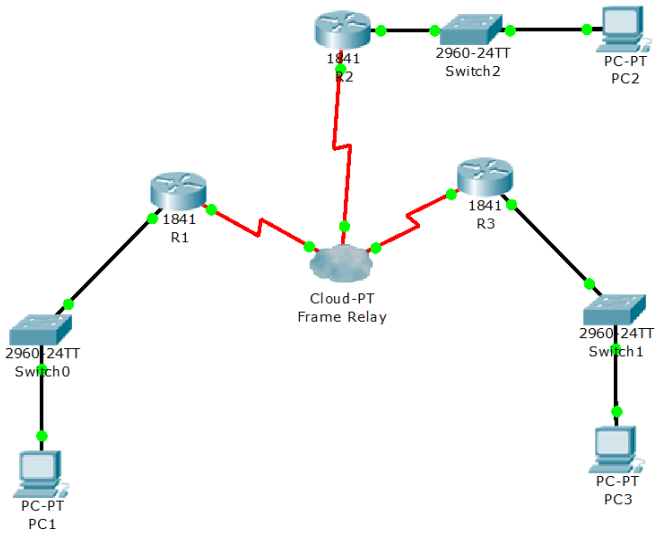

Figura 25 - Rede sem *broadcast* multiacesso (NBMA).

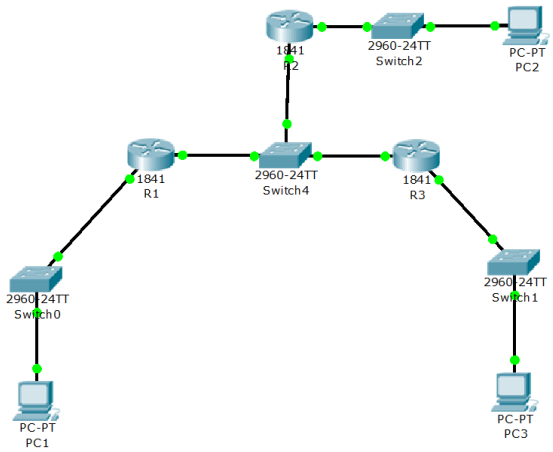

Figura 26 - Rede ponto-a-multiponto.

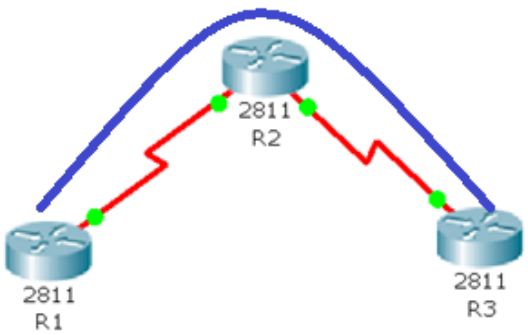

Figura 27 - Rede com *Link*s virtuais.

2.8.2 Eleição do *Domain Router* e do *Backup Domain Router*

As eleições do *Domain Router (*DR*) e Backup Domain Router* (BDR) não ocorrem em redes ponto-a-ponto. Portanto, numa topologia com três *routers* padrão, R1, R2 e R3, não, é necessário eleger um DR e um BDR, porque os *Link*s entre estes *routers* não representam redes multiacesso.

Para reduzir a quantidade de tráfego OSPF nas redes multiacesso, o OSPF elege um DR e um BDR. O DR é responsável por atualizar todos os outros *routers* OSPF (chamados de DROthers) quando uma alteração ocorrer na rede multiacesso. O BDR monitora o DR e assume-se como DR se o DR atual falhar.

A figura 28 ilustra uma situação em que os *routers* estão conectados através de *Link*s ponto-a-ponto e não em modo de multiacesso o que resulta na não necessidade de eleger o DR ou o BDR.

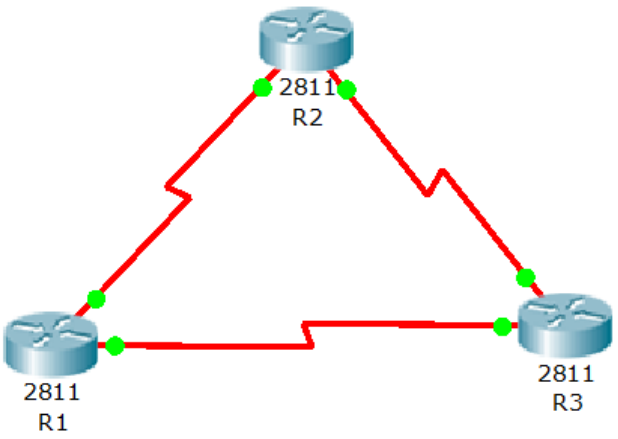

Figura 28 - *Routers* com *links* ponto-a-ponto onde não existe eleição de DR/BDR.

A eleição dos *routers* DR e BDR é feita de seguinte forma:

1. DR: *Router* com a mais alta prioridade de interface OSPF.
2. BDR: *Router* com a segunda mais alta prioridade de interface OSPF.
3. Se as prioridades de interface OSPF são iguais, a ID de *router* mais alta é utilizada para desempatar.

OS DROthers só formam adjacências FULL com o DR e BDR, mas ainda formarão uma adjacência de vizinho com qualquer DROther que se unir à rede. Adjacência FULL acontece quando dois *routers* têm informação completa um do outro, isto é, ambos trocaram as suas bases de dados na íntegra. Todos os *routers* DROther na rede multiacesso recebem pacotes *Hello* de todos os outros *routers DROther*. Deste modo, ficam com a informação de todos os *routers* na rede. Quando dois *routers* DROther formam uma adjacência de vizinho o estado é exibido como 2WAY. O vizinho OSPF recebe o estado de 2WAY quando uma ligação bidirecional é estabelecida.

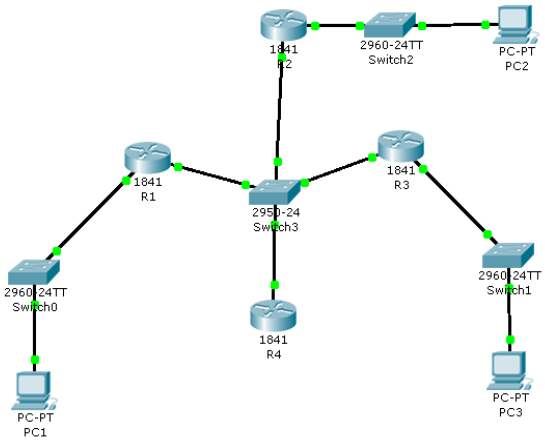

Figura 29 - Esquema de rede do tipo multiacesso em OSPF.

Quando um *router* vê que dois dos seus vizinhos são DR e BDR então é porque ele próprio é um DROther. Isto pode ser verificado com o uso do comando *show ip ospf interface* <*interface*>. Este comando também fornece mais informações nomeadamente as IDs dos DR e BDR numa rede multiacesso, figura 29.

O processo de eleição do DR e do BDR acontece assim que o primeiro *router* com uma interface habilitada de OSPF está ativo na rede multiacesso. Isto pode acontecer quando os *routers* forem ligados ou quando o comando *network* do OSPF para aquela interface for configurado. O processo de eleição demora apenas alguns segundos. Se todos os *routers* na rede multiacesso não terminarem a iniciação, é possível que um *router* com uma ID de *router* inferior se torne o DR. Este poderia ser um *router lower-end* que demorou menos tempo para iniciar. Quando o DR é eleito, ele permanece como DR até que uma das condições seguintes ocorra:

- O DR falha.
- O processo OSPF no DR falha.
- A interface multiacesso no DR falha.

2.8.2 Prioridade de Interfaces OSPF

Uma vez que o DR se torna o foco para coleta e distribuição de LSAs, é importante que este *router* tenha CPU suficiente e capacidade de memória para arcar com a responsabilidade. Em vez de confiar na ID do *router* para decidir quais *routers* são eleitos DR e BDR, é preferível controlar a eleição destes *routers* com o comando de interface *ip ospf priority*.

```
Router(config-if)#ip ospf priority {0 - 255}
```

Por omissão, o valor da prioridade é 1 para todas as interfaces do *router*. Portanto, a ID de *router* determina o DR e o BDR. No entanto, se o valor padrão for alterado de 1 para um valor mais elevado, o *router* com a prioridade mais alta se tornará o DR e o *router* com a próxima prioridade mais alta irá tornar-se o BDR. Um valor de 0 desabilita a hipótese de um *router* ser qualificado como DR ou BDR. Como as prioridades são um valor específico de interface, elas proporcionam melhor controlo das redes multiacesso OSPF. É igualmente possível que um determinado *router* seja o DR numa rede e um DROther em outra.

2.9 Redistribuição de uma Rota Padrão em OSPF

Tal como com RIP e EIGRP, um *router* conectado à Internet é utilizado para propagar uma rota padrão a outros *routers* no domínio de encaminhamento OSPF. Este *router* é por vezes, designado por *router* de borda, de entrada ou *router gateway*. Porém, na terminologia OSPF, o *router* localizado entre um domínio de encaminhamento OSPF e uma rede não-OSPF é designado por ASBR. Para propagar rotas estáticas aos restantes *routers* dessa área usa-se o comando *default-information orginate* no modo global de configuração dentro do processo *router ospf* <*number*>.

2.10 Comparação de RIP com OSPF

O rápido crescimento e expansão das redes de hoje levaram o RIP aos seus limites. Este possui certas limitações que podem causar problemas em redes de grandes dimensões. Uma rede que tem como protocolo de encaminhamento o RIP e tem destinos com um número de saltos superior a 15 resulta que essas redes ficarão com o estado de inacessíveis.

O RIP não pode lidar com máscaras de comprimento variável de sub-rede (VLSM), o que resulta numa utilização de endereçamento IP ineficiente, além do fato das topologias descontínuas não convergirem com RIPv1. A figura 30 mostra uma topologia de rede e alguns endereçamentos referentes às redes locais (/24) e às redes ponto a ponto (/30).

Apesar da configuração RIPv1 estar correta, os *routers* são incapazes de determinar todas as redes dessa topologia descontínua dado que um *router* só anunciará endereços de redes principais por interfaces que não pertencem à rota anunciada. Como resultado, R1 não anunciará 172.10.1.0 ou 172.10.2.0 para R2 na rede 193.136.67.0. R3 não anunciará 172.10.150.0 ou 172.10.151.0 para R2 na rede 193.136.67.0. No entanto, os *routers* R1 e R3 anunciarão o endereço de rede principal 172.10.0.0.

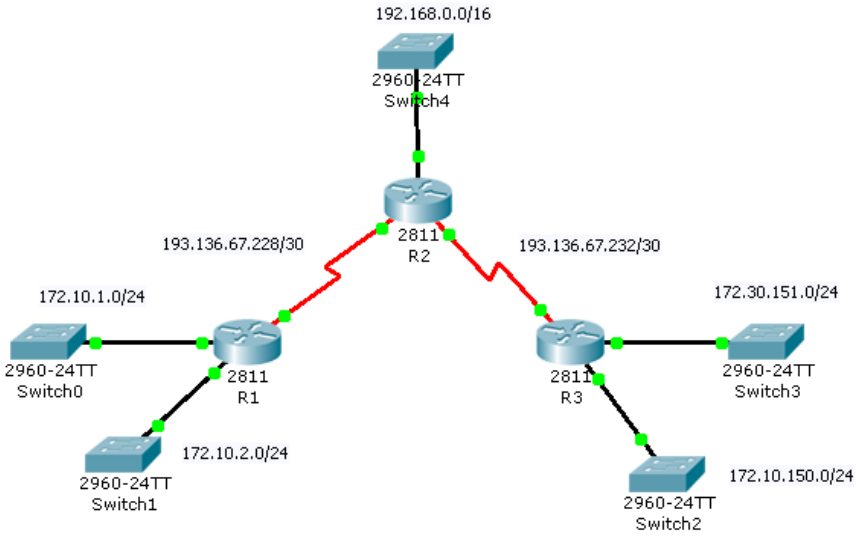

Figura 30 - Topologia descontígua que não converge em RIPv1.

Como resultado e dado que não existe inclusão da máscara de sub-rede na atualização de encaminhamento, RIPv1 não pode anunciar informações de encaminhamento específicas que permitirão aos *routers* estabeleçam a rota correta para as sub-redes 172.10.0.0/24. Como resultado final: R1 não tem nenhuma rota para as redes locais conectadas a R3, R3 não tem nenhuma rota para as redes locais conectadas a R1, R2 tem dois caminhos de custos iguais para a rede 172.10.0.0. R2 fará balanceamento de carga do tráfego destinado a qualquer sub-rede de 172.10.0.0. Isto significa que R1 obterá metade do tráfego e R3 obterá a outra a metade independentemente do destino do tráfego ser ou não destinado a uma das suas redes locais.

As transmissões periódicas da tabela de rotas completa em *broadcast* consome uma grande quantidade de largura de banda com especial impacto em redes de baixa largura de banda. O RIP converge mais lentamente do que o OSPF, nomeadamente em redes de grande diâmetro, podendo esta convergência chegar a vários minutos. O RIP não tem noção de atrasos de rede e custos de ligação e as decisões de encaminhamento são baseadas na contagem de saltos. O caminho com o menor número de saltos para o destino é sempre preferível, mesmo que o caminho mais longo tenha uma largura de banda melhor agregada e atrasos menores. Na figura 31 podemos facilmente verificar que o troço com mais largura de banda entre R1 e R3 seria através de R2. No entanto, o protocolo RIP irá escolher o troço que está diretamente ligado a R3 e que tem um menor número de saltos.

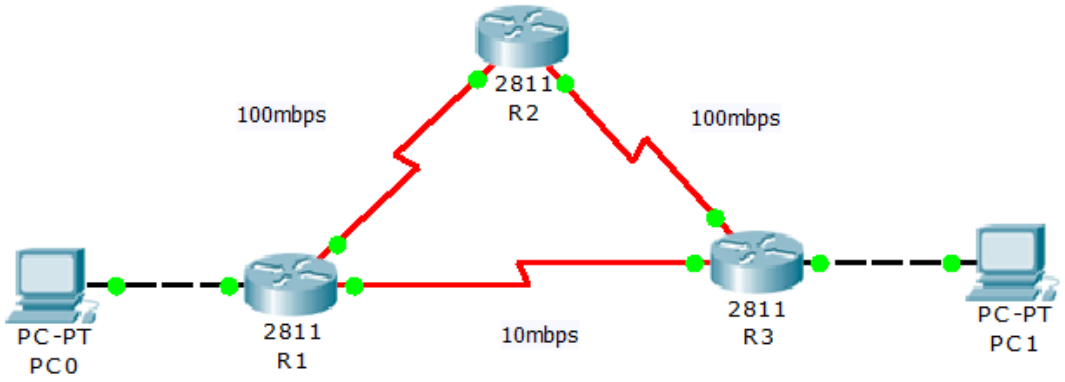

Figura 31 - O menor número de saltos não implica o melhor caminho.

As redes RIP são redes planas, não existindo os conceitos de áreas ou limites. Com a introdução de encaminhamento sem classes e sem o uso inteligente da agregação e sumarização, as redes RIP começaram a conhecer os seus limites e consequente término.

De modo a ultrapassar estas limitações surgiu o RIPv2 com funcionalidades adicionais tais como VLSM, autenticação e atualizações de encaminhamento em *multicast*. Apesar de ter sido uma melhoria significativa em relação ao RIPv1, ainda assim sofre de caraterísticas que não coabitam com as grandes redes dos dias de hoje tais como o limite de saltos e os tempos de convergência.

Com o OSPF não há limitação sobre a contagem de saltos e o uso inteligente de VLSM é muito útil na alocação de endereços IP. OSPF usa *multicast* para enviar atualizações *Link-state* o que garante uma menor ocupação dos processadores dos *routers* que não estão a escutar pacotes OSPF. Estas atualizações de encaminhamento só são enviadas aquando da alteração no encaminhamento, o que resulta numa poupança da largura de banda. O OSPF tem uma melhor convergência em relação ao RIP dado que as mudanças de encaminhamento são

propagadas instantaneamente e não periodicamente. Permite um melhor balanceamento de carga bem como uma melhor definição lógica de redes onde os *routers* podem ser divididos em áreas. Esta caraterística limita a explosão de atualizações de *Link-states* sobre toda a rede, além de possibilitar um mecanismo para agregar rotas e reduzir a propagação desnecessária de informações de sub-redes. Com recurso à autenticação passa a ser mais seguro a propagação/aprendizagem de rotas de fontes fidedignas. O OSPF permite a transferência e marcação de rotas externas injetadas num Sistema Autónomo mantendo o controlo das rotas externas injetadas por protocolos exteriores tal como, por exemplo, o (*Border Gateway Protocol*) BGP.

Toda esta panóplia de funcionalidades leva, naturalmente, a uma maior complexidade na configuração e solução de problemas das redes OSPF. Os administradores de redes que estavam habituados à simplicidade do RIP ou, até, ao encaminhamento estático, são agora desafiados com uma enorme quantidade de informação nova sobre este protocolo de encaminhamento. Em alguns casos é necessário um aumento da memória e CPU dos *routers* de modo a acomodar este protocolo.

Dado que o OSPF é um protocolo do tipo *Link-state*, existe uma descrição da interface e da sua relação com os seus *routers* vizinhos. Uma descrição da interface inclui, nomeadamente, o endereço de IP da interface, a máscara, o tipo de rede a que está ligado e os *routers* ligados à referida rede. A coleção de todos estes estados do *Link* formam uma base de dados *Link-state*.

2.11 Encapsulamento de mensagens OSPF

2.11.1 Introdução

Os dados de uma mensagem OSPF são encapsulados num pacote IP que podem incluir um dos cinco tipos de pacote OSPF: *Hello*, DBD (Descrição de Base de Dados), LSR (Requisição de *Link* State), LSU (Atualização de *Link-State*) e LSAck (*Link State Acknowledgement*).

O cabeçalho do pacote OSPF é sempre incluído em todos os pacotes de natureza OSPF, independentemente do seu tipo. Os dados específicos do cabeçalho e do tipo do pacote OSPF são então encapsulados num pacote IP. No cabeçalho de pacote IP, o campo de protocolo é definido como 89 para indicar OSPF e o endereço de destino é definido como um dos dois endereços *multicast*: 224.0.0.5 ou 224.0.0.6. A razão de existirem dois IPs *multicast* para

encaminhar os pacotes *Hello* prende-se com um problema de desempenho onde todos os *routers* iriam enviar os seus pacotes *Hello* para um meio partilhado o que resultaria numa inundação de pacotes *Hello*. Assim sendo, existe uma eleição de um *Domain Router (DR)* e um *Backup Domain Router* (BRD) que irão gerir a publicitação das rotas. Assim sendo o endereço 224.0.0.5 é usado para comunicar com todos os *routers* desse segmento de rede e o endereço *multicast* 224.0.0.6 é usado pelos *routers* que não são DR nem BDR para enviar os seus pacotes *Hello* aos DR. Se o pacote OSPF for encapsulado num quadro *Ethernet*, o endereço MAC de destino também será um endereço *multicast*: 01-00-5E-00-00-05 ou 01-00-5E-00-00-06.

2.11.2 Hello

Os pacotes *Hello* são utilizados para estabelecer e manter a adjacência com outros *routers* OSPF. Esta é uma forma de *keepalive* utilizado pelos *routers*, a fim de reconhecer a sua existência num segmento e, de modo a eleger um *router* designado (DR) em redes de multiacesso. O valor de *Hello interval* especifica o período de tempo, em segundos, entre os pacotes *Hello* que um *router* envia numa interface OSPF. O *Dead interval* especifica em segundos o tempo que um *router* espera até declarar um vizinho como inatingível. Isto acontece quando este não recebe pacotes *Hello* de um *router* vizinho.

Para que dois *routers* estabeleçam uma relação de vizinhança é necessário que os valores de *Hello interval* e *Dead interval* sejam iguais sob prejuízo de não constituírem uma relação de adjacência, o que resultaria na perda de conetividade de um determinado segmento de rede. Para definir estes temporizadores usam-se os comandos: *ip ospf Hello-interval* e *ip ospf Dead-interval*.

2.12 Bidirectional Forwarding Detection (BFD)

O *Open Shortest Path First* (OSPF) é um *interior gateway routing protocol* que fornece serviços de encaminhamento dentro de um domínio, o que não significa, necessariamente, estar restrito a um Autonomous System [17]. O OSPF pertence à categoria dos protocolos de encaminhamento do tipo *Link-State* [18], o que implica que cada *router* tenha conhecimento de toda a topologia de rede. Por razões de escalabilidade, o OSPF permite que os domínios de encaminhamento sejam divididos em áreas e, neste sentido, um *router* não precisa de

conhecer toda a topologia de rede de todas áreas, somente aquelas onde tenha uma interface.

Quando ocorre uma rápida convergência da rede em consequência de uma mudança na topologia, aquela torna-se num processo crítico para as infraestruturas de encaminhamento. Dado que o OSPF é um protocolo distribuído, este protocolo carece de sincronização em determinadas operações, nomeadamente na criação e processamento de pacotes *Hello* pelos *routers* participantes. Por isso torna-se absolutamente necessário garantir que os *routers* não falhem de forma consecutiva as sincronizações. Estas falhas poderão crescer de forma exponencial resultando num possível colapso dos *routers*. De modo a prevenir sobrecargas de CPU, os *routers* atuais já têm uma arquitetura distribuída com processadores dedicados à execução de protocolos de encaminhamento e ASIC (*Application-Specific Integrated Circuit*) para o encaminhamento de pacotes. Esta seção analisa de que forma estes tempos de deteção podem ser reduzidos e com uma consequente convergência de rede mais rápida recorrendo ao protocolo *Bidirectional Fowarding Detection* (BFD).

A deteção de perdas de conetividade entre dois dispositivos de rede é um requisito de vários protocolos de encaminhamento. Por vezes estes protocolos não têm um mecanismo nativo de deteção de falhas resultando numa deteção tardia. Por exemplo, no caso do OSPF, o mecanismo nativo, o protocolo *Hello*, não consegue detetar estas falhas na ordem dos milissegundos. Hei [19] propôs um método de deteção de falhas baseado na análise do alagamento de LSAs.

O *Bidirectional fowarding detection* (BFD) é um protocolo que deteta falhas em caminhos bidirecionais entre dois dispositivos de rede de forma potencialmente rápida [20], [21]. O BFD opera independentemente de outros protocolos e deteta falhas na execução do encaminhamento de pacotes, por exemplo, na movimentação de pacotes entre interfaces dos dispositivos de rede. A função de encaminhamento de pacotes é tipicamente feitas pelos processadores das ASICs libertando assim o processador do plano de controlo para ficar, dedicado aos protocolos de encaminhamento. O BFD foi projetado para ser implementado nos ASICS. A rápida deteção na falha do plano de dados pode ser associado ao mecanismo nativo dos protocolos de encaminhamento na deteção de falhas nos planos de dados/controlo. Por exemplo, um *router* OSPF pode iniciar uma sessão BFD com um *router* vizinho e fazer uso do pacote *Hello* para detetar a perda de conetividade para com o seu vizinho.

Uma sessão BFD entre dois *routers* pode operar em dois modos diferentes. No modo *asynchronous* dois *routers* vizinhos enviam pacotes de controlo BFD e será declarada uma falha quando um deles não receber esse pacote num período de tempo pré-determinado. No modo *demand* não existem trocas periódicas de mensagens entre *routers* numa sessão BFD. Ao invés, é trocada um pequena sequência de pacotes de controlo quando um *router* sente a necessidade de validar a conetividade. O BFD também suporta a função *echo* onde um *router*

envia um pacote a um outro *router* com o destino para si próprio. Estes pacotes retornarão ao *router* de origem após viajarem através de toda a tabela de encaminhamento do outro *router*. A função *echo* permite que apenas uma das entradas da tabela do outro *router* seja testada de modo a determinar falhas mais rapidamente.

O BFD permite que dois *routers* estabeleçam uma sessão BFD a fim de negociar os intervalos de tempo entre a sucessão de pacotes de controlo BFD. Poderão ser obtidos tempos de deteção na ordem dos 50 ms se os *routers* dessa sessão conseguirem trocar estes pacotes de controlo a um ritmo muito rápido. Os intervalos de tempo do envio dos pacotes de controlo podem ser ajustados dinamicamente. O protocolo BFD é perfeitamente ajustado para ser implementado numa ASIC pois numa sessão BFD é expetável que sejam trocados pacotes idênticos enquanto não forem detetadas falhas.

O BFD não foi usado na parte experimental por limitação do *Cisco Packet Tracer* que não o suporta.

2.13 Conclusão

O OSPF tem uma distância administrativa padrão de 110 e é denotado na tabela de encaminhamento com um código de fonte de rota de O. O OSPF está habilitado com o comando de configuração global *router ospf process-id*. O *process-id* é localmente significativo, o que significa que não tem que corresponder a outros *routers* OSPF para estabelecer adjacências com vizinhos.

O comando *network* utilizado com o OSPF tem a mesma função de quando utilizado como outros protocolos de encaminhamento IGP, mas com sintaxe ligeiramente diferente: *network network-address wildcard-mask area area-id*. O *wildcard-mask* é o inverso da máscara de sub-rede e o area-id deve ser definido como 0. O pacote *Hello* do OSPF é utilizado pelo OSPF para estabelecer adjacências de vizinho. Por omissão, os pacotes *Hello* de OSPF são enviados a cada 10 segundos em segmentos multiacesso e ponto-a-ponto e a cada 30 segundos em segmentos de rede ponto-a-multiponto (NBMA) (Frame Relay, ATM). O intervalo de *Dead* é o período de tempo que um *router* OSPF esperará antes de finalizar a adjacência com um vizinho. Por omissão, o intervalo de *Dead* é quatro vezes o intervalo de *Hello*. Para segmentos multiacesso e ponto-a-ponto, este período é de 40 segundos. Para redes NBMA, o intervalo de *Dead* é de 120 segundos. Para que os *routers* se tornem adjacentes, o intervalo de *Hello*, o intervalo de *Dead*, os tipos de rede e as máscaras de sub-rede devem corresponder.

A RFC 2328 não especifica quais valores devem ser utilizados para determinar o custo. O Cisco IOS utiliza as larguras de banda cumulativas das interfaces de saída do *router* para a rede de destino como o valor de custo.

As Redes multiacesso podem criar dois desafios para o OSPF relativos ao envio de LSAs, inclusive a criação de múltiplas adjacências - uma adjacência para cada par de *routers* e envio excessivo de LSAs (Anúncios *Link*-State). O OSPF elege um *Router* Designado (DR) para agir como ponto de coleta e distribuição para os LSAs enviados e recebidos na rede multiacesso. Um BDR (*Router* Designado de Backup) é eleito para assumir a função do DR no caso de o DR falhar. Todos os outros *routers* são conhecidos como DROthers. Todos os *routers* enviam os seus LSAs para o DR, que, por sua vez, envia o LSA para todos os outros *routers* na rede multiacesso.

O *router* com a ID de *router* mais elevada é o DR e o *router* com a segunda ID de *router* mais elevada é o BDR. Isto pode ser substituído pelo comando *ip ospf priority* naquela interface. Por omissão, o *ip ospf priority* é "1" em todas as interfaces multiacesso. Se um *router* for configurado com um novo valor de prioridade, o *router* com o valor de prioridade mais alto será o DR e o próximo mais alto será o BDR. Um valor de prioridade de “0” significa que o *router* não é qualificado para se tornar um DR ou BDR. Uma rota padrão é propagada em OSPF semelhante àquela de RIP. O comando do modo do encaminhamento OSPF *default-information originate* é utilizado para propagar uma rota padrão estática. O comando *show ip protocols* é utilizado para verificar informações de configuração OSPF importantes, inclusive a ID do processo OSPF, ID de *router* e as redes que o *router* anuncia.

OSPF é um dos protocolos mais amplamente implantados na Internet. Em vinte anos de sua existência, este protocolo provou ser notavelmente flexível ao atender às consecutivas mudanças das infraestruturas de encaminhamento. O projeto original do protocolo centrou-se na escalabilidade e robustez contra falhas. Estes objetivos foram atingidos, dividindo o domínio de encaminhamento em múltiplas áreas, limitando assim a sobrecarga de processamento do protocolo. Estas características permitiram a existência de grandes redes OSPF no mesmo *router* evitando assim colapsos no encaminhamento enquanto existem frequentes alterações de topologia. Os tempos de convergência na ordem dos 10 segundos eram aceitáveis mas a situação mudou com o aumento do uso comercial na Internet. Qualquer deterioração/paralisação do serviço que dura mais de alguns segundos já não pode ser tolerada. De fato, aplicações de tempo real requerem tempos de convergência abaixo do segundo. Apesar da capacidade de processamento dos *routers* dos dias de hoje serem bem superiores, a implementação de algoritmos “pesados” em grandes domínios de encaminhamento podem colocar em causa o bom funcionamento da rede. A adoção destes sensores tipo BFD tornam-se viáveis e necessários em pequenos domínios de rede. *Goyal, M* [22] apresenta uma completa análise no âmbito da melhoria da velocidade de convergência e escalabilidade em OSPF.

Capítulo 3

Redundância e Convergência do Protocolo OSPF Numa Rede Institucional

Introdução

Este capítulo tem como objetivos:

i) uma análise de comandos que visam verificar o estado de uma rede OSPF de modo a identificar e eliminar problemas de configuração.
ii) Uma análise da velocidade de convergência com larguras de banda diferentes.
iii) Testes e análises laboratoriais da velocidade de convergência de duas topologias de rede OSPF com a mudança dos parâmetros *Hello e Dead timers*.
iv) Análise de uma rede Institucional, da Universidade da Beira Interior, e proposta de uma topologia de rede OSPF

Este capítulo encontra-se organizado em três partes: na primeira parte serão enunciados alguns métodos de análise no despiste de problemas de encaminhamento de pacotes e examinada uma tabela de encaminhamento. Na segunda parte será conduzida uma série de testes laboratoriais e na terceira parte será construída uma proposta de uma configuração para uma rede institucional, a rede de todo o campus da Universidade da Beira Interior recorrendo à plataforma *Cisco Packet Tracer*.

3.1 Análise da Configuração OSPF

A figura 32 representa esquematicamente uma topologia de rede OSPF com três *routers* e três *switches*. O comando *show ip ospf neighbor* pode ser utilizado para verificar e identificar problemas de relações de vizinhos OSPF. Para cada vizinho, este comando exibe a saída de

comando mostrado na figura 33, referente à topologia de rede da figura 32. As configurações dos *routers* R1, R2 e R3 estão disponíveis no Anexo A.

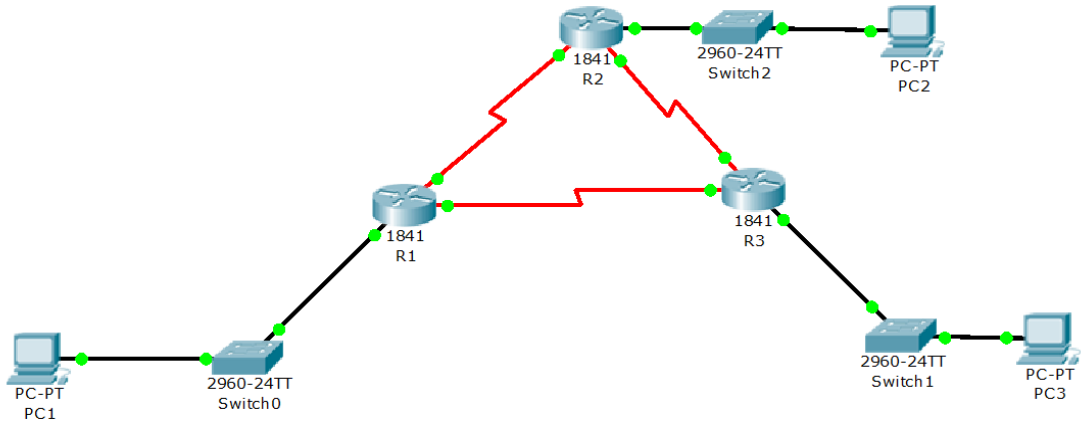

Figura 32 - Topologia de rede OSPF.

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
209.165.202.129   0   FULL/  -        00:00:33    172.16.7.1      Serial0/0/0
172.16.7.10       0   FULL/  -        00:00:34    172.16.7.10     Serial0/0/1

R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.7.9        0   FULL/  -        00:00:35    172.16.7.2      Serial0/0/0
172.16.7.10       0   FULL/  -        00:00:37    172.16.7.6      Serial0/0/1
R2#

R3#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.7.9        0   FULL/  -        00:00:36    172.16.7.9      Serial0/0/0
209.165.202.129   0   FULL/  -        00:00:36    172.16.7.5      Serial0/0/1
```

Figura 33 - Resultado do comando *show ip ospf neighbor* nos *routers* R1, R2 e R3.

Os campos obtidos pelo comando *show ip ospf neighbor* são: *Neighbor ID*, *Pri*, *Stare*, *Dead Time*, *Address* e *Interface*. Cada um destes campos indica:

- *Neighbor ID* - A ID do *router* vizinho.
- *Pri* - A prioridade OSPF da interface.
- *State* - O estado OSPF da interface. O estado FULL significa que o *router* e seu vizinho têm bancos de dados *Link-state* OSPF idênticos.

- *Dead Time* - A quantidade de tempo restante que o *router* esperará para receber um pacote *Hello* de OSPF do vizinho antes de declarar o vizinho inativo. Este valor é redefinido quando a interface recebe um pacote *Hello*.

- *Address* - O endereço IP da interface do vizinho ao qual este *router* está diretamente conectado.

- *Interface* - A interface na qual este *router* formou adjacência com o vizinho.

Ao identificar e solucionar problemas de redes OSPF, o comando do vizinho *show ip ospf* pode ser utilizado para verificar se um *router* formou uma adjacência com os seus *routers* vizinhos. Se a ID de *router* do *router* vizinho não for exibida, ou se não se não for mostrada como um estado de FULL, isto significa que os dois *routers* não formaram uma adjacência em OSPF. Se dois *routers* não estabelecerem adjacência, as informações *Link-state* não serão trocadas. As Bases de dados *Link-state* incompletas podem causar árvores SPF e tabelas de encaminhamento inexatas. As rotas para as redes de destino podem não existir ou podem não ser o melhor caminho. Em redes multiacesso Ethernet, dois *routers* adjacentes podem ter seus estados exibidos como 2WAY.

Dois *routers* podem não formar uma adjacência de OSPF se:

- As máscaras de sub-rede não corresponderem, fazendo os *routers* estarem em redes separadas.

- Os Temporizadores de *Hello* ou de *Dead* do OSPF não correspondem.

- Os tipos de rede OSPF não correspondem.

- Alguma das redes não foi declarada no comando *network*.

Outros comandos eficientes de identificação e solução de problemas OSPF incluem: *show ip protocols*, *show ip ospf* e *show ip ospf interface tal como ilustrado na figura 34*.

```
show ip protocols
show ip ospf
show ip ospf interface
```

Figura 34 - Comandos OSPF eficientes para a resolução de problemas de conetividade.

Conforme mostrado na figura 35, o comando *show ip protocols* é um modo rápido de verificar as informações vitais de configuração OSPF, inclusive a ID do processo OSPF, a ID do *router*, as redes que o *router* está anunciando, os vizinhos dos quais o *router* está recebendo atualizações e a distância administrativa padrão, que é 110 para OSPF.

```
R1#show ip protocols

Routing Protocol is "ospf 2"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.16.7.9
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.10.4.0 0.0.1.255 area 0
    172.16.7.0 0.0.0.3 area 0
    172.16.7.8 0.0.0.3 area 0
  Passive Interface(s):
    FastEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.7.9           110      00:24:12
    172.16.7.10          110      00:22:53
    209.165.202.129      110      00:22:53
  Distance: (default is 110)

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.16.7.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.10.4.0 0.0.1.255 area 0
    172.16.7.0 0.0.0.3 area 0
    172.16.7.8 0.0.0.3 area 0
  Passive Interface(s):
    FastEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.7.2           110      00:27:30
  Distance: (default is 110)
```

Figura 35 - Resultado do comando *show ip protocols* do *router* R1 da figura 32.

O comando *show ip ospf* também pode ser utilizado para examinar a ID do processo OSPF e a ID do *router*. Além disso, este comando exibe as informações de área do OSPF, os parâmetros relacionados com o algoritmo SPF, número de áreas a que o *router* pertence, número e tipos de LSA bem como a identificação e tipo de autenticação.

```
R1#show ip ospf
 Routing Process "ospf 2" with ID 172.16.7.9
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 1. Checksum Sum 0x00f418
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm executed 20 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x0140d4
        Number of opaque Link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0

 Routing Process "ospf 1" with ID 172.16.7.2
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0) (Inactive)
        Number of interfaces in this area is 0
        Area has no authentication
        SPF algorithm executed 1 times
        Area ranges are
        Number of LSA 1. Checksum Sum 0x00e0f6
        Number of opaque Link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Figura 36 - Resultado do comando *show ip ospf* do *router* R1 da figura 32.

A saída de comando inclui informações importantes do algoritmo SPF que incluem o atraso de programação SPF conforme ilustrado na figura 37:

```
SPF schedule delay 5 secs,
Hold time between two SPFs 10 secs,
Minimum LSA interval 5 secs.
Minimum LSA arrival 1 secs
```

Figura 37 - Extração de parte do resultado do comando *show ip ospf*:

schedule dealy, *hold time*, *LSA interval* e *LSA arrival*.

Sempre que um *router* recebe novas informações sobre a topologia (adição, exclusão ou modificação de um *Link*), o *router* deve executar novamente o algoritmo SPF, criar uma nova árvore SPF e atualizar a tabela de encaminhamento. O algoritmo SPF utiliza muito CPU e o tempo necessário para o cálculo depende do tamanho da área. O tamanho de uma área é medido pelo número de *routers* e pelo tamanho da base de dados *Link-state*.

```
R1#show ip ospf interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 172.16.7.2/30, Area 0
  Process ID 2, Router ID 172.16.7.9, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 209.165.202.129
  Suppress Hello for 0 neighbor(s)
```

Figura 38 - Resultado do comando *show ip ospf interface serial 0/0/0*.

Uma interface física que fica entre um estado *up* e um estado *down* é designada por *Link flapping* [23]. Um *Link flapping* pode fazer com que *routers* OSPF numa dada área executem

constantemente o algoritmo SPF, impedindo a convergência adequada. Para minimizar este problema, o *router* espera 5 segundos depois de receber um LSU antes de executar o algoritmo SPF. Isto é conhecido como atraso de programação SPF. Para impedir que um *router* execute constantemente o algoritmo SPF, há um tempo de espera (*Hold Time*) adicional de 10 segundos. O *router* espera 10 segundos depois de executar o algoritmo SPF antes de executar novamente o algoritmo.

O modo mais rápido de verificar os intervalos de *Hello* e de *Dead* é utilizar o *comando show ip ospf interface*. Conforme mostrado na figura 38, adicionar o tipo, módulo, slot e porta da interface ao comando exibe uma saída de comando para essa interface específica. Estes intervalos são incluídos nos pacotes *Hello* de OSPF enviados entre os vizinhos. O OSPF pode ter intervalos de *Hello* e de *Dead* diferentes em várias interfaces, mas para que os *routers* OSPF se tornem vizinhos, os seus intervalos de *Hello* e de *Dead* devem ser idênticos. Por exemplo, na figura 38, o *router* R1 está utilizando um intervalo de *Hello* de 10 segundos e um intervalo de *Dead* de 40 segundos na interface Serial 0/0/0. O *router* R2 também tem de utilizar os mesmos intervalos na sua interface Serial 0/0/0, caso contrário os dois *routers* não formarão uma adjacência.

3.2 Tabela de encaminhamento

Um administrador de rede precisa de conhecer profundamente as caraterísticas de uma tabela de encaminhamento de modo a identificar e solucionar problemas de rede. Entender a estrutura e o processo de procura da tabela de encaminhamento é fundamental para o diagnóstico de qualquer problema da tabela de encaminhamento, independentemente do nível de familiaridade com um protocolo de encaminhamento específico.

O modo mais rápido para verificar a convergência do OSPF consiste em observar a tabela de encaminhamento para cada *router* da topologia. O comando *show ip route* pode ser utilizado para verificar se o OSPF está a receber rotas via OSPF. O "O" no começo de cada rota indica que a origem da rota é o OSPF e "C" indique que são redes diretamente ligadas.

A tabela de encaminhamento IP é estruturada de uma maneira *classful*, o que significa que utiliza, por omissão, endereços *classful* para organizar as entradas de rota. A origem de uma entrada de rota pode ser uma rede diretamente conectada, uma rota estática ou uma rota reconhecida dinamicamente a partir de um protocolo de encaminhamento.

Existem rotas de nível 1 e nível 2. Uma rota de nível 1 pode ser uma rota definitiva ou uma rota primária. Uma rota definitiva de nível 1 é uma rota com uma máscara de sub-rede igual a ou menor que a máscara *classful* padrão da rede; e um endereço do próximo salto ou uma interface de saída. Por exemplo, uma rota reconhecida por RIP com o endereço de rede de 192.168.1.0 e uma máscara de rede /24 é uma rota definitiva de nível 1. Estas rotas são exibidas na tabela de encaminhamento como uma única entrada de rota tal como mostrado na figura 39.

```
R 192.168.1.0/24 [120/1] via 172.16.2.2, 00:00:25, Serial0/0/0
```

Figura 39 - Exemplo de uma rota RIP definitiva de nível 1.

Outro tipo de rota de nível 1 é uma rota primária. Uma rota primária de nível 1 é criada automaticamente quando uma rota de sub-rede é adicionada à tabela de encaminhamento. A rota de sub-rede é conhecida como uma rota secundária de nível 2. A rota primária é um cabeçalho para rotas secundárias de nível 2. Na figura 40 podemos observar um exemplo de uma rota primária de nível 1 e uma rota secundária de nível 2:

```
172.16.0.0/24 is subnetted, 1 subnets
R 172.16.1.0 [120/1] via 172.16.2.1, 00:00:07, Serial0/0/0
```

Figura 40 – Exemplo de uma rota primária de nível 1.

A máscara de sub-rede das rotas secundárias é exibida na rota primária a menos que o VLSM seja utilizado. Com o VLSM, a rota primária exibe a máscara *classful* e a máscara de sub-rede é incluída com as entradas de rota VLSM individuais.

Quando um pacote é recebido pelo *router*, este procura a correspondência mais longa com uma das rotas na tabela de encaminhamento. A correspondência mais longa é a rota com o número maior de bits à esquerda (bits de rede) que correspondem entre o endereço IP de destino do pacote e o endereço de rede da rota na tabela de encaminhamento. A máscara de sub-rede associada ao endereço de rede na tabela de encaminhamento define o número

mínimo de bits que devem corresponder para que a rota seja considerada uma correspondência.

Antes de examinar qualquer rota secundária de nível 2 (sub-redes) para verificar se há uma correspondência, deve haver primeiro uma correspondência com a rota primária de nível 1. A máscara *classful* da rota primária determina quantos bits devem corresponder à rota primária. Se houver uma correspondência com a rota primária, as rotas secundárias serão examinadas para verificar se há uma correspondência.

O que acontece quando há uma correspondência com a rota primária, mas não há com nenhuma das rotas secundárias: se o *router* estiver a utilizar um comportamento de encaminhamento *classful*, nenhuma outra rota será procurada e o pacote será descartado. O comportamento do encaminhamento *classful* pode ser implementado através do comando *no ip classless*.

Se houver uma correspondência com uma rota primária, mas não houver com nenhuma das rotas secundárias, o processo da tabela de encaminhamento continuará procurando outras rotas na tabela de encaminhamento, inclusive uma rota padrão, caso exista uma.

As rotas para as redes são adicionadas à tabela de encaminhamento a partir de diversas fontes, incluindo redes diretamente conectadas, rotas estáticas, protocolos de encaminhamento *classful* e protocolos de encaminhamento *classless*. O processo de procura, comportamento de encaminhamento *classful* ou *classless*, são independentes da origem da rota. Uma tabela de encaminhamento pode ter rotas reconhecidas de um protocolo de encaminhamento *classful*, como por exemplo RIPv1, mas deve utilizar o comportamento de encaminhamento *classless*, *no ip classless*, para o processo de procura.

3.3 Redundância e Convergência na Rede da UBI

Numa fase inicial esta proposta de configuração será replicada na plataforma Cisco Packet Tracer a topologia da rede da Universidade da Beira Interior com o total de sete *routers*.

3.3.1 Topologia de rede existente

Por motivos de simplicidade no desenho da topologia e dado que estamos perante *routers* com ligações ponto-a-ponto, são desprezados os *switches* de nível 2. Foi feito um levantamento em relação aos organizadores de fibras nos diferentes bastidores e registados os troços em fibra existentes e que se encontram livres.

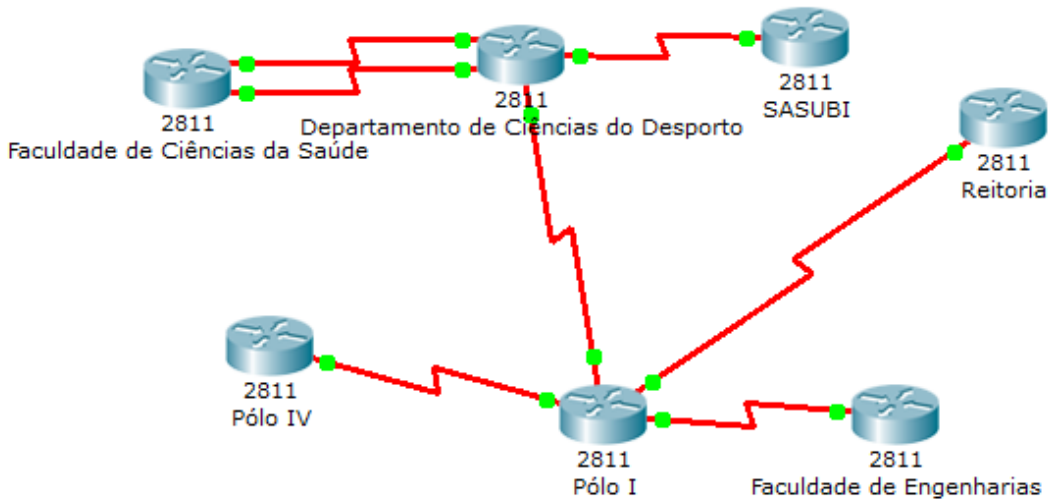

Figura 41 - Topologia de rede existente na UBI

Na figura 41 é de fácil observação que, tirando os *Links* sem fios entre a Faculdade de Ciências da Saúde e a Departamento de Ciências do Desporto, não existem mais ligações redundantes.

3.3.2 Camada Física da Rede

Após a verificação da existência de troços em fibra por usar é proposto um novo mapa topológico, representada na figura 42, onde são adicionados novas ligações físicas entre os *routers* da instituição. A direção principal no tocante ao número de ligações a usar seria o

mais próximo de uma *mesh*, onde o limite imposto seria o número de portas livres nos organizadores de fibra e portas dos ativos de redes.

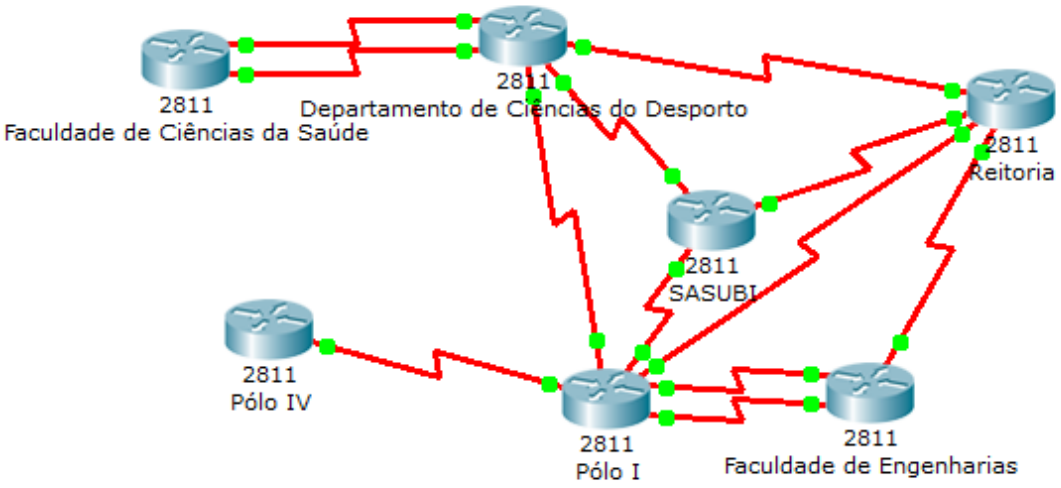

Figura 42 – Nova proposta para a topologia de rede da UBI

3.3.3 Configurações OSPF

O *router* localizado na Faculdade de Ciências da Saúde ficará numa área distinta visto que se encontra ligada via *wireless* o que previne o alagamento de *Link State Advertises* para resto da rede por cabo, podendo provocar excesso de mudanças de topologia. O balanceamento de carga entre o Departamento das Ciências do Desporto e a Faculdade de Ciências da Saúde não é possível pois estamos perante duas ligações sem fios de diferentes larguras de banda. Fica a ligação *laser* a 1Gbps com um custo inferior à ligação via *WiMax* a 100 Mbps de modo a que o protocolo dê preferência à interface onde está ligado o *laser*. Os *routers* do Departamento das Ciências do Desporto e do Polo I ficaram como *Area Border Routers* sendo que o do Polo I irá fornecer conetividade à internet. A duas ligações entre o *router* do Polo I e o da Faculdade de Engenharias ficaram ambas ativas a fazer balanceamento de carga entre as duas ligações aumentando assim a largura de banda disponível para este Pólo. O balanceamento será alcançado mediante a atribuição de um custo idêntico a todas as interfaces envolvidas em ambos os *routers*. Dado o tamanho da rede os restantes *routers* (excluindo o *router* da Faculdade de Ciências da Saúde) ficaram todos na mesma área.

Será propagada uma rota estática padrão para toda a área com destino no próximo salto que, neste caso, é uma interface IP da Fundação para a Computação Científica Nacional. As portas que não participam no domínio OSPF são configuradas como passivas a fim de prevenir o envio de tabelas de encaminhamento para destinos não fidedignos. A troca de LSAs entre routers da mesma área requer uma autenticação via *message digest* (MD-5) de modo a prevenir o envenenamento das base de dados de *Link States* e consequente disrupção de rede. Os intervalos de *Hello* e *Dead* serão reduzidos para valores mais baixos a fim de proporcionar tempos de convergência mais rápidos. A possibilidade de uma zona OSPF colapsar devido ao excesso de mudanças de topologias já constitui um grande problema nos dias de hoje dado que os novos *routers* têm ASICs para o encaminhamento de pacotes e um processador dedicado ao plano de controlo e aos algoritmos de encaminhamento.

3.4 Testes de Velocidade de Convergência

Nesta seção são feitos testes laboratoriais em ambiente controlado na plataforma Cisco Packet Tracer. Foram configuradas três topologias de rede em OSPF (Cenário I, II e III) onde serão provocadas várias disrupções de rede entre os *routers* R1 e R2. Durantes os testes serão registados os tempos de convergência da rede e, posteriormente, uma análise dos dados.

3.4.1 Cenário I

O cenário I envolve três routers ligados entre si em modo ponto-a-ponto. Foram atribuídos IPs às interfaces físicas e ligados os cabos como mostra a figura 43. Foi usado OSPF como protocolo de encaminhamento e configurada uma interface de loopback no router R1 com um IP para fins de testes de conetividade. Este tipo de interface tem a particularidade de nunca mudar o seu estado para *down* independentemente das disrupções ou mudanças de topologia rede. A disrupção de rede envolve o remoção da ligação entre os *routers* 1 e 2 forçando novos cálculos SFP para cada um dos routers para construir uma base de dados consistente com os restantes routers. O tempo desde o início da disrupção de rede até à convergência da rede são recolhidos através do modo de simulação que a plataforma disponibiliza. A cada pilha de 10 testes os parâmetros Dead-interval e Hello-interval foram alterados como reflete a tabela 5. Todas as combinações possíveis foram testadas para intervalos de *Dead* [1 a 13] segundos e intervalos de Hello [1 a 14] segundos.

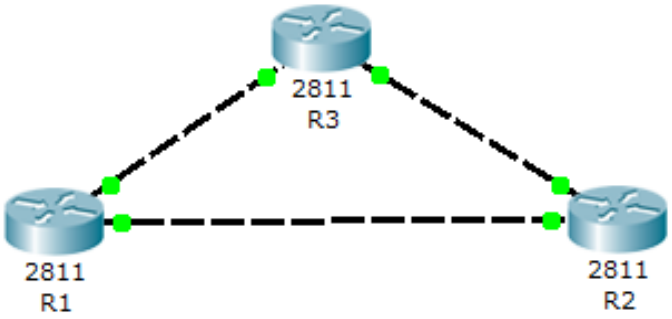

Figura 43 - Topologia de rede OSPF para teses laboratoriais (Cenário I).

A cada pilha de 10 testes os parâmetros Dead-interval e Hello-interval foram alterados como reflete a tabela 5. Todas as combinações possíveis foram testadas para intervalos de *Dead* [1 a 13] segundos e intervalos de Hello [1 a 14] segundos. Por n.c. entende-se: não convergiu.
A tabela 5 contém os resultados obtidos dos testes e a sua representação gráfica está ilustrada na figura 45.

Tabela 5 - Resultados laboratoriais para o Cenário I

		Tempos de Convergência (s) Cenário I												
		Dead Timers (s)												
		1	2	3	4	5	6	7	8	9	10	11	12	13
Hello Timers (s)	1	n.c.	5.11	5.13	5.24	5.10	5.01	5.11	5.12	5.10	5.21	5.37	5.18	5.21
	2	n.c.	n.c.	6.34	6.45	6.54	6.37	6.57	6.65	6.67	6.78	6.54	6.43	6.55
	3	n.c.	n.c.	n.c.	7.53	7.52	7.78	7.76	7.87	8.84	7.36	8.65	7.37	7.94
	4	n.c.	n.c.	n.c.	n.c.	8.65	9.71	8.67	9.13	9.47	8.41	9.34	8.64	9.01
	5	n.c.	n.c.	n.c.	n.c.	n.c.	10.12	10.35	10.64	10.35	10.31	10.75	10.37	10.59
	6	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	11.87	11.84	11.65	12.08	11.56	11.76	11.42
	7	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	12.78	12.91	13.06	13.13	12.16	13.63
	8	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	14.34	13.75	14.25	13.58	13.97
	8	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	15.57	15.38	15.17	15.85
	10	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	15.15	14.67	15.74
	11	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	15.68	16.01
	12	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	16.12
	13	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.
	14	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.

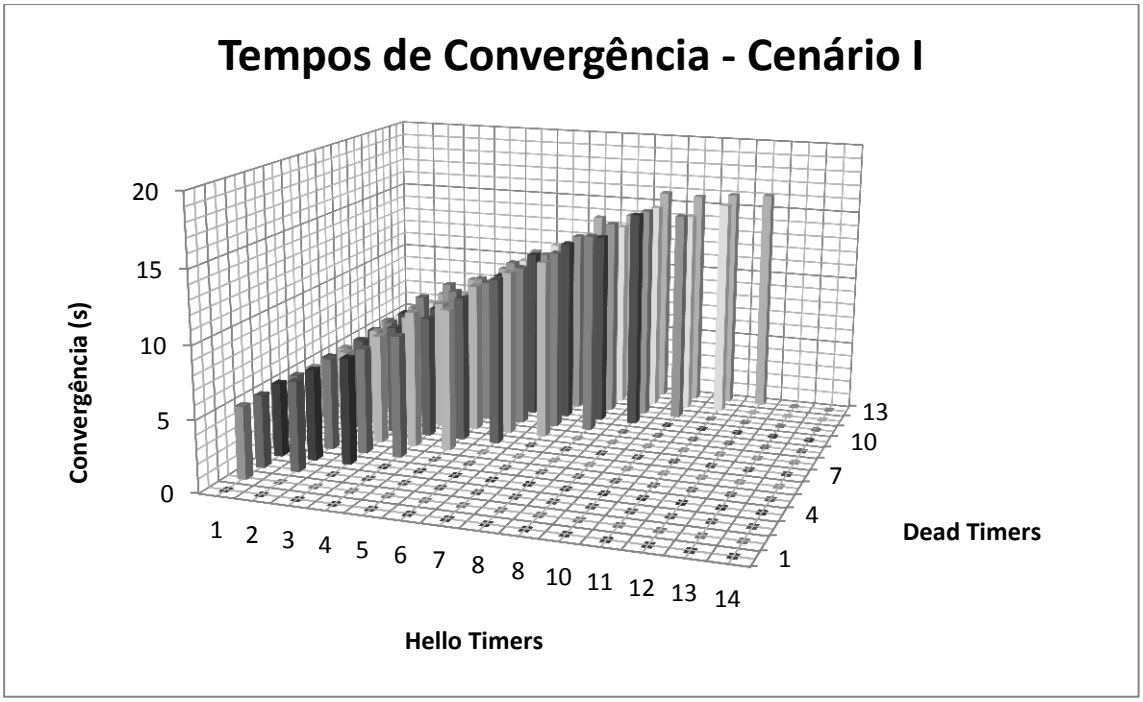

Figura 44 - Gráfico dos resultados obtidos para o Cenário I.

3.4.2 Cenário II

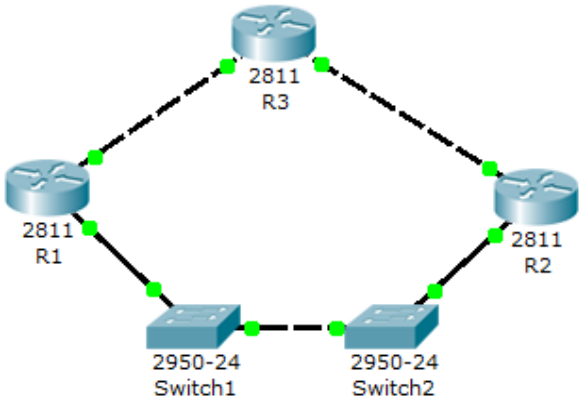

Figura 45 - Topologia de rede OSPF para teses laboratoriais (Cenário II)

O cenário II envolve três routers ligados entre si em modo ponto-a-ponto sendo que a ligação entre R1 e R2 envolve 2 switches. Foram atribuídos IPs às interfaces físicas e ligados os cabos como mostra a figura 45. Os switches estão em modo transparente e foi configurado o *spanning-tree portfast* para prevenir o envenenamento das estatísticas. As configurações dos

Routers são idênticas às do Cenário I. A cada pilha de 10 testes os parâmetros Dead-interval e Hello-interval foram alterados como reflete a tabela 6. Todas as combinações possíveis foram testadas para intervalos de *DEAD* [1 a 13] segundos e intervalos de Hello [1 a 14] segundos e resgistadas na tabela 6 e em forma de gráfico na figura 46. A disrupção de rede é feita na ligação entre o *switch* 1 e *switch* 2. Por n.c. entende-se: não convergiu.

Tabela 6 - Resultados laboratoriais para o Cenário II

		Tempos de Convergência (s) Cenário II												
		Dead Timers (s)												
		1	2	3	4	5	6	7	8	9	10	11	12	13
Hello Timers (s)	1	n.c.	7.65	8.86	9.46	10.0	11.64	12.21	13.67	14.89	16.01	16.79	18.10	19.54
	2	n.c.	n.c.	8.90	9.54	11.45	13.34	13.45	14.45	15.65	17.56	17.97	19.54	20.71
	3	n.c.	n.c.	n.c.	11.56	13.46	14.24	15.11	15.84	16.65	18.35	19.35	20.54	21.16
	4	n.c.	n.c.	n.c.	n.c.	14.62	15.73	16.73	17.12	17.84	17.92	19.23	21.48	22.83
	5	n.c.	n.c.	n.c.	n.c.	n.c.	16.32	14.47	18.20	19.31	20.12	17.34	21.44	20.45
	6	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	13.21	19.31	20.41	18.30	20.54	21.58	22.52
	7	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	18.34	19.56	20.27	20.45	22.12	22.46
	8	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	17.37	18.39	19.94	19.33	19.86
	8	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	20.35	18.45	24.32	23.57
	10	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	17.34	23.45	22.56
	11	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	24.45	29.34
	12	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	30.99
	13	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.
	14	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.

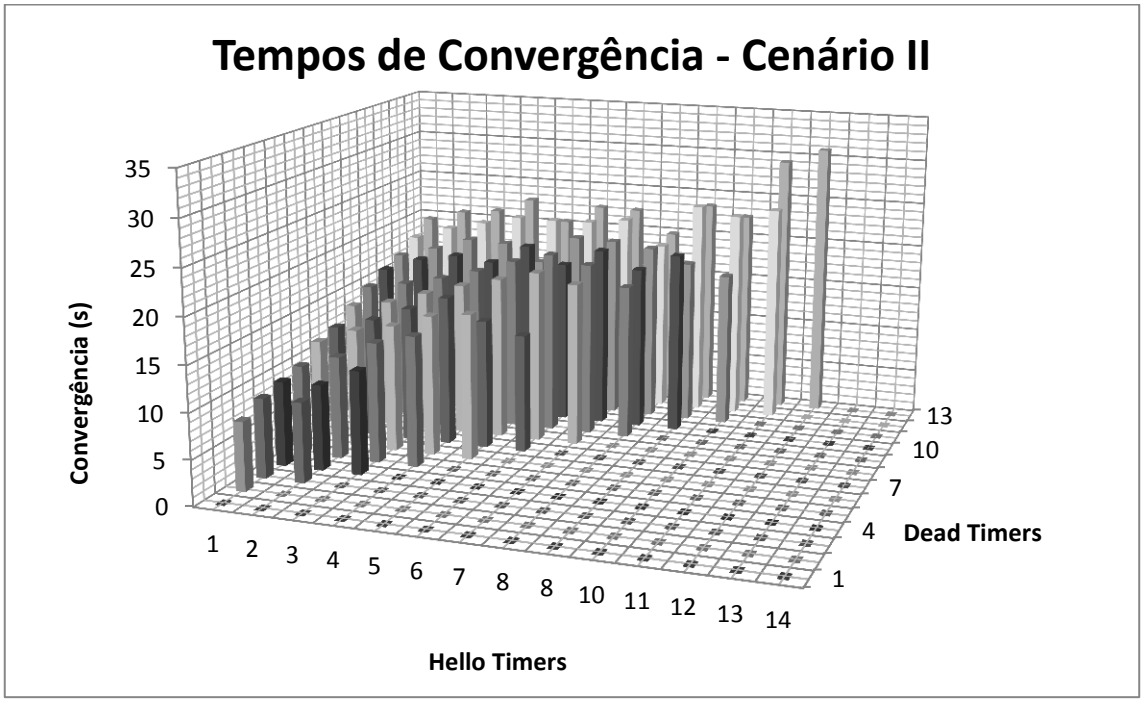

Figura 46 - Gráfico dos resultados obtidos para o Cenário II.

3.4.3 Cenário III

Na pilha de testes realizados foram usados 3 routers Cisco com ligações a 100 mbps e 1gbps. Procedeu-se à configuração dos *routers* numa área de OSPF com ligações entre eles. Procedeu-se ao corte de um cabo e observaram-se os tempos de convergência, nomeadamente o tempo decorrido entre o corte do cabo até ao final da convergência. Os parâmetros em análise são os seguintes:

- *minLSinterval* com um valor por omissão de 5 segundos que limita o número de LSA enviados. Só será enviado um novo LSA se minLSinterval já tiver sido atingido.
- *minLSarrival* com um valor por omissão de 1 segundo que limita o número de novos LSA recebidos.
- *RxmtInterval* com um valor por omissão de 5 segundos que define o tempo até que um *router* possa retransmitir um novo LSA após não ter recebido um *acknowledge* do LSA enviado anteriormente.

Para velocidades de transmissão de 100mbps e 1Gbps não foram notadas diferenças nos tempos de convergência pois o *tamanho* de um LSA é residual. Um elevado valor no parâmetro *minLSInterval* limita a geração de LSA o que resulta num fator estabilizador na convergência de grandes redes ou em situações de *Link-flap*. No entanto, foi notada uma significante melhoria nos tempos de convergência com o parâmetro *minLSInterval* a 1 segundo.

Várias contribuições foram feitas no domínio da velocidade de convergência em redes de domínio OSPF. Katz [24] sugere que LSAs importantes (LSA que descreve uma falha) podem ser alagados sem a aplicação de *minLSArrival*, *minLSInterval* ou *LSA pacing delays*. Choudhury et al [25] sugerem que um *router* deve ajustar, de forma dinâmica, os parâmetros *RxmtInterval* e *pacing delays* para um *router* vizinho baseado na sua perceção se o seu vizinho está congestionado ou não. Outras abordagens sobre este tema podem ser consultadas em M. Goyal et al. [26]. *Rastogi, et al*, [27] analisa o paradigma da agregação de rotas em domínios de OSPF em prol de uma base de dados *Link-state* mais leve mas em detrimento da perda de informação como consequência da agregação na escolha da melhor rota.

3.5 Conclusão

Conforme descrito neste capítulo, existem inúmeras ferramentas de diagnóstico que nos ajudam a identificar problemas de rede no domínio do protocolo OSPF. A complexidade de configurar uma rede OSPF é inversamente proporcional à dificuldade em resolver problemas de conetividade. Estes protocolos dinâmicos que, ao invés do encaminhamento estático, toma decisões sozinho baseado nas configurações existentes. Um protocolo de encaminhamento dinâmico requer um sistema de monitorização de redes bem configurado e que registe todas as mudanças da topologia da rede. Se houver uma mudança de topologia porque uma porta avariou, o algoritmo OSPF irá usar um caminho alternativo. No entanto, o administrador de redes precisa de ser notificado, por exemplo, via SNMP para que essa porta seja substituída sob prejuízo de um dia a rede ficar sem ligações redundantes (por estarem avariadas/inoperacionais) perdendo assim a última ligação disponível.

Dos testes realizados no cenário I verificou-se que os temos de convergência mínimos foram obtidos quando os parâmetros Hello e Dead eram 1 e 2 segundos respetivamente. À medida que os valores de *dead* e *hello* foram crescendo os tempos da velocidade de convergência também aumentaram numa proporção aproximada de 1 para 1, isto é, hello mais dead é aproximadamente igual ao tempo da velocidade de convergência.

No que respeita aos testes realizados no cenário II os tempos de convergência foram mais altos para idênticos valores de *hello* e *dead*. Neste caso é notório que o algoritmo OSPF demorou mais tempo a detetar a falha de conetividade motivado pelo fato de nenhuma das interfaces físicas dos *routers* ter ficado operacionalmente em baixo. Em ambos os cenários I e II a rede não convergiu com valores de *Hello* maiores ou iguais aos de *Dead*, este resultado verificou-se porque os routers davam os destinos aprendidos como expirados antes de receberem os pacotes *hello* dos *routers* vizinhos.

Em termos da velocidade convergência de uma rede OSPF (Cenário III), para larguras de banda de 100mbps e 1Gbps, não foram notadas diferenças nos tempos de convergência pois o *tamanho* de um LSA é residual. Um elevado valor no parâmetro minLSInterval limita a geração de LSA o que resulta num fator estabilizador na convergência de grandes redes ou em situações de *link-flap*. No entanto foi notada uma significante melhoria nos tempos de convergência com o parâmetro *minLSInterval* a 1 segundo.

Capítulo 4

Conclusão e Trabalho Futuro

Este capítulo apresenta as principais conclusões que resultaram do trabalho de investigação descrito nesta dissertação. No final são apresentados alguns tópicos de pesquisa relacionados com o trabalho desenvolvido e deixados como sugestão para trabalho futuro.

4.1 Conclusão

A necessidade de convergência rápida e escalabilidade em protocolos de encaminhamento do tipo *Link-state* continuam a desafiar a comunidade de investigação dado que os domínios de encaminhamento crescem em tamanho e em complexidade. Nesta dissertação foi feito um estudo aprofundado sobre o OSPF onde se verificou que os tempos de *Hello* e *Dead* são os principais atores no processo de convergência de um domínio de encaminhamento. O fato de OSPF não interpretar mais do que LSU a cada 5 segundos e não usar o algoritmo SPF mais que uma vez a cada 10 segundos impede que uma rede colapse se existirem sucessivas mudanças de topologia. Por outro lado estas proteções acabam por afetar os tempos de convergência. O protocolo BFD iria cooperar com o protocolo OSPF na determinação de falhas contornando assim os tempos OSPF. No entanto, este protocolo ficaria sediado nas placas ASIC dado que na maior parte do tempo seriam gerados pacotes de controlo idênticos até que uma falha fosse detetada. No tocante ao projeto de rede para a Universidade da Beira Interior foi implementado o protocolo OSPF com autenticação e prevenção de *routers* estranhos à instituição participem no domínio OSPF ou sequer que recebam pacotes *Hello*. Foram usadas infraestruturas físicas existentes que ainda não se encontram ativas de modo a melhorar a redundância da rede.

4.2 Trabalho Futuro

Dada a cumplicidade entre o tamanho dos domínios de encaminhamento e os tempos de convergência que, ao crescerem em tamanho, resultam num aumento exponencial dos tempos de convergência resultando na majoração do tamanho destes domínios. Uma potencial direção para trabalho futuro seria investigar a alocação, de forma dinâmica, os domínios de encaminhamento.

Referências

[1] Moy, J., "OSPF version 2," Internet Engineering Task Force, Request For Comments (Standards Track) RFC 2328 [1], April 1998.

[2] Coltun, R.; Ferguson, D,; Moy, J.; Lindem, A., "OSPF for IPv6," Internet Engineering Task Force, Request For Comments (Standards Track) RFC 5340, July 2008.

[3] Moy, J., "OSPF Specification," Internet Engineering Task Force, Request For Comments (Proposed Standard) RFC 1131, October 1989.

[4] Moy, J., "OSPF Version 2," Internet Engineering Task Force, Request For Comments (Draft Standard) RFC 1247, July 1991.

[5] Coltun, R.; Ferguson, D.; Moy, J., "OSPF for IPv6", Internet Engineering Task Force, Request For Comments (Proposed Standard) RFC 2740, December 1999.

[6] Bellur, B.; Ogier, R., "A reliable, efficient topology broadcast protocol for dynamic networks," in Proc. IEEE INFOCOM, 1999, pp. 178–186.

[7] Venkatesh, S., "Smart adjacency establishment in OSPF routing protocol," Master's thesis, University of Wisconsin - Milwaukee, 2006.

[8] Cisco Networking Academy, (2009, April, 21). Routing Protocols and Concepts (11.0.1) [Online]. Available at: http://www.cisco.com/web/learning/netacad/index.html

[9] Cisco, 2012. *Cisco Packet Tracer*. [Online] Available at: http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html

[10] Chia-Tai, Tsai; Rong-Hong, Jan; Chien, Chen; Chia-Yuan, Huang, "Implementation of Highly Available OSPF Router on ATCA," 13th Pacific Rim International Symposium on Dependable Computing, PRDC 2007.

[11] Hedrick, C., "Routing Information Protocol," Internet Engineering Task Force, Request For Comments RFC 2328 [1], June 1988.

[12] Hawkinson J.; Bates, T., "Guidelines for creation, selection and registration of an autonomous system (AS)," Internet Engineering Task Force, Request For Comments (Best Current Practice) RFC 1930, March 1996.

[13] Cisco Systems, (2005, August, 10). OSPF Design Guide (Apendix A) [Online]. Available: http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094e9e.shtml

[14] Cisco Networking Academy, (2009, April, 21). Routing Protocols and Concepts [Online]. Available: http://www.cisco.com/web/learning/netacad/index.html

[15] Arias, E., (2012, February, 24). Brief Explanation of OSPF LSA Types and Special Area Types [Online]. Available: https://learningnetwork.cisco.com/docs/DOC-13814

[16] Cisco Systems, (2005, August, 10). OSPF Design Guide (Link State Advertisements) [Online]. Available: http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094e9e.shtml

[17] Cisco Networking Academy, (2009, April, 21). Routing Protocols and Concepts [Online]. Available: http://www.cisco.com/web/learning/netacad/index.html

[18] Doyle, J., (2007, December). Reducing *Link* failure detection time with BFD [Online]. http://www.networkworld.com/community/node/23380.

[19] Hei, Y.; Ogishi, T.; Ano, S.; Hasegawa, T., "OSPF Failure Identification based on LSA Flooding Analysis", 10th IFIP/IEEE International Symposium on., Integrated Network Management, IM '07.

[20] Doyle, J., "Reducing *Link* failure detection time with BFD," Network World, December 2007, http://www.networkworld.com/community/node/23380.

[21] Katz, D.; Ward, D., "Bidirectional forwarding detection (BFD)," Internet Engineering Task Force, Request For Comments (Standards Track) RFC 5880, June 2010.

[22] Goyal, M.; Soperi, M.; Baccelli, E.; Choudhury, G.; Shaikh, A.; Hosseini, H.; Trivedi, K., "Improving Convergence Speed and Scalability in OSPF: A Survey", Communications Surveys & Tutorials, IEEE.

[23] "Information About Ports," Chapter 6, page 6-12 http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_1_4/troubleshooting/configuration/guide/n1000v_trouble_7port.pdf

[24] D. Katz, "Why are we scared of SPF? IGP scaling and stability," October 2002

[25] G. Choudhury, "Prioritized treatment of specific OSPF version 2 packets and congestion avoidance," Internet Engineering Task Force, Request For Comments (Best Current Practice) RFC 4222, October 2005.

[26] Goyal, M.; Soperi, M.; Baccelli, E.; Choudhury, G.; Shaikh, A.; Hosseini, H.; Trivedi, K., "Improving Convergence Speed and Scalability in OSPF: A Survey", IEEE Communications Surveys & Tutorials, Vol. 14, nº. 2, pág. 443-463, Second Quarter 2012.

[27] Rastogi, R.; Breitbart, Y.; Garofalakis, M.; Kumar, A., "Optimal configuration of OSPF aggregates", INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, vol. 2, no., ppág. 874-882 vol.2, 2002.

Anexo A

Configurações dos *routers* da figura 31.

R1#show running-config

Building configuration...

Current configuration : 1005 bytes

!

version 12.3

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname R1

!

no ip domain-lookup

!

spanning-tree mode pvst

!

interface FastEthernet0/0

 ip address 10.10.4.1 255.255.254.0

```
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 172.16.7.2 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 ip address 172.16.7.9 255.255.255.252
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 2
 log-adjacency-changes
 passive-interface FastEthernet0/0
 network 10.10.4.0 0.0.1.255 area 0
```

```
 network 172.16.7.0 0.0.0.3 area 0
 network 172.16.7.8 0.0.0.3 area 0
!
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/0
 network 10.10.4.0 0.0.1.255 area 0
 network 172.16.7.0 0.0.0.3 area 0
 network 172.16.7.8 0.0.0.3 area 0
!
ip classless
!
line con 0
line vty 0 4
 login
!
end


R2#show running-config
Building configuration...


Current configuration : 1023 bytes
!
version 12.3
```

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R2
!
no ip domain-lookup
!
spanning-tree mode pvst
!
interface Loopback1
 ip address 209.165.202.129 255.255.255.252
!
interface FastEthernet0/0
 ip address 10.10.0.1 255.255.252.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
```

```
interface Serial0/0/0
 ip address 172.16.7.1 255.255.255.252
!
interface Serial0/0/1
 ip address 172.16.7.5 255.255.255.252
 clock rate 64000
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/0
 passive-interface Loopback1
 network 172.16.7.0 0.0.0.3 area 0
 network 172.16.7.4 0.0.0.3 area 0
 network 10.10.0.0 0.0.7.255 area 0
 network 10.10.0.0 0.0.3.255 area 0
 default-information originate
!
ip classless
ip route 0.0.0.0 0.0.0.0 Loopback1
!
```

```
line con 0
line vty 0 4
 login
!
End
R3#show running-config
Building configuration...


Current configuration : 806 bytes
!
version 12.3
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R3
!
spanning-tree mode pvst
!
interface FastEthernet0/0
 ip address 10.10.6.1 255.255.254.0
 duplex auto
 speed auto
!
```

```
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 172.16.7.10 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 ip address 172.16.7.6 255.255.255.252
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/0
 network 172.16.7.4 0.0.0.3 area 0
 network 172.16.7.8 0.0.0.3 area 0
 network 10.10.6.0 0.0.1.255 area 0
!
```

ip *classless*

!

line con 0

line vty 0 4

login

!

end

Anexo B

Neste anexo encontra-se uma proposta de configuração para a rede da Universidade da Beira Interior. É apresentada a configuração do *router* do Polo I por ser o centro da estrela e as configurações dos restantes routers são tudo idênticas a este excetuando o endereçamento IP e, consequentemente, os *advertises*.

```
PoloI#show running-config
Building configuration...

Current configuration : 2262 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname PoloI
!
!
!
!
!
!
!
aaa new-model
!
!
!
!
!
!
!
!
!
!
!
!
!
ip ssh authentication-retries 2
```

```
ip ssh time-out 60
ip domain-name poloI.ubi.pt
!
!
spanning-tree mode pvst
!
!
!
!
interface Loopback1
 ip address 10.0.0.25 255.255.255.252
 ip ospf message-digest-key 10 md5 OMG
 ip ospf hello-interval 1
 ip ospf dead-interval 2
!
interface Loopback2
 ip address 10.0.0.29 255.255.255.252
 ip ospf message-digest-key 10 md5 OMG
 ip ospf hello-interval 1
 ip ospf dead-interval 2
!
interface Loopback3
 ip address 10.0.0.33 255.255.255.252
 ip ospf message-digest-key 10 md5 OMG
 ip ospf hello-interval 1
 ip ospf dead-interval 2
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
```

```
 ip address 10.0.0.1 255.255.255.252
 ip ospf message-digest-key 10 md5 OMG
 ip ospf hello-interval 1
 ip ospf dead-interval 2
!
interface Serial0/0/1
 ip address 10.0.0.5 255.255.255.252
 ip ospf message-digest-key 10 md5 OMG
 ip ospf hello-interval 1
 ip ospf dead-interval 2
 clock rate 2000000
!
interface Serial0/1/0
 ip address 10.0.0.9 255.255.255.252
 ip ospf message-digest-key 10 md5 OMG
 ip ospf hello-interval 1
 ip ospf dead-interval 2
 clock rate 2000000
!
interface Serial0/1/1
 ip address 10.0.0.13 255.255.255.252
 ip ospf message-digest-key 10 md5 OMG
 ip ospf hello-interval 1
 ip ospf dead-interval 2
 clock rate 2000000
!
interface Serial0/2/0
 no ip address
 clock rate 2000000
!
interface Serial0/2/1
 no ip address
 clock rate 2000000
!
interface Serial0/3/0
 ip address 10.0.0.17 255.255.255.252
 ip ospf message-digest-key 10 md5 OMG
 ip ospf hello-interval 1
 ip ospf dead-interval 2
!
```

```
interface Serial0/3/1
 ip address 10.0.0.21 255.255.255.252
 ip ospf message-digest-key 10 md5 OMG
 ip ospf hello-interval 1
 ip ospf dead-interval 2
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 area 0 authentication message-digest
 network 10.0.0.0 0.0.0.15 area 0
!
ip classless
!
!
!
!
!
!
!
line con 0
line vty 0 4
 transport input ssh
!
!
!
end
```