Universidade de Aveiro
2013

Departamento de Eletrónica,
Telecomunicações e Informática

José Pedro Costa Gonçalves

Estratégias de implementação de redes empresariais

Universidade de Aveiro
2013

Departamento de Eletrónica,
Telecomunicações e Informática

José Pedro Costa Gonçalves

Estratégias de implementação de redes empresariais

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Eletrónica e Telecomunicações, realizada sob a orientação científica do Professor Doutor Paulo Salvador, professor auxiliar do Departamento de Eletrónica, telecomunicações e Informática da Universidade de Aveiro, e do Professor Doutor António Nogueira, professor auxiliar, do Departamento de Eletrónica, telecomunicações e Informática da Universidade de Aveiro.

O júri

Presidente	Prof. Dr. Aníbal Manuel de Oliveira Duarte Professor catedrático da Universidade de Aveiro
Vogal	Prof. Dr. Rui Jorge Morais Tomaz Valadas Professor catedrático da Universidade Técnica de Lisboa
Vogal	Prof. Dr. Paulo Jorge Salvador Serra Ferreira Professor auxiliar da Universidade de Aveiro

Palavras-chave Arquitetura; Rede; Empresa; Switch; VLAN; Redundância; Resiliência; Encaminhamento

Resumo

Este trabalho pretende criar um manual que estabeleça os princípios básicos a adotar na conceção de desenhos de redes empresariais, sobretudo no que se refere ao balanceamento da sua disponibilidade, segurança e flexibilidade, tendo em atenção os requisitos próprios de cada empresa. Com esse intuito, serão apresentadas estratégias e procedimentos para a implementação de redes multicamada. As estratégias definidas pretendem atingir os seguintes objetivos: a implementação de grupos lógicos dentro da rede, o encaminhamento entre os mesmos e a garantia de alta disponibilidade e redundância da rede. Esta dissertação desenvolve-se em vários momentos, sendo de sublinhar: a apresentação dos conceitos indispensáveis à compreensão da temática; a análise de topologias, com recurso a um software de simulação de redes, a fim de exemplificar a configuração dos vários modelos que podem ser usados na conceção da rede empresarial; a análise de cada um dos cenários estudados.

Keywords Architecture; Network; Enterprise; Switch; VLAN; Redundancy; Resilience; Routing; Switching

Abstract The goal of this work is to create a manual, establishing the basic principles to adopt in the conception of enterprise network designs, mainly through the balancing of its availability, security and flexibility; taking into consideration the requirements of each company. For that purpose, strategies and procedures for implementation of multilayer networks will be presented. The defined strategies, aim to achieve the following purposes: implementing logical groups within the network, the forwarding between them and ensuring high availability and network redundancy. This essay develops at several moments in which we can highlight: introduction of necessary concepts for the comprehension of the subject¸ simulation of topologies, using a software network simulator, in order to illustrate the configuration of the various models that can be applied in the design of the enterprise network; the analysis of each studied scenarios.

Conteúdo

Conteúdo 11

Lista de Figuras 13

Lista de Tabelas 15

Lista de acrónimos 16

1. Introdução 17

1.1 Enquadramento e Objetivos 17

1.2 Estrutura da dissertação 19

2. Arquitetura de redes Empresariais 21

2.1 Conceitos básicos 21

2.2 Princípios e estrutura de uma arquitetura de rede 25

2.2.1 Camada de Acesso 27

2.2.2 Camada de distribuição 28

2.2.3 Camada de núcleo 29

2.2.4 Alta disponibilidade e redundância 29

2.2.5 Desenho da ligação acesso-distribuição 31

2.2.6 Daisy chain 33

3. Rede Ethernet 35

3.1 Conceito de VLAN 35

3.2.1 VLAN Local 36

3.2.2 VLAN End-To-End 37

3.2.3 Procedimentos para a configuração de VLANs 39

3.3 Trunking 40

3.4 STP (Spaning Tree Protocol) 43
4. Routing IP 47
4.1 Protocolos (RIP, IS-IS, EIGRP, OSPF) 47
4.1.1 RIP (Routing Information Protocol) 48
4.1.2 EIGRP (Enhanced Interior Gateway Routing Protocol) 49
4.1.3 OSPF (Open Shortest Path First) 50
4.1.4 IS-IS (Intermediate System-Intermediate System) 52
4.2 Metodologias de implementação com OSPF 53
4.2.1 V2 e v3 53
4.2.2 Áreas 53
4.2.3 Rotas por omissão 55
4.2.4 Interfaces passivos 56
4.2.5 Caminhos múltiplos 56
4.2.6 Redistribuição de rotas 57
5. Cenários de implementação 59
5.1 Estratégias de implementação 59
5.1.1 Cenário 1 62
5.1.2 Cenário 2 64
5.1.3 Cenário 3 66
5.1.4 Cenário 4: Redundância 70
5.1.5 Cenário 5: Utilização de subdomínios de encaminhamento 72
5.1.6 Cenário 6: Introdução de um bloco de acesso à Internet 72
5.2 Configuração dos elementos de rede 73
5.2.1 Cenário 1 73
5.2.2 Cenário 2 78
5.2.3 Cenário 3 79
5.2.4 Cenário 4: Redundância 84
5.2.5 Cenário 5: Utilização de subdomínios de encaminhamento 91
5.2.6 Cenário 6: Introdução de um bloco de acesso à Internet 94
6. Conclusões 95
Referências 99
Bibliografia 101

Lista de Figuras

Figura 2.1: Switch layer 2 23
Figura 2.2: Switch layer 3 23
Figura 2.3: Router 23
Figura 2.4: Modelo hierárquico 26
Figura 2.5: Desenho de camada 2 sem loop 31
Figura 2.6: Desenho de camada 2 com loop 32
Figura 2.7: Desenho de camada 3 33
Figura 3.1: VLAN Local 36
Figura 3.2: VLAN End-to-end 37
Figura 3.3: Pacote marcado com 802.1Q 41
Figura 5.1: Topologia de rede 60
Figura 5.2: Topologia de rede cenário 1 62
Figura 5.3: Topologia de rede cenário 2 65
Figura 5.4: Topologia de rede cenário 3 66
Figura 5.5: VLAN de interligação 68
Figura 5.6: Ligação multicamada 69
Figura 5.7: Pacote ICMP 69
Figura 5.8: Switches de distribuição com ligação única ao núcleo 70
Figura 5.9: Switches de distribuição com ligação dupla ao núcleo 70
Figura 5.10: Topologia com redundância 71
Figura 5.11: Cenário 4 com zona de acesso à internet 73
Figura 5.12: Mac-address-table de SW2 78
Figura 5.13: LANs de ligação 80
Figura 5.14: Tabela de encaminhamento de SW1 do cenário 3 sem VLAN End-to-end 81

Figura 5.15: Tabela de encaminhamento de SW1 do cenário 3 84
Figura 5.16: Tabela de encaminhamento de SW2 do cenário 3 84
Figura 5.17: Tabela de encaminhamento de SW3 do cenário 3 84
Figura 5.18: Cenário 3 com redundância 85
Figura 5.19: VLANs de interligação do cenário 3 com redundância 86
Figura 5.20: Tabela de encaminhamento de SW1 do cenário 3 com redundância 90
Figura 5.21: Tabela de encaminhamento de SW2 do cenário 3 com redundância 90
Figura 5.22: Tabela de encaminhamento de SW3 do cenário 3 com redundância 91
Figura 5.23: Tabela de encaminhamento de SW1 com áreas OSPF 93
Figura 5.24: Tabela de encaminhamento de SW2 com áreas OSPF 93
Figura 5.25: Tabela de encaminhamento de SW3 com áreas OSPF 93
Figura 5.26: Rota por omissão na tabela de encaminhamento de SW1 94

Lista de Tabelas

Tabela 2.1: Camadas do modelo OSI 22
Tabela 2.2: Tabela de endereços MAC 24
Tabela3.1: Modos de configuração DTP 42

Lista de acrónimos

ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
DTP	Dynamic Trunking Protocol
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
IA	Inter Area
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocol
IS-IS	Intermediate System - Intermediate System
ISL	Inter-Switch Link
ISP	Internet Service Provider
LAN	Local Area Network
LSA	Link State Advertisement
LSDB	Link State Data Base
MAC	Media Access Control
MAN	Metropolitan Area Network
MTU	Maximum Transmission Unit
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
QoS	Quality of Service
RIP	Routing Information Protocol
SA	Sistema Autónomo
SPF	Shortest Path First
STP	Spanning Tree Protocol
VLAN	Virtual Local Area Network
WAN	Wide Area Network

1. Introdução

1.1 Enquadramento e Objetivos

Uma rede de computadores é um conjunto de módulos processadores interligados por um sistema de comunicações, capazes de compartilhar informações e recursos, ou seja, um ou mais computadores e outros dispositivos, ligados em rede, com o objetivo de compartilhar recursos físicos e lógicos. Redes de computadores são o núcleo da comunicação moderna.

Uma característica fundamental numa rede empresarial é a sua fiabilidade, isto é, a continuidade do seu funcionamento, em qualquer circunstância, salvaguardando atividades que não podem ser interrompidas e prevenindo grandes prejuízos.

Outra característica do uso de redes numa organização moderna é a partilha de informação, evitando dados duplicados ou desatualizados.

Estas características e o necessário aumento dos níveis de competitividade e produtividade das empresas, com o passar do tempo, trouxeram a necessidade de melhorar a sua organização, no que respeita às telecomunicações.

A conceção de arquiteturas de rede, práticas, eficientes e capazes de salvaguardar sempre a relação preço – desempenho, tornou-se assim um desiderato fundamental no mundo empresarial. Para acompanhar esta mudança de atitude das empresas, as redes de telecomunicações empresariais têm evoluído, de simples meios de interligação de dispositivos, com apenas uma camada protocolar, para uma interligação mais avançada de equipamentos com funcionalidades multicamada.

Não admira, por isso, que as empresas tenham sentido a necessidade de redesenhar as suas infraestruturas de rede, de modo a poderem suportar serviços num

enquadramento local, relativo a uma zona da rede, ou num enquadramento abrangente, que englobe toda a rede. E tendam a abandonar modelos de rede fixos, preferindo modelos de rede desenhados de modo a permitir mais flexibilidade, resiliência e redundância.

Elaborar o desenho de uma rede empresarial não é diferente de projetar qualquer outro tipo de sistema. Para isso, é importante a existência de um manual que inclua os princípios básicos que permitam conceber uma rede balanceada em termos de disponibilidade, segurança, flexibilidade e gestão, tendo em atenção os requisitos específicos do negócio.

Esta dissertação vai ocupar-se de:

I) Apresentação dos conceitos relativos aos princípios de arquitetura, planeamento e implementação de redes empresariais.

II) Definição de estratégias necessárias para:
    1) Implementação de grupos lógicos dentro da rede.
    2) Encaminhamento entre eles.
    3) Garantir alta disponibilidade e redundância da rede.
    4) Preparar a infraestrutura para o suporte de serviços avançados.

III) Análise de várias topologias de rede, com vários grupos lógicos de dispositivos de saída, locais e abrangentes, utilizando um *software* apropriado.

IV) Avaliação da análise realizada em III).

1.2 Estrutura da dissertação

Esta dissertação está estruturada em 6 capítulos.

No primeiro capítulo, é feita uma introdução ao tema proposto e são indicados os objetivos pretendidos na execução deste trabalho.

No segundo capítulo, é feita a apresentação dos conceitos básicos associados à arquitetura de uma rede empresarial. Entre eles incluem-se: os elementos de rede utilizados na sua implementação; a definição do modelo hierárquico e as suas várias camadas.

O terceiro capítulo é dedicado ao estudo da segmentação de rede, ao nível da camada 2. Aqui serão discutidas as noções relacionadas com: VLANs (*Virtual Local Area Network*) e os seus dois modelos; os tipos de ligação entre elementos de rede e o protocolo responsável pelo encaminhamento de pacotes.

No quarto capítulo, são apresentados modos de encaminhamento IP de camada 3. Nesta fase, serão introduzidos vários protocolos responsáveis pelo encaminhamento de pacotes entre elementos de rede – RIP (*Routing Information Protocol*)[7], OSPF (*Open Shortest Path First*)[8], EIGRP (*Enhanced Interior Gateway Routing Protocol*)[10] e IS-IS (*Intermediate System – Intermediate System*)[9] –, sendo dada especial atenção ao protocolo OSPF, uma vez que, neste trabalho, é o que vai ser utilizado na configuração dos dispositivos de rede.

No quinto capítulo, serão analisados vários cenários de implementação de redes empresariais, utilizando os diferentes conceitos explorados ao longo do trabalho. Este capítulo desenvolve-se em duas fases: na primeira, apresentam-se os vários tipos de desenhos de rede; na segunda, demonstram-se os modos de configuração dos elementos de rede de cada topologia.

Por fim, o sexto capítulo é dedicado a apresentar as conclusões a que chegamos.

2. Arquitetura de redes Empresariais

2.1 Conceitos básicos

O termo rede é, geralmente, usado para identificar um conjunto de elementos do mesmo tipo ligados entre si. No entanto, o conceito de rede informática refere-se a um grupo de computadores ou periféricos conectados uns aos outros, com o objetivo de trocar informação entre si, partilhar recursos, garantir a comunicação entre pessoas e processos, e ainda, partilhar informação funcional entre todos os elementos de rede.

Atualmente, existem três tipos de rede: LAN (*Local Area Network*), MAN (*Metropolitan Area Network*) e WAN (*Wide Area Network*).

LAN é uma rede de caráter local, com uma área geográfica reduzida, interligando um não muito elevado número de dispositivos. Tipicamente de domínio privado.

MAN é a rede que abrange uma área maior que uma LAN mas menor que uma WAN. Normalmente é constituída pela interligação de várias LANs.

WAN é uma rede que se distingue pela dispersão por uma grande área geográfica, pelo seu porte e pela estrutura das telecomunicações. É normalmente de caráter público e gerida por um operador de telecomunicações.

Uma rede empresarial pode ter diferentes capacidades que dependem dos requisitos, características e necessidades da empresa. Normalmente, o desenho de uma rede depende dos seguintes critérios:

- Tipo de atividade.
- Segurança necessária.

- Dimensão da empresa.
- Volume de tráfego.
- Orçamento disponível.
- Necessidades dos seus utilizadores.

Na base da ligação de todos os dispositivos de qualquer rede encontra-se o modelo OSI (*Open Systems Interconnection*) que compreende sete camadas, a saber: *physical, data link, network, transport, session, presentation, application*. O quadro que segue evidencia o número, o nome e a função que cumpre cada uma dessas camadas.

Camadas		Função
Número	Nome	
7	Application	Aplicação/Serviço
6	Presentation	Definição, manipulação da informação
5	Session	Estabelecimento e manutenção de sessões
4	Transport	Comunicação extremo a extremo
3	Network	Endereçamento e encaminhamento
2	Data Link	Partilha do meio
1	Physical	Transmissão de sinais

Tabela 2.1: Camadas do modelo OSI

Neste modelo é particularmente importante compreender a função desempenhada pelas camadas 2 (partilha do meio) e 3 (endereçamento e encaminhamento de pacotes).

A camada 2 é conhecida como a camada de ligação de dados. Aqui os pacotes são codificados e descodificados em bits. Ela é responsável pela transmissão e receção de pacotes, assim como pelo controlo do seu fluxo. Cada placa de rede possui um endereço físico - MAC (*Media Access Control*) - que é utilizado no encaminhamento de pacotes, ao nível da camada 2. Esta camada pode, também, detetar e corrigir erros que ocorram na camada anterior, a camada 1 ou camada física.

A camada 3 cumpre várias funções: endereçamento e encaminhamento de pacotes, para a transmissão de dados entre dois dispositivos, criando caminhos lógicos, conhecidos como circuitos virtuais; no caso do encaminhamento de pacotes entre dois nós, sobretudo com vários intermediários, é responsável, também, pelo controlo de congestionamento das ligações, gestão de falhas e sequenciamento de pacotes.

Numa rede é possível encontrar, entre outros, três tipos de elementos: *switches layer 2*, *switches layer* 3 e *routers*. As figuras seguintes ilustram os símbolos que representam cada desses dispositivos.

Figura 2.1:
Switch layer 2

Figura 2.2:
Switch layer 3

Figura 2.3:
Router

Os *switches*, também conhecidos por *Switches layer 2,* trabalham na camada 2 do modelo OSI e utilizam endereços MAC. É um dispositivo que tem como função reencaminhar pacotes entre os vários nós da rede e é do tipo *store and forward*. A cada porta deste elemento de rede corresponde um domínio de colisão diferente,

impossibilitando assim a colisão de pacotes de segmentos diferentes. A possibilidade de segmentação de rede, é criada interligando a cada porta um grupo lógico de rede, para evitar que os pacotes cheguem a destinos não desejados. Cada placa ou adaptador de rede tem um endereço MAC associado (endereço com 48 bits em notação hexadecimal). Um *switch* possui uma tabela de encaminhamento de camada 2 e regista nessa tabela a porta em que recebeu uma trama e o seu endereço MAC. Para reencaminhar uma trama, procura na tabela o endereço MAC do destino para identificar através de que porta a deve enviar. No caso de o endereço destino da trama não existir na tabela de encaminhamento do *switch*, este envia-a para todas as portas, exceto para a porta de que recebeu a trama. A Tabela 2.2 exemplifica uma tabela de endereços MAC de um *switch*.

MAC ADRESS	PORT
11:11:11:11:11:11	1
22:22:22:22:22:22	2
33:33:33:33:33:33	3

Tabela 2.2: Tabela de endereços MAC

Um *router* é um dispositivo que trabalha ao nível da camada 3 do modelo OSI e utiliza endereços IP. É responsável pelo encaminhamento de pacotes entre redes de computadores. Está normalmente ligado a várias redes diferentes (interfaces diferentes ligados a redes diferentes, com endereços IP distintos), e quando um pacote chega a uma das suas interfaces, lê a informação relativa ao endereço destino e consulta a sua tabela de encaminhamento, de forma a enviar o pacote para o seu destino eficazmente.

Um *switch layer* 3 funciona ao nível de uma das camadas anteriores e utiliza endereços MAC ou endereços IP, para proceder ao encaminhamento de pacotes. Este dispositivo acumula funcionalidades mistas de *router* e *switch*. A grande diferença entre

um *switch layer* 3 e um router, é o facto de o primeiro fazer a comutação de pacotes baseada em hardware e o router usar um microprocessador para tomar decisões de encaminhamento de pacotes. Por vezes, é possível substituir um *router* por um *switch layer 3,* em vários pontos da rede, já que este é capaz de operar tráfego de rede, com alto desempenho, e proporcionar benefícios na relação custo - eficiência para a rede.

2.2 Princípios e estrutura de uma arquitetura de rede

Hoje, em geral, considera-se que uma rede apresenta um bom desempenho se cumpre três objetivos principais: modularidade, resiliência e flexibilidade.

Uma rede diz-se modular quando permite o seu crescimento e alteração consoante os requisitos da empresa. Uma rede modular permite o seu fácil reescalonamento, acrescentando ou retirando módulos, em vez do seu redesenho integral.

A definição de resiliência remete-nos para a capacidade de superar e recuperar de erros ou adversidades. Uma rede incapaz de recuperar de uma falha, de qualquer natureza e, ainda que por pouco tempo, não é resiliente e pode induzir custos muito elevados no funcionamento de uma empresa. Eis por que, hoje, se pede que uma rede seja operacional a 100%, ou perto disso, justamente para minimizar os custos associados a baixa resiliência. Em geral, a dificuldade que se coloca às empresas e aos engenheiros de rede é encontrar a melhor relação entre o orçamento disponível e o risco aceitável.

Se uma rede é capaz de acompanhar o crescimento da empresa e a evolução do negócio, ela diz-se flexível. É fácil de compreender que mudanças estruturais ao nível da empresa não devem ter repercussões ao nível do desempenho da rede. E, ainda que haja mudanças que impliquem alterações na rede, elas devem ser resolvidas de forma simples e rápida. As pequenas empresas usam redes desenhadas com recurso a um *switch layer 2* e um *router on a stick*. Este tipo de configuração permite assegurar velocidade e

facilidade de implementação. Mas tem desvantagens ao nível do escalonamento, da segurança, flexibilidade, resiliência e disponibilidade.

Com o aparecimento de *switches* de layer 3 foi possível desenhar redes com arquitetura simplificada e com velocidades semelhantes a redes de camada 2. As redes que recorrem a *switches layer 3* comportam várias camadas de funcionamento. Cada camada assegura o cumprimento de uma determinada função, ao mesmo tempo que facilita a sua implementação, garante a flexibilidade de rede e simplifica a resolução de problemas. Este tipo de arquitetura denomina-se arquitetura hierárquica. A figura 2.4 representa o modelo hierárquico que se divide em 3 camadas: a de acesso, a de distribuição e o núcleo.

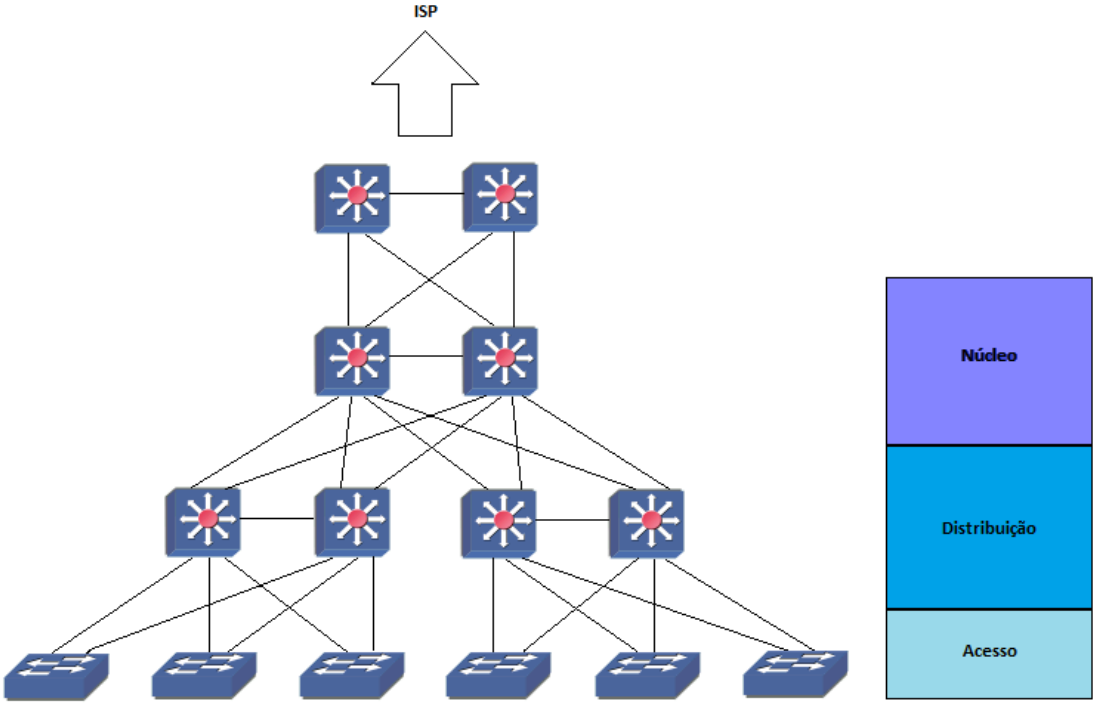

Figura 2.4: Modelo hierárquico

A camada de acesso é responsável pelo acesso à rede e, normalmente, é composta por *switches layer 2* que fornecem conectividade a computadores, telefones, servidores e a pontos de acesso *wireless*; inclui características de controlo de acesso, filtros, gestão e segurança. A camada de distribuição agrega dispositivos de rede, usa

switches layer 2 ou *layer 3*, para segmentar grupos de trabalho e isolar problemas na rede; funciona como serviço e controlo entre a camada de acesso e o núcleo; implementa políticas de teste de qualidade de serviço. O núcleo é desenhado para transporte a alta velocidade; é a camada crítica para a conectividade e tem de fornecer alta disponibilidade e capacidade de adaptação rápida a alterações; deve providenciar escalabilidade e rápida convergência. O modelo hierárquico é vantajoso em relação a modelos não hierárquicos por [6]:

- Permitir modularidade.
- Ser de fácil compreensão.
- Aumentar a flexibilidade da rede.
- Facilitar a expansão e a escalabilidade da rede.
- Tornar previsível o funcionamento da rede.
- Simplificar a resolução de problemas.

2.2.1 Camada de Acesso

O desenho da camada de acesso deve ser concebido de modo a garantir:

1) Alta disponibilidade da rede.

Isto só se consegue assegurando uma dupla redundância: no *default gateway*, procedendo de modo que cada *switch* da camada de acesso seja ligado a mais do que um *switch* da camada de distribuição; no fornecimento de energia para cada *switch*, assegurando que cada um deles tenha uma fonte de energia alternativa.

2) Convergência perfeita.

A camada de acesso deve fornecer convergência perfeita de voz, de redes de dados e de *roaming wireless* LAN.

3) Autorização de acesso.

Esta camada deve ser responsável também pela autorização do acesso à rede, providenciando ferramentas como IEE 802.1X, *port secutity*, DHCP (*Dynamic Host Configuration Protocol*) *snooping* e *dynamic* ARP (*Address Resolution Protocol*) *inspection*.

4) Qualidade de serviço.

A qualidade de serviço depende da capacidade de priorizar o tráfego de rede considerado crítico, usando classificação de tráfego e filas de espera o mais perto possível da entrada de rede.

5) Eficiência e largura de banda.

O desenho de rede tem de suportar gestão de eficiência e largura de banda para IP (*Internet Protocol*) *multicast*, no caso em que se utilize, por exemplo, IGMP (*Internet Group Management Protocol*) *snooping*.

6) Conexão adequada.

É nesta zona, que se define a que grupo lógico de rede cada dispositivo de acesso tem de se conectar.

2.2.2 Camada de distribuição

A camada de distribuição combina comutação de pacotes multicamada, para segmentar grupos de trabalho e isolar problemas de rede, prevenindo o impacto destes na camada do núcleo. Liga serviços de rede para a camada de acesso, equilibra carga de tráfego e implementa QoS (*Quality of Service*), segurança, assim como políticas de encaminhamento de pacotes. Normalmente, é também usada para terminar o acesso a grupos lógicos de rede de camada 2, dos *switches* da camada anterior. Com o objetivo de melhorar performance de encaminhamento, sumariza as rotas da camada de acesso.

.

2.2.3 Camada de núcleo

Esta camada é a espinha dorsal da conectividade da rede, sendo o ponto de agregação das outras camadas. Tem como obrigação garantir condições para alta disponibilidade, escalabilidade e rápida convergência da rede. Assim, o núcleo deve:

- Ser facilmente escalável.
- Ser composto por um ambiente de alta velocidade.
- Ter capacidade para se adaptar facilmente a alterações e redundância.
- Fornecer caminhos alternativos e balancear a carga de tráfego na rede.
- Evitar manipulação de pacotes, de forma a não atrasar o seu encaminhamento e não diminuir a velocidade do tráfego nesta camada.

Nem todas as redes necessitam desta camada. As pequenas redes podem acumular as funções de distribuição e núcleo na camada de distribuição.

2.2.4 Alta disponibilidade e redundância

O conceito de alta disponibilidade refere a capacidade de uma rede se manter operacional a todo o tempo ou perto disso. Uma rede altamente disponível tem como objetivo prevenir a existência de tempos de inatividade da rede, ou pelo menos minimizar o seu tempo de downtime.

Os fatores necessários a ter em conta para a obtenção de um desenho de rede com alta disponibilidade são:

- Redundância.
- Resiliência.
- Tecnologia.
- Pessoas qualificadas.
- Ferramentas.

A redundância e a tecnologia são componentes fáceis de alcançar, uma vez que podem ser comprados e implementados. Mas, para isso, é fundamental a presença de pessoas qualificadas, responsáveis pela sua implementação e manutenção. São necessárias também ferramentas para a gestão e documentação correta da rede.

O conceito de redundância descreve a capacidade da rede de proporcionar meios alternativos que assegurem o acesso constante a todos os caminhos da rede. Para obter um desenho de rede com redundância é necessário implementar elementos de rede alternativos e ligações alternativas, o que pressupõe duplicação de custos. Por isso, a construção de uma rede requer uma avaliação prévia da relação custo-benefício associada à sua implementação e manutenção, tendo em conta o seu custo de *downtime*. A chave é encontrar o equilíbrio entre a construção de uma rede com demasiada redundância, muito complexa, cara de construir e de manter e outra, mais barata, mais simples, com redundância limitada e comprometendo a alta disponibilidade.

A escolha de caminhos numa rede com redundância pode ser feita ao nível da camada 2 ou da camada 3, consoante estamos na presença de *switches layer 2* ou *layer 3*, respetivamente. Ao nível da camada 2, o STP (*Spanning Tree Protocol*)[11] é o protocolo responsável pela escolha das rotas a seguir, e pela convergência de rede em caso de falha numa das ligações. Enquanto que o protocolo de encaminhamento IP, ocupar-se-á da realização da mesma função, ao nível da camada 3.

Uma rede diz-se resiliente quando é capaz de recuperar de possíveis falhas nos caminhos de rede, identificando-as e de ultrapassando-as escolhendo novas rotas.

O que fica dito deixa claro que o desenho de uma rede altamente disponível exige que assegure tanto resiliência como redundância, quer dizer: por um lado, que todos os segmentos sejam capazes de recuperar, o mais rápido possível, quando ocorrem falhas na topologia; por outro, deve oferecer sempre, pelo menos, um caminho para cada ponto de acesso, servidores e ISP (*Internet Service Provider*).

2.2.5 Desenho da ligação acesso-distribuição

Existem três tipos de configurações possíveis para o bloco constituído pela zona de acesso e distribuição, dependendo do tipo de *switch* que é utilizado em cada zona: desenho de camada 2 sem *loop*, desenho de camada 2 com *loop*, desenho de encaminhamento de camada 3.

O desenho de camada 2 sem *loop* obedece aos seguintes requisitos:

- As ligações entre a camada de acesso e distribuição são configuradas de forma a transportar tráfego de segmentos de rede diferentes.
- As ligações entre *switches* de distribuição são configuradas como encaminhamento de camada 3.
- O STP não se envolve em matéria de convergência de rede, em caso de falha, e em balanceamento do tráfego.

A figura 2.5 ilustra um desenho de camada 2 sem *loop*.

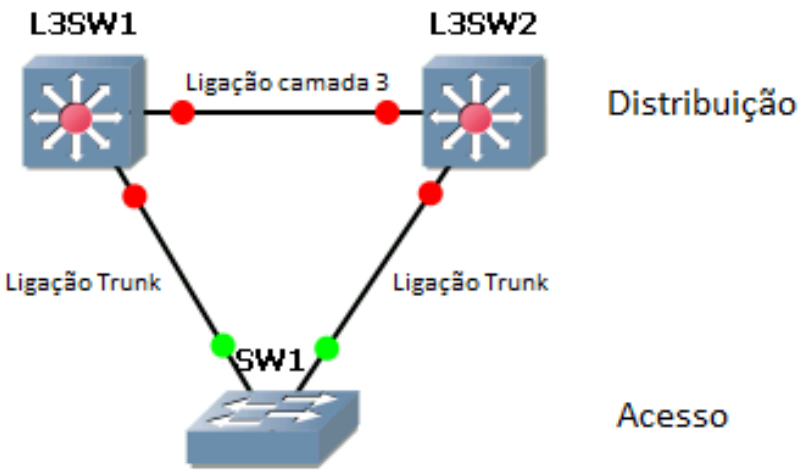

Figura 2.5: Desenho de camada 2 sem loop

O desenho de camada 2 com *loop* apresenta as seguintes características:

- As ligações, entre os *switches* da camada de acesso e da camada de distribuição e entre os *switches* da camada de distribuição, são configuradas como camada 2, com permissão para tráfego de diferentes segmentos de rede.
- Entre os *switches* das camada de acesso e de distribuição pode ocorrer um *loop* de camada 2, o qual pode ser eliminado através do STP.
- Apresenta desvantagens: em caso de falha numa das ligações, tem dependência do STP para a convergência de rede, em caso de falha; limitado balanceamento de carga na rede.

A figura 2.6 ilustra um desenho de camada 2 com *loop*.

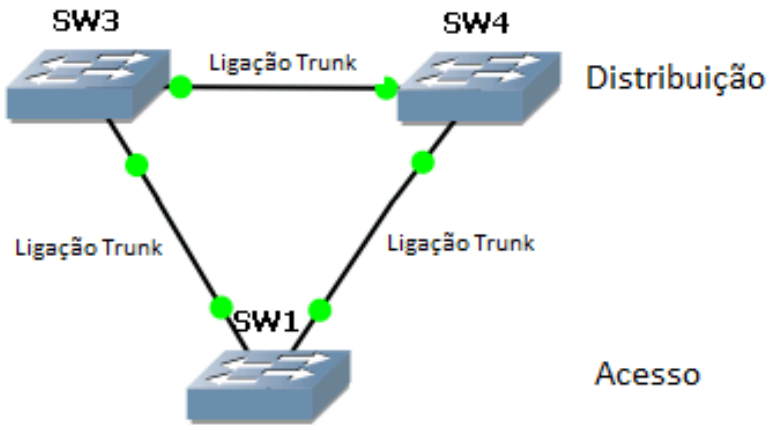

Figura 2.6: Desenho de camada 2 com *loop*

Um desenho de encaminhamento de camada 3 deve considerar os seguintes aspetos:

- Todas as ligações entre *switches*, independentemente da zona a que pertençam, são configuradas como encaminhamento de camada 3.

- Tem como vantagem de eliminar a dependência do STP nas ligações *interswitch*.
- A convergência na rede é determinada, em caso de falha, unicamente, pelo protocolo de encaminhamento utilizado.
- Como desvantagem, aparecem a complexidade e custo do *hardware* utilizado na camada de acesso.

A figura 2.7 ilustra um desenho de camada 3.

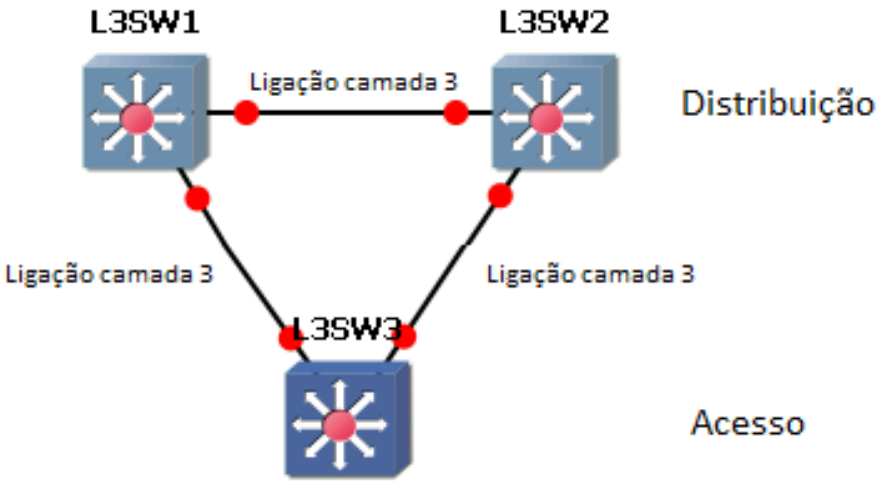

Figura 2.7: Desenho de camada 3

2.2.6 Daisy chain

Quando se projeta a camada de acesso, um tipo de configuração que se deve evitar é o chamado *Daisy chain*, ou seja, a ligação em serie de dispositivos.

Quando se usam ligações de camada 3 entre *switches* da zona de distribuição, na zona de acesso não deve haver ligações entre *switches* desta mesma camada. E caminho

entre *switches* da zona de distribuição nunca deve utilizar ligações entre os *switches* da zona de acesso.

No caso da existência de ligações camada 2, entre *switches* da zona de distribuição, o *daisy chain* é aceitável, mas pode sobrecarregar alguns *switches* da camada de acesso e pode aumentar o tempo de convergência de rede, em caso de falha numa das ligações.

3. Rede Ethernet

3.1 Conceito de VLAN

Um grupo lógico de dispositivos de saída com um conjunto de características e requisitos de rede comuns, independentemente da sua localização física, é definido como uma VLAN (*Virtual Local Area Network*)[12], ou seja, é um aglomerado de portas de *switches* atribuídas a um grupo de trabalho lógico. Uma VLAN tem um único domínio de *broadcast* e comunicação limitada apenas aos dispositivos ligados à mesma. É recomendável a atribuição de uma sub-rede IP. Resolve os problemas de escalabilidade de grandes redes, dividindo um único domínio de *broadcast* em vários pequenos domínios. Para dois dispositivos de VLANs diferentes comunicarem, os pacotes têm de passar por um *router* ou um *switch layer 3*. Geralmente, uma porta de um *switch* transporta apenas tráfego de uma VLAN. Para poder transportar múltiplas VLANS usam ligações *Trunk*. Uma ligação *Trunk* transporta pacotes de múltiplas VLANs usando ISL (*Inter-Switch Link*) *encapsulation* ou IEE802.1Q. Para planear, implementar e verificar VLANs deve-se:

- Descrever os diferentes tipos de modelos de segmentação de VLANs.
- Discutir implementação de VLANs no modelo hierárquico.
- Desenhar um plano para implementar, dado um determinado negócio, e fazer escolhas de acordo com os seus requisitos, para posteriormente analisar as suas consequências.
- Projetar e configurar VLANs.
- Verificar resolução de possíveis problemas de VLANs.

Geralmente, grandes redes com muitos dispositivos encaminham pacotes de *broadcast* e *unicast* por todas as portas da rede. A vantagem do uso de VLANs é a possibilidade de segmentar o domínio de *broadcast* da camada 2. Se forem transmitidos pacotes de *broadcast* dentro de uma VLAN, todos os dispositivos pertencentes á mesma recebem pacotes. Assim, os *switches* filtram a transmissão de todas as portas que não fazem parte dessa VLAN. Existem 2 tipos de segmentação de VLANs: *End-to-end* e *Local*. Quando utilizadores/serviços estão limitados a um determinado local geográfico e ligados á mesma VLAN é considerada uma VLAN *Local*. Enquanto uma VLAN *End-to-end* pode associar portas de *switches* dispersas por toda a rede.

3.2.1 VLAN Local

Como ficou dito, numa VLAN *Local*, todos os utilizadores ligados a *switches* de um local geográfico estão associados á mesma VLAN. Normalmente estão restringidas a um *switch* de acesso, mas o correto funcionamento da empresa pode determinar que assim não seja. Se um utilizador muda de local no interior da empresa, a sua conexão é alterada para uma nova VLAN no novo espaço físico [1]. A figura 3.1 ilustra o desenho de uma rede com apenas VLAN *Local*.

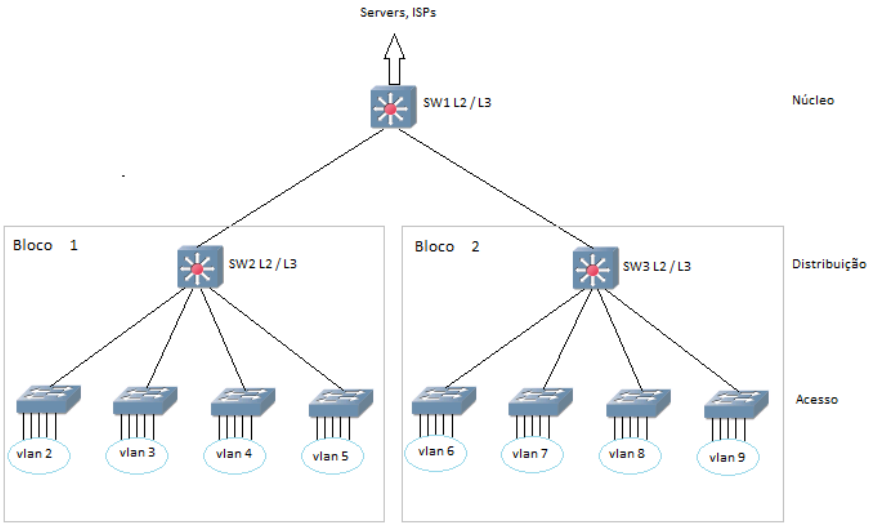

Figura 3.1: VLAN local

Este modelo tem como principais características [1]:

- O administrador da rede cria VLANs locais com fronteiras físicas.
- Normalmente, as VLANs locais existem entre os níveis de acesso e distribuição.
- O tráfego de uma VLAN *Local* é encaminhado até a zona de distribuição ou núcleo, dependendo donde se encontra o primeiro *switch layer 3* ou *router*, para seguir em direção a outro grupo lógico.
- Cada sub-rede IP é única de uma VLAN.

3.2.2 VLAN End-To-End

Uma VLAN *End-to-end* está associada a diferentes portas de *switches* dispersas por toda a rede. A rede de *switches* de camada 2 transporta o tráfego desta VLAN por toda a empresa[1]. A figura 3.2 ilustra o desenho de uma rede com apenas VLAN *End-to-end*.

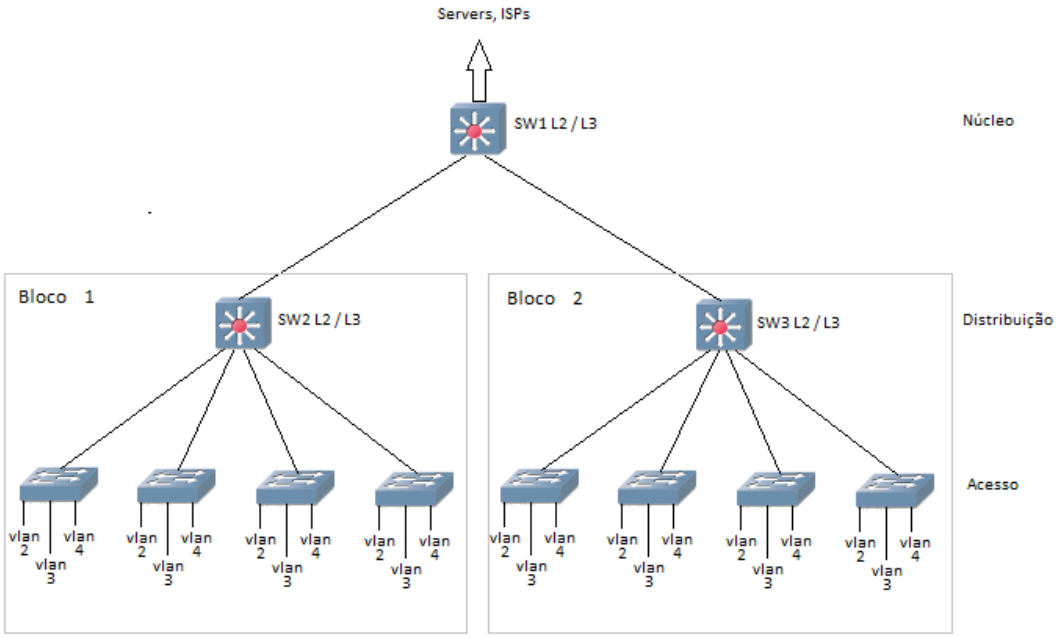

Figura 3.2: VLAN End-to-end

Se mais do que uma VLAN está ativa no modo *End-to-end*, é necessário o uso de ligações *Trunk* entre os switches, para ser possível transportar o tráfego de todas as VLANs. Este modelo tem como principais características [1]:

- A VLAN está dispersa por toda a rede;
- Os utilizadores podem ser agrupados á mesma VLAN, independentemente da sua localização geográfica;
- Se um utilizador se deslocar para um local diferente dentro da empresa, tem acesso á mesma VLAN;
- Utilizadores são agrupados na mesma VLAN, tipicamente por razões de gestão de rede. Sendo assim são mantidos na mesma VLAN, enquanto se deslocam por toda a empresa.
- Todos os dispositivos pertencentes á mesma VLAN têm a mesma sub-rede IP.

Uma vez que qualquer utilizador de uma VLAN *End-to-end* pode localizar-se em qualquer espaço físico da empresa, todos os *switches* têm de ter informação sobre essa VLAN. A resolução de problemas nos aparelhos, ao longo de todo o campus, pode ser mais problemático, uma vez que o tráfego deste tipo de VLAN atravessa toda a rede de *switches*, podendo originar facilmente potenciais problemas no protocolo STP. Para projetar uma VLAN *End-to-end*, devem seguir-se os seguintes passos [1]:

1. Entender o tráfego existente em toda a rede, definindo claramente os grupos pertencentes a cada VLAN e registar as suas máscaras de sub-rede, os seus nomes, objetivos e outras características consideradas relevantes para a rede.
2. Quando estivermos na presença da lista completa de VLANs, saber quais as VLANs necessárias em cada parte da rede, determinando assim o tráfego entre os *switches* e em que *switch* cada VLAN deve estar presente.
3. Ao configurar as portas dos switches ao longo da rede, deve saber-se o que fazer a portas não atribuídas a VLANs: deixá-las com a sua configuração por omissão, atribui-las a VLANs não usadas, por motivos de segurança, ou a uma VLAN por omissão.
4. Após a recolha de informação de todas as VLANs, o próximo passo é a configuração de ligações *Trunk*: decidir quais as ligações a configurar como *Trunk*,

quais as VLANs com permissão, e qual a VLAN nativa – numa ligação *Trunk* um pacote sem rótulo é assumido como sendo da VLAN nativa.

5. No caso de se usar equipamento da marca CISCO, pode utilizar-se o VTP (*VLAN Trunking Protocol*) para simplificar configurações associadas às VLANs. Neste caso, deve identificar-se: os *switches* em que o VTP deve estar ativo; que *switch* deve ter o modo *server*; quais devem ter o modo *client*.
6. Criar um plano de teste, para implementação de VLANs, e verificar se é adequado ao requisito do tráfego e ao seu crescimento futuro.

3.2.3 Procedimentos para a configuração de VLANs

Ao desenhar uma rede com sistema de VLANs, é necessário ter os seguintes cuidados [1]:

- Evitar atribuir a VLAN 1 a portas não usadas
- Tentar, sempre que possível, separar as VLANs, por tipos: dados, voz, gestão e VLAN nativa.
- Se uma porta não está especificada como *trunk*, configura-la manualmente como *access*.
- No caso de VLAN *Local*, é recomendável haver apenas uma a três VLANs por módulo de acesso e limitar essas VLANs a dois *switches* de acesso e distribuição.

Para resolução de problemas, deve-se confirmar sequencialmente: primeiro as conexões físicas; depois a configuração dos *switches*; e, finalmente, a configuração das VLANs.

Quando uma ligação tem problemas de velocidade de transmissão deve-se [1]:

- Verificar a consistência da configuração das duas portas da ligação.
- Usar o comando *show interface* para procurar possíveis erros.
- Verificar caminhos de pacotes e caminhos redundantes no STP.

Quando um aparelho não consegue comunicar com outro na mesma VLAN:

- Assegurar que as portas pertencem á mesma VLAN.

- Verificar se as portas dos *switches* estão ativas e ligadas usando o comando *show* interface.
- Fazer um *reset* às portas usando o comando *shutdown* e *no shutdown*.

3.3 Trunking

Uma ligação *trunk* pode transportar tráfego de várias VLANs. Para uma ligação entre dois *switches* ser do tipo *trunk*, é necessário configurar as portas das extremidades como *trunk*. Antes do transporte, um protocolo de *trunking* marca o pacote para identificar a que VLAN pertence. O switch recetor processa esta informação da melhor maneira, retirando o *VLAN ID* e encaminhando o pacote para a porta associada á respetiva VLAN. Como já foi referido, existem dois protocolos de *trunking*: ISL *encapsulation* e IEE802.1Q. Nesta dissertação, vamos focar-nos no segundo, uma vez que é protocolo mais usado e tem como vantagens [1]:

- Cabeçalho mais pequeno, mais eficiente, especialmente em pacotes mais pequenos. Cabeçalho com 4 bytes enquanto o ISL tem 30 bytes.
- É o protocolo mais abrangente e é aconselhada a sua utilização pela maioria dos fabricantes.
- Tem o suporte 802.1p para QoS.
- Tem um alcance de 1 a 4094 VLANs, enquanto o ISL permite de 1 a 1005 VLANs.

A figura 3.3 ilustra um pacote marcado com o protocolo 802.1Q e os seus campos estão descritos imediatamente a seguir.

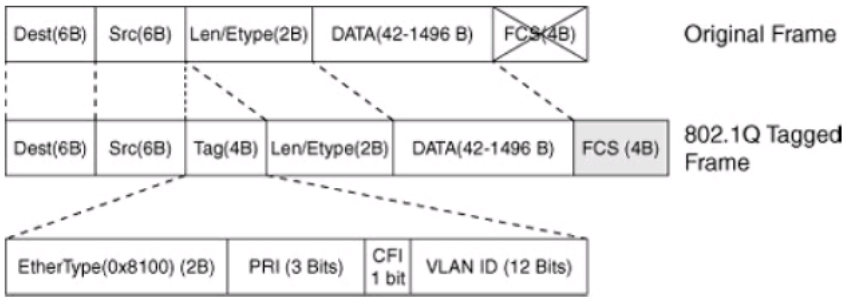

Figura 3.3: Pacote marcado com 802.1Q

Descrição dos campos de um pacote marcado com o protocolo 802.1Q [1]:

- Dest – endereço MAC do destino (6 bytes).
- Src - endereço MAC da origem (6 bytes).
- Tag - campo inserido pelo 802.1Q (4 bytes):
    - Ethertype (TPID) : 0x8100 para especificar que se trata de 802.1Q.
    - PRI : (3 bit) 802.1p campo de prioridade.
    - CFI (*Canonical Format Identifier*) : é definido a 0 para ethernet *switches* e a 1 para redes tipo *token ring*.
    - VLAN ID : (12 bits) Apesar de serem 4096 VLANs possíveis, o número máximo de VLANs são 4094. A VLAN 0 indica *priority frames* e a 4095 (FFF) está reservada.
- Len/Etype - especifica o tamanho ou o tipo (2 bytes).
- Data - Dados a transportar (42 – 1496 bytes).
- FCS - *Frame check sequence* (4 bytes).

A CISCO é proprietária de um protocolo que se encarrega de definir as ligações no modo *trunk* ou *acess*, garantindo a uniformidade das configurações das interfaces de uma ligação. Este protocolo chama-se DTP (*Dynamic Trunking Protocol*) e é do tipo ponto-a-ponto, usado para negociar o estado de *trunking* nas interfaces de um *switch* [1]. É uma prática recomendada porque evita inconsistências iniciais de configurações *trunking* em redes de *switches* multicamada. As interfaces de um *switch* podem ser configuradas de acordo com um dos seguintes modos:

- *Access* – Desativa o modo *trunking* de uma interface e negoceia de modo a converter a ligação para este tipo, independentemente da outra extremidade concordar com esta mudança.
- *Trunk* – Configura a interface em modo *trunk* mas previne a geração de pacotes DTP. É necessário configurar manualmente a outra extremidade, para definir a ligação como *trunk*.
- *Nonnegotiate* – Usada quando se pretende fazer a ligação a um dispositivo sem DTP. Configura a ligação como *trunk*. Também é necessário configurar manualmente a interface da outra extremidade para obter uma ligação *trunk*.
- *Dynamic desirable* – Uma interface configurada neste modo tenta, ativamente, converter a ligação para *trunk*. A interface torna-se *trunk*, se a interface na outra extremidade da ligação for configurada como: *trunk*, *desirable* ou *auto*. Esta é a configuração, por defeito, de todas as interfaces Ethernet que utilizam este protocolo.
- *Dynamic auto* – Obriga a interface a tentar converter a ligação em *trunk*. A interface torna-se do tipo *trunk*, se a interface da outra extremidade da ligação estiver definida como *trunk* ou *desirable*.

A tabela 3.1 refere os Modos de configuração DTP.

MODOS	**Dynamic auto**	**Dynamic desirable**	**Trunk**	**Access**
Dynamic auto	Access	Trunk	Trunk	access
Dynamic desirable	Trunk	Trunk	Trunk	access
Trunk	Trunk	Trunk	Trunk	Conectividade limitada
Access	Access	access	Conectividade limitada	access

Tabela 3.1: Modos de configuração DTP

As ligações do tipo *trunk* são, normalmente, usadas, numa estrutura hierárquica, nas junções dos *switches* da camada de acesso com os da camada de distribuição, para poderem transportar tráfego de várias VLANs. O protocolo DTP é útil quando o estado da interface do *switch* na outra extremidade da ligação é incerto ou pode mudar com o decorrer do tempo. É recomendada a configuração manual de interfaces no modo *nonnegotiate*, no caso de se pretender uma ligação *trunk* estável e pertencentes à mesma infra-estrutura, uma vez que acelera o tempo de convergência. Numa ligação *trunk*, pode pretender-se permitir apenas o tráfego a determinadas VLANs, normalmente a VLANs do tipo *End-to-end*, visto que estas alcançam toda a área da rede. Nesta situação, pode recorrer-se ao comando: *switch trunk allowed vlan VLAN_ID*. Não esquecer, porém, de autorizar o tráfego da VLAN nativa.

Para resolução de problemas numa ligação *trunk* é aconselhável verificar:

- Assegurar que a configuração das interfaces nas duas extremidades da ligação é válida e o modo *trunk* está ativo.
- Verificar se há compatibilidade no modo de encapsulamento nas duas interfaces em causa.
- Verificar que a VLAN nativa é a mesma nas duas extremidades da ligação.

3.4 STP (Spaning Tree Protocol)

O STP [11] é um protocolo utilizado por dispositivos de rede para a escolha do melhor caminho, ao nível da camada 2. Permite o uso de caminhos redundantes entre os *switches*, disponibilizando caminhos alternativos no caso de ocorrerem falhas em algumas ligações e permitindo a ativação e desativação automática dos mesmos. Ajuda, assim, na resolução de problemas de *loops*, em redes com anéis na sua topologia, melhorando a eficiência da rede.

Este protocolo funciona da seguinte forma:

- É designado um *switch* como raiz.

- Os *switches* restantes procuram o vizinho, que proporciona o percurso de menor custo para a raiz, usando o algoritmo de *Bellman-Ford* assíncrono e distribuído.
- É definida uma árvore com todas as ligações de custo mínimo de todos os *switches* para a raiz.
- Apenas as portas pertencentes aos caminhos da árvore definida ficam ativas.

No STP, a escolha do *switch* a desempenhar o papel de raiz é feita consultando o seu ID. O *switch* com menor ID é definido como a raiz da árvore. Este ID é um endereço composto por 8 bytes, onde os 2 primeiros são atribuídos á prioridade (definida pelo gestor de rede) e os restantes 6 bytes são, normalmente, relativo ao endereço MAC de uma das portas do *switch*. Uma vez que a prioridade tem precedência sobre o endereço MAC, o gestor de rede escolhe o *switch* que deve ser definido como a raiz da árvore. Cada LAN tem um *switch* que é responsável pelo encaminhamento de pacotes para a raiz, e da raiz para a LAN. A este *switch* é dado o nome de designado. A raiz é a *bridge* designada de todas as LANs a que estiver diretamente ligada. A porta que envia pacotes da LAN para a *bridge* raiz e vice-versa é a porta designada. Enquanto a porta responsável pelo envio de pacotes da *bridge* designada para a raiz é a porta raiz. Uma vez que todas as portas, que recebem pacotes enviados pela raiz, têm um custo e o custo total do percurso dos pacotes enviados para a raiz é igual à soma dos custos das portas de todo o percurso, a porta que providência o menor custo para a raiz, em cada *bridge*, é definida como a porta raiz. E a porta designada, de cada LAN, é a porta que fornece o melhor percurso para a raiz. As únicas portas ativas nestes elementos de rede são as portas raiz e as portas designadas. As portas de um *switch* podem tomar os seguintes estados:

- Estado *blocking*: Os processos de aprendizagem e envio de pacotes não estão ativos; apenas recebe e processa mensagens de configuração.
- Estado *listening*: Os processos de aprendizagem e envio de pacotes não estão ativos; passa para o estado *learning* depois de permanecer neste estado um período de tempo igual a *foward delay*. Recebe e processa mensagens de configuração.

- Estado *fowarding*: Os processos de aprendizagem e envio de pacotes estão ativos. Recebe e processa mensagens de configuração.
- Estado *disable*: Os processos de aprendizagem e envio de pacotes não estão ativos. Não recebe nem processa mensagens de configuração, uma vez que não participa no protocolo STP.

4. Routing IP

4.1 Protocolos (RIP, IS-IS, EIGRP, OSPF)

A um conjunto de *routers* com políticas de encaminhamento próprias e sob a responsabilidade de um único administrador dá-se o nome de sistema autónomo (SA). Cada sistema autónomo tem um endereço que o identifica, que é atribuído por um *internet registry* ou por um ISP. O encaminhamento de pacotes realizado no interior de um SA é assegurado por protocolos do tipo IGP (*Interior Gateway Protocol*), tais como: RIP, EIGRP, IS-IS e OSPF. Os SA comunicam entre si através de protocolos do tipo EGP (*Exterior Gateway Protocol*).

Neste capítulo, vamos abordar a forma como os *routers* tomam conhecimento de todas as redes existentes e o modo como determinam o melhor caminho para lhes enviar pacotes.

As redes podem estar diretamente ligadas às interfaces dos *routers* ou a redes mais longínquas. No caso de não estarem ligadas às suas interfaces, os *routers* têm duas formas de as conhecer e identificar o melhor percurso para alcança-las: *static routing* ou *dynamic routing*. Quando é um administrador a configurar a informação de cada *router* sobre quais as redes que pode alcançar e qual o melhor percurso diz-se que o protocolo é do tipo *static routing*. No entanto, se um *router* aprender essa mesma informação através de outros *routers*, estamos na presença de um protocolo do tipo *dynamic routing*. Uma rota estática não consegue responder dinamicamente a uma alteração na rede. Quando ocorre uma falha numa ligação, ou quando se introduz mais um *router*, a rota estática deixa de ser válida e torna-se necessário a configuração de novas rotas estáticas.

Nesta dissertação, vamos aprofundar apenas os protocolos que utilizam *dynamic routing*, uma vez que estes permitem que a rede se ajuste de acordo com as alterações feitas na sua topologia, sem a intervenção de um administrador. Neste caso, o administrador apenas configura o protocolo de encaminhamento IP em cada *router*, e são os *routers* que trocam informações sobre as redes que podem alcançar e o seu estado. Quando uma alteração na topologia da rede ocorre, a nova informação é propagada por toda a rede, e todos os *routers* atualizam a sua informação de acordo com as modificações realizadas. Na informação que é trocada por cada *router* está incluído o custo para cada destino. O custo de um caminho é determinante na sua escolha. Relativamente ao custo de uma rota, cabe esclarecer o seguinte: chama-se custo ao valor que os protocolos atribuem ao caminho que um pacote percorre até ao seu destino; este valor varia com o protocolo em uso.

4.1.1 RIP (Routing Information Protocol)

O protocolo RIP [7] é do tipo *distance vector*, ou seja, cada *router* armazena um *distance vector*, constituído por uma listagem de todas as redes que conhece e a estimativa de custo para cada uma delas. Utiliza *distance vector*, de modo a comparar matematicamente rotas para identificar o melhor trajeto para qualquer destino. Periodicamente, o *distance vector* de cada *router* é enviado para *routers* vizinhos, e estes utilizam-no para atualizar o seu próprio *distance vector*. O custo mínimo de um percurso de um *router* para uma rede é obtido pelo contagem do número de *routers* intermédios, onde o custo máximo é 15 e 16 representa o infinito. Esta característica cria estabilidade na rede, uma vez que limitando o número de saltos permitidos evita *loops* infinitos. No entanto, tem como desvantagem a restrição provocada no diâmetro da rede. As entradas da tabela de encaminhamento de cada *router* são determinadas com base nos *distance vector* recebidos dos seus vizinhos. Para cada rede, o *router* tem na sua tabela de encaminhamento uma entrada para os seus vizinhos que lhe proporcionam um caminho com menor custo [2].

Existem duas versões do protocolo RIP.

O RIPv1 tem as seguintes características:

- É um protocolo *classfull*, isto é: não anuncia submáscaras de rede.
- Usa o endereço 255.255.255.255 para enviar os seus anúncios.
- Não suporta autenticação de mensagens.

O RIPv2 tem as seguintes características:

- É um protocolo *classless*, os anúncios incluem prefixo e submáscaras de rede e suporta máscara de tamanho variável.
- Usa endereço *multicast* 224.0.0.9 para enviar os seus anúncios.
- Suporta autenticação de mensagens.

Em qualquer das duas versões, os *routers* podem ser configurados de duas formas: sem *split horizon* e com *split horizon*. No primeiro caso, todas as interfaces de cada *router* anunciam o *distance vector* completo. Enquanto que na configuração com *split horizon*, em cada interface, o router anuncia apenas as redes destino para as quais essa interface não é usada no encaminhamento dos pacotes de dados. Esta última opção, no caso de existir alteração de topologia, diminui o tempo de convergência das tabelas de encaminhamento.

A estas duas versões junta-se ainda o RIPng, com características muito semelhantes aos dois anteriores. As diferenças residem no facto de o RIPng usar IPv6 no transporte, em vez de IPv4, usar prefixos IPv6 e endereçamento IPv6. E ainda o facto de usar o endereço *multicast* ff02::9 como endereço destino para atualizações RIP.

4.1.2 EIGRP (Enhanced Interior Gateway Routing Protocol)

O EIGRP [10] é um protocolo avançado de encaminhamento IP que constitui uma evolução do antecessor IGRP; é propriedade da CISCO. A sua raiz é do tipo *distance vector* mas acumula as vantagens de um protocolo do tipo *link-state*, adicionando-lhe algumas das suas características, como por exemplo descoberta dinâmica de vizinhos. Este

protocolo armazena vários tipos de tabelas, como a tabela de vizinhos, tabela da topologia e a tabela de encaminhamento IP.

Tem um método sofisticado de cálculo dos custos dos percursos, que inclui 2 critérios, por defeito, e mais 3 critérios opcionais [2]. Os dois primeiros são a largura de banda e o atraso ao longo do caminho. Os três critérios opcionais são: a confiança das ligações entre a fonte e o destino, a carga das ligações, e MTU (*Maximum Transmission Unit*).

Uma vantagem deste protocolo em relação a outros, é o facto de permitir aos administradores uma melhor distribuição do tráfego ao logo de toda a rede, uma vez que permite um cálculo variado dos custos dos percursos para todos os destinos, dependendo dos critérios escolhidos, ou seja, o balanceamento de tráfego com custos desiguais.

4.1.3 OSPF (Open Shortest Path First)

O protocolo OSPF [8] foi criado para substituir o protocolo RIP, que apresentava alguns problemas e limitações quando implementado em redes de grande dimensão. O OSPF é um protocolo do tipo *link-state* e não *distance vector* como o RIP. *Routers* configurados com protocolos do tipo *distance vector*, a cada atualização, enviam para os *routers* vizinhos toda ou parte da sua tabela de encaminhamento, enquanto que, no caso de protocolos *link-state*, eles enviam avisos sobre o estado da conexão a todos os *routers* de uma mesma área hierárquica. Cada *router* guarda informação de encaminhamento IP de todos os *routers* de rede, para posteriormente fazer o cálculo do melhor percurso para todos os destinos, usando o algoritmo de *Dijkstra* ou SPF (*Shortest Path First*). Cada interface de um *router* tem associado um custo, e o custo de um percurso para uma rede é dado pela soma de todos os custos das interfaces de saída no sentido do *router*, para a rede alvo. Para tomarem decisões consistentes no que respeita á escolha do melhor percurso, numa primeira fase, a informação necessária é relativa a *routers* vizinhos. A informação de *routers* vizinhos é guardada na *neighbor table* ou na *adjacency table*. Quando um *router* perde contacto com um *router* vizinho, invalida todos os caminhos que

o atravessam e recalcula os percursos. Para garantir a consistência nas decisões é necessário também informação sobre os outros *routers* de rede. Para tanto, são enviados LSAs (*Link State Advertisement*) que são armazenados numa tabela de base de dados, LSDB (*Link State Data Base*). Com esta informação, o *router* está na posse de todos os dados que são necessários para o cálculo das melhores rotas a realizar para cada destino, recorrendo ao algoritmo SPF; percursos que são armazenados na tabela de encaminhamento, e que são consultados quando é necessário reencaminhar pacotes para algum destino [2].

Em redes *broadcast*, os *routers* OSPF escolhem um DR (*Designated Router)* e um BDR (*Backup Designated Router*), e todos os outros *routers* formam adjacências com estes dois. O primeiro *router* a ser ligado é eleito DR, o segundo torna-se BDR. No caso de dois *routers* se ligarem em simultâneo, é escolhido como DR o que tiver maior prioridade, a qual é atribuída pelo administrador; neste caso, o administrador é responsável pela escolha. No caso de o DR avariar, é substituído pelo BDR.

Para um *router* e uma rede serem facilmente identificados, na topologia de uma rede é atribuído a cada um deles um ID. O ID de um *router*, ou é o maior endereço IP de uma das suas interfaces, no momento de ativação do protocolo, ou pode ser atribuído pelo administrador. O ID de uma rede é o endereço IP da interface do seu DR.

Os LSA fazem relatórios sobre o estado dos *routers*, das suas ligações e devem estar sincronizados entre si. Esses relatórios têm as seguintes características:

- São de confiança, quer dizer: têm um método para confirmar a sua entrega.
- Possuem um número de sequência e tempo de vida definidos, para cada *router* saber qual é a versão mais atualizada.
- São atualizados periodicamente para confirmação da informação disponível, antes de expirarem na tabela LSDB.

Resumindo, o modo de operação de um protocolo do tipo *Link-state* pode ser descrito da seguinte forma:

- São geradas atualizações apenas quando são feitas alterações na topologia da rede.
- Quando uma ligação muda de estado, o dispositivo que deteta essa alteração gera

um LSA referente a essa ligação, que é propagado usando um endereço *multicast*.

- Cada *router* guarda e envia LSA para os vizinhos.
- Cada *router* atualiza a tabela LSDB.
- Os *routers* encontram os melhores caminhos, usando o algoritmo SPF, a partir da informação armazenada na tabela LSDB, para construir a árvore SPF.
- Cada *router* escolhe os melhores percursos da árvore SPF e coloca-os na tabela de encaminhamento.

4.1.4 IS-IS (Intermediate System-Intermediate System)

O protocolo IS-IS [9] é do tipo *link-state*. Todos os *routers* têm conhecimento da topologia rede e usa o algoritmo SPF, para determinar os percursos de custo mínimo para todos os destinos. Este protocolo: proporciona rápida convergência e é eficiente no uso da largura de banda; utiliza encaminhamento hierárquico; tem comportamento *classless* e um método de envio rápido de nova informação de rede; à semelhança do OSPF, recorre á divisão da rede em áreas; o seu comportamento hierárquico é dividido em duas camadas - comunicação dentro das áreas e comunicação entre áreas.

Um IS (*Intermediate System*) de nível 2 guarda rotas para áreas destino, enquanto um IS de nível 1 trata do encaminhamento de pacotes dentro das áreas. Para um pacote ser encaminhado para outra área, o IS de nível 1 envia o pacote para o IS de nível 2 mais próximo dentro da sua área. Posteriormente, o pacote é transmitido através de encaminhamento de nível 2 até à área destino e de seguida encaminhado via nível 1 para o seu destino final.

4.2 Metodologias de implementação com OSPF

4.2.1 V2 e v3

OSPFv3 está para o IPv6 como OSPFv2 para o IPv4. Apesar de terem muito em comum, existem diferenças no modo de funcionamento do protocolo. O OSPFv3 processa informação por ligação e não por sub-rede, usa o termo ligação, em vez de sub-rede, para definir um meio de comunicação entre *routers*. Várias sub-redes IP podem ser atribuídas a uma ligação, e dois *routers* podem comunicar entre si, mesmo não partilhando a sub-rede IP. A topologia não é, no entanto, específica de IPv6, mantendo o *router ID*, área ID e *link ID* com 4 bytes. Aos 7 tipos de LSA, que a segunda versão do protocolo OSPF inclui, são adicionados mais dois na terceira versão, o *Link* LSA e o *Intra-area Prefix* LSA.

4.2.2 Áreas

As redes de pequena dimensão têm uma estrutura relativamente simples, e os percursos para os destinos possíveis são facilmente calculados.

Em grandes redes, muito complexas, com elevado número de potenciais caminhos para os vários destinos, dificulta a comparação de todos esses trajetos no algoritmo SPF, para a obtenção do mais indicado. Uma área de *routers* OSPF muito grande pode originar alguns problemas, tais como:

- Cálculos sistemáticos do algoritmo SPF e respectivas atualizações das tabela de encaminhamento. Este problema pode ser provocado por alterações na estrutura de uma rede, que são inevitáveis.
- Excecional dimensão da tabela LSDB. Visto que a tabela LSDB cobre a topologia de toda a rede e todos os *routers* mantêm entradas na sua tabela para todas as sub-redes, pode acabar por acontecer que seja gerada uma tabela LSDB muito grande.
- Tabela de encaminhamento muito grande. Uma vez que OSPF não realiza resumos de rotas por defeito, a tabela de encaminhamento pode tornar-se muito grande.

Nestas redes, este protocolo pode tornar-se inaplicável, apesar de ser vantajoso ter toda a informação em todos os *routers*. Tal facto pode determinar a divisão da rede em áreas OSPF. Dentro de uma área, os *routers* guardam a informação relativa a ligações e *routers* dessa mesma área. Desta forma, uma falha numa ligação ou num *router* é transmitida apenas para *routers* dessa área. O protocolo OSPF pode ser configurado para que seja guardada apenas informação geral ou resumida, de outros *routers* e ligações exteriores a essa área. A rede fica definida com uma estrutura hierárquica em que o número de *routers*, dentro de uma área, é limitado; essa estrutura deve garantir que todas as áreas se liguem a uma área 0 central. O OSPF usa uma hierarquia de 2 camadas, a saber: *backbone* e *regular*. O *backbone* descreve-se da seguinte forma:

- Tem como nome área 0.
- É o núcleo onde todas as outras áreas se ligam.
- Interliga todas as outras áreas.
- A principal função é encaminhar rápido e eficientemente os pacotes IP.
- Os utilizadores terminais, normalmente, não pertencem a esta área.

O *non backbone* ou *regular* descreve-se da seguinte forma:

- A principal função é ligar utilizadores e recursos.
- Por defeito, não permite que o tráfego de outras áreas utilize as suas ligações, porque esse tráfego tem de passar pela área *backbone*.
- Pode ter vários sub-tipos: *standard area*, *stub area*, *totally stubby area*, *not-so-stubby area* ou *totally stubby area*.

Para controlar o tráfego dentro e fora das diferentes áreas, é necessário ter diferentes tipos de *router*. Os tipos de *routers* a adotar são:

- *Internal router* – *Routers* com todas as interfaces na mesma área.
- *Backbone router* – *Routers* na periferia da área 0, que possuem uma interface ligada a essa área, pelo menos.
- ABR (*Area border router*) – *Routers* que têm interfaces ligadas a várias áreas.
- ASBR (*Autonomous system boundary router*) – *Routers* com pelo menos uma interface ligada a um domínio diferente de encaminhamento IP.

O uso de áreas em OSPF tem como principais vantagens:

- Reduzir a frequência dos cálculos no algoritmo SPF – Uma vez que a informação detalhada de encaminhamento IP apenas circula dentro da mesma área, quando ocorre uma alteração na estrutura, apenas *routers* dentro dessa área necessitam recalcular o algoritmo SPF.
- Tabelas LSDB mais pequenas – as entradas detalhadas da tabela de encaminhamento, duma determinada área, podem ficar dentro dessa mesma área. Os routers podem ser configurados de forma a fazerem resumos de rotas, para os routers fora da sua área, diminuindo assim o número de LSAs propagados entre áreas, e mantendo toda a rede alcançável.

4.2.3 Rotas por omissão

Uma rota por omissão é usada quando não existe uma rota definida para um dado destino, na tabela de encaminhamento de um *router*. Para um *router* comunicar com redes exteriores ou para aceder á *internet* é aconselhável a sua configuração com rotas por omissão. Esta opção resulta em tabelas de encaminhamento mais pequenas e tempo de utilização de recursos e carga do CPU mais reduzidos. De facto, deixa de haver necessidade de recalcular o algoritmo SPF, quando uma rede exterior falha. Para um *router* OSPF gerar uma rota por omissão é necessário recorrer ao comando *default-information originate*. Sempre que esta configuração for usada num *router*, este torna-se ASBR.

Há duas formas para anunciar uma rota por omissão: a primeira é anunciando 0.0.0.0 (route IP 0.0.0.0) no domínio OSPF, garantindo que o *router* que anuncia já tem a rota por omissão, recorrendo ao comando *default-information originate*; a segunda é anunciando 0.0.0.0 e acrescentando *always* no comando *default-information originate*, independentemente do *router* que anuncia já ter uma rota por omissão. Assim o comando a usar é:

```
default-information originate [always] [metric metric_value][metric-type
type_value][route-map map_name]
```

Onde o campo *metric* é relativo ao custo associado à rota, no caso de não ser especificado é atribuído 1. O campo *metric-type* pode tomar dois valores, 1 ou 2. Se não for escolhido, é atribuído tipo 2. Quando se opta pelo tipo 1 neste campo, o custo do percurso é a soma de todas as ligações ao logo do mesmo. O tipo 2 mantém o custo fixo. A utilização deste comando leva o *router* a enviar a rota por omissão a todos os seus vizinhos OSPF.

4.2.4 Interfaces passivos

Em grandes redes empresariais os *routers* da camada de distribuição têm geralmente muitas interfaces e podem formar-se adjacências não desejadas. Para contrariar esta situação, existe a possibilidade de definir uma interface como passiva. Esta característica permite a interface participar no encaminhamento de pacotes, mas impede-a de formar adjacências. Não enviando pacotes do tipo *hello* e descartando pacotes do mesmo tipo. Este tipo de configuração é útil, no caso de existir na estrutura da rede uma camada de acesso nível 2 e uma camada de distribuição nível 3. Para evitar que os *routers/switches layer 3* formem adjacências através dos switches de acesso, continuando a participar na parte de encaminhamento de pacotes.

Para definir-se uma interface como passiva usa-se o comando:

```
passive-interface interface.
```

4.2.5 Caminhos múltiplos

A escolha de uma só rota para a transmissão de pacotes para um destino pode não ser a melhor opção, uma vez que pode implicar a sobrecarga de uma ligação. O protocolo OSPF

permite-nos proceder à divisão do tráfego em múltiplas rotas fazendo o balanceamento de carga nas ligações, de forma a evitar o seu congestionamento e a obter mais eficiência. Assim, o desenho de rede deve ser elaborado de modo a assegurar a possibilidade de encaminhamento de pacotes via caminhos múltiplos. Para isso, é necessário configurar o protocolo OSPF, com caminhos múltiplos e com os mesmos custos. Neste protocolo, é possível usar a opção que permite escolher o número de caminhos com o mesmo custo e para o mesmo destino, a inserir na tabela de encaminhamento. Por omissão, o OSPF permite um número máximo de caminhos com o mesmo custo/destino para balanceamento de rede (no caso do equipamento CISCO, são 4 o número desses caminhos).

Para configurar o número máximo de caminhos é necessário usar, no modo de configuração, o comando:

```
maximum-path path_number
```

É possível confirmar o número de rotas para cada destino, observando a tabela de encaminhamento de um *router* com o comando:

```
Switch# show IP route
```

4.2.6 Redistribuição de rotas

A troca de rotas entre domínios, com diferentes tipos de protocolos de encaminhamento, é dada o nome de redistribuição de rotas. A redistribuição pode ser apenas num sentido, quando um protocolo redistribui as sub-redes apreendidas de outro protocolo. Ou pode ser nos dois sentidos, quando há uma partilha de rotas entre os dois protocolos.

Os fatores a ter em conta, ao fazer uma redistribuição de rotas, são:

- A perda do custo das rotas do protocolo redistribuído.
- O aparecimento de possíveis *loops* no encaminhamento de pacotes. A forma mais segura é fazer uma redistribuição de rotas num só sentido, e

apenas num *router* fronteira entre os dois protocolos. No caso de haver necessidade de fazer uma redistribuição de rotas nos dois sentidos e em vários *routers* fronteira, deve-se ajustar as rotas para evitar *loops* e otimizar o encaminhamento.

As técnicas de redistribuição de rotas são:

- Redistribuição de rotas por omissão do núcleo para o limiar do sistema autónomo e redistribuição de rotas no sentido inverso. Esta opção ajuda a evitar *loops*, otimizar o encaminhamento e a prevenir o *feedback* de rotas.
- Redistribuição de rotas estáticas do núcleo para o limiar do sistema autónomo e redistribuição de rotas no sentido inverso. Esta técnica resulta se houver apenas um ponto de redistribuição, caso contrário pode causar *feedback* de rotas.
- Redistribuição de rotas do núcleo para o limiar do sistema autónomo, com filtragem para bloquear rotas indesejadas. Rotas redistribuídas do limiar do sistema autónomo para o núcleo num ponto de redistribuição, não devem voltar a ser redistribuídas novamente noutro ponto de redistribuição.
- Redistribuição de todas as rotas do núcleo para o limiar do sistema autónomo e redistribuição de todas as rotas no sentido inverso, modificando a distância administrativa associada a rotas redistribuídas, para que não sejam escolhidas quando estiverem na presença de múltiplos caminhos para o mesmo destino.

5. Cenários de implementação

Para simular os cenários de implementação que vão ser apresentados, utilizou-se o programa GNS3. As simulações realizadas servem para exemplificar a sua configuração e demonstrar o seu correto funcionamento. O GNS3 funciona com imagens reais IOS da Cisco, emuladas através do programa *dynamips* [5]. Tem uma interface intuitiva, fácil de utilizar e permite simular redes de elevada complexidade. Na simulação de todas as topologias de rede apresentadas foram utilizados sempre os mesmos modelos e as respetivas imagens IOS. Foi utilizado o módulo de *switch* com 16 portas do *router* 3640 com a imagem IOS *c3640-jk9o3s-mz.124-16a.bin*, para funcionar como *switch layer 2*. O *router* 3725, com a imagem IOS *c3725-advIPservicesk9-mz.124-21.bin*, para funcionar como *switch layer 3*. E por fim o modelo do *router* utilizado foi o 3640, com a mesma imagem IOS apresentada anteriormente.

5.1 Estratégias de implementação

Nesta parte, vão ser apresentados alguns cenários de implementação possíveis, utilizando alguns dos conceitos anteriormente discutidos, a saber:

- *Switches layer 2* e layer *3*.
- VLANs *Local* e VLANs *End-to-end*.
- Ligações *trunk*.

- Redundância.

Para isso, vai ser simulado o caso de uma empresa com dois blocos, onde o tráfego para cada um deles é encaminhado por um *switch* da camada de núcleo (SW1) para os *switches* da zona de distribuição (SW2 e SW3) que são responsáveis pela ligação à zona de acesso. Na figura 5.1 está representada a estrutura de rede, em que podemos ver os nós (SW1, SW2 e SW3) onde serão utilizadas várias combinações de *switches de layer 2* e *layer 3*. Pretende-se distinguir as vantagens e desvantagens de cada situação, não para identificar qual a melhor camada, mas sim para saber qual a camada adequada à realização do trabalho pretendido, em cada fase de uma rede empresarial.

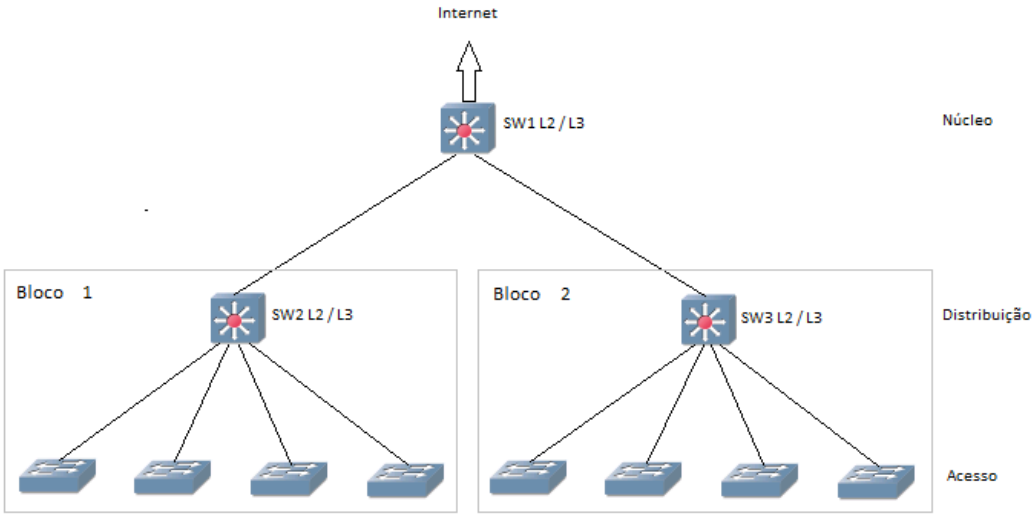

Figura 5.1: Topologia de rede

Na figura 5.1, é possível observar:

- Dois edifícios sendo cada um deles representado por um bloco.
- Cada bloco é constituído por uma zona de distribuição e uma zona de acesso.
- Cada bloco está ligado ao núcleo da rede.

Esta topologia pode ser implementada em grandes empresas, aumentando o número de blocos relativos a edifícios ligados ao núcleo da rede. Posteriormente, vão ser adicionados

switches em paralelo na zona do núcleo e da distribuição para introduzir redundância na estrutura da rede.

Em todas as situações a seguir apresentadas, inicialmente, vai ser configurado apenas o modelo de VLAN *Local*, e, posteriormente, vão ser indicadas as modificações a fazer na configuração da rede para a implementação do modelo *End-to-end*, de modo que o sistema seja capaz de operar com os dois modelos: VLAN *Local* e VLAN *End-to-end*.

Os cenários simulados foram:

- Cenário 1: Zonas de distribuição e do núcleo constituídas por *switches de layer 2*. Este cenário usa comutação de camada 2 para garantir a conectividade e a segmentação da rede. É o caso mais económico, mas é de difícil aplicação em redes de grande dimensão.
- Cenário 2: Zonas de distribuição constituída por *switch layer 2* e do núcleo por *switch layer 3*. Proporciona um bom balanceamento de caraterísticas de camada 2 e camada 3. Indicada para redes com necessidade de priorizar a comunicação entre as várias sub-redes dispersas pela empresa.
- Cenário 3: Zonas de distribuição e do núcleo constituídas por *switches layer 3*. Este cenário é indicado para redes de grande dimensão e com muitos segmentos de rede. Indicada para redes com necessidade de priorizar a comunicação entre as várias sub-redes presentes num mesmo bloco.
- Cenário 4: Introdução de redundância na estrutura de rede do cenário 3. Este cenário é indicado para empresas que procuram uma rede com alta disponibilidade e redundância.
- Cenário 5: Utilização de subdomínios de encaminhamento.
- Cenário 6: Introdução de um bloco de acesso à Internet.

5.1.1 Cenário 1

Dá-se o nome de domínio de comutação de camada 2 a um grupo de *switches de layer 2* ligados entre si [3].

Neste cenário, utiliza-se um domínio de comutação de camada 2, com *switches layer 2* em SW1, SW2 e SW3. Uma falha neste domínio, devido a uma configuração errada, ou a uma falha num dispositivo, ou numa ligação, pode provocar um erro e afetar toda a rede, originando problemas de comunicação entre diferentes elementos de rede.

Este domínio pode também ficar congestionado com pacotes de *broadcast* que são transportados por toda a rede de camada 2. A redução de possíveis congestionamentos das ligações e de perdas de eficiência da rede pode ser assegurada pela utilização de VLANs. Como foi dito anteriormente, a utilização de VLANs, ao promover a segmentação da rede, restringe os domínios de *broadcast* a membros de uma mesma VLAN.

O modelo *Local*, obriga o agrupamento físico de utilizadores/serviços de acordo com a sua função na organização, e apenas este tipo de configuração vai ser aplicado nesta fase. Nesta ordem de ideias, alguns fabricantes, nomeadamente a CISCO, aconselham a restrição de uma VLAN por *switch* de acesso, de modo a limitar os domínios de *broadcast*; no entanto, a localização geográfica dos dispositivos de rede pode, por vezes, não o permitir.

A Figura 5.2 ilustra a Topologia de rede deste cenário.

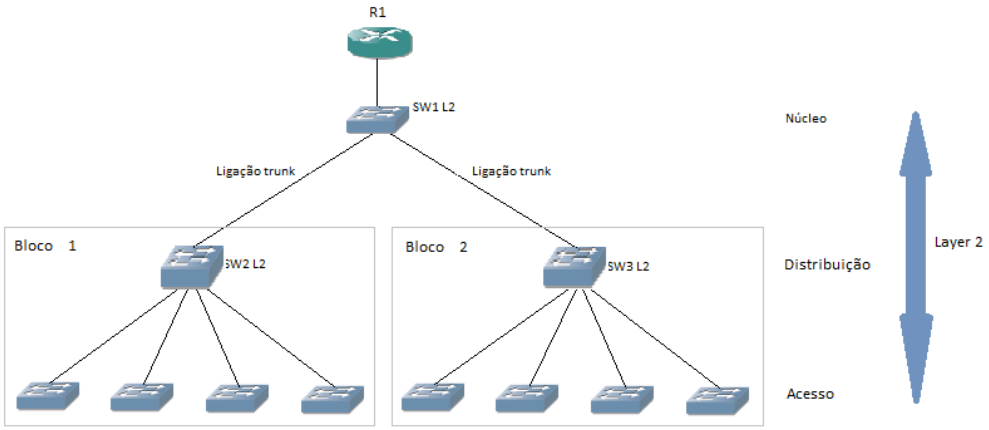

Figura 5.2: Topologia de rede cenário 1

Este tipo de configuração implica o uso de uma ligação entre o *switch* do núcleo (SW1) e os *switches* de distribuição de cada bloco (SW2 e SW3), no modo *trunk*, de forma a possibilitar o transporte de tráfego de várias VLANs. No entanto, em cada ligação para o núcleo, deve-se restringir o transporte de pacotes aos pertencentes a VLANs presentes no bloco a que a ligação respeita.

A ligação, entre os *switches* de distribuição e de acesso, pode ser configurada de uma de duas formas: em geral, essa ligação deve ser configurada no modo *trunk* assegurando o transporte de tráfego de várias VLANs e dando maior flexibilidade à rede, uma vez que fica assegurada a possibilidade de adição de novas VLANs, sempre que necessário e sem alteração da configuração desta ligação; no entanto, a ligação pode ser definida no modo de acesso a uma dada VLAN, no caso do *switch* de acesso estar configurado apenas para essa VLAN, evitando, assim, que o tráfego relativo a outras VLANs chegue a esse *switch*.

Neste caso, é possível obter uma rede simétrica, robusta e com o melhor desempenho possível, definindo o *switch* SW1 como raiz do STP.

A utilização de dispositivos de camada 2 tem as seguintes vantagens:

- Menor custo de implementação.
- Simplificação da comunicação, feita ao nível da camada 2 do modelo OSI, isto é, ligação de dados. Utiliza elementos de rede do tipo *store and forward*, proporcionando menor latência.

A implementação de uma rede, com zona de distribuição e núcleo, constituída por dispositivos que operam ao nível da camada 2, apresenta algumas desvantagens:

- Congestionamento das ligações, nas redes de grande dimensão.
- Reduzidos mecanismos de controlo de qualidade de serviços - definição de prioridades de VLANs.
- Limitados mecanismos de controlo de segurança - filtragem de endereços MAC nas tabelas de encaminhamento dos *switches*.

No que respeita á comunicação entre VLANs diferentes, os pacotes têm de ser encaminhados através de SW1 até um dispositivo capaz de operar ao nível da camada 3 - *router* ou *switch layer 3* -, para se efectuar o encaminhamento entre as mesmas.

Utilização de VLANs End-to-end

Uma VLAN do tipo *End-to-end* é uma VLAN que pode associar portas de vários *switches* dispersas por toda a rede á mesma VLAN.

Para uma VLAN deste tipo poder ser utilizada é necessário garantir que todas as ligações tenham capacidade de transportar pacotes a estas pertencentes.

Ao configurar a rede de modo a admitir VLANs do tipo *End-to-end*, é necessário considerar:

1) A inicialização das VLANs *End-to-end* em todos os switches da rede.

2) Que as ligações entre a zona de distribuição e o núcleo, definidas previamente como *trunk* e restringidas ao tráfego pertencente a VLANs *Local*, presentes em cada bloco, devam também poder assegurar o transporte de pacotes de todas as VLANs *End-to-end*.

3) Que as ligações do acesso à distribuição sejam estabelecidas no modo *trunk*.

Esta configuração permite que qualquer utilizador possa aceder aos recursos da sua VLAN, independentemente da sua localização no campus.

A este modelo está associado um maior domínio de *broadcast*, uma vez que todo o tráfego marcado com o *tag* de uma VLAN deste tipo pode circular por toda a rede, provocando o congestionamento das ligações definidas como *trunk* e dos próprios equipamentos de rede de camada 2.

5.1.2 Cenário 2

O segundo caso inclui o uso de *switches layer 3* no núcleo e *switches layer 2* na zona de distribuição.

A figura 5.3 ilustra a topologia de rede correspondente a este cenário.

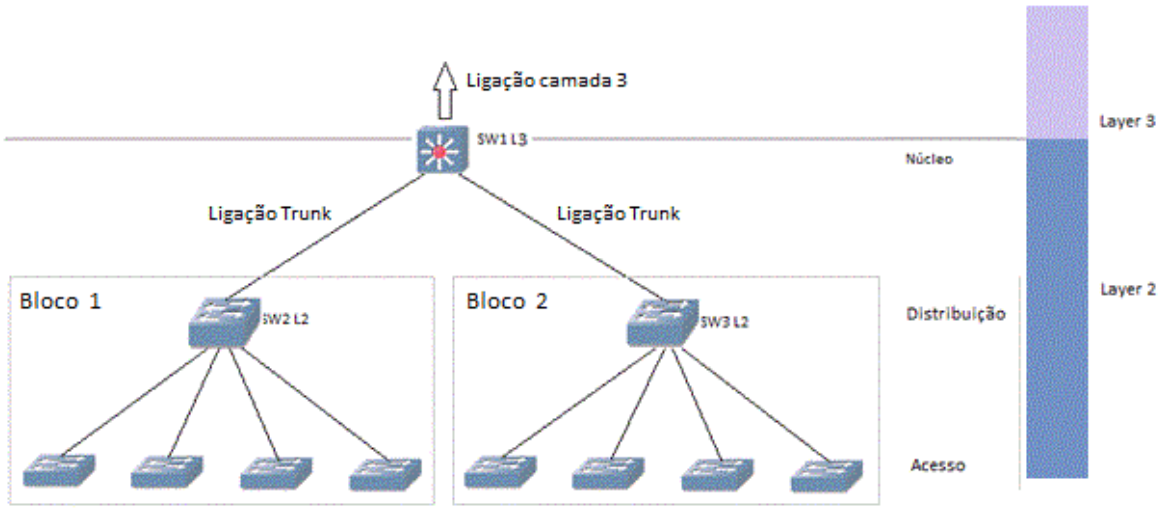

Figura 5.3: Topologia de rede cenário 2

O *switch* SW1 combina agora serviços de camada 2 e de camada 3 para fornecer maior facilidade de escalabilidade, segurança e rápida convergência. Os *switches* de distribuição operam ao nível da camada 2 e fazem *forwarding* de pacotes pelas ligações *trunk* até SW1, enquanto SW1 deve estar configurado de modo a trabalhar num ambiente *trunking* de camada 2 para a zona de distribuição e num ambiente de camada 3 nas ligações para o ISP e para os servidores. Assim, o núcleo é responsável pela ligação entre a zona de *switching* de camada 2 e a zona de encaminhamento de camada 3.

Ao nível da camada 3, a cada VLAN está atribuída uma sub-rede de IP, isto porque uma sub-rede IP é o equivalente lógico de camada 3 de uma VLAN de camada 2. No entanto, uma VLAN pode ter várias sub-redes IP simultaneamente. Este endereço de sub-rede IP é definido no *switch layer 3*, onde o domínio de comutação de camada 2 acaba.

Uma das vantagens deste modelo topológico reside no facto de a comunicação entre dispositivos pertencentes a VLANs diferentes ser efetuada no *switch layer 3* SW1, presente no núcleo. Esta configuração é indicada para o caso de redes que requerem uma maior flexibilidade de comunicação entre as várias sub-redes dispersas por toda a rede, ou seja, quando existe necessidade de várias VLANs, presentes em diferentes blocos, comunicarem entre si, uma vez que o *default gateway* de cada VLAN é agora configurado

em SW1. Além disso, proporciona um bom balanceamento entre características da camada 2 e 3.

No que diz respeito a VLANs *End-to-end*, a sua aplicação é semelhante ao caso anterior.

5.1.3 Cenário 3

A figura 5.4 ilustra o desenho de rede do cenário 3.

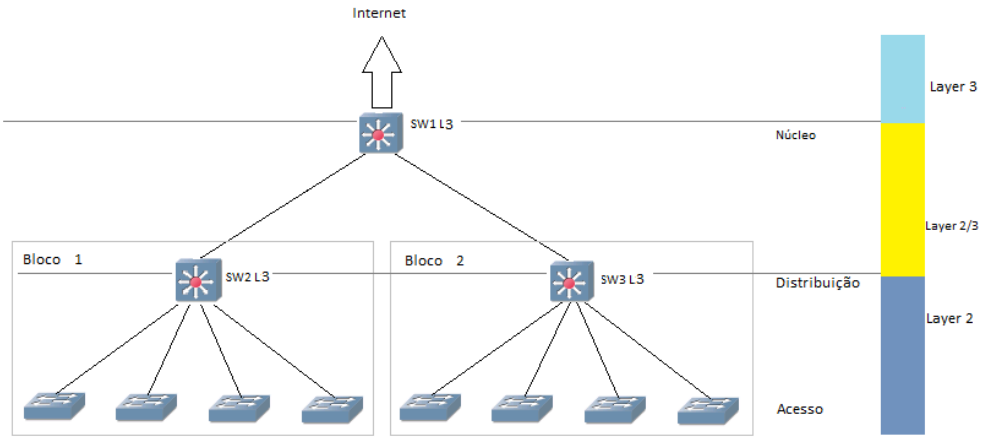

Figura 5.4: Topologia de rede cenário 3

Esta topologia de rede utiliza *switches layer 3* no núcleo e na zona de distribuição. Quando se substituem os *switches* SW2 e SW3 por *switches layer 3* são adicionadas propriedades de camada 3 à zona de distribuição. As ligações entre a zona de distribuição e o núcleo, antes realizadas por *trunking* de camada 2, são agora substituídas por encaminhamento de nível 3 ponto-a-ponto. A fronteira entre a camada 2 e 3 é, agora, feita no bloco de distribuição [4]. As ligações entre SW2/SW3 e os *switches layer 2* da zona de acesso continuam de camada 2, no modo *trunk*. Dentro do mesmo bloco, a comunicação entre diferentes VLANs não necessita agora de recorrer ao *switch* da zona de núcleo para se realizar, já que SW2 e SW3 operam também ao nível da camada 3. O *default gateway* e a raiz no STP são deslocados do núcleo para a zona de distribuição.

Esta situação é indicada para redes que necessitam de configuração simples, e possuem VLANs que têm como prioridade comunicar com outras VLANs do mesmo bloco, visto que o encaminhamento de pacotes entre grupos lógicos de cada bloco pode agora ser feito pelo *switch* de distribuição. Para VLANs de blocos diferentes comunicarem, os pacotes da VLAN fonte são enviados para o *default gateway*, na zona de distribuição, posteriormente passam pelo núcleo e seguem para o *switch* de distribuição do bloco da VLAN destino, através de encaminhamento IP. É recomendado a implementação de OSPF ou EIGRP como IGP nos *switches layer 3* do núcleo e de distribuição. Este modelo topológico, quando utilizado com *switches* redundantes na zona de distribuição e no núcleo, tem as seguintes vantagens:

- Rápida convergência.
- Balanceamento de tráfego dinâmico.
- Configuração de *multicast* simplificada.
- Ferramentas simples de resolução de possíveis problemas de encaminhamento extremo-a-extremo.

Utilização de VLANs End-to-end e Locais

A implementação de VLANs *End-to-end* nesta situação é semelhante aos dois casos anteriores. Pacotes com origem neste tipo de VLANs, são transportados ao nível da camada 2, pelas ligações *trunk*, para toda a rede, marcados com o *tag* da VLAN correspondente. Esta é a razão para na figura, as ligações entre a camada de distribuição e o núcleo estarem definidas como ligações de camada 2/3, uma vez que o transporte de pacotes relativo a VLANs *Local* é realizado ao nível da camada 3, através de uma VLAN de interligação - conceito apresentado a seguir. Neste modelo de VLANs, é mais adequado escolher-se para raiz do STP o *switch* SW1, uma vez que é o *switch* mais central e próximo do núcleo de rede, proporcionando a simetria desejada para uma VLAN que pode abranger toda a rede.

VLAN de interligação

Uma VLAN de interligação tem como função transportar tráfego de VLANs *Local* entre *switches layer 3*, quando existem VLANs *End-to-end* na topologia de rede, permitindo a utilização da mesma ligação para encaminhamento de pacotes ao nível da camada 2 e da camada 3. Os pacotes que usam a VLAN de interligação como meio de transporte são enviados utilizando encaminhamento IP, e são marcados durante o mesmo com o *tag* da VLAN de interligação.

Na figura 5.5 está representada a VLAN 100, definida como VLAN de interligação.

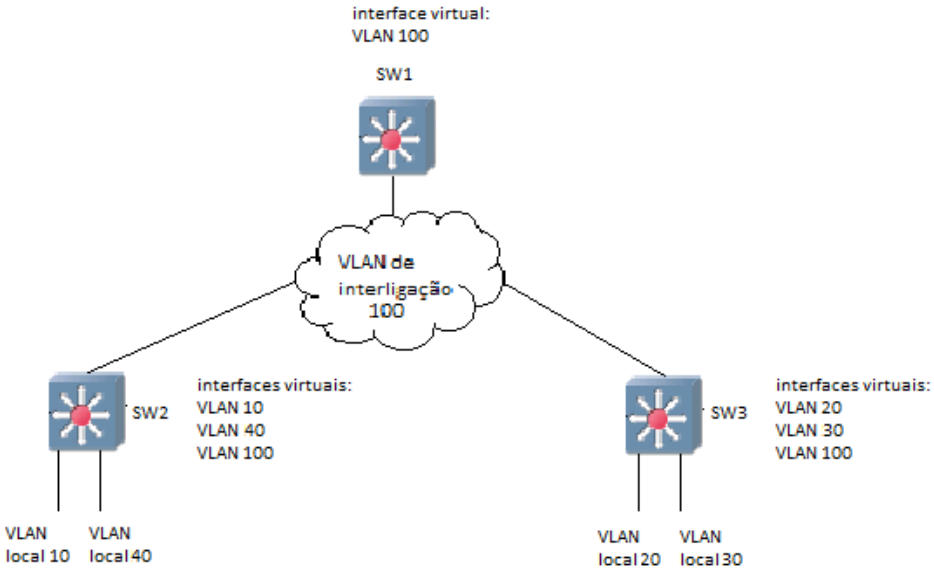

Figura 5.5: VLAN de interligação

Para facilitar a compreensão deste conceito, vamos simular um fluxo de pacotes entre a VLAN 10 e a VLAN 20. Quando a VLAN 10 pretende comunicar com a VLAN 20 os pacotes depois de chegarem ao seu *default gateway*, a interface virtual da VLAN 10 em SW2, são transportados utilizando o encaminhamento IP através da VLAN 100 até SW1 e posteriormente até SW3, que os reencaminha para as portas atribuídas à VLAN 20.

Não esquecer que as ligações SW1-SW2 e SW1-SW3 devem ser definidas no modo *trunk* e devem permitir apenas tráfego da VLAN de interligação e de VLANs do *tipo End-to-end*. Estas ligações têm assim capacidade para transportar o tráfego das VLANs *End-to-end* de camada 2 e o tráfego da VLAN de interligação, através de encaminhamento IP. É uma ligação com capacidade de transporte multicamada, como evidencia a figura 5.6.

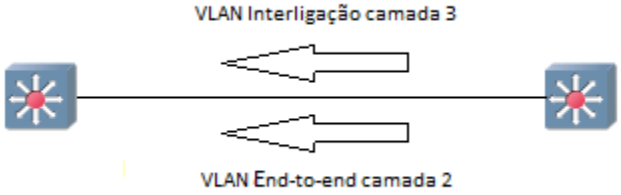

Figura 5.6: Ligação multicamada

Nesta situação, é obrigatório definir nos *switches* de distribuição, de cada bloco, as interfaces virtuais das VLANs, do respetivo bloco, bem como as interfaces responsáveis pelas ligações entre a distribuição e o acesso, como interfaces passivas, para evitar a formação de adjacências indesejáveis e a inundação das ligações com pacotes Hello não necessários. Para que o tráfego pertencente a uma VLAN *Local*, não utilize o canal reservado a uma VLAN *End-to-end* e seja transportado através da VLAN de interligação, é necessário configurar a interface virtual das VLANs *End-to-end* como interfaces passivas.

Quando se faz um *ping* de um pc da VLAN 10 para um pc da VLAN 20, e se captura um pacote na ligação entre a zona de distribuição e o núcleo, utilizando o programa wireshark, pode-se constatar que o identificador de VLAN tem o valor 100, correspondente à VLAN de interligação. A figura 5.7 ilustra a situação. Enquanto que um pacote que pertença a uma VLAN *End-to-end* e que atravesse a mesma ligação, é marcado com o *tag* dessa mesma VLAN e não com o valor da VLAN de interligação.

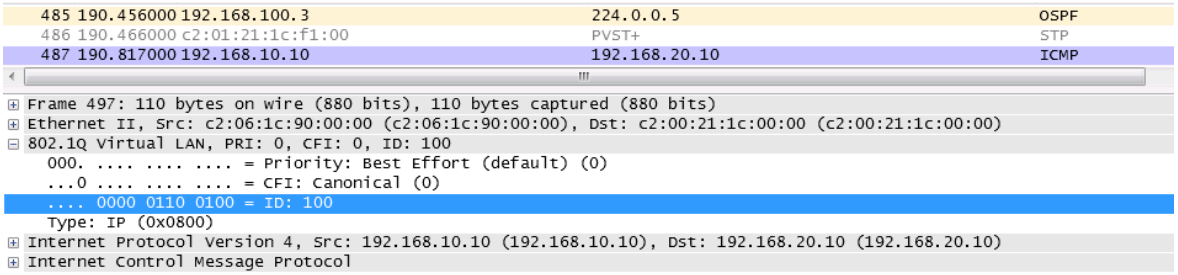

Figura 5.7: Pacote ICMP

5.1.4 Cenário 4: Redundância

Neste cenário acrescenta-se redundância no desenho de rede do cenário 3. A redundância será introduzida na zona de distribuição e do núcleo. Deste modo, os *switches* da zona de acesso passam a ter ligações alternativas à zona de distribuição, assim como a zona de distribuição passa a ter caminhos alternativos para encaminhar tráfego para o núcleo da rede.

Apesar da utilização de uma ligação única de cada um dos *switches* da zona de distribuição a cada um dos do núcleo da rede, separando os *switches* do núcleo, reduzir o número de relações de adjacência do protocolo de encaminhamento e o número de portas utilizado, este cenário não introduz a redundância desejada. A figura 5.8 evidencia a situação.

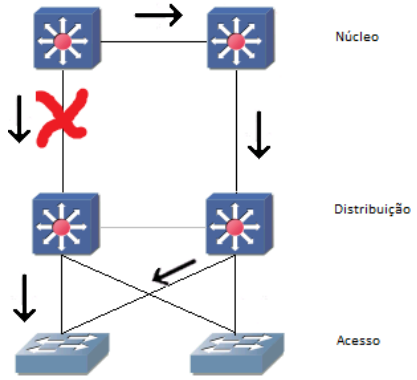

Figura 5.8: Switches de distribuição com ligação única ao núcleo

Como se pode ver, uma falha numa ligação implica a convergência do protocolo encaminhamento. Agora, observemos um desenho da figura 5.9.

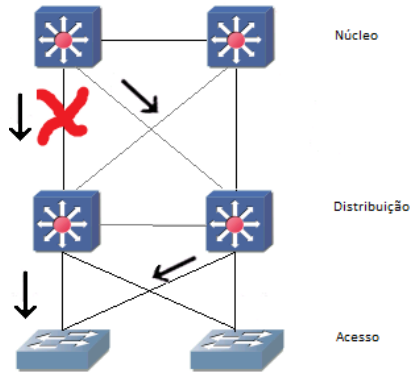

Figura 5.9: Switches de distribuição com ligação dupla ao núcleo

Aqui é visível a dupla ligação entre cada *switch* de distribuição e do núcleo em que a necessidade de convergência deixa de existir. É claro que, neste caso, é aconselhável não esquecer de:

- Ligar cada *switch* da zona de distribuição a cada um dos *switches* do núcleo da rede.
- Ligar os dois *switches* da zona de distribuição, para a sumarização de informação de encaminhamento IP para o núcleo e para um terceiro caminho redundante para o núcleo.

A utilização de um terceiro *switch* de distribuição, não só não é necessária como introduz complexidade à gestão de rede. Além de adicionar uma maior dificuldade na deteção de possíveis problemas de rede, coloca questões do tipo: determinação do *switch* raiz do STP, determinação das portas bloqueadas, etc.

Considerando tudo o que fica dito, o desenho final de uma rede com redundância apresenta-se como mostra a figura 5.10.

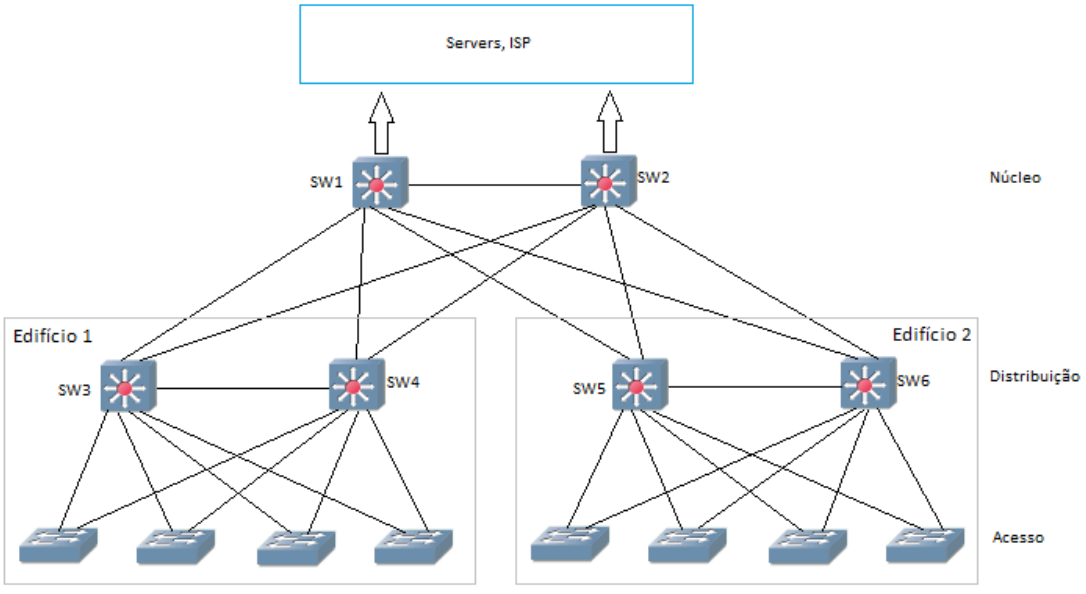

Figura 5.10: Topologia com redundância

5.1.5 Cenário 5: Utilização de subdomínios de encaminhamento

A rede, apresentada no ponto anterior, pode ser dividida em áreas OSPF, como foi descrito no capítulo 4.

O uso de áreas OSPF é recomendado quando uma empresa pretende adquirir dispositivos de rede *layer 3*, com baixo custo e com pouca memória. Esta configuração evita que a base de dados OSPF de um *router* tome proporções insustentáveis para a sua memória interna, uma vez que os *routers* de uma dada área apenas irão trocar informação relativa a redes dentro dessa mesma área, enquanto que *routers* de áreas diferentes trocam sumarizações de rotas. Também é aconselhável em redes de grande dimensão, com muitas sub-redes IP.

Nesta ordem de ideias, a rede pode ser dividida em 4 áreas:

- Área 0: constituída pelas VLANs de interligação responsáveis pelas ligações entre os dois *switches* do núcleo e entre o núcleo e a zona de distribuição.
- Área 1: constituída pelas VLANs *Local* presentes no bloco 1.
- Área 2: constituída pelas VLANs *Local* presentes no bloco 2.
- Área 3: constituída pelas VLANs *End-to-end*.

5.1.6 Cenário 6: Introdução de um bloco de acesso à Internet

Quando a rede destino de um pacote, não está definida na tabela de encaminhamento de um *router* é usada uma rota por omissão.

Para uma rede empresarial obter ligação à internet, é necessário no seu desenho, incluir uma zona que desempenhe funções de distribuição e acesso para o exterior da rede. Esta zona deve estar directamente ligada ao núcleo da rede e deve ser constituída por um par de *switches layer 3*, com dupla ligação aos *switches* do núcleo, de forma a garantir a redundância desejada. A figura 5.11 ilustra o desenho de uma rede com esta nova zona, constituída por SW7 e SW8. É nestes dois *switches* que devem ser geradas as rotas por omissão.

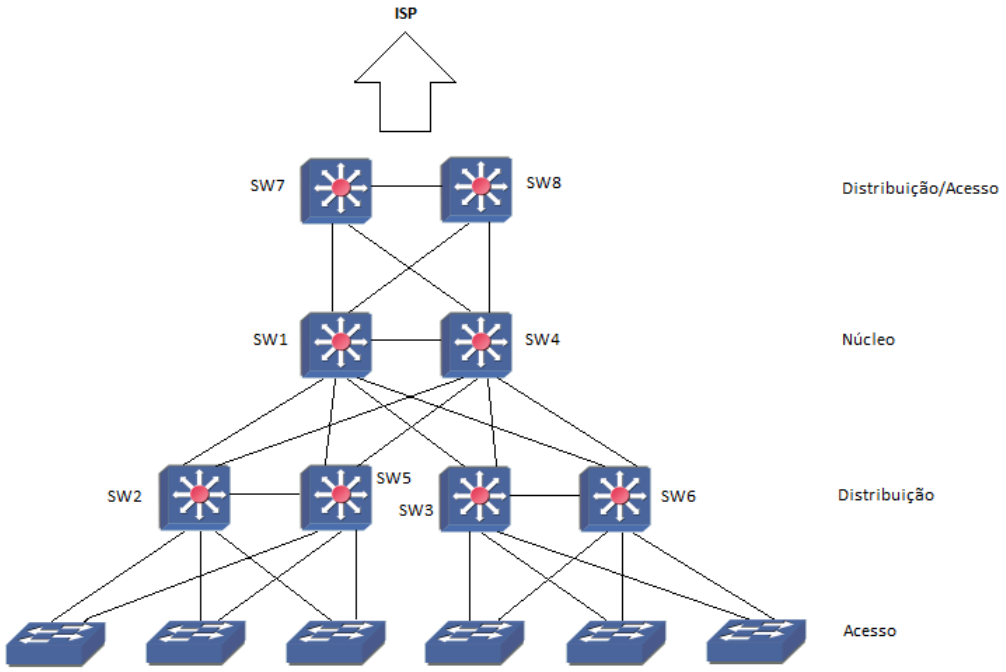

Figura 5.11: Cenário 4 com zona de acesso à internet

5.2 Configuração dos elementos de rede

5.2.1 Cenário 1

O primeiro passo é a configuração das VLANs presentes em cada *switch*, utilizando os comandos:

```
Switch# vlan database
Switch(vlan)# vlan VLAN_ID name VLAN_name
Switch(vlan)# exit
```

Posteriormente, para se atribuir uma interface de um *switch* a uma determinada VLAN utilizam-se os comandos:

```
Switch(config)# int interface_ID
```

```
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan VLAN_ID
```

No caso em estudo, nos *switches* de acesso, a configuração das portas que dão acesso a uma dada VLAN deve ser feita da seguinte forma:

```
Switch# vlan database
Switch(VLAN)# vlan 10 name administracao
Switch(VLAN)# exit
Switch# configure terminal
Switch(config)# int range f0/0 - 12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
```

Para definir uma interface no modo *trunk* é necessário configurar as interfaces das extremidades de cada ligação, utilizando os seguintes comandos:

```
Switch# configure terminal
Switch(config)# interface interface_ID
Switch(config-if)# switchport encapsilation dot1q
Switch(config-if)# switchport mode trunk
```

Para definir quais as VLANs com permissão para transportar pacotes através da ligação configurada como *trunk*, executar o comando:

```
Switch(config-if)# switchport trunk allowed vlan VLAN_ID
```

No *switch* SW2, depois de criadas as VLANs respetivas, vão ser definidas as interfaces responsáveis pelas ligações aos *switches* de acesso e a SW1, no modo *trunk*. É necessário ter em atenção que a ligação SW1-SW2 deve ser restringida a VLANs presente no respetivo bloco. A seguir está exemplificado o processo de configuração de SW2:

```
Switch# vlan database
Switch(vlan)# vlan 10 name administracao
```

```
Switch(vlan)# vlan 20 name markting
Switch(vlan)# exit
Switch# configure terminal
Switch(config-if)# interface range f0/0 - 4
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
Switch(config)# interface f0/0
Switch(config-if)# switchport trunk allowed vlan 1,10,20,1002-1005
Switch(config-if)# exit
```

Como foi referido anteriormente, é necessário atribuir manualmente a prioridade no STP para cada VLAN, no *switch* que se pretende definir como a raiz. Para o efeito, os comandos a utilizar são:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan VLAN_ID priority 0
```

Para definir SW1 como a raiz do STP, de modo a obter uma rede simétrica e com o melhor desempenho possível, atribui-se manualmente a prioridade de SW1 no STP para as VLANs existentes:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 10 priority 0
Switch(config)# spanning-tree vlan 20 priority 0
Switch(config)# spanning-tree vlan 30 priority 0
Switch(config)# spanning-tree vlan 40 priority 0
```

Depois de serem criadas todas as VLANs presentes na rede, na configuração de SW1 deve estar presente a definição de todas as interfaces, no modo *trunk*, e as responsáveis pela ligação a cada bloco devem ter permissão para encaminhar o tráfego relativo apenas às VLANs do respetivo bloco. A configuração de SW1 está exemplificada a seguir:

```
Switch# configure terminal
Switch(config-if)# interface range f0/0 - 2
Switch(config-if)# switchport encapsilation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# interface f0/1
Switch(config-if)# switchport trunk allowed vlan 1,10,20,1002-1005
Switch(config-if)# interface f0/2
Switch(config-if)# switchport trunk allowed vlan 1,30,40,1002-1005
Switch(config-if)# end
```

A configuração de SW3 é feita de forma idêntica à realizada em SW2, mas agora com as VLANs existentes no segundo bloco.

A configuração do *router* deve incluir o *default gateway* de todas as VLANs existentes na rede. Para simplificar a apresentação vamos considerar apenas 4 VLANs, às quais se atribuíram os seguintes IPs:

- VLAN 10: 192.168.10.0
- VLAN 20: 192.168.20.0
- VLAN 30: 192.168.30.0
- VLAN 40: 192.168.40.0

Deve também definir-se qual o protocolo de encaminhamento utilizado *router* - neste caso foi utilizado o protocolo OSPF. Os comandos utilizados para a configuração do protocolo OSPF são:

```
Switch# conf t
Switch(config)# router ospf 1
Switch(config)# network network_IP_ADD mask area area_ID
Switch(config)# exit
```

A configuração do *router* pode ser feita da seguinte forma:

```
Router# configure terminal
Router(config)# interface f0/0.10
Router(config-subif)# encapsulation dot1Q 10
```

```
Router(config-subif)# ip add 192.168.10.1 255.255.255.0
Router(config)# interface f0/0.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip add 192.168.20.1 255.255.255.0
Router(config)# interface f0/0.30
Router(config-subif)# encapsulation dot1Q 30
Router(config-subif)# ip add 192.168.30.1 255.255.255.0
Router(config)# interface f0/0.40
Router(config-subif)# encapsulation dot1Q 40
Router(config-subif)# ip add 192.168.40.1 255.255.255.0
Router(config-subif)# exit
Router(config)# router ospf 1
Router(config-router)# network 192.168.0.0 0.0.255.255 area 0
```

OS PCs de cada VLAN devem ser configurados com um endereço IP dentro do range da VLAN pretendida e com o *default gateway* correspondente, definido na interface virtual de SW1. Como exemplo, o PC1 da VLAN 10 pode ser configurado da seguinte forma:

- Endereço IP: 192.168.10.10
- Default gateway: 192.168.10.1

Utilizando o comando #show mac-address-table, pode-se consultar a tabela de encaminhamento de um *switch*. A tabela de encaminhamento de SW2 está representada na figura 5.12. Podemos constatar, que cada VLAN *Local* tem duas portas atribuídas, uma para a zona de acesso e outra para o núcleo da rede.

Destination Address	Address Type	VLAN	Destination Port
cc17.19e8.0000	Self	1	Vlan1
0050.7966.6800	Dynamic	10	FastEthernet0/0
cc1a.1c94.0000	Dynamic	10	FastEthernet0/2
0050.7966.6801	Dynamic	20	FastEthernet0/1
cc1a.1c94.0000	Dynamic	20	FastEthernet0/2

Figura 5.12: Mac-address-table de SW2

Implementação de VLAN End-to-end

Para implementar um modelo de rede que inclua VLANs dos tipos *Local* e *End-to-end*, é necessário que todas as ligações permitam o tráfego relativo a VLANs *End-to-end*. Uma vez que todas as ligações foram definidas no modo *trunk*, é necessário apenas acrescentar o identificador das VLANs do tipo *End-to-end* no comando *allowed*, nas ligações com restrição de tráfego. A título de exemplo e considerando que a VLAN 50 é do tipo *End-to-end*, a configuração da interface de SW1 responsável pela ligação ao bloco 1 deve ser feita da seguinte forma:

```
Switch(config-if)# switchport trunk allowed VLAN 1,10,20,50,1002-1005
```

Deve ser escolhido como a raiz do STP para as VLANs End-t-end o *switch* SW1, assim como foi para as VLANs locais.

Na configuração do router deve-se acrescentar o *default gateway* de todas as VLANs *End-to-end*.

5.2.2 Cenário 2

A configuração dos *switches* SW2 e SW3 é feita como no cenário anterior. Diferente é a configuração do *switch* do núcleo SW1, que passa a ser um *switch layer 3*, em que é necessário incluir a configuração das interfaces virtuais para as VLANs existentes na rede. As ligações devem ser configuradas da mesma forma que no caso anterior.

A configuração de uma interface virtual é feita recorrendo aos comandos:

```
Switch(config)# interface vlan VLAN_ID
Switch(config-if)# ip add IP_address mask
Switch(config-if)# no autostate
Switch(config-if)# exit
```

Como exemplo de utilização do novo comando apresentado, vamos ver a aplicação prática do mesmo na configuração de SW1:

```
Switch# configure terminal
Switch(config)# interface vlan 10
Switch(config-if)# ip add 192.168.10.1 255.255.255.0
Switch(config-if)# no autostate
Switch(config)# interface VLAN 20
Switch(config-if)# ip add 192.168.20.1 255.255.255.0
Switch(config-if)# no autostate
Switch(config)# interface vlan 30
Switch(config-if)# ip add 192.168.30.1 255.255.255.0
Switch(config-if)# no autostate
Switch(config-if)# exit
Switch(config)# router ospf 1
Switch(config)# network 192.168.0.0 0.0.255.255 area 0
Switch(config)# exit
```

Como já foi dito, no que respeita à configuração de VLANs *End-to-end*, os procedimentos são semelhantes aos do caso anterior.

5.2.3 Cenário 3

As ligações entre SW1, SW2 e SW3 são feitas por encaminhamento IP ponto-a-ponto. Para isso, deve-se atribuir uma sub-rede IP a cada LAN que faz a ligação aos diferentes

blocos. Os IPs atribuídos foram: 192.168.100.0 e 192.168.200.0, aos blocos 1 e 2, respetivamente.

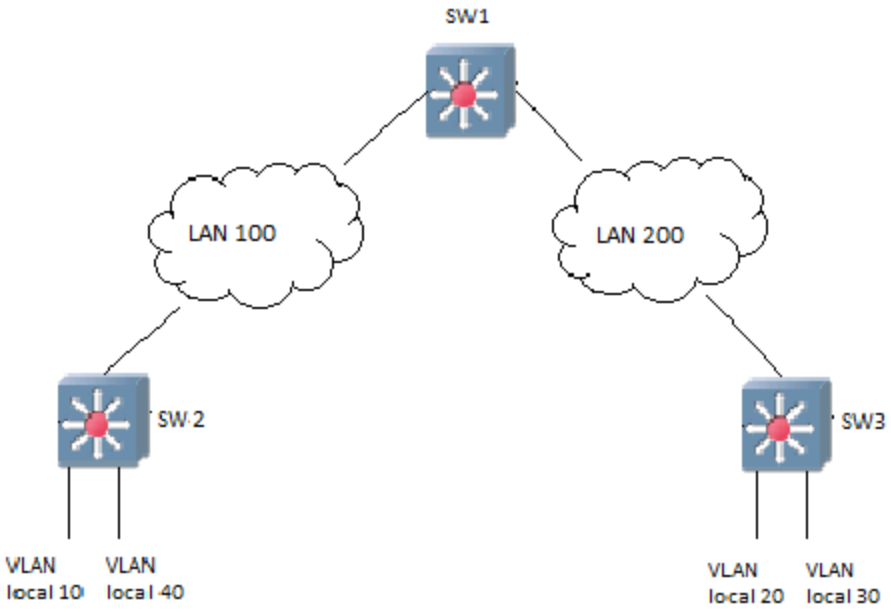

Figura 5.13: LANs de ligação

É necessária a configuração das interfaces dos *switches layer 3* referidos anteriormente, com IPs pertencentes ao bloco correspondente.

SW1: interface f0/0: 192.168.100.1 e interface f0/1: 192.168.200.1

SW2: interface f0/0: 192.168.100.2

SW3: interface f0/0: 192.168.200.2

A configuração das interfaces virtuais de cada VLAN é realizada nos *switches* de distribuição. No STP, os *switches* de distribuição de cada bloco devem ser definidos com a prioridade mais baixa para as VLANs presentes nesse bloco; deste modo eles são escolhidos para raiz da árvore.

A configuração de SW2, considerando a distribuição de VLANs representada na figura 5.13, é feita da seguinte forma:

```
Switch# configure terminal
Switch(config)# interface vlan 10
```

```
Switch(config-if)# ip add 192.168.10.1 255.255.255.0
Switch(config-if)# no autostate
Switch(config)# interface vlan 40
Switch(config-if)# ip add 192.168.40.1 255.255.255.0
Switch(config-if)# no autostate
Switch(config)# interface f0/0
Switch(config-if)# ip add 192.168.100.2 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# spanning-tree vlan 10 priority 0
Switch(config)# spanning-tree vlan 40 priority 0
Switch(config)# router ospf 1
Switch(config)# network 192.168.0.0 0.0.255.255 area 0
Switch(config)# exit
```

A configuração de SW3 é feita de forma idêntica a SW2. Quanto a SW1, é necessário configurar o IP das suas interfaces e o protocolo de encaminhamento IP utilizado.

Na tabela de encaminhamento de SW1, estão definidos os caminhos para as VLANs da rede, como se pode ver na figura 5.14.

```
O    192.168.30.0/24 [110/11] via 192.168.200.2, 00:00:01, FastEthernet0/1
O    192.168.10.0/24 [110/11] via 192.168.100.2, 00:00:01, FastEthernet0/0
O    192.168.40.0/24 [110/11] via 192.168.100.2, 00:00:01, FastEthernet0/0
C    192.168.200.0/24 is directly connected, FastEthernet0/1
O    192.168.20.0/24 [110/11] via 192.168.200.2, 00:00:01, FastEthernet0/1
C    192.168.100.0/24 is directly connected, FastEthernet0/0
```

Figura 5.14: Tabela de encaminhamento de SW1 do cenário 3 sem VLAN End-to-end

Implementação de VLANs End-to-end

Quando o modelo *End-to-end* é utilizado em simultâneo com o modelo *Local*, deve-se utilizar uma VLAN de interligação entre SW1, SW2 e SW3. A VLAN de interligação deve ser inicializada nos três *switches*. Nos *switches* devem ser configuradas as interfaces virtuais relativas á VLAN de interligação. As interfaces de SW1, SW2 e SW3, responsáveis pela conexão entre os mesmos, devem ser configuradas no modo trunk e permitir apenas o tráfego proveniente da VLAN de interligação e das VLANs *End-to-end*, para além do tráfego das VLAN 1, 1002-1005.

Consideremos:

- A distribuição de VLANs *Local*, tal como indica a figura 5.5.
- A utilização da VLAN 100 como VLAN de interligação.
- A utilização da VLAN 50 como VLAN *End-to-end*.

As interfaces virtuais de cada VLAN nos *switches* de distribuição e do núcleo serão definidas com os seguintes endereços IP:

SW1: VLAN 100: 192.168.100.1
VLAN 50: 192.168.50.1 (default gateway da VLAN 50)
SW2: VLAN 10: 192.168.10.2 (default gateway da VLAN 10)
VLAN 40: 192.168.40.2 (default gateway da VLAN 40)
VLAN 100:192.168.100.2
SW3: VLAN 20: 192.168.20.3 (default gateway da VLAN 20)
VLAN 40: 192.168.30.3 (default gateway da VLAN 30)
VLAN 100:192.168.100

A configuração de SW1, incluindo a definição das interfaces passivas necessárias, é feita da seguinte forma:

```
Switch# vlan database
Switch(vlan)# vlan 100 name interligacao
Switch(vlan)# vlan 50
Switch(vlan)# exit
```

```
Switch# configure terminal
Switch(config)# int range f0/0 – 1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed VLAN 1,50,100,1002-1005
Switch(config-if)# exit
Switch(config)# int vlan 100
Switch(config-if)# ip add 192.168.100.1 255.255.255.0
Switch(config-if)# no autostate
Switch(config)# interface vlan 50
Switch(config-if)# ip add 192.168.50.1 255.255.255.0
Switch(config-if)# no autostate
Switch(config-if)# exit
Switch(config)# router ospf 1
Switch(config-router)# network 192.168.0.0 0.0.255.255 area 0
Switch(config-router)# passive-interface vlan 50
```

A configuração da VLAN de interligação em SW2 e SW3 é realizada de forma semelhante a SW1. Agora tráfego pertencente a qualquer VLAN *Local* vai ser transportado nestas ligações com o *tag* da VLAN de interligação.

As ligações entre os *switches* de acesso e os de distribuição devem ser também configuradas como *trunk* e com limitação de tráfego, como foi dito no primeiro caso.

Para SW1 ser definido como a raiz do STP da VLAN 50, como foi explicado anteriormente, executou-se o comando:

```
Switch(config)# spanning-tree VLAN 50 priority 0
```

As figuras que seguem, mostram as tabelas de encaminhamento dos três *switches layer 3*.

```
O    192.168.30.0/24 [110/2] via 192.168.100.3, 00:00:07, Vlan100
O    192.168.10.0/24 [110/2] via 192.168.100.2, 00:00:07, Vlan100
O    192.168.40.0/24 [110/2] via 192.168.100.2, 00:00:07, Vlan100
O    192.168.20.0/24 [110/2] via 192.168.100.3, 00:00:07, Vlan100
C    192.168.50.0/24 is directly connected, Vlan50
C    192.168.100.0/24 is directly connected, Vlan100
```

Figura 5.15: Tabela de encaminhamento de SW1 do cenário 3

```
O    192.168.30.0/24 [110/2] via 192.168.100.3, 00:33:01, Vlan100
C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.40.0/24 is directly connected, Vlan40
O    192.168.20.0/24 [110/2] via 192.168.100.3, 00:33:01, Vlan100
O    192.168.50.0/24 [110/2] via 192.168.100.1, 00:33:01, Vlan100
C    192.168.100.0/24 is directly connected, Vlan100
```

Figura 5.16: Tabela de encaminhamento de SW2 do cenário 3

```
C    192.168.30.0/24 is directly connected, Vlan30
O    192.168.10.0/24 [110/2] via 192.168.100.2, 00:36:24, Vlan100
O    192.168.40.0/24 [110/2] via 192.168.100.2, 00:36:24, Vlan100
C    192.168.20.0/24 is directly connected, Vlan20
O    192.168.50.0/24 [110/2] via 192.168.100.1, 00:36:24, Vlan100
C    192.168.100.0/24 is directly connected, Vlan100
```

Figura 5.17: Tabela de encaminhamento de SW3 do cenário 3

Analisando a tabela de encaminhamento de SW1 podemos constatar que está ligado:

- Diretamente á VLAN 100.
- Às VLANS 10 e 40, via interface virtual da VLAN 100 de SW2.
- Às VLANS 20 e 30 via interface virtual da VLAN 100 de SW3.
- Diretamente à VLAN 50, uma vez que este *switch* está definido como o *default gateway* desta VLAN.

5.2.4 Cenário 4: Redundância

Para introduzir redundância na estrutura de uma rede, é aconselhável a introdução de *switches* em paralelo na zona de distribuição e do núcleo, como já foi referido. Nesta fase,

vai ser apresentada uma simulação de rede, onde estão presentes VLANs *Local*, VLANS *End-to-end* e VLANs de interligação.

As VLANs criadas na rede foram:

- VLANs *Local*: 10,20,30,40
- VLAN *End-to-end*: 50
- VLANs de interligação: 100, 200 e 250

Na figura 5.18 está representado o desenho da rede simulada, bem como a distribuição de VLANs pela mesma.

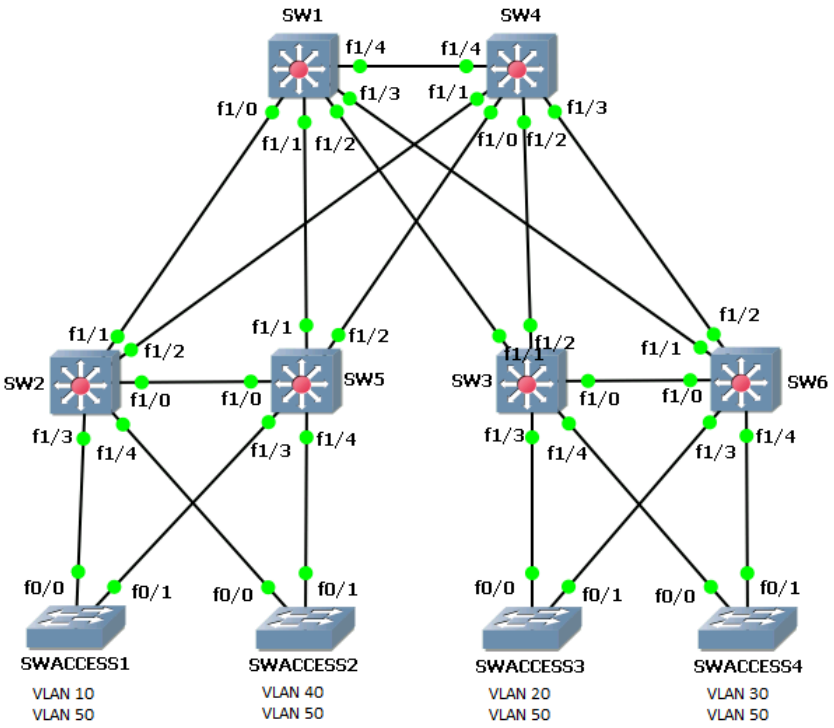

Figura 5.18: Cenário 3 com redundância

Neste modelo, utilizam-se VLANs de interligação, para assegurar o transporte multicamada entre a zona de distribuição e o núcleo. A ligação entre os dois *switches* que formam o núcleo da rede, é feita por uma terceira VLAN de interligação para garantir um caminho redundante adicional para as VLANs *End-to-end*. No entanto, esta ligação pode ser definida como uma ligação de encaminhamento IP quando não se pretender capacitar

a mesma para o transporte de tráfego de camada 2 e camada 3. A figura 5.19 ilustra a distribuição das VLANs de interligação.

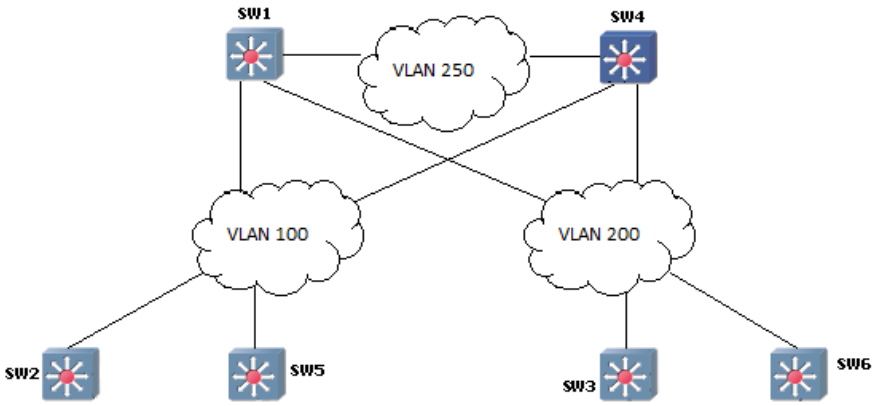

Figura 5.19: VLANs de interligação do cenário 3 com redundância

Configurações necessárias em cada switch

Configuração de SWACCESS1

- Criação de VLANs: 10(*Local*) e 50(*End-to-end*):

```
SWACCESS1# vlan database
SWACCESS1(vlan)# vlan 10
SWACCESS1(vlan)# vlan 50
```

- As interfaces responsáveis pelas ligações aos *switches* de distribuição, devem ser configuradas no modo *trunk*. Esta ligação poderia ser definida de forma a transportar pacotes pertencentes apenas ás VLANs 10 e 50, evitando que tráfego de outras VLANs que chegam ao *switch* de distribuição atinjam as interfaces do *switch* de acesso. Contudo esta restrição poderia causar uma maior complexidade, no caso de se desejar adicionar uma nova VLAN a este *switch* de acesso.

  Comandos a utilizar:

```
SWACCESS1(config)# interface range f0/0 - 1
SWACCESS1(config-if)# sw mode tr
```

- As portas para cada ponto de acesso devem ser configuradas no modo *access* para a VLAN pretendida, da seguinte forma:

```
SWACCESS1(config)# interface range f0/2 – 12
SWACCESS1(config-if)# sw mode acc
SWACCESS1(config-if)#sw acc vlan 10
```

A configuração dos restantes *switches* de acesso é realizada de forma idêntica.

Configuração de SW2

- Criação de VLANs: 10, 40 (*Local*), 100 (interligação) e 50(*End-to-end*).
- A ligação SW2-SW5 e as ligações ao núcleo devem ser configuradas no modo *trunk*, com permissão para as VLANs 50 e 100, deste modo:

```
SW2(config)# interface range f1/0 -2
SW2(config-if)# sw mode tr
SW2(config-if)# sw tr allowed vlan 1,50,100,1002-1005
```

- Configuração de interfaces virtuais para as VLAN 10 (*default gateway* da VLAN 10), 40 (*default gateway* da VLAN 40) e 100, assim:

```
SW2(config)# int vlan 10
SW2(config-if)# ip add 192.168.10.2 255.255.255.0
SW2(config-if)# no autostate
SW2(config)# int vlan 40
SW2(config-if)# ip add 192.168.40.2 255.255.255.0
SW2(config-if)# no autostate
SW2(config)# int vlan 100
SW2(config-if)# ip add 192.168.100.2 255.255.255.0
SW2(config-if)# no autostate
```

- Configuração do protocolo OSPF, com definição das interfaces virtuais das VLANs 10 e 40 como interfaces passivas, como segue:

```
SW2(config)# router ospf 1
```

```
SW2(config-router)# network 192.168.0.0 0.0.255.255 area 0
SW2(config-router)# passive-interface vlan 10
SW2(config-router)# passive-interface vlan 40
```

- As interfaces atribuídas para as ligações a SWACCESS1 e SWACCESS2 devem ser definidas no modo *trunk* e configuradas como interfaces passivas no protocolo OSPF, desta forma:

```
SWACCESS1(config)# interface range f1/3 - 4
SWACCESS1(config-if)# sw mode tr
SWACCESS1(config)# router ospf 1
SWACCESS1(config-router)# passive-interface f1/3
SWACCESS1(config-router)# passive-interface f1/4
```

- Definição de SW2 OU SW5 como a raiz do STP para as VLANs 10 e 40, atribuindo a prioridade, no STP, mais baixa a um deles. Definição da segunda prioridade mais baixa ao outro *switch*, para este o substituir em caso de falha do primeiro. Comando a utilizar:

```
SW2(config)# spanning-tree vlan 10 priority 0
```

A configuração de SW5 é feita de forma semelhante à de SW2. A configuração dos *switches* SW3 e SW6 são feitos de forma semelhante, mas agora com as VLANs 20, 30 e 200, em vez de 10, 40 e 100 respetivamente.

A configuração de SW1

- Criação das VLANs 100, 200, 250(interligaçãol) e 50(*End-to-end*);
- As interfaces que garantem as ligações a SW2 e SW5 devem ser configuradas no modo *trunk*, com permissão para as VLANs 100 e 50, da seguinte forma:

```
SW1(config)# interface  range f1/0 - 1
SW1(config-if)#  sw mode tr
SW1(config-if)# sw tr allowed vlan 1,50,100,1002-1005
```

- As interfaces das ligações a SW3 e SW6 devem ser configuradas no modo *trunk*, com permissão para as VLANs 200 e 50, deste modo:

```
SW1(config)# interface range f1/2 - 3
SW1(config-if)#  sw mode tr
SW1(config-if)# sw tr allowed vlan 1,50,200,1002-1005
```

- Definição das interfaces virtuais das VLANs 50 (*default gateway* da VLAN 50), 100 e 200 e 250, como segue:

```
SW1(config)# int vlan 50
SW1(config-if)# ip add 192.168.50.1 255.255.255.0
SW1(config-if)# no autostate
SW1(config)# int vlan 100
SW1(config-if)# ip add 192.168.100.1 255.255.255.0
SW1(config-if)# no autostate
SW1(config)# int vlan 200
SW1(config-if)# ip add 192.168.200.1 255.255.255.0
SW1(config-if)# no autostate
SW1(config)# int vlan 250
SW1(config-if)# ip add 192.168.250.1 255.255.255.0
SW1(config-if)# no autostate
```

- Configuração do protocolo OSPF, com a definição da interface virtual da VLAN 50 como interface passiva, do seguinte modo:

```
SW1(config)# router ospf 1
SW1(config-router)# network 192.168.0.0 0.0.255.255 area 0
SW1(config-router)# passive-interface vlan 50
```

- Ligação entre os dois *switches* do núcleo definida como *trunk*, com permissão para as VLANs 50 e 250, da seguinte forma:

```
SW1(config)# interface f1/5
SW1(config-if)#  sw mode tr
SW1(config-if)# sw tr allowed VLAN 1,50,250,1002-1005
```

- Definição de SW1 ou SW4 como a raiz do STP para a VLAN 50 (*End-to-end*), atribuindo a prioridade, no STP, mais baixa a um e a segunda prioridade mais baixa ao outro, para em caso de falha do primeiro o outro o substituir, usando o comando:

```
SW1(config)# spanning-tree vlan 50 priority 0
```

A configuração do *switch* SW4 realiza-se de forma semelhante á apresentada para SW1.

Após a configuração de todos os elementos de rede, para verificar as rotas disponíveis nos vários elementos de rede, foram consultadas as tabelas de encaminhamento dos *switches* SW1, SW2 e SW3, utilizando o comando:

```
SW# show ip route
```

```
O    192.168.30.0/24 [110/2] via 192.168.200.6, 00:00:22, Vlan200
                     [110/2] via 192.168.200.3, 00:00:22, Vlan200
O    192.168.10.0/24 [110/2] via 192.168.100.5, 00:00:22, Vlan100
                     [110/2] via 192.168.100.2, 00:00:22, Vlan100
O    192.168.40.0/24 [110/2] via 192.168.100.5, 00:00:22, Vlan100
                     [110/2] via 192.168.100.2, 00:00:22, Vlan100
C    192.168.200.0/24 is directly connected, Vlan200
C    192.168.250.0/24 is directly connected, Vlan250
O    192.168.20.0/24 [110/2] via 192.168.200.6, 00:00:24, Vlan200
                     [110/2] via 192.168.200.3, 00:00:24, Vlan200
C    192.168.100.0/24 is directly connected, Vlan100
```

Figura 5.20: Tabela de encaminhamento SW1 do cenário 3 com redundância

```
O    192.168.30.0/24 [110/3] via 192.168.100.4, 00:02:23, Vlan100
                     [110/3] via 192.168.100.1, 00:02:23, Vlan100
C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.40.0/24 is directly connected, Vlan40
O    192.168.200.0/24 [110/2] via 192.168.100.4, 00:02:23, Vlan100
                      [110/2] via 192.168.100.1, 00:02:23, Vlan100
O    192.168.250.0/24 [110/2] via 192.168.100.4, 00:02:23, Vlan100
                      [110/2] via 192.168.100.1, 00:02:23, Vlan100
O    192.168.20.0/24 [110/3] via 192.168.100.4, 00:02:24, Vlan100
                     [110/3] via 192.168.100.1, 00:02:24, Vlan100
C    192.168.100.0/24 is directly connected, Vlan100
```

Figura 5.21: Tabela de encaminhamento de SW2 do cenário 3 com redundância

```
C    192.168.30.0/24 is directly connected, Vlan30
O    192.168.10.0/24 [110/3] via 192.168.200.4, 00:03:59, Vlan200
                     [110/3] via 192.168.200.1, 00:03:59, Vlan200
O    192.168.40.0/24 [110/3] via 192.168.200.4, 00:03:59, Vlan200
                     [110/3] via 192.168.200.1, 00:03:59, Vlan200
C    192.168.200.0/24 is directly connected, Vlan200
O    192.168.250.0/24 [110/2] via 192.168.200.4, 00:03:59, Vlan200
                      [110/2] via 192.168.200.1, 00:03:59, Vlan200
C    192.168.20.0/24 is directly connected, Vlan20
O    192.168.100.0/24 [110/2] via 192.168.200.4, 00:04:00, Vlan200
                      [110/2] via 192.168.200.1, 00:04:00, Vlan200
```

Figura 5.22: Tabela de encaminhamento de SW3 do cenário 3 com redundância

Através da tabela de encaminhamento de SW1, pode verificar-se que:

- Está diretamente ligado ás VLANs 100, 200 e 250, para poder utilizá-las como meio de transporte para pacotes pertencentes a VLANs *Local* distribuídas pela zona de acesso.
- Estão representados os dois caminhos possíveis para cada VLAN *Local* através dos dois *switches* da zona de distribuição de cada bloco e, no caso da VLAN 10, pode-se constatar que o tráfego pode ser encaminhado para SW2 ou SW5.

Analisando a tabela de encaminhamento de SW2, verifica-se que:

- Está diretamente ligado às VLANs 10 e 40, o que seria de esperar uma vez que é o seu *default gateway*.
- Este *switch* tem 2 caminhos possíveis para comunicar com VLANs *Local* doutro bloco, utilizando a VLAN 100 conjugada com cada um dos dois *switches* do núcleo.

5.2.5 Cenário 5: Utilização de subdomínios de encaminhamento

A rede, simulada no ponto anterior, pode ser dividida em áreas OSPF. Nesta ordem de ideias, dividiu-se a mesma em 4 áreas:

- Área 0: constituída pelas VLANs de interligação responsáveis pelas ligações entre os dois *switches* do núcleo e entre o núcleo e a zona de distribuição.

- Área 1: constituída pelas VLANs *Local* presentes no bloco 1.
- Área 2: constituída pelas VLANs *Local* presentes no bloco 2.
- Área 3: constituída pelas VLANs *End-to-end*.

Configuração dos elementos de rede.

Alterações a introduzir em SW1/SW4:

```
SW1(config)# router ospf 1
SW1(config-router)# network 192.168.100.0 0.0.0.255 area 0
SW1(config-router)# network 192.168.200.0 0.0.0.255 area 0
SW1(config-router)# network 192.168.250.0 0.0.0.255 area 0
SW1(config-router)# network 192.168.50.0 0.0.0.255 area 3
```

Alterações a introduzir em SW2/SW5:

```
SW2(config)# router ospf 1
SW2(config-router)# network 192.168.100.0 0.0.0.255 area 0
SW2(config-router)# network 192.168.10.0 0.0.0.255 area 1
SW2(config-router)# network 192.168.40.0 0.0.0.255 area 1
```

Alterações a introduzir em SW3/SW6:

```
SW3(config)# router ospf 1
SW3(config-router)# network 192.168.200.0 0.0.0.255 area 0
SW3(config-router)# network 192.168.20.0 0.0.0.255 area 2
SW3(config-router)# network 192.168.30.0 0.0.0.255 area 2
```

As figuras que se seguem ilustram as tabelas de encaminhamento de SW1, SW2 e SW3. A simples observação permite verificar que o caminho relativo ao tráfego entre segmentos de áreas diferentes está marcado com o símbolo IA, que significa *Inter Area*. É possível constatar, também, que a área 0 está ligada a todas as outras áreas, como era desejável.

```
O    192.168.30.0/24 [110/2] via 192.168.200.6, 00:02:22, Vlan200
                     [110/2] via 192.168.200.3, 00:02:22, Vlan200
O    192.168.10.0/24 [110/2] via 192.168.100.5, 00:02:22, Vlan100
                     [110/2] via 192.168.100.2, 00:02:22, Vlan100
O    192.168.40.0/24 [110/2] via 192.168.100.5, 00:02:22, Vlan100
                     [110/2] via 192.168.100.2, 00:02:22, Vlan100
C    192.168.200.0/24 is directly connected, Vlan200
C    192.168.250.0/24 is directly connected, Vlan250
O    192.168.20.0/24 [110/2] via 192.168.200.6, 00:02:24, Vlan200
                     [110/2] via 192.168.200.3, 00:02:24, Vlan200
C    192.168.50.0/24 is directly connected, Vlan50
C    192.168.100.0/24 is directly connected, Vlan100
```

Figura 5.23: Tabela de encaminhamento SW1 com áreas OSPF

```
O IA 192.168.30.0/24 [110/3] via 192.168.100.4, 00:04:57, Vlan100
                     [110/3] via 192.168.100.1, 00:04:57, Vlan100
C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.40.0/24 is directly connected, Vlan40
O IA 192.168.200.0/24 [110/2] via 192.168.100.4, 00:04:57, Vlan100
                      [110/2] via 192.168.100.1, 00:04:57, Vlan100
O IA 192.168.250.0/24 [110/2] via 192.168.100.4, 00:04:57, Vlan100
                      [110/2] via 192.168.100.1, 00:04:57, Vlan100
O IA 192.168.20.0/24 [110/3] via 192.168.100.4, 00:04:58, Vlan100
                     [110/3] via 192.168.100.1, 00:04:58, Vlan100
O IA 192.168.50.0/24 [110/2] via 192.168.100.4, 00:01:56, Vlan100
                     [110/2] via 192.168.100.1, 00:01:56, Vlan100
C    192.168.100.0/24 is directly connected, Vlan100
```

Figura 5.24: Tabela encaminhamento SW2 com áreas OSPF

```
C    192.168.30.0/24 is directly connected, Vlan30
O IA 192.168.10.0/24 [110/3] via 192.168.200.4, 00:06:16, Vlan200
                     [110/3] via 192.168.200.1, 00:06:16, Vlan200
O IA 192.168.40.0/24 [110/3] via 192.168.200.4, 00:06:16, Vlan200
                     [110/3] via 192.168.200.1, 00:06:16, Vlan200
C    192.168.200.0/24 is directly connected, Vlan200
O IA 192.168.250.0/24 [110/2] via 192.168.200.4, 00:06:26, Vlan200
                      [110/2] via 192.168.200.1, 00:06:26, Vlan200
C    192.168.20.0/24 is directly connected, Vlan20
O IA 192.168.50.0/24 [110/2] via 192.168.200.4, 00:03:15, Vlan200
                     [110/2] via 192.168.200.1, 00:03:15, Vlan200
O IA 192.168.100.0/24 [110/2] via 192.168.200.4, 00:06:27, Vlan200
                      [110/2] via 192.168.200.1, 00:06:27, Vlan200
```

Figura 5.25: Tabela encaminhamento SW3 com áreas OSPF

5.2.6 Cenário 6: Introdução de um bloco de acesso à Internet

As rotas por omissão devem ser geradas em SW7 e SW8, uma vez que estes serão responsáveis pelo acesso ao exterior da rede. Para exemplificar esta configuração, foram criadas duas rotas por omissão com custos diferentes, 20 e 10, em SW7 e SW8, respectivamente. Para isso, depois da configuração de todas as ligações de camada 3 com os endereços IPs relativos a todas as interfaces e associadas todas as sub-redes responsáveis por estas ligações à área 0, utilizou-se o comando:

```
Default-information originate
```

No caso de SW8, a configuração da rota por omissão é feita da seguinte forma:

```
#SW8(config): router ospf 1
#SW8(config-router): Default-information originate always metric 10
```

A configuração a realizar em SW7 é idêntica à efectuada para SW8, alterando apenas o custo associado à rota por omissão, que deve tomar agora o valor 20.

Na tabela de encaminhamento de SW1, apresentada na figura 5.26, pode verificar-se a presença de uma nova rota, relativa ao endereço 0.0.0.0 através de SW8 (192.168.1.8 é o endereço de uma das interfaces de SW8).

```
C    192.168.100.0/24 is directly connected, Vlan100
O    192.168.3.0/24 [110/2] via 192.168.2.9, 00:00:10, FastEthernet1/6
                    [110/2] via 192.168.1.8, 00:00:10, FastEthernet1/5
O*E2 0.0.0.0/0 [110/10] via 192.168.1.8, 00:00:10, FastEthernet1/5
```

Figura 5.26: Rota por omissão na tabela de encaminhamento de SW1

Caso o custo associado às rotas por omissão geradas em SW7 e SW8 fosse igual, na tabela de encaminhamento de SW1 poderíamos observar duas rotas para o endereço 0.0.0.0.

6. Conclusões

A presente dissertação propôs-se a criação de um manual que estabeleça os princípios básicos que permitam a conceção de desenhos de rede empresarias, de forma a balanceá-la em termos de disponibilidade, segurança e flexibilidade, tendo em conta os requisitos próprios de cada empresa.

Com esse intuito, foram definidas estratégias e procedimentos para a implementação de redes multicamada. As estratégias definidas visaram a prossecução dos seguintes objetivos: implementação de grupos lógicos dentro da rede, o encaminhamento entre os mesmos e a garantia de alta disponibilidade e redundância da rede.

O recurso a um *software* de simulação de redes permitiu exemplificar a configuração e a análise dos vários modelos que podem ser aplicados na conceção de redes empresarias.

Posto isto, foram simuladas 4 cenários de rede:

- Cenário 1: Zonas de distribuição e do núcleo constituídas por *switches layer 2*.
- Cenário 2: Zonas de distribuição constituída por *switch layer 2* e do núcleo por *switch layer 3*.
- Cenário 3: Zonas de distribuição e do núcleo constituídas por *switches layer 3*.
- Cenário 4: Introdução de redundância na estrutura de rede do cenário 3.
- Cenário 5: Divisão do Cenário 4 em áreas OSPF.
- Cenário 6: Cenário 5 com zona de acesso ao exterior da rede, configurado com rotas por omissão.

Dentro de cada um dos três primeiros cenários foram feitas, primariamente, abordagens de segmentação de rede *Local* e, posteriormente, adicionado um ambiente *End-to-end*.

O primeiro cenário é de difícil implementação em redes de grande dimensão, tendo fraco controlo de qualidade de serviços bem como segurança limitada. É o cenário mais económico e mais fácil de implementar.

O segundo cenário é indicado para redes que necessitam, não só de grande flexibilidade mas também grande interligação entre os vários segmentos de rede. É o cenário que apresenta a melhor relação custo-benefício.

O terceiro cenário tem como grande vantagem a maior segmentação de rede disponível, com uma maior limitação do tráfego de *broadcast* de cada segmento, prevenindo possíveis congestionamentos. Tem ainda a vantagem de permitir maior capacidade de comunicação entre segmentos de rede, do mesmo espaço físico (bloco). Relativamente aos anteriores, é o cenário mais dispendioso e com implementação mais complexa.

Em qualquer dos três cenários anteriores, a utilização de uma segmentação de rede *Local* é indicada para grupos lógicos localizados no mesmo espaço físico (bloco), com os mesmos requisitos de rede e a mesma função dentro da empresa. O modelo *End-to-end* é aplicado normalmente para estabelecer ligações *wireless* e serviços globais, como por exemplo, grupos de impressoras.

No quarto cenário, a introdução de redundância na topologia de rede proporciona caminhos alternativos entre os elementos da rede, adicionando balanceamento do tráfego. Previne também, a quebra de comunicação entre os nós da rede em caso de falha num dispositivo ou numa ligação. É o cenário que implica um desenho de rede mais caro. A chave é encontrar o equilíbrio entre a construção de uma rede com demasiada redundância, muito complexa, cara de construir e de manter e outra mais barata, mais simples, com redundância limitada e comprometendo a alta disponibilidade.

Resumindo: A opção pela adoção de um dos modelos, estabelecidos nos cenários anteriores, deve ser feita depois de avaliada a relação custo-benefício associada à sua implementação e manutenção.

Referências

[1] R. Froom, B. Sivasubramanian and E. Frahim, Implementing Cisco IP Switched Networks (SWITCH) Foudation Guide, Indianapolis: Cisco Press, 2010.

[2] D. Teare, Implementing Cisco IP Rpoting (Route) Foundation Learning Guide, Indianapolis: Cisco Press, 2010.

[3] Cisco "Gigabit Campus Network Design—PrincIPles and Architecture", Indianapolis: Cisco Press,

[4] High Availability Campus Network Design--Routed Access Layer using EIGRP or OSPF (2013, Setembro) [Online]. Available: http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/routed-ex.html

[5] Mike Fuszner (2013, Junho) GNS3 Graphical Network Simulator (version 1.0) [Online] Available: http://www.av.it.pt/salvador/LR/GNS3-0.5-tutorial.pdf

[6] J. Tiso, Foudation Learning guide: Designing Cisco Network Service Architectures (ARCH) Ed. 3. Indianopolis: Cisco Press, 2010

[7] C. Hedrick. (2013, Set.). Routing Information Protocol. Network Working Group [Online]. Available: http://tools.ietf.org/html/rfc1058

[8] J. Moy. (2013, Set.). OSPF Version 2, Network Working Group [Online]. Available: http://tools.ietf.org/html/rfc1247

[9] R.Callon. (2013, Set.). Use of OSI IS-IS for routing in TCP/IP and Dual Environments. Network Working Group [Online]. Available: http://www.ietf.org/rfc/rfc1195.txt

[10] D. Savage, D. Slice, J. Ng, S. Moore, R. White. (2013, Set.). Enhanced Interior Gateway Routing Protocol draft-savage-eigrp-00.txt. Internet Engineering Task Force [Online]. Available: http://tools.ietf.org/html/draft-savage-eigrp-00

[11] E. Decker, P. Langille, A. Rijsinghani, K. McCloghrie. (2013, Set.). Definitions of Managed Objects for Bridges. Network Working Group [Online]. Available: http://www.ietf.org/rfc/rfc1493.txt

[12] Institute of Electrical and Electronics Engineers, “Virtual Bridged Local Area Networks”, IEEE Standard 802.1Q, 2005 Edition, May 2006.

Bibliografia

- R. Froom, B. Sivasubramanian and E. Frahim, Implementing Cisco IP Switched Networks (SWITCH) Foudation Guide, Indianapolis: Cisco Press, 2010
- D. Teare, Implementing Cisco IP Routing (Route) Foundation Learning Guide, Indianapolis: Cisco Press, 2010
- Cisco "Gigabit Campus Network Design—Principles and Architecture", Indianapolis: Cisco Press,
- High Availability Campus Network Design--Routed Access Layer using EIGRP or OSPF (2013, Setembro) [Online]. Available: http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/routed-ex.html
- Mike Fuszner (2013, Junho) GNS3 Graphical Network Simulator (version 1.0) [Online] Available: http://www.av.it.pt/salvador/LR/GNS3-0.5-tutorial.pdf
- GNS3 (2013, Junho), GNS3 Graphical Network Simulator [Online] Available: http://www.gns3.net/
- Cisco (2013, Outubro) Campus Network for High Availability Design Guide [Online] Available: http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html
- J. Tiso, Foudation Learning guide: Designing Cisco Network Service Architectures (ARCH) Ed. 3. Indianopolis: Cisco Press, 2010
- P. Oppenheimer, Top-Down Network Design, Third Edition. Indianapolis: Cisco Press, 2012

- J. D. McCabe, Networl Analysis, Architecture, and Design, Third Edition. USA: Morgan Kaufmann Publishers, 2007
- D. Serpanos, T. Wolf, Architecture of Network Systems, First Edition. USA: Morgan Kaufmann Publishers, 2011