INSTITUTO UNIVERSITÁRIO DA MAIA

Análise e otimização da tecnologia MPLS na rede da Universidade do Porto

DIOGO RAFAEL FERNANDES PEREIRA

Licenciado em Informática – Especialização em Redes de Nova Geração
no Instituto Universitário da Maia

Relatório de Projeto submetido ao Departamento de Ciências da Comunicação e Tecnologias da Informação do Instituto Universitário da Maia, para satisfação parcial dos requisitos do grau de Mestre em Tecnologias da Comunicação, Informação e Multimédia – Ramo Telecomunicações

Relatório de Projeto realizado sob a supervisão do Mestre Mário Paulo Monteiro Serrão, do Departamento de Ciências da Comunicação e Tecnologias da Informação do Instituto Universitário da Maia, e do Engenheiro Fernando Marques Correia, Diretor do Serviço de Infraestruturas Tecnológicas da Universidade do Porto

Maia, outubro de 2019

AGRADECIMENTOS

Termino assim aquela que para mim foi a etapa mais difícil de todo o percurso académico com um agradecimento a todos os que contribuíram direta ou indiretamente neste projeto.

Em primeiro lugar, ao orientador deste projeto, o professor Mário Serrão, pelo apoio contínuo ao longo da licenciatura e do mestrado. Sem dúvida que vou ter saudades das suas aulas.

Um agradecimento também ao coorientador do projeto, o engenheiro Fernando Correia, à Universidade do Porto e ao Centro Avançado de Telecomunicações do ISMAI, sem os quais a execução deste projeto não seria possível.

Aos meus colegas de curso, principalmente, ao Diogo Teixeira e ao João Lopes, um obrigado pela contínua presença na bela caminhada que foram os últimos 5 anos.

Aos meus amigos, Mota, Zé, Zé Nando, Tomás, Pinilha, Juliana e Joana, por serem os maiores e melhores amigos que podia desejar.

À Mariana, um enorme pedido de desculpas pelo desaparecimento que este projeto causou e um enorme obrigado pelo apoio incondicional e pela ajuda sempre presente.

E, por fim, à minha família, um especial agradecimento por todos os valores transmitidos que fazem de mim todos os dias mais e melhor pessoa, principalmente aos meus avós, pais e irmãos.

RESUMO

O presente relatório de projeto foi realizado em ambiente profissional, no âmbito do Mestrado em Tecnologias da Informação, Comunicação e Multimédia do Instituto Universitário da Maia – ISMAI, e teve como principal objetivo o estudo da tecnologia MPLS, e restruturação da mesma, na rede de comunicação de dados da Universidade do Porto. Para tal, a opção metodológica adotada foi a de *Action-Research*.

Numa primeira fase, examinou-se a implementação em produção, sendo, portanto, analisado o funcionamento e configuração dos protocolos relevantes para o funcionamento do MPLS, em particular o OSPF e o BGP, bem como os protocolos de sinalização (LDP e RSVP) responsáveis pela atribuição e distribuição de etiquetas.

Durante essa análise, constatou-se que o *backbone* da rede da Universidade do Porto não englobava uma distinção topológica entre equipamentos, nem contemplava a implementação de engenharia de tráfego, além de não oferecer redundância na conetividade, quer das diferentes Unidades Orgânicas, quer dos sistemas que suportam os serviços centralmente distribuídos.

Posteriormente, e com o intuito de colmatar as lacunas entretanto identificadas, preparou-se um conjunto de cenários de implementação, sobre os quais se realizou uma análise crítico-construtiva, no sentido de aferir qual o cenário topológico mais adequado à situação tecnológica da rede em operação.

Por fim, descreve-se a metodologia de implementação da solução técnica, cujas diretrizes visaram a proteção dos circuitos da rede de transporte, a redundância das ligações da rede de acesso e a garantia de SLA's extremo-a-extremo. Efetua-se também a implementação dos serviços de transporte tipicamente oferecidos em redes MPLS, apresentando um conjunto alargado de configurações, que contemplam não só os equipamentos de rede dos fabricantes Nokia e Cisco, mas também uma série de mecanismos de gestão técnica e operacional críticos para a continuidade do negócio, colmatando-se da melhor forma as lacunas identificadas.

PALAVRAS-CHAVE: Universidade do Porto, MPLS, engenharia de tráfego, proteção, redundância, VPLS, VPRN e OAM.

ABSTRACT

This project was carried out in a professional environment, within the scope of the master's degree in Information, Communication and Multimedia Technologies of Instituto Universitário da Maia – ISMAI. Its main objective was the study of the MPLS technology and it's restructuring in the communications network of the University of Porto. To this end, an Action-Research methodological approach was adopted.

At an initial stage, the implementation that was in production was examined, and the functioning and configuration of the protocols relevant to the operation of MPLS were analyzed, in particular, OSPF and BGP, as well as the signaling protocols (LDP and RSVP) responsible for the label attribution and distribution operations.

During this analysis, it was found that University of Porto's backbone network does not comprise a topological distinction between its nodes, nor does it contemplate the implementation of traffic engineering. Likewise, it also does not offer redundancy in the connectivity of either the Organic Units, or the systems that support the centrally distributed services.

Subsequently, in order to rectify the shortcomings previously identified, a set of implementation scenarios was prepared, on which a critical-constructive analysis was carried out, in order to assess which topological scenario is most appropriate to the technological status of the network in operation.

Finally, the methodology for implementing the technical solution is described, whose guidelines aimed at protecting the transport network circuits, the redundancy of access network connections and the guarantee of end-to-end SLAs. Typical MPLS transport services are also implemented, with a broad set of configurations that include not only Nokia and Cisco network equipment, but also a series of technical and operational management mechanisms that are critical for business continuity, rectifying the shortcomings previously identified.

KEYWORDS: University of Porto, MPLS, traffic engineering, protection, redundancy, VPLS, VPRN and OAM.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

AC	Attachment-Circuit
ASR	Aggregation Services Router
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CAT	Centro Avançado de Telecomunicações
CAUP	Centro de Astofísica da Universidade do Porto
CDUP	Centro de Desporto da Universidade do Porto
CE	Customer Edge
CEMUP	Centro de Materiais da Universidade do Porto
CIPES	Centro de Investigação de Políticas de Ensino Superior
CoS	Class of Service
CU	Currently Unused
CUP	Clínica Universitária de Psicologia
DiffServ	Differentiated Services
DSCP	Differentiated services codepoint
ELI	Entropy Label Indicator
FADEUP	Faculdade de Desporto da Universidade do Porto
FAUP	Faculdade de Arquitetura da Universidade do Porto
FBAUP	Faculdade de Belas Artes da Universidade do Porto
FCCN	Fundação para a Computação Científica Nacional
FCNAUP	Faculdade de Ciências da Nutrição e Alimentação da Universidade do Porto
FCT	Fundação para a Ciência e Tecnologia
FCUP	Faculdade de Ciências da Universidade do Porto
FDUP	Faculdade de Direito da Universidade do Porto
FEC	Forwarding Equivalence Class
FEP	Faculdade de Economia da Universidade do Porto
FEUP	Faculdade de Engenharia da Universidade do Porto
FFUP	Faculdade de Farmácia da Universidade do Porto
FIB	Forwarding Information Base
FIMS	Fundação Instituto Arquitecto José Marques da Silva
FLUP	Faculdade de Letras da Universidade do Porto

FMDUP	Faculdade de Medicina Dentária da Universidade do Porto
FMUP	Faculdade de Medicina da Universidade do Porto
FPCEUP	Faculdade de Psicologia e de Ciências da Educação da Universidade do Porto
FR	Frame Relay
FRR	Fast Reroute
GAL	Generic Associated Channel Label
I3S	Instituto de Investigação e Inovação em Saúde
IBMC	Instituto de Biologia Molecular e Celular
ICBAS	Instituto de Ciências Biomédicas Abel Salazar
ICETA	Instituto de Ciências, Tecnologias e Agroambiente da Universidade do Porto
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocols
INEGI	Instituto de Ciência e Inovação em Engenharia Mecânica e Engenharia Industrial
INESC-TEC	Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência
IntServ	Integrated Services
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISMAI	Instituto Universitário da Maia
ISP	Internet Service Provider
ISPUP	Instituto de Saúde Pública da Universidade do Porto
L2VPN	Layer 2 Virtual Private Network
L3VPN	Layer 3 Virtual Private Network
LAN	Local Area Network
LDP	Label Distribution Protocol
LER	Label Edge Router
LFIB	Label Forwarding Information Base
LIACC	Laboratório de Inteligência Artificial e Ciência de Computadores
LIB	Label Information Base
LSP	Label Switched Path
LSR	Label Switch Router
MAC	Media Access Control
MP	Merge Point

MP-BGP	Multiprotocol Border Gateway Protocol
MPLS	Multiprotocol Label Switching
netUP	Rede de Dados da Universidade do Porto
NREN	National Research and Education Network
NTP	Network Time Protocol
OAM	Operations, Administration and Maintenance
OSPF	Open Shortest Path First
OUP	Orfeão da Universidade do Porto
PBS	Porto Business School
PDU	Protocol Data Unit
PE	Provider Edge
PHB	Per-Hop Behavior
PHP	Penultimate Hop Popping
PLR	Point of Local Repair
PSN	Packet Switched Network
PW	Pseudowire
QoS	Quality of Service
RCTS	Rede de Ciência, Tecnologia e Sociedade
RD	Route Distinguisher
RFC	Request for Comments
RIP	Routing Information Protocol
RSVP	Resource Reservation Protocol
RT	Route Target
RUCA	Residência Universitária Campo Alegre
SASUP	Serviços de Acção Social da Universidade do Porto
SLA	Service Level Aggrement
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TE	Traffic Engineering
ToS	Type of Service
TTL	Time to Live
UO	Unidade Orgânica
UP	Universidade do Porto
UPTEC	Parque da Ciência e Tecnologia da Universidade do Porto

VC	Virtual Circuit
VCI	Virtual Channel Identifier
VLAN	Virtual Local Area Network
VLL	Virtual Leased Line
VPI	Virtual Path Identifier
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VPRN	Virtual Private Routed Network
VPWS	Virtual Private Wire Service
VRF	Virtual Route Forwarding
VSI	Virtual Switching Instance
WDM	Wavelength Division Multiplexing

1. INTRODUÇÃO

O presente projeto de dissertação foi realizado em ambiente profissional, na Universidade do Porto (UP), e teve como principal objetivo a otimização da rede IP/MPLS (*Multiprotocol Label Switching*) que se encontra atualmente em operação. Para tal, foi necessário estudar os conceitos intrínsecos a esta tecnologia, bem como o atual cenário de implementação de modo a que fossem propostas melhorias.

No presente capítulo apresenta-se o enquadramento ao tema, seguido dos objetivos a alcançar com este projeto. É ainda indicada a metodologia de investigação adotada e a estrutura do projeto em questão.

1.1 Enquadramento

A Universidade do Porto, dispõe de uma infraestrutura de comunicações transversal que serve as várias Unidades Orgânicas (UO's), que se encontram geograficamente distribuídas pela cidade do Porto, mais precisamente localizadas em torno de quatro pólos ou áreas geográficas, nomeadamente:

- Pólo 1: localiza-se no centro histórico da cidade e o respetivo nó de comutação encontra-se situado no Data Center localizado no edifício da Reitoria da Universidade do Porto;
- Pólo 2: localiza-se na zona da Asprela e o respetivo nó de comutação encontra-se situado no Data Center localizado no edifício da Faculdade de Engenharia da Universidade do Porto (FEUP);
- Pólo 3: localiza-se na zona do Campo Alegre e o respetivo nó de comutação encontra-se situado no Data Center localizado no edifício da Faculdade de Ciências da Universidade do Porto (FCUP);
- Pólo 4: localiza-se na zona de Cedofeita e o respetivo nó de comutação encontra-se situado no Data Center localizado no edifício da Faculdade de Direito da Universidade do Porto (FDUP);

No total a rede de dados da Universidade do Porto (netUP) conta com cerca de 51 nós de acesso, entre os quais faculdades, residências universitárias, institutos de investigação e desenvolvimento, entre outros organismos.

Com recurso à rede metropolitana de fibra ótica implementada no âmbito do projeto Porto Digital, a interligação entre os quatro pólos tecnológicos é possível recorrendo a serviços de fibra escura, que permitem atualmente ligações a 10 Gb/s.

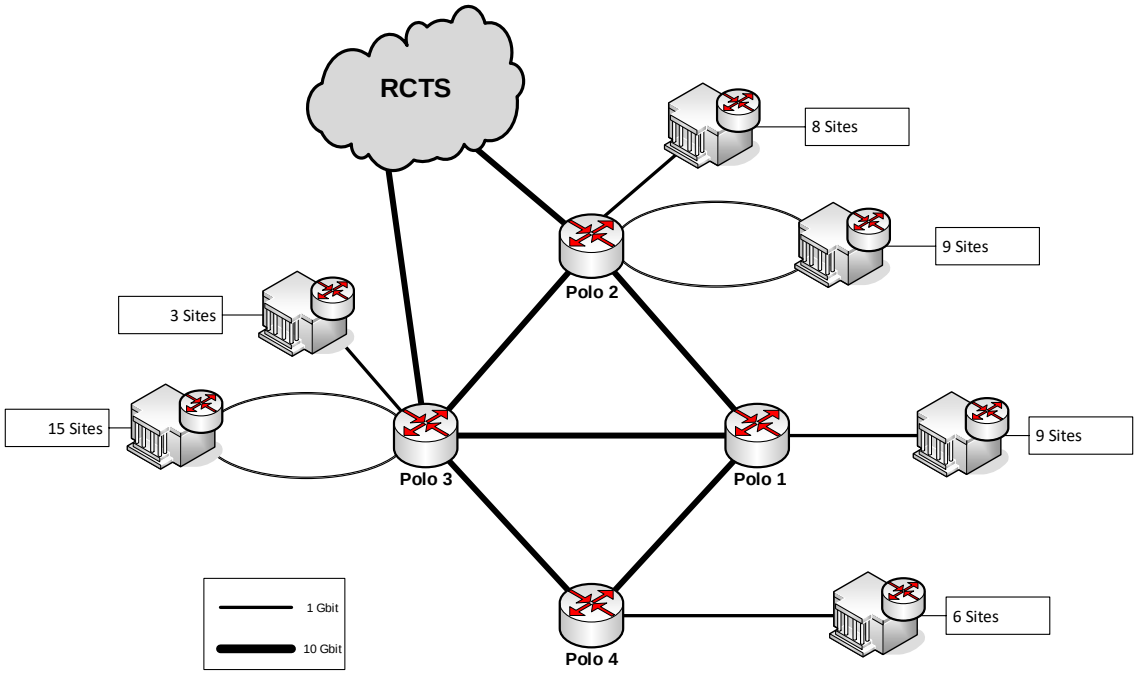

Figura 1 – Topologia da rede da Universidade do Porto

Além do referido, e como se verifica na Figura 1, o acesso à Internet efetua-se através da interligação com a RCTS (Rede de Ciência, Tecnologia e Sociedade), que corresponde à rede nacional de investigação e ensino, também designada internacionalmente por NREN (*National Research and Education Network*). Esta rede é gerida e operada pela FCCN (Fundação para a Computação Científica Nacional), que atualmente é mais uma unidade da FCT (Fundação para a Ciência e Tecnologia).

Neste momento em operação, a netUP conta com duas ligações à RCTS por intermédio dos polos 2 e 3, no entanto apenas uma das ligações se encontra ativa (ligação do pólo 2 – 10 Gb/s) enquanto que a outra serve como redundância (ligação do pólo 3 – 10 Gb/s), sendo ativada no caso da primeira ligação falhar.

Até à implementação da tecnologia de transporte MPLS, era utilizada a tecnologia IP como solução de transporte de serviços comuns a todas as faculdades, como o caso do serviço NTP (*Network Time Protocol*), sendo que a grande maioria dos serviços presentes em cada unidade orgânica eram da sua responsabilidade.

A mudança de paradigma, em que a maior parte dos serviços passou a ser oferecido centralmente, motivou a introdução da tecnologia MPLS de modo a oferecer uma infraestrutura flexível, escalável e com capacidade de oferecer serviços de QoS (*Quality of Service*) diferenciados aos seus clientes/colaboradores.

Esta necessidade conduziu à operacionalização de uma rede MPLS distribuída ao longo dos quatro pólos, que oferece serviços de conetividade *ethernet* assentes sobre soluções baseadas em VPLS (*Virtual Private LAN Services*).

No entanto, a rede MPLS implementada na Universidade do Porto em 2012 não foi alvo de qualquer atualização tecnológica, apesar de se ter adquirido equipamento que permite a integração de técnicas de resiliência e engenharia de tráfego.

Posto isto, o presente projeto de mestrado pretende analisar e discutir possíveis melhorias ao cenário tecnológico que atualmente se encontra em operação.

1.2 Objetivos

Tal como qualquer projeto tecnológico é fundamental a definição clara dos seus objetivos. Neste caso concreto, os objetivos gerais são, nomeadamente:

- Estudar, analisar e implementar uma nova topologia de rede (MPLS) com integração de novos equipamentos ativos que garantam a redundância no acesso aos serviços disponibilizados centralmente;
- Acautelar a integração da nova topologia na rede existente, para que haja o mínimo de impacto nos serviços atualmente disponibilizados;
- Integrar na rede MPLS funcionalidades de otimização de largura de banda e qualidade de serviço, tendo em conta a escalabilidade da rede.

Inerente a todos os objetivos encontra-se o estudo (detalhado) da tecnologia MPLS, incluindo a descrição pormenorizada do cenário que se encontra de momento em produção na Universidade do Porto, os equipamentos existentes e respetivas configurações, bem como a análise sobre a possibilidade de utilização de mais equipamentos.

Intrinsecamente, aliado ao processo académico em curso, salienta-se ainda um objetivo pessoal, que visa o aumento de conhecimento e experiência na área de comunicação de dados, em particular na tecnologia MPLS, para que seja possível também uma evolução no âmbito profissional.

1.3 Metodologia de investigação e plano de trabalhos

Para realizar o presente projeto de dissertação tornou-se pertinente definir qual a estratégia de investigação/trabalho a adotar. Desta forma, recorreu-se à estratégia *Action-Research*, que se baseia na participação ativa do investigador e de todos os envolvidos na implementação de uma ou mais ações [1].

Assim sendo, e de acordo com o que é pretendido, a estratégia traduz-se nas seguintes fases:

- **Fase 1:** Pesquisa da literatura relevante e elaboração do estado de arte;
- **Fase 2:** Diagnóstico e análise crítica da rede da Universidade do Porto;
- **Fase 3:** Elaboração e planeamento das propostas de melhoria;
- **Fase 4:** Implementação de cenários de estudo;
- **Fase 5:** Análise dos resultados obtidos;
- **Fase 6:** Especificação da aprendizagem;

Numa primeira fase recorreu-se à análise documental de forma a reunir o máximo de informação possível a culminar em soluções que cumpram os objetivos definidos. Toda a análise documental teve como base a revisão bibliográfica, recorrendo-se a fontes primárias, tais como teses e dissertações, e também fontes secundárias, isto é, livros e artigos científicos.

A segunda fase compreende o esclarecimento e descrição técnica da solução de rede IP/MPLS atualmente em operação na camada de transporte da rede da Universidade do Porto. A operação crítica sobre esta rede tende a convergir nos objetivos técnicos a alcançar no projeto, os quais são abordados na terceira e quarta fase, através da elaboração de propostas de melhoria e a implementação de vários cenários para análise.

A fase de implementação entende a utilização de equipamentos Cisco e Nokia, cedidos pela Universidade do Porto e pelo Instituto Universitário da Maia, onde se coloca em prática vários cenários com vista à disponibilização de serviços de nível 2 e 3.

Posteriormente à fase de implementação, entende-se a necessidade de avaliar a solução estudada e implementada, especificando também toda a aprendizagem através das conclusões (sexta fase).

Definidas as fases de investigação a adotar, resta adicionar uma sétima fase referente à escrita do relatório do projeto de mestrado. Deste modo, o plano de trabalhos foi definido podendo o mesmo ser visualizado com base na Tabela 1.

Tabela 1 – Cronograma com as fases a desenvolver no projeto

Fase	2018		2019									
	Nov	**Dez**	**Jan**	**Fev**	**Mar**	**Abr**	**Mai**	**Jun**	**Jul**	**Ago**	**Set**	**Out**
Fase 1												
Fase 2												
Fase 3												
Fase 4												
Fase 5												
Fase 6												
Fase 7												

1.4 Estrutura do relatório

O presente documento encontra-se dividido em cinco capítulos. No primeiro capítulo apresenta-se o enquadramento geral, os objetivos pretendidos com este projeto, bem como a metodologia de investigação e a estrutura do relatório.

No segundo capítulo encontra-se a revisão bibliográfica respeitante à tecnologia MPLS, referindo-se as tecnologias de transporte concorrentes e quais os seus componentes arquitetónicos. Posteriormente, descreve-se a unidade de informação e seu respetivo cabeçalho, a ação de atribuição e distribuição de etiquetas, os serviços de transporte tipicamente oferecidos em cenários IP/MPLS, o paradigma da engenharia de tráfego, o conceito de qualidade de serviço e, por fim, as técnicas de OAM (Operations, Administration and Maintenance) fundamentais na gestão, operação, monitorização e aprovisionamento.

No terceiro capítulo apresenta-se uma memória descritiva técnica sobre a rede da Universidade do Porto, analisando-se inicialmente a solução de rede antecedente ao cenário atual, isto é, quando a solução de transporte se baseava em protocolos dinâmicos de *routing* IP, sendo que posteriormente se apresenta o esquema de funcionamento atual, onde são abordadas as topologias e configurações atualmente em operação. Sobre cada um dos temas é também realizada uma breve análise crítica, que visa primordialmente a introdução do quarto capítulo.

Mediante a reflexão crítica realizada no momento do estudo da situação atual da tecnologia MPLS na Universidade do Porto, no quarto capítulo são apresentados os aspetos a melhorar e é definida a estratégia e as propostas de melhoria. De seguida, são apresentados vários cenários de implementação, e perante a identificação do cenário mais indicado é apresentado e

demonstrado o plano de implementação adotado, bem como as configurações realizadas, por tipo de equipamento

Por fim e em resumo do trabalho realizado, são apresentadas as principais conclusões, bem como algumas sugestões para trabalho futuro.

2. MULTIPROTOCOL LABEL SWITCHING

2.1 Introdução

Com a crescente procura de aplicações e serviços com necessidades intrínsecas de largura de banda e qualidade de serviço, surge a oportunidade do aparecimento de uma tecnologia de transporte alternativa às redes IP tradicionais, uma vez que estas pressupõem necessariamente um conjunto complexo de operações associados ao processo de comutação que influem diretamente na latência, bem como assentam o seu funcionamento em mecanismos, que resultam em falta de escalabilidade e qualidade de serviço.

Esta tecnologia está intrinsecamente associada à camada de transporte de uma rede de telecomunicações, que pode ser considerada segundo Serrão [2] "como uma plataforma tecnológica que assegura a transferência transparente, fiável e independente da informação à distância, sendo constituída por diferentes elementos de rede interligados segundo uma certa topologia física".

Assente na tecnologia de rede atrás referida (IP), foi desenvolvido o protocolo MPLS com o intuito de colmatar as necessidades existentes nas redes IP, através da comutação de etiquetas e técnicas avançadas de engenharia de tráfego [3].

A comutação por etiquetas permite que equipamentos com menor poder de processamento tenham um maior desempenho neste tipo de arquitetura, uma vez que as informações necessárias para o encaminhamento são obtidas através do cabeçalho MPLS de 32 *bits*, ao invés dos 20 *bytes* que compõem o cabeçalho IP (ver secção 2.4) [4].

Neste capítulo encontra-se o estudo realizado sobre a tecnologia MPLS, que se inicia pela comparação com outras tecnologias concorrentes. Posteriormente, são objeto de estudo os componentes arquitetónicos, os modos de distribuição de etiquetas, os tipos de serviços oferecidos pela tecnologia, bem como um conjunto de funções essenciais tais como a engenharia de tráfego, a qualidade de serviço e as técnicas de operação, administração e gestão.

2.2 Tecnologias concorrentes

Ao longo da presente secção pretende-se descrever algumas das tecnologias que se encontram/encontraram tipicamente implementadas nas redes de transporte. O desenvolvimento das tecnologias ATM (*Asynchronous Transfer Mode*), WDM (*Wavelength*

Division Multiplexing) e IP conduziram ao aparecimento da tecnologia MPLS, não só pelas "falhas" que as tecnologias podiam apresentar, mas também pela necessidade de retro compatibilidade que é necessária existir com o protocolo IP, pois este é apresentado como a base do *routing*.

2.2.1 ATM

A evolução dos meios de transmissão, o aumento de utilização de serviços baseados no modelo cliente/servidor e o aumento da capacidade de processamento dos equipamentos dos utilizadores, são algumas das razões que levaram ao aparecimento de tecnologias como o *Frame Relay* (FR) [5]. No entanto, a necessidade de fornecimento de elevados débitos, que com a tecnologia anteriormente mencionada não iam para além dos 30 Mb/s por circuito, e classes de serviços diferenciadas, levou ao desenvolvimento da tecnologia ATM [6].

O ATM refere-se a uma tecnologia de comutação de células (de comprimento fixo), orientada à conexão e com débitos variáveis até 622 *Mbits/s*. O tipo de comutação oferecida pelo ATM permite que a transmissão seja realizada de modo assíncrono relativamente às *slots* (intervalos de tempo) disponíveis [7].

Esta tecnologia é frequentemente utilizada para o transporte de protocolos de rede, tais como o IP (*IP over* ATM), sendo que os dados protocolares são segmentados em *Protocol Data Units* (PDUs), de 48 *bytes*. A estas PDUs precede-se o cabeçalho da célula ATM de 5 *bytes*, perfazendo um total de 53 *bytes* por célula [8].

A definição do encaminhamento é determinada no cabeçalho de cada célula ATM, mais precisamente através do identificador de caminho virtual (*Virtual Path Identifier* - VPI) e do identificador de canal virtual (*Virtual Channel Identifier* – VCI). Ambos os parâmetros combinados formam o circuito virtual, o qual é estabelecido através de um processo de sinalização.

Tabela 2 – Tabela de comutação ATM

Tabela de Comutação ATM					
Entrada			**Saída**		
Porta	VPI	VCI	Porta	VPI	VCI
1	6	2	4	4	7
3	4	9	2	1	2

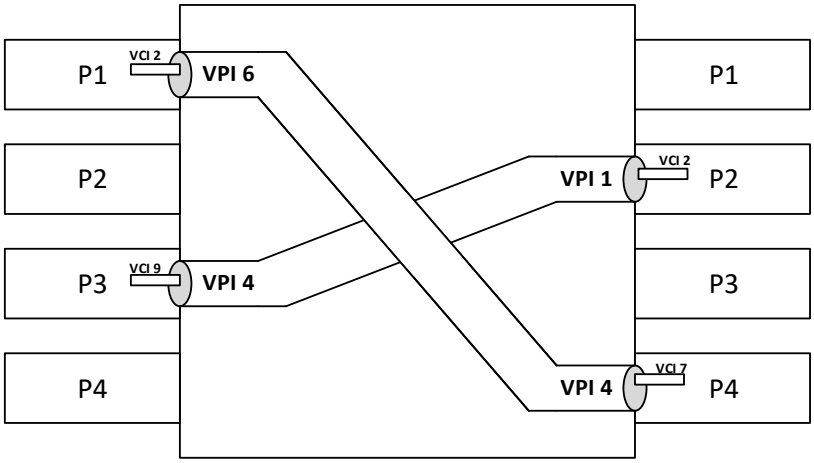

Figura 2 – Processo de comutação ATM

A Figura 2 com auxílio da Tabela 2, ilustra o tratamento para a decisão de comutação que é dado para duas células ATM distintas, onde se verifica que os identificadores têm significado local e não correspondem a endereços extremo-a-extremo, permitindo uma rápida comutação [9]. Note-se que o exemplo corresponde a uma conexão ponto-a-ponto, pois como refere Coutinho [6] "embora estejam previstas topologias multiponto em redes ATM, a sua implementação é extremamente complexa, pelo que raramente são utilizadas", o que por si só é um problema.

2.2.2 WDM

A introdução da fibra ótica como meio de transmissão dos sinais de telecomunicações nas redes de transporte, trouxe inúmeros benefícios tais como menor latência e maior segurança, mas este meio oferece também a possibilidade de prover débitos de serviço apenas limitados pelos sistemas terminais.

Neste cenário, surgiu a tecnologia *Wavelength Division Multiplexing* (WDM), que como a nomenclatura indica, refere-se a uma tecnologia que tem como princípio de operação a multiplexagem por divisão do comprimento de onda (λ).

O espaçamento entre comprimentos de onda diferentes limita a largura de banda máxima disponível com a utilização desta tecnologia, no entanto avanços tecnológicos apontam para a utilização de filtros que permitem diminuir o espaçamento entre os diferentes comprimentos de onda, o que possibilita um elevado aumento da largura de banda disponibilizada por canal de comunicação [10].

O funcionamento desta tecnologia consiste na divisão do espetro de frequências através da alocação de informação em comprimentos de onda distintos. O multiplexador/emissor, ver Figura 3, ao receber um conjunto de comprimentos de onda, modula-os e combina-os de forma a que possam ser transmitidos sobre uma mesma fibra ótica. Por sua vez, o desmultiplexador/ recetor "separa" cada um dos vários comprimentos de onda e transmite-os por saídas distintas [11].

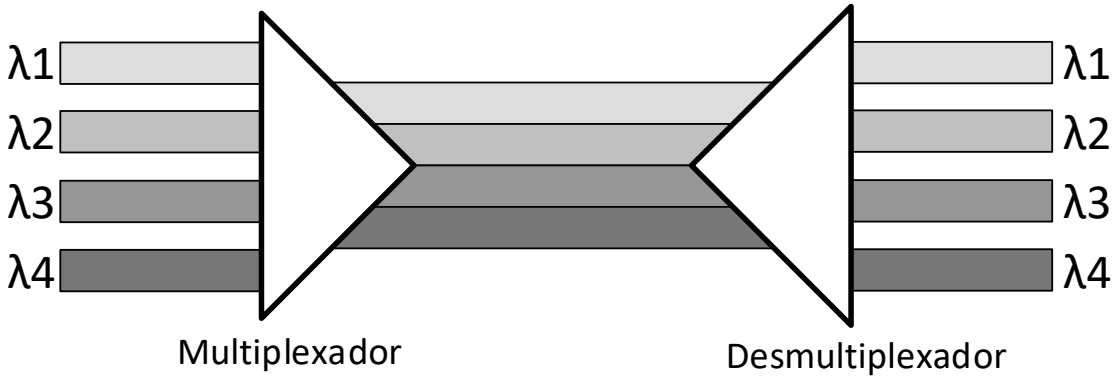

Figura 3 – Multiplexagem por divisão do comprimento de onda [12]

2.2.3 IP

O protocolo IP pode ser referido como um dos protocolos cruciais para o funcionamento da *Internet*, apresentando funções como a definição do esquema de endereçamento global, a definição de pacotes, que correspondem à unidade de dados transmitidos na *Internet*, e ainda a função de encaminhamento (*routing*) dos pacotes.

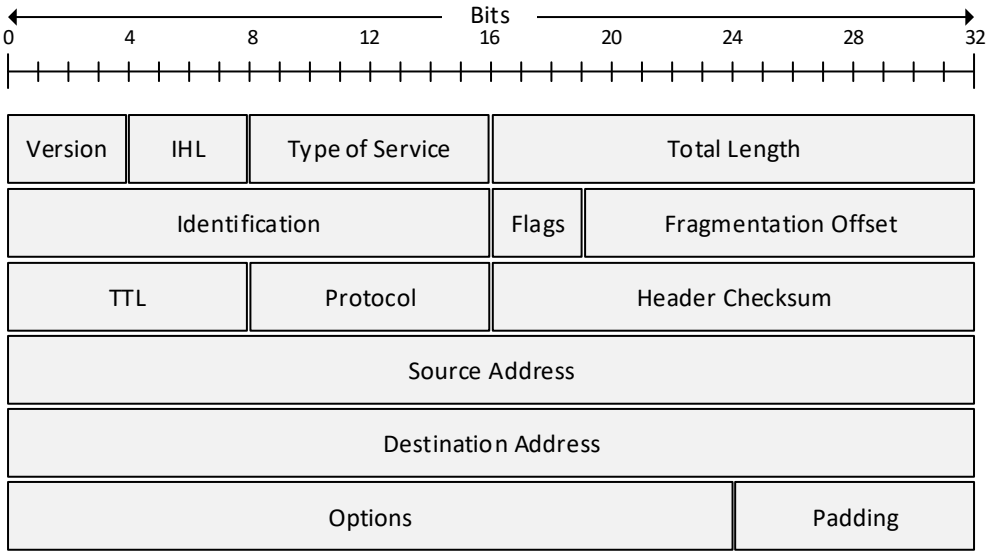

Figura 4 – Formato do pacote IP [13]

A Figura 4 representa o formato de um pacote IP, ao qual se devem reter alguns parâmetros responsáveis pela função de encaminhamento operada por este protocolo, nomeadamente o endereço de origem (*source address*) e o endereço de destino (*destination address*). Ambos os parâmetros permanecem inalterados durante todo o seu percurso, sendo que é apenas com base no endereço de destino que os equipamentos da rede tomam as decisões de encaminhamento.

Nas denominadas redes de transporte, os equipamentos de rede usam preferencialmente protocolos dinâmicos de *routing* para que as decisões de encaminhamento sejam facilmente tomadas. Protocolos como o RIP (*Routing Information Protocol*), OSPF (*Open Shortest Path First*) e BGP (*Border Gateway Protocol*) foram desenhados expressamente para o efeito.

Este protocolo apresenta também alguns aspetos relevantes a ter em conta, como o facto de ser *connectionless* e *unreliable* [13]. O primeiro aspeto significa que o IP não troca informações de forma a estabelecer uma ligação extremo-a-extremo, ou seja, não consegue garantir a entrega de dados por si só (sem recorrer a protocolos de camadas superiores, como o *Transmission Control Protocol* - TCP) [14]. Já o segundo aspeto diz respeito ao facto desta tecnologia não apresentar deteção e correção de erros, no entanto, assim como acontece com a definição anterior, esta característica é ultrapassada com outros protocolos da arquitetura TCP/IP.

2.3 Componentes da arquitetura MPLS

A arquitetura MPLS abrange vários componentes/conceitos [4] que se devem reter para que se entenda melhor o funcionamento desta tecnologia apresentado ao longo das próximas secções. Cada conceito é, de seguida, brevemente explicado, sendo que alguns serão ainda alvo de maior estudo devido à sua importância. A Figura 5 apresenta os componentes principais inerentes ao domínio MPLS num dado processo de comutação.

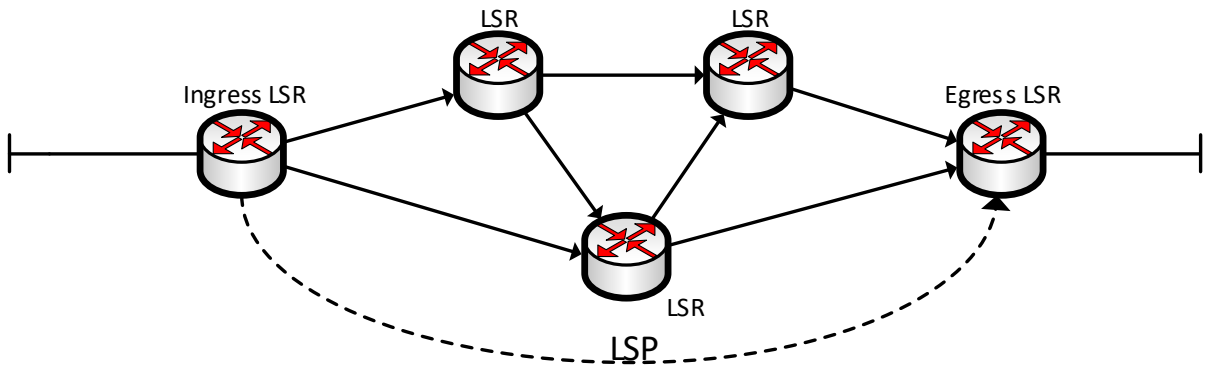

Figura 5 – Elementos da rede MPLS [3]

1. *Forwarding Equivalence Class (FEC*): representa um grupo de pacotes IP que são encaminhados sob o mesmo caminho e sob o mesmo tratamento de encaminhamento. Numa arquitetura *non*-MPLS, a associação do pacote a uma FEC é exclusivamente baseada na rede de destino, enquanto que no MPLS, além da informação presente no cabeçalho do pacote, a associação do pacote a uma FEC pode ser influenciada pelos seguintes critérios de classificação de pacotes [15]:
    - Combinação das redes de origem e destino;
    - Combinação da rede de destino e tipo de aplicação;
    - Grupos *Multicast* IP;
    - Túneis com engenharia de tráfego;
    - Identificador de *Virtual LAN* (VLAN);
    - Identificador de *Virtual Private Network* (VPN);
    - Requisitos de Qualidade de Serviço e Classes de Serviço (CoS);
2. *Label*: identificador de tamanho fixo (20 *bits*), com significado local, utilizado para identificar uma FEC;
3. *Label Swap*: consiste numa operação de encaminhamento básico onde se verifica qual a etiqueta de entrada para determinar qual a etiqueta e porta de saída, bem como outras informações necessárias para o tratamento dos dados;
4. *Label Distribution Protocols* (LDP's): cada protocolo de distribuição de etiquetas realiza um conjunto de operações onde todos os nós de uma determinada rede MPLS trocam informações acerca da atribuição de etiquetas. Alguns dos protocolos responsáveis pela distribuição de etiquetas são o LDP e o RSVP (*Resource Reservation Protocol*);
5. *Label Information Base* (LIB): representa uma tabela de decisão de encaminhamento existente em *control plane* através da qual se relaciona a etiqueta de entrada com a etiqueta de saída e consequente interface. Esta tabela pode apresentar mais do que uma etiqueta para um determinado destino com base no mesmo protocolo de distribuição de etiquetas;
6. *Label Forwarding Information Base* (LFIB): representa uma tabela de encaminhamento de etiquetas, existente em *data plane* e construída a partir da LIB, contendo, no entanto,

apenas as entradas necessárias para o encaminhamento das etiquetas. É comummente apresentada em forma de tabela (Figura 6), sendo esta construída através do protocolo de distribuição de etiquetas em utilização;

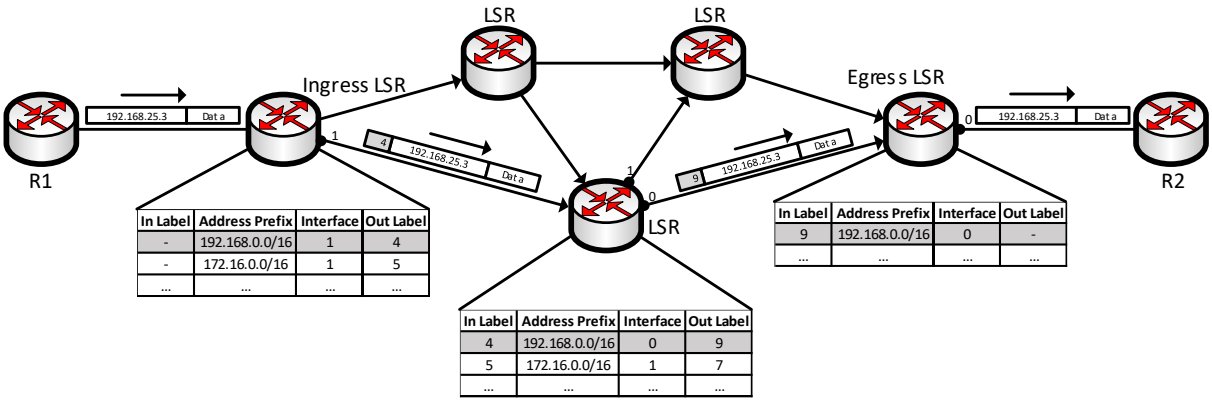

Figura 6 – Exemplos de tabelas de comutação de etiquetas [3]

7. *Label Edge Router* (LER): também designado como MPLS *edge node*. Este nó é responsável por interligar um domínio MPLS com um nó que não opera com MPLS ou simplesmente que se encontra num outro domínio. Podem distinguir-se dois tipos de LER's, o *ingress* e o *egress*, podendo obviamente um LER desempenhar ambas as funções.
    - *Ingress LER*: nó de entrada no domínio MPLS, cuja principal função é tratar os dados de forma a que estes cumpram os requisitos necessários ao processo de comutação no domínio. Este tratamento corresponde à inserção de uma etiqueta, ato denominado como *Push*;
    - *Egress LER*: nó de saída do domínio MPLS, cuja principal função é receber uma dada etiqueta e retirá-la, encaminhando o pacote para o exterior do domínio MPLS. O ato de remover a etiqueta denomina-se por *Pop*.
8. *Label Switch Router* (LSR): os LSRs são parte integrante do *core* do domínio MPLS. Têm a função de comutar as etiquetas, isto é, ao receberem uma etiqueta, analisam a LFIB, inserem uma nova etiqueta e encaminham a unidade de informação para o próximo *hop*;
9. *Label Switched Path* (LSP): o caminho que uma FEC percorre num determinado domínio MPLS.

Os componentes referidos devem ser retidos para entendimento das ações intrínsecas a esta tecnologia, como é o caso da atribuição e distribuição de etiquetas e formação de LSP's. É também importante mencionar que a nomenclatura de componentes como o LER e LSR é alterada quando abordados nos serviços de transporte apesar do funcionamento ser semelhante.

2.4 Cabeçalho MPLS

O cabeçalho MPLS, também designado como *MPLS shim header* [16], representa o conjunto de entradas na pilha de etiquetas (*label stack*). Antes de se focar nas funcionalidades inerentes ao MPLS, é importante analisar-se cada entrada da pilha de etiquetas (*label stack entry*) [17]. Na Figura 7 pode-se verificar que são quatro os campos que compõem uma dada entrada.

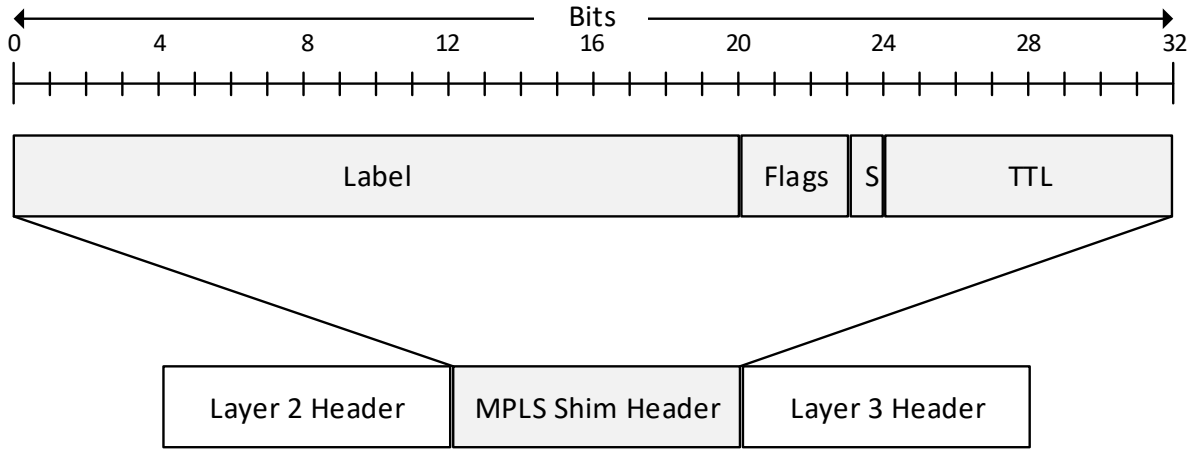

Figura 7 – Cabeçalho MPLS [15]

Estes campos são fundamentais no processo de comutação de etiquetas, tendo de igual forma cada um deles um papel relevante no funcionamento do MPLS. Os campos que compõe cada entrada da *label stack* são [17]:

- *Bottom of Stack (S)*: constituído por apenas 1 *bit*. É importante para se identificar a última entrada da pilha de etiquetas. Toma o valor de "1" caso seja a última entrada e "0" nas restantes;
- *Time to Live (TTL)*: utilizado para prevenir que um determinado pacote seja comutado infinitamente. Por cada operação de comutação o valor é decrementado, e caso atinja o valor "0" o pacote é descartado. Este campo tem 8 *bits*;
- *Experimental Use (Exp)*: este campo possuí 3 *bits* dedicados a cenários de utilização futura;

- *Label Value (Label)*: corresponde ao valor da etiqueta. Os 20 *bits* resultam em 1048575 (2^{20}-1) valores possíveis de etiquetas, no entanto alguns destes valores encontram-se reservados, nomeadamente:
    - 0 – *IPv4 Explicit NULL Label*: indica que a etiqueta deve ser retirada (*POP*) e a decisão de encaminhamento deverá ser tomada com base no cabeçalho *IPv4*;
    - 1 – *Router Alert Label*: caso seja recebida uma etiqueta com este valor, a respetiva entrada será processada por um módulo de *software* local;
    - 2 – *IPv6 Explicit NULL Label*: indica que a etiqueta deve ser retirada (*POP*) e a decisão de encaminhamento deverá ser tomada com base no cabeçalho *IPv6;*
    - 3 – *Implicit NULL Label*: apesar de nunca comparecer no processo de encapsulamento, esta etiqueta pode ser atribuída/distribuída por um LSR, no entanto quando recebida deverá ser retirada a etiqueta;
    - 7 – *Entropy Label Indicator* (*ELI*) [18];
    - 13 – *Generic Associated Channel Label* (*GAL*) [19];
    - 14 – *Operations, Administration and Maintenance Alert Label* [20];
    - 15 – *Extension Label* [21];
    - As etiquetas entre [4,6] e [8,12] encontram-se reservadas para utilização futura;

No momento em que o *ingress* LER recebe um pacote e lhe atribui a respetiva etiqueta, é automaticamente adicionado o cabeçalho MPLS entre o cabeçalho de nível 3 e o cabeçalho de nível 2. Por esta razão esta tecnologia é muitas vezes descrita como sendo de nível 2,5 [22].

2.5 Atribuição e distribuição de etiquetas

Para que a comutação possa ocorrer através do domínio MPLS é primeiramente necessário que os nós constituintes deste domínio formem LSP's, bem como operacionalizem e populem as tabelas de comutação de etiquetas.

A criação de um LSP advém da atribuição de etiquetas pelo nó mais a jusante (*downstream*) para uma determinada FEC, e consequentemente na informação que este nó sinaliza a montante (*upstream*) acerca da atribuição realizada. Ou seja, em relação a uma FEC, o nó mais a jusante atribui as etiquetas e essa informação é distribuída no sentido *downstream-to-upstream* [4].

Após o nó *upstream* atribuir uma etiqueta local para a determinada FEC, este além de encaminhar a informação da etiqueta no sentido *upstream* (caso faça sentido), também replica essa informação para o nó *downstream*, de forma a que sejam criadas tabelas de comutação de etiquetas.

Segundo o exemplo apresentado na Figura 8, em relação à FEC-1, o LER "Lisboa" atribuí uma etiqueta e transmite essa informação para o nó *upstream*, ou seja, para o LSR "Coimbra" que por sua vez notifica o LER "Porto" e o LER "Lisboa" acerca da atribuição de etiquetas efetuada por si. Após a receção da informação por parte do LER "Porto", este atribui uma etiqueta à FEC-1 e informa o LSR "Coimbra" sobre a atribuição realizada.

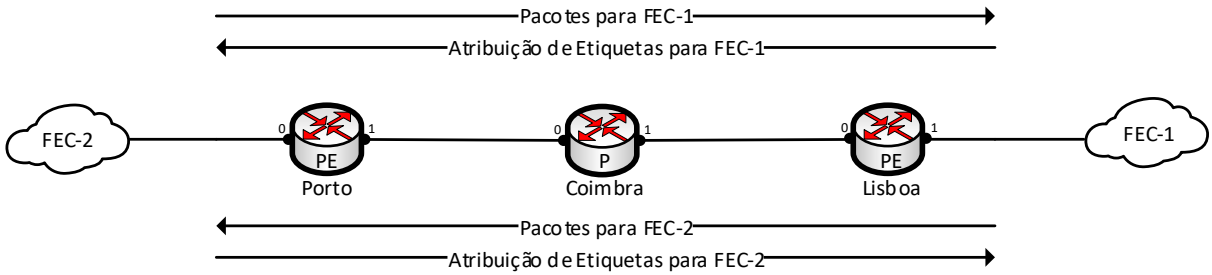

Figura 8 – Atribuição de etiquetas por FEC

A atribuição e distribuição de etiquetas por cada nó, cria a denominada LFIB, que corresponde a uma tabela baseada nos campos "*Label IN, Label OUT*". A Tabela 3, Tabela 4 e Tabela 5 apresentam possíveis tabelas de comutação de etiquetas para o exemplo apresentado.

Tabela 3 – LFIB (PE - Porto)

PE - Porto (LFIB)			
In Label	**Address Prefix**	**Interface**	**Out Label**
-	FEC-1	1	11
22	FEC-2	0	-

Tabela 4 – LFIB (P-Coimbra)

P - Coimbra (LFIB)			
In Label	**Address Prefix**	**Interface**	**Out Label**
11	FEC-1	1	21
32	FEC-2	0	22

Tabela 5 – LFIB (PE-Lisboa)

PE - Lisboa (LFIB)			
In Label	**Address Prefix**	**Interface**	**Out Label**
21	FEC-1	1	-
-	FEC-2	0	32

A distribuição de etiquetas referida é realizada com base em dois protocolos definidos para o efeito, nomeadamente o LDP e o RSVP. Inerente a estes protocolos existem também três modos de distribuição de etiquetas, nomeadamente o modo de distribuição, o modo de controlo e o modo de retenção, que serão analisados nos subcapítulos 2.5.1, 2.5.2, 2.5.3 e no subcapítulo 2.5.4. Estes modos encontram-se definidos através do RFC 3031 [4].

2.5.1 Protocolos para distribuição de etiquetas

Cada LSP pode ser formado de duas formas distintas. De forma estática onde o mapeamento das etiquetas é realizado em cada nó manualmente, ou de forma alternativa dinamicamente, por recurso a protocolos de distribuição de etiquetas. Cada protocolo de distribuição de etiquetas representa um conjunto de operações onde todos os LSRs de uma determinada rede MPLS trocam informações acerca da atribuição de etiquetas, sinalizando um túnel MPLS entre dois (ou mais) LERs. Este processo de negociação de etiquetas, com o objetivo de formar o LSP, denomina-se por processo de sinalização [23].

Entre os protocolos de sinalização disponíveis, importa realçar o LDP e o RSVP.

- O termo LDP, além de abranger sintaticamente todos os protocolos de distribuição de etiquetas, é por si só um protocolo utilizado para a construção de LSP's. Este protocolo tem como base as informações de *routing* existentes entre os nós do domínio MPLS, mais concretamente, este protocolo faz uso de informações provenientes de protocolos internos de *routing* (*Interior Gateway Protocols* - IGPs), como o caso do OSPF, para a distribuição de etiquetas e construção das LIBs [24];
- O RSVP é o protocolo utilizado quando existem pré-requisitos de engenharia de tráfego ou qualidade de serviço. Por recurso a este protocolo, é possível a definição concreta de LSP's, indicando os nós pelo qual o pacote vai ser comutado desde o nó *ingress* até ao nó *egress*. Este protocolo é analisado com maior detalhe no subcapítulo 2.7.1 [25].

2.5.2 Modo de distribuição de etiquetas

A distribuição das etiquetas distingue-se em duas técnicas, *downstream on-demand* (RSVP) e *downstream unsolicited* (LDP). A primeira pressupõe que um determinado nó solicita ao nó a jusante uma etiqueta para uma dada FEC, enquanto que a segunda técnica compreende o envio da informação proveniente da atribuição de etiquetas por parte do nó a jusante, sem que exista um pedido explícito da mesma por parte do nó mais a montante [15].

Contudo, é necessário ter em conta que em ambos os casos os nós que negoceiam as etiquetas devem chegar a acordo no que diz respeitos às etiquetas a utilizar.

2.5.3 Modo de controlo da distribuição de etiquetas

Os nós de um domínio MPLS possuem duas formas distintas para a atribuição das etiquetas locais, de forma independente (*Independent LSP Control*) ou de forma ordenada (*Ordered LSP Control*) [4].

No modo ordenado os nós do domínio MPLS apenas criam a associação etiqueta-FEC se reconhecerem que são nós de saída (*egress* LER), ou se receberem essa informação proveniente do nó *downstream*, ou seja, do nó a jusante.

O modo independente assume que um LER ou LSR pode criar uma associação etiqueta-FEC de forma independente, sem recorrer a informação proveniente de outro nó. Esta especificidade acontece quando um determinado nó tem conhecimento de uma FEC específica, isto é, mal essa informação lhe seja transmitida por via do protocolo de *routing*. Ou seja, de cada vez que um determinado prefixo de rede é adicionado na tabela de rotas desse nó, ele automaticamente pode criar uma etiqueta para essa FEC.

A desvantagem de utilização deste modo advém do facto de que um LER pode iniciar a comutação de pacotes antes que o LSP esteja construído na totalidade, e assim o pacote pode ser comutado sem os requisitos pretendidos ou mesmo perdido [26].

2.5.4 Modo de retenção de etiquetas

A classificação do modo de retenção de etiquetas divide-se no modo liberal e no modo conservativo, e diz respeito à forma de como os nós do domínio MPLS guardam a informação de cada etiqueta correspondente a cada FEC.

No modo de retenção liberal, toda a informação relativa a etiquetas proveniente dos nós vizinhos é armazenada na LIB, sendo posteriormente escolhida para cada FEC uma determinada etiqueta para que o pacote seja comutado. A etiqueta escolhida é denominada como *active label* e é armazenada na tabela de comutação (LFIB).

O LDP é um caso de utilização do modo liberal. Este protocolo prevê que um nó MPLS receba etiquetas de todos os nós adjacentes que tenham uma rota para uma determinada FEC. Todas estas etiquetas serão armazenadas na LIB, mas apenas uma se torna ativa e consta na LFIB. Este aspeto é fundamental numa situação de falha, uma vez que no caso de uma alteração topológica, a escolha de um novo caminho é quase imediata, uma vez que a etiqueta para um novo vizinho já se encontrará guardada na LIB.

O modo conservativo é diferente do modo liberal, uma vez que as etiquetas presentes na LIB são exatamente as mesmas que se encontram na LFIB. Este modo de retenção apresenta como vantagem a economia de recursos de memória dos nós MPLS.

Da mesma forma que o LDP é um exemplo do modo liberal, o protocolo RSVP-TE é um exemplo do modo conservativo. Uma vez que utiliza o modo de distribuição *downstream on-demand*, a única etiqueta que um nó recebe para uma FEC provém do nó mais a jusante para essa FEC, e assim sendo não existem etiquetas "secundárias" para essa FEC [27].

2.6 Serviços MPLS

Ao longo dos anos, diversas tecnologias foram desenvolvidas com o intuito de fornecer diferentes serviços de telecomunicações, tal como o ATM para serviços de redes privadas e o IP para serviços de dados do tipo *best-effort*. Com isto, os fornecedores de serviços foram levados a implementar várias infraestruturas de rede, uma para cada tipo de serviço, o que conduziu a uma maior divergência das redes de telecomunicações, que compreendia automaticamente custos de manutenção mais elevados [27].

O MPLS surge com a necessidade da convergência das redes de telecomunicações, tendo como principal objetivo o fornecimento de serviços de redes privadas virtuais (VPNs). Podemos definir informalmente VPNs, como redes que se estendem por diversos locais (cidades por exemplo) com capacidade de comunicação entre si, ou de uma forma mais formal um conjunto de políticas administrativas que controlam a comunicação e a qualidade de serviço [28].

Atualmente, o MPLS suporta uma variedade de serviços de transporte, que são disponibilizados pelos ISP's (*Internet Service Providers*), tais como [29]:

- *Virtual Leased Line* (VLL): também comummente referido como *Virtual Private Wire Service* (VPWS). Define o fornecimento de serviços ponto-a-ponto capaz de transportar tráfego do cliente entre dois locais;
- *Virtual Private LAN Service* (VPLS): corresponde a um serviço *Ethernet* multiponto idêntico a uma *switch Ethernet*, capaz de estender um serviço por vários pontos geograficamente distribuídos;
- *Virtual Private Routed Network* (VPRN): disponibiliza um serviço multiponto IP capaz de encaminhar tráfego do cliente ao longo de vários locais, sendo que as rotas desses locais são distribuídas entre todos os locais inerentes ao serviço. O serviço VPRN apresenta topologias requeridas pelos clientes, tais como:

- *Intranet*: esta topologia refere a base do VPRN, ou seja, a disponibilização de um serviço multiponto IP ao longo de diferentes *sites* do cliente;
- *Extranet*: providencia a partilha de redes entre diferentes clientes, mas também permite o isolamento daquelas que o cliente indicar;
- *Overlay VPN*: topologia utilizada no caso de os clientes pretenderem ter acesso à *Internet* a partir de alguns dos seus *sites*, enquanto que outros se encontram isolados no que diz respeito ao acesso à Internet;
- *Hub-Spoke VPN*: para clientes que possuem um ponto central de comutação, e pretendem que todo o tráfego proveniente dos diferentes locaus consumam recursos disponibilizados centralmente.

A Tabela 6 resume os tipos de serviço MPLS classificados segundo a taxionomia apresentada.

Tabela 6 – Tipos de serviço MPLS [6]

Descrição	Camada OSI	Multiplicidade de operação	Implementação de túneis exteriores	Implementação dos túneis interiores
VPRN	3	Multiponto	LDP, RSVP, MP-BGP	*Pseudowires* MPLS ou túneis IP
VPWS	2	Ponto-a-ponto	LDP, RSVP	*Pseudowires* MPLS ou túneis IP
VPLS	2	Multiponto	LDP, RSVP	*Pseudowires* MPLS ou túneis IP

Tendo em conta o contexto atual de disponibilização de serviços pela Universidade do Porto, que se baseia em serviços de nível 2, o próximo subcapítulo apresenta o conceito de *pseudowire* de forma a introduzir o funcionamento dos serviços VPLS e VPWS.

2.6.1 Pseudowire ethernet

O conjunto de serviços apresentados aglomera um outro conceito que importa salientar e que é parte integrante da arquitetura de serviços MPLS, isto é, o *pseudowire Ethernet* [30]. Este conceito descreve um mecanismo que simula os atributos de um circuito de telecomunicações, como a não partilha do meio e a entrega ordenada de tramas [6]. Apesar de focar apenas os atributos do *pseudowire Ethernet*, importa salientar que os serviços de transporte MPLS, pressupõem a existência de túneis interiores de acordo com as tecnologias de acesso a transportar, tais como o ATM, *Ethernet*, *Frame Relay* e TDM (*Time Division Multiplexing*), uma vez que para cada serviço é criado um circuito virtual (VC – *Virtual Circuit*) capaz de

emular um circuito dedicado sobre a rede de comutação de pacotes (PSN – *Packet Switched Network*) [31].

A arquitetura do *pseudowire* é elementar para a perceção do funcionamento dos serviços capazes de serem fornecidos pelo MPLS. Para o entendimento desta arquitetura, deve-se ter em consideração os elementos apresentados na Figura 9, onde se encontram definidos dois PE's (*Provider Edge*) sendo que cada um destes se interliga a um CE (*Customer Edge*) a partir do AC (*Attachment-Circuit*). Cada PE é responsável pelo fornecimento de *pseudowires* ao CE, de forma a que estes se comuniquem através da PSN, que representa o caminho do *pseudowire*. As unidades de informação originadas na rede do cliente (*bits*, células, pacotes) que são recebidos pelos PE's, são encapsulados numa PW-PDU (*Pseudowire PDU*), que representa o conjunto de informações de controlo e de dados necessários para emular o serviço desejado, e são transportados através do túnel PSN num *pseudowire*. Assim que os dados são recebidos pelo segundo PE, o PW-PDU é desencapsulado e os dados são entregues ao CE.

Posto isto, pode-se aferir que o *pseudowire* é responsável pelas funcionalidades mínimas capazes de emularem um "fio" com a fiabilidade necessária para o funcionamento de um serviço. Estas funcionalidades subentendem nomeadamente:

- Encapsular as tramas que provêm do terminal do cliente e adaptadas ao *pseudowire* a partir do PE;
- Transportar os dados encapsulados sobre o túnel PSN;
- Estabelecer o *pseudowire*, incluindo a troca e distribuição dos identificadores de *pseudowire* entre os terminais do túnel PSN;

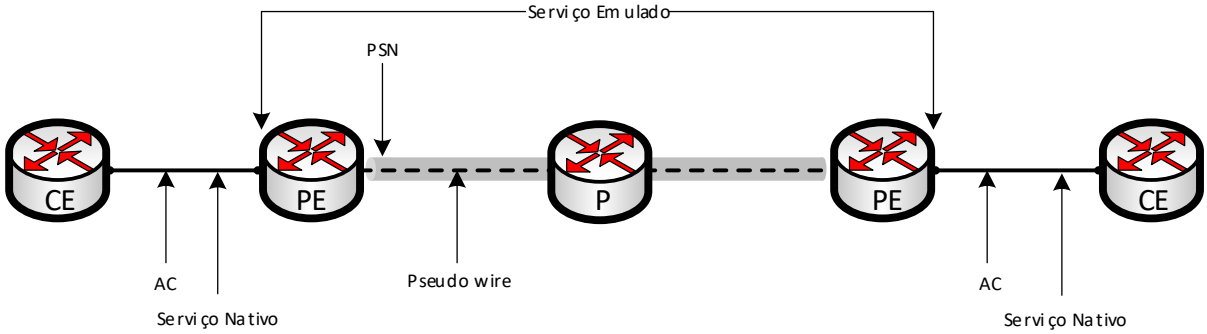

Figura 9 – Arquitetura do *pseudowire* [30]

No procedimento de encapsulamento, encontra-se ainda incluído a adição de informação de controlo (*control word*), cuja principal função é garantir a entrega ordenada das tramas, e um

identificador único por *pseudowire*, criado através da sessão estabelecida entre os dois PE's onde o *pseudowire* é formado. Este último parâmetro permite que num mesmo túnel PSN sejam formados vários *pseudowires*.

As vantagens relevantes na utilização dos *pseudowires* prendem-se com a demarcação entre a rede do cliente e a rede do fornecedor de serviços, o que permite ao fornecedor a expansão do serviço sem interrupção do mesmo, bem como o transporte de diferentes tecnologias como já referido.

2.6.2 Serviços nível 2

Os serviços de nível 2 intrínsecos ao MPLS baseiam-se nas arquiteturas VLL e VPLS, possibilitando estas serviços ponto-a-ponto e multiponto, respetivamente. Pode-se pensar no VPLS como o último estado de evolução dos serviços de nível 2 do MPLS, sendo por isso de elevada importância abordar este tipo de arquitetura.

Como referido anteriormente, este serviço tem como objetivo a extensão de serviços *ethernet* através de pontos geograficamente distribuídos (Figura 10), sendo toda a informação transportada através de *pseudowires*, também designados como túneis interiores. Cada *pseudowire* tem duas etiquetas MPLS associadas, uma por cada sentido da interligação entre o par de PE's em causa, negociadas no contexto das sessões inerentes aos protocolos de sinalização. Neste contexto, as etiquetas MPLS atribuídas a cada FEC denominam-se PW-*label*.

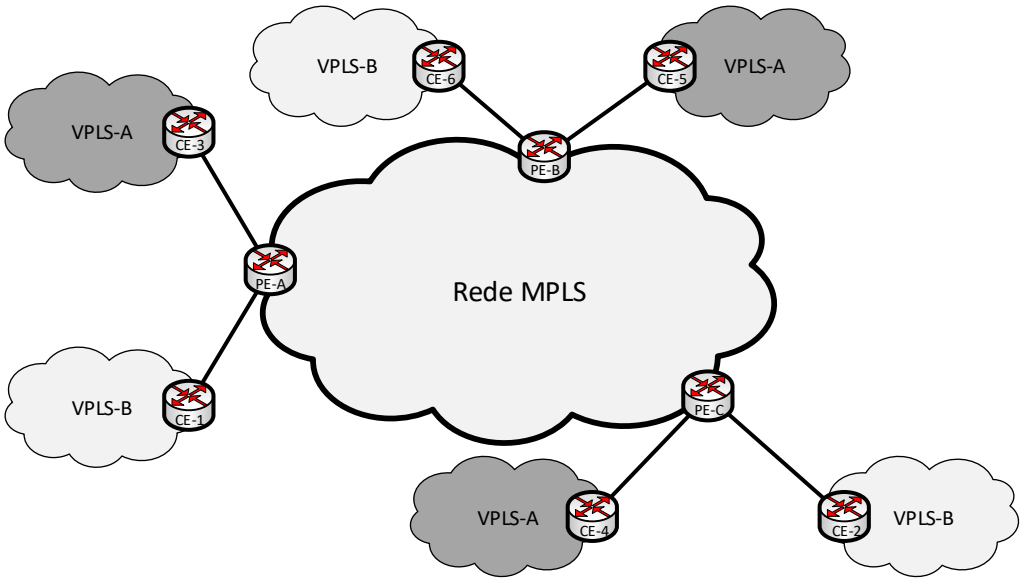

Figura 10 – Arquitetura VPLS (1)

De forma a possibilitar o acesso a um serviço *ethernet* transparente aos CEs, por cada instância VPLS os PE's deverão ser capazes de realizar um conjunto de operações semelhantes às que se associam aos comutadores *ethernet* comuns, nomeadamente: MAC (*Media Access Control*) *learning* (aprendizagem de endereços MAC), MAC *aging* (descarte por envelhecimento de endereços MAC) e encaminhamento de tramas. Estas operações deverão estar presentes em pelo menos duas das interfaces de cada PE, a de interligação com o CE (que representa o *attachment-circuit*) e a que liga ao núcleo MPLS (o *pseudowire*). Esta última interface faz uso de uma nova entidade de forma a realizar a associação entre endereços MAC e *pseudowires*, denominada *Virtual Switching Instance* (VSI) [32]. Assim, cada PE fica habilitado a encaminhar corretamente as tramas recebidas de cada CE.

Segundo o exemplo representado através da Figura 11, é possível analisar o percurso de uma trama desde que é emitida pelo CE 1, até que é recebida pelo CE 2. O processo remonta para o nó PE A, que recebe uma trama inicialmente transmitida por M1, e através do *attachment-circuit* onde o PE recebe a trama, este determina qual a instância VPLS a que pertence, bem como regista o endereço MAC de M1 para o AC no qual recebeu a trama.

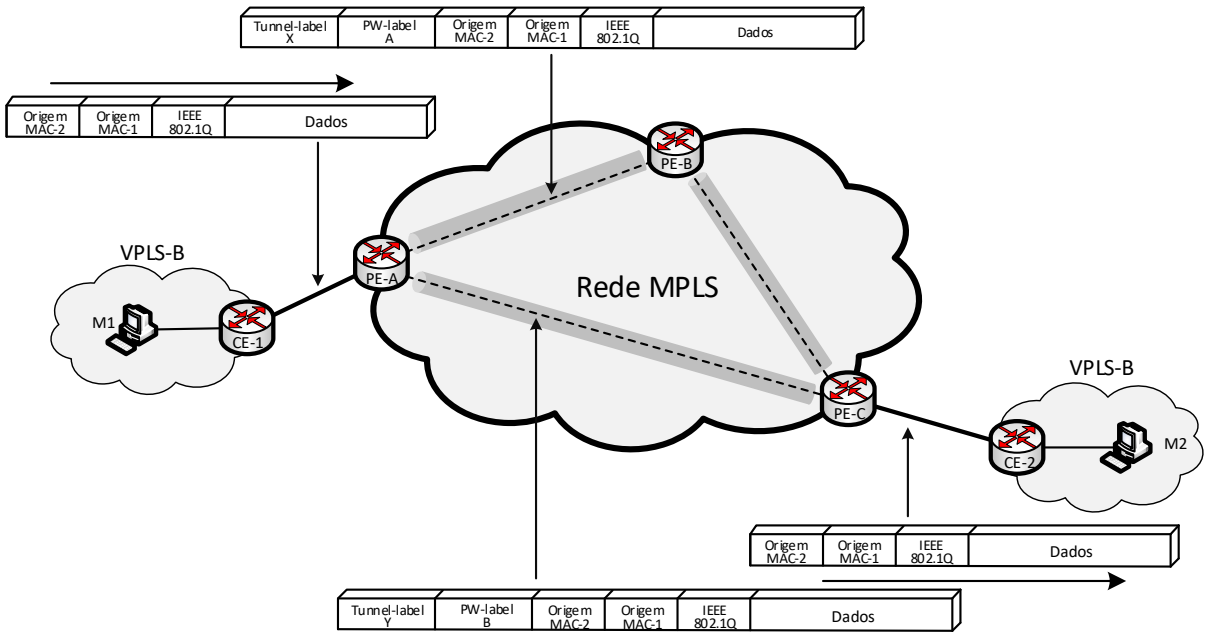

Figura 11 – Arquitetura VPLS (2) [6]

No caso em que o PE de destino não é conhecido, a trama tem de ser replicada por todos os *pseudowires* associados à instância VPLS em causa. À trama original é adicionada a etiqueta que identifica o *pseudowire* (PW-*label*), e ainda a etiqueta que identifica o LSP ao qual o PE se está a ligar (*tunnel-label*). Apesar do serviço ser multiponto, cada LSP é estabelecido ponto-

a-ponto e unidireccionalmente, pelo que a trama é transmitida através de um LSP para o PE B e outro para o PE C.

Posto isto, os nós da nuvem MPLS iniciam o processo de comutação de etiquetas (*label swap*) apenas com base na etiqueta associada ao LSP, uma vez que as etiquetas relacionadas com os *pseudowires* estão apenas sob o conhecimento dos PE's. Tendo como base a tecnologia *ethernet* como método de comutação, novos pares de endereços MAC (origem e destino) serão adicionados à trama, tendo esta a estrutura apresentada na Figura 12.

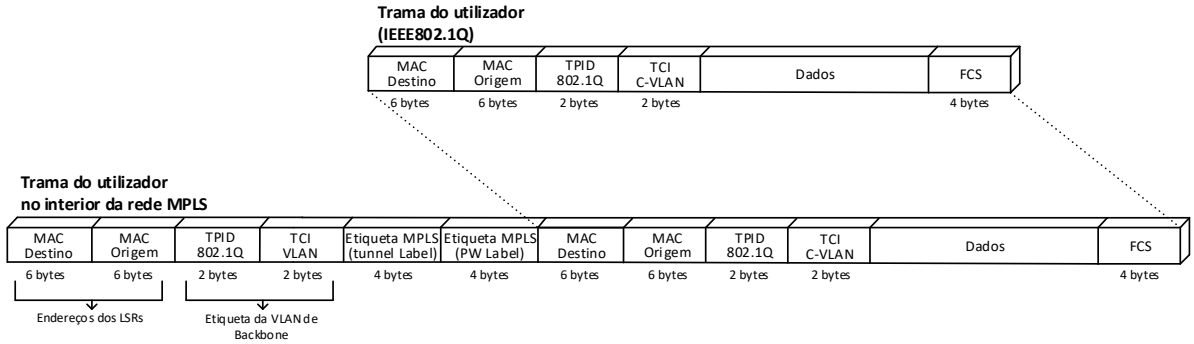

Figura 12 – Estrutura da trama *ethernet* no núcleo da rede MPLS [6]

Após a receção da trama por parte dos PE's B e C, estes realizam o processo de desencapsulamento por ordem inversa, e retiram a etiqueta exterior (alusiva ao LSP), analisam a etiqueta interior (PW-*label*) de forma a determinar a instância VPLS a que a trama pertence, e associam o endereço MAC de origem (pertencente a M1) ao *pseudowire* onde receberam a trama (processo de MAC *learning*).

Uma vez que os PE's B e C não conhecem o AC onde o endereço MAC de M2 se encontra, replicam a trama por todos os *attachment-circuits* que pertençam à instância VPLS em causa. Desta feita, M2 irá receber a trama e irá transmitir uma resposta com destino a M1. Por sua vez, o PE C irá associar o endereço MAC de M2 ao AC em questão, e tendo já realizado o processo de aprendizagem do endereço MAC de M1 anteriormente, irá enviar a trama unicamente através do LSP para o PE A. Finalmente, o PE A recebe a trama, desencapsula-a e entrega-a diretamente através do *attachment-circuit* ao qual M1 está ligado.

Pesquisas sobre os serviços VPLS constataram que soluções baseadas no serviço que aglomerem um elevado número de PE's apresenta bastantes problemas no que diz respeito aos recursos necessários para manter informação sobre túneis e endereços MAC. Este aspeto levou ao desenvolvimento do modelo VPLS hierárquico, que reduz as necessidades de sinalização e replicação de tramas em redes de elevada dimensão. Dada a dimensão do presente projeto de

dissertação este tema não tem interesse em ser debatido, no entanto fica a nota para um problema a ser estudado [33].

2.6.3 Serviços nível 3

Os serviços de nível 3 MPLS baseiam-se na arquitetura VPRN (*Virtual Private Routed Network*) que consiste no fornecimento de um serviço de *routing* multiponto, definido pela RFC 4364. Intrínseco a estes serviços encontra-se o fornecimento de uma interface de nível 3 como ponto de acesso ao serviço, disponibilizada ao cliente para maior flexibilidade e acesso a técnicas tais como qualidade de serviço e *accounting*. Esta técnica é nomenclada por *Internet Enhanced Service*, e como acontece nas redes IP tradicionais, os clientes podem fazer uso destas interfaces IES como *neighbors* para protocolos como OSPF e BGP.

Existem quatro definições fundamentais para entender o funcionamento dos serviços VPRN, nomeadamente VRF (Virtual Route Forwarding), Route Distinguisher (RD), Route Target (RT) e MP-BGP (*Multiprotocol* BGP).

- VRF – Representa um *router* virtual por cada instância de serviço VPRN disponibilizada em cada PE;
- Route Distinguisher – Trata-se de uma *string* adicionada às rotas do cliente para que estas possam ser distinguidas de outros clientes na rede do operador. Esta *string* é constituída por 8 *bytes* que são adicionados ao prefixo IPv4, criando-se assim um prefixo VPN conhecido por endereço VPN-IPv4;

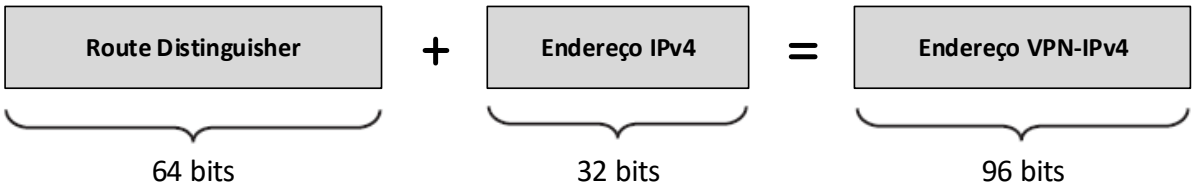

Figura 13 – Construção do endereço VPN-IPv4

- Route Target - Representa uma *string* utilizada para identificar que rotas são legíveis para exportação por via do MP-BGP, para uma determinada VRF;
- MP-BGP – Representa uma extensão do protocolo BGP capaz de suportar a família de endereços VPN-IPv4, ou seja, endereços de 12 *bytes*.

Em termos de operação sobre os dados do cliente, o tratamento efetuado em VPRN é bastante similar ao oferecido em serviços de nível 2, pois ao atingirem um nó PE são encapsulados por recurso a duas etiquetas MPLS (a etiqueta de serviço e etiqueta de transporte). No entanto, ao contrário do que sucede nos serviços de nível 2, a informação de *layer* 2 é removida, sendo encapsulado o pacote IP, o que pressupõe que a decisão de encaminhamento se encontra do lado do PE. Se nos posicionarmos do ponto de vista do cliente, o PE apresenta-se como um *router* IP tradicional, mas do ponto de vista do operador trata-se de um *router* IP virtual.

Outra diferença comparativamente aos serviços de nível 2 diz respeito à propagação das rotas do cliente sobre a VPRN. Isto permite que as rotas do cliente sejam distribuídas para vários *sites* do cliente, permitindo também que as decisões de encaminhamento de cada PE sejam baseadas na informação de *routing* do cliente. A Figura 14 apresenta as três interações no momento de propagação de rotas: CE → PE, PE → PE e PE → CE.

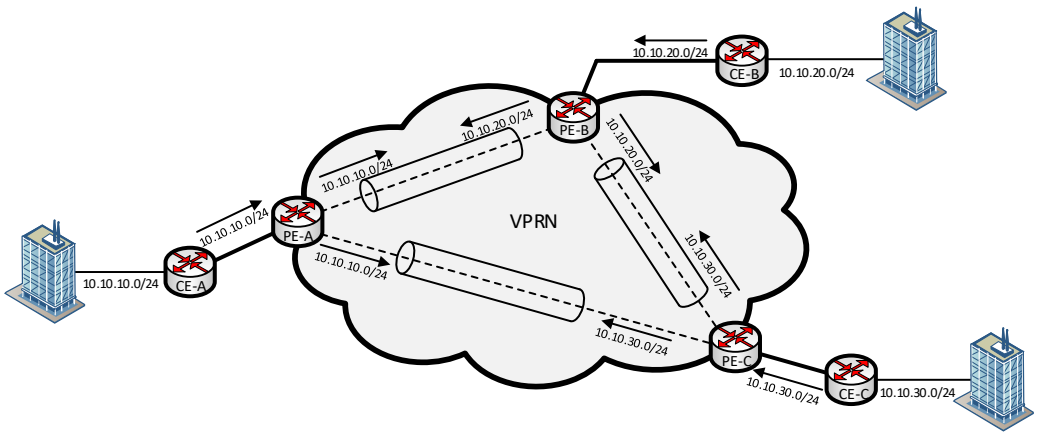

Figura 14 – Propagação das rotas do cliente em VPRN

Na primeira interação (CE → PE), o *router* CE interliga-se ao *router* PE com o objetivo de trocar informação de *routing* dos clientes. Esta troca de informação recorre à utilização de protocolos dinâmicos de *routing*, tais como BGP, OSPF e RIP entre os nós CE e PE, apesar de ser obviamente possível, em cenários mais simples, a utilização de rotas estáticas. Nos *routers* PE a informação é mantida numa instância VRF, criada e associada a cada serviço VPRN.

Uma vez transmitidas as rotas do cliente para os PE's, estes começam a propagá-las entre si por recurso ao MP-BGP, aliado às *route targets* (PE → PE). Através destes é possível transmitir as rotas de uma dada instância VRF, única e exclusivamente para os nós (PE) que também estão associados a esta instância.

Por fim, na última interação do processo de propagação de rotas (PE → CE), os nós PE realizam a redistribuição de rotas aprendidas na segunda interação para o equipamento do cliente.

Na implementação de serviços VPRN, devemos ter em consideração a existência de condições técnicas e físicas ao nível da infraestrutura do cliente. Estes serviços têm um *overhead* significativo quer ao nível da gestão e operação da rede, como também ao nível dos custos de investimento, uma vez que obriga à existência de um *router* como equipamento de acesso [34].

Apesar dos serviços de nível 2 apresentarem maior eficácia no processo de comutação, estes também conduzem a problemas como *broadcast storms*, o que não acontece em serviços de nível 3 [35].

Um aspeto a ter em conta por parte do cliente na escolha do serviço remete para a partilha de informação acerca da sua topologia de rede, que acontece nos serviços de nível 3. Enquanto que nos serviços de nível 2 o cliente tem total controlo sobre as políticas de *routing*, nos serviços de nível 3 é o operador a definir as mesmas.

2.7 Engenharia de tráfego

Os protocolos dinâmicos de *routing* surgiram de forma a responder à questão "qual o melhor caminho?", sendo esta preferencialmente respondida com base na largura de banda disponibilizada por circuito. Com isto, as redes *backbone* podem debater-se com problemas de latência sobre caminhos de maior largura de banda, o que pode significar desperdício de recursos, resultado de tráfego elevado em algumas ligações enquanto que outras poderão encontrar-se em situação de subutilização [36]. A Figura 15, ilustra um caso concreto onde todo o tráfego com destino a R5 segue o mesmo caminho, encontrando-se a ligação R1-R2-R5 a servir apenas como "*backup*".

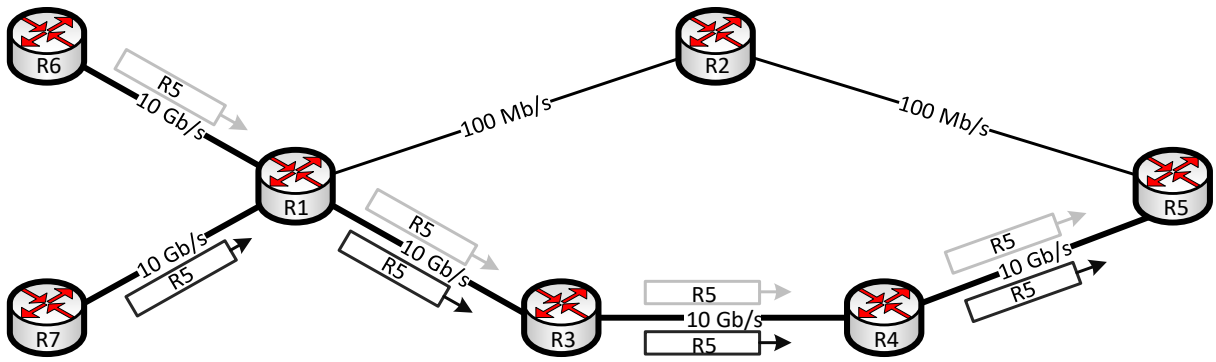

Figura 15 – *Routing* IP tradicional

A solução para este problema passa pela utilização do conceito *explicit routing*, que consiste na formação de caminhos explícitos, podendo o tráfego ser comutado numa rede MPLS-TE (MPLS – Traffic Engineering) com base na origem, e não apenas com base no endereço de destino, como sucede com o *routing* IP tradicional. Desta forma é possível definir, por exemplo, que o trajeto do tráfego de R6 para R5 será R6-R1-R2-R5, enquanto que o caminho de R7 para R5 será R7-R1-R3-R4-R5 (ver Figura 16).

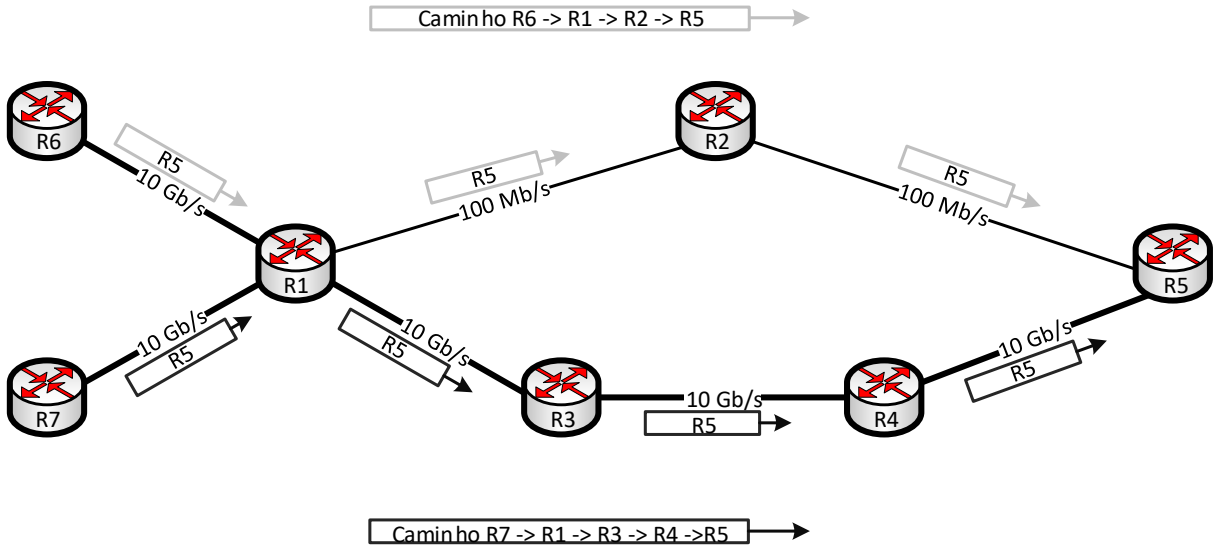

Figura 16 – *Routing* explícito

Verifique-se que ambos os caminhos têm um nó convergente, R1, o qual analisa a origem do tráfego de forma a comutá-lo conforme as configurações de engenharia de tráfego. Além da funcionalidade de criação de rotas explicitas, que aumenta a eficiência das redes *backbone* através do mapeamento dos recursos, a engenharia de tráfego oferece também uma solução para proteção, denominada por *Fast Reroute*.

2.7.1 Protocolo RSVP

O RSVP é o protocolo utilizado quando existem requisitos de engenharia de tráfego ou qualidade de serviço. A partir deste é possível a definição manual de LSP's extremo-a-extremo, indicando os nós pelo qual o pacote vai ser comutado desde o nó *ingress* até ao nó *egress* [25].

Originalmente, este protocolo foi desenvolvido de forma a fornecer aos *hosts* a capacidade de requisitar qualidade de serviço para fluxos de dados numa dada rede. Rapidamente se entendeu que esta funcionalidade teria vantagens ao ser utilizada por *routers*, sendo que os mesmos adquiriram a capacidade de reservar recursos numa rede conforme solicitações de QoS (*Quality of Service*), de forma a garantir níveis de serviço exigidos pelos clientes [27].

Mais tarde, o RSVP foi otimizado de forma a fornecer funcionalidades de engenharia de tráfego passíveis de utilização em redes MPLS. Apesar da funcionalidade principal basear-se na sinalização de um LSP à escolha, este pode também ser usado para sinalizar LSP's que incluam ou não opções de resiliência, largura de banda ou outras opções [25].

2.7.2 Proteção

A engenharia de tráfego intrínseca às redes MPLS, garante técnicas de proteção de rede capazes de minimizar as perdas de serviço causadas, por exemplo, pela falha de uma ligação ou de um nó. Do ponto de vista do operador de telecomunicações, a resiliência de uma rede é um aspeto crítico e determinante para o cumprimento do SLA (*Service Level Aggrement*) acordado com os clientes.

Enquanto que os IGP's são reativos, ou seja, apenas implementam técnicas de restauro que calculam um novo caminho quando detetam uma falha no caminho em operação, o MPLS com engenharia de tráfego, isto é, associado ao RSVP-TE garante funcionalidades tais como a criação de caminhos secundários e *Fast Reroute*, adquirindo-se assim um nível de proteção proactiva e preditiva.

Assim sendo, a sinalização por RSVP oferece dois níveis de proteção, a proteção extremo-a-extremo garantida pela criação de um LSP secundário, e a proteção local com a integração do *Fast Reroute*. É importante salientar que estes níveis de proteção podem ainda atuar em conjunto, sendo que em primeiro lugar ocorre a proteção local e posteriormente a proteção extremo-a-extremo.

Proteção extremo-a-extremo

O primeiro mecanismo de resiliência garantido pelo RSVP pressupõe a criação de um LSP's secundário, o qual pode ser sinalizado no momento da sua criação, ou apenas no momento de falha do LSP primário, situação que obviamente aumenta o tempo de recuperação do circuito.

Com a criação de LSP's secundários, o administrador da rede deverá ter em conta os *hops* do caminho primário, sendo que idealmente o caminho secundário não deverá ter nenhum nó ou ligação partilhada com o caminho primário. Esta gestão torna-se mais dificultada se um dos caminhos for proveniente do IGP, criando-se o risco de se perder o controlo do tráfego, sendo que neste caso se pode utilizar em contrapartida um caminho primário e secundário a partir de caminhos explícitos.

Na Figura 17, podemos analisar um caso concreto de criação de um caminho primário protegido por um caminho secundário, ambos explícitos.

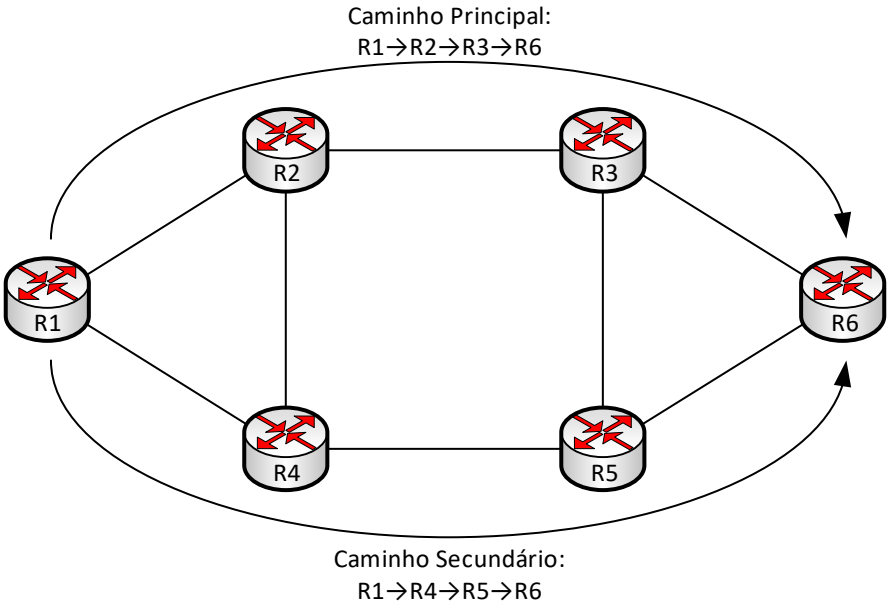

Figura 17 – Proteção extremo-a-extremo (1)

Neste exemplo, verifica-se que uma falha no caminho principal não afeta o caminho secundário uma vez que estes não partilham qualquer nó ou ligação. Para análise de uma situação de falha, considere-se a Figura 18, que representa a falha do *link* entre R3 e R6.

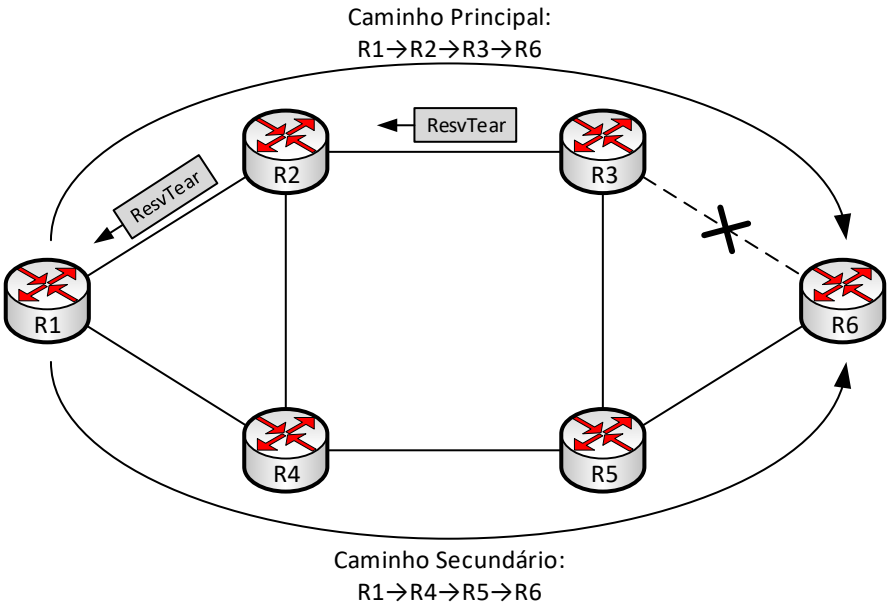

Figura 18 – Proteção extremo-a-extremo (2)

Com a falha do *link* entre R3 e R6, o nó a montante da falha (R3) envia uma mensagem RESV *tear* para o nó mais a montante do LSP (R1), e por consequência este comuta o tráfego para o caminho secundário, que já se encontrava previamente sinalizado. Para situações em que o caminho secundário não esteja já sinalizado, o nó mais a montante teria de sinalizar o caminho e apenas depois poderia encaminhar tráfego por esse LSP.

Este tipo de proteção apresenta, contudo, um nível de serviço questionável uma vez que podem acontecer situaçãoes de elevada perda de pacotes, nomeadamente enquanto o nó mais a montante não comuta o tráfego para o LSP secundário. É importante ainda salientar que a técnica de proteção extremo-a-extremo é uma medida de utilização duvidável mormente em cenários topologicamente complexos.

Proteção local

A proteção local, ou *Fast Reroute* (FRR), consiste numa solução que prevê tempos de recuperação de falha na ordem dos 50 milissegundos, e que não depende da quantidade de nós da rede ou da localização específica da falha. A rápida comutação baseia-se no conceito de proteção local, pois a "reparação" do LSP é realizada a montante da falha, e não a montante do LSP como acontece na proteção extremo-a-extremo.

O *Fast Reroute* pressupõe alguns conceitos a ter em conta, tais como:

- LSP Protegido – O LSP primário protegido pela proteção local;
- LSP Protetor – Um LSP que protege o LSP protegido. O LSP protetor é pré-sinalizado para minimizar interrupções de tráfego;
- Ponto de Reparação Local (*Point of Local Repair* – PLR) – Representa o nó a montante da falha responsável por encaminhar o tráfego para o LSP protetor;
- Ponto de Convergência (*Merge Point* - MP) – O ponto em que o tráfego do LSP protetor converge novamente com o LSP protegido.

A vantagem de utilização do *Fast Reroute* remete para o facto do LSP Protetor ser sinalizado no momento de criação do LSP, o que permite solucionar rapidamente situações de falha, uma vez que se encaminha o tráfego para o LSP protetor de imediato.

O *Fast Reroute* compreende dois métodos de proteção distintos, o *one-to-one backup* e o *facility backup*. Estas técnicas apresentam diferenças significativas em termos de escalabilidade de acordo com o modo de operação, pelo que se torna necessário analisar o seu funcionamento.

O primeiro método é denominado por *one-to-one* uma vez que os túneis de proteção são estabelecidos para cada LSP, e nunca partilhados entre LSP's protegidos, o que numa rede de elevada dimensão pode resultar num problema de escalabilidade. Neste método, cada PLR tem como função encaminhar o tráfego até ao último nó do LSP utilizando para isso o menor trajeto possível.

A Figura 19 ilustra um exemplo de funcionamento do método *One-to-One*, onde se verifica que o nó a montante da falha (R2), encaminha o tráfego por um LSP protetor calculado através do menor caminho possível.

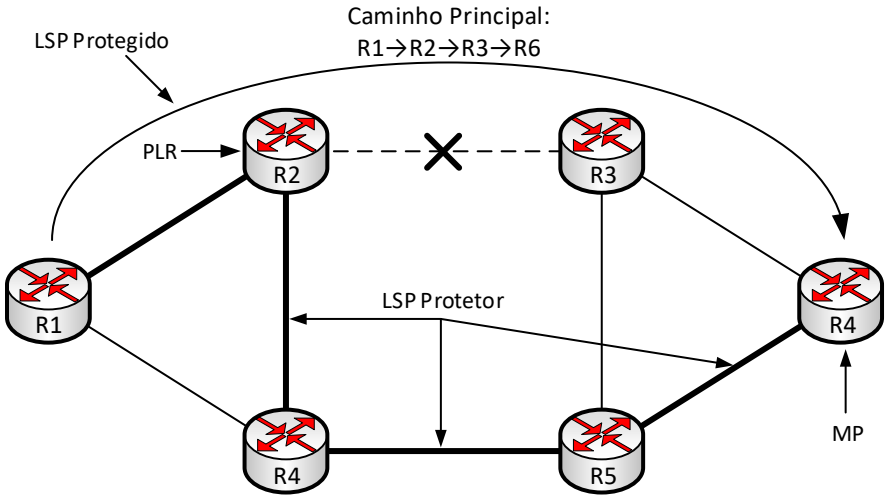

Figura 19 – *Fast reroute one-to-one*

O segundo método denominado por *facility backup* garante maior escalabilidade pelo facto de que um único LSP protetor pode proteger vários LSP's. Além disso, este método ao contrário do anterior, cria túneis com vista a atingir o nó a *downstream* da falha, respeitando o restante caminho definido no LSP.

A Figura 20 apresenta um exemplo de funcionamento do método *facility backup*, onde se pode verificar as diferenças existentes para com o método anterior. Com este método, o PLR (R2) comuta o tráfego por um LSP protetor até ao nó a *downstream* da falha (R3), respeitando-se o LSP principal.

Apesar dos exemplos apresentados remeterem para a proteção de ligação, o *fast reroute* compreende também a solucionar falhas de nó, ou seja, situações em que o nó a jusante (*downstream*) falha.

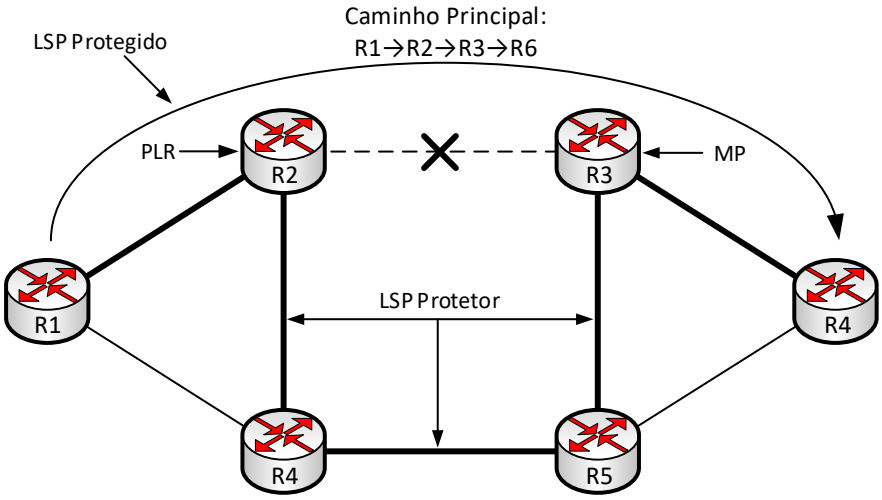

Figura 20 – *Fast reroute facility*

Quando o *Fast Reroute* é despoletado no momento de criação do LSP, cada PLR é responsável por criar um conjunto de caminhos alternativos, de preferência, na sequência de uma possível falha do nó *downstream* pois desta forma abrange simultaneamente as ligações *downstream* (Figura 21). Em situações que não seja possível criar um caminho alternativo ao nó *downstream*, o PLR apenas forma um caminho alternativo à falha de *link*.

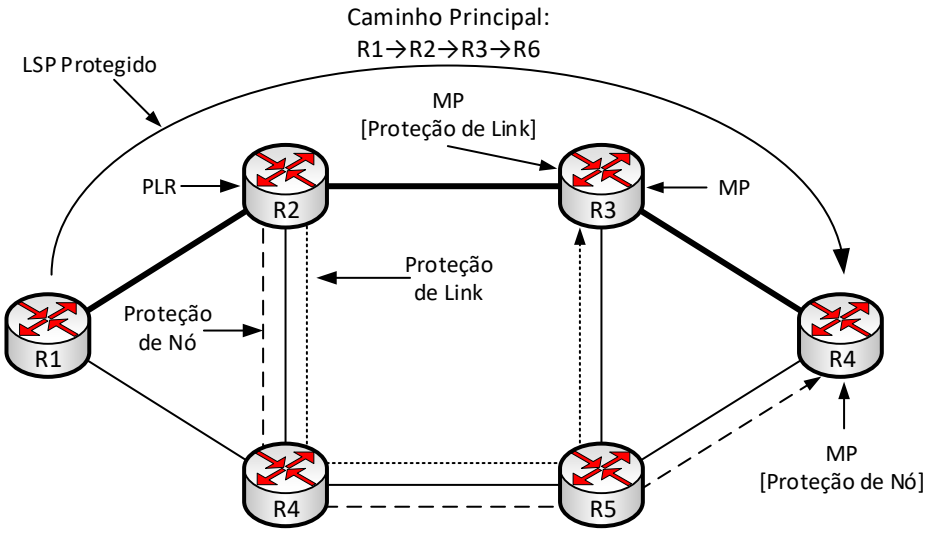

Figura 21 – Proteção de *link* vs. proteção de nó

LAG e MC-LAG

Apesar do MPLS contemplar a proteção da rede de *backbone* é igualmente importante abordar as técnicas de redundância passíveis de utilização na rede de interligação com o cliente, nomeadamente o LAG (*Link Aggregation Group*) e o MC-LAG (*Multi-Chassis* LAG).

O LAG é constituido por um conjunto de portas associadas numa só interface lógica, cujo principal objetivo visa o aumento de largura de banda, o aumento da flexibilidade e a redundância de ligações entre dois equipamentos, protegendo a ligação no caso da ocorrência de falhas [37].

O MC-LAG, do ponto de vista da rede de acesso, visa a criação de uma interface lógica LAG ligada a dois equipamentos físicos distintos, protegendo-se assim da quebra de ligações e da falha de nós adjacentes. Por outro lado, do ponto de vista da rede de transporte, a implementação do MC-LAG visa a criação de uma interface lógica LAG distribuída por dois nós distintos [38].

A Figura 22 apresenta o esquema de proteção entre a rede de operador e a rede de cliente através das técnicas de LAG e MC-LAG.

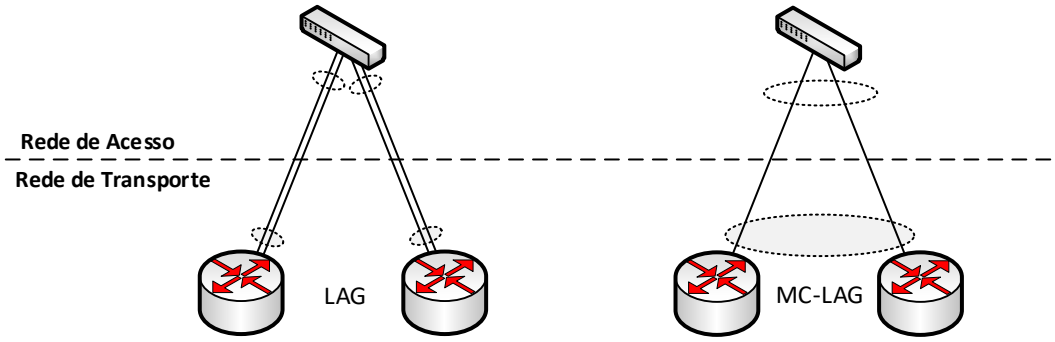

Figura 22 – LAG e MC-LAG

2.8 Qualidade de serviço

O funcionamento da *Internet* é baseado no protocolo IP, o que corresponde a uma uniformização ou inexistência da qualidade de serviço, onde todos os pacotes são tratados de igual forma, independentemente de encapsularem aplicações em tempo real ou não. Em situações de congestionamento, os pacotes acabam por ser descartados de forma indiscriminada, facto que acaba por afetar o correto funcionamento de alguns serviços, perdendo-se a garantia dos mesmos [39].

Com as necessidades impostas pelos clientes e pelas aplicações, e devido à convergência nas redes de transporte onde todo o tipo de tráfego é transportado, foi necessário atuar com uma arquitetura de qualidade de serviço capaz de garantir tratamento diferenciado. Com isto, entende-se a capacidade de tratar diferentes tipos de tráfego, mediante múltiplos critérios e prioridades [40].

Atualmente, os fornecedores de serviço são capazes de capacitar as redes de transporte MPLS com qualidade de serviço. O IETF (*Internet Engineering Task Force*) define duas arquiteturas para implementação de qualidade de serviço, são elas a arquitetura de serviços integrados (*IntServ*) e a arquitetura de serviços diferenciados *(DiffServ*) [41].

2.8.1 Serviços integrados

O modelo de serviços integrados, definido pelo RFC 1633 [42], tem o propósito de providenciar qualidade de serviço a fluxos individuais de pacotes através da garantia de largura de banda e latência reduzida, tendo por base um protocolo para reserva de recursos (RSVP) [43]. O RFC 1633 propõe a utilização de duas classes de serviço, além do serviço *best-offer* já inerente ao IP [44]:

- *Guaranteed Service*: utilizado para aplicações que necessitam de garantias quanto ao atraso, não devendo o mesmo ultrapassar um valor pré-definido;
- *Controlled-Load Service*: para aplicações que são tolerantes a perdas ocasionais de pacotes. Fornece qualidade de serviço equivalente a uma rede sem congestionamento;

Este modelo compreende ainda quatro componentes fundamentais para a entrega da qualidade de serviço, sendo estes o protocolo de sinalização, o controlo de admissão, o classificador, e por fim o escalonador de pacotes.

- Protocolo de Sinalização: necessário para criar, e manter, um determinado fluxo de dados entre todos os nós que o mesmo fluxo percorre;
- Controlo de Admissão: representa o algoritmo de decisão utilizado pelos nós de rede para determinar se um novo fluxo de dados pode receber garantias de qualidade de serviço, sem que garantias anteriores sejam afetadas;
- Classificador: para fins de controlo de tráfego, cada pacote de entrada deve ser mapeado numa classe, sendo que todos os pacotes de uma classe recebem o mesmo tratamento proveniente do algoritmo de escalonamento. A associação pacote-classe é realizada pelo classificador;
- Escalonador de Pacotes: realiza a gestão do encaminhamento de diferentes pacotes utilizando um conjunto de filas, ou outros mecanismos como temporizadores. É utilizado no momento em que os pacotes são ordenados para encaminhamento;

A estrutura do modelo de encaminhamento de pacotes pode ser observada na Figura 23.

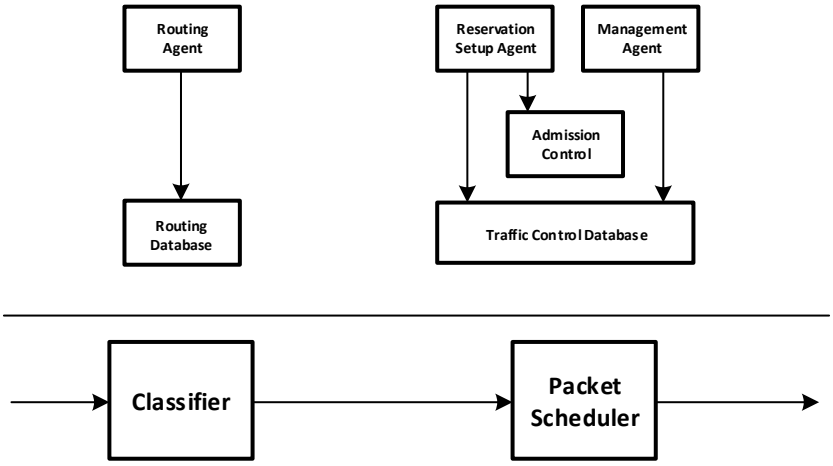

Figura 23 – Componentes do modelo *IntServ* [42]

De forma sintetizada, o agente de encaminhamento utiliza um protocolo de *routing*, utilizando-o para popular a tabela de rotas. Posteriormente, é utilizado o protocolo de reserva de recursos de forma a manter disponíveis os recursos necessários para um determinado fluxo de pacotes, sendo os mesmos disponíveis com base na resposta do controlo de admissão. Se o controlo de admissão retornar "OK" para a garantia de qualidade de serviço do novo fluxo de dados, as devidas informações são guardadas na base de dados de controlo de tráfego, e os recursos disponibilizados. Por sua vez, o classificador determina a classe em que cada fluxo pertence.

É de referir ainda a função do agente de gestão. A cada momento, este agente pode alterar a base de dados de controlo de tráfego, alterando assim o tratamento que o classificador e o escalonador aplicam a cada fluxo de dados.

Pode-se concluir que a grande vantagem deste serviço se prende com a reserva de recursos realizada previamente, garantindo assim a entrega dos fluxos de dados mediante o pretendido. No entanto apresenta a desvantagem de não ser uma arquitetura escalável, pois a quantidade de informação armazenada na base de dados de controlo de tráfego é diretamente proporcional à quantidade de fluxos de dados, o que torna inviável o processamento dos nós de rede, numa topologia de grande dimensão.

2.8.2 Serviços diferenciados

Os serviços diferenciados (*DiffServ*), como solução de qualidade de serviço definido pelas RFCs 2474 [45] e 2475 [46], foram desenvolvidos com vista a serem uma alternativa aos serviços integrados, apresentados na secção 2.8.1. O principal objetivo deste modelo é permitir a diferenciação de serviços, sem que haja a necessidade de manter informação de estado por fluxo e de executar procedimentos de sinalização em cada nó de rede.

Cada serviço define as características de transmissão de um pacote ao longo da rede, podendo os atributos de cada um ser distinguidos em termos quantitativos (e.g. valores de débito, atraso), ou em termos de prioridades relativas no acesso a recursos (e.g. diferenciação de classes).

Inicialmente, cada pacote é classificado a partir de uma informação denominada por "*Differentiated Services*". Este campo encontra-se presente no cabeçalho IP e foi definido de forma a ser compatível com o campo *Type of Service* (ToS) em *IPv4*, e *Traffic Class* em *IPv6*, sendo constituído pelos parâmetros "*Differentiated services codepoint*" (DSCP – 6 *bits*) e "*Currently unused*" (CU – 2 *bits*) [45].

A componente de controlo na entrada de um domínio *DiffServ* mapeia o valor contido no campo DSCP para um comportamento que se deve ter em conta por cada nó desde a origem até ao destino, denominado por "*per-hop behavior*" (PHB). Uma vez que o campo DSCP tem 6 *bits*, podemos aferir a possibilidade de 64 classes de serviço, onde a cada uma irá corresponder um tratamento diferenciado [47].

O esquema de funcionamento inerente a este serviço de QoS apresenta assim grande escalabilidade, pois as questões de classificação e mapeamento dos pacotes nos PHBs estão somente a cargo dos nós de entrada, enquanto que os nós de *core* apenas realizam as operações de leitura do campo DSCP e mapeamento para um PHB.

No entanto, uma das adversidades rapidamente encontradas no que diz respeito à integração deste serviço em MPLS, tem a ver com o facto da não análise do pacote IP ao longo de todo o domínio MPLS. A resolução prende-se sobre a definição do PHB na etiqueta que é inserida no pacote na entrada do domínio MPLS [48].

Como visto anteriormente na secção 2.4, cada etiqueta MPLS possuí um campo denominado por "Exp", alusivo a utilizações futuras, composto por 3 *bits*. A integração dos serviços diferenciados no domínio MPLS passa pela utilização deste campo, no entanto, com a limitação de apenas 8 classes de serviço (2^3=8). Nesta abordagem, cada LSP é formado com o objetivo de agregar pacotes da mesma classe de serviço, a partir do conteúdo do "Exp" nos PHBs dos LSRs.

2.9 Técnicas de OAM

O OAM, definido como *standard* pelo IETF a partir da RFC 6291 [49], representa um conjunto de ações que visam a otimização da produtividade da infraestrutura e dos recursos utilizados, integrando-se funções de operação, administração e manutenção de todos os elementos da rede responsáveis pela prestação de serviços de telecomunicações. Estas funções compreendem nomeadamente:

- Operação: atividades operacionais que garantem o funcionamento da rede, tendo em conta as necessidades administrativas (e.g. monitorização e descoberta de erros);
- Administração: conjunto de funções que permitem uma melhor prestação de serviços do ponto de vista do gestor da rede;
- Manutenção: procedimentos que permitem o funcionamento contínuo da rede (e.g. atualizações de *software* e *hardware*).

Desta forma, e segundo Menezes e Santos [50], o OAM é capaz de providenciar indicações de falhas, informações de desempenho, diagnósticos de rede e funcionalidades como escalabilidade, multisserviço, qualidade e custo-benefício.

No que toca à integração do OAM com o MPLS, pode-se afirmar que para a correta gestão sobre a rede MPLS deve-se ter a capacidade de monitorizar a vitalidade de um LSP e isolar rapidamente as causas de falha no encaminhamento de pacotes. Para tal, pode-se dar uso aos conceitos práticos “ping MPLS LSP” e “traceroute MPLS LSP” [51].

O primeiro conceito torna possível verificar a existência de LSP’s entre dois nós de periferia e o seu estado de operação, enquanto que o segundo conceito retorna ao administrador de rede, qual o LSP utilizado para comunicação entre dois nós de periferia, ou até mesmo todos os LSP’s possíveis entre o nó de origem e o nó de destino.

Outro conceito chave a ter em conta para os processos de operação, administração e manutenção é o *service mirroring*. Este serviço permite ao administrador de redes a cópia integral de unidades de dados para uma interface dedicada a este serviço, que tem como ponto terminal um servidor com ferramentas capazes de analisar cada pacote (e.g. Wireshark) [52].

3. REDE MPLS DA UNIVERSIDADE DO PORTO

3.1 Introdução

A análise da situação atual da rede MPLS da Universidade do Porto é pertinente quando o objetivo principal deste projeto é a sua otimização. Ainda que o foco deva recair sobre a situação atual da rede, é importante ter a visão da infraestrutura antecedente à solução MPLS, de forma a constatarmos os benefícios desta tecnologia de transporte em detrimento da anteriormente utilizada, isto é o IP *routing*.

Após uma breve introdução, será analisado o esquema de operação atual, bem como as configurações e detalhes de funcionamento conseguidos através da análise detalhada sobre um dado serviço.

3.2 IP *routing* como tecnologia de transporte

Precedente à utilização da atual tecnologia de comutação de tráfego (MPLS), a Universidade do Porto utilizava como tecnologia de rede de transporte o IP *routing*, sendo a topologia física representada na Figura 24.

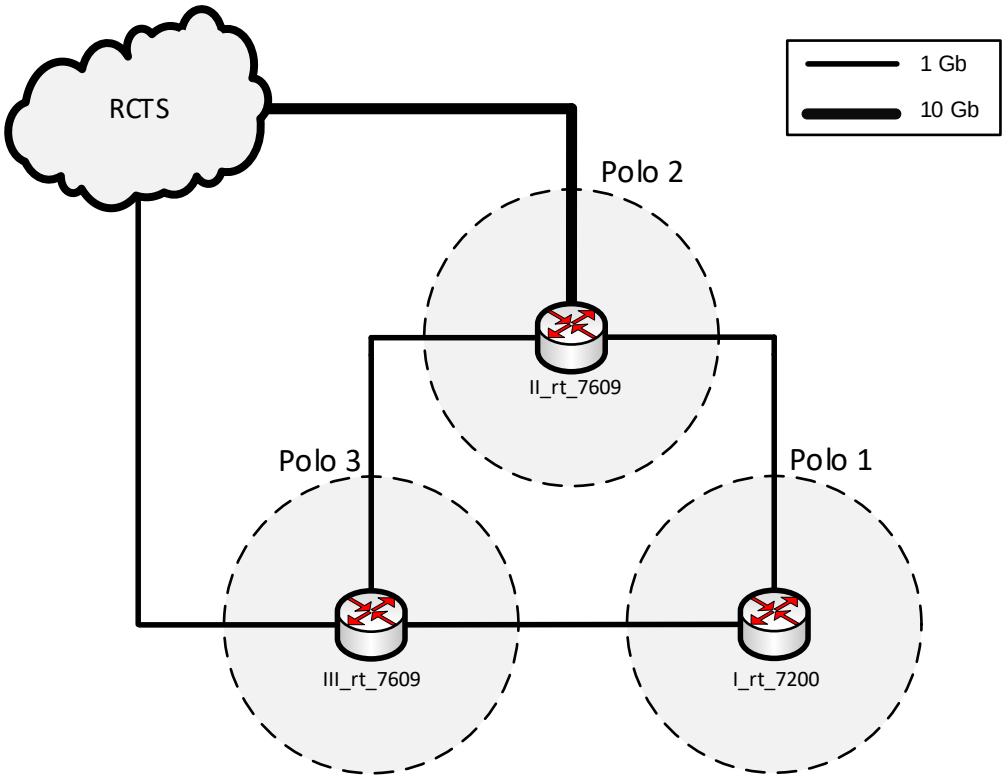

Figura 24 - Antiga topologia da rede *backbone* da Universidade do Porto

A rede da UP era constituida por três equipamentos de comutação (*routers* Cisco) instalados respetivamente no edifício da Reitoria, da FEUP e da FCUP, e cujo principal objetivo era o fornecimento de acesso à Internet a cada uma das unidades orgânicas. Neste paradigma, cada unidade orgânica era responsável pelos serviços que ofereciam internamente, sendo apenas alguns serviços disponibilizados centralmente, como o caso do DNS, Mail Relay, FTP e NTP.

Com a utilização transversal de um sistema de informação académico (SIGARRA), que abrange na UP as atividades de administração e gestão dos processos de ensino, investigação e desenvolvimento surgiu a necessidade de centralizar recursos e serviços TIC (Tecnologias da informação e comunicação). Por forma a garantir que as condições de infraestrutura tecnológica, tenham os mesmos padrões de qualidade em todos os organismos que compõem a UP, nomeadamente a nível das infraestruturas de telecomunicações e de sistemas, criticas nos modelos centralizados, procedeu-se também à reorganização dos recursos humanos afetos às TIC, por forma a garantir procedimentos mais eficazes e de maior qualidade.

Posto isto, e mantendo a tecnologia IP como base da rede de transporte, surgem uma série de desafios e problemas associados ao IP *routing* nomeadamente:

- Os pacotes eram encaminhados com base no endereço de destino, perdendo-se a possibilidade de definir caminhos dedicados;
- Elevado tráfego IP na rede de *backbone* no acesso a serviços internos, o que provoca o aumento da latência da rede, devido às operações de encapsulamento;
- A utilização de protocolos dinâmicos de *routing* aumenta o tempo de convergência dada a dimensão topológica da rede
- Maior necessidade de utilização de endereçamento IP público;
- A extensão de domínios de nível 2 até aos servidores centrais, aportam problemas relacionados com os protocolos de controlo da camada de ligação lógica, nomeadamente a nível do STP e VLAN

Tendo em conta os problemas apresentados, foi estudada a possibilidade de integração da tecnologia MPLS, que colmatava a necessidade de transporte de serviços multiponto de nível 2, transversais a múltiplos *sites*.

Para a implementação desta tecnologia foram adquiridos quatro novos equipamentos para a rede *backbone*, com o objetivo de substituir os existentes, dispostos ao longo de quatro pólos, mais precisamento no edifício da Reitoria, FEUP, FCUP e FDUP.

3.3 Topologia de rede atual

A rede da Universidade do Porto encontra-se distribuída ao longo de 4 polos geograficamente distribuídos ao longo da cidade do Porto, fornecendo serviços de conetividade de qualidade às várias unidades orgânicas referidas na Tabela 7.

Tabela 7 – Unidades orgânicas da Universidade do Porto

Polo 1	**Polo 2**		**Polo 3**		**Polo 4**
FBAUP	CIPES	FMUP	CEMUP	LIACC/C3P	Ed. Coronel Pacheco
Res. Aníbal Cunha	FEUP	FCNAUP	PBS	FLUP	UPTEC-PINC
CDUP	INEGI	FADEUP	ICBAS/FFUP	RUCA	ICETA
FIMS	INESC TEC	FPCEUP	Casa Andersen/ Salabert	IBMC	FDUP
Res. Bandeirinha	Campus Vairão	Pav. J. Falcão	CUP	CDUP	OUP
Res. Jayme Rios de Sousa	I3S	SASUP – Cant. FEUP	FCUPTEC	CAUP	SASUP
ISPUP	FEP	SASUP – Cant. São João	FAUP	Res. 2010	FLUP – Pós Doc
Reitoria	FMDUP	UPTEC	Res. Alberto Amaral	FCUP	
Serra do Pilar	Res. Paranhos		Res. Novais Barbosa	Res. Ciências	

O fornecimento de serviços às UO's referidas é da responsabilidade de quatro nós centrais de rede, denominados por Cisco ASR's (*Aggregation Services Routers*). Estes equipamentos encontram-se interligados através de ligações de 10 Gigabit/s, no entanto não se interligam numa topologia *full-mesh* por falta de circuitos de telecomunicações entre os polos 2 e 4.

Por consulta da Figura 25 é possível visualizar de modo sucinto o esquema de interligações do *core* da rede, e a interligação do mesmo com a RCTS e com as diferentes UO's. Na interligação do *core* com os diferentes *sites*/UO's, importa relevar a existência de anéis de fibra ótica detidos e operados pela UP, existentes nos polos 2 e 3, capazes de oferecer um serviço de conetividade redundante (Anexo I).

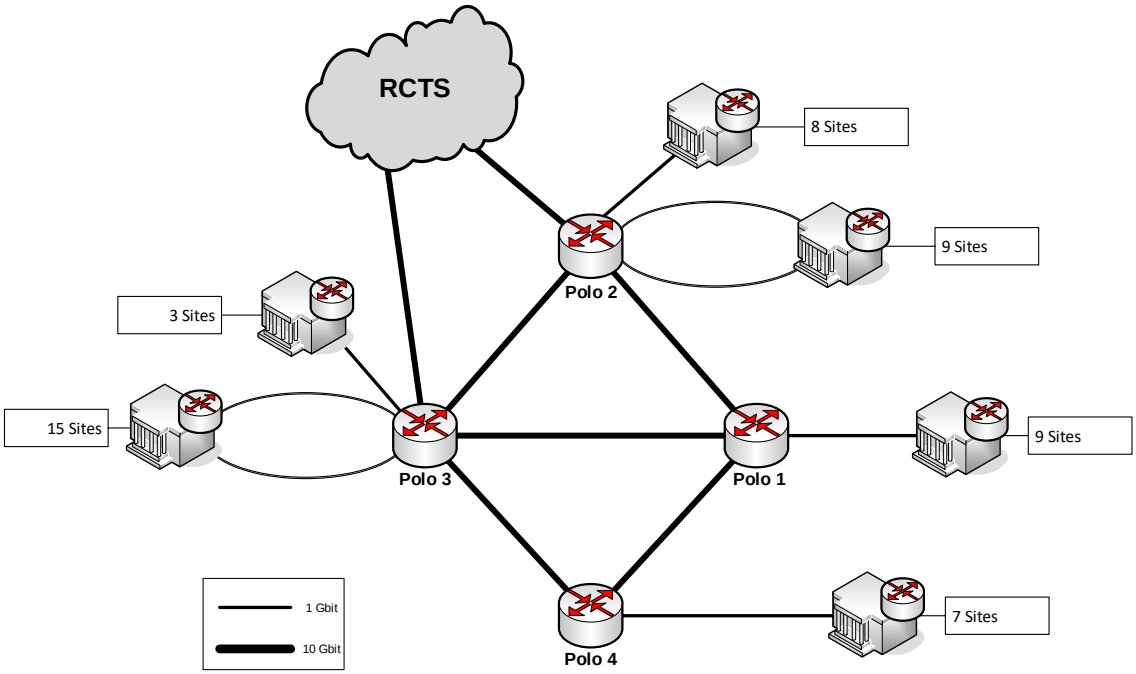

Figura 25 – Topologia atual da rede *backbone* da Universidade do Porto

O facto de a Universidade ser detentora da sua própria infraestrutura de rede enquadra a estratégia de uniformização da prestação de serviços de conetividade para com todas as UO's, como referido anteriormente. No entanto, existem algumas instituições, tais como a FEUP, a FCUP e a Reitoria que beneficiam do facto dos equipamentos de rede centrais (ASR's) estarem localizados com os equipamentos de rede local, pelo que nestas situações a probabilidade de existirem problemas de ligação entre o ASR e a instituição são práticamente "inexistentes".

3.4 Configuração IP/MPLS atual

A disponibilização de serviços transversais na UP é fruto da implementação do protocolo MPLS nos 4 equipamentos centrais, os quais têm a capacidade de transportar serviços de transporte *ethernet*, com encapsulamento 802.1Q (VLAN), ao longo do domínio MPLS. Por forma a caracterizar concretamente a prestação de serviços, optou-se por analisar o serviço de impressão distribuída, disponibilizado a todas as faculdades pertencentes à Universidade do Porto.

O serviço de impressão funciona de forma simples na ótica do utilizador. O cliente, utiliza um serviço *web* onde se autentica, para colocar todos os ficheiros que deseja imprimir na fila de impressão dos servidores centrais, depois pode realizar a impressão do material desejado, em qualquer uma das múltiplas impressoras existentes nas instalações das diferentes UO's.

A Figura 26 ilustra a localização fictícia do servidor de impressão, bem como uma impressora localizada numa das faculdades da UP.

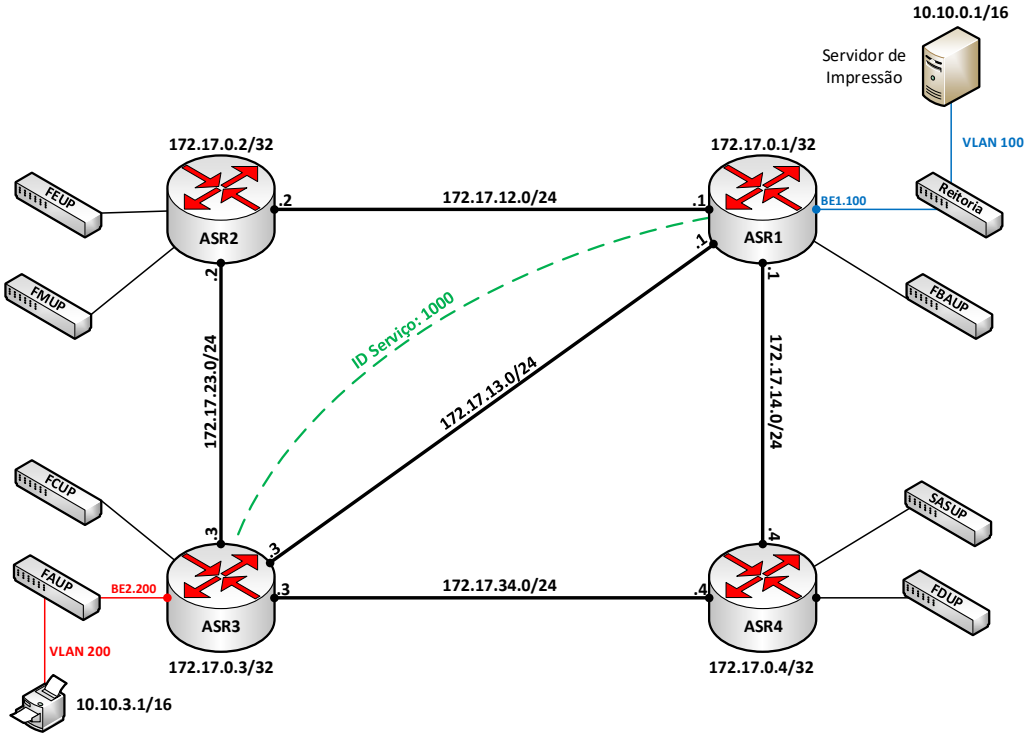

Figura 26 – Topologia do serviço de Impressão

Relativamente à configuração propriamente dita, esta pode ser referida como simplificada, uma vez que nenhum serviço contém conceitos associados à engenharia de tráfego ou à qualidade de serviço.

Atualmente, todos os serviços são transportados com base em dois grupos de configuração, a definição dos nós a quem se destina a entrega do serviço recorrendo ao protocolo MP-BGP, e a sinalização dos caminhos, neste momento efetuada pelo protocolo LDP.

Além do transporte do serviço, foi também analisada a entrega do mesmo, no qual o entendimento rege-se pela configuração das interfaces e tipo de encapsulamento.

Para o cenário em causa devem-se reter alguns aspetos, nomeadamente o facto do servidor de impressão se localizar na VLAN 100, as impressoras na Faculdade se encontrarem na VLAN 200, e o *id* do serviço de impressão, que corresponde à VLAN do serviço na rede MPLS, ser o 1000.

As configurações mais básicas como a configuração das interfaces físicas e lógicas encontram-se presentes no Anexo II, tendo em vista o plano de endereçamento da Figura 26.

3.4.1 Protocolos de sinalização

A sinalização de caminhos realizada pelo protocolo LDP tem como base as configurações provenientes do protocolo IGP (ver Figura 53), que neste caso concreto corresponde ao OSPF.

Quanto a este protocolo, cada nó definiu uma nova instância OSPF (através de um *id*), bem como uma área na qual se inseriram as interfaces locais que se pretendem distribuir dinamicamente, incluindo o endereço de *loopback*, que uma vez que não está associado a nenhuma interface física foi configurado como *router-id*.

Este novo processo OSPF foi criado de forma a auxiliar o LDP, onde a configuração se baseia na identificação das interfaces que irão realizar troca/associação de etiquetas. Por fim, e de forma a obter um melhor funcionamento proveniente da utilização paralela dos protocolos foi necessária uma sincronização entre eles.

Quando a sincronização entre o IGP e o LDP não existe podem ocorrer situações de perda de pacotes. Exemplo disso é quando se forma uma nova adjacência pelo IGP, onde o nó em causa, pode começar a comutar pacotes sem que a troca de etiquetas entre *neighbors* esteja completa para essa ligação.

Concluída a referência às configurações relativas à sinalização, os diferentes nós do domínio MPLS dão inicio à negociação de etiquetas.

3.4.2 Mecanismo de descoberta

O protocolo BGP foi configurado de forma a implementar o mecanismo BGP *Auto Discovery*, que se cinge a uma questão técnica que facilita a disponibilização de novos serviços.

Na implementação da rede MPLS existente, constatou-se que a definição de *neighbors* no momento de criação de cada serviço era uma tarefa morosa, principalmente quando se tratava de um serviço multiponto. Por exemplo, ao ser criado o serviço de impressão no ASR1 ter-se-ia que definir como *neighbors* os restantes ASRs, através da inserção do endereço *loopback* de cada um destes nós, sendo que o mesmo processo teria de se repetir em todos os nós.

Portanto e de forma a simplificar o processo, foi configurado um grupo BGP, com o *id* 65100, onde se especificaram os endereços das interfaces *loopback* dos nós remotos até onde se deseja estender os serviços MPLS (ver Figura 54), tendo em conta que estes endereços estão acessíveis através do protocolo OSPF anteriormente configurado.

No momento de criação do serviço, os *neighbors* são definidos através da invocação do protocolo de descoberta automática (BGP *Auto Discovery*) [53]. Desta forma, passa a ser dispensável definir cada *host* remoto até ao qual se deseja transportar um dado serviço no momento de criação, bastando, portanto, apenas definir o grupo onde se inserem todos os nós de periferia.

3.4.3 Definição do serviço

A criação de serviços VPLS fundamenta-se hierarquicamente, primeiro sobre um grupo geral de serviços multiponto denominado por *l2vpn*, depois por grupos concretos evocados de *bridge groups* onde se encontram instâncias dos diferentes serviços criados, os quais são referidos como *bridge-domains*.

Em cada serviço (*bridge-domain*) é necessário indicar quais as interfaces através das quais se deseja entregar o serviço, e criar uma instância de encaminhamento virtual (VFI – *Virtual Forwarding Instance*). Nesta VFI encontra-se especificado o VPN ID, os endereços dos restantes LERs através do *auto discovery bgp*, e por fim o protocolo de sinalização adotado, ou seja, o LDP (ver Figura 57).

3.4.4 Configuração do attachment-circuit

A entrega do serviço a cada faculdade por parte dos nós centrais (ASRs) efetua-se na interface de interligação entre os intervenientes, mais propriamente no *attachment-circuit*. No que toca ao encapsulamento, os ACs encontram-se a utilizar o modo de operação "*Basic Dot1Q Attachment Circuit*", no qual o AC abrange todas as *frames* que são enviadas e recebidas com uma VLAN *tag* específica [54].

A configuração da interface responsável pela entrega do serviço é bastante simples. Na interface de interligação do ASR1 para o *switch* da UO, interface "Bundle-Ethernet 1.100", é encapsulada a VLAN 1000 que representa a VLAN de serviço (ver Figura 56). Como se trata de uma interface dedicada à entrega de um serviço de nível 2, esta é também definida como *l2transport*, de forma a que todo o tráfego recebido por esta interface seja tratado mediante as regras do serviço VPLS, onde se inclui.

3.5 Análise à implementação IP/MPLS em operação

O funcionamento de uma rede MPLS é distribuído por dois componentes, o plano de controlo (*control plane*) e o plano de encaminhamento (*forwarding plane*). Em síntese, no plano de controlo encontram-se as informações relativas aos protocolos de distribuição de etiquetas e aos protocolos de *routing*, já no plano de encaminhamento encontra-se a tabela de comutação de etiquetas (LFIB) e a tabela de comutação de pacotes (FIB). Desta forma, pode-se constatar que a informação do plano de encaminhamento provém de informação gerada no plano de controlo.

Pela importância que os componentes representam, o objetivo principal deste subcapítulo é demonstrar o funcionamento prático de processos como a distribuição de etiquetas (*control plane*) e o processo de comutação de pacotes (*forwarding plane*), sobre a rede MPLS da Universidade do Porto, tendo em vista o serviço de impressão exemplificado na Figura 26.

3.5.1 Distribuição de etiquetas

O entendimento sobre a distribuição de etiquetas e consequente formação dos LSP's é crucial para a perceção do funcionamento da rede MPLS. Desta forma, cada nó da rede MPLS tem disponível um *range* de etiquetas a utilizar para cada prefixo de rede, ou seja, o ASR-1 foi configurado de forma a inserir valores de etiquetas entre 100000-199999, enquanto que o ASR-2 entre 200000-299999, e assim sucessivamente pelos quatro nós. A definição manual do valor das etiquetas facilita o processo de depuração e de *troubleshooting*.

Analisando o processo de distribuição de etiquetas para o endereço *loopback* do ASR-1 (endereço 172.17.0.1/32), através da Figura 27, verifica-se que o primeiro passo remete para a alocação da etiqueta local de ASR-1 para o endereço 172.17.0.1/32, onde é atribuído o valor "0" à etiqueta (que irá facilitar o processo de comutação como explicado na secção 3.5.2). Depois da associação local, o ASR-1 anuncia o prefixo de rede aos *neighbors* adjacentes, através da indicação do prefixo de rede e da etiqueta local [172.17.0.1/32 ; 0].

De seguida, no passo 2, os nós que receberam a informação do ASR-1 (ASR-2, ASR-3 e ASR-4), guardam a informação na LIB e atribuem uma etiqueta local ao prefixo de rede. Posto isto, os nós em causa, anunciam novamente o prefixo de rede aos seus *neighbors*, incluindo o nó de onde proveio a informação inicial. Este processo de troca de informação é responsável pela formação da tabela de comutação de etiquetas cada nó.

Finalizada a troca de etiquetas (passo 3), cada nó mantém na LIB uma associação entre o prefixo de rede 172.17.0.1/32 e a etiqueta local, bem como as etiquetas remotas dos *neighbors*.

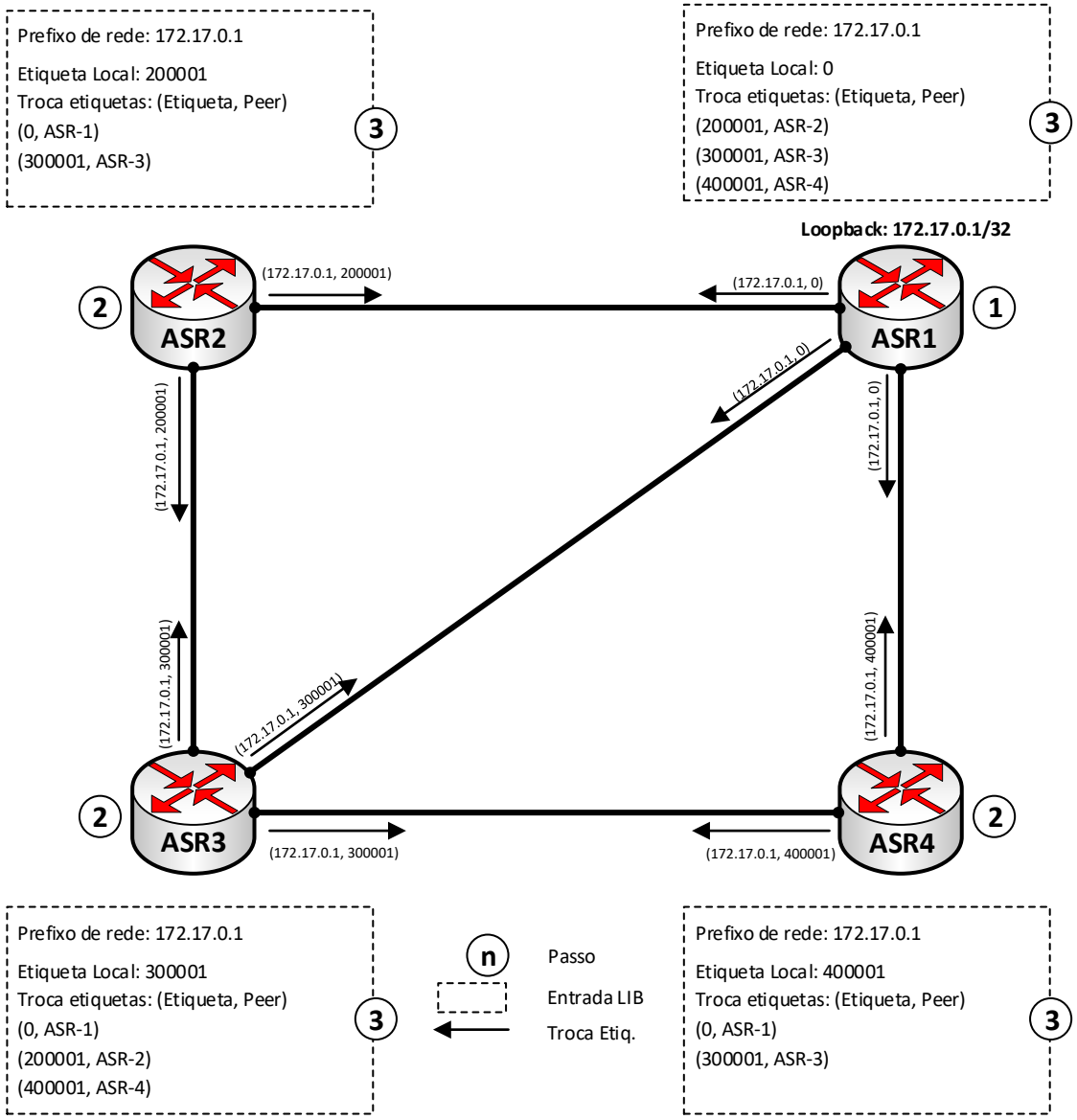

Figura 27 – Distribuição de etiquetas

O mesmo processo repetido para todos os prefixos de rede do domínio MPLS leva à formação da tabela de comutação de etiquetas (LFIB) e consequentes LSP's, responsáveis pela comutação dos pacotes.

3.5.2 Processo de comutação de pacotes

Após a negociação de etiquetas entre todos os nós do domínio MPLS para os prefixos de rede inerentes a este domínio, fica concluída a formação da tabela de comutação de etiquetas (LFIB) para cada nó (ver Tabela 23, Tabela 24, Tabela 25, Tabela 26 [Anexo III]). Desta forma, os LSP's entre todos os nós ficam estabelecidos (ver Figura 58, Figura 59 e Figura 60 [Anexo IV]), permitindo assim transportar serviços.

Tal como acontece com os prefixos de rede, também para cada serviço os nós do domínio MPLS realizam troca de etiquetas, formando-se assim o *pseudowire*. Cada LER apresenta um par <*PW Label Local-PW Label Remote*>, pelo que mesmo que os LER's não sejam adjacentes não há troca de etiquetas de *pseudowire*.

Um exemplo concreto do processo de comutação de pacotes para este serviço encontra-se ilustrado na Figura 28.

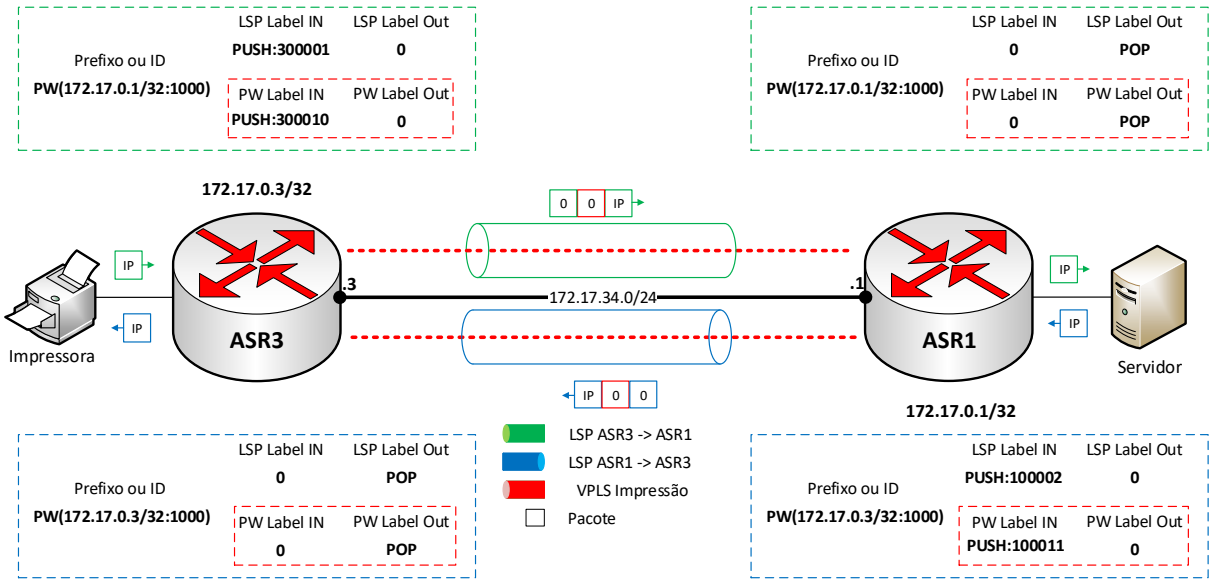

Figura 28 – Processo de comutação de pacotes (1)

Sendo os LSP's unidirecionais, a figura apresenta um túnel no sentido ASR-3 → ASR-1, e outro no sentido ASR-1 → ASR-3, onde é transportado o serviço de impressão (ID:1000). Tendo como exemplo o primeiro LSP, o nó ASR-3 ao receber um pacote proveniente da impressora a partir do *attachment-circuit* que corresponde ao serviço "1000", atribui-lhe a etiqueta "300001" (processo de *push*). Esta etiqueta corresponde ao LSP, e juntamente a esta encontra-se a etiqueta de serviço (*pseudowire*). A etiqueta do serviço é selecionada mediante o destino do serviço, e com base na Tabela 25 pode-se constatar que a etiqueta a ser "colocada" é a "300010".

Depois, e de forma a comutar o pacote, o ASR-3 analisa a tabela de comutação (LFIB) e toma como decisão de encaminhamento comutar o pacote com o valor de etiqueta "0". Esta etiqueta, de valor reservado, é sinónima de "*Explicit Null Label*" e quando recebida pelo ASR-1 este sabe automaticamente que deverá retirar o cabeçalho MPLS (operação de POP) e entregar o pacote com base no cabeçalho IP. Esta operação é comummente referida como *Penultimate Hop Popping* (PHP) [40], onde o penúltimo nó informa o último que deve retirar a etiqueta a partir do valor da etiqueta.

3.5.3 Resolução de falhas

Uma das características importantes a ter em conta na rede MPLS atualmente implementada é a predisposição a falhas a que esta se encontra sujeita. Por análise ao cenário demonstrado anteriormente (Figura 25) , entende-se que infelizmente a rede não disponibiliza redundância de equipamentos *core*, os ASRs, contando apenas com redundância de *links* de ligação. Isto leva a que uma instituição ligada ao ASR-1 fique limitada à rede local caso este nó seja desligado, e todos os serviços que façam uso de recursos presentes neste nó serão afetados.

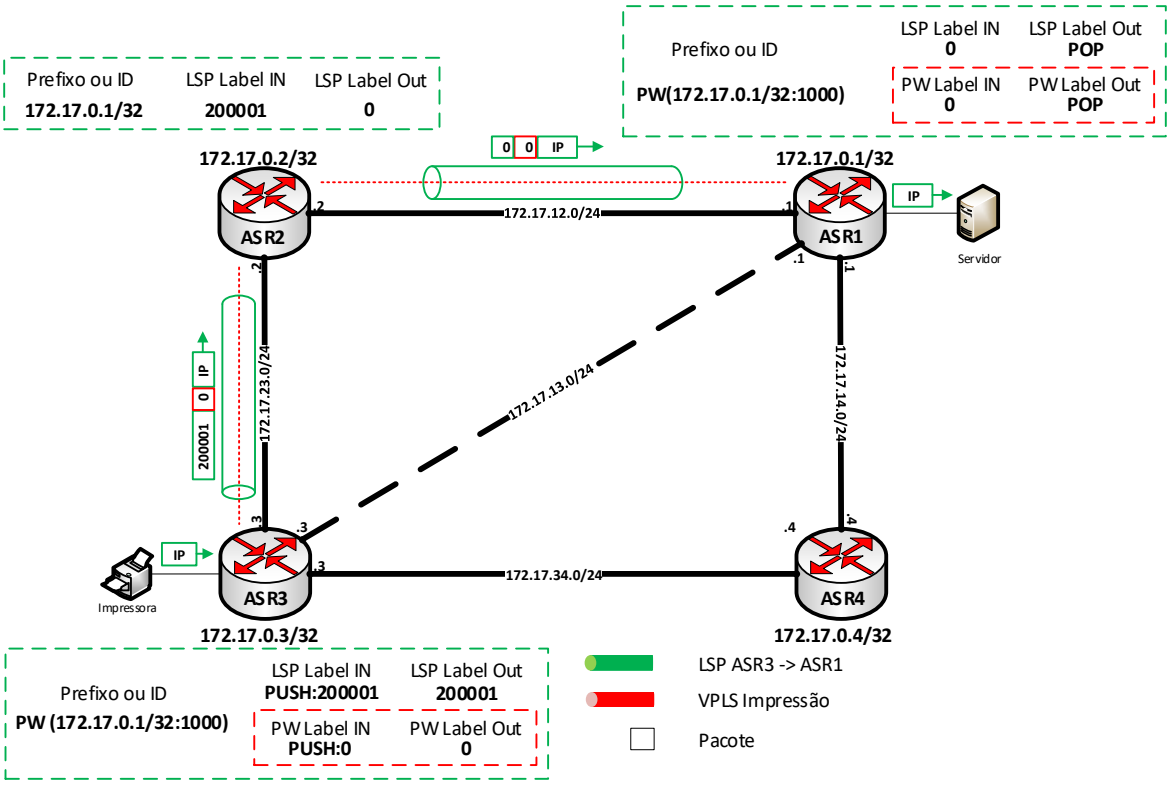

Figura 29 – Redundância de *link*

No caso de falha de um dos *links* de ASR-1 para outro nó de *backbone*, a ligação é reestabelecida através dos outros *links* de interligação. Tendo como exemplo uma falha de

ligação entre os nós ASR-1 e ASR-3, o protocolo dinâmico de *routing* irá convergir novamente, e irá selecionar um novo caminho para a comunicação entre os nós referidos, através das interligações entre o ASR-2 e o ASR-4.

Na Figura 29 podemos visualizar a via de comunicação entre o ASR-1 e o ASR-3 em caso de falha no *link* de ligação entre os nós. Como a troca de etiquetas já tinha sido anteriormente realizada entre todos os nós de *core* a quebra do *link* não leva à necessidade de uma nova negociação de etiquetas, apenas a uma reformulação das entradas na LFIB a partir da LIB.

4. PROVA DE CONCEITO

4.1 Introdução

O estudo sobre a implementação da tecnologia MPLS na rede de comunicação de dados da Universidade do Porto, permitiu formar uma opinião crítica capaz de propor algumas melhorias sobre a infraestrutura tecnológica.

Em concreto, a falta de redundância dos nós MPLS de cada pólo, a ausência de engenharia de tráfego e qualidade de serviço, bem como a carência de demarcação topológica realçaram-se, e foram definidos como aspetos a retificar.

Para a realização das propostas de melhoria, um dos aspetos fundamentais a ter em conta foi o conjunto de equipamentos que a Universidade do Porto possuía no âmbito da otimização da rede de *backbone*. Posto isto, verificou-se que além dos quatro *routers* Cisco ASR-9000 utilizados, a Universidade detinha ainda três equipamentos Cisco 6840-X, que possuem 16 interfaces físicas a 10 Gb/s, sobre os quais foi realizado um estudo sobre o esquema de configuração das versões IOS e IOS-XR (Anexo V e Anexo VI). Para além disso, foi também constatado que várias UO's, como por exemplo a FCUP e a FEP (Faculdade de Economia da Universidade do Porto), possuíam nas suas instalações equipamentos Cisco *Switch* ME 3600X, que tinham versões de *firmware* capazes de suportar serviços VPLS.

4.2 Análise de propostas

Tendo em consideração o objetivo principal da UP, deu-se início ao estudo de vários cenários de implementação, onde se identificaram os seguintes requisitos, nomeadamente:

- Avaliar a possibilidade de estender o domínio MPLS até às várias unidades organizacionais;
- Responsabilizar os *Switches* ME pela extensão dos serviços MPLS às UOs;
- Dotar os equipamentos de comutação específicos aos Data Centers, de redundância na interligação ao *backbone*;
- Distinguir topologicamente os nós responsáveis pelo transporte e os nós responsáveis pelo acesso;
- Dotar a rede IP/MPLS de engenharia de tráfego e qualidade de serviço.

Uma vez estipulados os principais objetivos a atingir, foram elaboradas várias propostas de implementação, concluindo-se a análise na identificação de três propostas, que se endendeu serem as mais adequadas, quer do ponto de vista dos requisitos acima identificados, quer do ponto de vista operacional. Estes cenários foram objeto de estudo de forma a avaliar qual serviria melhor as necessidades da UP, sendo apresentada a implementação prática dos cenários identificados no capítulo 5 deste relatório.

4.2.1 Análise ao cenário 1

O principal foco do primeiro cenário de implementação (Figura 30) foi a extensão do domínio MPLS até aos *Switches* ME de cada UO, considerando a inclusão dos equipamentos Cisco 6840-X na topologia de rede, a distinção de funções de cada nó (definindo quais os nós P e PE) e a capacitação da rede para a integração de engenharia de tráfego e qualidade de serviço.

Cada pólo, com exceção do pólo 4, possui centralmente um nó P ligado em *full-mesh* com os restantes P's, e um nó PE em *dual homed* (ligado a dois P's distintos). Além disto, cada UO possui nas suas instalações um nó PE, fora do seu domínio de gestão, interligado também a dois P's. O objetivo é providenciar resiliência tanto aos equipamentos de rede dedicados aos serviços centrais, como aos equipamentos de acesso dedicados a cada UO.

No que diz respeito ao pólo 4, e uma vez que este não contempla servidores centrais, nem possui infraestrutura com as características físicas necessárias para suportar equipamentos de rede de transporte, considerou-se, numa primeira fase, a substituição do equipamento Cisco ASR 9006 instalado, por um equipamento Cisco *Switch* ME de forma a colmatar as necessidades das UOs interligadas nesse pólo.

No entanto, foi identificado que este cenário apresenta alguns constrangimentos, nomeadamente a falta de redundância de ligação ao *core* por parte dos equipamentos de rede de *data center*, uma vez que se interligam apenas ao PE de cada pólo, e ainda a complexidade topológica da arquitetura MPLS, nomeadamente ao nível do aprovisionamento de serviços decorrente da falta de uma ferramenta de aprovisionamento transversal.

Desta forma, tendo em conta os problemas aferidos, desenvolveu-se um segundo cenário de implementação que solucionasse as menos valias acima identificadas, sem alterar os objetivos propostos.

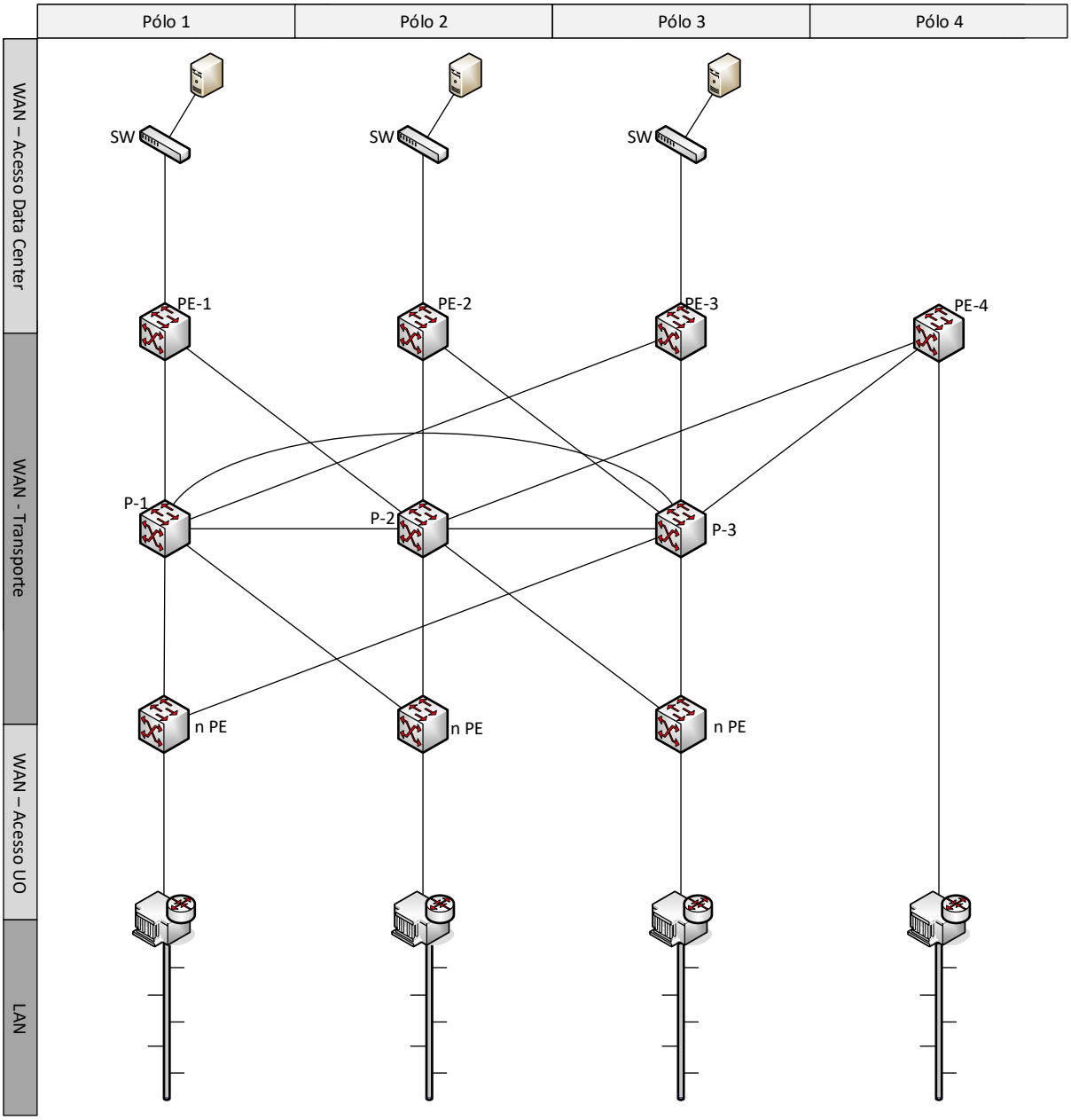

Figura 30 – Cenário de implementação 1

4.2.2 Análise ao cenário 2

O segundo cenário, apresentado na Figura 31, apresenta uma série de estratégias a salientar, nomeadamente:

- A complexidade da rede MPLS aumenta em relação à atual, no entanto é menor do que aquela apresentada no primeiro cenário, uma vez que o domínio MPLS não se estende até às UOs;
- O nó Cisco ASR-9006 do pólo 4 é substituído por um equipamento Cisco *Switch* ME 3600X que garante as funções de entrega dos serviços MPLS, nas UO's dependentes a este pólo;
- Nos pólos 1, 2 e 3, além dos nós ASRs já presentes, é acrescentado um nó Cisco 6840-X, que garante a redundância de ligação dos equipamentos de rede de *data center*, que na topologia inicial só se interligavam ao ASR de cada um dos pólos;
- Quanto aos nós P, apresentados no centro da figura, são utilizados dois equipamentos Cisco ASR 9006 (um deles retirado do pólo 4), sendo os mesmos colocados nos pólos 2 e 3, respetivamente.

Algumas considerações acima tomadas podem levantar questões pertinentes no que concerne à arquitetura MPLS, como por exemplo o facto de equipamentos PE poderem estar interligados diretamente. No entanto importa salientar que estas ligações seriam mantidas inicialmente por uma questão de continuidade de operação, isto é, para a implementação deste cenário a rede em exploração manter-se-ia em atividade sendo que posteriormente as ligações PE-PE seriam removidas.

Outra questão, e em comparação com o cenário anterior, remete para o relevo da extensão do domínio MPLS até às diferentes UO's, que neste cenário foi um requisito descartado, não só pela inixistência de uma ferramenta de aprovisionamento, mas também pela perspetiva de prestação de serviços que cada vez mais assenta nos cenários de centralização.

Em paralelo ao que foi mencionado, este cenário foi também considerado tendo em vista a inclusão de engenharia de tráfego, efacto que fundamenta a adição dos nós P no *core* da rede MPLS. Com isto, pretende-se dotar a rede da UP da capacidade de se estabelecerem caminhos explícitos e dinâmicos, críticos para se estabelecerem SLAs extremo-a-extremo.

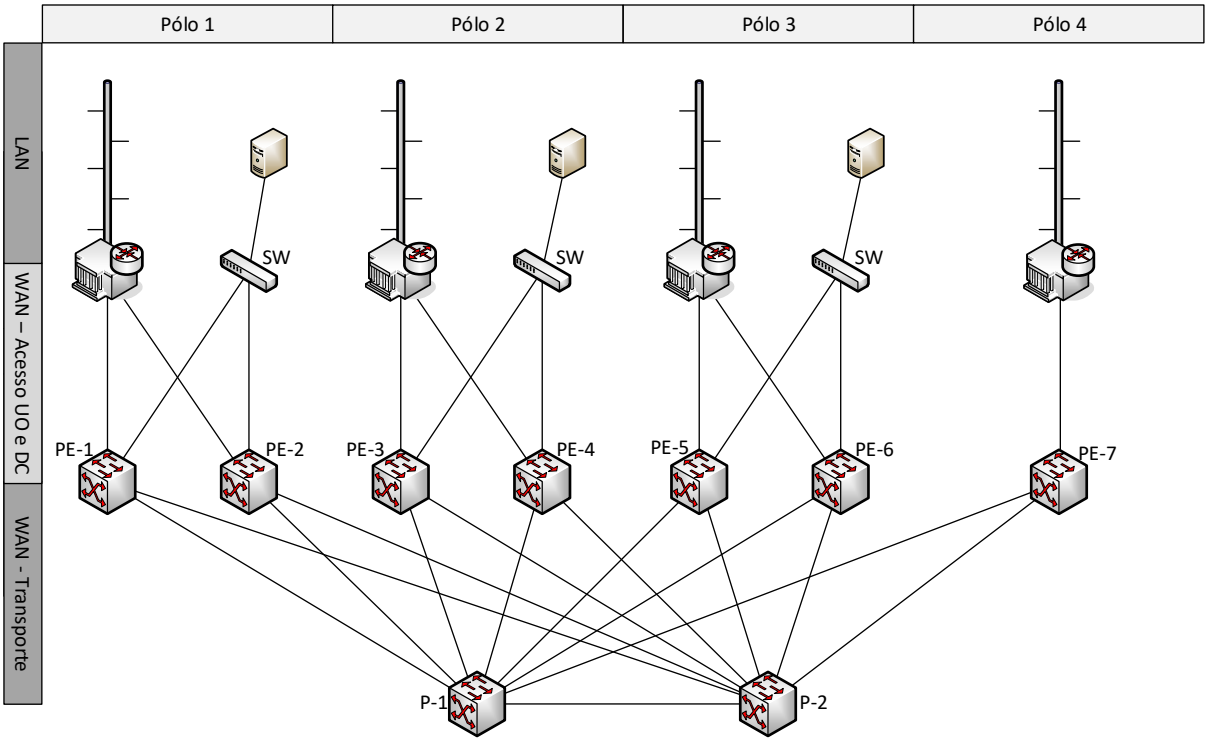

Figura 31 – Cenário de implementação 2

4.2.3 Análise ao cenário 3

O terceiro cenário proposto à Universidade do Porto apresentado na Figura 32, resulta de uma atualização sobre o cenário anterior, onde as alterações relevantes assentam na obrigatoriedade da instalação de um nó P nas por cada pólo, com exceção do pólo 4, o que por si só garante a possibilidade de criação de um maior número de caminhos explícitos e, portanto, de se alcançarem cenários com maior nível de proteção.

Para o pólo 4 e mediante uma análise mais cuidada, apresenta-se como hipótese a inexistência de equipamento MPLS, propondo-se a sua substitutuição por equipamento de *layer* 2, mais especificamente e por questões de redundância de equipamento e de ligações, uma pilha de *switches*. Nesta solução, a pilha de *switches* iria comportar-se como um nó CE, interligando-se a dois PE's de pólos distintos (pólo 2 e pólo 3).

Além do referido, esta solução volta a integrar ligações *full-mesh* entre os nós P, assim como ligações *dual homed* por parte dos PE's e redundância de *attachment-circuit* para cada UO e para cada *data center*.

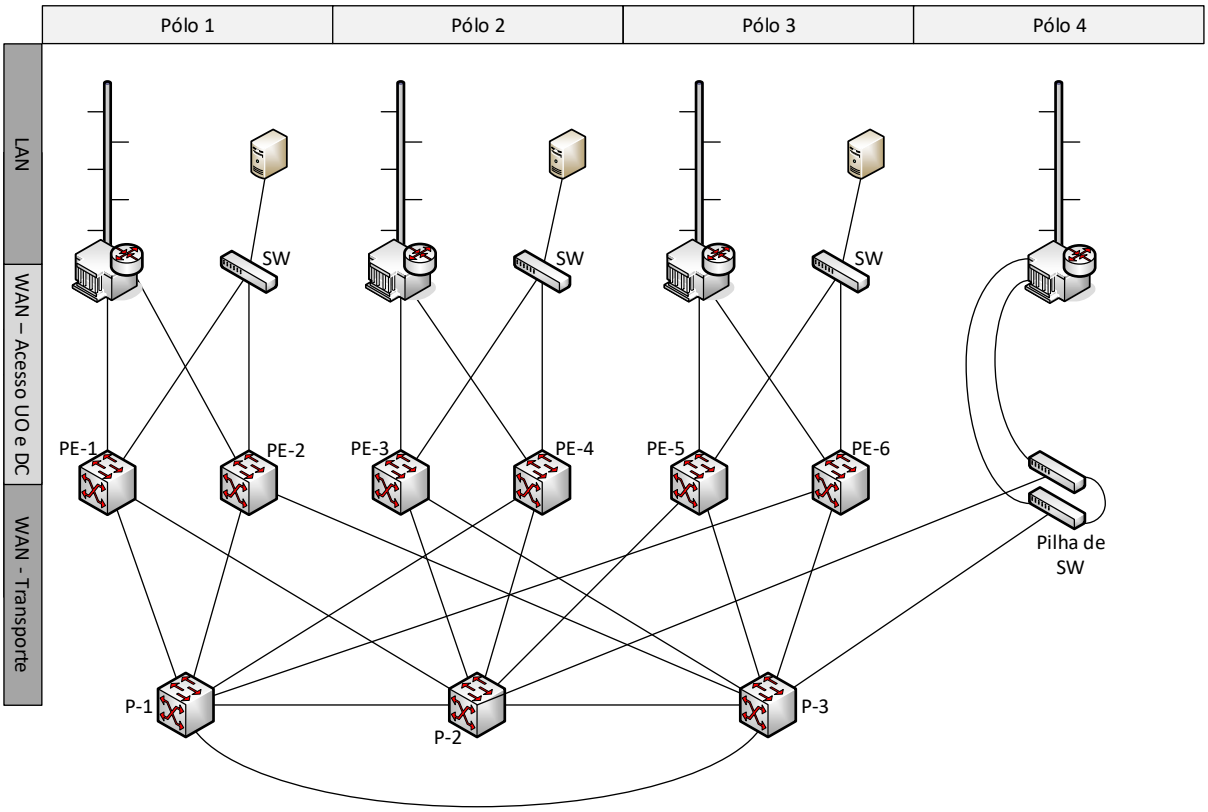

Figura 32 – Cenário de implementação 3

4.2.4 Estratégia para implementação

A estratégia para implementação da topologia proposta contemplou cinco fases distintas, nomeadamente:

- Fase 1: Definição do endereçamento lógico de todos os nós do domínio MPLS;
- Fase 2: Integração dos novos nós da rede nos protocolos OSPF, BGP e MPLS;
- Fase 3: Inclusão de engenharia de tráfego, definindo LSP's primários e secundários protegidos por técnicas de reencaminhamento eficaz;
- Passo 4: Estabelecimento de técnicas de qualidade de serviço que incluam restrições e otimizem a largura de banda;
- Passo 5: Análise da inclusão de técnicas de Operação, Administração e Gestão (OAM).

Fase 1

Durante a componente de análise do endereçamento lógico, constatou-se que os nós que compreendiam o *core* da rede tinham endereços *loopback* (usados para identificar univocamente os nós) pertencentes à rede 172.17.0.0/24. Posto isto, e ainda de acordo ao cenário em produção, o último octeto do endereço *loopback* permite identificar o pólo onde o equipamento se encontra instalado (e.g. nó do polo 1 tem o endereço 172.17.0.1/32).

Uma vez que é proposto que os pólos técnicos da rede da UP passem a ter mais do que um nó de *core*, à exceção do pólo 4, foi necessário alterar a organização do endereçamento IPv4, apresentando-se na Tabela 8 o esquema de endereçamento proposto.

Tabela 8 – Endereçamento IPv4 – interfaces *loopback*

Endereçamento IPv4			
Pólo	**Nó**	**Equipamento**	**Endereço IP**
Pólo 1	PE-1	Cisco ASR	172.17.0.1/32
	PE-2	Cisco SW 6840-X	172.17.0.2/32
	P-7	Cisco ASR	172.17.0.7/32
Pólo 2	PE-3	Cisco ASR	172.17.0.3/32
	PE-4	Cisco SW 6840-X	172.17.0.4/32
	P-8	Cisco ASR	172.17.0.8/32
Pólo 3	PE-5	Cisco ASR	172.17.0.5/32
	PE-6	Cisco SW 6840-X	172.17.0.6/32
	P-9	Cisco ASR	172.17.0.9/32

Como é possível de analisar pela tabela acima, a nomenclatura IP atribuída a cada nó é resultado do seu número identificador. Deste modo, o endereço IP do nó P-8, por exemplo, será preenchido com o valor ".8" no quarto octeto.

Existiu também a necessidade de definir o endereçamento das redes de interligação entre os nós do *core* da rede, sendo que o proposto se encontra apresentado na Tabela 9.

Tabela 9 – Endereçamento IPv4 – redes de interligação

Endereçamento IPv4	
Nome Ligação	**Endereço de Rede**
PE-1_to_P-7	172.17.17.0/24
PE-1_to_P-8	172.17.18.0/24
PE-2_to_P-7	172.17.27.0/24
PE-2_to_P-9	172.17.29.0/24

PE-3_to_P-8	172.17.38.0/24
PE-3_to_P-9	172.17.39.0/24
PE-4_to_P-7	172.17.47.0/24
PE-4_to_P-8	172.17.48.0/24
PE-5_to_P-8	172.17.58.0/24
PE-5_to_P-9	172.17.59.0/24
PE-6_to_P-7	172.17.67.0/24
PE-6_to_P-9	172.17.69.0/24
PE-7_to_P-8	172.17.78.0/24
PE-7_to_P-9	172.17.79.0/24
P-8_to_P-9	172.17.89.0/24

Para cada rede de interligação restava apenas indicar o endereço IP de cada nó, sendo que o mesmo seria preenchido no quarto octeto com atribuição do número identificador do nó (e.g. P8 seria sempre preenchido com o endereço ".8").

Estando o endereçamento IP atribuído, dá-se então início às configurações relativas aos protocolos OSPF, BGP e MPLS.

Fase 2

Tendo sido já analisada, no capítulo 3, toda a configuração relativa aos protocolos OSPF, BGP e MPLS da topologia lógica da rede da Universidade do Porto, o processo de inclusão dos novos nós no domínio MPLS torna-se mais simplificado.

Tabela 10 – *Range* de etiquetas

***Range* de Etiquetas**		
Equipamento	**Valor mínimo**	**Valor máximo**
PE-1	10000	19999
PE-2	20000	29999
PE-3	30000	39999
PE-4	40000	49999
PE-5	50000	59999
PE-6	60000	69999
P-7	70000	79999
P-8	80000	89999
P-9	90000	99999

É de realçar o *range* de etiquetas atribuído a cada nó MPLS, o qual é importante definir para um melhor nível de *troubleshooting*. A definição do *range* teve como base o identificador de cada nó, assim como demonstra a Tabela 10.

Fase 3 e fase 4

Tal como referido anteriormente, a rede MPLS da Universidade do Porto não possuí a capacidade de implementação de regras de engenharia de tráfego. Mais especificamente, a definição de caminhos explícitos neste momento não é possível, uma vez que as funções de transporte e acesso se encontram operacionalizadas nos mesmos nós e não existe em operação um protocolo de sinalização capaz de responder ao desafio da engenharia de tráfego.

Assim sendo, o esquema de engenharia de tráfego proposto pressupõe a implementação de dois caminhos explícitos, um primário e o outro secundário. De forma a que o caminho secundário possa servir como ligação de *backup*, foi definido que os dois caminhos não poderiam partilhar pontos de falha, quer estes fossem nós ou *links*.

Mediante o cenário proposto, foi possível constatar que entre dois nós de periferia existem três nós de *backbone*, os nós "P-7", "P-8" e "P-9". Assim, o estabelecimento dos dois caminhos explícitos referidos anteriormente (o primário e o secundário) terão como principal ponto diferenciador o nó de *backbone* (Tabela 11 e Tabela 12).

Tabela 11 – Caminhos explícitos (1)

Origem	Destino	Caminho Primário	Caminho Secundário
PE-1	PE-2	PE-1 → P-1 → PE-2	PE-1 → P-2 → P-3 → PE-2
	PE-3	PE-1 → P-8 → PE-3	PE-1 → P-7 → P-9 → PE-3
	PE-4	PE-1 → P-7 → PE-4	PE-1 → P-8 → PE-4
	PE-5	PE-1 → P-8 → PE-5	PE-1 → P-7 → P-9 → PE-5
	PE-6	PE-1 → P-7 → PE-6	PE-1 → P-8 → P-9 → PE-6
PE-2	PE-1	PE-2 → P-1 → PE-1	PE-2 → P-3 → P-2 → PE-1
	PE-3	PE-2 → P-9 → PE-3	PE-2 → P-7 → P-8 → PE-3
	PE-4	PE-2 → P-7 → PE-4	PE-2 → P-9 → P-8 → PE-4
	PE-5	PE-2 → P-9 → PE-5	PE2 → P-7 → P-8 → PE-5
	PE-6	PE2 → P-7 → PE-6	PE-2 → P-9 → PE-6
PE-3	PE-1	PE-3 → P-8 → PE-1	PE-3 → P-9 → P-7 → PE-1
	PE-2	PE-3 → P-9 → PE-2	PE-3 → P-8 → P-7 → PE-2
	PE-4	PE-3 → P-2 → PE-4	PE-3 → P-3 → P-1 → PE-4
	PE-5	PE-3 → P-8 → PE-5	PE-3 → P-9 → PE-5
	PE-6	PE-3 → P-9 → PE-6	PE-3 → P-8 → P-7 → PE-6

Tabela 12 – Caminhos explícitos (2)

Origem	Destino	Caminho Primário	Caminho Secundário
PE-4	PE-1	PE-4 → P-8 → PE-1	PE-4 → P-7 → PE-1
	PE-2	PE-4 → P-7 → PE-2	PE-4 → P-8 → P-9 → PE-2
	PE-3	PE-4 → P-2 → PE-3	PE-4 → P-1 → P-3 → PE-3
	PE-5	PE-4 → P-8 → PE-5	PE-4 → P-7 → P-9 → PE-5
	PE-6	PE-4 → P-7 → PE-6	PE-4 → P-8 → P-9 → PE-6
PE-5	PE-1	PE-5 → P-8 → PE-1	PE-5 → P-9 → P-7 → PE-1
	PE-2	PE-5 → P-9 → PE-2	PE-5 → P-8 → P-7 → PE-2
	PE-3	PE-5 → P-9 → PE-3	PE-5 → P-8 → PE-3
	PE-4	PE-5 → P-8 → PE-4	PE-5 → P-9 → P-7 → PE-4
	PE-5	PE-5 → P-3 → PE-6	PE-5 → P-2 → P-1 → PE-6
PE-6	PE-1	PE-6 → P-7 → PE-1	PE-6 → P-9 → P-8 → PE-1
	PE-2	PE-6 → P-9 → PE-2	PE-6 → P-7 → PE-2
	PE-3	PE-6 → P-9 → PE-3	PE-6 → P-7 → P-8 → PE-3
	PE-4	PE-6 → P-7 → PE-4	PE-6 → P-9 → P-8 → PE-4
	PE-5	PE-6 → P-3 → PE-5	PE-6 → P-1 → P-2 → PE-5

Fase 5

A inclusão de técnicas de OAM permite ao administrador de rede dispor de uma maior capacidade de gestão sobre a tecnologia na qual a rede é implementada, neste caso, o MPLS. Posto isto, foi estudado de que forma se poderia obter um maior controlo operacional, administrativo e de gestão sobre a rede MPLS da Universidade do Porto.

Em concreto, no que toca à operabilidade da rede MPLS, esta deve ser monitorizada tanto ao nível lógico como ao nível físico. No que diz respeito ao nível lógico, deve ser monitorizado o estado dos *pseudowires* e LSP's. Quanto ao nível físico o estado dos *attachment-circuits* deverá também ser vigiado.

Apesar de a Universidade do Porto utilizar a ferramenta Nagios para monitorizar a disponibilidade da rede e gerar alertas em caso de falhas, o *software* que se considera mais adequado é o Zabbix, devido às suas capacidades de autodescoberta [55]. Estas funcionalidades permitem que a cada novo serviço VPLS implementado, o mesmo seja automaticamente monitorizado, assim como os LSP's e *attachment-circuits*.

Além da ferramenta de monitorização é ainda sugerido que a instituição adquira uma ferramenta de aprovisionamento que permita a realização de configurações de serviços, através de uma interface gráfica, garantindo assim um menor número de falhas humanas, bem como maior rapidez de configuração.

5. IMPLEMENTAÇÃO TÉCNICA

5.1 Introdução

O estudo sobre a atual implementação da tecnologia MPLS na Universidade do Porto permitiu adquirir uma opinião crítica capaz de identificar uma série de melhorias, tais como a ausência de redundância dos nós MPLS de cada pólo, a necessidade de engenharia de tráfego e qualidade de serviço, bem como a inexistência de demarcação topológica.

Posto isto, e recorrendo aos recursos existentes no Centro Avançado de Telecomunicações (CAT) do ISMAI, foram criados vários cenários laboratoriais com o intuito de se analisar com detalhe algumas valências dos mecanismos MPLS, tais como como a engenharia de tráfego, a proteção local e proteção extremo-a-extremo, a qualidade de serviço, os serviços de nível 2 (VPWS e VPLS) e de nível 3 (VPRN).

A necessidade de a implementação técnica ser efetuada em cenário laboratorial recai sobre o facto de que não ser possível realizar testes sobre a rede MPLS da Universidade do Porto, uma vez que centenas de serviços, alguns deles críticos, iriam ser afetados.

Apesar de a Universidade do Porto recorrer apenas tecnologia serviços VPLS, foi estabelecido como objetivo adicional incluir o estudo e implementação da tecnologia VPRN pela possibilidade de integrar futuramente o catálogo de serviços MPLS na Universidade.

Este capítulo contempla assim dois cenários relativos aos serviços MPLS, nomeadamente VPLS e VPRN. Estes cenários incluem um conjunto de subcenários, onde se combinam uma série de protocolos e funcionalidades relativos à tecnologia MPLS, de modo a serem analisadas e comparadas.

5.2 Topologia da rede de transporte

A topologia implementada como rede de transporte teve como base dois pontos fundamentais, em primeiro, colmatar o requisito essencial que visa a criação de redundância dos nós MPLS centrais, e em segundo as lacunas apresentadas no subcapítulo 5.1. A Figura 33 apresenta a rede *backbone* implementada.

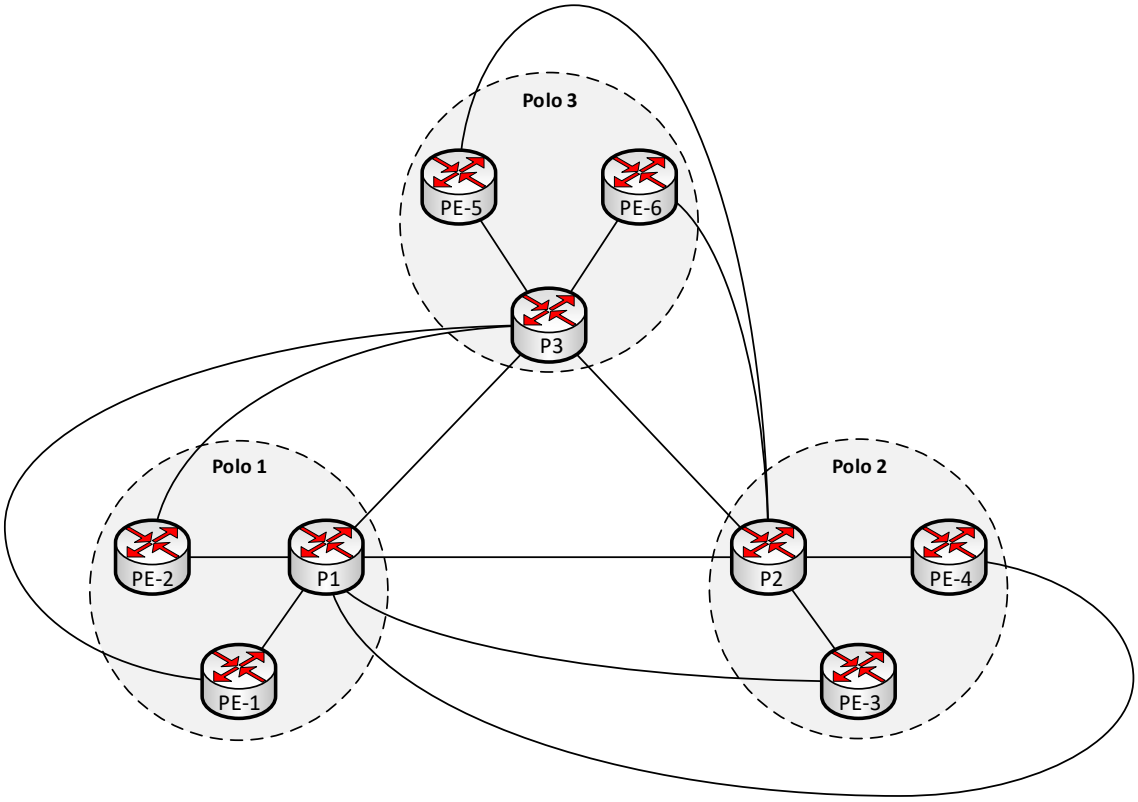

Figura 33 – Topologia da rede de transporte

Analisando a topologia, identifica-se a clara demarcação topológica dos equipamentos, verificando-se a existência de três nós P e de 6 nós PE. Além disto, as ligações entre P's encontra-se assente numa topologia *full-mesh*, e cada nó PE tem intrinsecamente associado um elevado grau de redundância, visto possuir ligação obrigatória a dois nós P's, um instalado no mesmo pólo e outroinstalado num pólo distinto. Com a inclusão de dois nós PE em cada pólo pretende-se estudar também os cenários de redundância a oferecer simultaneamente às unidades orgânicas e aos sistemas que suportam as aplicações centrais.

Apesar da Universidade do Porto utilizar unicamente equipamento Cisco no *core* da rede, foram utilizados nestes cenários de implementação equipamentos de fabricantes distintos (Cisco e Nokia), por falta de equipamento Cisco disponibilizado capaz de criar a topologia apresentada.

A Tabela 13 e a Figura 137 apresentam o conjunto de equipamentos utilizados, sendo que os equipamentos Nokia foram disponibilizados pelo ISMAI, e os equipamentos Cisco pela Universidade do Porto.

Tabela 13 - Equipamentos utilizados na rede de transporte

Nó	Equipamento	Versão
P1	Nokia 7750 SR	TiMOS-B-8.0.R4
P2	Nokia 7750 SR	TiMOS-B-8.0.R4
P3	Nokia 7750 SR	TiMOS-B-8.0.R4
PE-1	Nokia 7750 SR	TiMOS-B-8.0.R4
PE-2	Nokia 7750 SR	TiMOS-B-8.0.R4
PE-3	Nokia 7750 SR	TiMOS-B-8.0.R4
PE-4	Cisco SW 6848-X	IOS - 15.2(2)SY2
PE-5	Cisco SW 6848-X	IOS - 15.2(2)SY2
PE-6	Cisco SW 6848-X	IOS - 15.2(2)SY2

5.3 Topologia da rede de acesso

Uma vez que o projeto se enquadra na otimização da rede de transporte, foi necessário criar uma rede de acesso capaz de utilizar os serviços assentes sobre a rede de transporte para testar o funcionamento dos vários cenários a implementar.

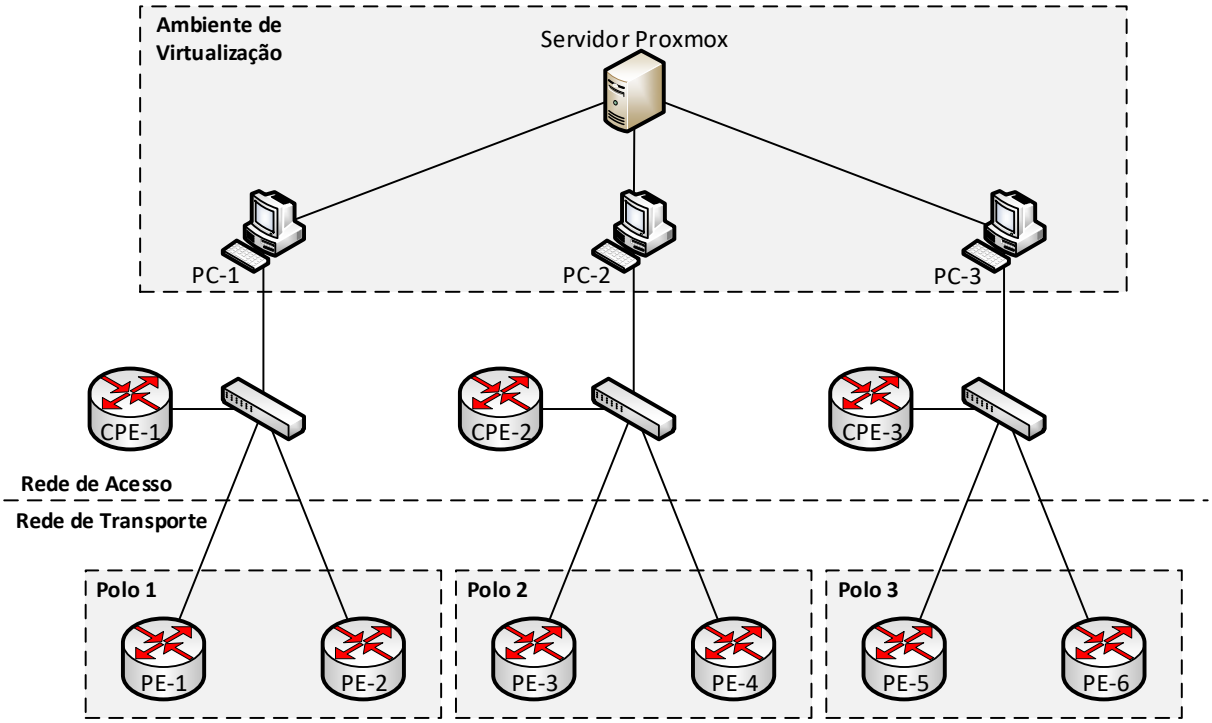

Figura 34 – Topologia da rede de acesso

Conforme se pode visualizar na Figura 34 em cada *site* cliente existe um *switch* CPE e um *router* CPE. Além disto e em complemento ao cenário de implementação, foi integrado neste projeto um ambiente de virtualização disponibilizado pelo CAT-ISMAI, mais especificamente o Proxmox Virtual Environment [56], onde puderam ser criadas, a pedido, várias máquinas

virtuais de forma a serem realizados testes de conetividade, de largura de banda, de disponibilidade dos serviços e de inspeção de pacotes.

A Tabela 14 apresenta o conjunto de equipamentos utilizados, disponibilizados pelo CAT-ISMAI.

Tabela 14 – Equipamentos utilizados na rede de acesso

Nó	Equipamento	Versão
CPE-1	Cisco ISR4221	IOS-XE 16.9.2
CPE-2	Cisco ISR 4221	IOS-XE 16.9.2
CPE-3	Cisco ISR 4221	IOS-XE 16.9.2
SW-1	Cisco 2960	IOS 15.2(2)
SW-2	Cisco 2960	IOS 15.2(2)
SW-3	Cisco 2960	IOS 15.2(2)
Ambiente de Virtualização	Proxmox VM	5.4-3
PC's	Máquinas Virtuais	Ubuntu 18.04 LTS

5.4 Esquema de endereçamento IPv4

O esquema de endereçamento utilizado separou o endereçamento de gestão do endereçamento de interfaces lógicas, ao contrário do que acontece na Universidade do Porto, em que o endereço de gestão é o mesmo endereço utilizado para as interfaces lógicas utilizadas como identificar de nó para protocolos como OSPF, MPLS e BGP.

Uma vez que o cenário apresentado foi construído no ISMAI, foi utilizado o endereçamento de gestão já em utilização pela instituição. Esta decisão foi de encontro ao facto de haver uma VPN já configurada que permite o acesso a esta rede, sendo possível trabalhar remotamente sobre a topologia.

A Tabela 15 e Tabela 16, apresentam o esquema de endereçamento de gestão e de interfaces lógicas, respetivamente.

Tabela 15 – Esquema de endereçamento de gestão

Endereçamento de Gestão			
Pólo	**Nó**	**Equipamento**	**Endereço IP**
Pólo 1	P1	Nokia 7750 SR	192.168.200.1/24
	PE-1	Nokia 7750 SR	192.168.200.4/24
	PE-2	Nokia 7750 SR	192.168.200.5/24
	SW-1	Cisco 2960	192.168.200.40/24
	CPE-1	Cisco ISR 4221	192.168.200.30/24

Pólo 2	P2	Nokia 7750 SR	192.168.200.2/24
	PE-3	Nokia 7750 SR	192.168.200.6/24
	PE-4	Cisco SW 6848-X	192.168.200.7/24
	SW-2	Cisco 2960	192.168.200.41/24
	CPE-2	Cisco ISR 4221	192.168.200.31/24
Pólo 3	P3	Nokia 7750 SR	192.168.200.3/24
	PE-5	Cisco SW 6848-X	192.168.200.8/24
	PE-6	Cisco SW 6848-X	192.168.200.9/24
	SW-3	Cisco 2960	192.168.200.42/24
	CPE-3	Cisco ISR 4221	192.168.200.32/24

Tabela 16 – Esquema de endereçamento lógico

Endereçamento Lógico			
Pólo	**Nó**	**Equipamento**	**Endereço IP**
Pólo 1	P1	Nokia 7750 SR	1.1.1.1/32
	PE-1	Nokia 7750 SR	4.4.4.4/32
	PE-2	Nokia 7750 SR	5.5.5.5/32
Pólo 2	P2	Nokia 7750 SR	2.2.2.2/32
	PE-3	Nokia 7750 SR	6.6.6.6/32
	PE-4	Cisco SW 6848-X	7.7.7.7/32
Pólo 3	P3	Nokia 7750 SR	3.3.3.3/32
	PE-5	Cisco SW 6848-X	8.8.8.8/32
	PE-6	Cisco SW 6848-X	9.9.9.9/32

No que toca às redes de interligação da topologia, foi elaborada a Tabela 17 de forma a organizar o endereçamento IPv4, e por fim, a Tabela 18 onde se encontra o esquema de interfaces de interligação da topologia.

Tabela 17 – Endereçamento IPv4 das redes de interligação

	P1	P2	P3	PE-1	PE-2	PE-3	PE-4	PE-5	PE-6
P1	-	172.16.12.1	172.16.13.1	172.16.14.1	172.16.15.1	172.16.16.1	172.16.17.1	-	-
P2	172.16.12.2	-	172.16.23.2	-	-	172.16.26.2	172.16.27.2	172.16.28.2	172.16.29.2
P3	172.16.13.3	172.16.23.3	-	172.16.34.3	172.16.35.3	-	-	172.16.38.3	172.16.39.3
PE-1	172.16.14.4	-	172.16.34.4	-	-	-	-	-	-
PE-2	172.16.15.5	-	172.16.35.5	-	-	-	-	-	-
PE-3	172.16.16.6	172.16.26.6	-	-	-	-	-	-	-
PE-4	172.16.17.7	172.16.27.7	-	-	-	-	-	-	-
PE-5	-	172.16.28.8	172.16.38.8	-	-	-	-	-	-
PE-6	-	172.16.29.9	172.16.39.9	-	-	-	-	-	-

Tabela 18 – Interfaces de interligação

	P1	P2	P3	PE-1	PE-2	PE-3	PE-4	PE-5	PE-6	CPE-1 SW	CPE-2 SW	CPE-3 SW	CPE-1 RT	CPE-2 RT	CPE-3 RT
P1	-	5	10	6	7	8	9	-	-	-	-	-	-	-	-
P2	5	-	10	-	-	6	7	8	9	-	-	-	-	-	-
P3	5	10	-	8	9	-	-	6	7	-	-	-	-	-	-
PE-1	6	-	7	-	-	-	-	-	-	10	-	-	-	-	-
PE-2	6	-	7	-	-	-	-	-	-	10	-	-	-	-	-
PE-3	7	6	-	-	-	-	-	-	-	-	10	-	-	-	-
PE-4	7	6	-	-	-	-	-	-	-	-	16	-	-	-	-
PE-5	-	7	6	-	-	-	-	-	-	-	-	16	-	-	-
PE-6	-	7	6	-	-	-	-	-	-	-	-	16	-	-	-
CPE-1 SW	-	-	-	1	2	-	-	-	-	-	-	-	24	-	-
CPE-2 SW	-	-	-	-	-	1	2	-	-	-	-	-	-	24	-
CPE-3 SW	-	-	-	-	-	-	-	1	2	-	-	-	-	-	24
CPE-1 RT	-	-	-	-	-	-	-	-	-	0/0/0	-	-	-	-	-
CPE-2 RT	-	-	-	-	-	-	-	-	-	-	0/0/0	-	-	-	-
CPE-3 RT	-	-	-	-	-	-	-	-	-	-	-	0/0/0	-	-	-

5.5 Implementação do serviço VPLS

Tendo em conta o estudo prévio da tecnologia MPLS identificaram-se um conjunto de cenários (Tabela 19) com vista à sua implementação (Anexo VII), de modo a transpor para a prática toda a análise mais teórica.

Tabela 19 – Cenários VPLS

Cenário	Descrição	Protocolo de Sinalização do LSP	Protocolo de Sinalização do Pseudowire	Engenharia de Tráfego	Proteção Extremo-a-Extremo	Proteção Local
1	Descoberta dos nós PE por BGP Auto-Discovery e sinalização do PW por T-LDP.	LDP com BGP Auto-Discovery	Target - LDP	Não	Não	Não
2	Sinalização do LSP por LDP.	LDP	Target - LDP	Não	Não	Não
3	Sinalização do LSP por RSVP, recorrendo túneis dinâmicos.	RSVP	Target - LDP	Não	Não	Não
4	Integração de TE com LSP's estabelecidos manualmente.	RSVP-TE	Target - LDP	Sim	Sim	Não
5	TE com túnel manual protegido por um túnel dinâmico, com FRR One-to-One.	RSVP-TE	Target - LDP	Sim	Sim	Sim (Fast Reroute One-to-One)
6	TE com túnel manual protegido por um túnel dinâmico, com FRR Facility.	RSVP-TE	Target - LDP	Sim	Sim	Sim (Fast Reroute Facility)
6.1	Implementação de LAG	RSVP-TE	Target - LDP	Sim	Sim	Sim (Fast Reroute Facility)
6.2	Implementação de MC-LAG	RSVP-TE	Target - LDP	Sim	Sim	Sim (Fast Reroute Facility)

A identificação de cada cenário teve como principal objetivo analisar as valências na utilização de cada protocolo de sinalização, bem como das técnicas de engenharia de tráfego onde se incluem os mecanismos de proteção local e de proteção extremo-a-extremo. Para além destas técnicas, foram ainda implementados os conceitos de *Link Aggregation Group* (LAG) e *Multi-chassis* LAG (MC-LAG), que se referem a técnicas de redundância disponiveis para utilização na integração com o equipamento do cliente.

Uma vez que se trata de um serviço MPLS de nível 2, foi retirado o equipamento de nível 3 da topologia da rede de acesso e atribuídos endereços IP a cada uma das máquinas virtuais configuradas e disponíveis para os testes (Figura 35).

Além do endereço IP, associou-se e configurou-se um identificador de VLAN para cada uma das máquinas virtuais, para não permitir a possibilidade de *routing* interno no servidor de virtualização Proxmox. Desta forma, e como premissa, ficou também pré-definida qual a VLAN a ser "entregue" por cada um dos PE's, na interface de acessoao cliente.

Por fim, sobre cada um dos cenários de implementação foram realizados testes de convergência protocolar em situações de falha, com auxílio da ferramenta *iperf* [57], configurada nas três máquinas do servidor de virtualização.

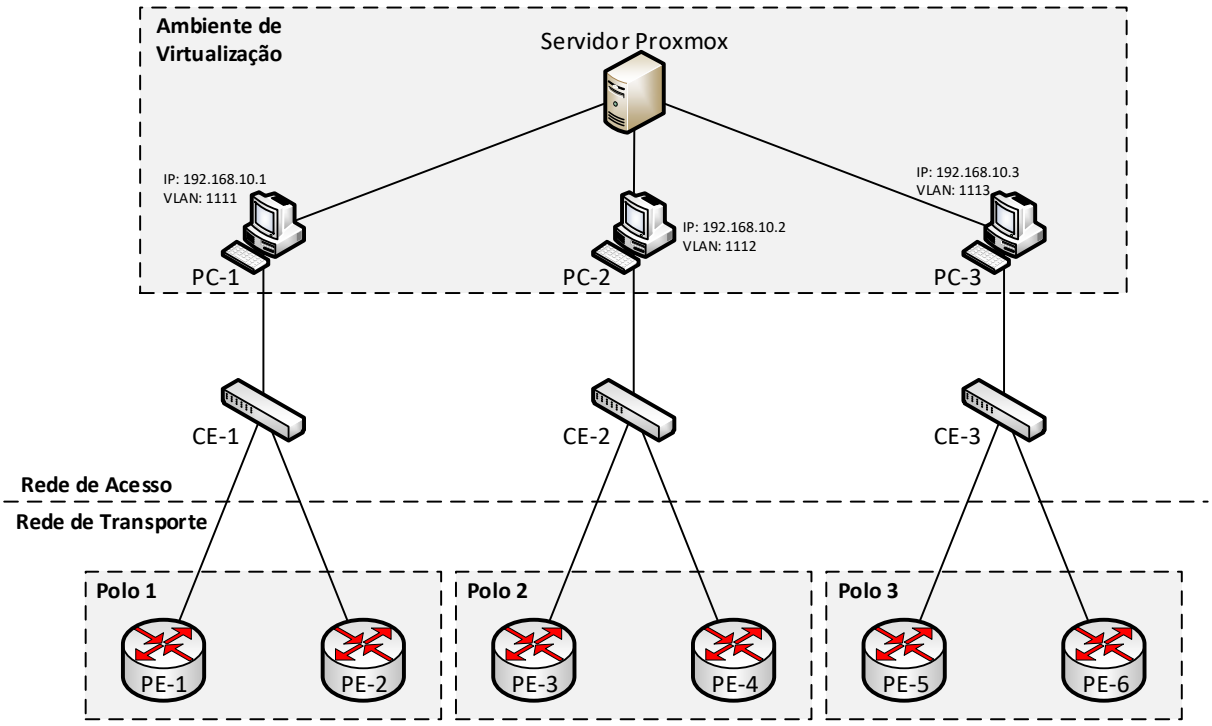

Figura 35 – Topologia do laboratório VPLS

5.5.1 Descrição dos cenários implementados

O primeiro cenário implementado teve como base o esquema de configuração atual da rede da Universidade do Porto, ou seja, o OSPF como protocolo dinâmico de *routing*, o BGP *auto-discovery* para descoberta automática dos nós PE e o LDP como protocolo de sinalização dos LSP's e *pseudowires*.

De seguida, criou-se um segundo cenário onde se removeu o BGP *auto-discovery* e utilizou-se a definição manual de cada PE para cada serviço configurado. Neste ponto, verificaram-se mais valias na utilização de BGP *auto-discovery* pelo automatismo oferecido na formação de LSP's e *pseudowires*.

Com o intuito de introduzir o conceito de engenharia de tráfego no quarto cenário, o terceiro cenário foi desenvolvido com o objetivo de substituir o protocolo de sinalização (LDP) dos LSP's pelo RSVP-TE, utilizando-se, contudo, apenas caminhos dinâmicos, isto é definidos com base na informação retornada pelo IGP (OSPF).

Apesar da utilização do protocolo RSVP-TE o cenário anterior não faz uso da engenharia de tráfego por ausência das técnicas de proteção. Desta forma, no quarto cenário foram criados dois caminhos configurados estáticamente para cada nó PE de pólos vizinhos. Estes caminhos têm como aspeto relevante a ausência de pontos (nós e ligações) comuns de falha, obviamente para além dos nós PE de entrada e saída do domínio MPLS, e que tem especial relevância na implementação da proteção extremo-a-extremo.

Após a implementação da proteção extremo-a-extremo, o próximo objetivo é a integração da proteção local, sendo que a mesma apresenta dois modos de funcionamento, nomeadamente o *Fast Reroute One-to-One* e o *Fast Reroute Facility*, implementados nos cenários cinco e seis, respetivamente.

Por fim, no sexto cenário foram criados dois subcenários com vista à inclusão das técnicas de redundância oferecidas ao cliente, sendo estas alusivas aos mecanismos LAG e MC-LAG.

5.5.2 Cenário 1

O primeiro cenário resume-se à oferta de serviços VPLS sobre uma rede baseada na sinalização por LDP, tanto ao nível dos LSP's como dos *pseudowires*. A particularidade deste cenário encontra-se na descoberta automática dos nós PE, realizada com base no protocolo BGP, assim como acontece atualmente na Universidade do Porto.

Tendo em conta as configurações gerais realizadas previamente, seguiram-se três passos de configuração:

1. Configuração do protocolo de sinalização LDP;
2. Configuração do MP-BGP;
3. Configuração do serviço VPLS.

O primeiro passo cinge-se à identificação das interfaces que participam no processo de distribuição de etiquetas (Figura 71, Figura 72 e Figura 73). É importante referir que nas versões Cisco IOS ao ativarmos o MPLS nas interfaces estamos também a habilitar a sinalização por

LDP, tanto ao nível do LSP como ao nível do *pseudowire*. Neste cenário a distribuição de etiquetas é realizada com base no protocolo de *routing* dinâmico OSPF.

No segundo passo foi configurado o protocolo BGP onde se deve exercer especial atenção sobre a criação da família de endereços L2 VPN, onde se incluem todos os endereços *system*/*loopback* dos nós PE (Figura 74 e Figura 75).

Por fim, foi configurado um serviço VPLS, recorrendo ao MP-BGP para propagar o serviço por todos os PE's que faziam uso do mesmo identificador de serviço (Figura 76 e Figura 77). Nesse serviço foi também adicionada a configuração relativa à ligação ao cliente (*attachment-circuit*) de forma a que conseguissem ser realizados testes ao serviço.

De forma a dar por terminado o primeiro cenário de implementação realizou-se um teste de conetividade entre o PC-1 e o PC-2, seguido de um teste de resiliência. Através de *debug* constatou-se que o tráfego entre os dois terminais seguia entre os nós PE-1, P-1 e PE-4, pelo que, de forma a analisar o tempo de convergência da ligação em caso de falha, se realizou um corte entre PE-1 e PE-4.

Com auxílio da ferramenta *iperf* verificou-se a ausência de troca de dados entre os dois terminais durante o intervalo de tempo em que ocorreu a falha, verificando-se um tempo de indisponibilidade de 6,6 segundos (11,40s aos 18,00s) (Figura 36).

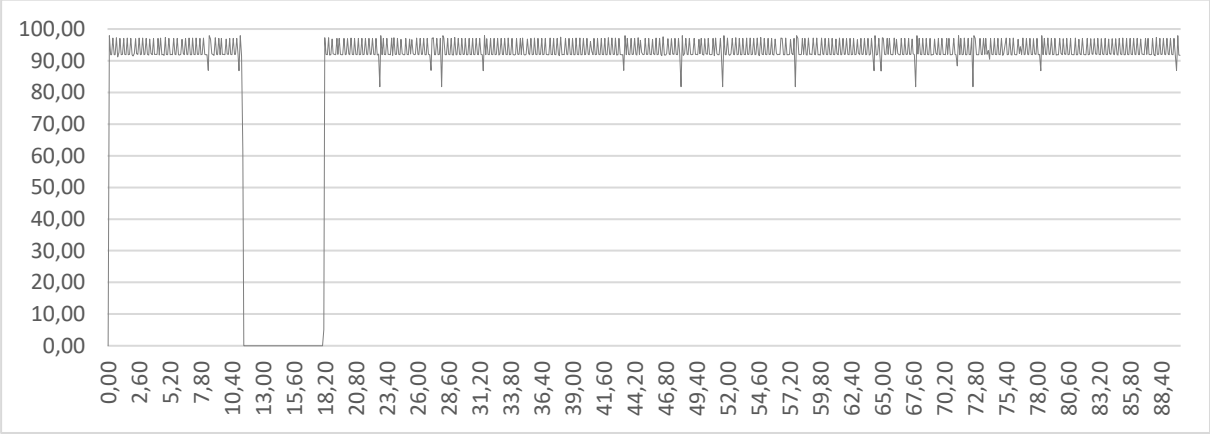

Figura 36 – Tempo de convergência em caso de falha (Cenário 1)

5.5.3 Cenário 2

Para o segundo cenário de implementação reutilizaram-se as configurações realizadas no cenário anterior, descartando apenas as configurações alusivas à configuração do serviço e do protocolo BGP.

Desta forma, a sinalização continuou a ser por meio do protocolo LDP, no entanto sem a descoberta automática dos nós PE, pelo que na configuração do serviço foi necessário identificar manualmente o nó PE até onde se desejava estender o serviço (Figura 78 e Figura 79).

Por fim, e tal como aconteceu no primeiro cenário, foi realizado um teste de convergência em caso de falha, onde não se verificam alterações em relação ao primeiro cenário, uma vez que a diferença entre cenários se encontra na definição automática ou manual dos nós aos quais se deseja entregar os vários serviços VPLS. A Figura 37 apresenta o tempo de indisponibilidade do segundo cenário correspondente a 6,7 segundos (10,90s a 17,60s).

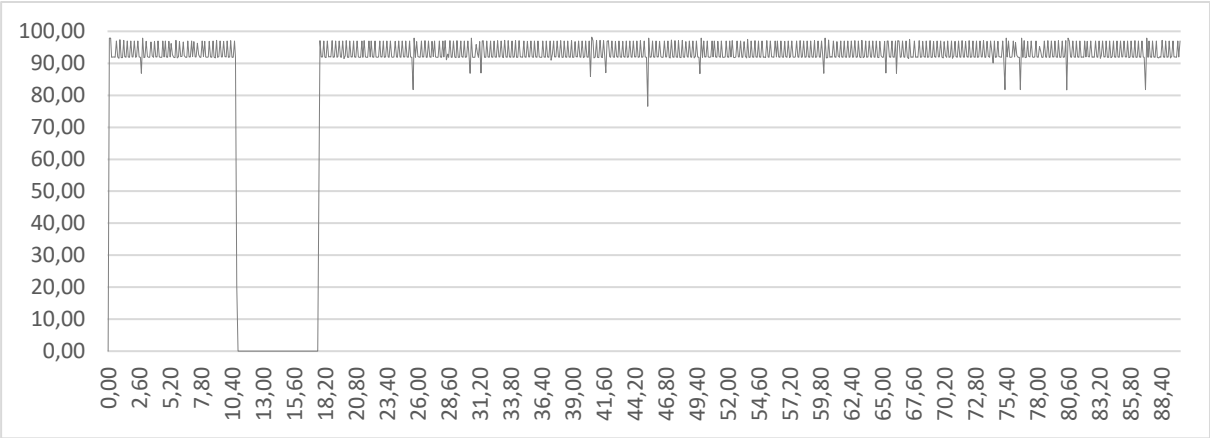

Figura 37 – Tempo de convergência em caso de falha (Cenário 2)

5.5.4 Cenário 3

No terceiro cenário o objetivo passava pela integração do protocolo de sinalização RSVP sobre LSP's estabelecidos dinâmicamente através do protocolo de *routing* OSPF. Assim sendo, foram retiradas as configurações alusivas à identificação das interfaces que iriam participar na sinalização por LDP e de seguida procedeu-se aos seguintes passos de configuração:

1. Configuração do protocolo de sinalização RSVP;
2. Configuração das extensões de engenharia de tráfego para o protocolo OSPF;
3. Configuração dos LSP's estabelecidos dinâmicamente.

A configuração do protocolo RSVP é idêntica aquela realizada no protocolo OSPF, ou seja, em todos os nós do domínio MPLS identificaram-se quais as interfaces que iriam participar no processo de sinalização por RSVP (Figura 80, Figura 81 e Figura 82).

Depois, no protocolo OSPF, foi ativada a extensão de engenharia de tráfego de forma a que o protocolo RSVP, recorra à informaçãoretornada pelo protocolo OSPF, de modo asinalizar os LSP's (Figura 83, Figura 84 e Figura 85).

Por último, foram configurados os tuneis exteriores dinâmicos, ou seja, LSP's estabelecidos mediante informação associada ao OSPF (Figura 86, Figura 87). Nos nós PE Nokia foi ainda necessário definir em cada PW o LSP dinâmico configurado (Figura 88). Este aspeto não se verifica nos equipamentos Cisco com versão IOS pois ao configurarmos um LSP este fica generalizado para todos os serviços, o que se revela como uma desvantagem.

Após a configuração do cenário realizou-se novamente um teste à resiliência da rede, constatando-se um tempo de convergência de 56,6 segundos (10,80s a 67,40s) (Figura 38), o que em comparação com os cenários anteriores era significativamente mais elevado.

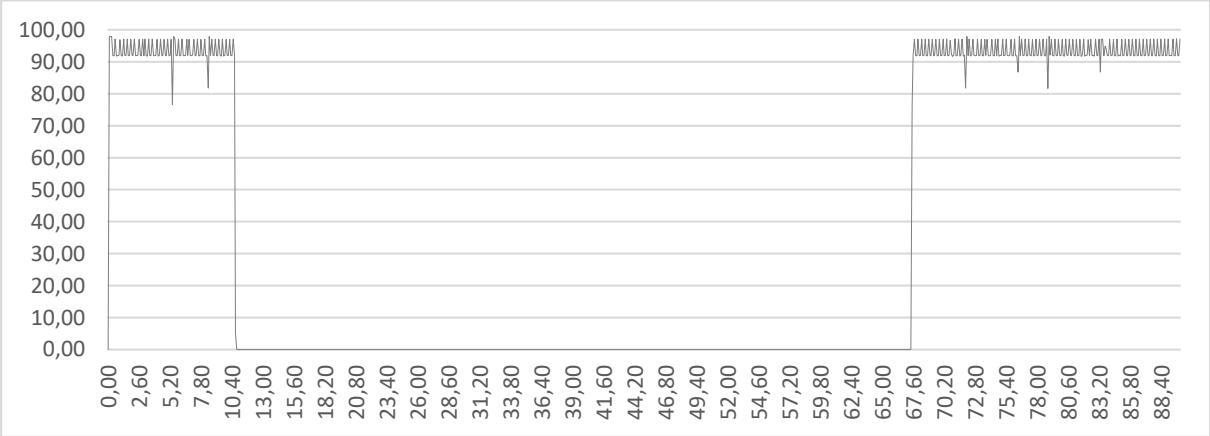

Figura 38 – Tempo de convergência em caso de falha (Cenário 3)

5.5.5 Cenário 4

Uma vez que se pretende integrar caminhos explícitos no quarto cenário, removeram-se as configurações relativas à criação de LSP's dinâmicos.

Foram então configurados, em cada PE, dois caminhos explícitos para cada nó PE de pólos vizinhos (Figura 89 e Figura 90). Estes dois caminhos explícitos foram formados de forma a também oferecerem proteção extremo-a-extremo, sendo para isso necessário que não possuíssem nenhum nó ou ligação coincidente. A Tabela 20 apresenta todos os caminhos explícitos configurados.

Tabela 20 – Caminhos explícitos

Origem	Destino	Caminho	Origem	Destino	Caminho
PE-1	PE-2	PE-1 → P1 → PE-2	PE-4	PE-1	PE-4 → P2 → P3 → PE-1
		PE-1 → P3 → PE-2			PE-4 → P1 → PE-1
	PE-3	PE-1 → P3 → P2 → PE-3		PE-2	PE-4 → P2 → P3 → PE-2
		PE-1 → P1 → PE-3			PE-4 → P1 → PE-2
	PE-4	PE-1 → P3 → P2 → PE-4		PE-3	PE-4 → P2 → PE-3
		PE-1 → P1 → PE-4			PE-4 → P1 → PE-3
	PE-5	PE-1 → P1 → P2 → PE-5		PE-5	PE-4 → P1 → P3 → PE-5
		PE-1 → P3 → PE-5			PE-4 → P2 → PE-5
	PE-6	PE-1 → P1 → P2 → PE-6		PE-6	PE-4 → P1 → P3 → PE-6
		PE-1 → P3 → PE-6			PE-4 → P2 → PE-6
PE-2	PE-1	PE-2 → P1 → PE-1	PE-5	PE-1	PE-5 → P2 → P1 → PE-1
		PE-2 → P3 → PE-1			PE-5 → P3 → PE-1
	PE-3	PE-2 → P3 → P2 → PE-3		PE-2	PE-5 → P2 → P1 → PE-2
		PE-2 → P1 → PE-3			PE-5 → P3 → PE-2
	PE-4	PE-2 → P3 → P2 → PE-4		PE-3	PE-5 → P3 → P1 → PE-3
		PE-2 → P1 → PE-4			PE-5 → P2 → PE-3
	PE-5	PE-2 → P1 → P2 → PE-5		PE-4	PE-5 → P3 → P1 → PE-4
		PE-2 → P3 → PE-5			PE-5 → P2 → PE-4
	PE-6	PE-2 → P1 → P2 → PE-6		PE-6	PE-5 → P3 → PE-6
		PE-2 → P3 → PE-6			PE-5 → P2 → PE-6
PE-3	PE-1	PE-3 → P2 → P3 → PE-1	PE-6	PE-1	PE-6 → P2 → P1 → PE-1
		PE-3 → P1 → PE-1			PE-6 → P3 → PE-1
	PE-2	PE-3 → P2 → P3 → PE-2		PE-2	PE-6 → P2 → P1 → PE-2
		PE-3 → P1 → PE-2			PE-6 → P3 → PE-2
	PE-4	PE-3 → P2 → PE-4		PE-3	PE-6 → P3 → P1 → PE-3
		PE-3 → P1 → PE-4			PE-6 → P2 → PE-3
	PE-5	PE-3 → P1 → P3 → PE-5		PE-4	PE-6 → P3 → P1 → PE-4
		PE-3 → P2 → PE-5			PE-6 → P2 → PE-4
	PE-6	PE-3 → P1 → P3 → PE-6		PE-5	PE-6 → P3 → PE-5
		PE-3 → P2 → PE-6			PE-6 → P2 → PE-5

Com a introdução da proteção extremo-a-extremo era expectável que o tempo de convergência em caso de falha fosse bastante mais reduzido do que os cenários anteriores. Para analisarmos este facto na prática foi novamente realizado um teste para mensurar o tempo de convergência. O gráfico da Figura 39 apresenta o resultado da convergência com cerca de 0,1 segundos (10,30s a 10,40s).

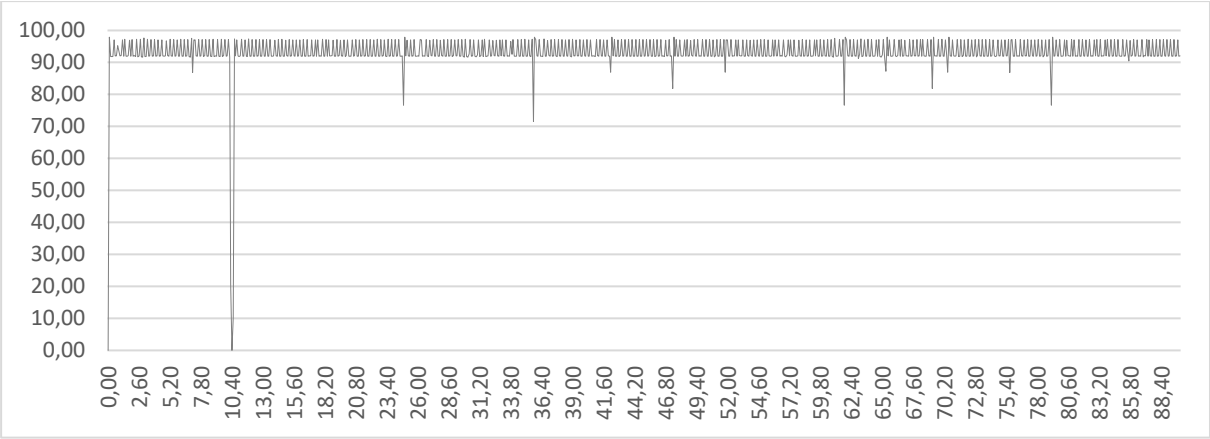

Figura 39 – Tempo de convergência em caso de falha (Cenário 4)

5.5.6 Cenário 5

No quinto cenário foi novamente pretendida a utilização de proteção extremo-a-extremo, assim como no cenário anterior, com a diferença de que no estabelecimento do caminho secundário se recorre à informação dinâmica associada ao OSPF. Adicionalmente, foi também configurada a proteção local com a integração da técnica *fast reroute one-to-one* (Figura 91 e Figura 92). Devido à impossibilidade de utilização de proteção local nos nós PE Cisco, não foi possível a implementação das técnicas de *fast reroute*, pelo que se utilizou exclusivamente equipamento do fabricante Nokia na camada de transporte.

Com a integração da proteção local por *fast reroute one-to-one* torna-se relevante analisar os *detours* criados pelos nós intervenientes, ou seja, os nós que participam no caminho protegido (PE-1 e P1). A Figura 40 ilustra os caminhos protetores sinalizados pelos nós PE-1 e P1, em detrimento da proteção local configurada em PE-1.

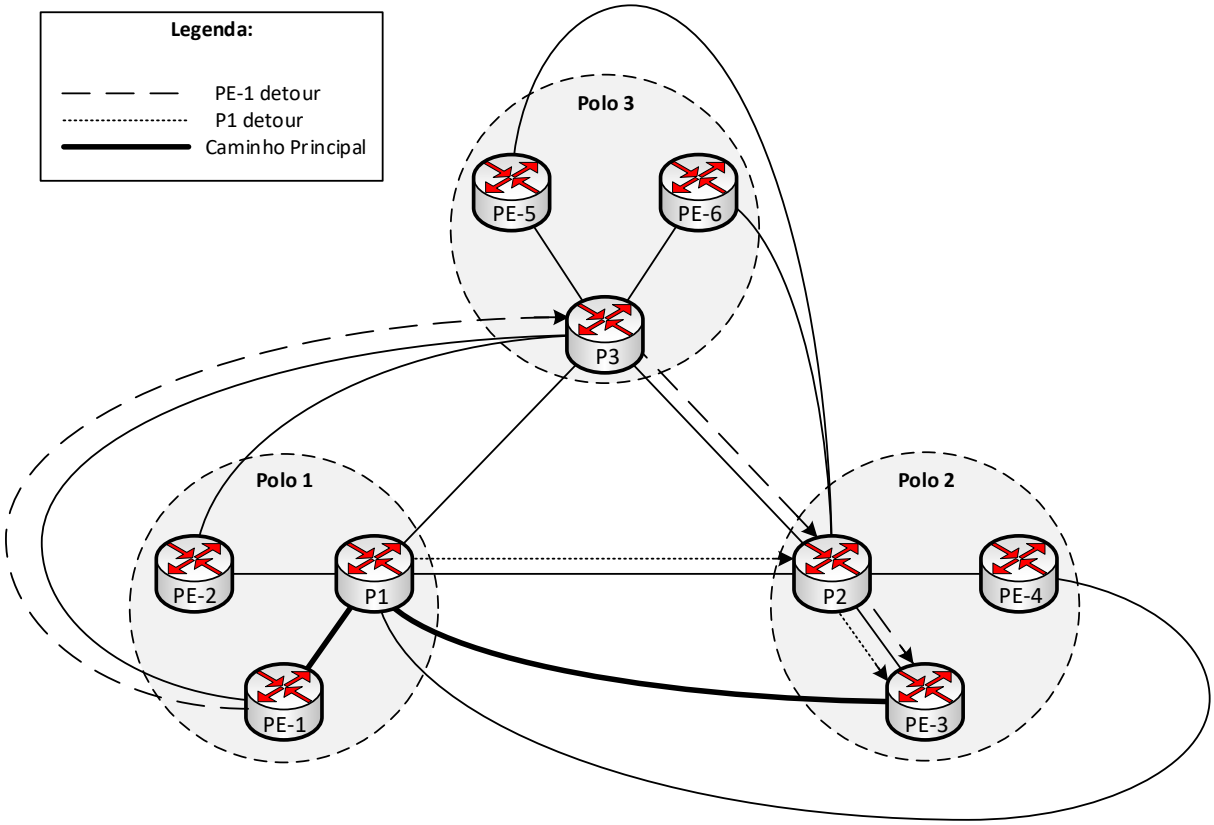

Figura 40 – Esquema de proteção local com *fast reroute one-to-one* em PE-1

De modo a aferirmos o tempo de convergência em caso de falha foi realizada uma quebra de ligação entre P-1 e PE-3. O gráfico apresentado na Figura 41 demonstra um tempo de indisponibilidade de 0,6 segundos (11,20s a 11,80s).

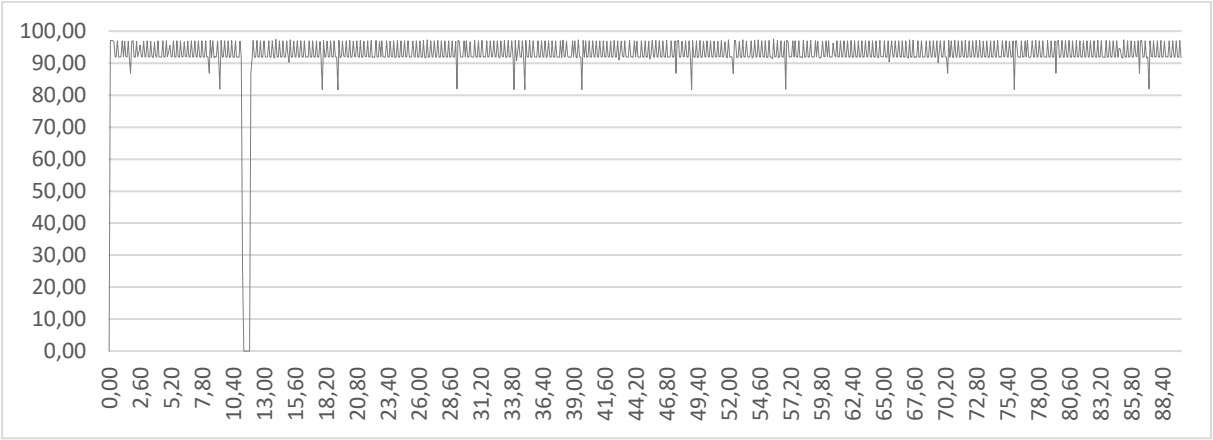

Figura 41 - Tempo de convergência em caso de falha (Cenário 5)

5.5.7 Cenário 6

O último cenário de implementação de serviços VPLS abrange a utilização da proteção local por *Fast Reroute Facility*, e acrescenta ainda a redundância nos *attchment-circuits* com a adição de LAG, e posteriormente MC-LAG. Assim como aconteceu no cenário anterior, neste também não foram integrados equipamentos Cisco, pela falta de capacidade nos modelos disponíveis, de suporte das técnicas de *fast reroute*.

A implementação de proteção local por *Fast Reroute Facility* foi bastante simples uma vez que apenas se teve de alterar o tipo de proteção em relação ao cenário anterior (Figura 93). Assim como aconteceu no cenário anterior, esta técnica de proteção foi analisada, como se pode verificar pela Figura 42.

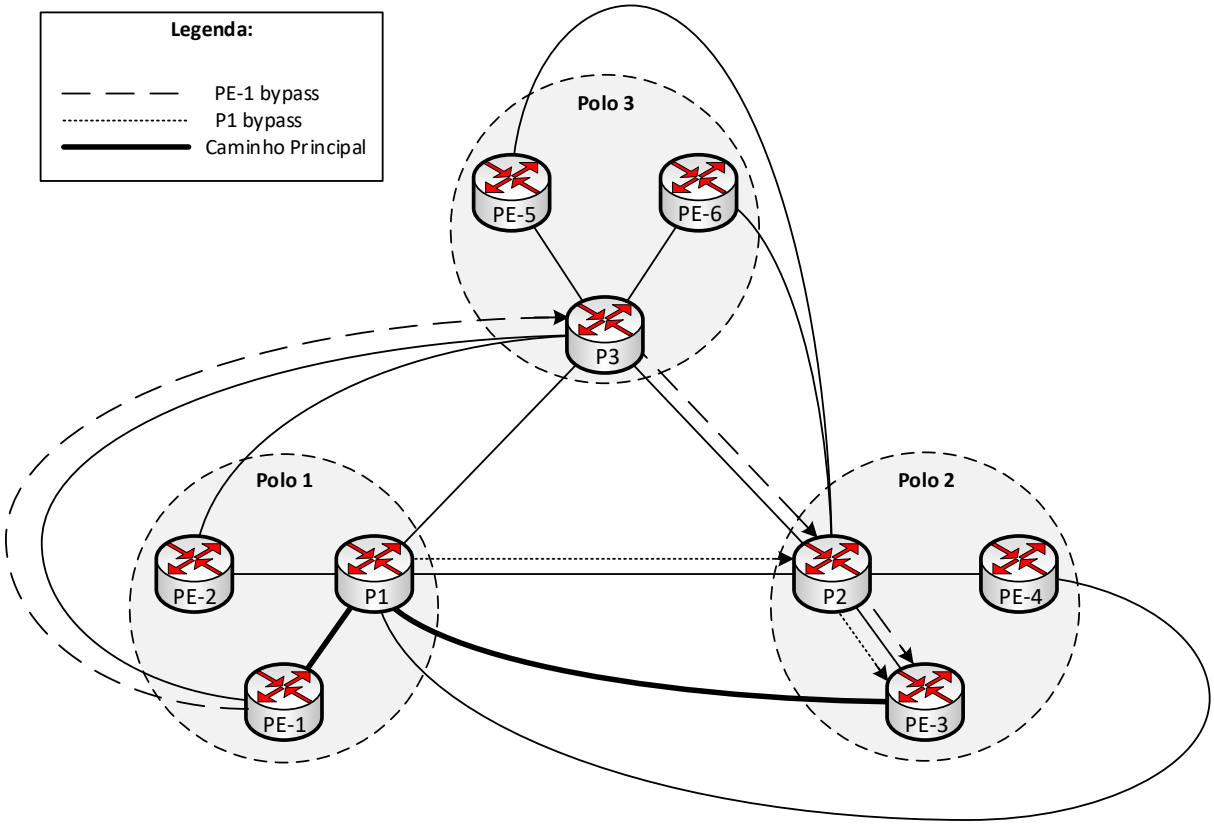

Figura 42 – Esquema de proteção local com *fast reroute facility* em PE-1

Por comparação ao esquema de proteção local com *fast reroute one-to-one*, apresentado no cenário anterior, verifica-se para o caso em concreto que os túneis *detour* e *bypass* seguem o mesmo caminho. O mesmo acontece com o tempo de indisponibilidade que é o mesmo, 0,6 segundos (10,40s a 11,00s), como se pode visualizar pela Figura 43.

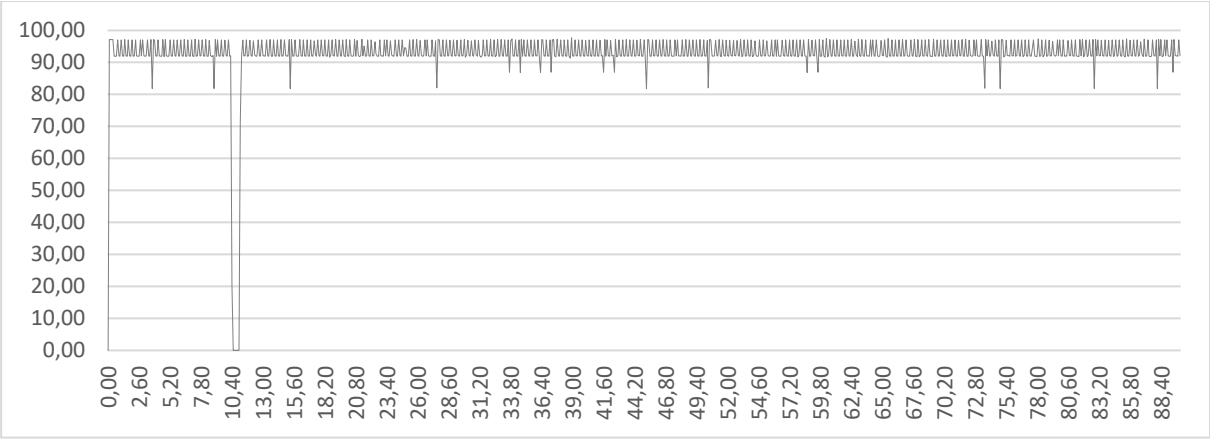

Figura 43 - Tempo de convergência em caso de falha (cenário 6)

Depois de analisada a proteção no *core* da rede MPLS decidiu-se implementar as técnicas de redundância para o *attachment-circuit* anteriormente referidas, nomeadamente por recurso aos mecanismos LAG e MC-LAG.

Redundância de *attachment-circuit* - LAG

A implementação de LAG como técnica de proteção do *attachment-circuit* sugere a interligação de duas ou mais ligações entre o nó PE e o equipamento do cliente ou CPE. A Figura 44 ilustra o esquema de redundância implementado com a utilização de LAG, onde rapidamente se verifica que esta técnica apenas assegura quebras de *link* e não falhas do nó.

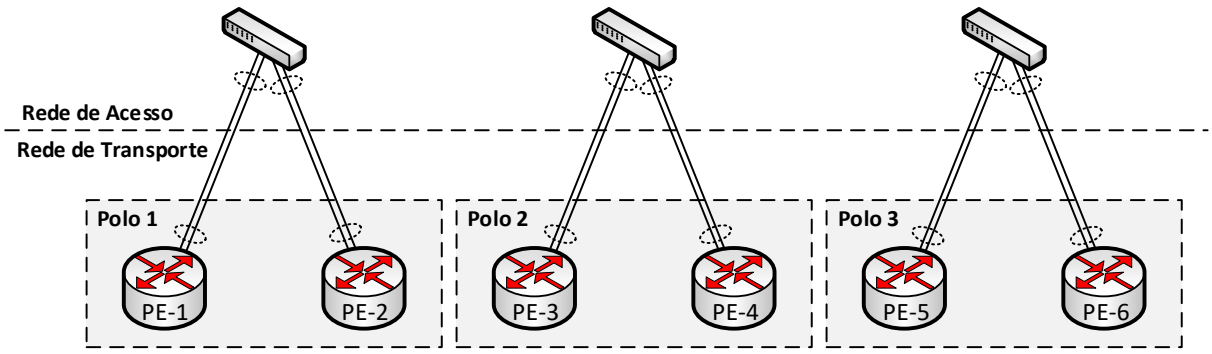

Figura 44 – Esquema de redundância para *attachment-circuit* com LAG

Tendo em conta o esquema apresentado, em cada PE foi configurado um LAG constituído por duas interfaces ligadas ao equipamento do cliente, enquanto que em cada CE do cliente foram configurados dois LAG's, um para cada PE de ligação (Figura 94, Figura 95 e Figura 96).

De modo a analisar uma possível quebra de conetividade foi, de forma propositada, cortada uma das ligação entre o PE-1 e o CE-1, onde se verificou um tempo de indisponibilidade de 1,5 segundos (10,40s a 11,90s) (Figura 45).

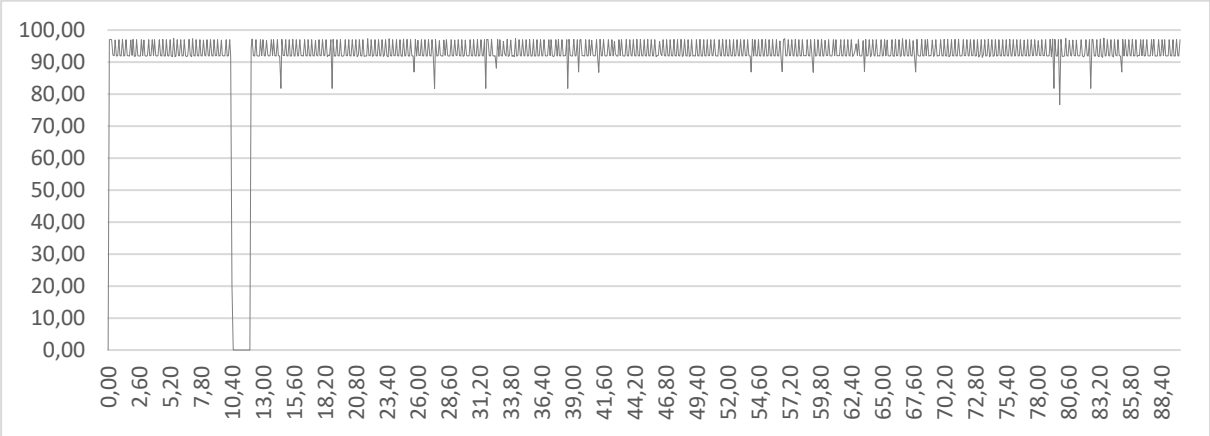

Figura 45 – Tempo de convergência em caso de falha (LAG)

Redundância de *attachment-circuit* – MC-LAG

Ao analisarmos o LAG como técnica de redundância para o *attachment-circuit* verificámos que esta não oferece redundância de nó, ou seja, se o nó PE falhar os serviços irão também falhar. Posto isto, recorreu-se a implementação de MC-LAG com o intuito de oferecer redundância de serviços MPLS a partir de diferentes PE's. A Figura 46 apresenta o esquema de redundância por MC-LAG, onde se verifica que o equipamento do cliente se interliga a dois nós PE distintos, no entanto com a mesma interface LAG.

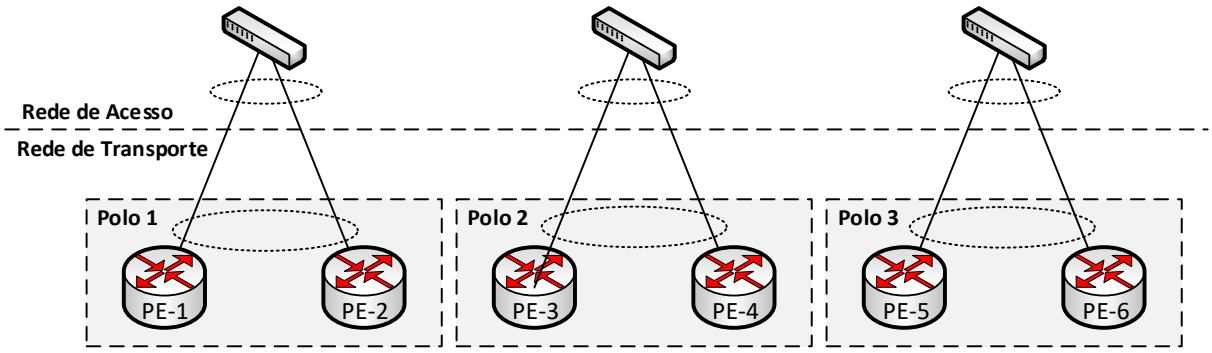

Figura 46 - Esquema de redundância para *attachment-circuit* com MC-LAG

Infelizmente, os nós PE Cisco IOS não possuiam a capacidade de oferecer MC-LAG, e assim sendo esta técnica foi apenas testada nos nós Nokia PE-1 e PE-2 (Figura 97 e Figura 98). Do ponto de vista do equipamento do cliente a configuração resume-se à definição de um LAG, no

entanto, com a particularidade de que os *links* que o compõem não têm o mesmo destino na rede de transporte

Nesse contexto, foram também realizados testes de aferição de comportamento de falha, analisando-se o tempo de convergência. Para simular a falha realizou-se a interrupção da ligação entre PE-1 e o CE-1, onde se verificou um tempo de indisponibilidade do serviço durante 56,4 segundos (10,40s a 66,80s) como se verifica na Figura 47.

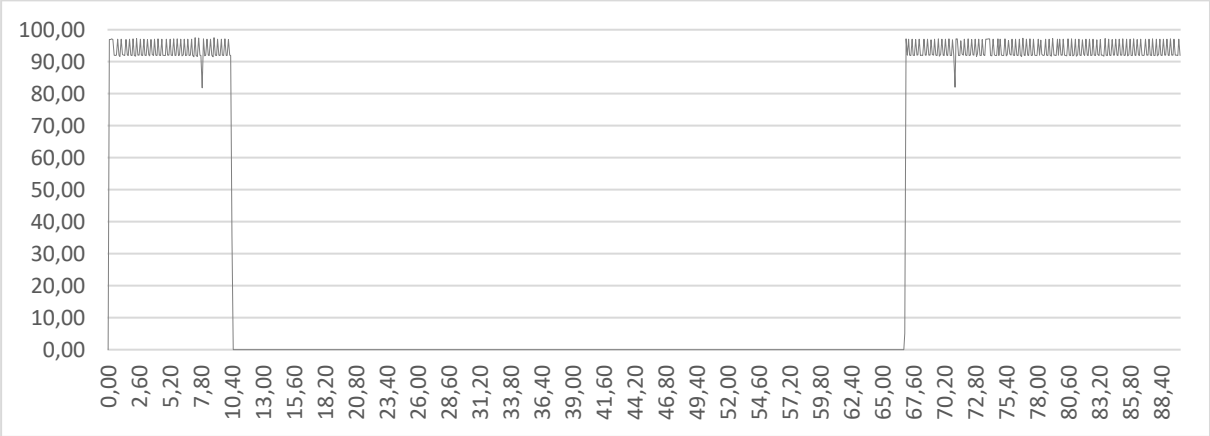

Figura 47 - Tempo de convergência em caso de falha (LAG)

5.5.8 Implementação de técnicas de OAM

Para além dos cenários que visam o estudo do tema da proteção, foram também analisadas e implementadas técnicas de operação, administração e manutenção, com o objetivo de se analisar o correto funcionamento dos LSP's extremo-a-extremo. Além disto, foi também configurado um *service mirror* de forma a analisarmos a informação trocada na rede de *backbone*, mais precisamente a informação enviada e recebida pelo nó PE-1 (Nokia).

Quanto à análise sobre o correto funcionamento dos LSP's, foram, manualmente, inseridos comandos com o objetivo de validar a conetividade dos LSP's e também os *hops* do mesmo. A Figura 100 e Figura 101 apresentam as configurações efetuadas nos nós PE-1 (Nokia) e PE-4 (Cisco), onde se avaliou a disponibilidade do LSP's e ainda se aferiu o "caminho" do mesmo.

De seguida, e de forma a analisar o processo de troca de etiquetas na rede *backbone*, procedeu-se à configuração de um *service mirror* local em PE-1 (Figura 102). O esquema da Figura 48 representa o cenário de testes, onde se definiu que todo o tráfego de entrada ou de saída proveniente da porta 1/1/6 do PE-1 é copiado integralmente e encaminhado para a porta 1/1/9, onde se encontra à escuta um servidor Wireshark [58].

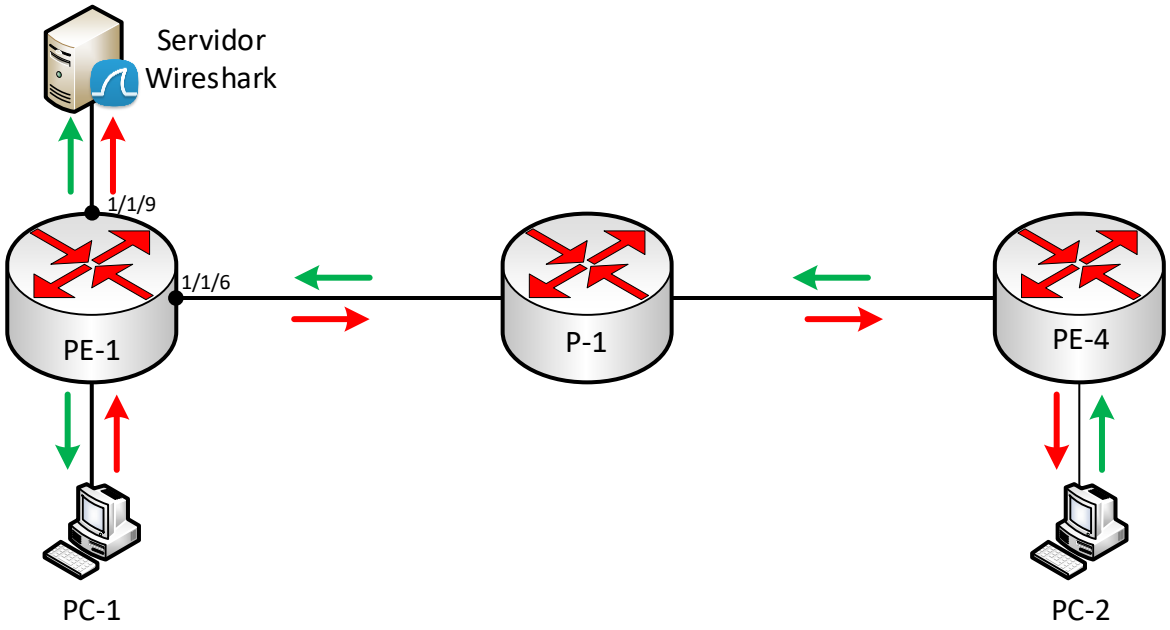

Figura 48 – Esquema de *service mirror* local

Através do processo de captura foi possível analisar os dados provenientes de PE-1, que juntamente com comandos de *troubleshooting* permitiram identificar as origens e destinos dos pacotes analisados, tendo-se concluido que um dos pacotes pertencia ao par origem-destino <PE-1 – PE-4> e o outro ao par <PE-4 – PE-1>.

No anexo VII são apresentadas as informações de *troubleshooting* sobre os equipamentos de rede apresentados no esquema acima, através das quais foi também possível formar as tabelas de etiquetas apresentadas pela Tabela 21.

Tabela 21 – Tabelas de comutação de etiquetas

	Túneis PE-1 para PE-4			
	LSP Label		PW Label	
	In	Out	In	Out
PE-1	n/a	131069	n/a	52
P-1	131069	0	n/a	n/a
PE-4	0	n/a	52	n/a

	Túneis PE-4 para PE-1			
	LSP Label		PW Label	
	In	Out	In	Out
PE-4	n/a	131066	n/a	131046
P-1	131066	131043	n/a	n/a
PE-1	131043	n/a	131046	n/a

5.6 Implementação do serviço VPRN

Apesar da rede de transporte da Universidade do Porto não prestar serviços MPLS de nível 3 às suas unidades orgânicas, decidiu-se estudar a implementação dos mesmos de modo a também aferir as suas mais valias de utilização, comparativamente aos serviços de nível 2.

Ao analisar os serviços de nível 3, surge a necessidade imperativa de integração de um protocolo dinâmico de routing inerente ao serviço VPRN em causa, para que assim as rotas dos clientes possam ser distribuídas pelos diferentes *sites*. No entanto, deve-se referir que a utilização de um protocolo dinâmico não é obrigatória, podendo-se em detrimento, utilizar rotas estáticas apesar de não ser uma opção escalável.

Foram elaborados dois cenários de implementação com o intuito de analisar os protocolos de sinalização a efetuar e respetivas configurações (Anexo VIII):

- Cenário 1: Utilização do protocolo LDP para sinalização dos LSP's, o protocolo MP-BGP para sinalização dos *pseudowires* e o protocolo OSPF na ligação IP com os clientes;
- Cenário 2: Utilização do protocolo RSVP para sinalização dos LSP's, o protocolo MP-BGP para sinalização dos *pseudowires* e o protocolo OSPF para interligação com os clientes;

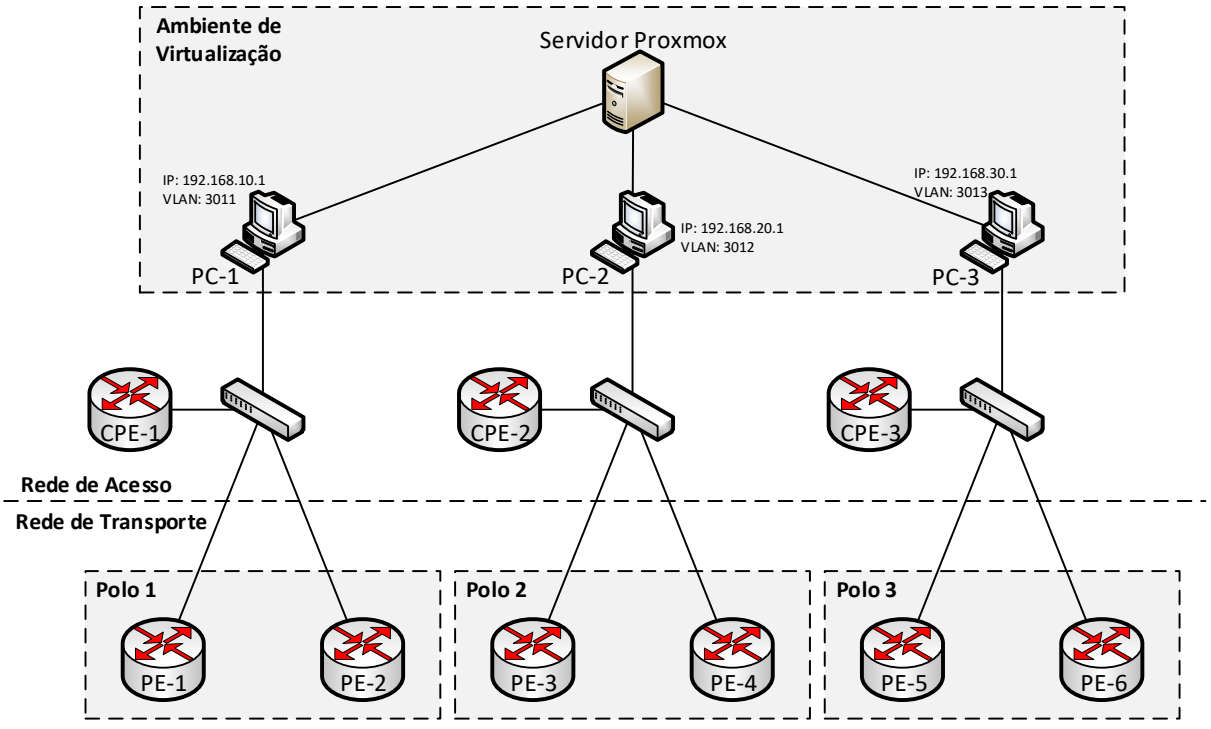

Figura 49 – Topologia do laboratório VPRN

Dada a necessidade de utilização do protocolo OSPF no equipamento presente na periferia do cliente, foi essencial voltar a incluir na topologia CPE's de nível 3, isto é, *routers* capazes de suportar o protocolo dinâmico de *routing* em causa (Figura 49).

As tarefas de configuração adotadas foram semelhantes às utilizadas anteriormente nos serviços VPLS, ou seja, primeiramente foram realizadas as configurações genéricas a ambos os cenários onde se incluía o aprovisionamento das interfaces de rede e configuração dos protocolos OSPF, MPLS e BGP.

A configuração prévia do protocolo BGP teve especial relevo pela necessidade de integração da família de endereços *vpn-ipv4*, a partir da qual é possível fazer uso do MP-BGP para sinalização dos túneis de serviço (*pseudowires*) como proposto em ambos os cenários.

Depois de toda a configuração genérica na rede de transporte, foi configurado o serviço VPRN entre PE-1 e PE-4, onde se fez uso de um novo processo OSPF intrínseco ao serviço para propagação de rotas do cliente. Posto isto, em cada *router* CPE do cliente foi também configurado um processo OSPF onde são indicadas as redes a propagar pelo serviço em questão (Figura 136).

De modo a testar o funcionamento do serviço fez-se uma vez mais uso do sistema de virtualização Proxmox, onde se realizaram testes de conetividade entre máquinas virtuais de diferentes *sites* clientes.

5.7 Análise de resultados

A implementação dos serviços de transporte tipicamente oferecidos em redes IP/MPLS, nomeadamente o VPLS e o VPRN permitiram obter uma série de resultados importantes a ter em conta para uma futura otimização da rede da Universidade do Porto.

Paralelamente aos serviços, a implementação focou-se na análise das estratégias de proteção, tanto ao nível do operador como ao nível do cliente.

Os resultados relativos aos tempos de indisponibilidade em situações de falha, por cenário testado, encontram-se demonstrados pela tabela abaixo.

Tabela 22 – Sumário dos tempos de indisponibilidade obtidos

Cenário	Descrição	Proteção Extremo-a-Extremo	Proteção Local	Tempo de Indisponibilidade
1	Descoberta dos nós PE por BGP Auto-Discovery e sinalização do PW por T-LDP.	Não	Não	6,6 segundos
2	Sinalização do LSP por LDP.	Não	Não	6,7 segundos
3	Sinalização do LSP por RSVP, recorrendo túneis dinâmicos.	Não	Não	56,6 segundos
4	Integração de TE com LSP's estabelecidos manualmente.	Sim	Não	0,1 segundos
5	TE com túnel manual protegido por um túnel dinâmico, com FRR One-to-One.	Sim	Sim (Fast Reroute One-to-One)	0,6 segundos
6	TE com túnel manual protegido por um túnel dinâmico, com FRR Facility.	Sim	Sim (Fast Reroute Facility)	0,6 segundos
6.1	Implementação de LAG	Sim	Sim (Fast Reroute Facility)	1,5 segundos
6.2	Implementação de MC-LAG	Sim	Sim (Fast Reroute Facility)	56,4 segundos

No que diz respeito aos resultados obtidos a nível dos vários cenários onde se aferiu a questão da resiliência, verificou-se como era expectável, que os cenários que incluem proteção têm melhores tempos de recuperação e que a proteção local acrescenta eficácia ao processo, ao contrário do cenário 3 onde o tempo de recuperação à falha foi cerca de um minuto.

O primeiro cenário apresentado contempla os protocolos em operação na rede da Universidade do Porto onde se verificou um tempo de indisponibilidade de 6,6 segundos em caso de falha, que em comparação com o cenário 4 apresenta um tempo de recuperação mais moroso em 6,5 segundos.

Quanto aos testes de convergência causados na ligação com o cliente (*attachment-circuit*), estes devem também ser objeto de análise. Ao protegermos a ligação ao cliente com LAG verificou-se um tempo de indisponibilidade de 1,5 segundos, que em comparação com o MC-LAG é bastante mais reduzido. No entanto, devemos ter em consideração o facto de que o MC-LAG protege a ligação do cliente da falha do nó a jusante.

Neste capítulo, ao terem sido abordados os serviços de nível 2 e nível 3, levantou-se também uma questão relativa à escolha de serviços de nível 3 em detrimento de serviços de nível 2, e vice-versa, e ainda a possibilidade da Universidade do Porto implementar serviços de nível 3. Estas questões, pela importância que auferem, serão abordadas no capítulo 6 relativo às conclusões e trabalho futuro.

É importante salientar que todos os cenários foram testados em ambiente controlado, tanto ao nível do número de serviços em operação, como relativamente à dimensão topológica. Posto isto, é expectável que os tempos de recuperação a falhas obtidos aumentem em redes de larga escala.

6. CONCLUSÕES E TRABALHO FUTURO

O presente capítulo apresenta as principais conclusões do projeto realizado, assim como as principais dificuldades ao longo do mesmo. Por fim, apresenta-se algumas diretrizes para trabalho futuro.

6.1 Conclusões

A Universidade do Porto contempla 51 unidades orgânicas às quais oferece serviços de conetividade internos e externos, recorrendo a uma rede de transporte. Em 2012, o *core* da rede foi migrada da tecnologia IP *routing* para a tecnologia MPLS, opção que se revelou essencial e acertada uma vez que o MPLS oferece eficácia na comutação de pacotes, flexibilidade na oferta de serviços possibilitando cenários ponto-a-ponto e multiponto quer de nível 2 como de nível 3, e elevada adaptabilidade em cenários tecnológicos convergentes.

Contudo, e até intrínseco ao objetivo fundamental deste projeto, a ausência de funcionalidades de proteção, mecanismos de garantia de SLA's extremo-a-extremo e estratégias de otimização de largura de banda são, sem dúvida, aspetos a melhorar na rede em operação.

O ponto fulcral dos cenários propostos foi a disposição dos equipamentos de rede, criando-se uma distinção topológica entre os nós de periferia e os nós de *backbone*. Este aspeto permite a inclusão de engenharia de tráfego, oferecendo-se a possibilidade de tratamento diferenciado aos diversos serviços prestados.

De igual forma, apesar da rede de transporte em exploração fornecer fundamentalmente serviços multiponto de nível 2, pareceu igualmente essencial estudar os serviços VPRN, as suas particularidades de implementação e os protocolos inerentes ao seu funcionamento. Este tipo de serviços, enquadra o caso concreto do fornecimento de acesso à *internet* fundamental no portefólio dos serviços disponibilizados na rede MPLS, e que deve evoluir para um cenário de *routing* dinâmico.

A falta de uma ferramenta de aprovisionamento dedicada à rede de *backbone* aliada à estratégia de centralização de serviços disponibilizados nos *data centers* condicionou alguns dos cenários propostos para alteração topológica do núcleo de rede.

Importa salientar que a dinâmica de centralização dos serviços condiciona uma possível atualização da infraestrutura, uma vez que a Universidade do Porto terá de ter a capacidade de

aliar os requisitos do operador e do cliente simultaneamente, tendo especial atenção às ligações do equipamento de rede do *data center* ao *core*.

Esta problemática justifica a obrigatoriedade de implementação de cenários resilientes, por recurso à utilização de engenharia de tráfego, fator crítico para a garantia dos SLA's, uma vez que as redes locais das unidades orgânicas serão constituídas "apenas" por equipamentos terminais.

A este nível, o presente projeto de mestrado comprova a necessidade de implementação do protocolo RSVP aliado às técnicas de proteção local por *fast reroute* e proteção extremo-a-extremo, bem como a definição de túneis explícitos, e ainda a necessidade de salvaguardar a rede de acesso através de técnicas de proteção oferecidas pelo LAG e/ou MC-LAG.

Importa salientar que os equipamentos Cisco 6840-X adquiridos com o objetivo de integrarem a rede IP/MPLS não possuem a capacidade de implementação dos mecanismos de proteção local e de proteção por via de MC-LAG, pelo que é necessário que na renovação da topologia de rede sejam estrategicamente colocados na periferia.

Apesar de a rede de transporte estar distribuída por quatro pólos, nomeadamente na FCUP, FDUP, FEUP e Reitoria, a sala técnica da FDUP não contempla equipamento responsável pela disponibilização dos serviços centrais. Assim, propõe-se que o equipamento de comutação do pólo 4 não integre o domínio MPLS em operação, preconizando-se a instalação de *switches ethernet*.

A gestão operacional deve incluir técnicas de operação, administração e manutenção de forma a garantir o controlo sobre o estado e utilização dos túneis associados aos serviços MPLS, nomeadamente os exteriores (LSP's) e os interiores (*pseudowires*). De forma a tornar o processo de gestão automatizado deve-se recorrer a ferramentas como o Zabbix, com funcionalidades de descoberta automática.

Para além disto, a rede *backbone* deve ainda contemplar a capacidade de realizar *service mirroring* de forma a complementar a gestão operacional e garantir uma técnica integrada de *troubleshooting*.

6.2 Trabalho futuro

Enumeram-se de seguida um conjunto de ações em termos de trabalho futuro, a realizar no âmbito deste projeto de mestrado.

Avaliar a possibilidade de melhoria das condições de resiliência do *backbone* da Universidade do Porto, ao nível da infraestrutura ativa e passiva.

Enquadrado com as conclusões do presente relatório é necessário definir uma estratégia de renovação da infraestrutura ativa, incluindo a demarcação das funcionalidades de cada equipamento na rede MPLS, impondo na medida do possível, uma topologia *full-mesh* entre nós P, a interligação P-PE por via de ligações *dual-homed* e os *attachment-circuits* protegidos por mecanismos de resiliência.

Na componente passiva sugere-se a renegociação das condições técnicas oferecidas pela rede metropolitana Porto Digital com vista à prestação de serviços de fibra-escura em detrimento de serviços comutados, passando desta forma a para o âmbito da UP a componente de transmissão na interligação com as unidades orgânicas não abrangidas pelos anéis de fibra ótica próprios.

Incluir na infraestrutura de transporte da Universidade do Porto técnicas de engenharia de tráfego, nomeadamente mecanismos de proteção e ferramentas que garantam SLA's extremo-a-extremo.

Suprir a ausência de uma plataforma de aprovisionamento e gestão de configurações dedicada à rede de transporte por meio de uma ferramenta comercial, ou por recurso a *standards open-source* tais como YANG e Netconf [59].

Integração na plataforma de gestão e monitorização atualmente em operação, de um módulo que permita aferir em tempo real SLA's extremo-a-extremo por cada serviço de transporte disponibilizado.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] R. Westbrook, "Action research: a new paradigm for research in production and operations management," *Int. J. Oper. Prod. Manag.*, vol. 15, no. 12, pp. 6–20, 1995.

[2] M. Serrão, "Implementação de uma rede de difusão ótica de TV no Município do Porto," Relatório de Projeto de Mestrado, ISMAI, 2017.

[3] J. M. Oliveira, R. D. Lins, and R. Mendonça, *Redes MPLS: Fundamentos e Aplicações*. Brasport, 2012.

[4] E. C. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture," p. 11, 2001.

[5] R. A. Downing, "Frame Relay + MPLS," *Frame Relay Forum*. pp. 1–4, 2001.

[6] G. Coutinho, "Estudo para uma Rede Metropolitana Comunitária," Tese de Mestrado, FEUP, 2006.

[7] M. S. Nunes, "Redes com Integração de Serviços (RIS)," 2004.

[8] O. O.A, "Asynchronous Transfer Mode (ATM) Network," pp. 70–82, 2009.

[9] J. A. Nakamura, "Evolução das Redes de Telecomunicação e o Multiprotocol Label Switching (MPLS)," 2009.

[10] J.-P. Laude, *DWDM Fundamentals, Components, and Applications*. 2002.

[11] Sudhir Dixit, *IP OVER WDM: Building the Next Generation Optical Internet*. New Jersey: John Wiley & Sons, Inc., 2003.

[12] Cianet, "O que é a tecnologia WDM e como ela pode otimizar a transmissão de um provedor," 2014. [Online]. Available: https://www.cianet.com.br/blog/infraestrutura-e-tecnologia/o-que-e-tecnologia-wdm-e-como-ela-pode-otimizar-transmissao-de-um-provedor/.

[13] C. Hunt, *TCP/IP Network Administration*. 2002.

[14] A. G. Blank, *TCP/IP JumpStart: Internet Protocol Basics*. Neil Edde, 2006.

[15] N.-K. Tan, *MPLS for Metropolitan Area Networks*, vol. 15. 2004.

[16] F. Palmieri, "Introducing virtual private overlay network services in large scale Grid infrastructures," *J. Comput.*, vol. 2, no. 2, pp. 61–72, 2007.

[17] E. Rosen *et al.*, "MPLS Label Stack Encoding," 2001.

[18] K. Kompella *et al.*, "The Use of Entropy Labels in MPLS Forwarding," 2012.

[19] E. M. Bocci, E. M. Vigoureux, Alcatel-Lucent, E. S. Bryant, and C. Systems, "MPLS Generic Associated Channel," 2009.

[20] H. Ohta, “Assignment of the ’OAM Alert Label’ for Multiprotocol Label Switching Architecture (MPLS) Operation and Maintenance (OAM) Functions,” 2002.

[21] K. Kompella, J. Networks, L. Andersson, and A. Farrel, “Allocating and Retiring Special-Purpose MPLS Labels,” 2014.

[22] S. J. Harnedy, *The MPLS Primer*. Prentice Hall PTR, 2002.

[23] P. Brittain and A. Farrel, “Mpls Traffic Engineering : a Choice of Signaling Protocols,” pp. 1–31, 2000.

[24] L. Andersson, P. Doolan, N. Feldman, A. Fredette, and B. Thomas, “LDP Specification,” 2001.

[25] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, and G. Swallow, “RSVP-TE: Extensions to RSVP for LSP Tunnels,” 2001.

[26] L. De Ghein, *MPLS Fundamentals - A Comprehensive Introduction to MPLS Theory and Practice*. 2006.

[27] G. Warnock and A. Nathoo, *Alcatel-Lucent Network Routing Specialist II (NRS II)*. 2011.

[28] B. S. Davie and A. Farrel, *MPLS: Next Steps*. 2008.

[29] Z. Xu, *Designing and Implementing IP/MPLS Based Ethernet Layer 2 VPN Services - An Advanced Guide for VPLS and VLL*. Wiley, 2010.

[30] S. Bryant and P. Pate, “Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture,” p. 42, 2005.

[31] L. Martini, N. El-Aawar, G. Heron, E. C. Rosen, and T. Smith, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*. 2006.

[32] L. Andersson *et al.*, “Framework for Layer 2 Virtual Private Networks (L2VPNs),” pp. 1–44, 2006.

[33] Juniper, “Demystifying H-Vpls,” *Juniper Appl. note*, pp. 1–11, 2010.

[34] Juniper Networks. Inc, “Junos ® OS MPLS Applications Feature Guide,” pp. 1237–1240, 2018.

[35] Vertel, “Layer 2 versus Layer 3 services: A Dummies Guide,” 2015. [Online]. Available: https://www.vertel.com.au/news-and-resources/blog/layer-2-versus-layer-3-services-a-dummies-guide.

[36] K. Ullah, H. Askary, A. Ajaz, A. Hassan, and H. Khan, “Routing Protocols and Their Limitations,” pp. 1–4, 2018.

[37] I. Cisco Systems, “Link Aggregation Group (LAG) Management and Settings on Sx500 Series Stackable Switches,” 2018. [Online]. Available:

https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-500-series-stackable-managed-switches/smb2860-link-aggregation-group-lag-management-and-settings-on-sx500.html.

[38] I. Cisco Systems, “High Scale Data Center Interconnect, LAN Extension Using MC-LAG to VPLS on the Cisco ASR-9000,” 2011. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DCI/vpls/vpls_asr9k/VPLS-ASR9K_4.html.

[39] W. Odom and M. J. Cavanaugh, *IP Telephony Self-Study Cisco DQOS Exam Certification Guide*. 2004.

[40] L. Lobo and U. Lakshman, *MPLS Configuration on Cisco IOS Software*. 2006.

[41] Cisco, “DiffServ - The Scalable End-to-End QoS Model,” 2005. [Online]. Available: https://www.cisco.com/en/US/technologies/tk543/tk766/technologies_white_paper09186a00800a3e2f.html. [Accessed: 30-Dec-2018].

[42] R. Braden, D. Clark, and S. Shenker, “Integrated Services in the Internet Architecture: an Overview,” pp. 1–28, 1994.

[43] J. Davidson, J. Peters, M. Bhatia, S. Kalindindi, and S. Mukherjee, *Voice over IP Fundamentals*. 2007.

[44] J. Ruela, “Serviços Integrados na Internet,” 2002.

[45] K. Nichols, S. Blake, F. Baker, and D. L. Black, “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers,” pp. 1–20, 1998.

[46] S. Blake, D. L. Black, M. A. Carlson, E. Davies, Z. Wang, and W. Weiss, “An Architecture for Differentiated Services,” pp. 1–36, 1998.

[47] R. A. Dias, “Serviços Diferenciados Baseado na Tecnologia MPLS em Redes Heterogêneas,” p. 8, 2001.

[48] B. S. Davie and Y. Rekhter, *MPLS: Technology and Applications*. Morgan Kaufmann Publishers, 2000.

[49] L. Andersson, H. van Helvoort, R. Bonica, D. Romascanu, and S. Mansfield, “Guidelines for the Use of the ‘OAM’ Acronym in the IETF Abstract,” pp. 1–9, 2011.

[50] D. P. Menezes and C. Roberto, “MPLS-TP : Técnicas de OAM,” pp. 1–5, 2017.

[51] I. Cisco Systems, “Cisco ASR 9000 Series Aggregation Services Router MPLS Configuration Guide, Release 4.2.x,” 2016. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-2/mpls/configuration/guide/b_mpls_cg42asr9k/b_mpls_cg42asr9k_chapter_0101.html. [Accessed: 23-May-2019].

[52] I. Nokia, “7750 SR OS OAM and Diagnostics Guide - Mirror Services,” pp. 17–48.

[53] I. Cisco Systems, “VPLS Autodiscovery: BGP Based,” 2007. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios/12_2sr/12_2srb/feature/guide/fs_vpls.html. [Accessed: 07-Jan-2019].

[54] I. Cisco Systems, “Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide, Release 4.2.x.” [Online]. Available: https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-2/lxvpn/configuration/guide/lesc42book/lesc42ethi.html. [Accessed: 08-Jan-2019].

[55] P. U. Rihards Olups, *Zabbix 4 Network Monitoring - Third Edition*. 2019.

[56] “Proxmox.” [Online]. Available: https://www.proxmox.com/en/about. [Accessed: 17-Jul-2019].

[57] “iPerf.” [Online]. Available: https://iperf.fr/. [Accessed: 08-Jun-2019].

[58] “Wireshark.” [Online]. Available: https://www.wireshark.org/.

[59] A. Filipe and B. Cardoso, “Automatização de Instanciação de Serviços de Rede numa Rede de Operador,” Relatório do Trabalho Final de Mestrado, ISEL, 2019.

[60] I. Cisco Systems, “MPLS Traffic Engineering : Shared Risk Link Groups (SRLG),” p. 30, 2004.

ANEXO I – ANÉIS DE FIBRA ÓTICA NA UNIVERSIDADE DO PORTO

As próximas figuras apresentam os dois anéis de fibra ótica própria existentes em operação na Universidade do Porto, mais especificamente em torno dos pólos 2 e 3.

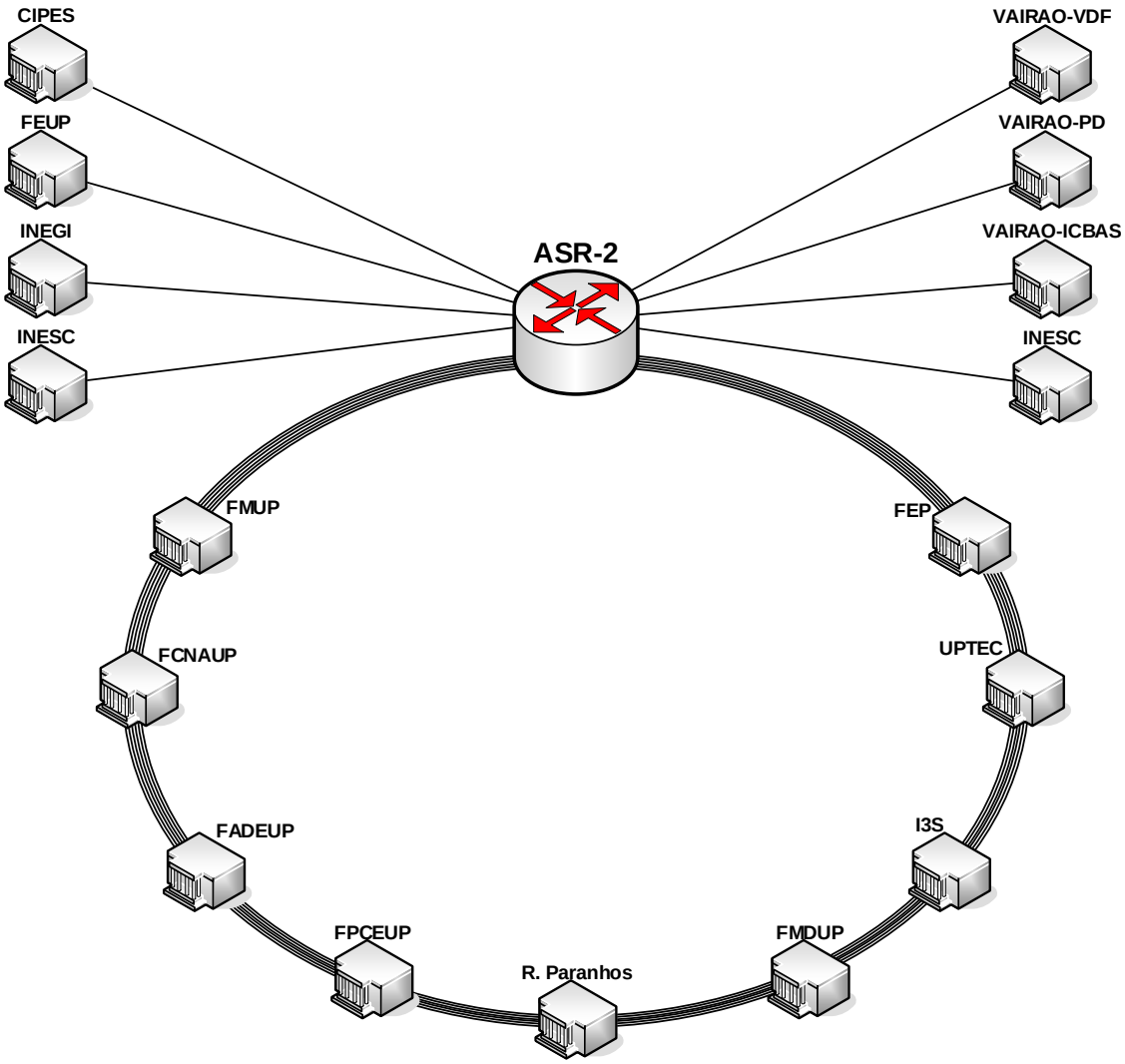

Figura 50 – Anel de fibra ótica no pólo 2 da Universidade do Porto

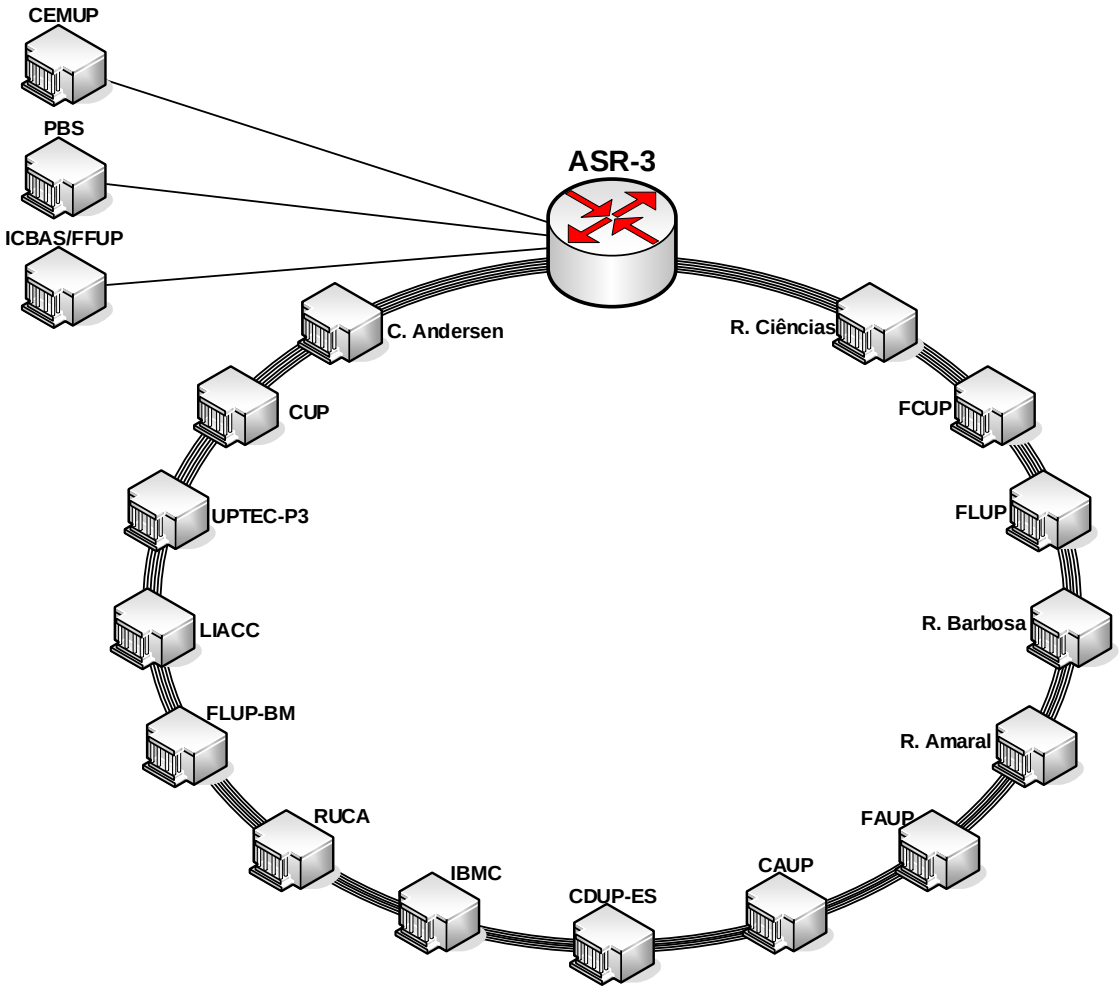

Figura 51 – Anel de fibra ótica no pólo 3 da Universidade do Porto

ANEXO II – CONFIGURAÇÃO DO SERVIÇO DE IMPRESSÃO NO ASR1

```
interface Loopback 10
 ipv4 address 172.17.0.1 255.255.255.255
!
```

Figura 52 – Configuração da interface *loopback*

```
router ospf 10
 nsr
 log adjacency changes detail
 router-id 172.17.0.1
 area 0.0.0.0
  mpls ldp sync
  interface Loopback10
  !
  interface TenGigE0/0/0/0.12
  !
  interface TenGigE0/0/0/1.14
  !
  interface TenGigE0/1/0/0.13
  !
```

Figura 53 – Configuração do processo OSPF

```
router bgp 65100
 nsr
 bgp router-id 172.17.0.1
 neighbor-group mbgp-session-PEERs
  remote-as 65100
  password encrypted ***secret***
  update-source Loopback10
 !
 neighbor 172.17.0.2
  use neighbor-group mbgp-session-PEERs
  description Polo 2 - FEUP
 !
 neighbor 172.17.0.3
  use neighbor-group mbgp-session-PEERs
  description Polo 3 - FCUP
 !
 neighbor 172.17.0.4
  use neighbor-group mbgp-session-PEERs
  description Polo 4 - FDUP
 !
```

Figura 54 – Configuração do processo BGP

```
mpls ldp
 router-id 172.17.0.1
 nsr
 graceful-restart
 session protection for LDP-PEERS
 explicit-null
 igp sync delay 10
 interface TenGigE0/0/0/0.12
 !
 interface TenGigE0/0/0/0.12
 !
 interface TenGigE0/0/0/0.12
 !
```

Figura 55 – Configuração do protocolo MPLS/LDP

```
interface Bundle-Ether1.100 l2transport
 description ***Serviço Impressao***
 encapsulation dot1q 1000
!
```

Figura 56 – Configuração do *attachment-circuit*

```
l2vpn
 ignore-mtu-mismatch-ad
 bridge-group Services-VPLS
  bridge-domain Servico-Impressao
   interface Bundle-Ether1.100
   !
   vfi VFI-Servico-Impressao
    vpn-id 1000
    autodiscovery bgp
     rd 65100:1000
     route-target 65100:1000
     signaling-protocol ldp
!
```

Figura 57 – Configuração do serviço de impressão - VPLS

ANEXO III – TABELAS DE COMUTAÇÃO DE ETIQUETAS

Tabela 23 – LFIB de ASR-1

ASR-1			
Prefixo de Rede	**Local Label**	**Remote Label**	**Next-Hop**
172.17.0.1/32	0	POP	-
172.17.0.2/32	100001	0	172.17.12.2
172.17.0.3/32	100002	0	172.17.13.3
172.17.0.4/32	100003	0	172.17.14.4
172.17.12.0/24	0	POP	-
172.17.13.0/24	0	POP	-
172.17.14.0/24	0	POP	-
172.17.23.0/24	100004	0	172.17.12.2
	100004	0	172.17.13.3
172.17.34.0/24	100005	0	172.17.13.3
	100005	0	172.17.14.4
172.17.0.2:1000	100010	POP	
172.17.0.3:1000	100011	POP	
172.17.0.4:1000	100012	POP	

Tabela 24 – LFIB de ASR-2

ASR-2			
Prefixo de Rede	**Local Label**	**Remote Label**	**Next-Hop**
172.17.0.1/32	200001	0	172.17.12.1
172.17.0.2/32	0	POP	-
172.17.0.3/32	200002	0	172.17.23.3
172.17.0.4/32	200003	100003	172.17.12.1
	200003	300003	172.17.23.3
172.17.12.0/24	0	POP	-
172.17.23.0/24	0	POP	-
172.17.13.0/24	200004	0	172.17.12.1
	200004	0	172.17.23.3
172.17.14.0/24	200005	0	172.17.12.1
	200005	300005	172.17.23.3
172.17.34.0/24	200006	0	172.17.23.3
	200006	100005	172.17.12.1
172.17.0.1:1000	200010	POP	
172.17.0.3:1000	200011	POP	
172.17.0.4:1000	200012	POP	

Tabela 25 – LFIB de ASR-3

ASR-3			
Prefixo de Rede	**Local Label**	**Remote Label**	**Next-Hop**
172.17.0.1/32	300001	0	172.17.13.1
172.17.0.2/32	300002	0	172.17.23.2
172.17.0.3/32	0	POP	-
172.17.0.4/32	300003	0	172.17.34.4
172.17.13.0/24	0	POP	-
172.17.23.0/24	0	POP	-
172.17.34.0/32	0	POP	-
172.17.12.0/24	300004	0	172.17.13.1
	300004	0	172.17.23.2
172.17.14.0/24	300005	0	172.17.13.1
	300005	0	172.17.34.4
172.17.0.1:1000	300010	POP	
172.17.0.2:1000	300011	POP	
172.17.0.4:1000	300012	POP	

Tabela 26 – LFIB de ASR-4

ASR-4			
Prefixo de Rede	**Local Label**	**Remote Label**	**Next-Hop**
172.17.0.1/32	400001	0	172.17.14.1
172.17.0.2/32	400002	100001	172.17.14.1
	400002	300002	172.17.34.3
172.17.0.3/32	400003	0	172.17.34.3
172.17.0.4/32	0	POP	-
172.17.14.0/24	0	POP	-
172.17.34.0/24	0	POP	-
172.17.12.0/24	400004	0	172.17.14.1
	400004	300004	172.17.34.3
172.17.13.0/24	400005	0	172.17.14.1
	400005	0	172.17.34.3
172.17.23.0/24	400006	0	172.17.34.3
	400006	100004	172.17.14.1
172.17.0.1:1000	400010	POP	
172.17.0.2:1000	400011	POP	
172.17.0.3:1000	400012	POP	

ANEXO IV – CAMINHOS DE COMUTAÇÃO DE ETIQUETAS (LSP'S)

Nas versões Cisco IOS-XR é possível verificar os LSP's criados através do comando *traceroute mpls ipv4 <ipv4_address/mask>*. A Figura 58, Figura 59 e Figura 60, demonstram os LSP's com origem no nó do pólo 1 e com destino aos restantes nós de *core*.

```
Tracing MPLS Label Switched Path to 172.17.0.2/32, timeout is 2 seconds

Codes: '!' - success

  0 172.17.12.1 MRU 9202 [Labels: explicit-null Exp: 0]
! 1 172.17.12.2 3 ms
```

Figura 58 – Caminho de ASR-1 para ASR-2

```
Tracing MPLS Label Switched Path to 172.17.0.3/32, timeout is 2 seconds

Codes: '!' - success

  0 172.17.13.1 MRU 9202 [Labels: explicit-null Exp: 0]
! 1 172.17.13.3 4 ms
```

Figura 59 – Caminho de ASR-1 para ASR-3

```
Tracing MPLS Label Switched Path to 172.17.0.4/32, timeout is 2 seconds

Codes: '!' - success

  0 172.20.17.1 MRU 9202 [Labels: explicit-null Exp: 0]
! 1 172.20.17.4 4 ms
```

Figura 60 – Caminho de ASR-1 para ASR-4

ANEXO V – ESTRUTURA DE CONFIGURAÇÕES (PARTE 1)

O conjunto de tabelas apresentadas de seguida, visa retratar as operações de configuração dos protocolos MPLS, OSPF, BGP, bem como a configuração relativa ao serviço VPLS em equipamento Cisco (IOS).

Tabela 27 – Configuração das interfaces MPLS

Comando	Propósito
`Router(config)# interface type number`	Seleciona uma interface a configurar
`Router(config-if)# ip address ip_address mask`	Define um endereço IP à interface
`Router(config-if)# encapsulation dot1q vlan_id`	Define uma *vlan id* à interface
`Router(config-if)# description description`	Permite inserir uma descrição à interface
`Router(config-if)# mpls ip`	Ativa o MPLS na interface

Tabela 28 – Configuração do processo OSPF

Comando	Propósito
`Router(config)# router ospf process_id`	Ativa um processo de *routing* OSPF
`Router(config-router)# router id ip_address`	Identifica o endereço IP do *router* para o processo OSPF
`Router(config-router)# nsr`	Ativa o *Nonstop Routing* para o processo OSPF
`Router(config-router)# network ip_address wildcard_mask area area_id`	Define a interface onde o OSPF vai ser executado e é definida a área para essa interface
`Router(config-router)# mpls ldp sync`	Ativa a sincronização do IGP do MPLS para as interfaces presentes no processo OSPF

Tabela 29 – Configuração do processo BGP

Comando	Propósito
`Router(config)# router bgp autonomous-system-number`	Ativa um processo de *routing* BGP
`Router(config-router)# bgp router-id ip_address`	Identifica o endereço IP do *router* para o processo BGP
`Router(config-router)# bgp log-neighbor-changes`	Ativa os *logs* do processo BGP
`Router(config-router)# bgp graceful-restart`	Ativa o *graceful-restart* para o processo BGP
`Router(config-router)# neighbor peer_group_name peer-group`	Cria um grupo de *neighbors*
`Router(config-router)# neighbor peer_group_name remote-as remote-autonomous-system-number`	Associa o número de *Autonomous System* ao grupo de *neighbors*

`Router(config-router)# neighbor peer_group_name password <0-7> type_password`	Define o nível de encriptação e a password para o grupo de *neighbors*
`Router(config-router)# neighbor peer_group_name update-source interface`	Seleciona a interface que recebe as atualizações provenientes da tabela de rotas
`Router(config-router)# neighbor peer_group_name ha-mode graceful-restart`	Ativa o *graceful-restart* para o *neighbor*
`Router(config-router)# neighbor ip_address peer-group peer_group_name`	Associa o endereço de um *neighbor* ao *peer-group*
`Router(config-router)# address-family l2vpn [vpls]`	Especifica a família de endereços L2VPN e entra no modo de configuração da família de endereços • A chave *vpls* é opcional. Esta especifica que os serviços VPLS serão distribuídos pelos *peers* BGP
`Router(config-router-af)# neighbor ip_address activate`	Permite que o *neighbor* troque informações de serviços L2VPN
`Router(config-router-af)# neighbor peer_group_name prefix-length-size <1-2>`	Especifica o tamanho em *bytes* dos prefixos anunciados e associa o grupo à família de endereços
`Router(config-router-af)# exit-address-family`	Termina a configuração na família de endereços L2VPN
`Router(config-router)# address-family ipv4`	Especifica a família de endereços IPv4 e entra no modo de configuração da família de endereços
`Router(config-router-af)# neighbor ip_address activate`	Permite a troca de informação com o *neighbor* BGP

Tabela 30 – Configuração do protocolo MPLS

Comando	**Propósito**
`Router(config)# mpls ip`	Configura o encaminhamento MPLS *hop-by-hop* globalmente. Este comando está ativo por *default*
`Router(config)# mpls label protocol [ldp | tdp | both]`	Determina o protocol de distribuição utilizado pelo MPLS
`Router(config)# mpls ldp router-id interface`	Especifica a interface com o LDP *router* ID
`Router(config)# mpls label range label-mínimo label-máximo`	Configura o *range* de etiquetas a utilizar
`Router(config)# mpls ldp explicit-null`	Configurar o parâmetro *explicit-null*
`Router(config)# mpls ldp graceful-restart`	Configurar o parâmetro *graceful-restart*
`Router(config)# mpls ldp igp sync holddown <time in miliseconds>`	Configura o tempo de espera da sincronização do LDP-IGP

Tabela 31 – Configuração de um serviço VPLS com autodescoberta

Comando	**Propósito**
`Router(config)# l2 vfi service-name autodiscovery`	Configura um novo serviço utilizando a autodescoberta
`Router(config-vfi)# vpn id id_number`	Determina o ID do serviço
`Router(config-vfi)# rd ASN:id_number`	Determina a distribuição do serviço através do par *Autonomous System – VPN ID*

`Router(config-vfi)# route-target export ASN:id_number`	
`Router(config-vfi)# route-target import ASN:id_number`	

Tabela 32 – Configuração de um serviço VPLS

Comando	Propósito
`Router(config)# l2 vfi service-name manual`	Configura um novo serviço manualmente
`Router(config-vfi)# vpn id id_number`	Determina o ID do serviço
`Router(config-vfi)# neighbor ip_address encapsulation mpls`	Determina o *host* para o qual se deseja entregar o serviço

Tabela 33 – Configuração do *attachment-circuit*

Comando	Propósito
`Router(config)# interface type number`	Seleciona uma interface a configurar
`Router(config-if)# service instance si-id ethernet`	Configura uma instância de serviço *Ethernet* numa interface
`Router(config-if-srv)# encapsulation dot1q vlan-id`	Define o critério para mapear as *frames* 802.1Q de entrada para o serviço apropriado
`Router(config-if-srv)# rewrite ingress tag pop number [symmetric]`	(Opcional) Especifica o ajuste do encapsulamento a ser realizado numa *frame* que entra numa instância de serviço.
`Router(config-if-srv)# bridge-domain bd-id`	Associa uma instância de serviço a uma instância de *bridge domain*

ANEXO VI – ESTRUTURA DE CONFIGURAÇÕES (PARTE 2)

Neste anexo encontram-se as configurações necessárias para a implementação do MPLS *Traffic Engineer* nos equipamentos Cisco IOS e IOS-XR. A estrutura de configurações apresentada é dividida em seis secções, sendo estas: ativação do protocolo MPLS-TE; definição de túneis TE; distribuição da informação das ligações com OSPF; Caminhos Explícitos MPLS TE; Sinalização dos TE LSP's; Recuperação Rápida de Falhas.

1. Ativação do MPLS *traffic-engineer*

Para habilitar no MPLS, o mecanismo de engenharia de tráfego torna-se necessário realizar configurações tanto ao nível do nó, como das interfaces. Estas configurações envolvem principalmente a definição da extensão de *traffic engineering* e do protocolo RSVP. As versões Cisco IOS utilizam o comando ***mpls traffic-eng*** para configurações relacionadas com o MPLS-TE, e ***ip rsvp*** para configurações relativas ao RSVP. Já as versões Cisco IOS-XR utilizam os comandos ***mpls traffic-eng*** e ***rsvp***, para as configurações relacionadas com a engenharia de tráfego e o protocolo RSVP, respetivamente.

1.1. Ativar MPLS TE num nó (Cisco IOS)

Na versão Cisco IOS, o comando que permite habilitar um nó das capacidades de MPLS-TE é o ***mpls traffic-eng tunnels***, o qual deve ser configurado antes de qualquer implementação de engenharia de tráfego. Além deste, existem outros comandos de utilização opcional, que configuram aspetos como temporizadores, automação e *logs*. Alguns destes comandos encontram-se apresentados na Tabela 34.

Tabela 34 – Ativar MPLS-TE num nó (Cisco IOS)

Comando	Propósito
`Cisco-IOS(config)# mpls traffic-eng tunnels`	Ativar o MPLS-TE no nó
`Cisco-IOS(config)# mpls traffic-eng logging lsp setups`	(Opcional) Retorna *logs* sobre a instalação de novos TE LSP's
`Cisco-IOS(config)# mpls traffic-eng logging lsp teardowns`	(Opcional) Retorna *logs* sobre baixas de TE LSP's
`Cisco-IOS(config)# mpls traffic-eng reoptimize events link-up`	(Opcional) Otimização do caminho quando uma interface física fica operacional

1.2. Ativar MPLS TE num nó (Cisco IOS-XR)

Os equipamentos com a versão IOS-XR ativam o MPLS TE através do comando ***mpls traffic-eng***. Este comando define um grupo isolado onde se encontram as configurações do MPLS TE, excetuando-se as extensões de engenharia de tráfego para os protocolos IGP. Apesar de ser abordado com mais detalhe nos próximos subcapítulos, adianta-se desde já o facto de que as configurações das interfaces a utilizar funcionalidades de engenharia de tráfego também são incluídas neste grupo. No entanto, resta salientar algumas das características gerais capazes de implementar nestes equipamentos, como as que se encontram presentes na Tabela 35.

Tabela 35 – Ativar MPLS-TE num nó (Cisco IOS-XR)

Comando	Propósito
`Cisco-IOS-XR(config)# mpls traffic-eng`	Ativar o MPLS-TE no nó
`Cisco-IOS-XR(config-mpls-te)# interface type number`	Identifica a(s) interface(s) a utilizar MPLS TE
`Cisco-IOS-XR(config-mpls-te)# maximum tunnels number`	(Opcional) Define um número máximo de TE LSP's
`Cisco-IOS-XR(config-mpls-te)# signaling advertise explicit-null`	(Opcional) Desativa o PHP

1.3. Ativar MPLS TE numa interface (Cisco IOS)

Para se proceder à ativação do MPLS TE nas interfaces utiliza-se o comando ***mpls traffic-eng tunnels*** dentro do grupo de parâmetros da interface. Este comando, além de ativar o MPLS TE na interface, ativa também o processo de sinalização do protocolo RSVP, responsável pela instalação de TE LSP's. Em conformidade com a configuração realizada no nó, o comando atrás referido garante a configuração mínima para a operabilidade da engenharia de tráfego, no entanto comandos adicionais podem ser configurados para as diferentes interfaces (ver Tabela 36).

Tabela 36 – Ativar MPLS TE numa interface (Cisco IOS)

Comando	Propósito
`Cisco-IOS(config)# interface type number`	Seleciona uma interface a configurar
`Cisco-IOS(config-if)# ip address ip_address mask`	Define um endereço IP à interface
`Cisco-IOS(config-if)# mpls traffic-eng tunnels`	Ativa o MPLS TE na interface
`Cisco-IOS(config-if)# mpls traffic-eng administrative-weight number`	(Opcional) Define o peso administrativo
`Cisco-IOS(config-if)# mpls traffic-eng srlg number (1*)`	(Opcional) Relaciona a interface com um *Shared Risk Link Group* (SRLG) (a utilizer no *fast reroute*)

(1*) – Os grupos de link de risco partilhados referem-se a situações em que diversas ligações numa rede partilham o mesmo atributo físico. Se um link falha, os outros falham também. Assim sendo, esta funcionalidade aprimora a seleção do túnel backup para que este evite os links que estejam no mesmo SRLG do link que falhou. [60]

1.4. Ativar MPLS TE numa interface (Cisco IOS-XR)

Como referido anteriormente, a configuração das interfaces inerentes ao MPLS TE efetua-se no grupo de configurações relativas ao comando ***mpls traffic-eng***. Associado a este grupo de configurações inserem-se as interfaces a realizar operações de MPLS TE, e para cada uma delas é possível atribuir vários atributos, como demonstra a Tabela 37. Ao contrário do que acontece com as versões Cisco IOS, ativar o MPLS TE nas interfaces não ativa o processo de sinalização RSVP.

Tabela 37 – Ativar MPLS TE numa interface (Cisco IOS-XR)

Comando	Propósito
`Cisco-IOS-XR(config)# mpls traffic-eng`	Ativar o MPLS-TE no nó
`Cisco-IOS-XR(config-mpls-te)# interface` *type number*	Identifica a(s) interface(s) a utilizar MPLS TE
`Cisco-IOS-XR(config-mpls-te)# admin-weight` *number*	(Opcional) Define o peso administrativo
`Cisco-IOS-XR(config-mpls-te)# attribute-flags` *flag*	(Opcional) Atribui uma *flag*

2. Definição de túneis TE

Os nós de uma rede MPLS dotada de engenharia de tráfego utilizam interfaces *tunnel* para a definição de TE LSP's. Cada uma destas interfaces especifica algumas características do TE LSP, como o destino, a largura de banda, o caminho, os requisitos de proteção, os parâmetros de encaminhamento, entre outros. Destas características, no mínimo deverá ser definido o destino, o caminho e o tipo de túnel.

2.1. Criar interface TE *tunnel* (Cisco IOS)

As versões Cisco IOS identificam as interfaces *tunnel* com a palavra chave ***tunnel***. Para a versão indicada estas interfaces podem ser utilizadas para diversos mecanismos de *tunneling*, como *Layer 2 Tunnel Protocol* (L2TP) e *Generic Routing Encapsulation* (GRE). Por esta razão é primordialmente necessário identificar este túnel como do tipo MPLS TE, seguindo-se as restantes configurações (ver Tabela 38).

Tabela 38 – Criar interface TE *tunnel* (Cisco IOS)

Comando	Propósito
`Cisco-IOS(config)# interface Tunnel` *number*	Identifica uma interface do tipo *tunnel*
`Cisco-IOS (config-if)# ip unnumbered` *interface*	
`Cisco-IOS (config-if)# tunnel destination` *ip*	Define o destino do túnel

`Cisco-IOS (config-if)# tunnel mode mpls traffic-eng`	Ativa o MPLS TE na interface
`Cisco-IOS (config-if)# tunnel mpls traffic-eng path-option number type`	

2.2. Criar interface TE *tunnel* (Cisco IOS-XR)

As versões Cisco IOS-XR identificam as interfaces *tunnel* com a palavra chave ***tunnel-te***. Como o nome sugere, este tipo de interface é utilizado exclusivamente para túneis do tipo MPLS TE. Como pode ser observado na Tabela 39 os comandos a utilizar são bastante similares aqueles utilizados na versão Cisco IOS.

Tabela 39 – Criar interface TE *tunnel* (Cisco IOS-XR)

Comando	Propósito
`Cisco-IOS(config)# interface tunnel-te number`	Identifica uma interface do tipo *tunnel*
`Cisco-IOS (config-if)# ipv4 unnumbered interface`	
`Cisco-IOS (config-if)# destination ip`	Define o destino do túnel
`Cisco-IOS (config-if)# path-option number type`	

3. Distribuição da informação das ligações com OSPF

As versões Cisco IOS e Cisco IOS-XR suportam a extensão de MPLS TE para o protocolo dinâmico de *routing* OSPF. Como se pode verificar a partir da Tabela 40 e Tabela 41, as configurações são idênticas em ambas as versões, onde de identifica a presença da engenharia de tráfego associado ao prefixo ***mpls traffic-eng***.

Tabela 40 – Configurar processo OSPF TE (Cisco IOS)

Comando	Propósito
`Cisco-IOS(config)# router ospf process-id`	Criação de um processo OSPF
`Cisco-IOS (config-ospf)# mpls traffic-eng router-id interface`	Definição da interface *router-id*
`Cisco-IOS (config-ospf)# mpls traffic-eng router-id area area-id`	Definição da área OSPF
`Cisco-IOS (config-ospf)# network network mask area area`	Definição da rede a distribuir dinamicamente por OSPF

Tabela 41 – Configurar processo OSPF TE (Cisco IOS-XR)

Comando	Propósito
`Cisco-IOS-XR(config)# router ospf process-id`	Criação de um processo OSPF
`Cisco-IOS-XR (config-ospf)# area area-id`	Definição da área OSPF

`Cisco-IOS-XR (config-ospf-area)# interface interface`	Definição da rede a distribuir dinamicamente por OSPF através da interface na qual a rede se encontra
`Cisco-IOS-XR (config-ospf)# mpls traffic-eng router-id interface`	Definição da interface *router-id*
`Cisco-IOS-XR (config-ospf)# mpls traffic-eng area area-id`	Definição da área OSPF

3.1. Configurar atributos das ligações

Encontrando-se o IGP (neste caso o OSPF) configurado com a extensão de TE, o nó inicia o anuncia dos atributos de MPLS TE para um determinado *link*. Como descrito na secção anterior, estas características incluem o peso administrativo, as *flags* e a largura de banda.

Algo a tomar em consideração é o facto de que nem todos os *links* de um nó necessitarem de estarem incluidos no domínio MPLS TE. No entanto, um *link* configurado com características de engenharia de tráfego terá de se ligar a um nó também com a extensão de TE. Caso um dos *links* de interligação não esteja configurado com as extensões de TE, a interligação fará uso apenas dos valores *default* até que seja ativo o MPLS TE e o RSVP nas respetivas interfaces.

Tabela 42 – Configurar características dos *links* MPLS TE (Cisco IOS)

Comando	**Propósito**
`Cisco-IOS (config)# interface type number`	Seleciona uma interface a configurar
`Cisco-IOS (config-if)# ip address ip_address mask`	Define um endereço IP à interface
`Cisco-IOS (config-if)# mpls traffic-eng tunnels`	Ativa o MPLS TE na interface
`Cisco-IOS (config-if)# mpls traffic-eng attribute-flags flags`	(Opcional) Atribui uma *flag*
`Cisco-IOS (config-if)# ip rsvp bandwidth number`	Define a largura de banda (em kbps)

Tabela 43 – Configurar características dos *links* MPLS TE (Cisco IOS-XR)

Comando	**Propósito**
`Cisco-IOS-XR(config)# rsvp`	Entra no grupo de configuração do RSVP
`Cisco-IOS-XR (config-rsvp)# interface type number`	Configura uma interface para funcionar em conjunto com o protocol de sinalização RSVP
`Cisco-IOS-XR (config-rsvp-if)# bandwidth number`	Define a largura de banda (em kbps)
`Cisco-IOS-XR (config)# mpls traffic-eng`	Ativar o MPLS-TE no nó
`Cisco-IOS-XR (config-te)# interface type number`	Identifica a(s) interface(s) a utilizar MPLS TE
`Cisco-IOS-XR (config-te-if)# admin-weight number`	(Opcional) Define o peso administrativo
`Cisco-IOS-XR (config-te-if)# attribute-flags flag`	(Opcional) Atribui uma *flag*

4. Caminhos explícitos MPLS TE

O nó a montante é responsável por definir o caminho de um TE LSP. A interface túnel TE tem a capacidade de definir o destino do TE LSP, bem como um conjunto de opções do caminho até ao destino. Neste conjunto de operações inclui-se a definição de um caminho explícito, ou então uma referência à necessidade de um caminho dinâmico, associado ao IGP.

4.1. Configurar caminhos de TE LSP's

Cada TE LSP pode ser configurado mediante um conjunto de opções de caminhos. Estas opções podem definir um caminho explícito por completo ou apenas parcialmente, bem como definir o caminho completo dinamicamente até ao destino. Como analisado no momento da definição da interface túnel TE, é possível configurar o destino do TE LSP sem a descrição do caminho, utilizando por consequência o caminho definido pelo IGP.

Na Tabela 44 e Tabela 45 estão presentes os comandos de configuração para as versões Cisco IOS e IOS-XR. Apresentam-se os comandos necessários para a criação de caminhos e respetivos túneis TE LSP com a especificação do caminho.

Tabela 44 – Configurar caminhos e túneis MPLS TE (Cisco IOS)

Comando	**Propósito**
`Cisco-IOS (config)# ip explicit-path name name1 enable`	Configurar um caminho atribuindo um nome
`Cisco-IOS (config-expl)# next-address loose ip_address`	Utilizado para configurar um caminho explicito de forma parcial
`Cisco-IOS (config-expl)# exclude-address ip_address`	Excluir endereços do LSP
`Cisco-IOS (config-expl)# next-address ip_address`	Seleciona os endereços pelos quais se deseja que o LSP seja formado. O comando deverá ser repetido
`Cisco-IOS (config)# interface Tunnel number`	Identifica uma interface do tipo *tunnel*
`Cisco-IOS (config-if)# ip unnumbered interface`	
`Cisco-IOS (config-if)# tunnel destination ip_address`	Define o destino do túnel
`Cisco-IOS (config-if)# tunnel mode mpls traffic-eng`	Define a utilidade do túnel para MPLS TE
`Cisco-IOS (config-if)# tunnel mpls traffic-eng priority number`	Define a prioridade para o túnel em questão
`Cisco-IOS (config-if)# tunnel mpls traffic-eng bandwidth number`	Define a largura de banda para o túnel em questão
`Cisco-IOS (config-if)# tunnel mpls traffic-eng path-option number explicit name name`	Define uma prioridade para um caminho explicito para o túnel em questão
`Cisco-IOS (config-if)# tunnel mpls traffic-eng path-option number dynamic`	Define uma prioridade para um caminho explicito dinâmico para o túnel em questão

Tabela 45 – Configurar caminhos e túneis MPLS TE (Cisco IOS-XR)

Comando	Propósito
`Cisco-IOS-XR(config)# explicit-path name name`	Configurar um caminho atribuindo um nome
`Cisco-IOS-XR (config-path)# index number next-address ipv4 unicast ip_address`	Seleciona os endereços pelos quais se deseja que o LSP seja formado. O comando deverá ser repetido
`Cisco-IOS-XR (config-path)# index number exclude-address ipv4 unicast ip_address`	Excluir endereços do LSP
`Cisco-IOS-XR (config)# interface tunnel-te number`	Identifica uma interface do tipo *tunnel*
`Cisco-IOS-XR (config-if)# ipv4 unnumbered interface`	
`Cisco-IOS-XR (config-if)# signaled-bandwidth number`	Define a largura de banda para o túnel em questão
`Cisco-IOS-XR (config-if)# destination ip_address`	Define o destino do túnel
`Cisco-IOS-XR (config-if)# path-option number explicit name name`	Define uma prioridade para um caminho explicito para o túnel em questão
`Cisco-IOS-XR (config-if)# path-option number dynamic`	Define uma prioridade para um caminho explicito dinâmico para o túnel em questão

5. Sinalização dos TE LSP's

A sinalização dos LSP's dotados de engenharia de tráfego é da responsabilidade do protocolo RSVP. Este pode ser configurado ao nível do nó e também ao nível da interface, sendo que a sintaxe de comandos difere consoante a versão (Cisco IOS ou Cisco IOS-XR). Na Tabela 46 e Tabela 47 encontram-se listados os comandos necessários para a configuração da sinalização associada aos TE LSP's, bem como a função de cada um.

Tabela 46 – Configuração do RSVP TE (Cisco IOS)

Comando	Propósito
`Cisco-IOS (config)# interface type number`	Seleciona uma interface a configurar
`Cisco-IOS (config-if)# ip address ip_address mask`	Define um endereço IP à interface
`Cisco-IOS (config-if)# mpls traffic-eng tunnels`	Define a interface como parte do domínio MPLS TE
`Cisco-IOS (config-if)# ip rsvp bandwidth number`	Define a largura de banda (em kbps)
`Cisco-IOS (config)# ip rsvp signaling refresh reduction`	Configura a extensão de redução de atualizações
`Cisco-IOS (config)# ip rsvp signaling hello graceful-restart mode help-neighbor`	Ativa o *graceful-restart*

Tabela 47 – Configuração do RSVP TE (Cisco IOS-XR)

Comando	Propósito
`Cisco-IOS-XR (config)# rsvp`	Entra no grupo de configuração do RSVP
`Cisco-IOS-XR (config-rsvp)# interface type number`	Configura uma interface para funcionar em conjunto

	com o protocol de sinalização RSVP
`Cisco-IOS-XR (config-rsvp-if)# bandwidth number_kbps`	Define a largura de banda (em kbps)
`Cisco-IOS-XR (config-rsvp-if)# signalling refresh reduction reliable retransmite-time number_ms`	Valor em ms
`Cisco-IOS-XR (config-rsvp)# signalling graceful-restart`	Ativa o *graceful-restart*
`Cisco-IOS-XR (config-rsvp)# signalling hello graceful-restart refresh interval number_ms`	Define um intervalo de atualização (e ms)

6. *Fast reroute*

As versões Cisco IOS e Cisco IOS-XR oferecem a funcionalidade de *fast reroute* de modo a oferecer simultaneamente proteção de nó e de *link*. Além disso, é possível configurar a rede de forma a fornecer proteção de conetividade e/ou proteção de largura de banda.

Para que o FRR seja implementado deve-se configurar o nó mais a montante do túnel primário para solicitar proteção, bem como pelo menos um ponto médio com um túnel de *backup* para redirecionar TE LSP's primários. O túnel de *backup* deverá ultrapassar a falha e voltar a intersetar o TE LSP primário.

Quanto à configuração, em ambas as versões deverá ser indicado qual o túnel a necessitar de proteção, como pode ser analisado pelos esquemas de configuração apresentados pela Tabela 48 e Tabela 49.

Tabela 48 – Configuração de FRR para proteção de nó e largura de banda (Cisco IOS)

Comando	**Propósito**
`Cisco-IOS (config)# interface Tunnel number`	Identifica uma interface do tipo *tunnel*
`Cisco-IOS (config-if)# description text`	Define uma descrição à interface *tunnel*
`Cisco-IOS (config-if)# ip innumbered interface`	
`Cisco-IOS (config-if)# tunnel destination ip_address`	Define o destino do túnel
`Cisco-IOS (config-if)# tunnel mode mpls traffic-eng`	Define a interface como parte do domínio MPLS TE
`Cisco-IOS (config-if)# tunnel mpls traffic-eng priority number`	Define uma prioridade para um caminho explicito para o túnel em questão
`Cisco-IOS (config-if)# tunnel mpls traffic-eng bandwidth number`	Define a largura de banda (em kbps)
`Cisco-IOS (config-if)# tunnel mpls traffic-eng path-option number explicit name name`	Define uma prioridade para um caminho explicito para o túnel em questão
`Cisco-IOS (config-if)# tunnel mpls traffic-eng fast-reroute bw-protect node-protect`	Ativa o *fast-reroute* para a interface *tunnel*

Tabela 49 – Configuração de FRR para proteção de nó e largura de banda (Cisco IOS-XR)

Comando	Propósito
`Cisco-IOS-XR (config)# interface tunnel-te number`	Identifica uma interface do tipo *tunnel*
`Cisco-IOS-XR (config-if)# description text`	Define uma descrição à interface *tunnel*
`Cisco-IOS-XR (config-if)# ipv4 innumbered interface`	
`Cisco-IOS-XR (config-if)# destination ip_address`	Define o destino do túnel
`Cisco-IOS-XR (config-if)# priority number`	Define uma prioridade para um caminho explicito para o túnel em questão
`Cisco-IOS-XR (config-if)# signalled-bandwidth number`	Define a largura de banda (em kbps)
`Cisco-IOS-XR (config-if)# fast-reroute`	Ativa o *fast-reroute* para a interface *tunnel*
`Cisco-IOS-XR (config-if)# path-option number explicit name name`	Define uma prioridade para um caminho explicito para o túnel em questão

6.1 Proteção de nó e *link*

Para se implementar a proteção de nó e de ligação é necessário estabelecer previamente um backup TE LSP, que é configurado recorrendo aos mesmos comandos de configuração de uma interface *tunnel*. O nó a montante do túnel *backup* será sempre o PLR, enquanto que o nó mais a jusante será sempre o ponto de convergência com o túnel primário (*merge point*). O túnel de *backup* pode depender de um caminho dinamicamente calculado ou de um caminho explicitamente definido, sendo que a única restrição óbvia que existe é o facto de que o túnel de *backup* não pode fazer uso de recursos existentes na falha que se está a proteger (exemplos: *link*, nó ou SRLGs). Geralmente os túneis de *backup* não fazem uso de uma reserva de largura de banda explicita, uma vez que permanecem inutilizados na maior parte do tempo.

Na Tabela 50 e Tabela 51 encontra-se demonstrado os esquemas de configuração necessários para a implementação de proteção de nó e *link* nas versões Cisco IOS e Cisco IOS-XR.

Tabela 50 – Configuração da proteção de nó e *link* com túneis *backup* (Cisco IOS)

Comando	Propósito
`Cisco-IOS (config)# interface Tunnel number`	Identifica uma interface do tipo *tunnel*
`Cisco-IOS (config-if)# description text`	Define uma descrição à interface *tunnel*
`Cisco-IOS (config-if)# ip innumbered interface`	
`Cisco-IOS (config-if)# tunnel destination ip_address`	Define o destino do túnel
`Cisco-IOS (config-if)# tunnel mode mpls traffic-eng`	Define a interface como parte do domínio MPLS TE
`Cisco-IOS (config-if)# tunnel mpls traffic-eng path-option number explicit name name`	Define uma prioridade para um caminho explicito para o túnel em questão

`Cisco-IOS (config)# interface type number`	Seleciona uma interface a configurar
`Cisco-IOS (config-if)# ip address ip_address mask`	Define um endereço IP à interface
`Cisco-IOS (config-if)# mpls traffic-eng tunnels`	Define a interface como parte do domínio MPLS TE
`Cisco-IOS (config-if)# mpls traffic-eng backup-path interface_tunnel`	Define qual a interface *tunnel backup*
`Cisco-IOS (config-if)# ip rsvp bandwidth number`	Define a largura de banda (em kbps)
`Cisco-IOS (config)# ip explicit-path name name enable`	Configurar um caminho explícito atribuindo um nome
`Cisco-IOS (config)# exclude-address ip_address`	Excluir endereços do LSP

Tabela 51 – Configuração da proteção de nó e *link* com túneis *backup* (Cisco IOS-XR)

Comando	**Propósito**
`Cisco-IOS-XR (config)# interface tunnel-te number`	Identifica uma interface do tipo *tunnel*
`Cisco-IOS-XR (config-if)# description text`	Define uma descrição à interface *tunnel*
`Cisco-IOS-XR (config-if)# ipv4 innumbered interface`	
`Cisco-IOS-XR (config-if)# destination ip_address`	Define o destino do túnel
`Cisco-IOS-XR (config-if)# path-option number explicit name name`	Define uma prioridade para um caminho explicito para o túnel em questão
`Cisco-IOS-XR (config)# mpls traffic-eng`	Ativar o MPLS-TE no nó
`Cisco-IOS-XR (config-eng)# interface type number`	Seleciona uma interface a configurar
`Cisco-IOS-XR (config-eng-if)# backup-path tunnel-te number`	Define qual a interface *tunnel backup*
`Cisco-IOS-XR (config)# explicit-path name name`	Configurar um caminho explícito atribuindo um nome
`Cisco-IOS-XR (config-exp)# index number exclude-address ipv4 unicast ip_address`	Excluir endereços do LSP

ANEXO VII – CONFIGURAÇÕES DO LABORATÓRIO VPLS

Neste anexo encontram-se as configurações essenciais para elaboração dos diferentes cenários VPLS. Primeiramente são apresentadas as configurações genéricas a todos os cenários e posteriormente as configurações relevantes de cada cenário.

Configurações gerais

Antes de apresentar as configurações especificas aos diferentes cenários para a oferta de serviços MPLS, foram realizadas configurações genéricas a todos os cenários de implementação.

Para a rede de transporte, inicialmente foram configuradas as interfaces de interligação, o protocolo de *routing* dinâmico OSPF e ativado o protocolo MPLS em todos os nós da rede de transporte. Na rede de acesso, foram configurados os nós CE e criadas 3 máquinas virtuais com o sistema operativo Ubuntu, disponíveis por recurso a um servidor de virtualização Proxmox, para realizar os testes de aferição aos tempos de recuperação a falha.

Configuração de interfaces

Tendo em conta o esquema de endereçamento IP e de interfaces de interligação demonstrado no subcapítulo 5.4 todos os nós de rede foram configurados. As figuras abaixo demonstram um exemplo em cada nó de rede, ou seja, nos nós PE-1 (Nokia), PE-4 (Cisco), P-1(Nokia) e CE-1 (Cisco).

```
port 1/1/6
    ethernet
    exit
    no shutdown
exit
port 1/1/7
    ethernet
    exit
    no shutdown
exit
port 1/1/10
    ethernet
        mode access
    exit
    no shutdown
exit
router
    interface "PE1-P1"
        address 172.16.14.4/24
        port 1/1/6
    exit
    interface "PE1-P3"
        address 172.16.34.4/24
        port 1/1/7
    exit
    interface "system"
        address 4.4.4.4/32
    exit
```

Figura 61 - Configuração das interfaces em PE-1 (Nokia)

```
interface Loopback1
  ip address 7.7.7.7 255.255.255.255
!
interface TenGigabitEthernet1/6
  description PE4-P2
  ip address 172.16.27.7 255.255.255.0
!
interface TenGigabitEthernet1/7
  description PE4-P1
  ip address 172.16.17.7 255.255.255.0
!
```

Figura 62 – Configuração das interfaces em PE-4 (Cisco IOS)

```
   port 1/1/5
       ethernet
       exit
       no shutdown
   exit
   port 1/1/6
       ethernet
       exit
       no shutdown
   exit
   port 1/1/7
       ethernet
       exit
       no shutdown
   exit
   port 1/1/8
       ethernet
       exit
       no shutdown
   exit
   port 1/1/9
       ethernet
       exit
       no shutdown
   exit
   port 1/1/10
       ethernet
         mode access
         encap-type dot1q
       exit
       no shutdown
   exit
```

```
   router
       interface "P1-P2"
           address 172.16.12.1/24
           port 1/1/5
       exit
       interface "P1-P3"
           address 172.16.13.1/24
           port 1/1/10
       exit
       interface "P1-PE1"
           address 172.16.14.1/24
           port 1/1/6
       exit
       interface "P1-PE2"
           address 172.16.15.1/24
           port 1/1/7
       exit
       interface "P1-PE3"
           address 172.16.16.1/24
           port 1/1/8
       exit
       interface "P1-PE4"
           address 172.16.17.1/24
           port 1/1/9
       exit
       interface "system"
           address 1.1.1.1/32
       exit
```

Figura 63 – Configuração das interfaces em P-1 (Nokia)

```
interface FastEthernet0/1
  description CPE1-to-Virt
  switchport trunk allowed vlan 1111
  switchport mode trunk
  !
interface GigabitEthernet0/1
  description to_PE1
  switchport trunk allowed vlan 1111
  switchport mode trunk
!
interface GigabitEthernet0/2
  description to_PE2
  switchport trunk allowed vlan 1111
  switchport mode trunk
  shutdown
!
```

Figura 64 – Configuração das interfaces em CE-1 (Switch Cisco)

Configuração do protocolo OSPF

A configuração do protocolo OSPF apenas é possível após a configuração de todas as interfaces incluidas no domínio MPLS. Este protocolo foi configurado em todos os nós P e PE, sendo que as próximas figuras apresentam a configuração em PE-1 (Nokia), PE-4 (Cisco IOS) e P1 (Nokia).

```
        ospf
            area 0.0.0.0
                interface "system"
                exit
                interface "PE1-P1"
                    interface-type point-to-point
                exit
                interface "PE1-P3"
                    interface-type point-to-point
                exit
                interface "loopback"
                exit
            exit
        exit
```

Figura 65 – Configuração do protocolo OSPF em PE-1 (Nokia)

```
router ospf 1                                    interface TenGigabitEthernet1/6
  router-id 7.7.7.7                                description PE4-P2
  nsr                                              ip address 172.16.27.7 255.255.255.0
  redistribute static subnets                      ip ospf network point-to-point
  network 7.7.7.7 0.0.0.0 area 0.0.0.0            !
  network  172.16.17.0  0.0.0.255  area           interface TenGigabitEthernet1/7
0.0.0.0                                            description PE4-P1
  network  172.16.27.0  0.0.0. 255  area           ip address 172.16.17.7 255.255.255.0
0.0.0.0                                            ip ospf network point-to-point
  default-information       originate            !
metric-type 1
!
```

Figura 66 – Configuração do protocolo OSPF em PE-4 (Cisco IOS)

```
 ospf                                              interface "P1-PE2"
   area 0.0.0.0                                      interface-type point-to-point
     interface "system"                              exit
     exit                                            interface "P1-PE3"
     interface "P1-P2"                                 interface-type point-to-point
       interface-type point-to-point                 exit
     exit                                            interface "P1-PE4"
     interface "P1-P3"                                 interface-type point-to-point
       interface-type point-to-point                   mtu 1500
     exit                                            exit
     interface "P1-PE1"                            exit
       interface-type point-to-point             exit
     exit
```

Figura 67 – Configuração do protocolo OSPF em P-1 (Nokia)

Configuração da tecnologia MPLS

Após a configuração das interfaces e do protocolo OSPF chega o momento de configurar o MPLS, sendo esta configuração genérica aos tipos de serviços oferecidos, quer estes sejam de nível 2 ou de nível 3.

Como o MPLS é o principal tema em discussão as configurações efetuadas são alvo de explicação. As figuras seguintes demonstram as configurações efetuadas em PE-1, PE-4 e P1.

```
        mpls
            interface "system"
            exit
            interface "PE1-P1"
            exit
            interface "PE1-P3"
            exit
            no shutdown
        exit
```

Figura 68 – Configuração das interfaces MPLS em PE-1 (Nokia)

```
interface TenGigabitEthernet1/6
 description PE4-P2
 ip address 172.16.27.7 255.255.255.0
 ip ospf network point-to-point
 mpls ip
!
interface TenGigabitEthernet1/7
 description PE4-P1
 ip address 172.16.17.7 255.255.255.0
 ip ospf network point-to-point
 mpls ip
!
```

Figura 69 – Configuração das interfaces MPLS em PE-4 (Cisco IOS)

```
        mpls
            interface "system"
            exit
            interface "P1-PE1"
            exit
            interface "P1-PE2"
            exit
            interface "P1-PE3"
            exit
            interface "P1-PE4"
            exit
            interface "P1-P2"
            exit
            interface "P1-P3"
            exit
            no shutdown
        exit
```

Figura 70 – Configuração das interfaces MPLS em P-1 (Nokia)

Enquanto que nos equipamentos Nokia é necessário ativar a tecnologia MPLS e configurar as interfaces que farão parte deste domínio, nos equipamentos Cisco IOS o MPLS é automaticamente habilitado no momento de configuração das interfaces. Além disto, nesta versão de *software* ao habilitarmos o MPLS na interface estamos também a habilitar o protocolo de sinalização LDP por defeito.

Cenário 1

O primeiro cenário resume-se à oferta de serviços VPLS sobre uma rede baseada na sinalização por LDP, tanto ao nível dos LSP's como dos *pseudowires*. A particularidade deste cenário encontra-se na descoberta automática dos nós PE, realizada com base no protocolo BGP.

Inicialmente foi ativado e configurado o protocolo LDP em todos os nós da topologia.

```
   router                                              policy-options
       ldp-shortcut                                        begin
       ldp                                                 policy-statement "to_LDP"
           export "to_LDP"                                     entry 10
           interface-parameters                                    from
               interface "PE1-P1"                                      protocol
               exit                            direct
               interface "PE1-P3"                                      exit
               exit                                                    action accept
           exit                                                        exit
           targeted-session                                    exit
           exit                                                commit
       exit                                            exit
   exit
```

Figura 71 – Configuração do protocolo LDP e política de redistribuição em PE-1 (Nokia)

```
mpls label protocol ldp
mpls ldp router-id Loopback1
!
interface TenGigabitEthernet1/6
  description PE4-P2
  mpls ip
!
interface TenGigabitEthernet1/7
  description PE4-P1
  mpls ip
!
router ospf 1
  mpls ldp sync
!
```

Figura 72 – Configuração do protocolo LDP em PE-4 (Cisco IOS)

```
router
    ldp
        interface-parameters
            interface "P1-PE1"
            exit
            interface "P1-PE2"
            exit
            interface "P1-PE3"
            exit
            interface "P1-PE4"
            exit
            interface "P1-P2"
            exit
            interface "P1-P3"
            exit
        exit
        targeted-session
        exit
```

Figura 73 – Configuração do protocolo LDP em P-1 (Nokia)

Depois de configurado o protocolo LDP, deu-se início à configuração do protocolo BGP em todos os PE's.

```
router
    autonomous-system 65100
    bgp
        group "mbgp-session-PEERs"
            family l2-vpn
            type internal
            peer-as 65100
            local-address 4.4.4.4
            neighbor 5.5.5.5
            exit
            neighbor 6.6.6.6
            exit
            neighbor 7.7.7.7
            exit
            neighbor 8.8.8.8
            exit
            neighbor 9.9.9.9
            exit
```

Figura 74 – Configuração do protocolo BGP em PE-1 (Nokia)

```
router bgp 65100
  bgp router-id 7.7.7.7
  neighbor mbgp-session-PEERs peer-group
  neighbor mbgp-session-PEERs remote-as 65100
  neighbor mbgp-session-PEERs update-source Loopback1
  neighbor 4.4.4.4 peer-group mbgp-session-PEERs
  neighbor 5.5.5.5 peer-group mbgp-session-PEERs
  neighbor 6.6.6.6 peer-group mbgp-session-PEERs
  neighbor 8.8.8.8 peer-group mbgp-session-PEERs
  neighbor 9.9.9.9 peer-group mbgp-session-PEERs
  !
  address-family ipv4
    neighbor mbgp-session-PEERs activate
  exit-address-family
  !
  address-family l2vpn vpls
    neighbor mbgp-session-PEERs prefix-length-size 2
    neighbor mbgp-session-PEERs activate
  exit-address-family
!
```

Figura 75 – Configuração do protocolo BGP em PE-4 (Cisco IOS)

Após a configuração dos protocolos LDP e BGP, foi configurado um serviço VPLS.

```
   service
       customer 10 create
           description "Cliente 10"
       exit
       vpls 1001 customer 10 create
           bgp
               route-distinguisher 65100:1001
               route-target export target:65100:1001 import target:65100:1001
           exit
           bgp-ad
               vpls-id 65100:1001
               vsi-id
                   prefix 4.4.4.4
               exit
               no shutdown
           exit
           sap 1/1/10:1111 create
           exit
           no shutdown
       exit
```

Figura 76 – Configuração do serviço VPLS (Nokia)

```
l2 vfi 1001 autodiscovery
  vpn id 1001
  rd 65100:1001
  route-target export 65100:1001
  route-target import 65100:1001
!
interface TenGigabitEthernet1/16
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1112
!
interface Vlan1112
  no ip address
  xconnect vfi 1001
!
```

Figura 77 – Configuração do serviço VPLS (Cisco IOS)

Cenário 2

No segundo cenário de implementação retirou-se a funcionalidade de descoberta automática dos PE's utilizada no primeiro cenário. Passou-se a utilizar a definição manual dos PE's para cada serviço VPLS.

Foi retirada toda a configuração alusiva ao protocolo BGP, alterando-se apenas o esquema de configuração do serviço VPLS nos nós PE.

```
   service
       sdp 47 mpls create
           description "SDP-PE2toPE3"
           far-end 7.7.7.7
           ldp
           keep-alive
               no shutdown
           exit
           no shutdown
       exit
       vpls 1001 customer 10 create
           stp
               shutdown
           exit
           sap 1/1/10:1111 create
           exit
           mesh-sdp 47:1001 create
           exit
           no shutdown
       exit
   exit
```

Figura 78 – Configuração do SDP e serviço VPLS em PE-1 (Nokia)

```
l2 vfi 1001 manual
  vpn id 1001
  neighbor 4.4.4.4 encapsulation mpls
!
```

Figura 79 – Configuração do serviço VPLS em PE-4 (Cisco IOS)

Cenário 3

Uma vez que no terceiro cenário era pretendida a implementação do protocolo RSVP para sinalização de LSP's dinâmicos, foram retiradas as configurações alusivas ao LDP em todos os nós, e configurado o protocolo pretendido.

Assim como acontece para o protocolo LDP, foi necessário identificar as interfaces associadas ao protocolo RSVP.

```
        rsvp
            interface "system"
            exit
            interface "P1-P2"
            exit
            interface "P1-P3"
            exit
            interface "P1-PE1"
            exit
            interface "P1-PE2"
            exit
            interface "P1-PE3"
            exit
            interface "P1-PE4"
            exit
            no shutdown
        exit
```

Figura 80 - Configuração do protocolo RSVP em P-1 (Nokia)

```
        rsvp
            interface "system"
            exit
            interface "PE1-P1"
            exit
            interface "PE1-P3"
            exit
            no shutdown
        exit
```

Figura 81 – Configuração do protocolo RSVP em PE-1 (Nokia)

```
interface TenGigabitEthernet1/6
  description PE4-P2
  mpls traffic-eng tunnels
!
interface TenGigabitEthernet1/7
  description PE4-P1
  mpls traffic-eng tunnels
!
```

Figura 82 – Configuração do protocolo RSVP em PE-4 (Cisco IOS)

Depois de identificadas as interfaces pelas quais irá ocorrer a sinalização por RSVP ativaram-se as extensões de engenharia de tráfego para o protocolo OSPF.

```
ospf
    traffic-engineering
    exit
exit
```

Figura 83 – Configuração da extensão de engenharia de tráfego em P-1 (Nokia)

```
ospf
    traffic-engineering
    rsvp-shortcut
    exit
exit
```

Figura 84 – Configuração da extensão de engenharia de tráfego em PE-1 (Nokia)

```
router ospf 1
    mpls traffic-eng router-id Loopback1
    mpls traffic-eng area 0.0.0.0
!
```

Figura 85 – Configuração da extensão de engenharia de tráfego em PE-4 (Cisco IOS)

Segue-se a configuração dos LSP's dinâmicos nos nós PE.

```
mpls
    path "path_loose_to_PE4"
        no shutdown
    exit
    lsp "lsp_to_PE4"
        to 7.7.7.7
        cspf
        primary "path_loose_to_PE4"
        exit
        no shutdown
    exit
    no shutdown
exit
```

Figura 86 – Configuração de LSP dinâmico em PE-1 (Nokia)

```
interface Tunnel74
    ip unnumbered Loopback1
    tunnel mode mpls traffic-eng
    tunnel destination 4.4.4. 4
    tunnel mpls traffic-eng autoroute announce
    tunnel mpls traffic-eng path-option 1 dynamic
!
```

Figura 87 – Configuração de LSP dinâmico em PE-4 (Cisco IOS)

Por fim, é configurado o serviço VPLS onde em relação ao cenário anterior foi apenas necessário configurar o SDP nos nós PE do fabricante Nokia.

```
service
    sdp 47 mpls create
        description "SDP-PE1toPE4"
        far-end 7.7.7.7
        lsp "lsp_to_PE4"
        keep-alive
            shutdown
        exit
        no shutdown
    exit
```

Figura 88 – Configuração do SDP em PE-1 (Nokia)

Cenário 4

Uma vez que se pretende integrar caminhos explícitos no quarto cenário, foram descartadas as configurações relativas à criação de LSP's dinâmicos.

Foram então configurados, em cada PE, dois caminhos explícitos para cada nó PE de pólos vizinhos. Estes dois caminhos explícitos foram formados de forma a também oferecer proteção extremo-a-extremo, sendo para isso necessário que não tivessem nenhum nó ou *link* coincidente, além dos nós PE a jusante e a montante.

As figuras seguintes apresentam as configurações realizadas entre PE-1 e PE-4.

```
mpls
    path "path_PE1-P3-P2-PE4"
        hop 1 3.3.3.3 strict
        hop 2 2.2.2.2 strict
        hop 3 7.7.7.7 strict
        no shutdown
    exit
    path "path_PE1-P1-PE4"
        hop 1 1.1.1.1 strict
        hop 2 7.7.7.7 strict
        no shutdown
    exit
    lsp "lsp_to_PE4"
        to 7.7.7.7
        primary "path_PE1-P1-PE4"
        exit
        secondary "path_PE1-P3-P2-PE4"
            standby
        exit
        no shutdown
    exit
    no shutdown
exit
```

Figura 89 – Configuração de LSP e proteção extremo-a-extremo em PE-1 (Nokia)

```
ip explicit-path name PE4-P2-P3-PE1 enable
  next-address 172.16.27.2
  next-address 172.16.23.3
  next-address 172.16.34.4
!
ip explicit-path name PE4-P1-PE1 enable
  next-address 172.16.17.1
  next-address 172.16.14.4
!
interface Tunnel74
  ip unnumbered Loopback1
  tunnel mode mpls traffic-eng
  tunnel destination 4.4.4.4
  tunnel mpls traffic-eng autoroute announce
  tunnel mpls traffic-eng path-option 1 explicit name PE4-P1-PE1
  tunnel mpls traffic-eng path-option 2 explicit name PE4-P2-P3-PE1
!
```

Figura 90 – Configuração de LSP e proteção extremo-a-extremo em PE-4 (Cisco IOS)

Cenário 5

No quinto cenário é novamente pretendida a utilização de proteção extremo-a-extremo, assim como no cenário anterior, com a diferença de que o caminho protetor é alterado por um caminho dinâmico e os nós PE envolventes são ambos Nokia (PE-1 e PE-3). Além disto, é também acrescentada a proteção local com a integração do *Fast Reroute One-to-One*.

As figuras seguintes apresentam as configurações dos LSP's, que incluem a proteção extremo-a-extremo e a proteção local com *Fast Reroute One-to-One*.

```
        mpls
            path "path_to_PE3_loose"
                no shutdown
            exit
            path "path_PE1-P1-PE3"
                hop 1 1.1.1.1 strict
                hop 2 6.6.6.6 strict
                no shutdown
            exit
            lsp "lsp_to_PE3"
                to 6.6.6.6
                cspf
                fast-reroute one-to-one
                primary "path_PE1-P1-PE3"
                exit
                secondary "path_to_PE3_loose"
                    standby
                exit
                no shutdown
            exit
            no shutdown
        exit
```

Figura 91 – Configuração de LSP com proteção extremo-a-extremo e local em PE-1 (Nokia)

```
mpls
    path "path_to_PE1_loose"
        no shutdown
    exit
    path "path_PE3-P1-PE1"
        hop 1 1.1.1.1 strict
        hop 2 4.4.4.4 strict
        no shutdown
    exit
    lsp "lsp_to_PE1"
        to 4.4.4.4
        cspf
        fast-reroute one-to-one
        primary "path_PE3-P1-PE1"
        exit
        secondary "path_to_PE1_loose"
            standby
        exit
        no shutdown
    exit
    no shutdown
exit
```

Figura 92 - Configuração de LSP com proteção extremo-a-extremo e local em PE-3 (Nokia)

Cenário 6

De modo a analisar as diferentes técnicas de proteção local, no último cenário a técnica utilizada para proteção local foi alterada para *Fast Reroute Facility*. Além disto, foram ainda criados subcenários de implementação com o intuito de criar redundância para o *attachment-circuit*, tendo sido implementado LAG e MC-LAG.

A Figura 93 apresenta a configuração realizada em PE-1 para configuração de proteção local com *Fast Reroute Facility*.

```
        mpls
            path "path_to_PE4_loose"
                no shutdown
            exit
            path "path_PE1-P1-PE4"
                hop 1 1.1.1.1 strict
                hop 2 7.7.7.7 strict
                no shutdown
            exit
            lsp "lsp_to_PE4"
                to 7.7.7.7
                cspf
                fast-reroute facility
                primary "path_PE1-P1-PE4"
                exit
                secondary "path_to_PE4_loose"
                    standby
                exit
                no shutdown
            exit
            no shutdown
        exit
```

Figura 93 - Configuração de proteção local com *fast reroute facility* em PE-1 (Nokia)

Redundância de *attachment-circuit* com LAG

```
   port 1/1/5
       ethernet
           mode access
           encap-type dot1q
       exit
       no shutdown
   exit
   port 1/1/10
       ethernet
           mode access
           encap-type dot1q
       exit
       no shutdown
   exit
```

```
   lag 1
       port 1/1/5
       port 1/1/10
       no shutdown
   exit
```

Figura 94 – Configuração de LAG em PE-3 (Nokia)

```
 interface port-channel1
  switchport mode trunk
  switchport trunk allowed vlan 1112
!
interface TenGigabitEthernet1/15
  switchport mode trunk
  switchport trunk allowed vlan 1112
!
```

```
 interface TenGigabitEthernet1/16
  switchport mode trunk
  switchport trunk allowed vlan 1112
!
```

Figura 95 – Configuração de LAG em PE-4 (Cisco IOS)

```
interface Port-channel1
  description lag-to-PE3
  switchport trunk allowed vlan 1112
  switchport mode trunk
!
interface GigabitEthernet0/1
  description to-PE3-1/1/5
  switchport access vlan 1112
  switchport mode access
  channel-group 1 mode active
!
interface GigabitEthernet0/2
  description to-PE3-1/1/10
  switchport trunk allowed vlan 1112
  switchport mode trunk
  channel-group 1 mode active
!
```

```
interface Port-channel2
   description lag-to-PE4
   switchport trunk allowed vlan 1112
   switchport mode trunk
 !
 interface GigabitEthernet0/3
   description to-PE4-GE15
   switchport access vlan 1112
   switchport mode access
   channel-group 2 mode active
 !
 interface GigabitEthernet0/4
   description to-PE4-GE16
   switchport trunk allowed vlan 1112
   switchport mode trunk
   channel-group 2 mode active
 !
```

Figura 96 – Configuração de LAG em CE-2 (Cisco IOS)

Redundância de *attachment-circuit* com MC-LAG

Infelizmente, os nós PE-4, PE-5 e PE-6 não tinham a capacidade de oferecer MC-LAG, e assim sendo esta técnica foi apenas testada nos nós PE-1 e PE-2 (Nokia). A Figura 97, Figura 98 e apresentam as configurações realizadas nos nós PE-1 e PE-2 e CE-1, respetivamente.

```
port 1/1/10
    ethernet
        mode access
        encap-type dot1q
        no autonegotiate
    exit
    no shutdown
exit
lag 1
    mode access
    encap-type dot1q
    port 1/1/10
    lacp active administrative-key 32768
    no shutdown
exit
redundancy
    multi-chassis
        peer 5.5.5.5 create
            mc-lag
                lag 1 lacp-key 1 system-id 00:00:00:00:00:01 system-priority 100
                no shutdown
            exit
            no shutdown
        exit
    exit
exit
```

Figura 97 – Configuração de MC-LAG em PE-1 (Nokia)

```
    port 1/1/10
        ethernet
            mode access
            encap-type dot1q
            no autonegotiate
        exit
        no shutdown
    exit
    lag 1
        mode access
        encap-type dot1q
        port 1/1/10
        lacp active administrative-key 32768
        no shutdown
    exit
    redundancy
        multi-chassis
            peer 4.4.4.4 create
                mc-lag
                    lag 1 lacp-key 1 system-id 00:00:00:00:00:01 system-priority 100
                    no shutdown
                exit
                no shutdown
            exit
        exit
    exit
```

Figura 98 – Configuração de MC-LAG em PE-2 (Nokia)

```
interface Port-channel1
  switchport trunk allowed vlan 1111
  switchport mode trunk
!
interface GigabitEthernet0/1
  description to_PE1
  switchport trunk allowed vlan 1111
  switchport mode trunk
  channel-group 1 mode active
!
interface GigabitEthernet0/2
  description to_PE2
  switchport trunk allowed vlan 1111
  switchport mode trunk
  channel-group 1 mode active
!
```

Figura 99 – Configuração de MC-LAG em CE-1 (Cisco IOS)

Troubleshooting

De forma a analisarmos o correto funcionamento dos LSP's, validando a sua conetividade e respetivo caminho, foram implementadas técnicas de operação, administração e manutenção, inserindo-se para o efeito comandos manualmente, nos nós PE-1 (Nokia) e PE-4 (Cisco IOS).

No equipamento Nokia foram utilizados os comandos "oam lsp-ping <nome do LSP>" e "oam lsp-trace <nome do LSP>", e no equipamento Cisco IOS os comandos "ping mpls traffic-eng tunnel <*id* do LSP>" e "traceroute mpls traffic-eng tunnel <*id* do LSP>". As figuras abaixo apresentam os comandos inseridos e a informação retornada.

```
A:PE-1# oam lsp-ping "lsp_to_PE4"
LSP-PING lsp_to_PE4: 92 bytes MPLS payload
Seq=1, send from intf PE1-P1, reply from 172.16.17.7
       udp-data-len=32 ttl=255 rtt=1.66ms rc=3 (EgressRtr)
---- LSP lsp_to_PE4 PING Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min = 1.66ms, avg = 1.66ms, max = 1.66ms, stddev = 0.000ms

A:PE-1# oam lsp-trace "lsp_to_PE4"
lsp-trace to lsp_to_PE4: 0 hops min, 0 hops max, 116 byte packets
1  1.1.1.1  rtt=2.77ms rc=8(DSRtrMatchLabel)
2  172.16.17.7  rtt=1.64ms rc=3(EgressRtr)
```

Figura 100 – Análise sobre o LSP em PE-1 (Nokia)

```
PE-4#ping mpls traffic-eng tunnel 74
Sending 5, 100-byte MPLS Echos to Tunnel74,
     timeout is 2 seconds, send interval is 0 msec:
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
Type escape sequence to abort.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

PE-4#traceroute mpls traffic-eng tunnel 74
Tracing MPLS TE Label Switched Path on Tunnel74, timeout is 2 seconds
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
Type escape sequence to abort.
  0 172.16.17.7 MRU 1500 [Labels: 131066 Exp: 0]
L 1 1.1.1.1 MRU 9198 [Labels: 131043 Exp: 0] 0 ms
! 2 4.4.4.4 4 ms
```

Figura 101 – Análise sobre o LSP em PE-4 (Cisco IOS)

Service mirroring local e Wireshark

Depois de analisados os LSP's, procedeu-se à configuração de um *service mirror* com o objetivo de encaminhar tráfego proveniente do *backbone* para uma interface onde se encontrava à escuta um *sniffer*.

A configuração apresentada pela próxima figura foi realizada em PE-1 (Nokia), onde para todo o tráfego de saída (*egress*) ou de entrada (*ingress*) proveniente da porta 1/1/6, era realizada uma cópia integral dos dados, sendo os mesmos posteriormente encaminhados para a porta 1/1/9.

```
mirror
    mirror-dest 10 create
        sap 1/1/9:0 create
        exit
        no shutdown
    exit
exit
debug
   mirror-source 10
          port 1/1/6 egress ingress
          no shutdown
   exit
exit
```

Figura 102 – Configuração de um *service mirroring* local

À porta 1/1/9 foi ligado um servidor Wireshark com o objetivo de capturar os pacotes encaminhados. As próximas figuras apresentam dois dos pacotes capturados.

```
> Frame 144076: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
v Ethernet II, Src: Alcatel-_e5:6c:49 (7c:20:64:e5:6c:49), Dst: Alcatel-_58:00:30 (7c:20:64:58:00:30)
  v Destination: Alcatel-_58:00:30 (7c:20:64:58:00:30)
      Address: Alcatel-_58:00:30 (7c:20:64:58:00:30)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Alcatel-_e5:6c:49 (7c:20:64:e5:6c:49)
      Address: Alcatel-_e5:6c:49 (7c:20:64:e5:6c:49)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: MPLS label switched packet (0x8847)
v MultiProtocol Label Switching Header, Label: 131043, Exp: 0, S: 0, TTL: 254
    0001 1111 1111 1110 0011 .... .... .... = MPLS Label: 131043
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...0 .... .... = MPLS Bottom Of Label Stack: 0
    .... .... .... .... .... .... 1111 1110 = MPLS TTL: 254
v MultiProtocol Label Switching Header, Label: 131046, Exp: 0, S: 1, TTL: 255
    0001 1111 1111 1110 0110 .... .... .... = MPLS Label: 131046
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label Stack: 1
    .... .... .... .... .... .... 1111 1111 = MPLS TTL: 255
> Data (78 bytes)
```

Figura 103 – Dados de entrada (*ingress*) em PE-1

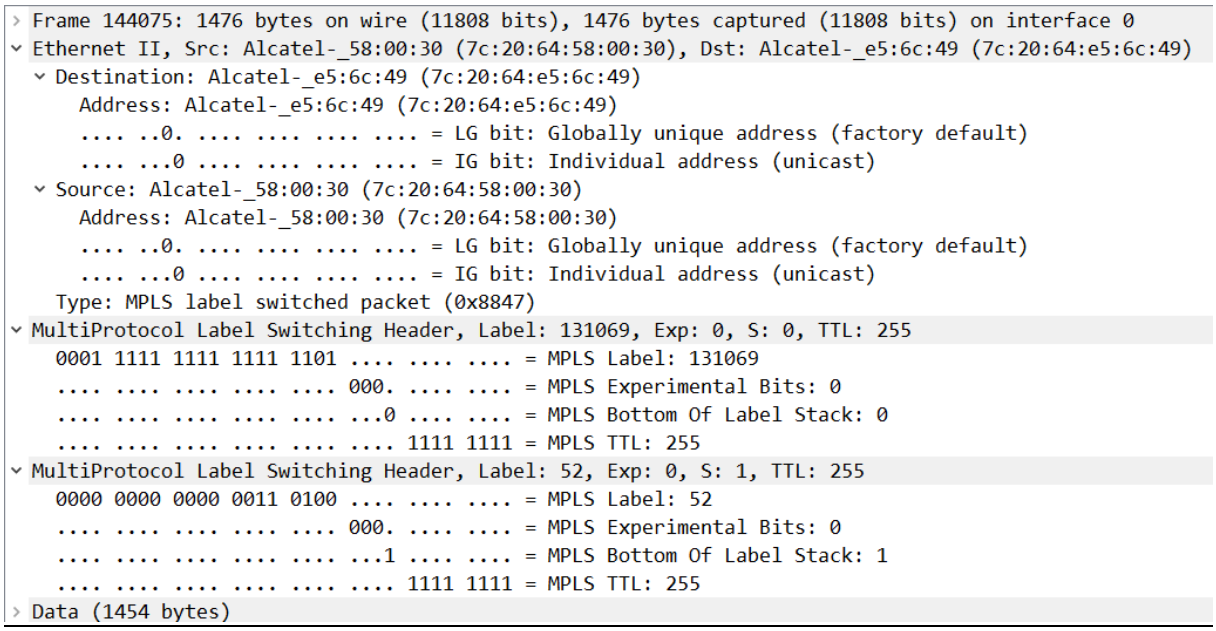

Figura 104 – Dados de saída (*egress*) de PE-1

No exemplo da Figura 103, relativo a um pacote de entrada, verifica-se que, proveniente de P-1 chega uma LSP *label* com o valor “131043”, e uma PW *label* com o valor “131046”. Enquanto que, no exemplo relativo a um pacote de saída, verifica-se que a LSP *label* tem o valor “131069”, e uma PW *label* com o valor “52”. A distinção entre a LSP *label* e a PW *label* é possível através do campo “S”, como explicado no subcapítulo 2.4.

De forma a descobrirmos os PE’s sobre os quais correspondiam a etiqueta do LSP e do *pseudowire*, foram inseridos comandos de *troubleshooting* sobre os nós de *backbone*, primeiro sobre o LSP e depois sobre o *pseudowire*, demonstrados pelas figuras abaixo. Constatou-se que os pacotes de entrada e saída analisados pela ferramenta Wireshark diziam respeito ao serviço 1001, de PE-1 para PE-4 e vice-versa. Assinalado a verde encontra-se a informação relativa ao par origem-destino <PE-1 – PE-4>, e a assinalou-se a vermelho a informação relativa a <PE-4 – PE-1>.

```
A:PE-1# show router rsvp session detail
RSVP Sessions (Detailed)
===============================================================================
LSP : lsp_to_PE4::path_loose_to_PE4
-------------------------------------------------------------------------------
From           : 4.4.4.4                 To             : 7.7.7.7
Tunnel ID      : 1                       LSP ID         : 4608
Style          : SE                      State          : Up
Session Type   : Originate
In Interface   : n/a                     Out Interface  : 1/1/6
In Label       : n/a                     Out Label      : 131069
-------------------------------------------------------------------------------
LSP : PE-4_t74
-------------------------------------------------------------------------------
From           : 7.7.7.7                 To             : 4.4.4.4
Tunnel ID      : 74                      LSP ID         : 1
Style          : SE                      State          : Up
Session Type   : Terminate
In Interface   : 1/1/6                   Out Interface  : n/a
In Label       : 131043                  Out Label      : n/a
```

Figura 105 – *Troubleshooting* sobre os LSP's de origem ou destino a PE-1 (Nokia)

```
A:P1# show router rsvp session detail
RSVP Sessions (Detailed)
===============================================================================
LSP : lsp_to_PE4::path_loose_to_PE4
-------------------------------------------------------------------------------
From           : 4.4.4.4                 To             : 7.7.7.7
Tunnel ID      : 1                       LSP ID         : 4608
Style          : SE                      State          : Up
Session Type   : Transit
In Interface   : 1/1/6                   Out Interface  : 1/1/9
In Label       : 131069                  Out Label      : 0
-------------------------------------------------------------------------------
LSP : PE-4_t74
-------------------------------------------------------------------------------
From           : 7.7.7.7                 To             : 4.4.4.4
Tunnel ID      : 74                      LSP ID         : 1
Style          : SE                      State          : Up
Session Type   : Transit
In Interface   : 1/1/9                   Out Interface  : 1/1/6
In Label       : 131066                  Out Label      : 131043
```

Figura 106 – *Troubleshooting* sobre os LSP's de trânsito em P-1 (Nokia)

```
PE-4#show mpls l2transport vc detail
Local interface: VFI 1001 VFI up
  Interworking type is Ethernet
  Destination address: 4.4.4.4, VC ID: 1001, VC status: up
    Output interface: Tu74, imposed label stack {131066 131046}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Load Balance: none
  Flow Label: Disabled
  Create time: 14:34:29, last status change time: 14:30:24
  Signaling protocol: LDP, peer 4.4.4.4:0 up
    Targeted Hello: 7.7.7.7(LDP Id) -> 4.4.4.4
    Status TLV support (local/remote)   : enabled/not supported
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: no fault
      Last local SSS circuit status rcvd: no fault
      Last local SSS circuit status sent: no fault
      Last local  LDP TLV    status sent: no fault
      Last remote LDP TLV    status rcvd: not sent
    MPLS VC labels: local 52, remote 131046
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 1537647, send 768659
    byte totals:   receive 2213582436, send 54152465
    packet drops:  receive 0, seq error 0, send 0
```

Figura 107 – *Troubleshooting* sobre os LSP's e serviços com origem em PE-4 (Cisco IOS)

```
A:PE-1# show service id 1001 sdp

===============================================================================
Services: Service Destination Points
===============================================================================
SdpId            Type IP address      Adm     Opr       I.Lbl       E.Lbl
-------------------------------------------------------------------------------
47:1001          Mesh 7.7.7.7         Up      Up        131046      52
-------------------------------------------------------------------------------
Number of SDPs : 1
```

Figura 108 – *Troubleshooting* sobre os serviços com origem em PE-1 (Nokia)

ANEXO VIII - CONFIGURAÇÕES DO LABORATÓRIO VPRN

Neste anexo encontram-se as configurações essenciais para implementação dos dois cenários VPRN. Primeiramente são apresentadas as configurações genérias aos dois cenários de implementação e posteriormente as configurações relevantes de cada cenário.

Configurações gerais

Para a rede de transporte, inicialmente foram configuradas as interfaces de interligação, o protocolo de *routing* dinâmico OSPF e ativado o MPLS em todos os nós da rede MPLS. Na rede de acesso foram configurados os nós CE de nível 2 e nível 3, e criadas 3 máquinas virtuais com o sistema operativo Ubuntu, disponibilizadas no servidor de virtualização Proxmox e essenciais para a realização dos testes de tempos de recuperação a falha. Além destes, e uma vez que em ambos os cenários VPRN se recorre ao MP-BGP, o protocolo BGP também se torna genérico aos próximos cenários.

Configuração de interfaces

Tendo em conta o esquema de endereçamento IPv4 e de interfaces de interligação demonstrado no subcapítulo 5.4 todos os nós de rede foram configurados. As figuras abaixo demonstram um exemplo em cada nó de rede, ou seja, nó PE-1 (Nokia), PE-4 (Cisco), P-1(Nokia), Switch CE-1 (Cisco) e Router CE-1 (Cisco).

```
port 1/1/6
    ethernet
    exit
    no shutdown
exit
port 1/1/7
    ethernet
    exit
    no shutdown
exit
port 1/1/10
    ethernet
        mode access
        encap-type dot1q
    exit
    no shutdown
exit
```

```
router
    interface "PE1-P1"
        address 172.16.14.4/24
        port 1/1/6
    exit
    interface "PE1-P3"
        address 172.16.34.4/24
        port 1/1/7
    exit
    interface "system"
        address 4.4.4.4/32
    exit
```

Figura 109 – Configuração das interfaces em PE-1 (Nokia)

```
interface Loopback1
  ip address 7.7.7.7 255.255.255.255
!
interface TenGigabitEthernet1/6
  description PE4-P2
  ip address 172.16.27.7 255.255.255.0
!
interface TenGigabitEthernet1/7
  description PE4-P1
  ip address 172.16.17.7 255.255.255.0
!
```

Figura 110 – Configuração das interfaces em PE-4 (Cisco IOS)

```
   port 1/1/5
       ethernet
       exit
       no shutdown
   exit
   port 1/1/6
       ethernet
       exit
       no shutdown
   exit
   port 1/1/7
       ethernet
       exit
       no shutdown
   exit
   port 1/1/8
       ethernet
       exit
       no shutdown
   exit
   port 1/1/9
       ethernet
       exit
       no shutdown
   exit
   port 1/1/10
       ethernet
         mode access
         encap-type dot1q
       exit
       no shutdown
   exit
```

```
    router
        interface "P1-P2"
            address 172.16.12.1/24
            port 1/1/5
        exit
        interface "P1-P3"
            address 172.16.13.1/24
            port 1/1/10
        exit
        interface "P1-PE1"
            address 172.16.14.1/24
            port 1/1/6
        exit
        interface "P1-PE2"
            address 172.16.15.1/24
            port 1/1/7
        exit
        interface "P1-PE3"
            address 172.16.16.1/24
            port 1/1/8
        exit
        interface "P1-PE4"
            address 172.16.17.1/24
            port 1/1/9
        exit
        interface "system"
            address 1.1.1.1/32
        exit
```

Figura 111 – Configuração das interfaces em P-1 (Nokia)

```
interface FastEthernet0/1
  description CPE1-to-Virt
  switchport trunk allowed vlan 3011
  switchport mode trunk
  !
interface FastEthernet0/23
  description to_CPE1-RT
  switchport trunk allowed vlan 3001,3011
  switchport mode trunk
!
interface GigabitEthernet0/1
  description to_PE1
  switchport trunk allowed vlan 3001
  switchport mode trunk
!
interface GigabitEthernet0/2
  description to_PE2
  switchport trunk allowed vlan 3001
  switchport mode trunk
  shutdown
!
```

Figura 112 – Configuração das interfaces no *switch* CE-1 (Cisco)

```
interface GigabitEthernet0/0/1
  no ip address
  negotiation auto
!
interface GigabitEthernet0/0/1.3001
  description WAN
  encapsulation dot1Q 3001
  ip address 10.10.11.2 255.255.255.0
!
interface GigabitEthernet0/0/1.3011
  description LAN
  encapsulation dot1Q 3011
  ip address 192.168.10.0 255.255.255.0
!
```

Figura 113 – Configuração das interfaces no *router* CE-1 (Cisco)

Configuração do protocolo OSPF

A configuração do protocolo OSPF apenas é possível depois de configuradas todas as interfaces participantes na VPRN. Este protocolo foi configurado em todos os nós MPLS (P e PE), sendo que as próximas figuras apresentam a configuração em PE-1 (Nokia), PE-4 (Cisco IOS) e P-1 (Nokia).

```
        ospf
            area 0.0.0.0
                interface "system"
                exit
                interface "PE1-P1"
                    interface-type point-to-point
                exit
                interface "PE1-P3"
                    interface-type point-to-point
                exit
            exit
        exit
```

Figura 114 – Configuração do protocolo OSPF em PE-1 (Nokia)

```
 router ospf 1
   router-id 7.7.7.7
   nsr
   redistribute static subnets
   network 7.7.7.7 0.0.0.0 area 0.0.0.0
   network  172.16.17.0  0.0.0.255  area
0.0.0.0
   network 172.16.27.0  0.0.0. 255  area
0.0.0.0
   default-information        originate
metric-type 1
 !
interface TenGigabitEthernet1/6
   description PE4-P2
   ip address 172.16.27.7 255.255.255.0
   ip ospf network point-to-point
 !
interface TenGigabitEthernet1/7
   description PE4-P1
   ip address 172.16.17.7 255.255.255.0
   ip ospf network point-to-point
 !
```

Figura 115 – Configuração do protocolo OSPF em PE-4 (Cisco IOS)

```
ospf
  area 0.0.0.0
    interface "system"
    exit
    interface "P1-P2"
      interface-type point-to-point
    exit
    interface "P1-P3"
      interface-type point-to-point
    exit
    interface "P1-PE1"
      interface-type point-to-point
    exit
    interface "P1-PE2"
      interface-type point-to-point
    exit
    interface "P1-PE3"
      interface-type point-to-point
    exit
    interface "P1-PE4"
      interface-type point-to-point
      mtu 1500
    exit
  exit
exit
```

Figura 116 – Configuração do protocolo OSPF em P-1 (Nokia)

Configuração da tecnologia MPLS

Após a configuração das interfaces e do protocolo OSPF chega o momento de configurar o protocolo MPLS, sendo esta configuração genérica aos tipos de serviços oferecidos, quer estes sejam de nível 2 ou de nível 3. As figuras seguintes demonstram as configurações efetuadas em PE-1, PE-4 e P1.

```
      mpls
          interface "system"
          exit
          interface "PE1-P1"
          exit
          interface "PE1-P3"
          exit
          no shutdown
      exit
```

Figura 117 – Configuração das interfaces MPLS em PE-1 (Nokia)

```
interface TenGigabitEthernet1/6
 description PE4-P2
 ip address 172.16.27.7 255.255.255.0
 ip ospf network point-to-point
 mpls ip
!
interface TenGigabitEthernet1/7
 description PE4-P1
 ip address 172.16.17.7 255.255.255.0
 ip ospf network point-to-point
 mpls ip
!
```

Figura 118 – Configuração das interfaces MPLS em PE-4 (Cisco IOS)

```
    mpls
        interface "system"
        exit
        interface "P1-PE1"
        exit
        interface "P1-PE2"
        exit
        interface "P1-PE3"
        exit
        interface "P1-PE4"
        exit
        interface "P1-P2"
        exit
        interface "P1-P3"
        exit
        no shutdown
    exit
```

Figura 119 – Configuração das interfaces MPLS em P-1 (Nokia)

Enquanto que nos equipamentos Nokia é necessário ativar a tecnologia MPLS e configurar as interfaces que farão parte deste domínio, as versões Cisco IOS o MPLS é automaticamente habilitado no momento de configuração das interfaces. Além disto, nesta versão de *software* ao habilitarmos o MPLS na interface estamos também a habilitar o protocolo de sinalização LDP.

Por fim, e como em ambos os cenários do laboratório VPRN se utiliza o MP-BGP para sinalização dos serviços, foi configurado o protocolo BGP nos nós PE-1 e PE-4.

```
router                                          begin
    autonomous-system 65001                   policy-statement "MBGP-to-OSPF"
    bgp                                           entry 10
        group "iBGP"                                  from
            family ipv4 vpn-ipv4                        protocol bgp-vpn
            peer-as 65001                             exit
            local-address 4.4.4.4                     action accept
            neighbor 7.7.7.7                          exit
            exit                                  exit
        exit                                    exit
    exit                                        commit
    policy-options                            exit
```

Figura 120 – Configuração do protocolo BGP em PE-1 (Nokia)

```
router bgp 65001                                    neighbor 4.4.4.4 active
  bgp router-id 7.7.7.7                           exit-address-family
  bgp log-neighbor-changes                        !
  neighbor 4.4.4.4 remote-as 65001                address-family vpnv4
  neighbor    4.4.4.4    update-source              neighbor 4.4.4.4 activate
Loopback1                                           neighbor send-community extended
  !                                               exit-address-family
  address-family ipv4                           !
```

Figura 121 – Configuração do protocolo BGP em PE-4 (Cisco IOS)

Uma vez realizada a configuração genérica passou-se para as configurações específicas de cada cenário.

Cenário 1

No primeiro cenário de implementação de um serviço VPRN utilizou-se os protocolos LDP para sinalização dos LSP's e o protocolo MP-BGP para sinalização dos *pseudowires*.

As figuras abaixo apresentam as configurações realizadas em PE-1, PE-4 e P-1, para configuração do protocolo LDP.

```
   router                                          policy-options
       ldp-shortcut                                    begin
       ldp                                             policy-statement "to_LDP"
           export "to_LDP"                                 entry 10
           interface-parameters                                from
               interface "PE1-P1"                                 protocol direct
               exit                                            exit
               interface "PE1-P3"                              action accept
               exit                                            exit
           exit                                            exit
           targeted-session                            exit
           exit                                        commit
       exit                                            exit
   exit
```

Figura 122 – Configuração do protocolo LDP em PE-1 (Nokia)

```
mpls label protocol ldp                     interface TenGigabitEthernet1/7
mpls ldp router-id Loopback1                  description PE4-P1
!                                             mpls ip
interface TenGigabitEthernet1/6             !
  description PE4-P2                        router ospf 1
  mpls ip                                     mpls ldp sync
!                                           !
```

Figura 123 – Configuração do protocolo LDP em PE-4 (Cisco IOS)

```
   router                                              exit
       ldp                                             interface "P1-PE4"
           interface-parameters                        exit
               interface "P1-PE1"                      interface "P1-P2"
               exit                                    exit
               interface "P1-PE2"                      interface "P1-P3"
               exit                                    exit
               interface "P1-PE3"                  exit
```

Figura 124 – Configuração do protocolo LDP em PE-1 (Nokia)

Por fim, realizou-se a configuração de um serviço VPRN onde foi utilizado um novo processo OSPF como protocolo dinâmico de *routing* para propagar as rotas dos clientes. A Figura 125, Figura 126 e Figura 127 apresentam as configurações realizadas em PE-1, PE-4 e *router* CPE-1, respetivamente.

```
   service
       customer 20 create
       exit
       vprn 3000 customer 20 create
           interface "PE1_to_CPE1" create
           exit
       exit
       vprn 3000 customer 20 create
           autonomous-system 65001
           route-distinguisher 65001:3000
           auto-bind mpls
           vrf-target target:65001:3000
           interface "PE1_to_CPE1" create
               address 10.10.11.1/24
               sap 1/1/10:3001 create
               exit
           exit
           ospf 10.10.1.1
               export "MBGP-to-OSPF"
               area 0.0.0.10
                   interface "PE1_to_CPE1"
                       interface-type point-to-point
                   exit
               exit
           exit
           no shutdown
       exit
   exit
```

Figura 125 – Configuração do serviço VPRN no PE-1 (Nokia)

```
interface TenGigabitEthernet1/16.3002
  encapsulation dot1Q 3002
  ip vrf forwarding 3000
  ip address 10.10.22.1 255.255.255.0
  ip ospf network point-to-point
!
router bgp 65001
  address-family ipv4 vrf 3000
    redistribute connected
    redistribute ospf 10
   exit-address-family
!
```

Figura 126 – Configuração do serviço VPRN no PE-4 (Cisco IOS)

```
interface GigabitEthernet0/0/1
  no ip address
  negotiation auto
!
interface GigabitEthernet0/0/1.3001
  description WAN
  encapsulation dot1Q 3001
  ip address 10.10.11.2 255.255.255.0
  ip ospf network point-to-point
!
interface GigabitEthernet0/0/1.3011
  description LAN
  encapsulation dot1Q 3011
  ip address 192.168.11.0 255.255.255.0
!
router ospf 10
  network 10.10.11.0 0.0.0.255 area 0.0.0.10
  network 192.168.11.0 0.0.0.255 area 0.0.0.10
!
```

Figura 127 – Configuração do processo OSPF no *router* CE-1 (Cisco)

Cenário 2

No segundo cenário pretendeu-se substituir o protocolo LDP (responsável pela sinalização dos LSP's) pelo protocolo RSVP. Assim sendo, foram retiradas todas as configurações alusivas ao protocolo LDP e configurado o RSVP em todos os nós de rede. As figuras seguintes apresentam a configuração realizada em P-1, PE-1 e PE-4.

```
        rsvp
            interface "system"
            exit
            interface "P1-P2"
            exit
            interface "P1-P3"
            exit
            interface "P1-PE1"
            exit
            interface "P1-PE2"
            exit
            interface "P1-PE3"
            exit
            interface "P1-PE4"
            exit
            no shutdown
        exit
```

Figura 128 - Configuração do protocolo RSVP em P-1 (Nokia)

```
        rsvp
            interface "system"
            exit
            interface "PE1-P1"
            exit
            interface "PE1-P3"
            exit
            no shutdown
        exit
```

Figura 129 – Configuração do protocolo RSVP em PE-1 (Nokia)

```
interface TenGigabitEthernet1/6
  description PE4-P2
  mpls traffic-eng tunnels
!
interface TenGigabitEthernet1/7
  description PE4-P1
  mpls traffic-eng tunnels
!
```

Figura 130 – Configuração do protocolo RSVP em PE-4 (Cisco IOS)

Depois de identificadas as interfaces pelas quais irá ocorrer a sinalização por RSVP ativaram-se as extensões de engenharia de tráfego para o protocolo OSPF.

```
        ospf
            traffic-engineering
            exit
        exit
```

Figura 131 – Configuração da extensão de engenharia de tráfego no P-1 (Nokia)

```
        ospf
            traffic-engineering
            rsvp-shortcut
            exit
        exit
```

Figura 132 – Configuração da extensão de engenharia de tráfego no PE-1 (Nokia)

```
        router ospf 1
            mpls traffic-eng router-id Loopback1
            mpls traffic-eng area 0.0.0.0
        !
```

Figura 133 – Configuração da extensão de engenharia de tráfego no PE-4 (Cisco IOS)

Finalmente, foi instânciado o serviço VPRN nos nós PE-1 e PE-4, tal como aconteceu no cenário anterior, onde foi também configurado um novo processo OSPF para propagação das rotas dos clientes.

```
interface TenGigabitEthernet1/16.3002
  encapsulation dot1Q 3002
  ip vrf forwarding 3000
  ip address 10.10.22.1 255.255.255.0
  ip ospf network point-to-point
!
router bgp 65001
  address-family ipv4 vrf 3000
    redistribute connected
    redistribute ospf 10
   exit-address-family
!
```

Figura 134 – Configuração do serviço VPRN no PE-4 (Cisco IOS)

```
    service
        customer 20 create
        exit
        vprn 3000 customer 20 create
            interface "PE1_to_CPE1" create
            exit
        exit
        vprn 3000 customer 20 create
            autonomous-system 65001
            route-distinguisher 65001:3000
            auto-bind mpls
            vrf-target target:65001:3000
            interface "PE1_to_CPE1" create
                address 10.10.11.1/24
                sap 1/1/10:3001 create
                exit
            exit
            ospf 10.10.1.1
                export "MBGP-to-OSPF"
                area 0.0.0.10
                    interface "PE1_to_CPE1"
                        interface-type point-to-point
                    exit
                exit
            exit
            no shutdown
        exit
    exit
```

Figura 135 – Configuração de serviço VPRN no PE-1 (Nokia)

```
 interface GigabitEthernet0/0/1.3001
   description WAN
   encapsulation dot1Q 3001
   ip address 10.10.11.2 255.255.255.0
   ip ospf network point-to-point
 !
router ospf 10
   network 10.10.11.0 0.0.0.255 area 0.0.0.10
   network 192.168.11.0 0.0.0.255 area 0.0.0.10
 !
```

Figura 136 – Configuração do processo OSPF no *router* CE-1 (Cisco)

ANEXO IX – DISPOSIÇÃO DE EQUIPAMENTOS NO LABORATÓRIO DO CAT-ISMAI

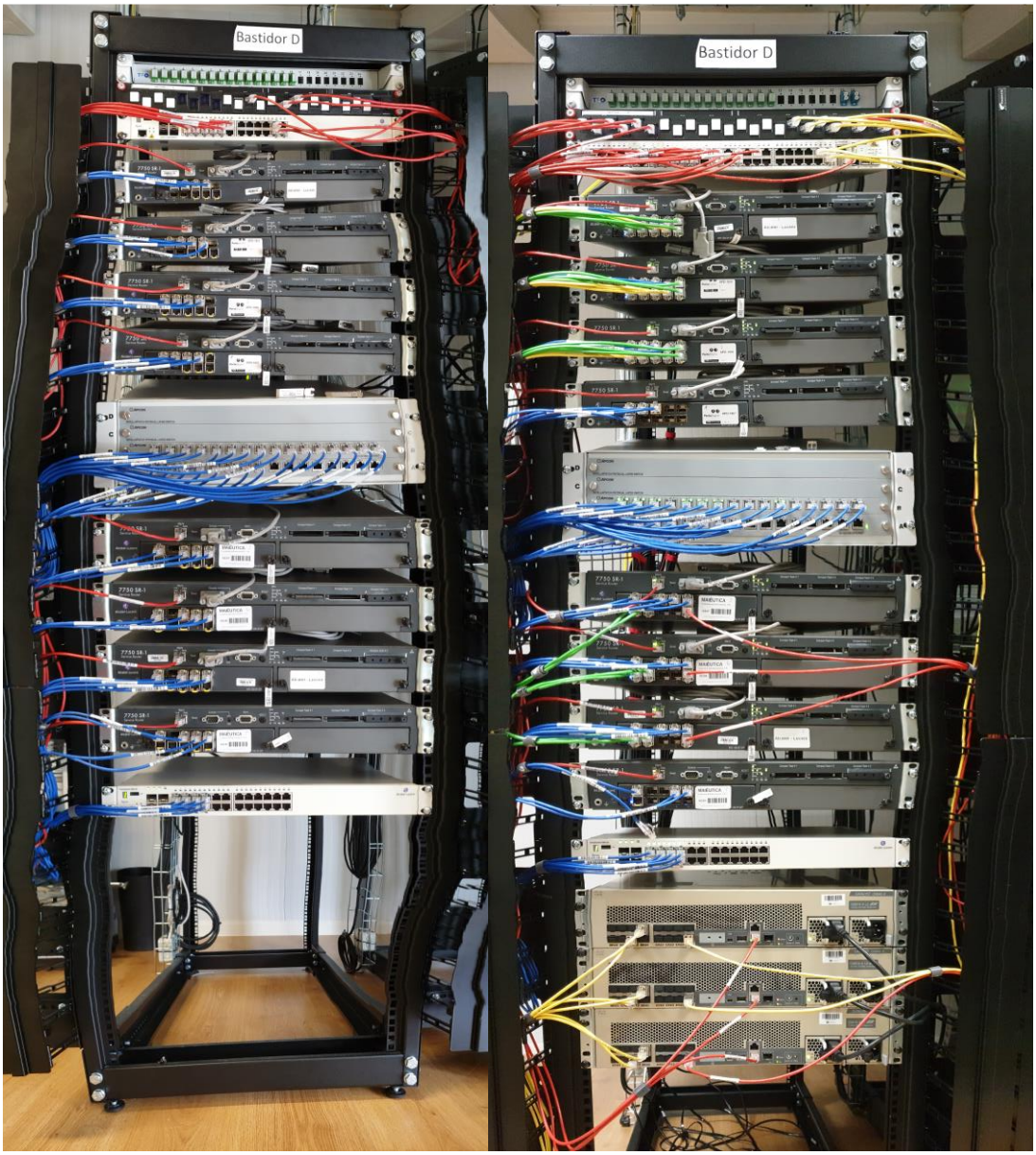

Figura 137 – Equipamento utilizado no CAT-ISMAI