INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

DEPARTAMENTO DE ENGENHARIA DE ELECTRÓNICA E TELECOMUNICAÇÕES E DE COMPUTADORES

ÁREA DE TELECOMUNICAÇÕES

Qualidade de Serviço em Redes Avançadas

João Eusébio Dionísio

DISSERTAÇÃO PARA OBTENÇÃO DO GRAU DE MESTRE
EM ENGENHARIA DE ELECTRÓNICA E TELECOMUNICAÇÕES

Orientador(a): Prof. Vitor Almeida
Co-Orientador: Prof. Pedro Ribeiro

Júri:
Presidente: Prof. Doutor Nuno Cruz
Vogais: Prof. Doutor João Ascenso
Prof. Doutor Pedro Ribeiro

dezembro de 2018

Agradecimentos

Gostaria de agradecer aos Professores Pedro Ribeiro e Vítor Almeida pelos conhecimentos transmitidos, pelo apoio e disponibilidade constantes ao longo de todo o projeto.

Queria também agradecer aos meus pais, irmã e à Sara pelo apoio ao longo de toda licenciatura e mestrado.

Índice

Índice de Figuras

Índice de tabelas

Acrónimos

ARPA - Advanced Research Projects Agency

BFD - Bidirectional Forwarding Detection

CSPF - Constrained-Based Shortest Path First

DS - Differentiated Services

DSCP - Differentiated Services Code Point

eLER - Egress Label Edge Router

EUA - Estados Unidos da América

ECN - Explicit Congestion Notification

ERO - Explicit Route Object

FRR - Fast Reroute

FF - Fixed Filter

iLER - Ingress Label Edge Router

IPL - Instituto Politécnico de Lisboa

IGP - Interior Gateway Protocol

IANA - Internet Assigned Number Authority

IETF - Internet Engineering Task Force

IP - Internet Protocol

ISP - Internet Service Providers

LDP - Label Distribution Protocol

LFIB - Label Forwarding Information Base

LIB - Label Information Base

LSP - Label Switched Path

LSR - Label Switch Router

LB - Largura de Banda

L2 - Layer 2

L3 - Layer 3

LSA - Link-state Advertisements

LAN - Local Area Network

MBB - Make-Before-Break

MAC - Media Access Control

MP - Merge Point

MPLS - Multiprotocol Label Switching

NSF - National Science Foundation

NCP - Network Control Protocol

OSPF - Open Short Path First

PHB - Per Hop Behavior

PLR - Point of Local Repair

PPP - Point-to-point Protocol

P - Provider (Core) Router

PE - Provider Edge Router

QoS - Quality of Service

RSVP - Resource Reservation Protocol

SLA - Service Level Agreement

SE - Shared Explicit

SRLG - Shared Risk Link Group

SPF - Shortest path first

T-LDP - Targeted LDP

TE - Traffic Engineering

TED - Traffic Engineering Database

TCP - Transmission Control Protocol

TLV - Type Length Values

UDP - User Datagram Protocol

VPLS - Virtual Private LAN Service

VPRN - Virtual Private Routed Network

VPWS - Virtual Private Wire Service

Resumo

O presente trabalho tem como objetivo a melhoria de QoS da rede MPLS do IPL. O IPL inclui 8 unidades orgânicas, entre as quais se inclui o ISEL, os serviços centrais e os serviços sociais. Estas entidades encontram-se disseminadas pela cidade de Lisboa e na Amadora, estando todas elas interligadas através de uma rede de fibra ótica onde se ligam os *routers* PE que dão suporte à WAN do IPL e que utilizam o protocolo MPLS com distribuição das suas *labels* através de LDP.

Foram desenvolvidas duas soluções, ambas com intuito de permitir o balanceamento da rede, de forma a maximizar a utilização dos recursos e melhorar a sua resiliência. Estas soluções foram testadas no laboratório da Alcatel-Lucent no ISEL.

A primeira solução utiliza o protocolo RSVP-TE com a reserva de largura de banda para balancear dinamicamente a rede. Foram disponibilizados 100 Mb/s em cada ligação e cada LSP reservou 10 Mb/s. Como resiliência foi utilizado o FRR *facility*.

A segunda solução utiliza o protocolo RSVP-TE com *admin-groups* para balancear "manualmente" a rede. Como resiliência foram utilizados *Hot-standby secondary-path* controlados através de restrições de *admin-groups* contrárias às aplicadas no *primary-path*. Foi ainda implementada uma versão alternativa que inclui o FRR *facility.*

Foram alvos de testes as configurações desenvolvidas e a configuração operacional existente na rede MPLS do IPL. Estes tiveram como objetivo medir a largura de banda, latência, *jitter* e o tempo de recuperação de uma falha de rede. Os resultados da largura de banda, latência e *jitter* não demonstraram diferenças significativas, tal como esperado. Os resultados do tempo de recuperação de falhas em ligações ponto-a-ponto mostraram que as configurações desenvolvidas conseguem recuperar 10 vezes mais rápido que a configuração atualmente em operação. Conclui-se que as configurações desenvolvidas melhoram o balanceamento e a resiliência da rede MPLS do IPL.

Abstract

The present work aims to improve the QoS of IPL MPLS network. The IPL comprises 8 organic units, including ISEL, central services and social services. These units, located in Lisbon and Amadora, are interconnected through a network of optic fiber that can include multiple PE routers in each location. This MPLS network uses the LDP protocol for label distribution.

In order to improve the QoS parameters, two solutions were developed with the goal of achieving a balanced network and also improved resilience. The solution were tested in the Alcatel-Lucent laboratory, at ISEL.

The first solution uses the RSVP-TE protocol with bandwidth reservation to dynamically balance the network. Each connection provided 100 Mb/s for reservation and each LSP reserved 10 Mb/s. The resilience was achieved using FRR facility.

The second solution uses the RSVP-TE protocol with admin-groups to manually balance the network. The network resilience was secured with a secondary-path hot-standby controlled through admin-groups constraints. It was also implemented an alternative version that includes the FRR facility.

The tests were performed using the developed configurations and the operational configuration in IPL MPLS network. The purpose of these tests was to measure the QoS parameters, bandwidth, latency, jitter and the recovery time on a network failure. Overall the results of bandwidth, latency and jitter were similar in all the configurations, as expected. The results obtained on the recovery time during a network failure in point-to-point connections have shown that the developed configurations were able to recover 10 times faster than the operational configuration. In conclusion, the developed configurations were capable of an improvement on the network balance and resilience, resulting in an upgrade of QoS in IPL MPLS network.

1. Introdução

Nos primórdios da computação no final dos anos 1960, a maioria das companhias tinha um único sistema para todo o processamento de informação. Estes sistemas eram proprietários, sendo o equipamento incompatível com outros fabricantes. Devido a estas limitações as comunicações entre empresas enfrentavam vários problemas, como a incompatibilidade dos sistemas utilizados, a obrigatoriedade de construir as suas próprias infraestruturas de comunicações, etc. O problema estendeu-se aos sistemas militares dos Estados Unidos da América (EUA), dado estes terem adquirido diferentes sistemas para diferentes *sites* e devido a incompatibilidades não conseguirem comunicar entre si. Para a resolução deste problema foi concebido o projeto ARPANET, este foi desenvolvido pela *Advanced Research Projects Agency* (ARPA) do departamento da defesa dos EUA, para ser a primeira rede *packet-switched*. Com o desenvolvimento deste projeto apareceu o protocolo *Network Control Protocol* (NCP) que permitia a troca de *emails* e transferência de ficheiros entre máquinas de diferentes sistemas, resolvendo assim o problema inicial. No entanto este protocolo era limitado em vários aspetos, como o sistema de endereçamento e resiliência. Assim, em 1973 o *Transmission Control Protocol* (TCP) seria apresentado e mais tarde em 1978 algumas das suas funções seriam desviadas para o protocolo *Internet Protocol* (IP). Com esta alteração e com o desenvolvimento de outros protocolos auxiliares (ex: ICMP) surgiu a família de protocolos designada por TCP/IP, ainda utilizada nos dias de hoje [1].

Mais tarde em 1985, em resposta à sobrecarga da rede ARPANET a *National Science Foundation* (NSF) dos EUA criou o conceito de *Network Tiers* que utiliza uma arquitetura de rede hierárquica. Assim as redes locais das universidades estariam ligadas a uma rede regional que funcionaria como *tier* intermédio e esta por sua vez estaria ligada ao *backbone* da rede, o *tier* mais alto. Em 1990 com o crescimento comercial da rede nasceu a indústria dos *Internet Service Providers* (ISP) [1]. A evolução e expansão das redes dos ISP levaram a que as empresas deixassem de investir na criação das suas próprias infraestruturas de conectividade e passassem a contratar serviços aos ISP. A qualidade destes serviços é garantida através de *Service Level Agreements* (SLA), sendo estes tipos de contractos celebrados entre o ISP e o cliente que especifica os parâmetros de *Quality of Service* (QoS) que o ISP deve respeitar, tendo penalidades em caso contrário. A disponibilidade, perdas de pacotes, latência e largura de banda são usualmente especificados nestes contractos como parâmetros de QoS [2].

Com o aumento exponencial de negócios à volta da *Internet*, cresceu também a necessidade de garantir parâmetros de QoS cada vez mais exigentes para diferentes tipos de tráfego. Assim as redes inicialmente baseadas em serviços *best-effort*, ou seja pacotes processados por ordem de chegada sem distinção do tipo de tráfego, não conseguiam responder às necessidades de QoS do mercado. Em resposta, o *Internet Engineering Task Force* (IETF) propuseram novos modelos e mecanismos, como o modelo *Integrated Services/Resource Reservation Protocol* (RSVP), o modelo *Differentiated Services* (DS) e ainda *Multiprotocol Label Switching* (MPLS) com a possibilidade de realizar *Traffic Engineering* (TE) e *Constraint-based Routing*. O MPLS-TE permite a manipulação da largura de banda atribuída a cada serviço e ainda novos

métodos de resiliência que oferecem uma maior disponibilidade da rede. Os modelos *Intserv* e *Diffserv* permitem de diferentes formas atribuir aos pacotes IP prioridades distintas para os vários tipos de tráfego. Com esta atribuição é possível controlar a ordem de processamento dos pacotes, diminuindo a latência dos tráfegos com requisitos temporais exigentes e ainda os pacotes a descartar seletivamente em caso de congestão da rede, diminuindo a perda de pacotes de serviços prioritários. Os modelos MPLS-TE e MPLS *DiffServ*-TE são atualmente os mais utilizados para melhorar os parâmetros de QoS em todas as suas vertentes [3] [4]. No entanto, a melhoria das infraestruturas e da capacidade de processamento dos equipamentos também permite melhorar as condições de QoS, embora esta seja uma solução mais dispendiosa e que não garante o aproveitamento da capacidade da rede.

Neste projeto pretende-se fazer um estudo sobre os parâmetros de QoS na rede MPLS do Instituto Politécnico de Lisboa (IPL). Serão alvo de estudo as técnicas de MPLS e MPLS-TE, tendo como objetivo a melhoria dos parâmetros de QoS na rede do IPL. Para efeitos de testes foi utilizado o laboratório Alcatel-Lucent no ISEL com o intuito de simular a rede MPLS do IPL.

1.1. *Quality of Service* (QoS)

A qualidade de serviço pode ser definida de forma subjetiva como o nível de satisfação do utilizador do serviço face ao desempenho geral do serviço [5]. Sendo que a forma mais comum de avaliar os serviços de rede IP é através dos parâmetros disponibilidade, perda de pacotes, latência e largura de banda [2], como se pode observar na Figura 1.

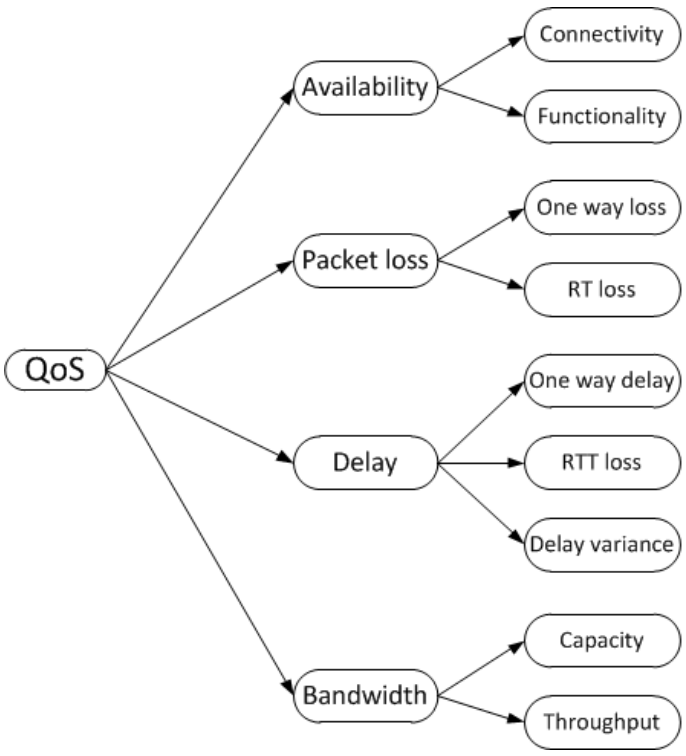

Figura 1 – Parâmetros de QoS, retirado de H. Lee *et al.* [2].

O perfil de qualidade de serviço está diretamente ligado ao tipo de tráfego do serviço, pois é o tipo de tráfego que determina as suas necessidades de QoS. Os tipos de tráfego podem ser atualmente definidos através das seguintes características [6]:

- **Tráfego em tempo real:** Essencial para tráfegos com a necessidade de manter constante o tempo entre pacotes e manter o tempo mínimo de transmissão entre emissor e recetor. Existe também o tráfego que não é em tempo real, logo não considera o tempo de transmissão prioritário [6].
- **Rajadas:** Quando o tráfego está sujeito a rajadas de pacotes existe uma flutuação considerável no número de pacotes transmitidos por segundo. Com este tipo de tráfego é usual ter problemas de *delay* variável, também conhecido por *jitter* [6].
- **Importância:** Alguns tipos de tráfego são mais importantes que outros dependendo da sua aplicação. Assim para tráfegos de alta importância qualquer deformação ou interrupção pode ter consequências negativas para o cliente e para o ISP [6].
- **Largura de banda:** Todos os tipos de tráfego necessitam de uma determinada largura de banda e quando esta é maior do que a que está disponível os fluxos são afetados [6].

1.1.1. Disponibilidade

A disponibilidade ou *availability* contabiliza o tempo em que o serviço se encontra indisponível. Normalmente as causas das quebras de serviço são a perda de ligações físicas e a avaria dos equipamentos. Os ISP podem tomar medidas de prevenção, como a instalação de uma topologia de rede redundante, como se pode observar na Figura 2. Nesta está representada a redundância de topologia e de ligações físicas, sendo a primeira a ligação em anel e a segunda o número de ligações entre os mesmos equipamentos.

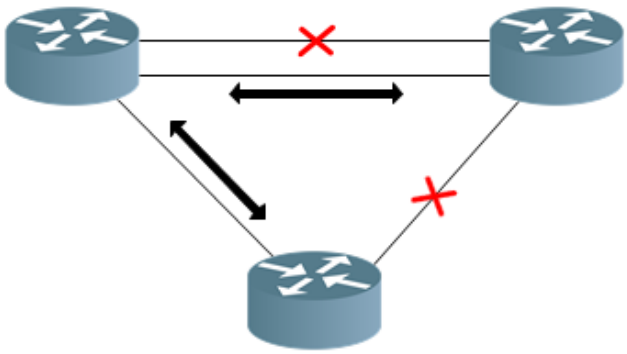

Figura 2 – Exemplo de redundância de topologia e de ligações físicas.

A redundância de equipamento passa pela duplicação dos equipamentos mantendo o serviço operacional em caso de avaria de um equipamento, como se pode observar na Figura 3.

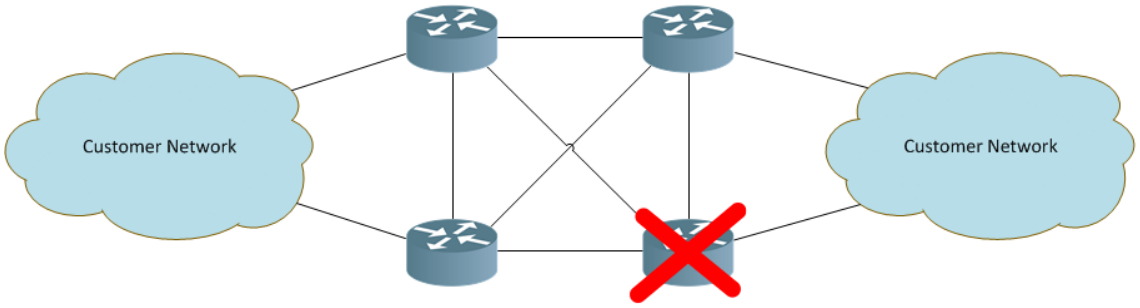

Figura 3 – Exemplo da redundância de equipamento.

Além dos esforços da rede ao nível físico, existe também um planeamento ao nível protocolar que pode melhorar a resposta da rede no caso de perdas de ligações ou equipamentos, este será abordado em maior pormenor nos próximos capítulos. A verificação de conectividade é feita essencialmente através de testes regulares de "*echo*" (pergunta-resposta), sendo que se considera uma quebra de serviço quando este apresenta 100% de perda de pacotes [6].

1.1.2. Perda de pacotes

A perda de pacotes ou *packet loss* indica a percentagem média de pacotes perdidos na rede do ISP em determinado período de tempo, sendo esta medida apenas num sentido ou na ida e volta. Existem várias possibilidades para a perda de pacotes, sendo as mais comuns:

- Congestão da rede
- Degradação do sinal
- Corrupção dos pacotes
- Falhas de *hardware*

O tráfego pode ainda ser descartado devido a uma limitação da largura de banda imposta pelo ISP de acordo com o SLA, ou seja caso o cliente envie uma quantidade de tráfego superior ao que foi contratado este poderá ser descartado [6] [7].

1.1.3. Latência

A latência ou *delay* representa o atraso da transmissão dos pacotes extremo-a-extremo (*end-to-end*). Alguns serviços, como uma chamada telefónica, suportam atrasos até 150 ms sem que seja auditivamente notória a degradação de qualidade da chamada. Assim é importante que os atrasos na rede sejam mínimos, para garantir a qualidade dos serviços implementados sobre a rede [6] [7]. Os atrasos podem ser acumulados pelas seguintes formas:

- **Transmissão:** É necessário tempo para criar os impulsos eletrónicos dos bits correspondentes ao pacote [6].
- ***Queuing*:** Corresponde ao tempo que um pacote espera em *buffer* para ser processado ou transmitido. Este apenas adiciona atrasos em caso de congestão [6].

- **Processamento:** Corresponde ao tempo necessário para o *router* verificar a tabela de encaminhamento e encapsular o pacote antes de o transmitir [6].
- **Propagação:** É o tempo que o pacote demora a atravessar o cabo de um *router* até ao próximo. Este depende do tipo de cabo utilizado e ainda da distância entre *routers* [6].

Os atrasos podem ser medidos de várias formas, como o tempo de transmissão numa direção (*one way delay*), o tempo de ida e volta (*round trip time*) e ainda o atraso variável (*jitter*).

1.1.3.1. *Jitter*

O *Jitter* é uma medida de atrasos variáveis, que mede o intervalo de tempo variável entre pacotes. Assim se todos os pacotes forem transmitidos com a mesma diferença temporal entre eles não há variações, logo não há *jitter*. No entanto, o *queuing* e o processamento dos pacotes no *router* adicionam um atraso variável aos pacotes, logo estes serão transmitidos em intervalos variáveis, o que leva ao aparecimento de *jitter* [6]. O *jitter* pode ser definido das seguintes formas:

- ***Jitter* negativo:** Representa os pacotes recebidos com um intervalo entre eles maior do que o esperado [6].
- ***Jitter* positivo:** Representa os pacotes recebidos com um intervalo entre eles menor do que o esperado [6].

Para alguns tipos de tráfegos mais exigentes, como o tráfego de voz, é aceitável um *jitter* até 20 ms [6]. Na Figura 4 pode-se observar uma representação da transmissão de pacotes com as várias formas de *jitter* e na sua ausência.

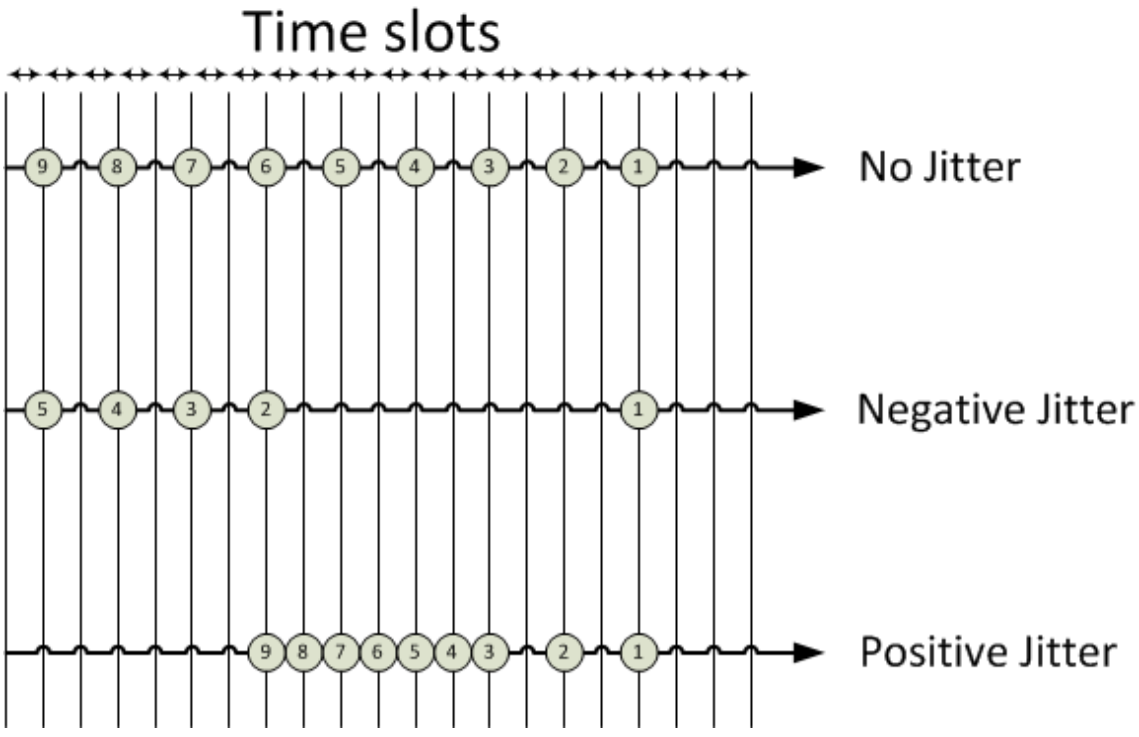

Figura 4 – Representação das várias formas de *jitter*.

1.1.4. Largura de banda

A largura de banda define a quantidade de informação (bits) que pode ser transferida entre dois equipamentos num determinado período. Normalmente é medida em bits por segundo e o valor mais alto que consiga atingir é referido como a capacidade da ligação [6].

1.2. *Service Level Agreement* (SLA)

Para um melhor entendimento dos parâmetros QoS é necessário entender o propósito do SLA. Este é um contrato formal entre o prestador do serviço e o cliente, pode ser utilizado em qualquer indústria e define o que o cliente pode esperar do serviço prestado em termos de desempenho, fiabilidade, segurança e procedimentos a seguir [8]. Tipicamente um SLA contêm a seguinte informação:

- **Descrição da natureza do serviço prestado, que inclui o tipo e especificações do serviço a ser prestado:** No caso de um serviço de rede IP deve ser especificada a manutenção do serviço em questão [8].
- **O desempenho esperado do serviço, especialmente a fiabilidade e resposta em caso de quebra de serviço:** Por fiabilidade entende-se quanto tempo se espera que o serviço esteja ativo e que perdas de serviço podem ser esperadas. No caso de quebra de serviço ficará definido quanto tempo este poderá estar desativo sem consequências para o ISP [8].
- **Procedimento para reportar problemas com o serviço:** Indica informações sobre a pessoa a ser contactada para a resolver o problema, assim como o tempo máximo para o problema ser assignado e obter resposta [8].
- **Janela temporal para resolução de problemas:** Esta indica o tempo máximo para a resolução de problemas, como por exemplo no caso de uma falha de uma ligação poderá ter um limite de 24h para voltar a ativar a ligação [8].
- **Processo de monitorização de QoS:** Define como e quem fará a monitorização do desempenho do serviço, que estatísticas serão utilizadas, períodos de levantamento de dados, etc [8].
- **Consequências para o ISP caso não cumpra com as suas obrigações:** Por norma são oferecidos alguns créditos ao cliente, no entanto pode também levar à rescisão do contrato ou a um reembolso pelos prejuízos causados pela perda de serviço [8].
- **Outras cláusulas e regras:** Nestas são apresentadas condições ao qual as cláusulas de QoS contratada não são aplicadas, como por exemplo em casos onde os equipamentos do ISP sejam danificados por desastres naturais ou guerras. Algumas destas regras aplicam-se também ao cliente, como por exemplo no caso de o cliente tentar quebrar a segurança da rede do ISP [8].

Os ISP têm uma vasta variedade de serviços, no entanto apenas os serviços de conectividade são alvo de estudo neste projeto. Assim na Figura 5 pode-se observar o típico cenário da rede ISP e os seus clientes.

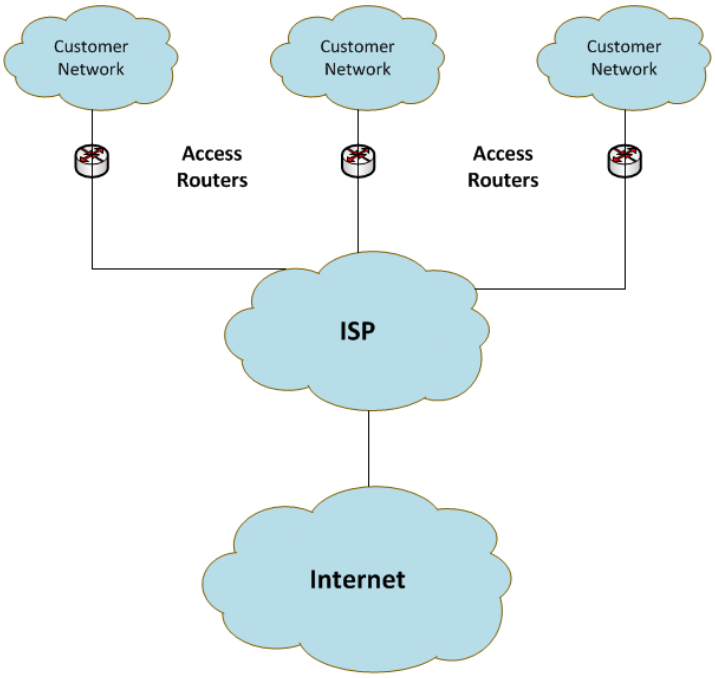

Figura 5 – Cenário Logico da típica rede de um ISP.

Os ISP que oferecerem as melhores condições de QoS serão mais competitivos no mercado, tornando essencial a utilização de técnicas MPLS-TE e de MPLS DS-TE para extrair a capacidade máxima das infraestruturas.

1.3. Modelo TCP/IP

O encaminhamento de pacotes pode ser definido através dos modelos OSI ou TCP/IP, tendo sido ambos concebidos com o intuito de permitir comunicações entre equipamentos independentemente da sua marca. Para esta breve introdução ao encaminhamento de pacotes será apenas abordado o modelo TCP/IP.

O modelo TCP/IP divide as funções da rede em quatro camadas, como se pode observar na Figura 6.

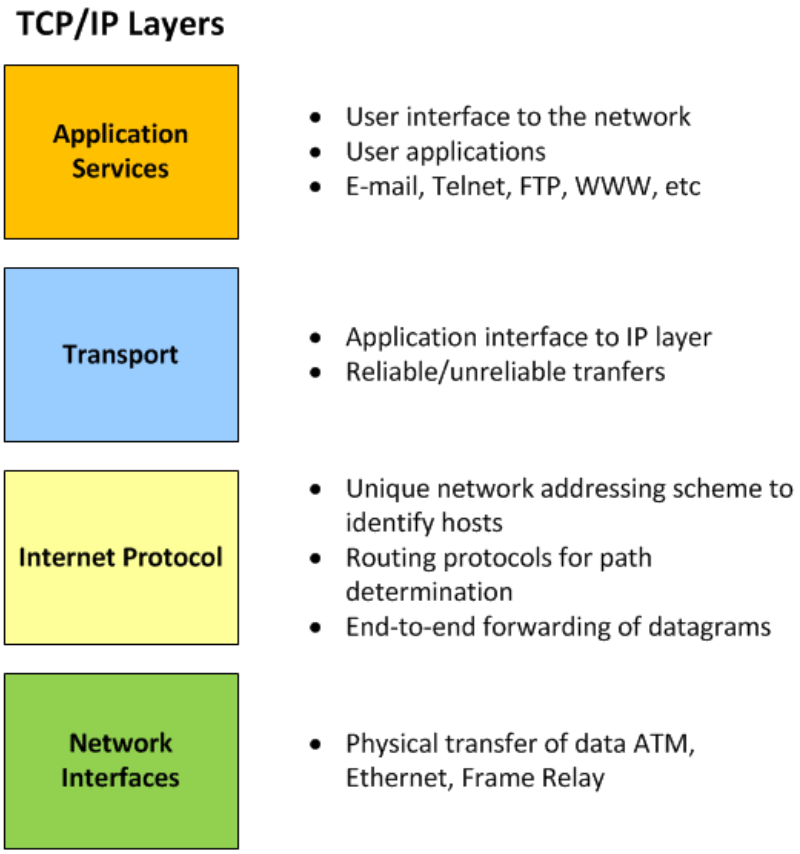

Figura 6 – Modelo TCP/IP

- Na primeira camada, *Network interfaces* conhecida usualmente por *Layer 2* (L2), representa a transmissão física dos pacotes e as redes locais com os protocolos usualmente envolvidos neste processo, ATM, *Ethernet* e *Frame Relay* [9].
- Na segunda camada, está o *Internet Protocol*, usualmente referida por *Layer 3* (L3). Nesta camada associada ao protocolo IP é realizado o encaminhamento de pacotes entre redes locais [9].
- A camada *Transport* está associada ao protocolo TCP que permite comunicações fiáveis. Esta pode usar ainda o protocolo *User Datagram Protocol* (UDP) para comunicações sem necessidade de fiabilidade. Ambos têm ainda a função de associar os pacotes às aplicações através de portos [9].
- Por fim, a camada de aplicação onde circula a informação que será transmitida *end-to-end* [9].

De acordo com o modelo apresentado será introduzido um cabeçalho por camada. Na Figura 7 pode-se observar o encapsulamento dos pacotes nas várias camadas do modelo TCP/IP.

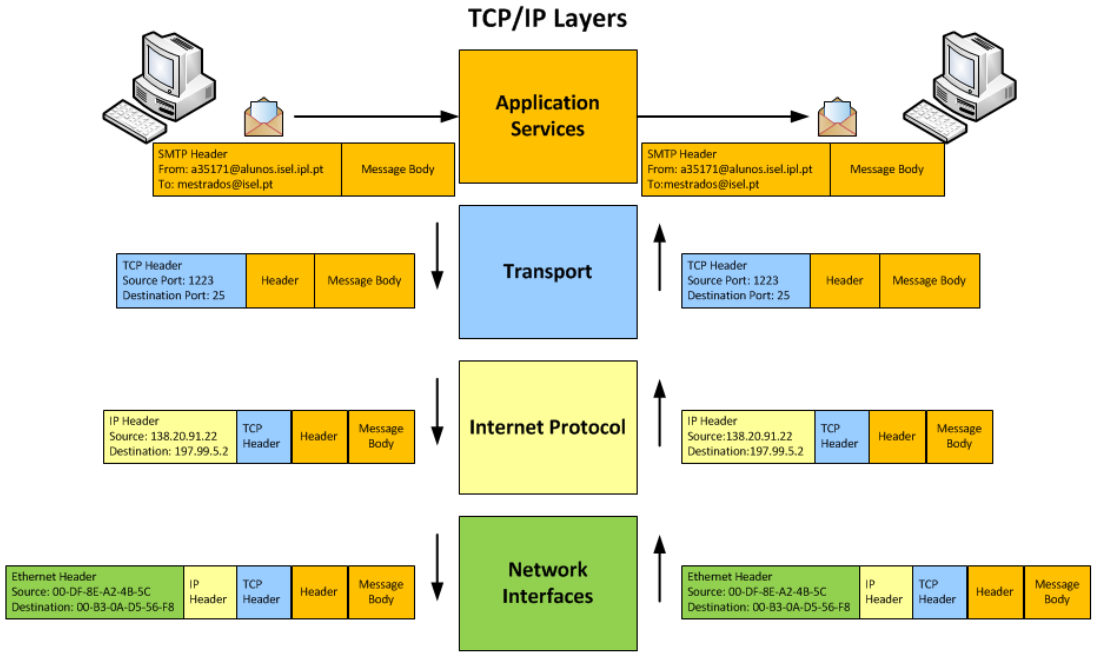

Figura 7 – Modelo TCP/IP com alusão ao encapsulamento das mensagens.

O encaminhamento de pacotes é necessário entre redes locais, sendo necessária a utilização de um ou mais *routers* para encaminharem o pacote até à rede de destino. O protocolo TCP tem como objetivo a comunicação *end-to-end*, logo o cabeçalho TCP só será processado no equipamento de destino.

1.3.1. *Layer 2* (L2)

As redes L2 podem ser classificadas em três tipos:

- ***Point-to-point***: Representam uma ligação direta entre dois equipamentos, estes podem comunicar entre si sem utilizar endereços de origem e destino. O *Point-to-point Protocol* (PPP) é um exemplo dos protocolos que podem ser utilizados nestas ligações [9].
- ***Circuit-based***: Criam circuitos virtuais entre os equipamentos numa rede. Os protocolos ATM e *Frame Relay* utilizam este mecanismo [9].
- ***Shared***: Numa rede partilhada os vários equipamentos estão ligados entre si através de *hubs* ou *swicthes*. O protocolo *Ethernet* é um exemplo dos protocolos utilizados neste tipo de rede [9].

1.3.1.1. *Ethernet Protocol*

Neste projeto foi utilizado apenas o protocolo *Ethernet*. Este tem como principais características:

- Utilização de redes multiponto, com a introdução de *hubs* ou *switches* [9].
- Utiliza os endereços *Media Access Control* (MAC) para identificar os equipamentos presentes na rede [9].

- Permite o envio de mensagens para destinos (endereço MAC) específicos ou de difusão (*multicast* e *broadcast*) na rede [9].
- A rede multiponto entre os equipamentos é também referida como *Local Area Network* (LAN) [9].
- Pode funcionar em *half-duplex* ou *full-duplex* [9].

Na Figura 8 pode-se observar de uma forma geral o formato da trama *Ethernet*. O campo *Length/Type* depende da estrutura/norma que está a ser usada. No caso do campo *Length* refere-se à norma IEEE 802.3 e este campo terá um valor inferior a 1536. Caso seja *Type* refere-se à norma *Ethernet* II, este campo terá um valor igual ou superior a 1536, e identifica qual é o protocolo da carga (*payload*), o próximo cabeçalho [9].

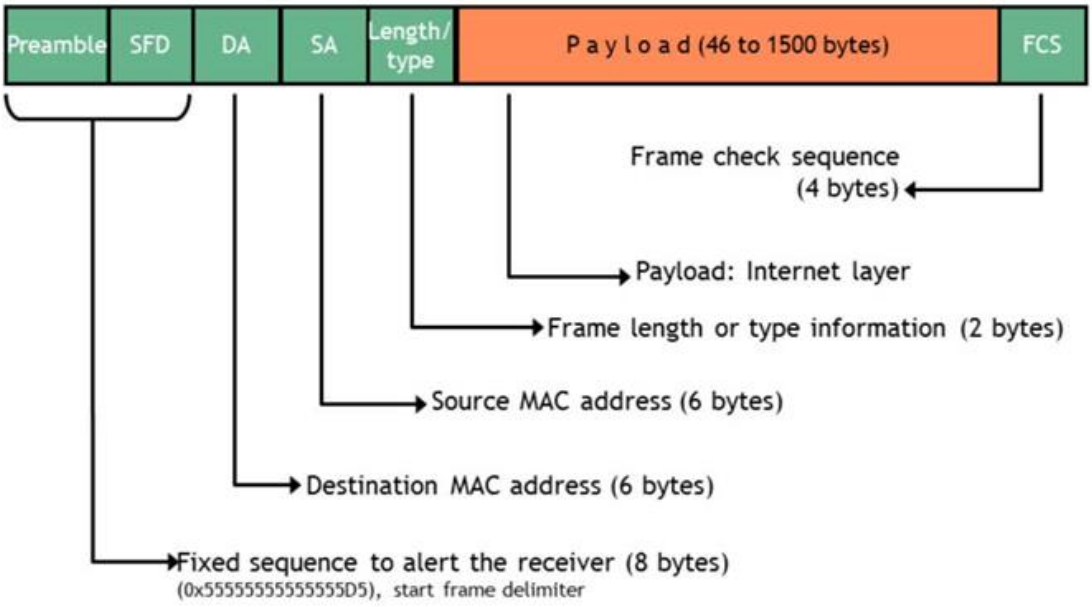

Figura 8 – Formato geral da trama *Ethernet*, retirado de K. Hundley [1].

1.3.2. *Internet Protocol* (L3)

O protocolo IP está associado à camada 3 do modelo TCP/IP e tem como função o encaminhamento de pacotes entre destinos, independentemente do protocolo L2 utilizado. Isto é possível através do endereçamento IP, que atribui um endereço único a cada equipamento. A atribuição de endereços IP é controlada pela autoridade global *Internet Assigned Number Authority* (IANA) [9]. O protocolo IP tem duas versões, IPv4 e IPv6, no entanto neste projeto foi utilizada apenas a versão 4 (IPv4) considerando-se que o objeto de estudo é independente deste e as conclusões obtidas serão aplicáveis indiferentemente ao transporte de dados de qualquer das gerações de Internet Protocol. Para fazer o encaminhamento entre redes locais é necessário um *router*, sendo este responsável por encaminhar os pacotes com base na informação do cabeçalho IP, como se pode observar na Figura 9.

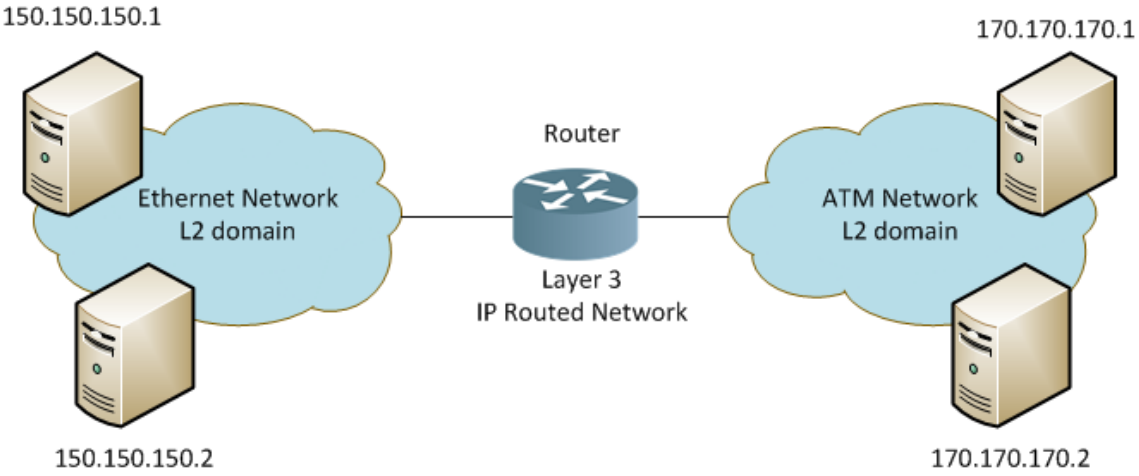

Figura 9 – Representação de diferentes domínios L2 ligados através de um *router*.

O IP é um protocolo *connectionless*, ou seja não garante que os pacotes sejam entregues e não notifica o equipamento de origem sobre os pacotes que foram perdidos. Esta função é remetida para a *transport layer* através do protocolo TCP.

1.4. *Open Short Path First* (OSPF)

Para realizar o encaminhamento de pacotes, o *router* tem de conhecer a rede de destino e por onde encaminhar os pacotes. Existem várias formas de o *router* adquirir esse conhecimento, seja de forma manual ou dinâmica. Neste projeto foi apenas utilizado como IGP o protocolo OSPF, o qual é utilizado na rede MPLS do IPL.

O protocolo OSPF é do tipo *Link-State*, ou seja controla as mudanças de estado das ligações entre os *routers* para manter o mapa da topologia atualizado e consequentemente a tabela de encaminhamento [9] [10]. Assim estes utilizam três bases de dados comuns entre todos:

- **Topologia** – (*link-state database*): Esta base de dados contém os endereços IP, máscaras, etc, sobre todas as ligações ativas de cada *router* OSPF [9].
- **Vizinhos** – (*adjacency database*): Base de dados com informação sobre os *routers* com quem partilha ligações, ou seja *routers* vizinhos [9].
- **Tabela de encaminhamento** – (*forwarding database*): Base de dados com a tabela de encaminhamento construída com base na partilha de informação entre os *routers* OSPF [9].

A transmissão da informação necessária para construir estas bases de dados é realizada através da troca de pacotes *Link-state Advertisements* (LSA). Esta troca é realizada até que todos os *routers* na mesma área tenham bases de dados iguais, sendo depois atualizada periodicamente ou em caso de alterações. Após a convergência das bases dados, cada *router* calcula individualmente o melhor caminho para os vários destinos possíveis através do algoritmo *Shortest path first* (SPF) [9] [10]. Na Figura 10 está representado este processo.

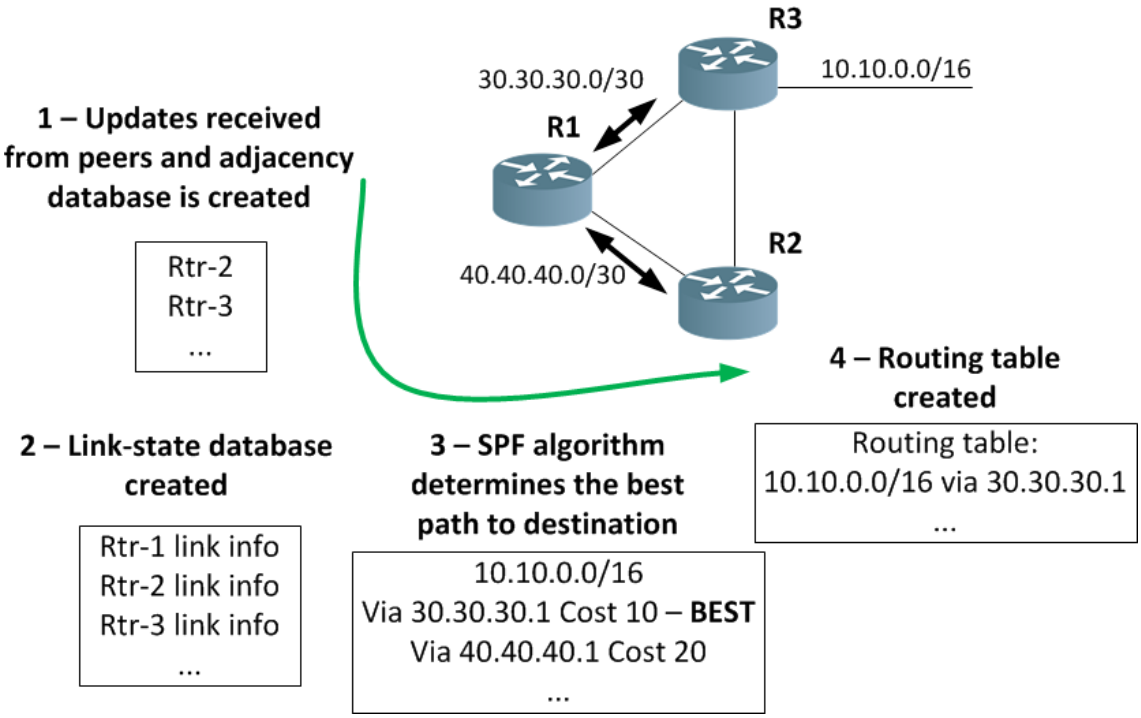

Figura 10 – Processo de criação da tabela de encaminhamento através do OSPF.

Para calcular o melhor caminho para cada rede de destino é necessário atribuir um custo a cada ligação. Este é por omissão calculado de acordo com a seguinte fórmula, utilizando um valor de referência que deve ser comum a todo o domínio OSPF e que pode variar de fabricante para fabricante, sendo na Alcatel-Lucent (Nokia) utilizado o seguinte valor - *bandwidth reference* = 100 000 000 kb/s:

$$link\ cost = bandwidth\ reference \div link\ bandwidth$$

Nota: Normalmente referenciado como múltiplo de kbit/s.

Assim cada ligação terá um custo de ligação (*link cost*) de acordo com a sua largura de banda e o caminho escolhido para cada destino será aquele que menor valor apresentar na soma do custo de todas as ligações do trajeto [9]. O valor de referência utilizado neste cálculo pode ser alterado, no entanto caso se mantenha no seguinte exemplo estão representados alguns custos:

- **Ligação de 10 Mb/s:** custo de 10 000
- **Ligação de 100 Mb/s:** custo de 1000
- **Ligação de 1 Gb/s:** custo de 100
- **Ligação de 10 Gb/s:** custo de 10

Após o cálculo e criação da tabela de encaminhamento, caso existam alterações na topologia será realizado um novo cálculo. No caso de existir uma falha numa ligação intermédia, ou seja uma ligação entre dois *switches*, esta só será detetada quando o *dead interval* for atingido. O *dead interval* tem um valor de 40 segundos e consiste na perda de quatro menagens *Hello*, logo se o *router* não receber quatro mensagens *Hello* consecutivas a ligação considera-se quebrada. As mensagens *Hello* são utilizadas para

descobrir os *routers* vizinhos e para manter as adjacências criadas, sendo enviados por omissão de 10 em 10 segundos [9].

1.4.1. OSPF com múltiplas áreas

Uma rede OSPF (domínio OSPF) pode ser divida em várias áreas, esta divisão permite diminuir o tamanho das bases de dados dos *routers* e minimizar o processamento nos *routers* devido a alterações na topologia de uma área [9] [10]. No entanto a divisão deve obedecer às seguintes regras:

- ***Backbone area*:** Esta é a área de referência, logo a sua existência é obrigatória. Está diretamente ligada a todas as outras áreas [9] [10].
- ***Non-backbone area*:** Estas têm de estar diretamente ligadas à área *backbone* e não podem ter ligações entre si - estrutura em árvore de dois níveis [9] [10].

Na seguinte Figura 11 está um exemplo de uma rede OSPF com várias áreas.

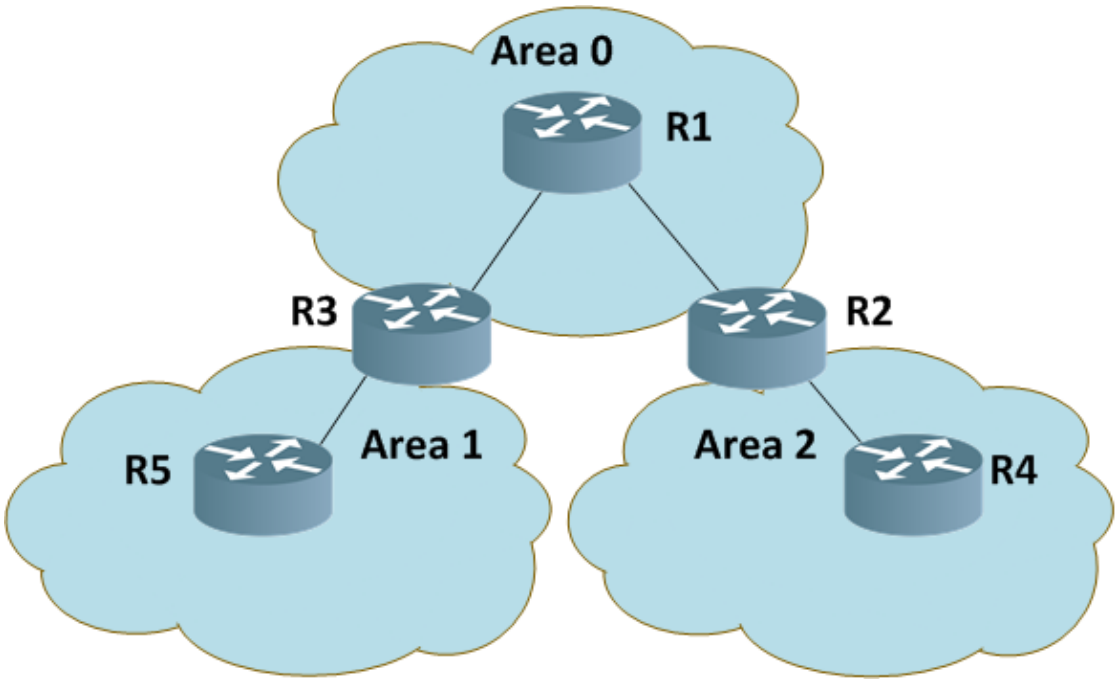

Figura 11 – Exemplo de uma rede OSPF com várias áreas.

Idealmente as redes MPLS-TE devem ser utilizadas com o OSPF *single area*, devido à limitação da propagação dos Opaque LSA entre as áreas. No entanto, a utilização de MPLS-TE com múltiplas áreas OSPF é possível com a solução LDP-over-RSVP, que estabelece túneis RSVP-TE entre os routers da mesma área e utiliza túneis LDP sobre os túneis RSVP-TE para atingir os routers das outras áreas OSPF. Neste projeto, de acordo com a rede MPLS do IPL, será utilizada uma topologia de OSPF *single area*. Desta forma, este capítulo e a solução LDP-over-RSVP não serão desenvolvidos.

1.4.2. OSPF-TE

As extensões de engenharia de tráfego foram feitas apenas para os protocolos OSPF e ISIS. Usualmente referidos como OSPF-TE e ISIS-TE, esta extensão têm como objetivo a

partilha de informação adicional referente à engenharia de tráfego utilizada no MPLS. No OSPF esta informação é transportada em Opaque LSAs ou LSAs do tipo 10 [9] [11]. Para que o OSPF suporte a opção TE todos os *routers* Alcatel-Lucent (Nokia) pertencentes à rede MPLS têm de ter a seguinte configuração:

```
configure router ospf traffic-engineering
```

Assim é criada em cada um dos *routers* OSPF a *Traffic Engineering Database* (TED), onde será guardada toda a informação transmitida nos Opaque LSAs. Estes são incluídos no *database summary* e enviados apenas aos vizinhos com o *traffic-engineering* ativo. Os Opaque LSA contêm apenas a informação relevante para o MPLS-TE, logo apenas as interfaces utilizadas pelo RSVP-TE serão referenciadas nestas mensagens [9] [11]. Na Figura 12 pode-se observar o formato do Opaque LSA.

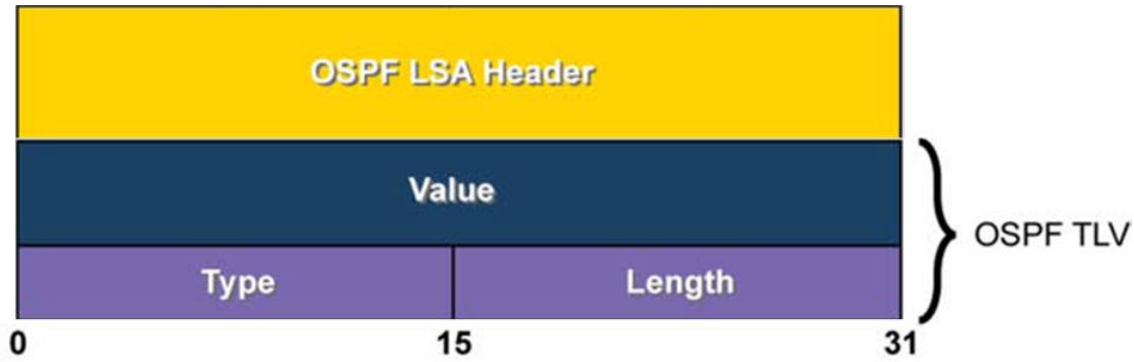

Figura 12 – Formato do Opaque LSA.

O Opaque LSA utiliza o cabeçalho padrão dos LSA, sendo depois preenchido com um ou mais *Type/Length/Value* (TLV).

- ***Type*:** Existem dois tipos de informação, *Router Address* TLV e *Link* TLV. O *Router Address* TLV transporta informação sobre o *router* (*router*-ID). Por outro lado, no *Link* TLV são anunciadas as informações sobre os vários *links* sendo este subdivido em vários sub-TLVs [9] [11].
- ***Length*:** Este contém o valor do tamanho do campo *Value* em octetos [9] [11].
- ***Value*:** Este campo é preenchido com as informações de *traffic-engineering* organizadas em sub-TLVs [9] [11].

Existem 10 tipos de sub-TLVs transportados no *Link* TLV [9] [11]:

- ***Link type* sub-TLV:** Define qual é o tipo da ligação, 1 para ponto-a-ponto e 2 para *broadcast*.
- ***Link ID* sub-TLV:** Contém o *router* ID do vizinho, no caso duma ligação *broadcast* será utilizado o endereço IP da interface do *Designated Router* (DR).
- ***Local interface* IP *address* sub-TLV:** Define o endereço IP da interface correspondente à ligação local.
- ***Remote interface* IP *address* sub-TLV:** Define o endereço IP da interface do vizinho correspondente à ligação. No caso de uma ligação *broadcast* este é preenchido com 0.0.0.0.

- ***Traffic Engineering metric* sub-TLV:** Por omissão é igual à utilizada no *Interior Gateway Protocol* (IGP), mas pode ser alterada manualmente.
- **Maximum bandwidth sub-TLV:** Especifica a capacidade de largura de banda à saída do *router* para a ligação.
- ***Maximum reservable bandwidth* sub-TLV:** Define a percentagem de largura de banda que pode ser reservada na ligação, que por omissão é 100%. De notar que esta percentagem pode ser menor ou maior que a verdadeira capacidade da ligação, sendo possível fazer *over-booking* e *under-booking*.
- ***Unreserved bandwidth* sub-TLV:** Especifica a quantidade de largura de banda reservável à saída do *router*. Contém ainda 8 prioridades diferentes ao qual podem ser atribuídas reservas. Sempre que um LSP realizar uma reserva ou libertar a largura de banda este valor será atualizado.
- ***Administrative group* sub-TLV:** Este campo contém apenas 32 bits, cada bit representa um grupo e cada ligação pode pertencer a um ou mais grupos. A cada grupo é atribuído um nome e um ID de 0-31, por exemplo "GREEN 3". O número 3, no exemplo anterior, indica que o bit que irá representar o grupo, ou seja neste caso o bit nº 3, sendo em decimal equivalente ao valor 8.
- ***Shared Risk Link Group* (SRLG) sub-TLV:** Este campo tem um tamanho variável, que depende do número de grupos SRLG atribuídos à ligação. Cada grupo tem um valor decimal atribuído que é representado por 32 bits.

Na Figura 13 pode-se observar uma Opaque LSA com o valor de 20.000 kb/s no *Unreserved bandwidth* sub-TLV, ou seja estas ligações têm apenas 20 Mb/s disponíveis para futuras reservas.

```
------------------------------------------------------------------------------
Opaque LSA
------------------------------------------------------------------------------
Area Id          : 0.0.0.0             Adv Router Id    : 192.168.0.5
Link State Id    : 1.0.0.3             LSA Type         : Area Opaque
Sequence No      : 0x80000013          Checksum         : 0xcf2e
Age              : 1230                Length           : 124
Options          :  E
Advertisement    :
     LINK INFO TLV  (0002) Len 100 :
       Sub-TLV: 1     Len: 1     LINK_TYPE     : 1
       Sub-TLV: 2     Len: 4     LINK_ID       : 192.168.0.6
       Sub-TLV: 3     Len: 4     LOC_IP_ADDR   : 10.5.6.5
       Sub-TLV: 4     Len: 4     REM_IP_ADDR   : 10.5.6.6
       Sub-TLV: 5     Len: 4     TE_METRIC     : 100
       Sub-TLV: 6     Len: 4     MAX_BDWTH     : 100000 Kbps
       Sub-TLV: 7     Len: 4     RSRVBL_BDWTH  : 100000 Kbps
       Sub-TLV: 8     Len: 32    UNRSRVD_CLS0  :
         P0:   20000 Kbps P1:   20000 Kbps P2:   20000 Kbps P3:   20000 Kbps
         P4:   20000 Kbps P5:   20000 Kbps P6:   20000 Kbps P7:   20000 Kbps
       Sub-TLV: 9     Len: 4     ADMIN_GROUP   : 0 None
```

Figura 13 – Exemplo de um Opaque LSA com reserva de largura de banda atribuída.

Na Figura 14 pode-se observar um Opaque LSA com o *admin-group* "3" atribuído, ou seja esta ligação pertence ao grupo 3.

```
------------------------------------------------------------------------------
Opaque LSA
------------------------------------------------------------------------------
Area Id          : 0.0.0.0              Adv Router Id    : 192.168.0.1
Link State Id    : 1.0.0.2              LSA Type         : Area Opaque
Sequence No      : 0x80000003           Checksum         : 0x348b
Age              : 169                  Length           : 124
Options          :  E
Advertisement    :
     LINK INFO TLV  (0002) Len 100 :
       Sub-TLV: 1     Len: 1     LINK_TYPE    : 1
       Sub-TLV: 2     Len: 4     LINK_ID      : 192.168.0.2
       Sub-TLV: 3     Len: 4     LOC_IP_ADDR  : 10.1.2.1
       Sub-TLV: 4     Len: 4     REM_IP_ADDR  : 10.1.2.2
       Sub-TLV: 5     Len: 4     TE_METRIC    : 100
       Sub-TLV: 6     Len: 4     MAX_BDWTH    : 100000 Kbps
       Sub-TLV: 7     Len: 4     RSRVBL_BDWTH : 100000 Kbps
       Sub-TLV: 8     Len: 32    UNRSRVD_CLS0 :
         P0:  100000 Kbps P1:  100000 Kbps P2:  100000 Kbps P3:  100000 Kbps
         P4:  100000 Kbps P5:  100000 Kbps P6:  100000 Kbps P7:  100000 Kbps
       Sub-TLV: 9     Len: 4     ADMIN_GROUP  : 00000008 (8)
```

Figura 14 – Exemplo de um Opaque LSA com *admin-groups* atribuídos.

Os Opaque LSA serão enviados no caso de mudança de estado das ligações, alterações das restrições, mudanças na largura de banda (LB) reservada em cada ligação e ainda quando o tempo de vida do LSA acabar [9] [11].

No próximo capítulo será abordado o protocolo MPLS onde os TLV são necessários para utilizar as regras de *traffic-engineering*.

1.5. *Multiprotocol Label Switching* (MPLS)

O MPLS permite que o tráfego seja comutado com base numa *label* que é transportada no cabeçalho MPLS do pacote. Isto simplifica e otimiza o processo de encaminhamento de pacotes diminuindo o tempo necessário para encaminhar os pacotes. O pacote irá apenas consultar uma tabela de *labels* para verificar qual é a *label* seguinte, em vez de consultar a tabela de encaminhamento IP para escolher o *next-hop* com melhor correspondência.

Nota: Com o avanço tecnológico do *hardware*, esta diferença deixou progressivamente de ser significativa [9]. Os resultados apresentados por Kaur *et al.* [12], revelam uma latência inferior a 1 ms entre o encaminhamento de pacotes numa rede MPLS e numa convencional rede IP.
Assim sendo a grande vantagem da utilização de MPLS é a possibilidade de utilizar engenharia de tráfego e serviços L2/L3 VPN. Os protocolos de encaminhamento não conseguem utilizar todos os recursos disponíveis na rede, devido à limitação dos mecanismos para a seleção do melhor caminho. O MPLS permite balancear a rede, melhorando o aproveitamento de todos os recursos da rede e garante ainda uma alta disponibilidade da rede ao oferecer vários mecanismos de proteção contra falhas na rede, como por exemplo o *Fast Reroute* que permite a recuperação em menos de 50 ms [9] [11] [13].

1.5.1. Fundamentos do MPLS

As redes MPLS têm a sua própria terminologia, como se pode verificar na Figura 15.

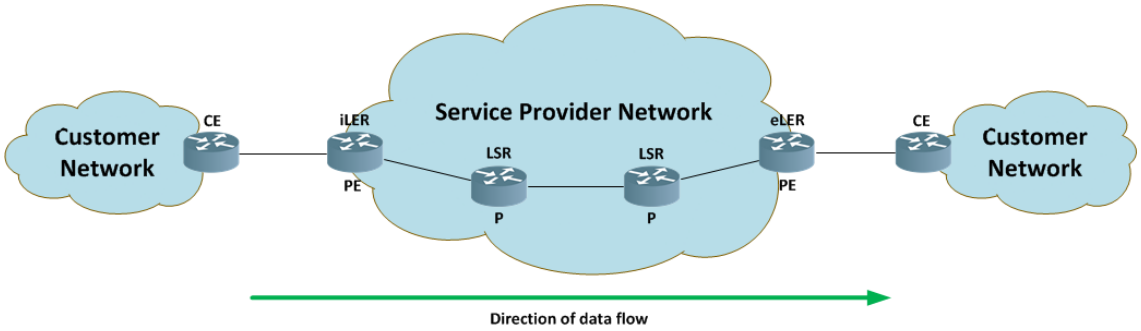

Figura 15 – Representação duma rede MPLS com a terminologia adequada.

Assim os *routers* de acesso à rede MPLS podem ser designados por [11]:

- **PE:** *Provider Edge Router*
- **iLER:** *Ingress Label Edge Router*
- **eLER:** *Egress Label Edge Router*

Os equipamentos no interior da rede MPLS podem ser definidos por [11]:

- **P:** *Provider (Core) Router*
- **LSR:** *Label Switch Router*

As definições de cada equipamento estão diretamente relacionadas com as suas funções ao nível MPLS. Na Figura 16 pode-se verificar que um equipamento PE/iLER coloca a *label* MPLS na trama, os equipamentos P/LSR trocam a *label* e por fim um equipamento PE/eLER retira a *label* da trama [11].

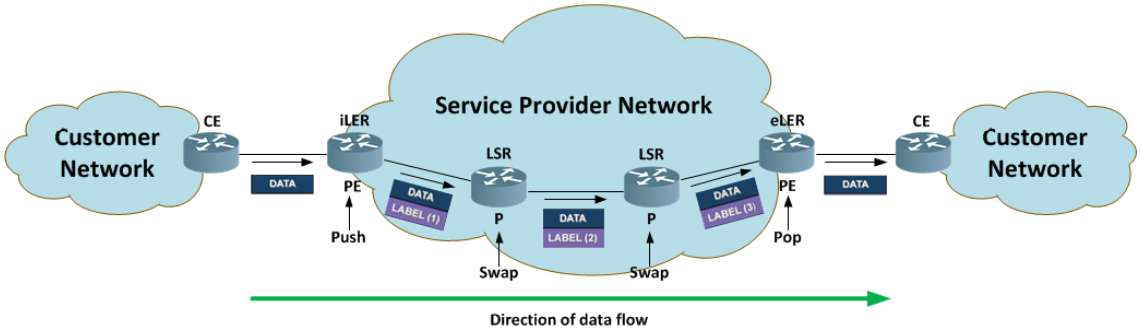

Figura 16 – Representação da mudança de *labels* numa rede MPLS.

O conjunto de *labels* e ações realizadas nos *routers* MPLS para encaminhar as tramas entre *routers* PE pode ser definido como *Label Switched Path* (LSP) [11]. Os LSP são considerados túneis unidirecionais com início no iLER e fim no eLER, como se pode observar na Figura 17.

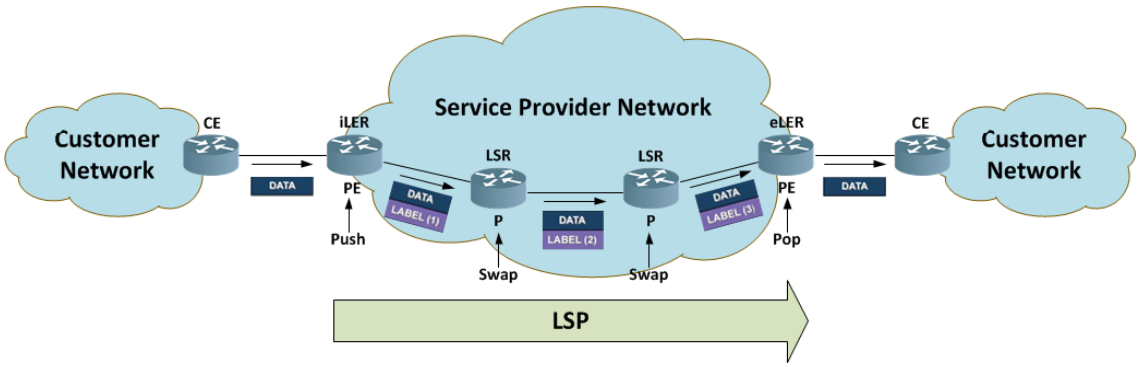

Figura 17 – Representação de um túnel LSP numa rede MPLS.

Desta forma, apenas no iLER é realizada uma verificação na *Label Information Base* (LIB), que atua ao nível do *control plane*, para de acordo com o destino final do pacote definir o próximo LSR e a *label* a utilizar. A LIB é preenchida com a informação recebida pelos outros *routers* através dos protocolos de distribuição *Label Distribution Protocol* (LDP) e/ou *Resource Reservation Protocol with Traffic Engineering* (RSVP-TE). Após o preenchimento desta serão escolhidas as *labels* a utilizar de acordo com o LSP que estiver ativo. As *labels* escolhidas serão transferidas para a *Label Forwarding Information Base* (LFIB) que atua ao nível do *data plane*. Quando uma trama é recebida pelo iLER este verifica a LFIB e comuta a trama para o seguinte LSR com *label* definida na LFIB. Esta *label* será trocada ao longo do caminho até chegar ao eLER, onde será removida [9] [11].

1.5.2. Protocolo MPLS

O protocolo MPLS é considerado um protocolo de nível 2.5, pois em termos lógicos encontra-se entre os níveis 2 e 3 do modelo TCP/IP, como se pode ver na Figura 18.

Figura 18 – Representação do modelo TCP/IP com alusão ao protocolo MPLS.

O cabeçalho MPLS é composto pelos campos *Label*, EXP, S e TTL, como se pode verificar na Figura 19.

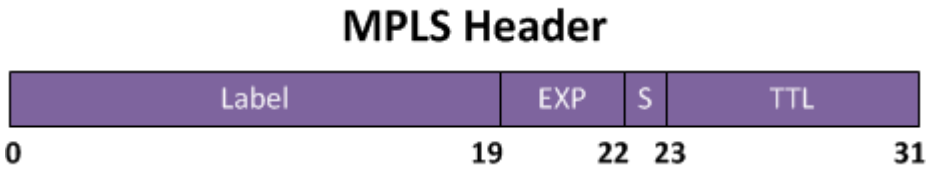

Figura 19 – Cabeçalho do protocolo MPLS.

- ***Label*:** Campo com 20 bits que contém o valor da *label* [9].
- **EXP:** Campo com 3 bits, utilizado para marcação de QoS nos pacotes [9].
- **S:** Utilizado para indicar se é a última *label* do MPLS *stack* [9].
- **TTL:** *Time-to-Live* para pacotes MPLS, apenas descontado em MPLS *hops* [9].

Um *stack* MPLS é composto por várias *labels*, tendo no mínimo uma *label* para o túnel MPLS (*Outer label*, *Top label* ou *label* de transporte) e outra para o serviço a que este está associado (*Inner label*, *Bottom label* ou *label* de serviço). Na Figura 20 pode-se observar que diferentes serviços podem utilizar o mesmo túnel MPLS, sendo que a *Inner label* representa os serviços e por isso, para um mesmo serviço, será a mesma entre iLER e eLER. Já a *Outer label* é utilizada para a comutação no túnel MPLS e por isso é trocada em cada *hop* [9].

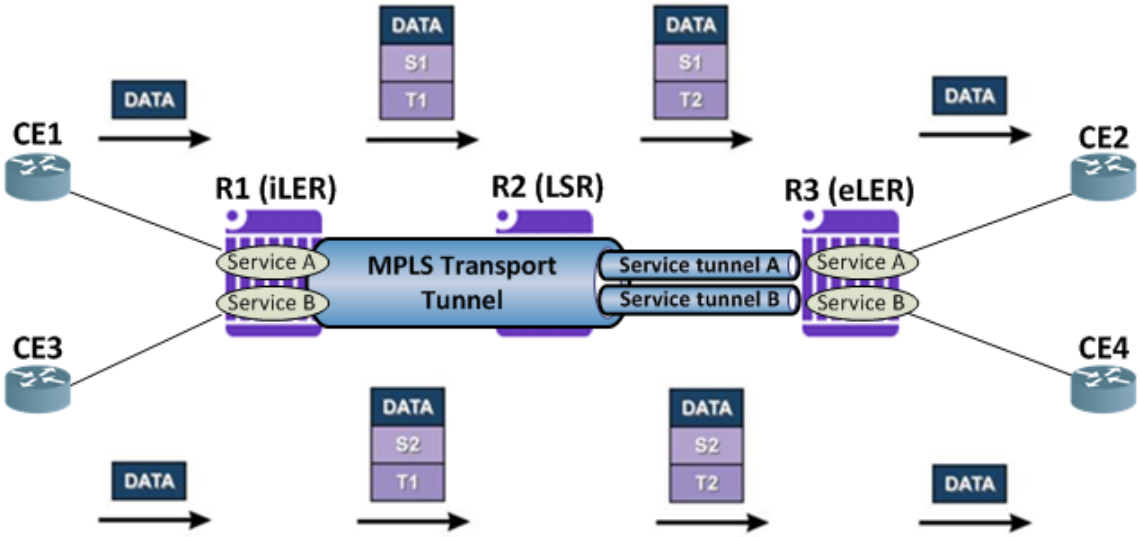

Figura 20 – Representação das *labels* MPLS utilizadas entre iLER e eLER.

Os serviços associados aos túneis MPLS podem ser L2 VPN ou L3 VPN. No caso de um serviço L2 VPN será transmitida a trama com os cabeçalhos L2 e L3 originais através da rede MPLS, como se pode observar na Figura 21.

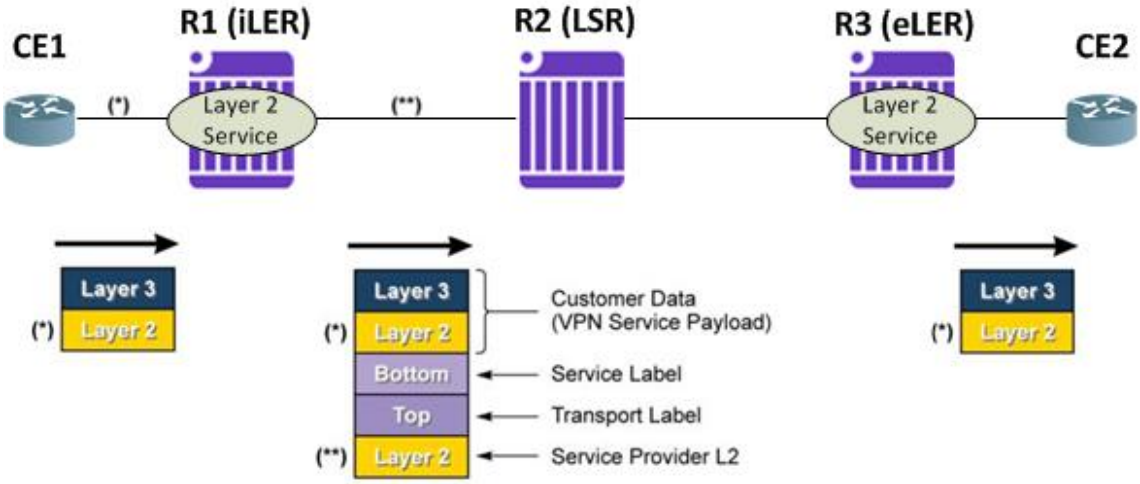

Figura 21 – Representação dos cabeçalhos envolvidos na transmissão de pacotes de um serviço L2 VPN.

No caso de um serviço L3 VPN apenas o cabeçalho L3 é transportado, como se pode observar na Figura 22.

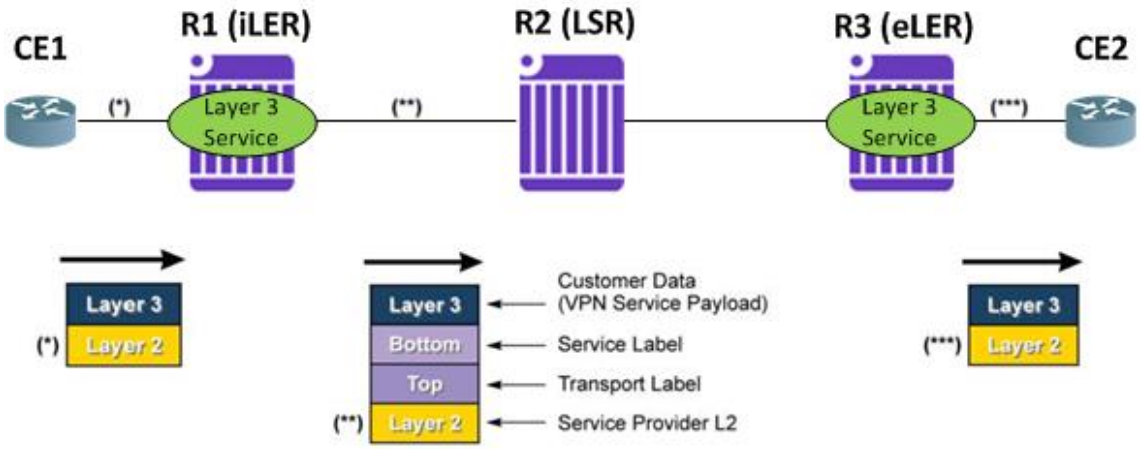

Figura 22 – Representação dos cabeçalhos envolvidos na transmissão de pacotes de um serviço L3 VPN.

Estes serviços permitem que o tamanho da rede MPLS seja indiferente para o cliente. Num serviço L2 VPN o cabeçalho IP mantém-se original sem alterações no campo TTL, apesar de passar por vários *routers* como se pode verificar na Figura 23.

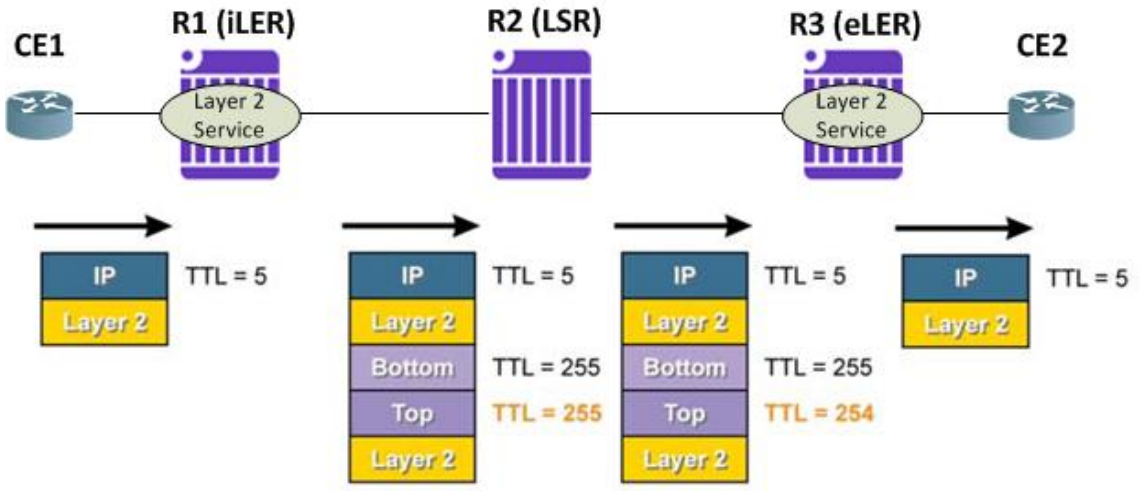

Figura 23 – Representação do TTL dos pacotes ao passar num serviço L2 VPN.

Já no caso de um serviço L3 VPN o campo TTL do cabeçalho IP será decrementado duas vezes, uma no iLER e outra no eLER como se pode observar na Figura 24. Este comportamento é adotado por omissão nos equipamentos Alcatel-Lucent (Nokia), no entanto este pode ser configurado para que nos serviços L3 VPN o valor do campo TTL seja decrementado de acordo com o número de *routers* do caminho do LSP.

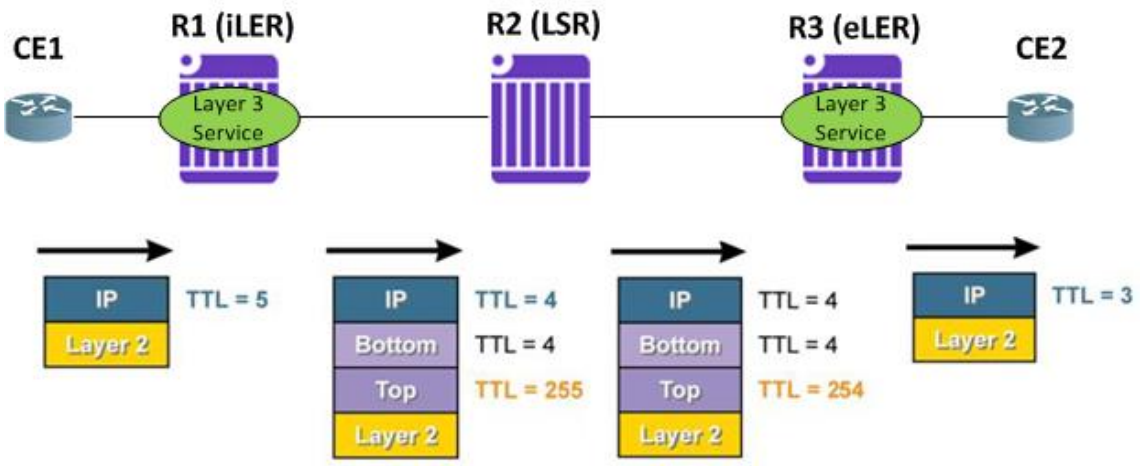

Figura 24 – Representação do TTL dos pacotes ao passar num serviço L3.

O protocolo MPLS tal como o IP necessita de outros protocolos especializados na distribuição da informação necessária para que os *routers* possam comutar as tramas. Nos próximos capítulos serão abordados os protocolos LDP e RSVP que distribuem a informação MPLS pelos vários intervenientes.

1.5.3. *Label Distribution Protocol* (LDP)

O LDP é um protocolo de distribuição de *labels* MPLS. Para realizar a troca de *labels* é necessário que os *routers* estabeleçam uma sessão LDP. Desta forma a troca de *labels* é independente do protocolo de encaminhamento que for utilizado.

Existem dois tipos de sessão LDP:

- ***Link* LDP (LDP):** Utilizado para trocar as *labels* que permitem estabelecer os LSP [9] [11].
- ***Targeted* LDP (T-LDP):** Utilizado para trocar as *labels* de serviço que permitem estabelecer serviços VPN [9] [11].

1.5.3.1. *Link* LDP

Todos os *routers* LDP estabelecem sessões de *Link* LDP com os seus vizinhos LDP diretamente ligados, como se pode verificar na Figura 25.

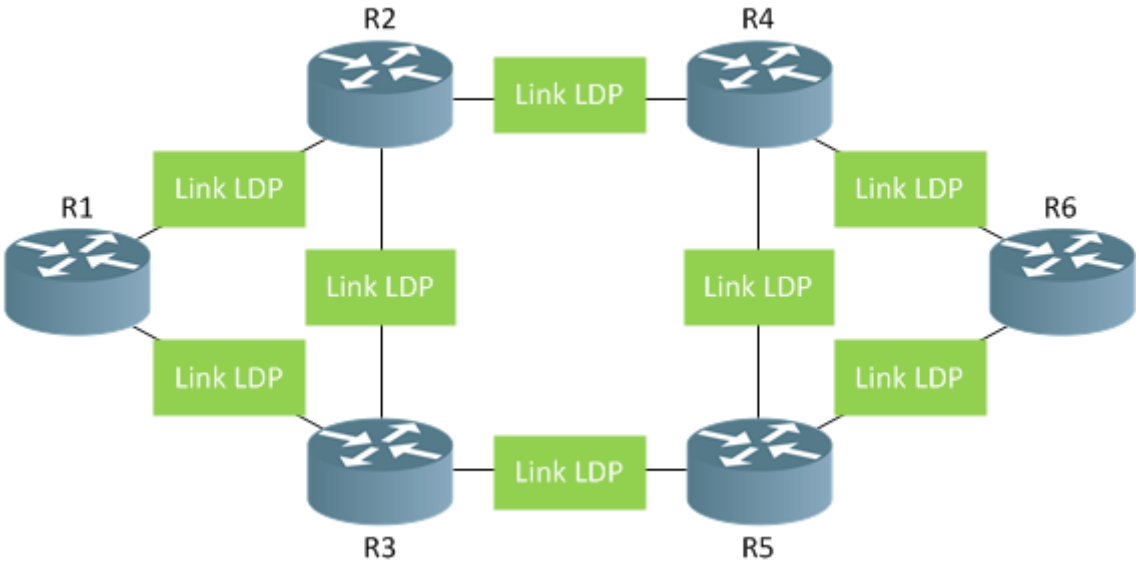

Figura 25 – Exemplo das sessões *Link* LDP estabelecidas numa rede MPLS-LDP.

Para estabelecer e manter uma sessão *Link* LDP são realizados três processos:

- **Deteção de vizinhos:** A deteção é feita através de mensagens LDP *Hello* enviadas para o endereço *multicast* 224.0.0.2 e com porto UDP 646. Após a deteção de vizinhos a sessão de adjacência LDP fica estabelecida e são enviadas mensagens LDP *Hello* periodicamente para manter a adjacência ativa [9].
- **Estabelecer e manter a sessão LDP:** Após a sessão de adjacência ser estabelecida é necessário estabelecer uma sessão LDP. Esta é estabelecida através de uma ligação TCP no porto 646, para o *Transport address* do vizinho que é igual ao endereço IP da interface *System* (*routers* Alcatel-Lucent) e que foi recebido nas mensagens de LDP *Hello*. Para que a ligação TCP seja estabelecida o endereço IP de destino tem de constar na tabela de encaminhamento. Após o estabelecimento da sessão esta é mantida através de mensagens *Keepalive* [9].
- **Distribuição e gestão de *labels*:** Após o estabelecimento da sessão são iniciadas as trocas de *labels*. Cada *router* gera uma *label* LDP para o endereço IP da sua interface *System* e envia aos seus vizinhos. As *labels* recebidas através de um vizinho são guardadas na LIB, por sua vez o *router* gera uma nova *label* para o destino recebido e anuncia a *label* para o novo destino aos restantes vizinhos. No final deste processo os *routers* MPLS terão uma ou mais *labels* para atingir todos os *routers* MPLS [9].

Os túneis MPLS são estabelecidos entre *routers* MPLS e transportam apenas o tráfego dos serviços VPN, logo estes apenas precisam adquirir *labels* para comutar o tráfego entre *routers* MPLS. Assim, para atingir os outros *routers* MPLS é consultada a tabela de encaminhamento IP para determinar o *next-hop*, a LFIB será depois preenchida com a *label* recebida do *next-hop* definido [9]. Na Figura 26 pode-se observar um exemplo de uma LFIB.

```
*A:SARF-1(CORE)# show router ldp bindings active

===============================================================================
Legend:  (S) - Static
===============================================================================
LDP Prefix Bindings (Active)
===============================================================================
Prefix                  Op   IngLbl    EgrLbl    EgrIntf/LspId  EgrNextHop
-------------------------------------------------------------------------------
192.168.0.1/32          Pop  131071      --        --             --
192.168.0.2/32          Push   --      131071    1/2/5          10.1.2.2
192.168.0.2/32          Swap 131068    131071    1/2/5          10.1.2.2
192.168.0.3/32          Push   --      131057    1/2/5          10.1.2.2
192.168.0.3/32          Swap 131057    131057    1/2/5          10.1.2.2
192.168.0.5/32          Push   --      131068    1/2/6          10.1.6.6
192.168.0.5/32          Swap 131067    131068    1/2/6          10.1.6.6
192.168.0.6/32          Push   --      131071    1/2/6          10.1.6.6
192.168.0.6/32          Swap 131069    131071    1/2/6          10.1.6.6
192.168.0.11/32         Push   --      131063    1/2/5          10.1.2.2
192.168.0.11/32         Swap 131063    131063    1/2/5          10.1.2.2
192.168.0.12/32         Push   --      131058    1/2/5          10.1.2.2
192.168.0.12/32         Swap 131058    131058    1/2/5          10.1.2.2
192.168.0.13/32         Push   --      131056    1/2/5          10.1.2.2
192.168.0.13/32         Swap 131056    131056    1/2/5          10.1.2.2
-------------------------------------------------------------------------------
No. of Prefix Bindings: 15
===============================================================================
```

Figura 26 – Exemplo de LFIB.

Desta forma, o LDP depende do protocolo de IGP para definir as suas rotas e para definir um novo caminho no caso de uma falha de rede.

1.5.3.2. *Targeted* LDP (T-LDP)

O T-LDP é utilizado para sinalizar e estabelecer os túneis de serviços L2 VPN. Os túneis de serviço utilizam *labels* de serviço e são transportados dentro dos túneis de transporte (LSP). As *labels* de serviços servem para que os *routers* PE possam identificar o serviço a que o tráfego pertence. O processo para estabelecer e manter uma sessão T-LDP é semelhante ao *Link* LDP, tendo como principal diferença o facto de as mensagens trocadas serem todas em *unicast* e direcionadas apenas a *routers* PE [9] [11].

1.5.4. *Resource Reservation Protocol with Traffic Engineering* (RSVP-TE)

O RSVP-TE ao contrário do LDP, apenas estabelece sessões RSVP quando estas são necessárias. Todos os LSP são configurados individualmente no *router* iLER, para cada LSP é enviada uma mensagem RSVP *PATH* para o *router* eLER. Na ausência de regras de TE, esta mensagem é em encaminhada em cada *hop* (LSR) de acordo com o melhor caminho IGP para o endereço IP da interface *System* do *router* eLER [9] [11]. Na Figura 27 está um exemplo deste processo.

Figura 27 – Exemplo da mensagem RSVP *PATH* enviada ao *router* de destino.

A mensagem RSVP *RESV* é a resposta ao pedido RSVP *PATH*, esta é enviada pelo mesmo caminho. Cada *hop* envia nesta mensagem a *label* que deve ser utilizada com o LSP que está a ser estabelecido. O LSP fica ativo assim que o *router* iLER receber a mensagem RSVP *RESV* com a *label* que deve utilizar [9] [11], como se pode observar na Figura 28.

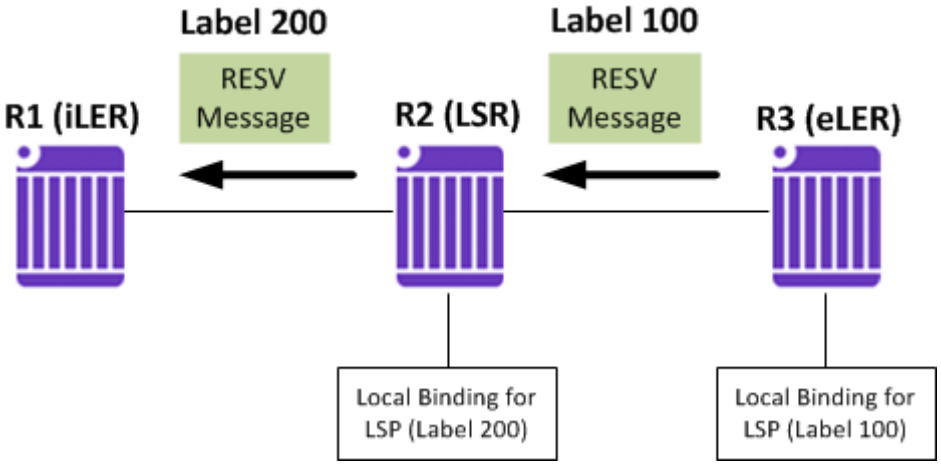

Figura 28 – Exemplo da mensagem RSVP *RESV* enviada para o *router* iLER.

Os LSP ativos podem ser afetados por falhas de rede. Caso isso aconteça os *routers* que detetarem a falha enviam mensagens RSVP *RESV TEAR* na direção *upstream* e RSVP *PATH TEAR* na direção *downstream*. A sessão RSVP é desativada em todos os *hops* e as *labels* retiradas da LFIB [9] [11]. Na Figura 29 está um exemplo deste processo.

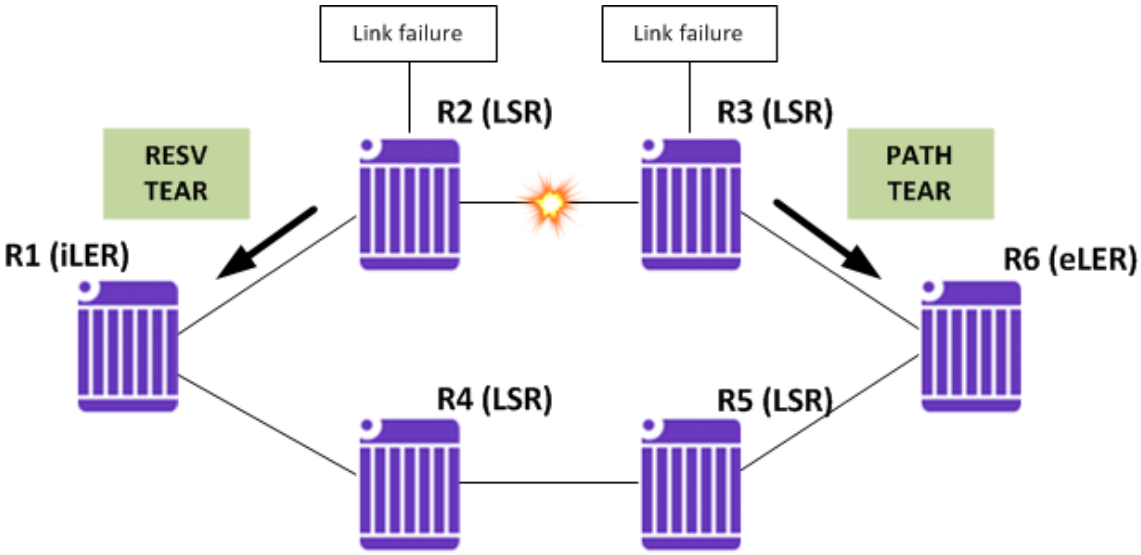

Figura 29 – Exemplo da mensagem de RSVP *RESV TEAR* enviada na direção *upstream*, e a mensagem *PATH TEAR* na direção *downstream*.

As falhas em ligações remotas são detetadas através de mensagens RSVP *Hello* que são utilizadas para manter as sessões RSVP ativas na ligação. Estas são enviadas por omissão em períodos de 3 segundos e consideram a ligação perdida após a perda de três mensagens consecutivas, demorando assim 9 segundos a detetar uma falha. Se a ligação for considerada perdida todos os LSP estabelecidos através da ligação são desativados. O período das mensagens RSVP *Hello* pode ser diminuído até 1 segundo, demorando assim 3 segundos a detetar uma falha [9] [11].

O RSVP-TE acrescentou a possibilidade de controlar os caminhos estabelecidos pelos LSP através da aplicação de restrições no cálculo do caminho do LSP e ainda novos métodos de resiliência que permitiram melhorar a resposta a falhas de rede. O RSVP-TE disponibiliza as seguintes restrições para o cálculo dos caminhos dos LSP [9] [11]:

- *Explicit Route* (*Strict and Loose hops*)
- TE-*Metric*
- *Hop Limit*
- *Administrative Groups*
- *Shared Risk Link Group* (SRLG)
- *Bandwidth Reservation Information*

Estas restrições implicam que novas informações sejam trocadas entre os *routers* e o RSVP-TE requer que todos os *routers* contenham a mesma informação atualizada na base de dados TED. Desta forma, é necessário utilizar as extensões OSPF-TE ou ISIS-TE para difundir e manter a informação de RSVP-TE atualizada em todos os *routers*. Para maior pormenor sobre o OSPF-TE refira-se ao capítulo 1.4.2.

A utilização de RSVP-TE requer um novo algoritmo para calcular os caminhos tendo em conta as restrições aplicadas. O *Constrained-Based Shortest Path First* (CSPF) permite realizar este cálculo, utilizando as informações da TED para ter uma visão global da rede e excluir as ligações afetadas pelas restrições do cálculo final do caminho. Entre

os caminhos disponíveis para o cálculo final é aplicado o algoritmo SPF (Dijkstra). Desta forma, no *router* iLER é realizado um cálculo do caminho *end-to-end*, utilizando depois o campo *Explicit Route Object* (ERO) na mensagem RSVP *PATH* para transmitir aos próximos *routers* qual é o *next-hop* desta mensagem [9] [11]. Na Figura 30 pode-se observar um exemplo deste processo.

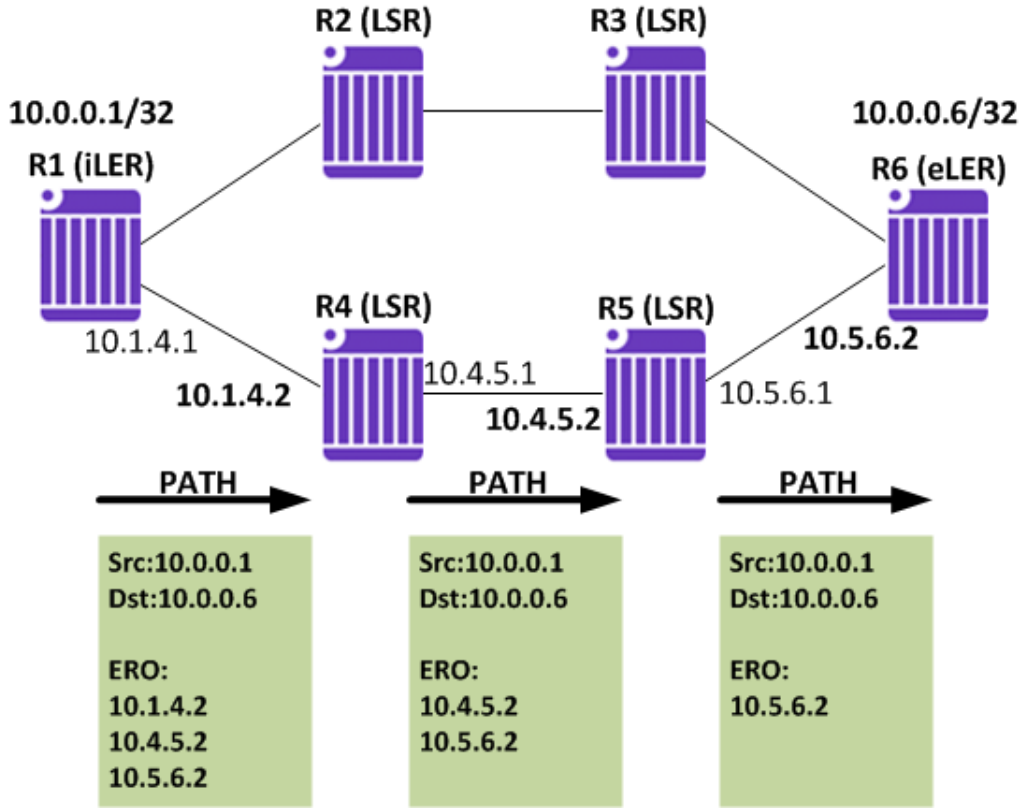

Figura 30 – Exemplo da mensagem RSVP *PATH* com a utilização do campo ERO.

No entanto, algumas restrições podem ser utilizadas sem o CSPF mas desta forma o *router* iLER não consegue calcular o caminho *end-to-end*. Cada *hop* aplica as restrições para definir apenas o *next-hop*, assim as tentativas para estabelecer os LSP podem resultar em erros devido a escolhas de caminhos iniciais que apenas se revelam impossíveis depois de alguns *hops* ou a restrições mal dimensionadas. O CSPF prevê estas situações utilizando uma visão global da rede para calcular previamente os caminhos *end-to-end* [9] [11].

1.5.4.1. *Explicit Routes*

Os *Path* dos LSP configurados no *router* iLER podem ter *Strict Hops*, *Loose Hops* ou ainda uma mistura dos dois. Os *Strict Hops* obrigam a que o *router* definido seja o *next-hop* do *router* anterior da lista, ou seja se for configurada uma lista de *Strict Hops* não poderão existir outros *hops* entre os *routers* da lista. No caso dos *Loose Hops* é possível que existam outros *hops* entre os *routers* da lista, obrigando apenas a que o LSP passe pelo *router* definido na lista. Por fim, existe ainda a possibilidade de utilizar as duas opções no mesmo LSP *Path* ou de definir apenas alguns *hops* deixando os restantes para serem calculados pelo CSPF. Os LSP *Path* podem ser ainda considerados *Fully*

Strict LSP *Path* caso todos os *hops* sejam manualmente configurados *end-to-end* ou ainda *Fully Loose* LSP *Path* se não tiverem restrições [9] [11].

1.5.4.2. TE *Metric*

A métrica IGP tem apenas em conta a largura de banda das ligações. A métrica TE permite que seja atribuída uma métrica personalizada às ligações e que esta seja utilizada em vez da métrica IGP. Esta pode ser útil caso algumas ligações tenham características diferentes, como o meio utilizado, que não são contabilizadas pela métrica IGP e podem ser um fator de escolha [9] [11].

1.5.4.3. *Hop Limit*

Esta restrição pode ser utilizada para reduzir o número de *routers* que o LSP pode passar. Assim mesmo que exista um caminho com uma métrica IGP menor, se o número de *hops* for excedido este caminho não será escolhido. O número de *hops* de cada caminho inclui os *routers* iLER e eLER, logo no mínimo poderá ser utilizado um *hop-limit* de 2 [9] [11].

1.5.4.4. *Administrative Groups*

Os *Administrative Groups* ou *admin-groups* são grupos de ligações que podem ser identificados através de um valor único em toda a rede e uma "cor" que torna a sua identificação intuitiva. Cada ligação pode ter um ou mais grupos associados e estes grupos podem ser incluídos ou excluídos do cálculo do LSP *Path*. Na Figura 31 pode-se observar um exemplo do LSP *Path* estabelecido de forma a excluir as ligações do grupo "Green".

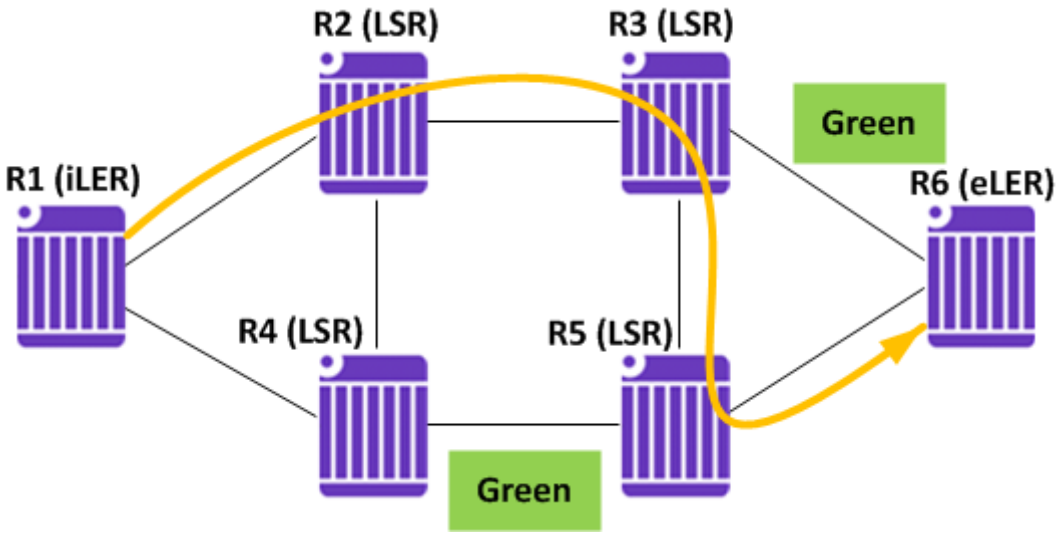

Figura 31 – Exemplo da exclusão de um *admin-group* do cálculo do LSP *Path*.

A inclusão de um *admin-group* no LSP *Path* só é possível se existir um caminho *end-to-end* associado ao *admin-group*. A utilização de *admin-groups* exige um planeamento rigoroso de forma a evitar situações em que os LSP não consigam encontrar um

caminho de acordo com as restrições aplicadas. Estas restrições podem ser utilizadas aos *primary-path* e *secondary-path* mas não ao FRR [9] [11].

1.5.4.5. *Shared Risk Link Group* (SRLG)

O SRLG é semelhante aos *admin-groups*, tendo também grupos que são associados às ligações, no entanto este tem como objetivo criar um *secondary-path* que não utilize as ligações dos grupos SRLG que o *primary-path* utilizou. Assim, também é necessário realizar um planeamento rigoroso de atribuição de grupos SRLG às ligações, para que não existam situações em que o *secondary-path* não se consegue estabelecer. O cálculo do *secondary-path* é um processo automático e o SRLG pode ainda ser utilizado com o *Fast Reroute* nos *hardwares*/*softwares* mais recentes [9] [11].

1.5.4.6. *Bandwidth Reservation Information*

A reserva de largura de banda permite que cada LSP reserve um determinado valor de largura de banda em todas as ligações por onde o LSP é estabelecido. O valor utilizado pode ter como base valores definidos no SLA ou previsões de máximos ou média de largura de banda que o tráfego possa utilizar. No entanto, esta reserva de largura de banda tem apenas efeito ao nível do *control-plane*, ou seja serve apenas para limitar o número de LSP que se podem estabelecer em determinada ligação de acordo com a largura de banda que a ligação disponibiliza. Desta forma, numa ligação de um 1 Gb/s apesar de um LSP reservar apenas 200 Mb/s este pode utilizar a totalidade da largura de banda da ligação. A limitação da largura de banda ao nível do *data-plane* pode ser implementada em conjunto com o modelo *DiffServ* [9] [11]. Na Figura 32 está um exemplo da reserva de largura de banda.

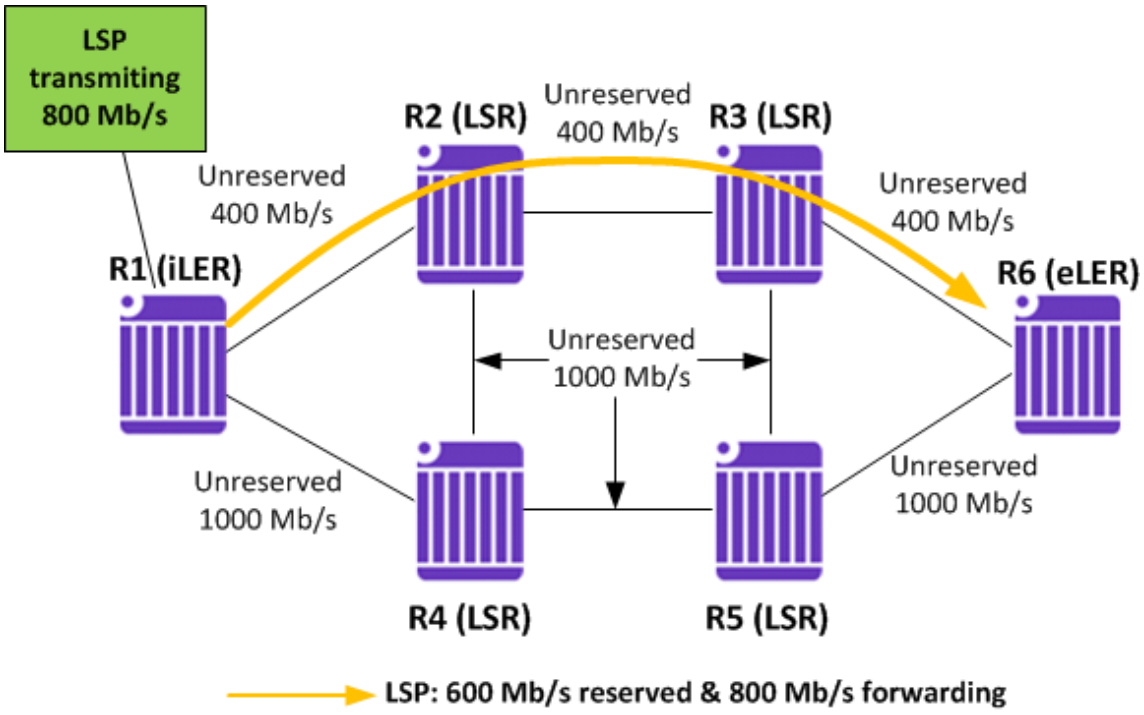

Figura 32 – Exemplo da reserva de largura de banda de 600 Mb/s, transmitindo na verdade 800 Mb/s.

Tal como as restrições anteriores, é necessário realizar um planeamento da atribuição de largura de banda a cada LSP, para garantir que todos os LSP se conseguem estabelecer. Estes utilizando o CSPF verificam todas as ligações que tem largura de banda disponível e calculam o melhor caminho com as ligações previamente examinadas. A largura de banda disponibilizada pelas ligações para a reserva é por omissão a capacidade da ligação. No entanto é possível realizar *under-booking* e *over-booking* da LB numa ligação, realizando uma "*subscription*" onde os valores percentuais podem variar dos 0-1000, sendo o valor por omissão de 100. Esta alteração permite "disponibilizar" até 10 vezes mais largura de banda que a real capacidade da ligação [9] [11].

A reserva de LB também pode ser aplicada aos *secondary-path*, se este estiver em modo *Hot-standby* a largura de banda será reservada apesar de não estar a ser utilizado. Caso contrário apenas será reservada quando este se tentar estabelecer após a queda do *primary-path*. Existem dois tipos de reserva possíveis, por omissão as ligações partilhadas pelos *primary-path* e *Hot-standby secondary-path* reservam apenas o maior valor LB configurado entre os dois, sendo este modo o *Shared Explicit* (SE). No entanto, com o modo *Fixed Filter* (FF) é possível que cada LSP *Path* reserve a largura de banda configurada independentemente de a ligação ser partilhada ou não entre o *primary-path* e o *Hot-standby secondary-path* [9] [11]. Na Figura 33 está um exemplo do comportamento realizado por omissão.

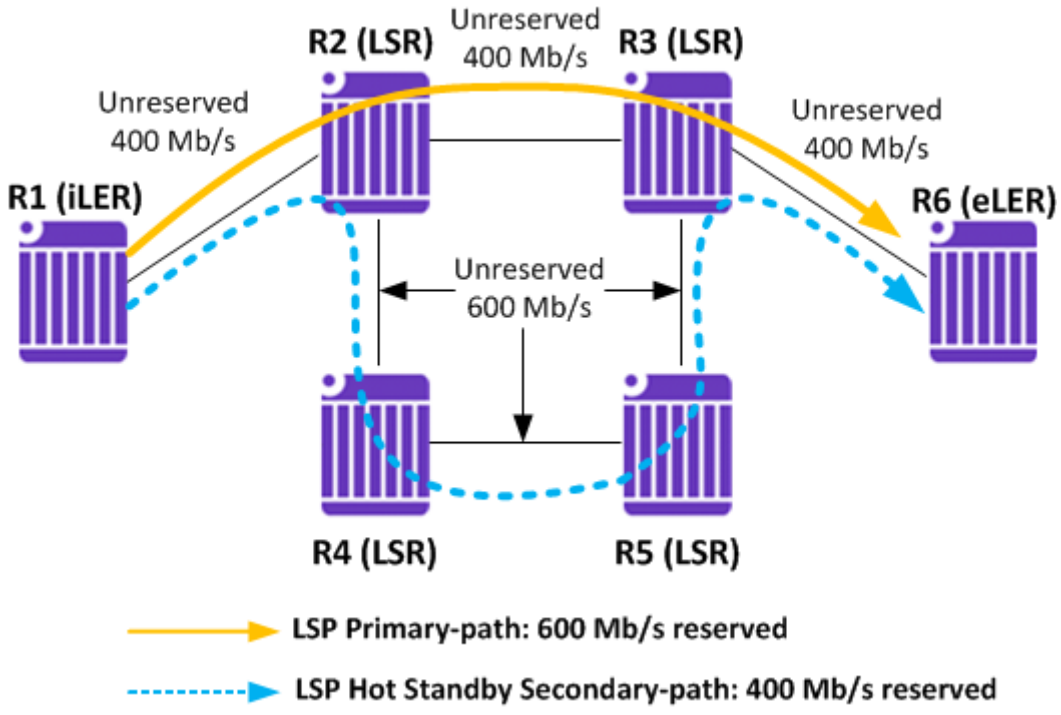

Figura 33 – Exemplo do modo SE da reserva da largura banda.

A ocupação de largura de banda pode ser otimizada com a opção "*least-fill*", esta define que caso exista mais do que um caminho com largura de banda disponível e com a mesma métrica IGP, o LSP *Path* será estabelecido pelo caminho com menos largura de banda ocupada. Sem esta opção a escolha do caminho seria aleatória [9] [11].

1.5.4.7. *Bandwidth Reservation Information with Soft Preemption*

A reserva de largura de banda pode ainda ser otimizada com o modo *Soft Preemption*. Este permite que sejam atribuídas prioridades aos LSP, para que os LSP com maior prioridade possam ocupar a reserva dos LSP com menor prioridade, obrigando estes a procurar um novo caminho. A prioridade atribuída é na verdade constituída por duas prioridades com valores de 0 a 7, onde 0 é o máximo e 7 o mínimo.

- ***Setup Priority*:** Este valor define a prioridade a partir do qual outros LSP podem ser obrigados a mudar. Com o valor 7 de prioridade o LSP não consegue "obrigar" outros LSP a mudar [9] [11].
- ***Hold Priority*:** Este valor define a prioridade a partir do qual o LSP pode ser obrigado a procurar outro caminho. Com uma prioridade de 0 este LSP não pode ser obrigado a mudar de caminho [9] [11].

Apesar de poderem ter valores diferentes é considerada uma boa prática atribuir o mesmo valor às duas prioridades. Caso o valor da prioridade de *Setup* seja menor que o valor da prioridade *Hold* podem acontecer "*preemption loops*". Pode-se observar no seguinte exemplo uma configuração de prioridades, onde o primeiro valor é referente à prioridade de *Setup* e o segundo à prioridade de *Hold*.

```
Primary "Loose"
      bandwidth 500
      priority 2 2
```

Na Figura 34 pode-se observar um exemplo de um LSP prioritário a obrigar o LSP estabelecido a procurar outro caminho e ainda um LSP com baixa prioridade que não se consegue estabelecer porque todos os caminhos estão ocupados por LSP prioritários.

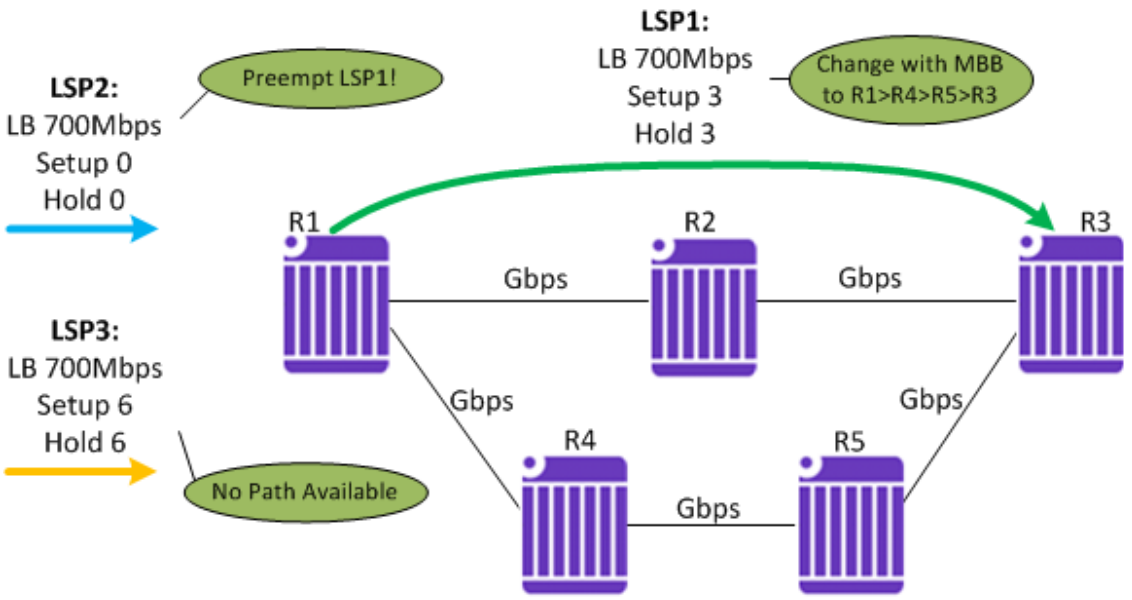

Figura 34 – Exemplo do funcionamento das prioridades com reserva de largura de banda.

No exemplo anterior, o LSP2 verifica se existe largura de banda disponível no caminho R1>R2>R3 com a prioridade 0 0. A largura de banda deste caminho está ocupada apenas a partir da prioridade 3 3 pelo LSP1, logo o LSP2 pode-se estabelecer neste caminho obrigando o LSP1 a procurar outro caminho. O LSP1 calcula um novo caminho que contenha largura de banda disponível, resultando no caminho R1>R4>R5>R3. Este sinaliza o novo caminho e efetua a reserva de largura de banda, mudando o tráfego através do MBB. Por fim, o LSP3 com uma prioridade inferior em relação aos LSP1 e LSP2, não se conseguirá estabelecer. No entanto, se este diminuir a reserva para 300 Mb/s já conseguirá estabelecer um caminho, pois as prioridades apenas afetam os LSP caso não exista largura de banda disponível para todos os LSP. Note-se que o LSP1 tem por omissão 300 segundos para calcular um novo caminho e este cálculo é realizado por omissão de 30 em 30 segundos [9] [11].

1.5.5. MPLS *DiffServ*-TE

Os modelos de MPLS-TE e DS podem ser utilizados em conjunto para melhorar as medidas de QoS nos serviços. O MPLS-TE permite escolher um caminho diferente do caminho calculado pelo IGP e melhorar a resiliência da rede, enquanto o DS permite que sejam aplicadas medidas *Per Hop Behavior* (PHB) para determinar os pacotes que devem ser transmitidos com maior prioridade e em caso de congestão os pacotes que devem ser descartados primeiro. A combinação destes modelos permite ajustar todas as medidas de QoS às necessidades de cada serviço [3] [14].

O DS utiliza o código *DiffServ Code Point* (DSCP) para transmitir a prioridade atribuída ao pacote. Em conjunto com o MPLS, este código é transmitido no campo EXP do cabeçalho MPLS, permitindo assim que todos os *routers* MPLS tenham em conta a prioridade dos pacotes no processo de comutação [3] [14].

1.5.6. Resiliência RSVP-TE

Os métodos de resiliência servem para recuperar o serviço de rede em caso de falhas. O primeiro passo será a deteção da falha, esta depende se a falha é provocada por um problema físico ou por um problema de *software*. Os problemas físicos podem ainda ser locais ou remotos. As falhas locais são imediatamente detetadas, devido à perda de sinal no cabo. No caso das falhas remotas, se os equipamentos remotos, como por exemplo *switches*, não propagarem a falha de rede, os *routers* vão manter as suas interfaces ativas. Desta forma, os *routers* necessitam de mecanismos adicionais como as mensagens *Hello* dos protocolos IGP e RSVP para detetar as falhas remotas. Os protocolos IGP demoram por omissão 30 s a detetar uma falha remota, enquanto que o RSVP demora 9 s por omissão. No entanto ambos podem ser configurados para enviar mensagens *Hello* com uma periocidade de 1 s. Como alternativa existem ainda protocolos especializados na deteção de falhas remotas, como o BFD que permite a deteção em menos de 100 ms [9] [11].

1.5.6.1. *Secondary-path*

Os *secondary-path* são caminhos alternativos configurados para substituir o *primary-path* em caso de falha de rede. Podem ser configurados até 7 *secondary-path* no modo

Hot-standby ou no modo *Cold-standby*. O *Hot-standby secondary-path* é estabelecido após o *primary-path* e permanece em "*standby*" até uma falha de rede afetar o *primary-path*. No modo *Cold-standby* o *secondary-path* é apenas sinalizado e estabelecido após a ocorrência de uma falha de rede [9] [11]. O critério de escolha entre os vários *secondary-path* configurados segue a seguinte ordem:

- ***Hot-standby secondary-path*:** Estes *secondary-path* são prioritários na escolha, se existirem vários será escolhido o *secondary-path* com maior *uptime* [9] [11].
- ***Cold-standby secondary-path*:** Caso não existam *Hot-standby secondary-path*, este será utilizado. Se existirem vários *Cold-standby secondary-path* a escolha será feita pela ordem de configuração [9] [11].

No entanto, se o *primary-path* recuperar o tráfego será encaminhado de novo através deste LSP *Path*. O mesmo não acontece entre *secondary-paths*.

O caminho estabelecido pelos *secondary-path* pode ser influenciado através das restrições de TE para garantir que são utilizados caminhos diferentes do *primary-path*.

1.5.6.2. *Make-Before-Break* (MBB)

O MBB é um mecanismo de resiliência do RSVP-TE que permite a troca do LSP *Path* sem perdas de pacotes. O MBB é utilizado para transferir o tráfego de um *secondary-path* ou túnel FRR de volta para o *primary-path*, pode ser utilizado também nos LSP que utilizam *Soft Preemption* com a reserva de largura de banda. O MBB garante que o novo LSP *Path* está estabelecido e apenas depois transfere o tráfego para o novo LSP *Path*. Desta forma por um breve momento existem dois LSP *Path* ativos, sendo o caminho anterior desativado, nos casos aplicáveis, com a mensagem RSVP *PATH TEAR* após a mudança do tráfego [9] [11].

1.5.6.3. *Fast Reroute* (FRR)

O FRR é um método de resiliência do RSVP-TE que permite recuperar o serviço das falhas de rede em menos de 50 ms. O FRR pode ser utilizado de duas formas, FRR *One-to-One* ou FRR *Facility*. No entanto, o FRR *Facility* permite que os túneis de *bypass* sejam partilhados por vários LSP, diminuindo assim o número de túneis de proteção necessários. Por este motivo neste projeto apenas foi utilizado o FRR *Facility*, assim neste capítulo apenas será abordado este método.

Cada *router* calcula os túneis de proteção FRR através do CSPF. Estes túneis podem ser dos seguintes tipos:

- ***Link-protect*:** Estes túneis têm como objetivo proteger a ligação ao *next-hop*, procurando estabelecer um túnel de proteção por um caminho alternativo até ao *next-hop* [9] [11].
- ***Node-protect*:** Neste caso o objetivo é proteger o *primary-path* do *next-hop* e todas as suas ligações, procurando estabelecer um túnel de proteção por um caminho alternativo até ao *next-next-hop* [9] [11].

Na Figura 35 pode-se observar um exemplo dos dois tipos de proteção, assim como os *Point of Local Repair* (PLR) que são os *routers* onde os túneis de *bypass* têm origem e ainda os *Merge Point* (MP) que indicam os *routers* onde os túneis de *bypass* terminam [9] [11].

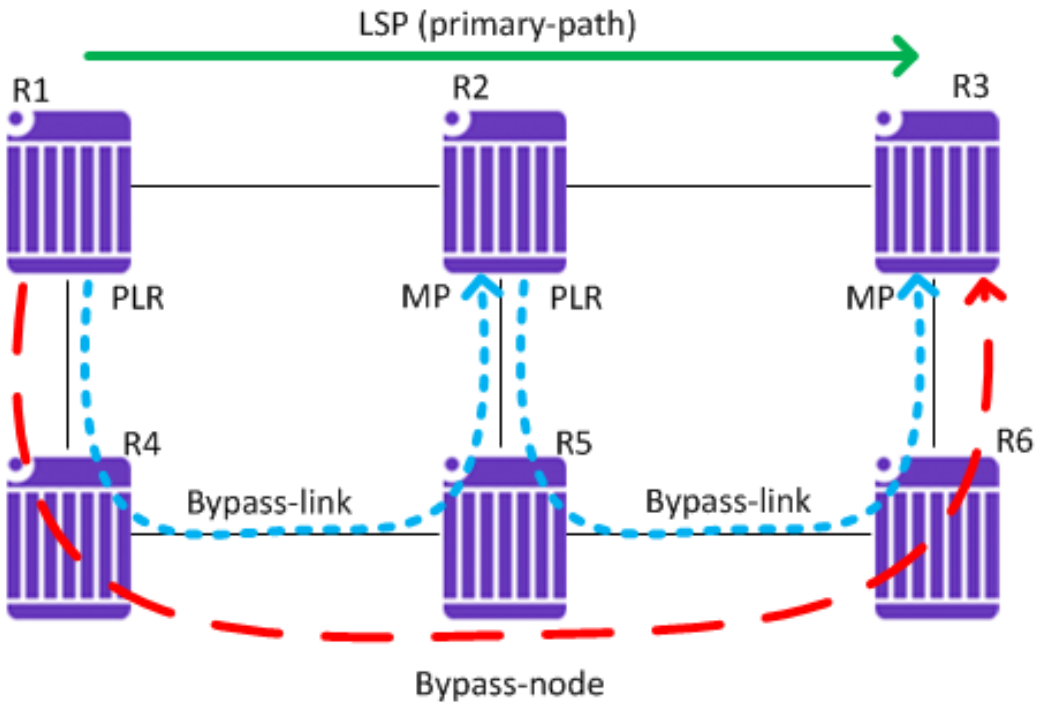

Figura 35 – Exemplo de túneis *bypass-link* e *bypass-node*.

Desta forma todos os LSP que utilizem as ligações R1>R2>R3 serão protegidos pelos túneis representados na figura anterior. Os túneis são criados apenas quando um LSP com o FRR configurado se estabelecer por ligações que ainda não tenham túneis de proteção. Cada *router* ao longo do LSP tem de ter conhecimento de todos os *routers* e *labels* seguintes para que possa estabelecer os túneis de *bypass* [9] [11]. Estas informações necessárias são transmitidas na mensagem RSVP *RESV* no campo *Record Route*, como se pode verificar no exemplo da Figura 36.

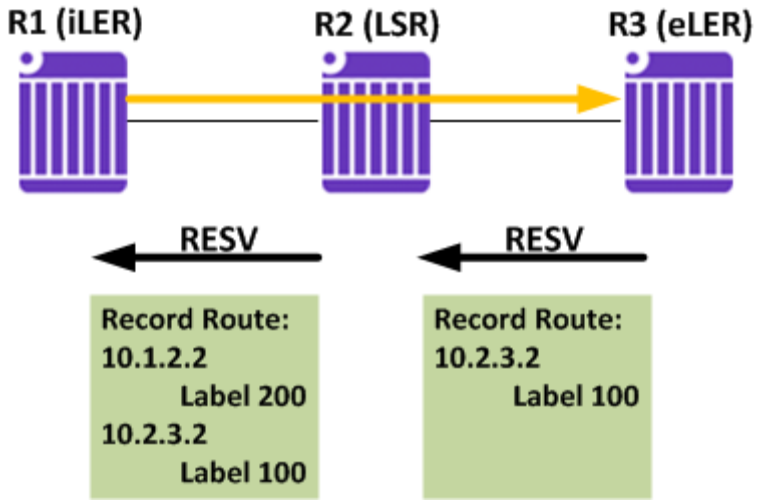

Figura 36 – Exemplo da mensagem RSVP *RESV* com a partilha de informação necessária para sinalizar os túneis de *bypass*.

Para que vários LSP possam utilizar os mesmos túneis de *bypass* é necessário que o tráfego destes LSP seja identificável no MP. Desta forma, a *label* que o *router* MP espera receber do *primary-path* é transmitida através do túnel de *bypass*. Isto é possível devido à nova *label* acrescentada na *stack* de *labels* referente ao túnel de *bypass*. Assim, a *label* do *primary-path* mantem-se inalterada ao longo do túnel de *bypass*, sendo apenas alterada em cada *hop* a *label* do túnel de *bypass* até que por fim é retirada no MP. Na Figura 37 pode-se observar este processo que permite que vários LSP partilhem os mesmos túneis de *bypass*.

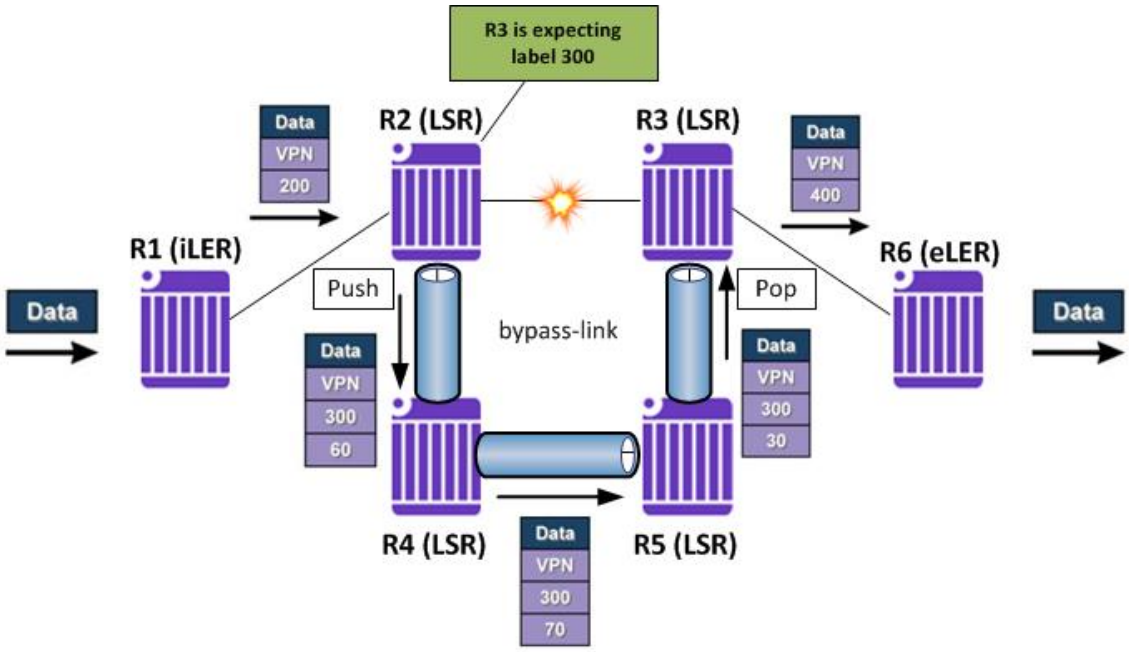

Figura 37 – Exemplo da *stack* de *labels* num túnel de *bypass*.

Este processo é igual para os dois tipos de proteção, *Link* e *Node*. Sendo que no caso da proteção de *Node* é necessário que os *routers* tenham uma visão do *nex-next-hop* para que o tráfego chegue a este *router* com as *labels* corretas.

Na ocorrência de uma falha de rede, após a deteção o tráfego é comutado para o túnel de *bypass*. O *router* PLR que detetou a falha envia uma mensagem RSVP *PATH ERR* para o *router* iLER, com um código de erro que indica que o LSP foi localmente reparado através do túnel de *bypass*. O *router* iLER mantem o *primary-path* ativo, no entanto se existir um *Hot-standby secondary-path* o tráfego será comutado para este com o auxílio do MBB. Se existir apenas um *Cold-standby secondary-path* o tráfego mantém-se no *primary-path* com o túnel de *bypass* ativo [9] [11].

1.6. Bidirectional Forwarding Detection (BFD)

O BFD tem como objetivo melhorar a deteção de falhas de rede remotas. Os *routers* conseguem apenas detetar as falhas nas suas ligações, assim as quebras de ligações entre equipamentos L2 são apenas detetáveis através de mensagens *Hello* dos protocolos IGP e RSVP-TE. O BFD envia e recebe pacotes de controlo num determinado período configurado em ambas as partes, este período pode ter um mínimo de 10 ms. Assim, caso não sejam recebidos 3 pacotes seguidos a ligação é considerada desligada, levando no mínimo 30 ms para realizar a deteção. Após a deteção da falha o BFD reporta o sucedido ao protocolo de IGP ou RSVP-TE, permitindo que estes desencadeiem os processos de resiliência para encontrar um novo caminho [9] [11].

1.7. Serviços L2 VPN

Existem dois tipos de serviços de L2, *Virtual Private Wire Service* (VPWS) e *Virtual Private LAN Service* (VPLS). Como os nomes indicam a VPWS é um serviço ponto-a-ponto, enquanto que a VPLS é serviço de LAN. A VPWS simula um cabo direto entre os equipamentos do cliente, como se pode observar na Figura 38.

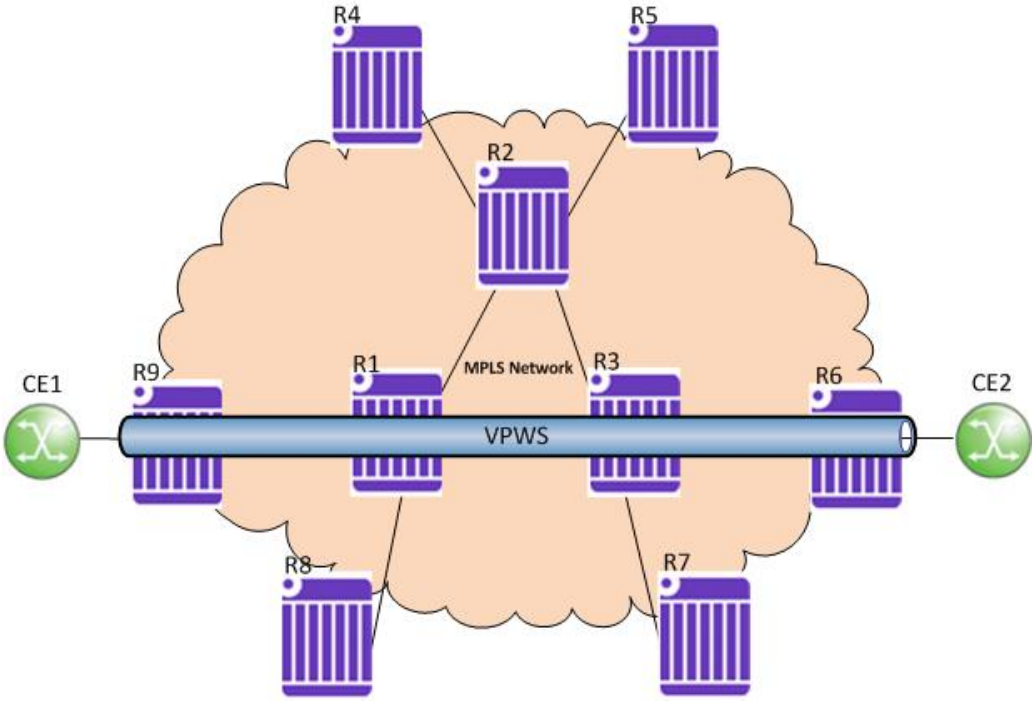

Figura 38 – Exemplo de uma rede MPLS com um serviço VPWS.

A VPWS transporta as tramas através da rede MPLS como se estes estivessem no seu meio nativo. Assim é possível servir redes *Ethernet* (ePipes), ATM (aPipes), *Frame Relay* (fPipes), IP (iPipes) e circuitos TDM (cPipes) [9] [11].

A VPLS é um serviço de *Ethernet* que permite simular um *switch* virtual entre os vários *routers* de acesso, como se pode observar na Figura 39. O *switch* virtual da VPLS tem capacidade para fazer MAC *learning* e encaminhar as tramas apenas pelos LSP necessários [9] [11].

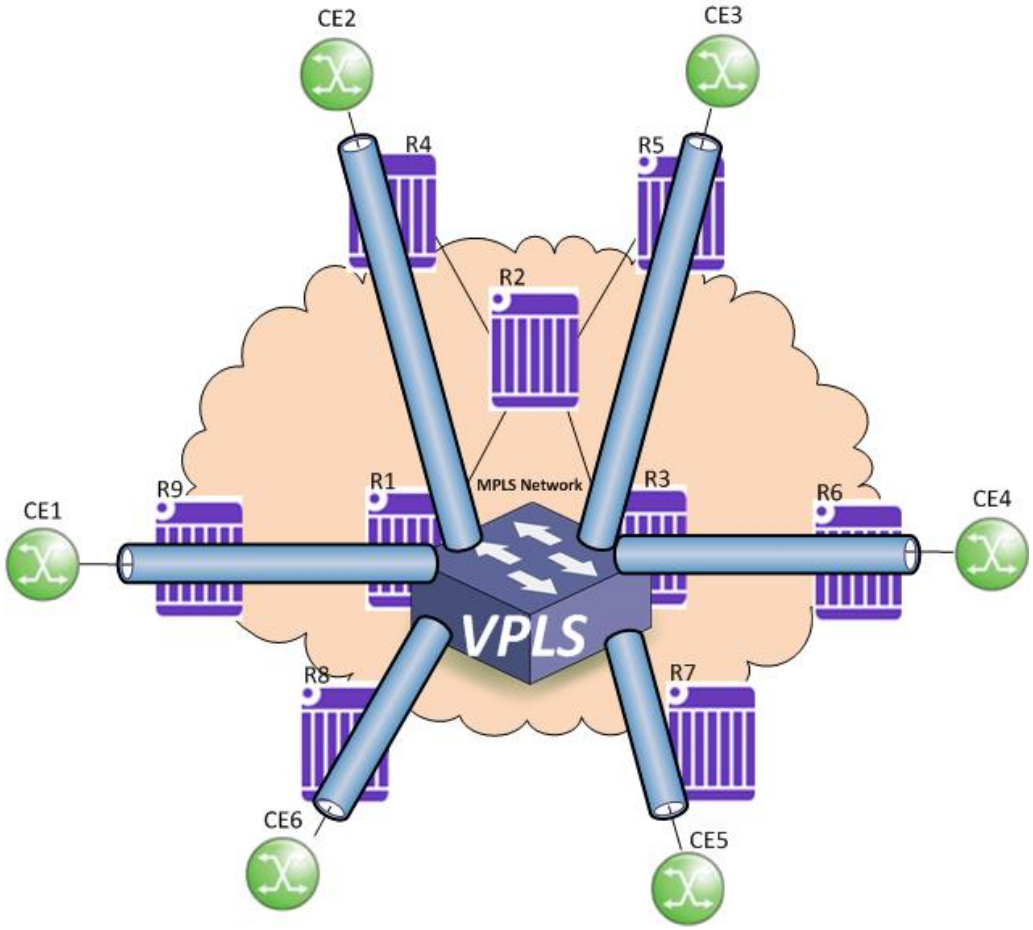

Figura 39 – Exemplo de uma rede MPLS com um serviço VPLS.

1.8. Serviços L3 VPN

O serviço L3 VPN é também conhecido por *Virtual Private Routed Network* (VPRN). Este serviço liga os vários clientes através de uma rede virtual L3, como se pode observar na Figura 40. Cada *router* PE tem uma tabela de encaminhamento para cada VPRN. Os endereços IP utilizados numa VPRN são independentes do endereçamento da rede MPLS e das outras VPRN [9] [11].

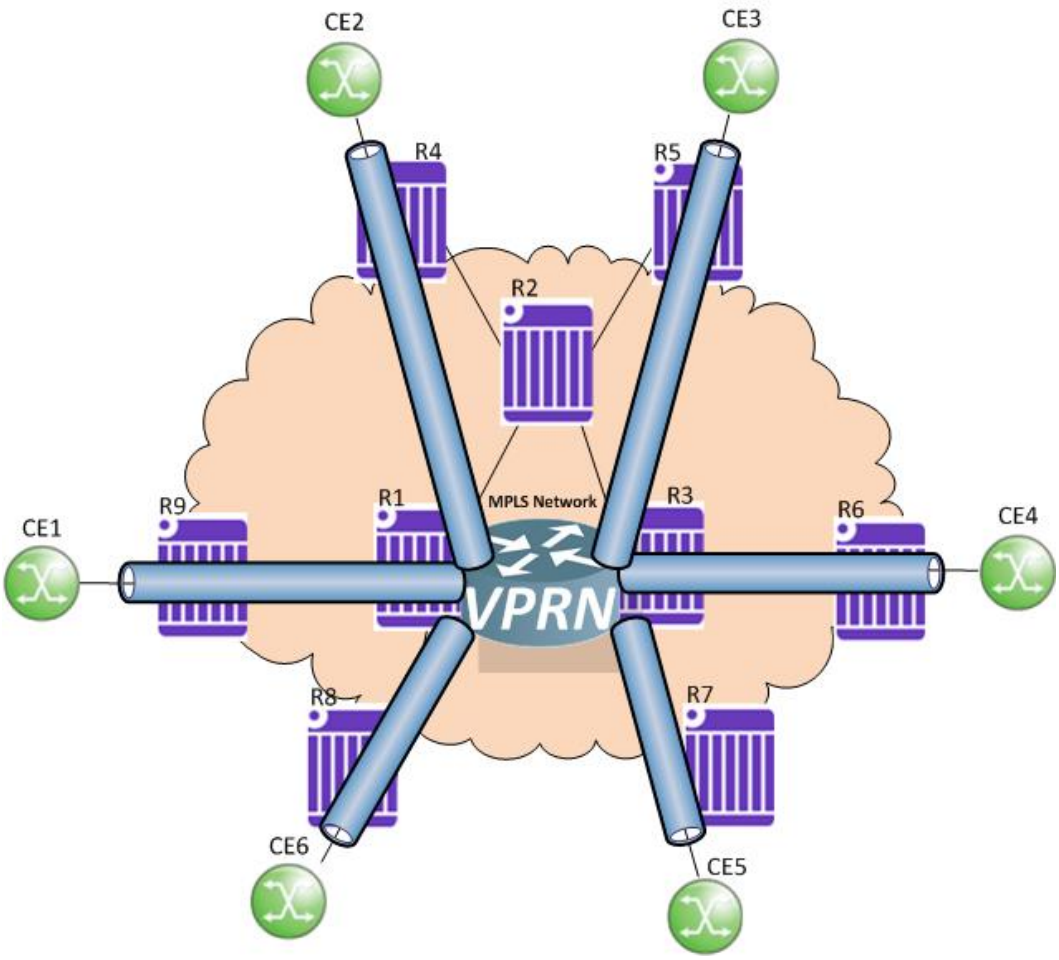

Figura 40 – Exemplo de uma rede MPLS com um serviço VPRN.

2. Análise à rede MPLS do IPL

Numa primeira fase foi realizada uma análise à situação atual da rede MPLS do IPL. Nesta tentou-se perceber a ligação entre o encaminhamento de pacotes, MPLS e serviços L2VPN utilizados.

O IPL inclui 8 unidades orgânicas, entre as quais se inclui o ISEL, os serviços centrais e os serviços sociais. Estas entidades encontram-se disseminadas pela cidade de Lisboa e na Amadora, estando todas elas interligadas através de uma rede de fibra ótica onde se ligam os *routers* PE da rede MPLS do IPL, como se pode observar na Figura 41.

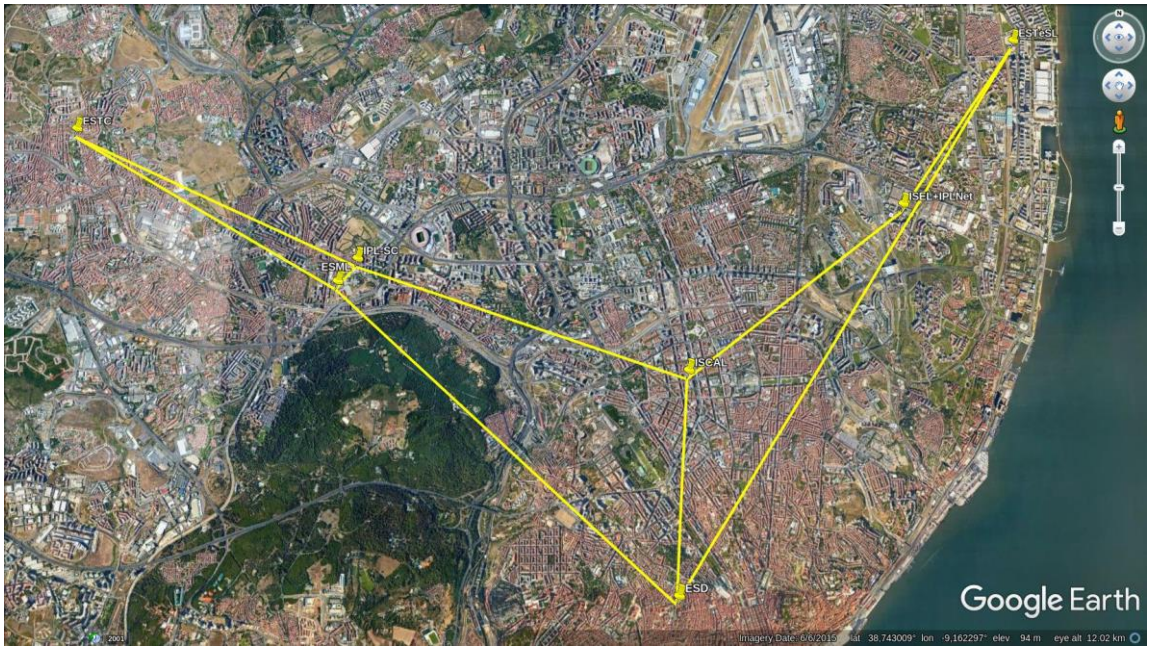

Figura 41 – Mapa de Lisboa com alusão à rede MPLS e aos polos do IPL distribuídos pela cidade, que contém *routers* PE da rede MPLS do IPL, retirado da documentação da rede do IPL [15].

A rede MPLS é constituída por equipamentos 7210-SAS-M da Alcatel-Lucent (Nokia), tendo cada polo pelo menos um equipamento destes. Na Figura 42 pode-se observar a topologia lógica da rede MPLS.

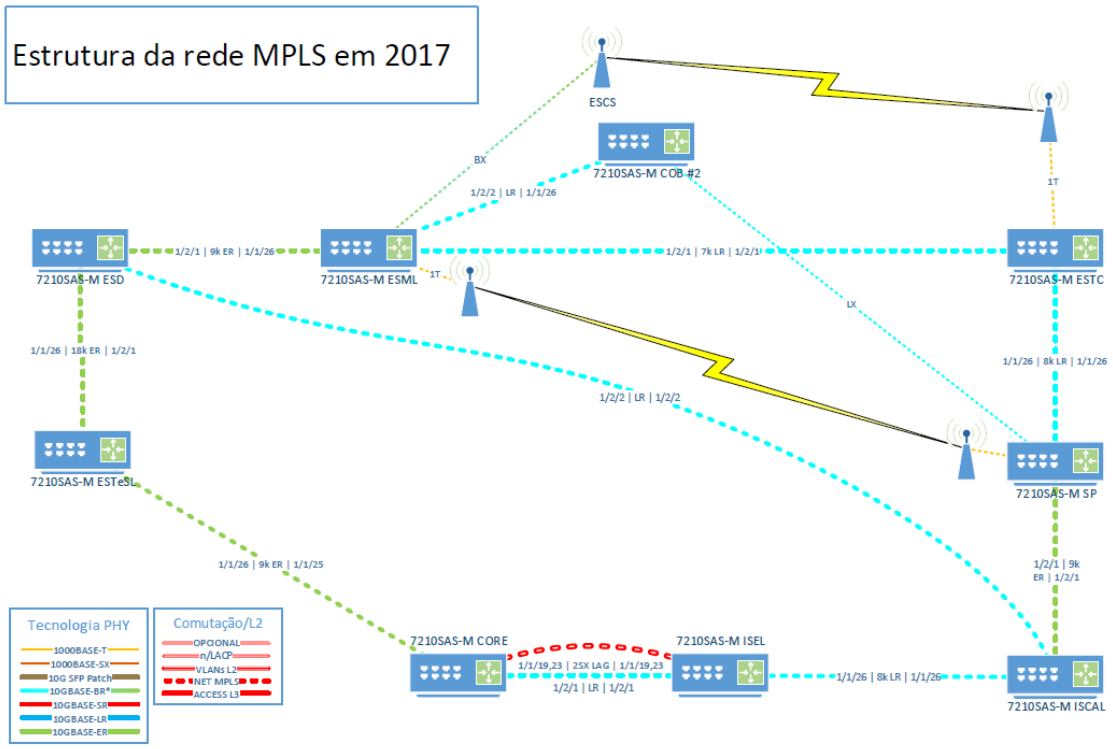

Figura 42 – Topologia lógica da rede MPLS do IPL, retirado da documentação da rede do IPL [15].

A rede é composta maioritariamente por ligações de 10 Gb/s, onde as cores de cada ligação identificam o tipo de norma utilizada. Note-se ainda que duas ligações complementares da rede MPLS são realizadas via rádio e uma ao débito de 1 Gb/s.

A análise será separada em três capítulos referentes ao roteamento, MPLS e serviços da rede. Os seguintes excertos de código têm origem no equipamento "MPLS-ESD", sendo a configuração de todos os outros elementos da rede idêntica.

2.1. Análise ao encaminhamento de pacotes

Para usufruir de todas as capacidades duma rede MPLS é necessário implementar um protocolo de encaminhamento IGP do tipo *link-state*, tendo como opção o OSPF-TE ou o ISIS-TE.

A rede do IPL utiliza o protocolo OSPF para realizar o encaminhamento. No seguinte exemplo pode-se verificar a configuração OSPF utilizada, note-se que todas as interfaces pertencem à área 0.0.0.0 e a opção *traffic-engineering* está ativa.

```
A: MPLS-ESD# admin display-config
...
#--------------------------------------------------
echo "OSPFv2 Configuration"
#--------------------------------------------------
       ospf
              traffic-engineering
              area 0.0.0.0
                 interface "system"
                     no shutdown
                 exit
                 interface "ESML"
```

```
                    interface-type point-to-point
                    hello-interval 1
                    dead-interval 3
                    authentication-type message-digest
                    message-digest-key 1 md5 "<DELETED>" hash2
                    no shutdown
                exit
                interface "ESTeSL"
                    interface-type point-to-point
                    hello-interval 1
                    dead-interval 3
                    authentication-type message-digest
                    message-digest-key 1 md5 "<DELETED>" hash2
                    no shutdown
                exit
                interface "ISCAL"
                    interface-type point-to-point
                    hello-interval 1
                    dead-interval 3
                    authentication-type message-digest
                    message-digest-key 1 md5 "<DELETED>" hash2
                    no shutdown
                exit
            exit
            no shutdown
        exit
```

Todas as interfaces estão configuradas com o *hello-interval* de 1 s e o *dead-interval* de 3 s, diminuindo assim o tempo de deteção de falhas do OSPF para 3 s. O facto de existir apenas uma área facilita os processos de comunicação do MPLS. A opção *traffic-engineering* permite a comunicação de informações de engenharia de tráfego entre equipamentos da rede MPLS.

2.2. Análise às configurações MPLS

Na rede do IPL estão ambas as opções LDP e RSVP configuradas. No seguinte exemplo pode-se verificar a configuração LDP.

```
A: MPLS-ESD# admin display-config
...
#--------------------------------------------------
echo "LDP Configuration"
#--------------------------------------------------
        ldp
            interface-parameters
                interface "ESTeSL"
                    ipv4
                        fec-type-capability
                            prefix-ipv6 disable
                            p2mp-ipv4 disable
                            p2mp-ipv6 disable
                        exit
                        no shutdown
                    exit
                    no shutdown
                exit
                interface "ISEL"
                    ipv4
                        fec-type-capability
                            prefix-ipv6 disable
                            p2mp-ipv4 disable
                            p2mp-ipv6 disable
```

```
                    exit
                    no shutdown
                exit
                no shutdown
            exit
            interface "ISEL2G"
                ipv4
                    fec-type-capability
                        prefix-ipv6 disable
                        p2mp-ipv4 disable
                        p2mp-ipv6 disable
                    exit
                    no shutdown
                exit
                no shutdown
            exit
            interface "CCR1036"
                ipv4
                    fec-type-capability
                        prefix-ipv6 disable
                        p2mp-ipv4 disable
                        p2mp-ipv6 disable
                    exit
                    no shutdown
                exit
                no shutdown
            exit
        exit
        targeted-session
        exit
        no shutdown
    exit
```

No caso do RSVP é necessário definir os LSP individualmente e todas as opções que podem ser aplicadas com o *traffic-engineering*. Na definição dos LSP foram utilizados *path* sem *hops* definidos para o *primary-path* e *secondary-path*. No *primary-path* é realizada uma reserva de LB de 1000 Mb/s, no caso do *secondary-path* a reserva de LB é de 100 Mb/s e está no modo *Hot-standby*. O FRR *facility* também está configurado, assim como a opção "*adspec*" que verifica qual é o menor MTU ao longo do LSP.

```
A: MPLS-ESD# admin display-config
...
#--------------------------------------------------
echo "MPLS LSP Configuration"
#--------------------------------------------------
        mpls
            path "dyn"
                no shutdown
            exit
            path "alt"
                no shutdown
            exit
            lsp "ISEL"
                to 10.8.0.64
                cspf
                adspec
                fast-reroute facility
                exit
                primary "dyn"
                    bandwidth 1000
                exit
                secondary "alt"
                    standby
                    bandwidth 100
```

```
            exit
            no shutdown
        exit
        lsp "SC"
            to 10.8.0.35
            cspf
            adspec
            fast-reroute facility
            exit
            primary "dyn"
                bandwidth 1000
            exit
            secondary "alt"
                standby
                bandwidth 100
            exit
            no shutdown
        exit
        lsp "ESML"
            to 10.8.0.37
            cspf
            adspec
            fast-reroute facility
            exit
            primary "dyn"
                bandwidth 1000
            exit
            secondary "alt"
                standby
                bandwidth 100
            exit
            no shutdown
        exit
        lsp "CORE"
            to 10.8.0.11
            cspf
            adspec
            fast-reroute facility
            exit
            primary "dyn"
                bandwidth 1000
            exit
            secondary "alt"
                standby
                bandwidth 100
            exit
            no shutdown
        exit
        lsp "ISCAL"
            to 10.8.0.43
            cspf
            adspec
            fast-reroute facility
            exit
            primary "dyn"
                bandwidth 1000
            exit
            secondary "alt"
                standby
                bandwidth 100
            exit
            no shutdown
        exit
        lsp "ESTeSL"
            to 10.8.0.44
            cspf
            adspec
            fast-reroute facility
```

```
                exit
                primary "dyn"
                    bandwidth 1000
                exit
                secondary "alt"
                    standby
                    bandwidth 100
                exit
                no shutdown
            exit
            lsp "ESTC"
                to 10.8.0.42
                cspf
                adspec
                fast-reroute facility
                exit
                primary "dyn"
                    bandwidth 1000
                exit
                secondary "alt"
                    standby
                    bandwidth 100
                exit
                no shutdown
            exit
            lsp "COB1"
                to 10.8.0.101
                cspf
                adspec
                fast-reroute facility
                exit
                primary "dyn"
                    bandwidth 1000
                exit
                secondary "alt"
                    standby
                    bandwidth 100
                exit
                no shutdown
            exit
            no shutdown
        exit
```

No seguinte exemplo pode-se verificar que algumas das interfaces foram associadas a *admin-groups* e SRLG-*groups*.

```
A: MPLS-ESD# admin display-config
...
#--------------------------------------------------
echo "MPLS Configuration"
#--------------------------------------------------
        mpls
            resignal-timer 500
            hold-timer 3
            interface "system"
                no shutdown
            exit
            interface "ESML"
                admin-group "green"
                srlg-group "FO_ARTELECOM"
                no shutdown
            exit
            interface "ESTeSL"
                admin-group "red"
                srlg-group "FO_ARTELECOM"
                no shutdown
```

```
            exit
            interface "ISCAL"
                admin-group "yellow"
                srlg-group "FO_ARTELECOM"
                no shutdown
            exit
        exit
```

2.2.1. Discussão

Analisando esta configuração verifica-se que estão a ser utilizados dois métodos diferentes de resiliência, *Hot-standby secondary-path* e FRR *facility*. Ambos os métodos são válidos e podem ser utilizados em conjunto, no entanto neste caso sem restrições adicionais no *primary-path* e no *secondary-path*, apenas o FRR *facility* pode garantir a resiliência de todos os LSP.

O *primary-path* irá procurar o melhor caminho IGP que tenha 1000 Mb/s de LB disponíveis, tornando imprevisível o caminho estabelecido por cada LSP. O FRR procura caminhos alternativos aos estabelecidos no *primary-path*, sendo neste caso bastante útil. A utilização de um *Hot-standby secondary-path* apenas com a reserva de 100 Mb/s não garante que este utilize um caminho diferente do caminho do *primary-path*. Assim o *primary-path* e *secondary-path* poderão ser ambos afetados pelas mesmas falhas.

De notar que em caso de falha o FRR ficará ativo e apenas depois será enviada uma mensagem RSVP *PATH ERR* para notificar o iLER do sucedido. Este ao receber a mensagem de erro tentará mudar o fluxo para *Hot-standby secondary-path* com o auxílio do MBB. Caso o *Hot-standby secondary-path* esteja também desativo, o tráfego manterá o seu caminho pelo túnel *bypass* do FRR.

O facto do *Hot-standby secondary-path* reservar 100 Mb/s de LB ativamente dificulta a escalabilidade desta solução. O aumento do número dos LSP irá esgotar a largura de banda reservável em vários troços, impondo dificuldades no estabelecimento de novos LSP na rede.

2.3. Análise aos serviços VPN implementados na rede

Na rede MPLS do IPL existe uma grande variedade de serviços, sendo na sua maioria VPLS e VPWS. Estes serviços são servidos apenas pelos túneis LDP apesar dos túneis RSVP também estarem estabelecidos. Na seguinte configuração pode-se verificar que todos os SDP estão associados ao LDP.

```
A: MPLS-ESD# admin display-config
...

#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
    service
        sdp 11 mpls create
            far-end 10.8.0.11
            ldp
            keep-alive
```

```
            shutdown
        exit
        no shutdown
    exit
    sdp 35 mpls create
        far-end 10.8.0.35
        ldp
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 37 mpls create
        far-end 10.8.0.37
        ldp
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 42 mpls create
        far-end 10.8.0.42
        ldp
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 43 mpls create
        far-end 10.8.0.43
        ldp
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 44 mpls create
        far-end 10.8.0.44
        ldp
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 64 mpls create
        far-end 10.8.0.64
        ldp
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 101 mpls create
        far-end 10.8.0.101
        ldp
        keep-alive
            shutdown
        exit
        no shutdown
    exit
```

Os *routers* 7210 SAS-M têm um comportamento ligeiramente diferente do habitual na verificação do MTU nas portas de acesso dos serviços. Normalmente antes do pacote ser encaminhado para o serviço, o tamanho da trama é verificado de acordo com o MTU do serviço. O *router* 7210 SAS-M inclui a *vlan tag* nesta verificação, logo o serviço

espera receber uma trama com um máximo de 1514 bytes e acaba por verificar que esta tem 1518 bytes (1514+4 bytes da *vlan tag*), resultando no descarte da trama. Assim, uma das soluções possíveis para contornar este mecanismo passa por aumentar o MTU do serviço para 1518 bytes, que neste caso foi a solução adotada como se pode verificar no seguinte exemplo.

```
A: MPLS-ESD# admin display-config
...
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
vpls 2 customer 1 svc-sap-type any create
            description "Segmento para transito Internet"
            service-mtu 1518
            discard-unknown
            stp
                shutdown
            exit
            sap 1/1/17 create
                egress
                exit
            exit
            sap 1/1/21 create
                egress
                exit
            exit
            mesh-sdp 11:2 create
                no shutdown
            exit
            mesh-sdp 35:2 create
                no shutdown
            exit
            mesh-sdp 37:2 create
                no shutdown
            exit
            mesh-sdp 42:2 create
                no shutdown
            exit
            mesh-sdp 43:2 create
                no shutdown
            exit
            mesh-sdp 44:2 create
                no shutdown
            exit
            mesh-sdp 64:2 create
                no shutdown
            exit
            no shutdown
        exit
```

Nos próximos capítulos serão apresentadas algumas soluções com o objetivo de melhorar as medidas de QoS da rede MPLS do IPL.

3. Soluções desenvolvidas para a melhoria de QoS da rede MPLS do IPL

Neste capítulo serão propostas algumas soluções com diferentes contornos e com o objetivo de melhorar os parâmetros de QoS da rede MPLS do IPL. As soluções apresentadas têm em vista a aplicação de um método de MPLS de uma forma geral, no entanto nada impede que os vários métodos sejam aplicados em conjunto para personalizar a rede às diferentes necessidades de QoS dos seus serviços.

A implementação das várias soluções foi realizada no laboratório Alcatel-Lucent do ISEL com a disposição representada na Figura 43. Este é constituído por três *routers* 7750 SR e seis *routers* 7705 SAR-F ambos da Alcatel-Lucent (Nokia). Note-se que as ligações por antenas de rádio não serão consideradas para esta representação devido à limitação de ligações disponíveis entre equipamentos no laboratório Alcatel-Lucent do ISEL. No entanto, estas ligações serão desativadas no futuro, deixando assim o cenário de testes mais próximo da topologia futura da rede MPLS do IPL.

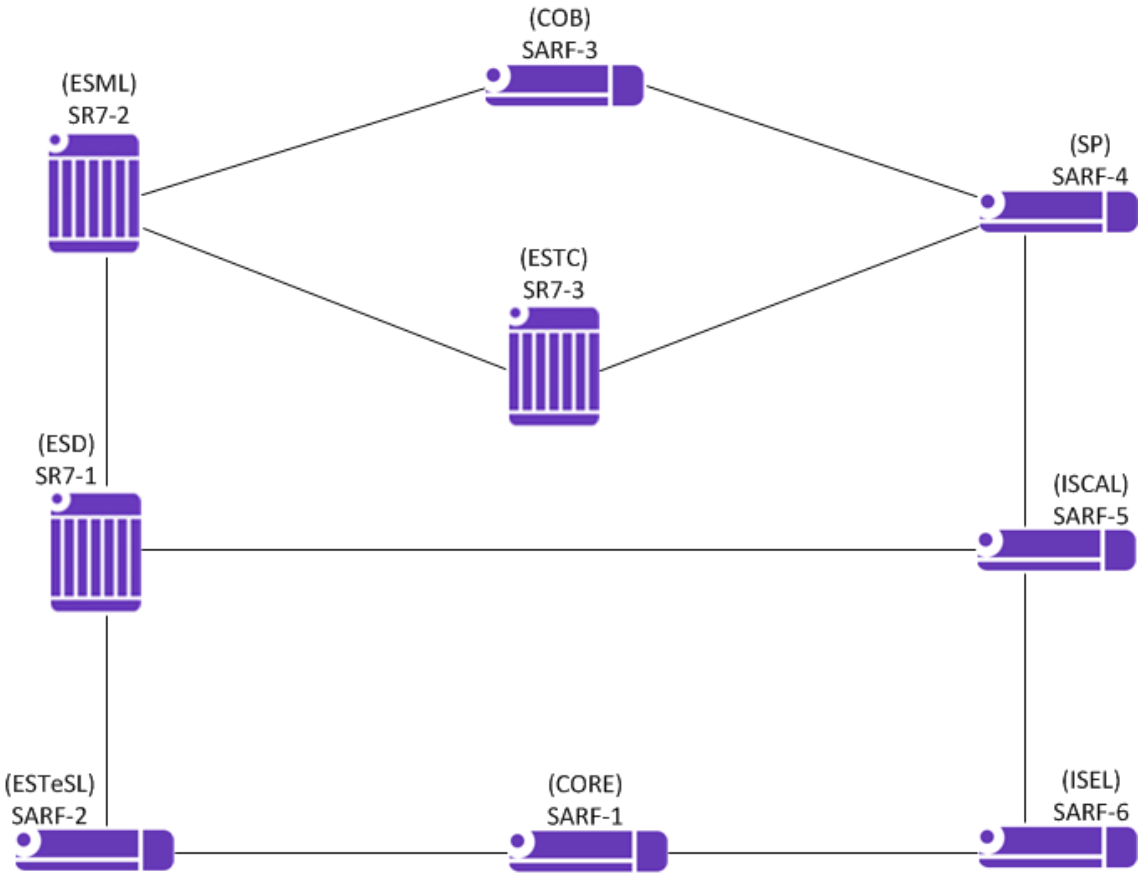

Figura 43 – Representação da rede MPLS do IPL no laboratório Alcatel-Lucent do ISEL.

3.1. Configuração base das soluções desenvolvidas

A topologia da rede do laboratório do ISEL foi organizada à imagem da rede MPLS do IPL, no entanto o endereçamento, configurações das interfaces, etc, diferem da rede

operacional. Assim na Figura 44 pode-se observar o tipo de ligação, a largura de banda, as portas utilizadas e os equipamentos do cenário de testes.

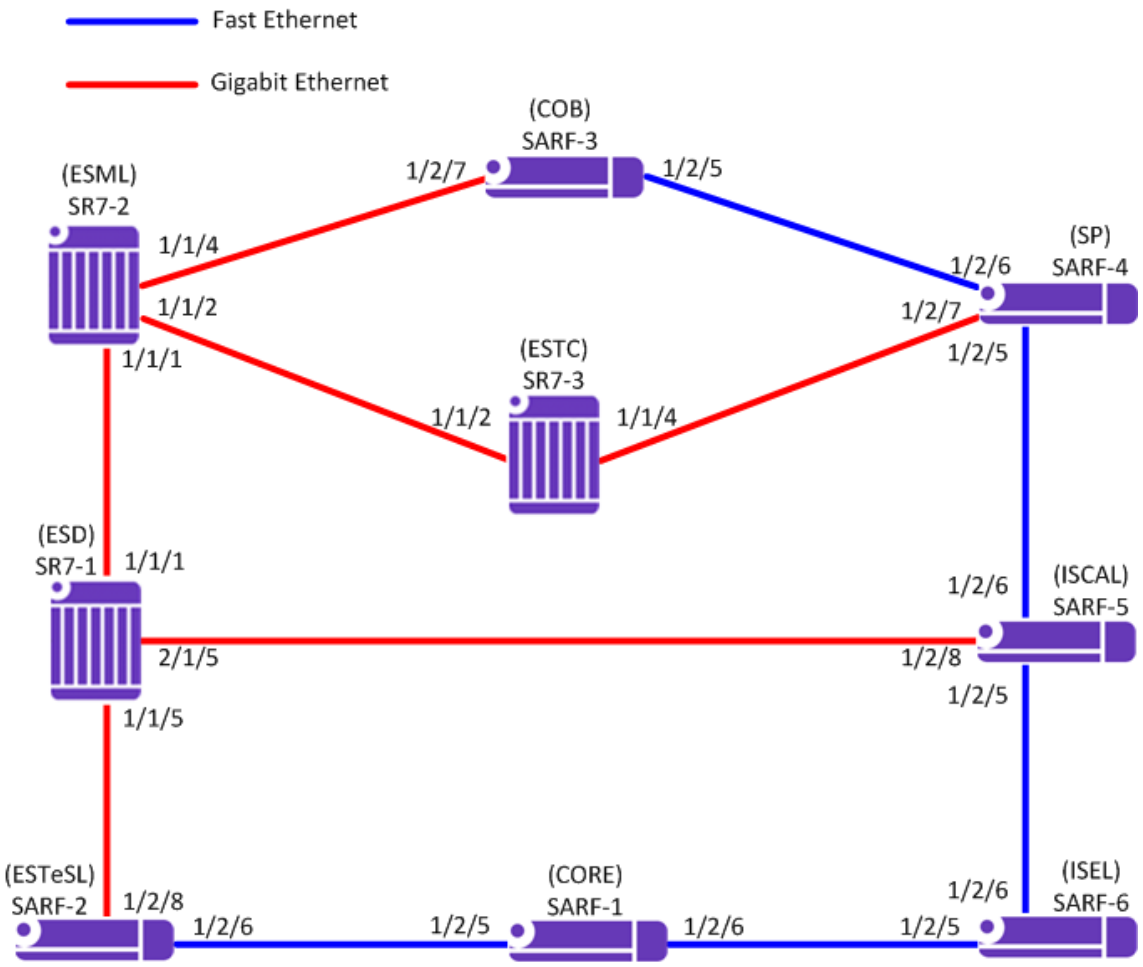

Figura 44 – Referência aos meios físicos que conectam os equipamentos no cenário de testes.

Todas as portas foram configuradas em modo network com o MTU de 2100 bytes, pois os *routers* 7705 SAR-F estão limitados ao valor máximo de 2106 bytes e não suportam *Jumbo frames* [16]. No entanto, para os testes realizados com serviços VPLS os pacotes poderão atingir no máximo os 1536 bytes, sendo que o MTU no mínimo teria de ser configurado para este valor.

Para simplificar a identificação de cada equipamento, foram atribuídos os seguintes números a cada equipamento:

SARF-1	**nº1**
SARF-2	**nº2**
SARF-3	**nº3**
SARF-4	**nº4**
SARF-5	**nº5**
SARF-6	**nº6**
SR7-1	**nº11**

SR7-2	**nº12**
SR7-3	**nº13**

Tabela 1 – Identificação de cada equipamento do cenário de testes.

3.1.1. Endereçamento IP

Seguindo a identificação anterior, os endereços da interface *System* dos equipamentos obedecem à seguinte regra:

$$\boldsymbol{x = nº\ equipamento}$$

Interface System	**192.168.0.x/32**

Tabela 2 – Regra de atribuição de endereços IP para interfaces *System*.

Todas as portas representadas na Figura 44 foram configuradas em modo *network*, logo todas as ligações são de nível 3 com um endereço IP atribuído. Desta forma a atribuição de endereços IP às ligações segue a seguinte regra:

$$\boldsymbol{x = nº\ equipamento\ (menor)}$$

$$\boldsymbol{y = nº\ equipamento\ (maior)}$$

Endereço IP da rede	**10.x.y.0/24**
Interface equipamento x	**10.x.y.x**
Interface equipamento y	**10.x.y.y**

Tabela 3 – Regra de atribuição de endereços IP para interfaces em modo *network*.

Tendo como exemplo a ligação entre **SARF-1 – SARF-2**:

Endereço IP da rede	**10.1.2.0/24**
Interface SARF-1	**10.1.2.1**
Interface SARF-2	**10.1.2.2**

Tabela 4 – Exemplo da atribuição de endereços IP a interfaces em modo *network*.

Na Figura 45 pode-se observar o cenário de testes com os endereços IP atribuídos.

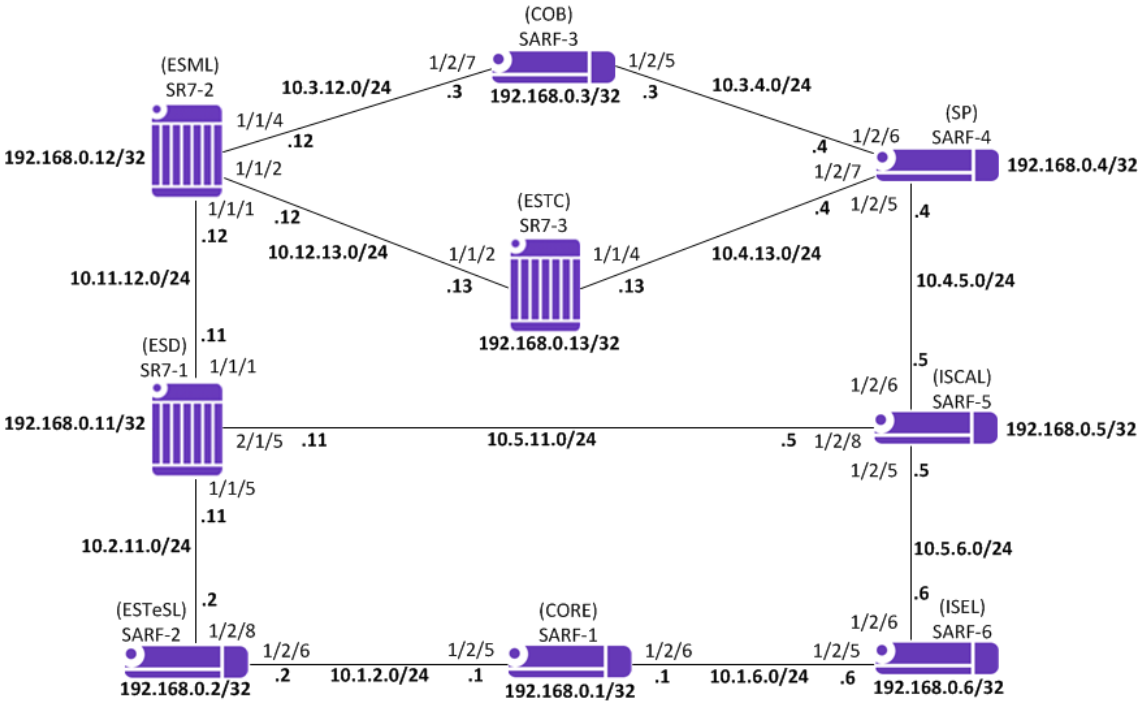

Figura 45 – Representação dos endereços IP atribuídos no cenário de testes.

3.1.2. Encaminhamento de pacotes

Como protocolo de encaminhamento de pacotes, à semelhança da rede MPLS do IPL, foi utilizado o OSPF *single-area*, assim todos os equipamentos pertencem à área 0.0.0.0. Existem dois tipos de ligação com diferentes larguras de banda entre os *routers* do cenário de testes, como se pode verificar na Figura 44. Para que estas diferenças não influenciem o cálculo do algoritmo SPF, foi configurada a métrica "100" para todas as ligações. Por fim foram ainda definidos os tempos de *hello* e *dead-interval* de acordo com a rede MPLS do IPL, como se pode verificar no seguinte exemplo de configuração do *router* SARF-1(CORE).

```
A:SARF-1(CORE)# admin display-config
...

#--------------------------------------------------
echo "OSPFv2 Configuration"
#--------------------------------------------------
        ospf
            area 0.0.0.0
                interface "system"
                exit
                interface "toSARF-2"
                    interface-type point-to-point
                    hello-interval 1
                    dead-interval 3
                    metric 100
                exit
                interface "toSARF-6"
                    interface-type point-to-point
                    hello-interval 1
                    dead-interval 3
                    metric 100
                exit
            exit
```

```
        exit
    exit
```

Na Figura 46 pode-se observar a tabela de encaminhamento do *router* SARF-1(CORE), que confirma a conectividade entre todos os equipamentos e que a métrica está de acordo com o que foi definido.

```
*A:SARF-1(CORE)# show router route-table
```

```
===============================================================================
Route Table (Router: Base)
===============================================================================
Dest Prefix                                       Type    Proto     Age          Pref
       Next Hop[Interface Name]                                          Metric
-------------------------------------------------------------------------------
10.1.2.0/24                                       Local   Local     00h08m38s    0
       toSARF-2                                                            0
10.1.6.0/24                                       Local   Local     00h08m38s    0
       toSARF-6                                                            0
10.2.11.0/24                                      Remote  OSPF      00h07m51s    10
       10.1.2.2                                                          200
10.3.4.0/24                                       Remote  OSPF      00h08m31s    10
       10.1.6.6                                                          400
10.3.12.0/24                                      Remote  OSPF      00h07m47s    10
       10.1.2.2                                                          400
10.4.5.0/24                                       Remote  OSPF      00h08m31s    10
       10.1.6.6                                                          300
10.4.13.0/24                                      Remote  OSPF      00h07m54s    10
       10.1.6.6                                                          400
10.5.6.0/24                                       Remote  OSPF      00h08m31s    10
       10.1.6.6                                                          200
10.5.11.0/24                                      Remote  OSPF      00h07m49s    10
       10.1.2.2                                                          300
10.11.12.0/24                                     Remote  OSPF      00h07m49s    10
       10.1.2.2                                                          300
10.12.13.0/24                                     Remote  OSPF      00h07m49s    10
       10.1.2.2                                                          400
192.168.0.1/32                                    Local   Local     00h08m41s    0
       system                                                              0
192.168.0.2/32                                    Remote  OSPF      00h08m33s    10
       10.1.2.2                                                          100
192.168.0.3/32                                    Remote  OSPF      00h07m49s    10
       10.1.2.2                                                          400
192.168.0.4/32                                    Remote  OSPF      00h08m33s    10
       10.1.6.6                                                          300
192.168.0.5/32                                    Remote  OSPF      00h08m33s    10
       10.1.6.6                                                          200
192.168.0.6/32                                    Remote  OSPF      00h08m33s    10
       10.1.6.6                                                          100
192.168.0.11/32                                   Remote  OSPF      00h07m49s    10
       10.1.2.2                                                          200
192.168.0.12/32                                   Remote  OSPF      00h07m49s    10
       10.1.2.2                                                          300
192.168.0.13/32                                   Remote  OSPF      00h07m49s    10
       10.1.2.2                                                          400
-------------------------------------------------------------------------------
No. of Routes: 20
===============================================================================
```

Figura 46 – Tabela de encaminhamento do *router* SARF-1(CORE).

Os próximos capítulos irão apresentar várias configurações MPLS, tendo todas por base a configuração referida neste capítulo.

3.2. Recriação da configuração da rede MPLS do IPL na rede do laboratório do ISEL

Para que seja possível comparar a configuração atual da rede MPLS do IPL com as soluções desenvolvidas, foi simulada a configuração operacional no laboratório. Nesta foram apenas configuradas as opções em uso. Assim, apenas o protocolo LDP foi configurado como se pode observar no seguinte exemplo de configuração no *router* SARF-1(CORE) e nos anexos **Error! Reference source not found.**.

```
A:SARF-1(CORE)# admin display-config
...

#--------------------------------------------------
echo "LDP Configuration"
#--------------------------------------------------
        ldp
            interface-parameters
                interface "toSARF-2"
                exit
                interface "toSARF-6"
                exit
            exit
            targeted-session
            exit
        exit
    exit
```

O protocolo LDP distribui *labels* para atingir os *routers* LDP, sendo apenas necessário definir em cada *router* LDP as interfaces que fazem parte da rede MPLS. Na Figura 47 pode-se observar as sessões LDP criadas após a configuração anterior.

```
*A:SARF-1(CORE)>show>router>ldp# session

===============================================================================
LDP Sessions
===============================================================================
Peer LDP Id        Adj Type   State         Msg Sent  Msg Recv  Up Time
-------------------------------------------------------------------------------
192.168.0.2:0      Both       Established   581       587       0d 00:21:58
192.168.0.3:0      Targeted   Established   241       244       0d 00:21:45
192.168.0.4:0      Targeted   Established   240       244       0d 00:21:45
192.168.0.5:0      Targeted   Established   240       243       0d 00:21:45
192.168.0.6:0      Both       Established   578       579       0d 00:21:58
192.168.0.11:0     Targeted   Established   233       236       0d 00:21:04
192.168.0.12:0     Targeted   Established   233       235       0d 00:21:03
192.168.0.13:0     Targeted   Established   233       236       0d 00:21:04
-------------------------------------------------------------------------------
No. of Sessions: 8
===============================================================================
```

Figura 47 – Sessões LDP estabelecidas no *router* SARF-1(CORE).

Com as sessões LDP já estabelecidas são trocadas as *labels* entre todos os *routers*. Na Figura 48 pode-se observar a tabela de *labels* LDP no *router* SARF-1(CORE).

```
*A:SARF-1(CORE)>show>router>ldp# bindings

===============================================================================
LDP LSR ID: 192.168.0.1
===============================================================================
Legend: U - Label In Use, N - Label Not In Use, W - Label Withdrawn
        S - Status Signaled Up,  D - Status Signaled Down
        E - Epipe Service, V - VPLS Service, M - Mirror Service
        A - Apipe Service, F - Fpipe Service, I - IES Service, R - VPRN service
        P - Ipipe Service, WP - Label Withdraw Pending, C - Cpipe Service
        TLV - (Type, Length: Value), H - Hpipe Service
===============================================================================
LDP Prefix Bindings
===============================================================================
Prefix              Peer            IngLbl    EgrLbl EgrIntf/    EgrNextHop
                                                     LspId
-------------------------------------------------------------------------------
192.168.0.1/32      192.168.0.2     131071U     --      --          --
192.168.0.1/32      192.168.0.6     131071U     --      --          --
192.168.0.2/32      192.168.0.2       --      131071 1/2/5       10.1.2.2
192.168.0.2/32      192.168.0.6     131065U   131066   --          --
192.168.0.3/32      192.168.0.2     131068N   131058 1/2/5       10.1.2.2
192.168.0.3/32      192.168.0.6     131068U   131069   --          --
192.168.0.4/32      192.168.0.2     131067U   131066   --          --
192.168.0.4/32      192.168.0.6     131067N   131068 1/2/6       10.1.6.6
192.168.0.5/32      192.168.0.2     131066U   131065   --          --
192.168.0.5/32      192.168.0.6     131066N   131067 1/2/6       10.1.6.6
192.168.0.6/32      192.168.0.2     131069U   131068   --          --
192.168.0.6/32      192.168.0.6       --      131071 1/2/6       10.1.6.6
192.168.0.11/32     192.168.0.2     131059N   131059 1/2/5       10.1.2.2
192.168.0.11/32     192.168.0.6     131059U   131060   --          --
192.168.0.12/32     192.168.0.2     131058N   131057 1/2/5       10.1.2.2
192.168.0.12/32     192.168.0.6     131058U   131059   --          --
192.168.0.13/32     192.168.0.2     131057N   131053 1/2/5       10.1.2.2
192.168.0.13/32     192.168.0.6     131057U   131058   --          --
-------------------------------------------------------------------------------
No. of Prefix Bindings: 18
```

Figura 48 – *Labels* LDP recebidas e transmitidas no *router* SARF-1(CORE).

A partir da tabela de *labels* da imagem anterior, será feita uma seleção das *labels* que serão utilizadas com base na tabela de encaminhamento. Na Figura 49 pode-se observar as *label* LDP ativas no *router* SARF-1(CORE).

```
*A:SARF-1(CORE)# show router ldp bindings active

===============================================================================
Legend:  (S) - Static
===============================================================================
LDP Prefix Bindings (Active)
===============================================================================
Prefix                  Op    IngLbl    EgrLbl    EgrIntf/LspId  EgrNextHop
-------------------------------------------------------------------------------
192.168.0.1/32          Pop   131071      --        --             --
192.168.0.2/32          Push    --      131071    1/2/5          10.1.2.2
192.168.0.2/32          Swap  131065    131071    1/2/5          10.1.2.2
192.168.0.3/32          Push    --      131058    1/2/5          10.1.2.2
192.168.0.3/32          Swap  131068    131058    1/2/5          10.1.2.2
192.168.0.4/32          Push    --      131068    1/2/6          10.1.6.6
192.168.0.4/32          Swap  131067    131068    1/2/6          10.1.6.6
192.168.0.5/32          Push    --      131067    1/2/6          10.1.6.6
192.168.0.5/32          Swap  131066    131067    1/2/6          10.1.6.6
192.168.0.6/32          Push    --      131071    1/2/6          10.1.6.6
192.168.0.6/32          Swap  131069    131071    1/2/6          10.1.6.6
192.168.0.11/32         Push    --      131059    1/2/5          10.1.2.2
192.168.0.11/32         Swap  131059    131059    1/2/5          10.1.2.2
192.168.0.12/32         Push    --      131057    1/2/5          10.1.2.2
192.168.0.12/32         Swap  131058    131057    1/2/5          10.1.2.2
192.168.0.13/32         Push    --      131053    1/2/5          10.1.2.2
192.168.0.13/32         Swap  131057    131053    1/2/5          10.1.2.2
-------------------------------------------------------------------------------
No. of Prefix Bindings: 17
===============================================================================
```

Figura 49 – Representação da tabela de *label* LDP ativas no *router* SARF-1(CORE).

Em caso de falha de rede, a tabela das *labels* ativas será alterada após o cálculo do novo caminho para a tabela de encaminhamento. De forma a provocar uma falha na rede, introduziu-se o comando "*shutdown*" na porta 1/2/5 do *router* SARF-6(ISEL). Na Figura 50 podem ser observadas as *label* LDP em uso após a recuperação da falha no *router* SARF-1(CORE).

```
*A:SARF-1(CORE)# show router ldp bindings active

===============================================================================
Legend:  (S) - Static
===============================================================================
LDP Prefix Bindings (Active)
===============================================================================
Prefix                  Op    IngLbl    EgrLbl    EgrIntf/LspId  EgrNextHop
-------------------------------------------------------------------------------
192.168.0.1/32          Pop   131071      --        --             --
192.168.0.2/32          Push    --      131071    1/2/5          10.1.2.2
192.168.0.3/32          Push    --      131058    1/2/5          10.1.2.2
192.168.0.4/32          Push    --      131066    1/2/5          10.1.2.2
192.168.0.5/32          Push    --      131065    1/2/5          10.1.2.2
192.168.0.6/32          Push    --      131064    1/2/5          10.1.2.2
192.168.0.11/32         Push    --      131059    1/2/5          10.1.2.2
192.168.0.12/32         Push    --      131057    1/2/5          10.1.2.2
192.168.0.13/32         Push    --      131056    1/2/5          10.1.2.2
-------------------------------------------------------------------------------
No. of Prefix Bindings: 9
===============================================================================
```

Figura 50 – Representação da tabela de *label* LDP ativas no *router* SARF-1(CORE) após o corte de rede provocado.

3.2.1. Discussão

A configuração atual da rede MPLS do IPL utiliza os mesmos caminhos definidos pelo protocolo IGP, sem balanceamento da rede. Com o protocolo LDP não é possível

controlar o caminho estabelecido pelos LSP e a recuperação da rede a falhas depende do protocolo IGP. Esta terá ainda a mesma escalabilidade que a rede IP que a suporta.

3.3. Solução de balanceamento dinâmico

Esta solução tem como objetivo que os LSP sejam estabelecidos de forma dinâmica com o protocolo RSVP. Através da reserva de largura de banda nas ligações espera-se obter um balanceando dinâmico da rede.

A reserva de LB é realizada ao nível de controlo, ou seja esta reserva não tem efeito no ritmo de tráfego que passa na ligação. Afeta apenas o número de LSP que se podem estabelecer na ligação. A implementação desta solução terá como principal desafio a definição de um critério de atribuição de LB a cada LSP.

3.3.1. Resiliência

Sendo esta uma solução dinâmica requer também uma resiliência dinâmica, ou seja FRR. Poderia ter sido utilizado qualquer um dos modos de FRR, no entanto optou-se pelo modo *facility*, devido à possibilidade dos túneis *bypass* serem partilhados pelos vários LSP, reduzindo assim o número de túneis FRR necessários. Desta forma, a resiliência dos LSP está garantida independentemente do caminho estabelecido. Opcionalmente, no caso de o *primary-path* e de o túnel de *bypass* serem ambos afetados pelas falhas de rede, poderá ser configurado um *Cold-standby secondary-path* sem restrições para recuperar o tráfego. Assim, se existir um caminho disponível que seja excluído do recalculo do *primary-path* devido às restrições aplicadas, o *Cold-standby secondary-path* poderá recuperar o tráfego.

3.3.2. Configuração

Esta solução tem como desafio a atribuição de LB a cada LSP para que todos os LSP se consigam estabelecer e que a largura de banda reservável de cada ligação seja preenchida. Assim, procurou-se um valor de reserva de LB que permita o seguinte compromisso:

- Todos os LSP sejam estabelecidos.
- Maximizar a reserva de LB nas ligações.

Note-se que tal como foi explicado no capítulo 1.5.4.6, a reserva da LB é realizada apenas à saída do equipamento, ou seja numa ligação existem duas larguras de banda reserváveis, uma em cada sentido. A largura de banda máxima em algumas ligações do laboratório é de 100 Mb/s, logo foram apenas considerados disponíveis para reserva 100 Mb/s bidirecionais em todas as ligações. Nas ligações com 1 Gb/s de largura de banda foi aplicado dentro da secção RSVP-TE o comando "*subscription* 10" que disponibiliza apenas 10% da largura de banda, ou seja 100 Mb/s para as reservas de LB como se pode ver no seguinte exemplo de configuração.

```
A:SR7-1(ESD)# admin display-config
...

#--------------------------------------------------
```

```
echo "RSVP Configuration"
#------------------------------------------------
        rsvp
            interface "system"
                no shutdown
            exit
            interface "toSARF-2"
                subscription 10
                no shutdown
            exit
            interface "toSARF-5"
                subscription 10
                no shutdown
            exit
            interface "toSR7-2"
                subscription 10
                no shutdown
            exit
            no shutdown
        exit
```

Realizou-se um mapeamento balanceado de todos os LSP que vão ser estabelecidos em cada equipamento, como se pode verificar na Figura 51 o exemplo para o caso do *router* SARF-1(CORE).

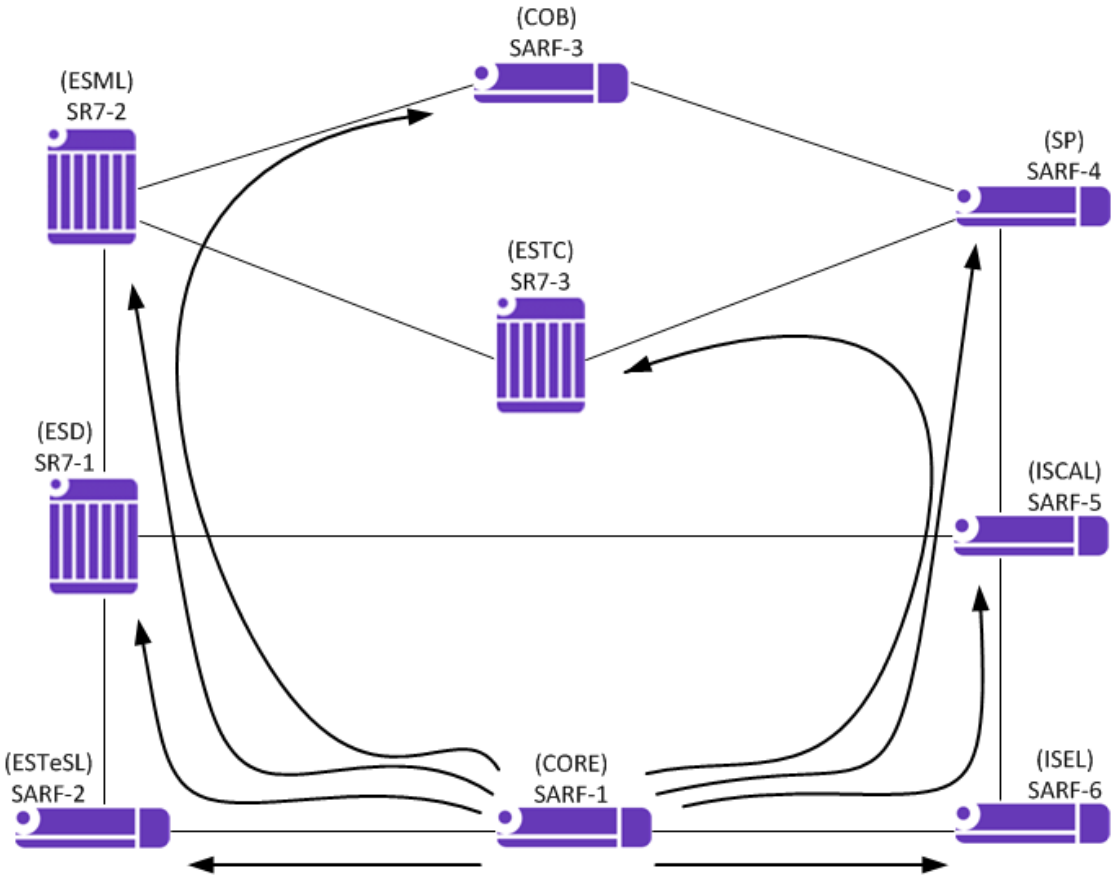

Figura 51 – Representação do mapeamento ideal dos LSP com origem no *router* SARF-1(CORE).

O resultado do mapeamento de todos os LSP pode-se observar nos anexos **Error! Reference source not found.**. Na Figura 52 está representado o número de LSP estabelecidos em cada ligação e em cada direção.

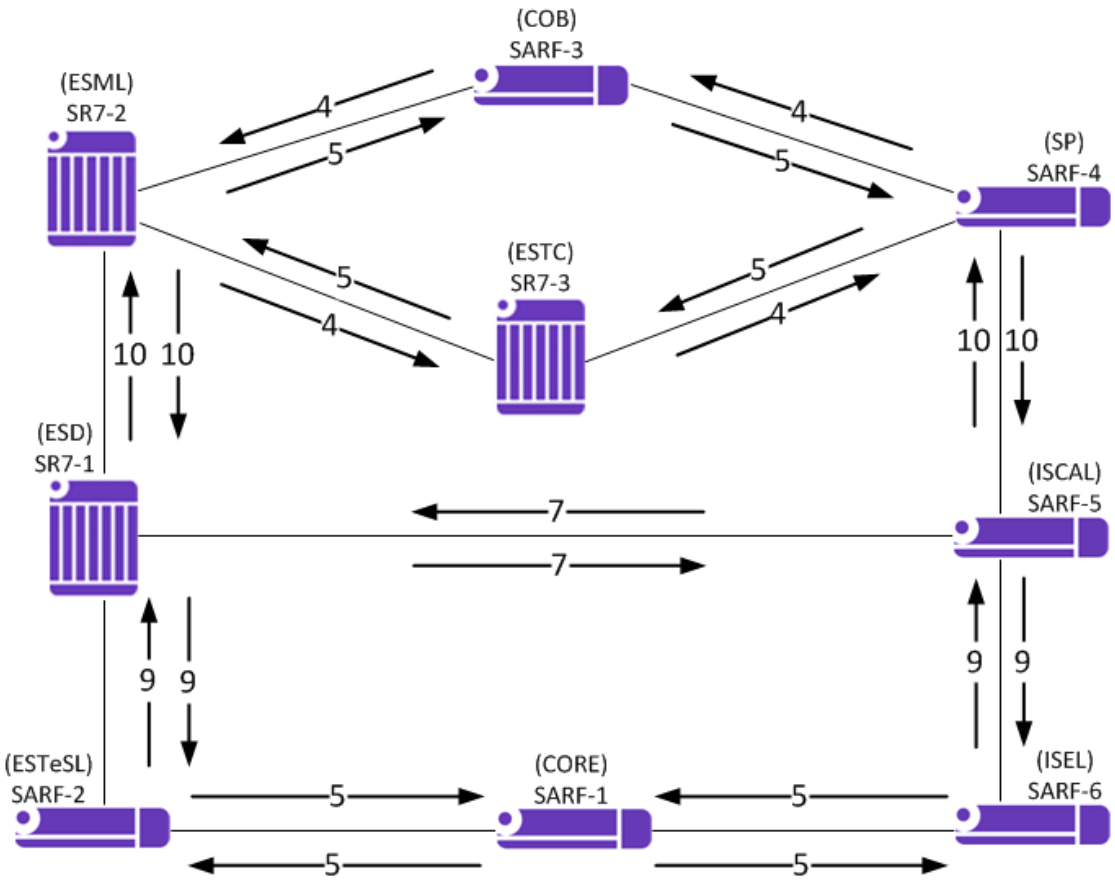

Figura 52 – Resultado do mapeamento de todos os LSP em cada ligação e direção.

Na figura anterior pode-se verificar que a ligação mais sobrecarregada tem um máximo de 10 LSP em cada direção. Assim o valor de LB a atribuir a cada LSP pode ser calculado através de:

$$LSP_{LB} = \frac{100\ Mb/s}{10LSP} = 10\ Mb/s/LSP$$

Desta forma foi definido que cada LSP reserva 10 Mb/s de LB. Este valor irá permitir teoricamente que todos os LSP se estabeleçam, enquanto que o uso da largura de banda é maximizado. Note-se que os 10 Mb/s são um valor de *control plane*, ou seja controla apenas o número de LSP que podem ser estabelecidos numa determinada ligação de acordo com a largura de banda que pretendem ocupar. Para estender este controlo ao *data plane* seria necessário configurar regras de policiamento de QoS.

Após a definição da reserva de LB a aplicar, foram configurados 8 LSP em cada equipamento com o protocolo RSVP-TE. Todos os LSP utilizam o *path* "*Loose*", que foi configurado sem *hops* definidos. A opção *"*cspf*"* é necessária para permitir o uso da restrição de largura de banda de 10 Mb/s e para obter a resiliência através do FRR *facility*. O balanceamento pode ainda ser melhorado com a opção "*least-fill*", esta estabelece o LSP pelo caminho com menos LB reservada caso existam vários caminhos com a mesma métrica IGP à sua disposição. No seguinte exemplo de configuração, pode-se observar a configuração MPLS desenvolvida no *router* SARF-1(CORE) e nos anexos **Error! Reference source not found.**.

```
A:SARF-1(CORE)# admin display-config
...

#--------------------------------------------------
echo "MPLS LSP Configuration"
#--------------------------------------------------
        mpls
            path "Loose"
                no shutdown
            exit
            lsp "toSARF2(ESTeSL)"
                to 192.168.0.2
                cspf
                fast-reroute facility
                exit
                least-fill
                primary "Loose"
                    bandwidth 10
                exit
                no shutdown
            exit
            lsp "toSARF3(COB)"
                to 192.168.0.3
                cspf
                fast-reroute facility
                exit
                least-fill
                primary "Loose"
                    bandwidth 10
                exit
                no shutdown
            exit
            lsp "toSARF4(SP)"
                to 192.168.0.4
                cspf
                fast-reroute facility
                exit
                least-fill
                primary "Loose"
                    bandwidth 10
                exit
                no shutdown
            exit
            lsp "toSARF5(ISCAL)"
                to 192.168.0.5
                cspf
                fast-reroute facility
                exit
                least-fill
                primary "Loose"
                    bandwidth 10
                exit
                no shutdown
            exit
            lsp "toSARF6(ISEL)"
                to 192.168.0.6
                cspf
                fast-reroute facility
                exit
                least-fill
                primary "Loose"
                    bandwidth 10
                exit
                no shutdown
            exit
            lsp "toSR71(ESD)"
                to 192.168.0.11
                cspf
```

```
                fast-reroute facility
                exit
                least-fill
                primary "Loose"
                    bandwidth 10
                exit
                no shutdown
            exit
            lsp "toSR72(ESML)"
                to 192.168.0.12
                cspf
                fast-reroute facility
                exit
                least-fill
                primary "Loose"
                    bandwidth 10
                exit
                no shutdown
            exit
            lsp "toSR73(ESTC)"
                to 192.168.0.13
                cspf
                fast-reroute facility
                exit
                least-fill
                primary "Loose"
                    bandwidth 10
                exit
                no shutdown
            exit
            no shutdown
        exit
```

Na Figura 53 pode-se observar que todos os LSP do *router* SARF-1(CORE) se conseguiram estabelecer, servindo de exemplo para todos os outros *routers*.

```
*A:SARF-1(CORE)>show>router>mpls# lsp

===============================================================================
MPLS LSPs (Originating)
===============================================================================
LSP Name                        To              Fastfail Config   Adm   Opr
-------------------------------------------------------------------------------
toSARF2(ESTeSL)                 192.168.0.2     Yes               Up    Up
toSARF3(COB)                    192.168.0.3     Yes               Up    Up
toSARF4(SP)                     192.168.0.4     Yes               Up    Up
toSARF5(ISCAL)                  192.168.0.5     Yes               Up    Up
toSARF6(ISEL)                   192.168.0.6     Yes               Up    Up
toSR71(ESD)                     192.168.0.11    Yes               Up    Up
toSR72(ESML)                    192.168.0.12    Yes               Up    Up
toSR73(ESTC)                    192.168.0.13    Yes               Up    Up
-------------------------------------------------------------------------------
LSPs : 8
===============================================================================
```

Figura 53 – Estado dos LSP no *router* SARF-1(CORE).

Na Figura 54 pode-se verificar que o caminho estabelecido pelo LSP "toSARF5(ISCAL)" coincide com aquele que foi mapeado anteriormente. Note-se que a largura de banda é de 10 Mb/s e que o FRR gerou uma proteção de *link* e de *node* no primeiro troço e apenas de *link* no segundo troço que liga ao eLER.

```
*A:SARF-1(CORE)>show>router>mpls# lsp toSARF5(ISCAL) path detail

===============================================================================
MPLS LSP toSARF5(ISCAL) Path  (Detail)
===============================================================================
Legend :
    @ - Detour Available                # - Detour In Use
    b - Bandwidth Protected             n - Node Protected
    s - Soft Preemption
===============================================================================
-------------------------------------------------------------------------------
LSP toSARF5(ISCAL) Path Loose
-------------------------------------------------------------------------------
LSP Name     : toSARF5(ISCAL)                  Path LSP ID : 29696
From         : 192.168.0.1                     To          : 192.168.0.5
Adm State    : Up                              Oper State  : Up
Path Name    : Loose                           Path Type   : Primary
Path Admin   : Up                              Path Oper   : Up
OutInterface: 1/2/6                            Out Label   : 131056
Path Up Time: 0d 01:41:38                      Path Dn Time: 0d 00:00:00
Retry Limit : 0                                Retry Timer : 30 sec
RetryAttempt: 0                                NextRetryIn : 0 sec
SetupPriori*: 7                                Hold Priori*: 0
Bandwidth    : 10 Mbps                         Oper Bw     : 10 Mbps
Hop Limit    : 255                             Class Type  : 0
Record Route: Record                           Record Label: Record
Oper MTU     : 2082                            Neg MTU     : 2082
Adaptive     : Enabled                         Oper Metric : 200
Include Grps:                                  Exclude Grps:
None                                          None
Path Trans   : 1                               CSPF Queries: 1
Failure Code: noError                          Failure Node: n/a
ExplicitHops:
    No Hops Specified
Actual Hops :
    10.1.6.1(192.168.0.1) @ n                  Record Label    : N/A
 -> 10.1.6.6(192.168.0.6) @                    Record Label    : 131056
 -> 10.5.6.5(192.168.0.5)                      Record Label    : 131053
ComputedHops:
    10.1.6.1        -> 10.1.6.6        -> 10.5.6.5
ResigEligib*: False
LastResignal: n/a                              CSPF Metric : 200
===============================================================================
```

Figura 54 – Características detalhadas do LSP "toSARF5(ISCAL)".

No entanto, verificou-se que nem sempre os LSP se estabeleceram pelos caminhos previstos pelo mapeamento. Este comportamento deve-se ao facto de os *routers* terem ligeiras diferenças nos tempos de *boot*, o que leva a que alguns LSP se estabeleçam pelos caminhos alternativos que estão disponíveis no momento. Na Figura 55 pode-se observar a diferença entre o caminho esperado e o estabelecido numa destas situações.

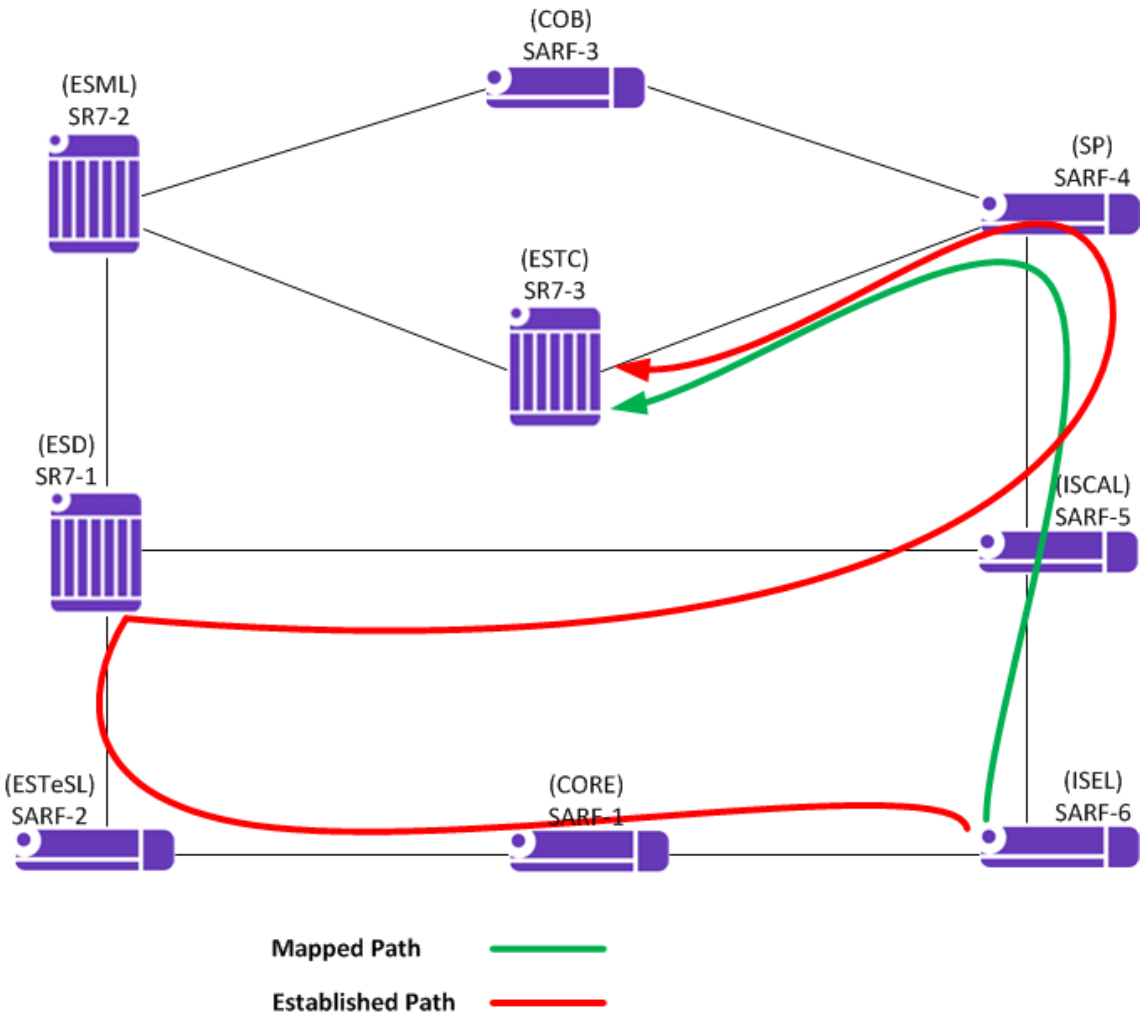

Figura 55 – Caminho mapeado VS caminho estabelecido pelo LSP "toSR73(ESTC)" no *router* SARF-6(ISEL).

Na Figura 56 pode-se observar em detalhe o caminho estabelecido pelo LSP "toSR73(ESTC)" no *router* SARF-6(ISEL).

```
*A:SARF-6(ISEL)# show router mpls lsp toSR73(ESTC) path detail

===============================================================================
MPLS LSP toSR73(ESTC) Path  (Detail)
===============================================================================
Legend :
    @ - Detour Available                # - Detour In Use
    b - Bandwidth Protected             n - Node Protected
    s - Soft Preemption
===============================================================================
-------------------------------------------------------------------------------
LSP toSR73(ESTC) Path Loose
-------------------------------------------------------------------------------
LSP Name     : toSR73(ESTC)                       Path LSP ID : 52228
From         : 192.168.0.6                        To          : 192.168.0.13
Adm State    : Up                                 Oper State  : Up
Path Name    : Loose                              Path Type   : Primary
Path Admin   : Up                                 Path Oper   : Up
OutInterface: 1/2/5                               Out Label   : 131024
Path Up Time: 0d 02:45:56                         Path Dn Time: 0d 00:00:00
Retry Limit : 0                                   Retry Timer : 30 sec
RetryAttempt: 0                                   NextRetryIn : 0 sec
SetupPriori*: 7                                   Hold Priori*: 0
Bandwidth    : 10 Mbps                            Oper Bw     : 10 Mbps
Hop Limit    : 255                                Class Type  : 0
Record Route: Record                              Record Label: Record
Oper MTU     : 2082                               Neg MTU     : 2082
Adaptive     : Enabled                            Oper Metric : 600
Include Grps:                                     Exclude Grps:
None                                            None
Path Trans   : 1                                  CSPF Queries: 4
Failure Code: noError                             Failure Node: n/a
ExplicitHops:
    No Hops Specified
Actual Hops :
    10.1.6.6(192.168.0.6) @ n                     Record Label    : N/A
 -> 10.1.6.1(192.168.0.1) @ n                     Record Label    : 131024
 -> 10.1.2.2(192.168.0.2) @ n                     Record Label    : 131026
 -> 10.2.11.11(192.168.0.11) @ n                  Record Label    : 131015
 -> 10.5.11.5(192.168.0.5) @ n                    Record Label    : 131022
 -> 10.4.5.4(192.168.0.4) @                       Record Label    : 131034
 -> 10.4.13.13(192.168.0.13)                      Record Label    : 131032
ComputedHops:
    10.1.6.6        -> 10.1.6.1        -> 10.1.2.2        -> 10.2.11.11
 -> 10.5.11.5       -> 10.4.5.4        -> 10.4.13.13
ResigEligib*: False
LastResignal: n/a                                 CSPF Metric : 600
===============================================================================
```

Figura 56 – Caminho alternativo estabelecido pelo LSP "toSR73(ESTC)" no *router* SARF-6(ISEL).

A largura de banda de algumas ligações foi inesperadamente ocupada obrigando também os restantes LSP a estabelecerem-se por caminhos alternativos, verificando-se ainda situações em que alguns LSP não se conseguiram estabelecer. Na Figura 57 pode-se verificar que a interface "toSARF-5" do *router* SARF-6(ISEL) tem a largura de banda completamente reservada, o que levou a que alguns LSP se estabelecessem por caminhos alternativos.

```
*A:SARF-6(ISEL)>show>router>rsvp# interface

===============================================================================
RSVP Interfaces
===============================================================================
Interface                        Total     Active    Total BW  Resv BW   Adm Opr
                                 Sessions  Sessions  (Mbps)    (Mbps)
-------------------------------------------------------------------------------
system                           -         -         -         -         Up  Up
toSARF-1                         19        19        100       100       Up  Up
toSARF-5                         18        18        100       100       Up  Up
-------------------------------------------------------------------------------
Interfaces : 3
===============================================================================
```

Figura 57 – Largura de banda reservada nas interfaces do *router* SARF-6(ISEL).

Na Figura 58 pode-se observar a reserva de 100 Mb/s de largura de banda nas interfaces do *router* SARF-1(CORE), onde seria de esperar 50 Mb/s de largura de banda reservada.

```
*A:SARF-1(CORE)>show>router>rsvp# interface

===============================================================================
RSVP Interfaces
===============================================================================
Interface                        Total     Active    Total BW  Resv BW   Adm Opr
                                 Sessions  Sessions  (Mbps)    (Mbps)
-------------------------------------------------------------------------------
system                           -         -         -         -         Up  Up
toSARF-2                         19        19        100       100       Up  Up
toSARF-6                         19        19        100       100       Up  Up
-------------------------------------------------------------------------------
Interfaces : 3
===============================================================================
```

Figura 58 – Largura de banda reservada nas interfaces do *router* SARF-1(CORE).

Nas figuras anteriores pode-se verificar que as interfaces têm 19 sessões estabelecidas, quando no máximo deveriam apresentar 10 sessões devido à limitação da reserva de LB. Estes valores devem-se aos túneis de *bypass* criados pelo FRR, no entanto os 9 túneis de *bypass* estabelecidos através do *router* SARF-1(CORE) não reservam largura de banda. Na Figura 59 pode-se observar que em relação ao planeamento transitam no total mais cinco LSP e ainda os 9 túneis *bypass* do FRR no *router* SARF-1(CORE).

```
*A:SARF-1(CORE)>show>router>rsvp# session transit

===============================================================================
RSVP Sessions
===============================================================================
From            To              Tunnel  LSP   Name                        State
                                ID      ID
-------------------------------------------------------------------------------
192.168.0.6     192.168.0.2     2       29184 toSARF2(ESTeSL)::Loose      Up
192.168.0.2     192.168.0.6     5       4608  toSARF6(ISEL)::Loose        Up
192.168.0.3     192.168.0.2     2       41984 toSARF2(ESTeSL)::Loose      Up
192.168.0.2     192.168.0.5     4       43008 toSARF5(ISCAL)::Loose       Up
192.168.0.2     192.168.0.4     3       18432 toSARF4(SP)::Loose          Up
192.168.0.2     192.168.0.3     2       20480 toSARF3(COB)::Loose         Up
192.168.0.4     192.168.0.2     2       6656  toSARF2(ESTeSL)::Loose      Up
192.168.0.5     192.168.0.2     2       21504 toSARF2(ESTeSL)::Loose      Up
192.168.0.5     10.1.6.6        63508   2     bypass-link10.5.6.6         Up
192.168.0.6     10.3.4.4        63505   2     bypass-node192.168.0.5      Up
192.168.0.11    10.1.6.6        61440   2     bypass-node192.168.0.5      Up
192.168.0.12    10.1.2.2        61443   6     bypass-node192.168.0.11     Up
192.168.0.4     10.1.6.6        63502   2     bypass-node192.168.0.5      Up
192.168.0.13    10.2.11.11      61441   4     bypass-node192.168.0.12     Up
192.168.0.11    10.1.2.2        61443   8     bypass-link10.2.11.2        Up
192.168.0.11    10.5.6.5        61444   10    bypass-link10.5.11.5        Up
192.168.0.13    192.168.0.6     6       51200 toSARF6(ISEL)::Loose        Up
192.168.0.6     10.2.11.11      63507   6     bypass-node192.168.0.5      Up
192.168.0.5     10.2.11.11      63512   10    bypass-link10.5.11.11       Up
192.168.0.2     10.5.11.11      63495   6     bypass-link10.2.11.11       Up
192.168.0.2     10.12.13.12     63496   8     bypass-node192.168.0.11     Up
192.168.0.11    192.168.0.6     5       42496 toSARF6(ISEL)::Loose        Up
192.168.0.6     10.5.11.5       63509   10    bypass-link10.5.6.5         Up
192.168.0.6     192.168.0.12    7       39938 toSR72(ESML)::Loose         Up
192.168.0.6     192.168.0.13    8       52228 toSR73(ESTC)::Loose         Up
192.168.0.2     10.5.6.5        63497   10    bypass-node192.168.0.11     Up
-------------------------------------------------------------------------------
Sessions : 26
===============================================================================
```

Figura 59 – Túneis MPLS-RSVP que transitam através do *router* SARF-1(CORE).

Note-se que na figura anterior estava apenas previsto a transição dos seguintes LSP:

- **toSARF2(ESTeSL)** de 192.168.0.6 para 192.168.0.2
- **toSARF6(ISEL)** de 192.168.0.2 para 192.168.0.6

Os restantes LSP não estavam previstos, fazendo assim um total de 6 LSP em cada ligação. Adicionando a esta contagem os 4 LSP com origem no SARF-1(CORE) em cada ligação, de acordo com o planeamento da Figura 51, temos um total de 10 LSP e uma reserva de 100 Mb/s como se verifica na Figura 58.

Na Figura 60 pode-se verificar os túneis de *bypass* com origem no *router* SARF-1(CORE) e ainda os LSP que estes protegem.

```
*A:SARF-1(CORE)>show>router>mpls# bypass-tunnel protected-lsp
===============================================================================
MPLS Bypass Tunnels
===============================================================================
Legend :  m - Manual      d - Dynamic      p - P2mp
===============================================================================
To              State  Out I/F        Out Label      Reserved    Protected  Type
                                                      BW (Kbps)   LSP Count
-------------------------------------------------------------------------------
10.5.6.6        Up     1/2/5          131055         0           4          d
  Protected LSPs -
  toSARF6(ISEL)::Loose                From: 192.168.0.2     To: 192.168.0.6
  toSARF6(ISEL)::Loose                From: 192.168.0.1     To: 192.168.0.6
  toSARF6(ISEL)::Loose                From: 192.168.0.11    To: 192.168.0.6
  toSARF6(ISEL)::Loose                From: 192.168.0.13    To: 192.168.0.6

10.5.11.5       Up     1/2/5          131047         0           6          d
  Protected LSPs -
  toSARF5(ISCAL)::Loose               From: 192.168.0.2     To: 192.168.0.5
  toSARF4(SP)::Loose                  From: 192.168.0.2     To: 192.168.0.4
  toSARF3(COB)::Loose                 From: 192.168.0.2     To: 192.168.0.3
  toSARF5(ISCAL)::Loose               From: 192.168.0.1     To: 192.168.0.5
  toSARF4(SP)::Loose                  From: 192.168.0.1     To: 192.168.0.4
  toSARF3(COB)::Loose                 From: 192.168.0.1     To: 192.168.0.3

10.2.11.2       Up     1/2/6          131037         0           5          d
  Protected LSPs -
  toSARF2(ESTeSL)::Loose              From: 192.168.0.6     To: 192.168.0.2
  toSARF2(ESTeSL)::Loose              From: 192.168.0.3     To: 192.168.0.2
  toSARF2(ESTeSL)::Loose              From: 192.168.0.1     To: 192.168.0.2
  toSARF2(ESTeSL)::Loose              From: 192.168.0.5     To: 192.168.0.2
  toSARF2(ESTeSL)::Loose              From: 192.168.0.4     To: 192.168.0.2

10.5.11.11      Up     1/2/6          131032         0           5          d
  Protected LSPs -
  toSR71(ESD)::Loose                  From: 192.168.0.1     To: 192.168.0.11
  toSR72(ESML)::Loose                 From: 192.168.0.1     To: 192.168.0.12
  toSR73(ESTC)::Loose                 From: 192.168.0.1     To: 192.168.0.13
  toSR73(ESTC)::Loose                 From: 192.168.0.6     To: 192.168.0.13
  toSR72(ESML)::Loose                 From: 192.168.0.6     To: 192.168.0.12
-------------------------------------------------------------------------------
Bypass Tunnels : 4
===============================================================================
```

Figura 60 – Túneis de *bypass* criados a partir do *router* SARF-1(CORE) e todos os LSP protegidos pelos mesmos.

Apesar do comportamento anteriormente demonstrado, na maioria das vezes os LSP estabeleceram-se de forma semelhante à que foi previamente mapeada. Na Figura 61 está um exemplo em que a reserva de largura de banda obteve um resultado semelhante ao que foi mapeado para o *router* SARF-4(SP).

```
*A:SARF-4(SP)# show router rsvp interface

===============================================================================
RSVP Interfaces
===============================================================================
Interface                        Total     Active    Total BW  Resv BW   Adm Opr
                                 Sessions  Sessions  (Mbps)    (Mbps)
-------------------------------------------------------------------------------
system                           -         -         -         -         Up  Up
toSARF-3                         13        13        100       50        Up  Up
toSARF-5                         15        15        100       100       Up  Up
toSR7-3                          13        13        100       50        Up  Up
-------------------------------------------------------------------------------
Interfaces : 4
===============================================================================
```

Figura 61 – Reserva de largura de banda nas interfaces do *router* SARF-4(SP).

Note-se que no mapeamento do *router* SARF-4(SP) esperava-se a seguinte reserva de largura de banda:

- ***toSARF-3*** – 40 Mb/s
- ***toSARF-5*** – 100 Mb/s
- ***toSR7-3*** – 50 Mb/s

Por fim, de forma a testar o FRR foi provocado um corte de rede através do comando "*shutdown*" na porta 1/2/5 do *router* SARF-6(ISEL). Na Figura 62, pode-se observar que o LSP "toSARF5(ISCAL)" no *router* SARF-1(CORE) foi protegido pelo túnel *bypass* "bypass-node192.168.0.6".

```
*A:SARF-1(CORE)>show>router>mpls# bypass-tunnel protected-lsp  toSARF5(ISCAL)::Loose detail

===============================================================================
MPLS Bypass Tunnels (Detail)
===============================================================================
-------------------------------------------------------------------------------
bypass-node192.168.0.6
-------------------------------------------------------------------------------
To              : 10.5.11.5           State               : Active
Out I/F         : 1/2/5               Out Label           : 131047
Up Time         : 0d 01:49:34         Active Time         : 0d 00:00:46
Reserved BW     : 0 Kbps              Protected LSP Count : 3
Type            : Dynamic
SetupPriority   : 7                   Hold Priority       : 0
Class Type      : 0
Actual Hops     :
    10.1.2.1        -> 10.1.2.2        -> 10.2.11.11      -> 10.5.11.5

Protected LSPs -
LSP Name        : toSARF5(ISCAL)::Loose
From            : 192.168.0.1         To                  : 192.168.0.5
Avoid Node/Hop  : 192.168.0.6         Downstream Label    : 131000
Bandwidth       : 10000 Kbps

===============================================================================
```

Figura 62 – Representação do túnel *bypass* ativo após o corte de rede provocado.

3.3.3. Discussão

Esta solução permite o balanceamento dinâmico da rede no entanto, dependendo da LB atribuída e até do tempo de arranque dos equipamentos, algumas ligações podem ficar com a LB inesperadamente reservada. No limite alguns LSP não se conseguirão estabelecer. Esta solução possibilita ainda a melhoria das seguintes características QoS:

- ***Bandwidth & Packet Loss*****:** Conforme o critério de LB atribuído a cada LSP é possível garantir que alguns caminhos sejam partilhados por poucos LSP, garantido assim menor concorrência pelos recursos e uma possível redução da probabilidade de engarrafamento que se traduz em menos perdas de pacotes.
- ***Availability*****:** Utilizando FRR como método de resiliência garante-se que a rede irá recuperar em menos de 50 ms, mantendo um alto nível de disponibilidade.

Um dos aspetos negativos desta solução será a sua escalabilidade, a qual depende do critério utilizado na atribuição de largura de banda aos LSP. No entanto, este fator pode ser minimizado utilizando a opção "*subscription*" para aumentar a largura de banda reservável até 10x mais que o valor por omissão. Assim, uma ligação de 1 Gb/s

no máximo poderá disponibilizar uma largura de banda reservável de 10 Gb/s com o comando "*subscription* 1000". A ausência de controlo sobre os caminhos estabelecidos é também um aspeto negativo, pois como foi demonstrado anteriormente alguns LSP podem se estabelecer por caminhos alternativos devido à reserva inesperada de LB em algumas ligações. Para minimizar este efeito poderá ser utilizada a opção "*resignal timer*" que periodicamente irá procurar um caminho melhor para todos os LSP ativos.

3.4. Solução de balanceamento dinâmico com serviços prioritários

Nesta solução pretende-se manter algum controlo, permitindo ao mesmo tempo que o estabelecimento dos LSP seja dinâmico. Para este efeito a proposta passa pela utilização da reserva de LB com a adição de prioridades.

Tendo por base a solução anterior, a introdução de prioridades permite que os LSP prioritários se estabeleçam no melhor caminho independentemente de este ter ou não LB disponível. Assim estes LSP podem "obrigar" que os LSP menos prioritários retirem a sua reserva de largura de banda e voltem a procurar outro caminho possível. Para maior pormenor refira-se ao capítulo 1.5.4.7.

3.4.1. Resiliência

Sendo esta solução idêntica à anterior, terá pelos mesmos motivos o FRR *facility* como resiliência.

3.4.2. Configuração

Este capítulo não será totalmente desenvolvido devido às limitações do *software*/*hardware* que não permitem atribuir prioridades aos LSP nos equipamentos do laboratório Alcatel-Lucent do ISEL. No entanto a configuração desta solução seria semelhante à anterior, com a adição de prioridades aos LSP. No seguinte exemplo pode-se verificar uma possível configuração desta solução, tendo sido configurada a prioridade máxima neste caso.

```
 #--------------------------------------------------
echo "MPLS LSP Configuration"
#--------------------------------------------------
        mpls
            path "loose"
                no shutdown
            exit
            lsp "toSARF6(ISEL)"
                to 192.168.0.6
                cspf
                fast-reroute facility
                exit
                primary "loose"
                    bandwidth 10
                    priority 0 0
                exit
                no shutdown
            exit
         no shutdown
        exit
```

3.4.3. Discussão

Apesar de não ser possível implementar a solução devido às limitações do *software*/*hardware* do laboratório, prevê-se que esta solução iria minimizar a falta de controlo sobre os caminhos estabelecidos pelos LSP da solução anterior. Seria também útil para estabelecer novos LSP pelo melhor caminho possível independentemente da reserva de LB registada. Prevê-se ainda que esta solução iria possibilitar a melhoria das seguintes características QoS:

- ***Delay*:** Garantindo que o serviço prioritário é encaminhado pelo melhor caminho possível, obtém-se também o menor atraso possível para o serviço.
- ***Bandwidth & Packet Loss*:** Conforme o critério de LB atribuído a cada LSP é possível garantir que um reduzido número de LSP se estabeleça nas mesmas ligações, garantido assim maior LB a cada um desses serviços e uma possível redução da probabilidade de engarrafamento, que se traduz em menos perdas de pacotes.
- ***Availability*:** Utilizando o FRR como método de resiliência obtém-se uma resposta da rede em menos de 50 ms, mantendo um alto nível de disponibilidade.

A introdução de prioridades não iria resolver o problema da escalabilidade, no entanto em conjunto com a opção "*subscription*" a escalabilidade pode ser controlada até um determinado nível. Esta solução está limitada aos *softwares*/*hardwares* mais recentes da Nokia, assim os equipamentos 7210 SAS-M utilizados na rede MPLS do IPL não suportam a atribuição de prioridades e seria necessário fazer um *upgrade* do *hardware* para implementar esta solução.

3.5. Solução de balanceamento "manual"

Pretende-se com esta solução obter melhorias de QoS num ambiente controlado através de *admin-groups*, realizando um balanceamento "manual" da rede com o controlo dos caminhos estabelecidos de todos os LSP. De referir que com esta técnica é possível ter em conta outros fatores na definição do caminho, como o meio físico utilizado por cada ligação, o fornecedor da ligação, entre outros.

Os *admin-groups* são grupos utilizados para identificar uma ou mais ligações. Cada ligação pode ter um ou mais grupos associados. Desta forma o caminho tomado pelo LSP pode ser influenciado através da inclusão ou exclusão de grupos. De notar que caso seja utilizada a inclusão de grupos este apenas se estabelece caso exista um caminho *end-to-end* associado aos referidos grupos. Este é um método versátil, pois permite que todos os LSP sejam controlados ou que seja utilizado apenas de forma complementar. A complexidade da implementação deste método depende da topologia, pois nem todas as topologias tornam viável um controlo *end-to-end* através de *admin-groups*, como por exemplo uma topologia em anel.

3.5.1. Resiliência

Os *admin-groups* permitem que os *secondary-path* sejam controlados da mesma forma que os *primary-path*. Utilizando medidas opostas às aplicadas no *primary-path*, consegue-se obter um caminho diferente para o *secondary-path*. Adicionalmente para melhorar o tempo de resposta poderá ser utilizado um *Hot-standby secondary-path* e ainda o FRR *facility*. A utilização destes dois métodos em simultâneo permite que a rede recupere em menos de 50 ms das falhas através do FRR e que após esta recuperação o tráfego seja reencaminhado para o *secondary-path* que foi definido, sem perdas adicionais.

3.5.2. Configuração

A utilização de *admin-groups* exige um planeamento para a distribuição de grupos pelas ligações, de acordo com os objetivos definidos. Neste caso pretende-se influenciar os caminhos de todos os LSP, *primary-path* e *secondary-path*, com as restrições dos grupos que estes podem ou não utilizar. De forma a otimizar a solução estabeleceu-se ainda um limite de duas regras para cada LSP. Na Figura 63 está representado um possível planeamento dos *admin-groups* na rede, onde se procurou reutilizar os grupos com o compromisso de existirem sempre dois caminhos possíveis com diferentes grupos atribuídos para cada *router*.

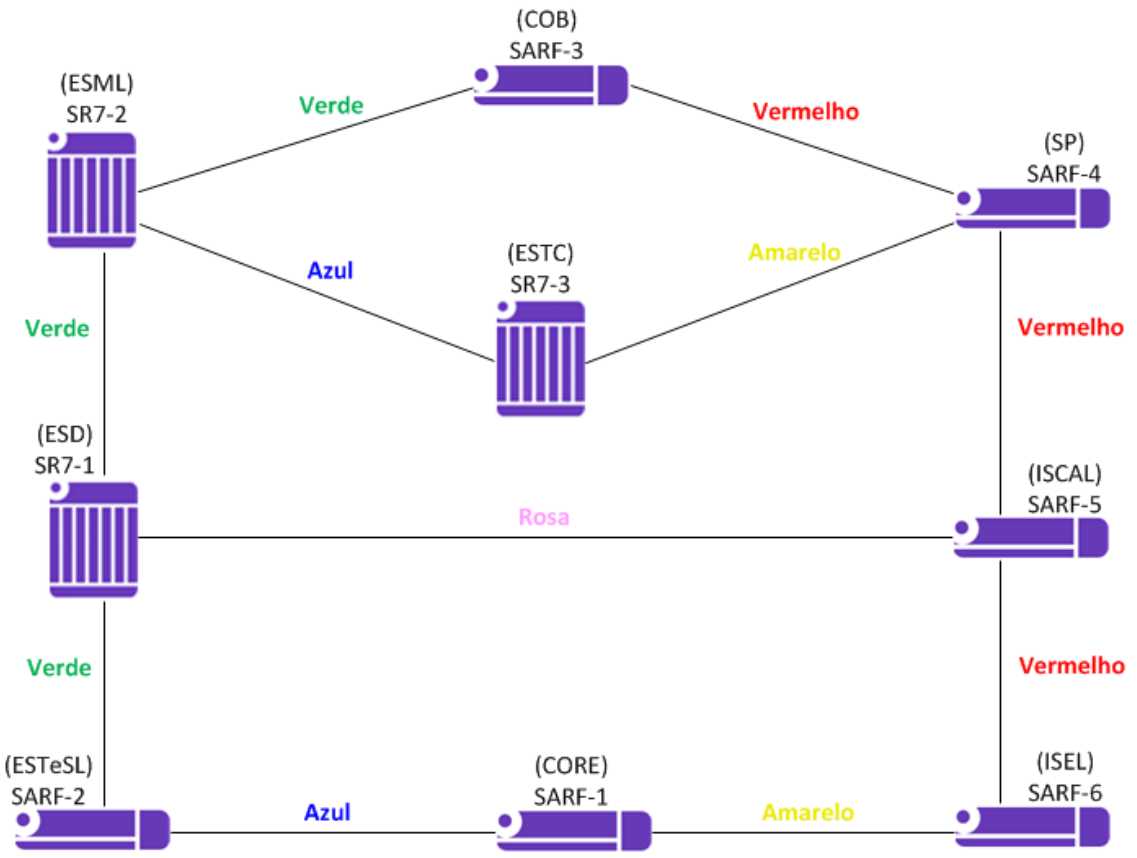

Figura 63 – Planeamento de atribuição de *admin-groups* na rede MPLS do IPL.

Na seguinte configuração pode-se observar a atribuição dos *admin-groups* às interfaces do *router* SARF1(CORE) conforme o planeamento anterior.

```
A:SARF-1(CORE)# admin display-config
...

#--------------------------------------------------
echo "MPLS Configuration"
#--------------------------------------------------
        mpls
            admin-group "AMARELO" 4
            admin-group "AZUL" 3
            admin-group "ROSA" 5
            admin-group "VERDE" 1
            admin-group "VERMELHO" 2
            interface "system"
            exit
            interface "toSARF-2"
                admin-group "AZUL"
            exit
            interface "toSARF-6"
                admin-group "AMARELO"
            exit
        exit
```

Na Figura 64 pode-se observar as interfaces MPLS do *router* SARF-1(CORE).

```
*A:SARF-1(CORE)>show>router>mpls# interface

===============================================================================
MPLS Interfaces
===============================================================================
Interface                          Port-id          Adm    Opr    TE-metric
-------------------------------------------------------------------------------
system                             system           Up     Up     None
  Admin Groups                     None
  Srlg Groups                      None
toSARF-2                           1/2/5            Up     Up     None
  Admin Groups                     AZUL
  Srlg Groups                      None
toSARF-6                           1/2/6            Up     Up     None
  Admin Groups                     AMARELO
  Srlg Groups                      None
-------------------------------------------------------------------------------
Interfaces : 3
===============================================================================
```

Figura 64 – Interfaces MPLS do *router* SARF-1(CORE).

Após o planeamento anterior foi necessário definir os caminhos que cada LSP iria estabelecer. De forma a exercer um controlo total sobre o *primary-path* utilizaram-se as combinações necessárias para definir o caminho *end-to-end* através das restrições de *admin-groups*. No caso do *secondary-path* definiu-se apenas que este não utilizaria os *admin-groups* do *primary-path*, deixando em alguns casos mais que um caminho possível, como se pode verificar na Figura 65.

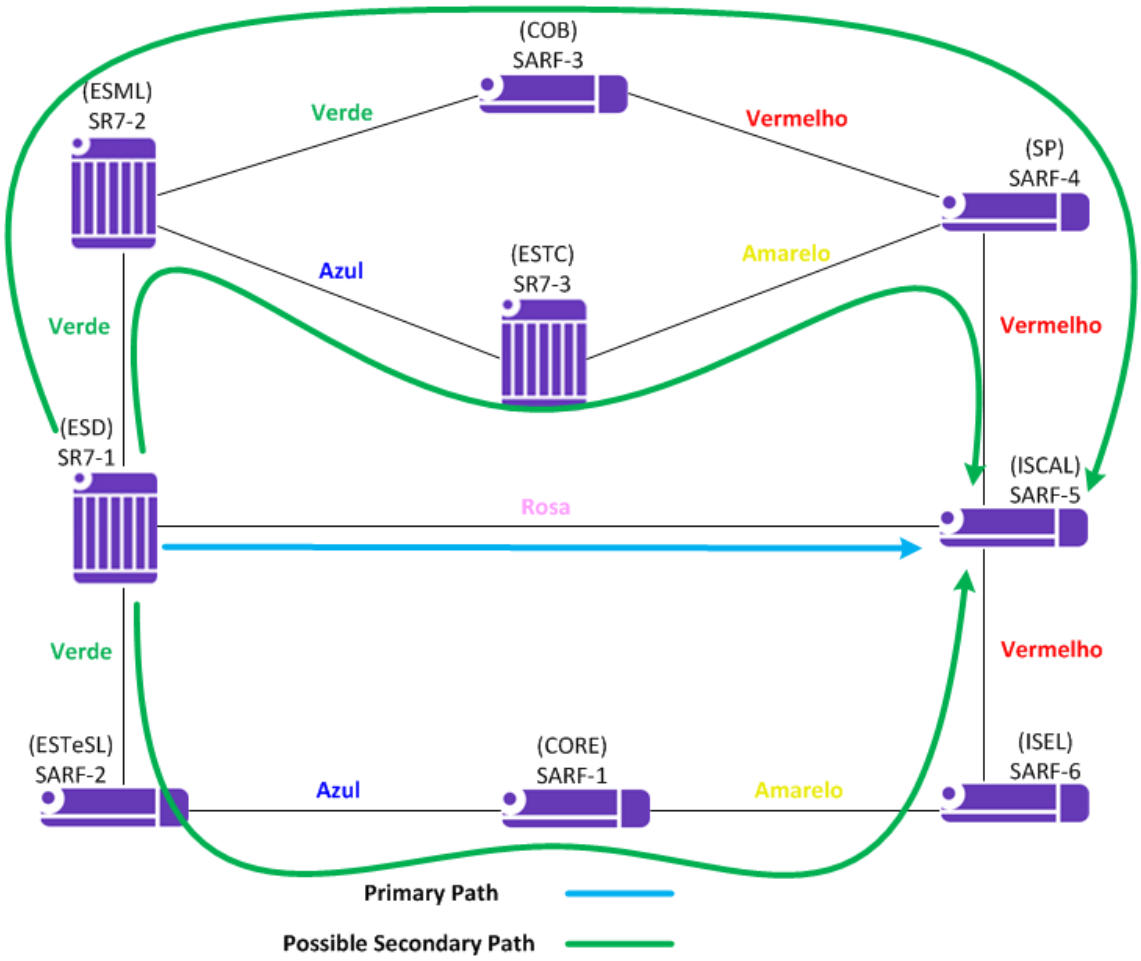

Figura 65 – Caminhos possíveis para o *secondary-path* após a restrição dos *admin-groups* utilizados no *primary-path*.

Os LSP foram estabelecidos de acordo com o planeamento dos caminhos referido na primeira solução e apresentados no anexo **Error! Reference source not found.**. Na seguinte configuração e nos anexos **Error! Reference source not found.** pode-se observar um exemplo da definição dos LSP no *router* SARF-1(CORE), com as restrições necessárias para que os caminhos sejam estabelecidos de acordo com o planeamento. Note-se que foram utilizados *Hot-standby secondary-path* e que estes utilizam o *path* "LooseALT" sem *hops* definidos.

```
A:SARF-1(CORE)# admin display-config
...

#--------------------------------------------------
echo "MPLS LSP Configuration"
#--------------------------------------------------
        mpls
            path "Loose"
                no shutdown
            exit
            path "LooseALT"
                no shutdown
            exit
            lsp "toSARF2(ESTeSL)"
                to 192.168.0.2
                cspf
                primary "Loose"
```

```
                include "AZUL"
            exit
            secondary "LooseALT"
                standby
                exclude "AZUL"
            exit
            no shutdown
        exit
        lsp "toSARF3(COB)"
            to 192.168.0.3
            cspf
            primary "Loose"
                include "AZUL"
                include "VERDE"
            exit
            secondary "LooseALT"
                standby
                exclude "AZUL"
                exclude "VERDE"
            exit
            no shutdown
        exit
        lsp "toSARF4(SP)"
            to 192.168.0.4
            cspf
            primary "Loose"
                include "AMARELO"
                include "VERMELHO"
            exit
            secondary "LooseALT"
                standby
                exclude "AMARELO"
                exclude "ROSA"
            exit
            no shutdown
        exit
        lsp "toSARF5(ISCAL)"
            to 192.168.0.5
            cspf
            primary "Loose"
                include "AMARELO"
                include "VERMELHO"
            exit
            secondary "LooseALT"
                standby
                exclude "AMARELO"
            exit
            no shutdown
        exit
        lsp "toSARF6(ISEL)"
            to 192.168.0.6
            cspf
            primary "Loose"
                include "AMARELO"
            exit
            secondary "LooseALT"
                standby
                exclude "AMARELO"
            exit
            no shutdown
        exit
        lsp "toSR71(ESD)"
            to 192.168.0.11
            cspf
            primary "Loose"
                include "AZUL"
                include "VERDE"
            exit
```

```
            secondary "LooseALT"
                standby
                exclude "AZUL"
            exit
            no shutdown
        exit
        lsp "toSR72(ESML)"
            to 192.168.0.12
            cspf
            primary "Loose"
                include "AZUL"
                include "VERDE"
            exit
            secondary "LooseALT"
                standby
                exclude "AZUL"
                exclude "ROSA"
            exit
            no shutdown
        exit
        lsp "toSR73(ESTC)"
            to 192.168.0.13
            cspf
            primary "Loose"
                include "AMARELO"
                include "VERMELHO"
            exit
            secondary "LooseALT"
                standby
                exclude "AMARELO"
                exclude "VERMELHO"
            exit
            no shutdown
        exit
        no shutdown
    exit
```

Na Figura 66 pode-se observar que o LSP “toSARF5(ISCAL)” no *router* SARF-1(CORE) foi estabelecido de acordo com o pretendido.

```
*A:SARF-1(CORE)>show>router>mpls# lsp path detail

===============================================================================
MPLS LSP  Path  (Detail)
===============================================================================
Legend :
    @ - Detour Available              # - Detour In Use
    b - Bandwidth Protected           n - Node Protected
    s - Soft Preemption
===============================================================================
LSP toSARF5(ISCAL) Path Loose
-------------------------------------------------------------------------------
LSP Name     : toSARF5(ISCAL)                    Path LSP ID : 7168
From         : 192.168.0.1                       To          : 192.168.0.5
Adm State    : Up                                Oper State  : Up
Path Name    : Loose                             Path Type   : Primary
Path Admin   : Up                                Path Oper   : Up
OutInterface: 1/2/6                              Out Label   : 131060
Path Up Time: 0d 00:23:16                        Path Dn Time: 0d 00:00:00
Retry Limit : 0                                  Retry Timer : 30 sec
RetryAttempt: 0                                  NextRetryIn : 0 sec
SetupPriori*: 7                                  Hold Priori*: 0
Bandwidth    : No Reservation                    Oper Bw     : 0 Mbps
Hop Limit    : 255                               Class Type  : 0
Record Route: Record                             Record Label: Record
Oper MTU     : 2086                              Neg MTU     : 2086
Adaptive     : Enabled                           Oper Metric : 200
Include Grps:                                    Exclude Grps:
VERMELHO                                        None
AMARELO
Path Trans   : 1                                 CSPF Queries: 1
Failure Code: noError                            Failure Node: n/a
ExplicitHops:
    No Hops Specified
Actual Hops :
    10.1.6.1(192.168.0.1)                            Record Label    : N/A
 -> 10.1.6.6(192.168.0.6)                            Record Label    : 131060
 -> 10.5.6.5(192.168.0.5)                            Record Label    : 131056
ComputedHops:
    10.1.6.1        -> 10.1.6.6        -> 10.5.6.5
ResigEligib*: False
LastResignal: n/a                                    CSPF Metric : 200
```

Figura 66 – Informação detalhada sobre o *primay-path* do LSP "toSARF5(ISCAL)" no *router* SARF-1(CORE).

Na sequência da figura anterior, pode-se observar ainda na Figura 67 que o *secondary-path* deste LSP foi estabelecido por um caminho diferente, resultante das restrições implementadas.

```
-------------------------------------------------------------------------------
LSP toSARF5(ISCAL) Path LooseALT
-------------------------------------------------------------------------------
LSP Name     : toSARF5(ISCAL)                    Path LSP ID : 7170
From         : 192.168.0.1                       To          : 192.168.0.5
Adm State    : Up                                Oper State  : Up
Path Name    : LooseALT                          Path Type   : Standby
Path Admin   : Up                                Path Oper   : Up
OutInterface: 1/2/5                              Out Label   : 131036
Path Up Time: 0d 00:22:54                        Path Dn Time: 0d 00:00:00
Retry Limit : 0                                  Retry Timer : 30 sec
RetryAttempt: 0                                  NextRetryIn : 0 sec
SetupPriori*: 7                                  Hold Priori*: 0
Bandwidth    : No Reservation                    Oper Bw     : 0 Mbps
Hop Limit    : 255                               Class Type  : 0
Record Route: Record                             Record Label: Record
Oper MTU     : 2086                              Neg MTU     : 2086
Adaptive     : Enabled                           Oper Metric : 300
Include Grps:                                    Exclude Grps:
None                                           AMARELO
Path Trans   : 1                                 CSPF Queries: 2
Failure Code: noError                            Failure Node: n/a
ExplicitHops:
    No Hops Specified
Actual Hops :
    10.1.2.1(192.168.0.1)                        Record Label    : N/A
 -> 10.1.2.2(192.168.0.2)                        Record Label    : 131036
 -> 10.2.11.11(192.168.0.11)                     Record Label    : 131020
 -> 10.5.11.5(192.168.0.5)                       Record Label    : 131010
ComputedHops:
    10.1.2.1        -> 10.1.2.2        -> 10.2.11.11      -> 10.5.11.5
Srlg         : Disabled
SrlgDisjoint: False
ResigEligib*: False
LastResignal: n/a                                CSPF Metric : 300
```

Figura 67 – Informação detalhada sobre o *secondary-path* do LSP "toSARF5(ISCAL)" no *router* SARF-1(CORE).

Nesta solução foi ainda criada uma versão que adiciona o FRR *facility* à anterior configuração. Assim na Figura 68 pode-se observar que as proteções do FRR estão ativas no *primary-path* do LSP "toSARF5(ISCAL)" no *router* SARF-1(CORE).

```
*A:SARF-1(CORE)>show>router>mpls# lsp path detail

===============================================================================
MPLS LSP  Path  (Detail)
===============================================================================
Legend :
    @ - Detour Available              # - Detour In Use
    b - Bandwidth Protected           n - Node Protected
    s - Soft Preemption
===============================================================================
LSP toSARF5(ISCAL) Path Loose
-------------------------------------------------------------------------------
LSP Name     : toSARF5(ISCAL)                    Path LSP ID : 18944
From         : 192.168.0.1                       To          : 192.168.0.5
Adm State    : Up                                Oper State  : Up
Path Name    : Loose                             Path Type   : Primary
Path Admin   : Up                                Path Oper   : Up
OutInterface: 1/2/6                              Out Label   : 131050
Path Up Time: 0d 00:41:25                        Path Dn Time: 0d 00:00:00
Retry Limit : 0                                  Retry Timer : 30 sec
RetryAttempt: 0                                  NextRetryIn : 0 sec
SetupPriori*: 7                                  Hold Priori*: 0
Bandwidth    : No Reservation                    Oper Bw     : 0 Mbps
Hop Limit    : 255                               Class Type  : 0
Record Route: Record                             Record Label: Record
Oper MTU     : 2082                              Neg MTU     : 2082
Adaptive     : Enabled                           Oper Metric : 200
Include Grps:                                    Exclude Grps:
VERMELHO                                        None
AMARELO
Path Trans   : 1                                 CSPF Queries: 1
Failure Code: noError                            Failure Node: n/a
ExplicitHops:
    No Hops Specified
Actual Hops :
    10.1.6.1(192.168.0.1) @ n                    Record Label    : N/A
 -> 10.1.6.6(192.168.0.6) @                      Record Label    : 131050
 -> 10.5.6.5(192.168.0.5)                        Record Label    : 131050
ComputedHops:
    10.1.6.1        -> 10.1.6.6        -> 10.5.6.5
ResigEligib*: False
LastResignal: n/a                                CSPF Metric : 200
```

Figura 68 – Informação detalhada do LSP "toSARF5(ISCAL)" no *router* SARF-1(CORE), com FRR ativo.

Neste caso o FRR estabeleceu os túneis *bypass* para proteção do LSP "toSARF5(ISCAL)" pelo mesmo caminho que o *secondary-path*, como se pode observar na Figura 69 o "bypass-node 192.168.0.6".

```
*A:SARF-1(CORE)>show>router>mpls# bypass-tunnel detail

===============================================================================
MPLS Bypass Tunnels (Detail)
===============================================================================
-------------------------------------------------------------------------------
bypass-link10.1.6.6
-------------------------------------------------------------------------------
To              : 10.5.6.6            State               : Up
Out I/F         : 1/2/5               Out Label           : 131052
Up Time         : 0d 00:24:20         Active Time         : n/a
Reserved BW     : 0 Kbps              Protected LSP Count : 2
Type            : Dynamic
SetupPriority   : 7                   Hold Priority       : 0
Class Type      : 0
Actual Hops     :
    10.1.2.1        -> 10.1.2.2         -> 10.2.11.11       -> 10.5.11.5
 -> 10.5.6.6

bypass-link10.1.2.2
-------------------------------------------------------------------------------
To              : 10.2.11.2           State               : Up
Out I/F         : 1/2/6               Out Label           : 131039
Up Time         : 0d 00:24:20         Active Time         : n/a
Reserved BW     : 0 Kbps              Protected LSP Count : 2
Type            : Dynamic
SetupPriority   : 7                   Hold Priority       : 0
Class Type      : 0
Actual Hops     :
    10.1.6.1        -> 10.1.6.6         -> 10.5.6.5         -> 10.5.11.11
 -> 10.2.11.2

-------------------------------------------------------------------------------
bypass-node192.168.0.6
-------------------------------------------------------------------------------
To              : 10.5.11.5           State               : Up
Out I/F         : 1/2/5               Out Label           : 131017
Up Time         : 0d 00:25:00         Active Time         : n/a
Reserved BW     : 0 Kbps              Protected LSP Count : 3
Type            : Dynamic
SetupPriority   : 7                   Hold Priority       : 0
Class Type      : 0
Actual Hops     :
    10.1.2.1        -> 10.1.2.2         -> 10.2.11.11       -> 10.5.11.5
-------------------------------------------------------------------------------
bypass-node192.168.0.2
-------------------------------------------------------------------------------
To              : 10.5.11.11          State               : Up
Out I/F         : 1/2/6               Out Label           : 131006
Up Time         : 0d 00:24:49         Active Time         : n/a
Reserved BW     : 0 Kbps              Protected LSP Count : 3
Type            : Dynamic
SetupPriority   : 7                   Hold Priority       : 0
Class Type      : 0
Actual Hops     :
    10.1.6.1        -> 10.1.6.6         -> 10.5.6.5         -> 10.5.11.11

===============================================================================
```

Figura 69 – Túneis *bypass* estabelecidos a partir do *router* SARF-1(CORE).

O FRR poderá ser útil não só pela melhoria do tempo de recuperação, mas também pela redundância extra caso o túnel *bypass* se estabeleça por um caminho diferente do *secondary-path*.

Para testar os métodos de resiliência das duas versões provocou-se um corte de rede através do comando "*shutdown*" na porta 1/2/5 do *router* SARF-6(ISEL). Este corte afeta o LSP "toSARF5(ISCAL)" no *router* SARF-1(CORE) apresentado nas figuras

anterior. Em ambas as versões o resultado foi o mesmo com o *secondary path* a ficar ativo após o corte de rede provocado, como se pode observar na Figura 70.

```
*A:SARF-1(CORE)# show router mpls lsp toSARF5(ISCAL) activepath

===============================================================================
MPLS LSP: toSARF5(ISCAL) (active paths)
===============================================================================
LSP Name      : toSARF5(ISCAL)                    LSP Id       : 47620
Path Name     : Loose                             Active Path  : Primary
To            : 192.168.0.5

===============================================================================
*A:SARF-1(CORE)# show router mpls lsp toSARF5(ISCAL) activepath

===============================================================================
MPLS LSP: toSARF5(ISCAL) (active paths)
===============================================================================
LSP Name      : toSARF5(ISCAL)                    LSP Id       : 47618
Path Name     : LooseALT                          Active Path  : Standby
To            : 192.168.0.5

===============================================================================
```

Figura 70 – LSP *Path* ativo antes e depois do corte da rede.

No caso da versão alternativa com FRR, após o corte de rede o tráfego é encaminhado pelo túnel de *bypass* e apenas depois com o auxílio do MBB será feita a transição do tráfego do túnel *bypass* para o *secondary-path*. Note-se que isto apenas acontece caso se trate de um *Hot-standby* seconday-path, ou seja com um *Cold-standby secondary-path* o tráfego mantém-se no túnel de *bypass*.

3.5.3. Discussão

Os *admin-groups* permitem obter um controlo total sobre a rede, sendo possível balancear a rede "manualmente". Este controlo pode ser viável ou não, dependendo da complexidade da topologia e da distribuição de *admin-groups* realizada. A solução poderá ser escalável, caso se mantenha uma topologia compatível sem esgotar o número de *admin-groups* disponíveis. Com esta abordagem é possível melhorar as seguintes características de QoS dos serviços prioritários:

- ***Delay*:** O caminho dos LSP pode ser controlado, ou seja pode ser atribuído o caminho mais curto não só ao nível de *hops*, mas também tendo em consideração a distância percorrida *end-to-end*.
- ***Bandwidth & Packet Loss*:** Com um balanceamento "manual" é possível determinar o número de LSP que cada ligação contém, e assim disponibilizar mais LB a alguns LSP. Desta forma a probabilidade de engarrafamento poderá ser diminuída, o que se traduz em menos perdas de pacotes.
- ***Availability*:** Utilizando FRR ou *Hot-standby secondary-path* como método de resiliência garante-se que a rede terá uma rápida recuperação, mantendo um alto nível de disponibilidade.

No entanto, este método é incompatível com topologias em anel, pois é impossível reutilizar os *admin-groups*. Topologias compostas apenas por *routers* PE aumentam a complexidade do planeamento, podendo colocar em causa a sua viabilidade. A

escalabilidade desta solução estará relacionada com o nível de complexidade do planeamento dos *admin-groups*. Assim quanto maior for a complexidade do planeamento menor será escalabilidade da solução. A proposta de planeamento para a rede MPLS do IPL têm um nível de complexidade alto, prevendo assim dificuldades na escalabilidade desta solução.

3.6. Estudo sobre a implementação de grupos SRLG

Este estudo pretende explorar outro método dinâmico de resiliência. À semelhança dos *admin-groups*, para utilizar o SRLG é necessário criar grupos SRLG e atribuir estes grupos às interfaces. Idealmente, entre *routers* PE haverá vários caminhos possíveis, pertencendo cada caminho a um dos grupos SRLG. Utilizando apenas o SRLG como restrição, os LSP serão estabelecidos de acordo com o melhor caminho encontrado através do IGP. No entanto terá a certeza que o *secondary-path* não irá utilizar as ligações dos mesmos grupos SRLG usados no *primary-path*.

3.6.1. Resiliência

A utilização do SRLG garante que o *secondary-path* não irá utilizar os mesmos caminhos que o *primary-path*. De forma a melhorar a resposta da rede a uma possível falha, poderá ser utilizado um *Hot-standby secondary-path*.

3.6.2. Configuração

A utilização de grupos SRLG exige um planeamento da atribuição destes grupos às interfaces. Idealmente os caminhos entre *routers* PE teriam apenas um grupo SRLG e seriam compostos apenas por *routers* do tipo P. A rede MPLS do IPL é apenas composta por *routers* PE, o que adiciona uma dificuldade extra na implementação deste método. Na Figura 71 pode-se observar uma proposta da atribuição de grupos SRLG às interfaces.

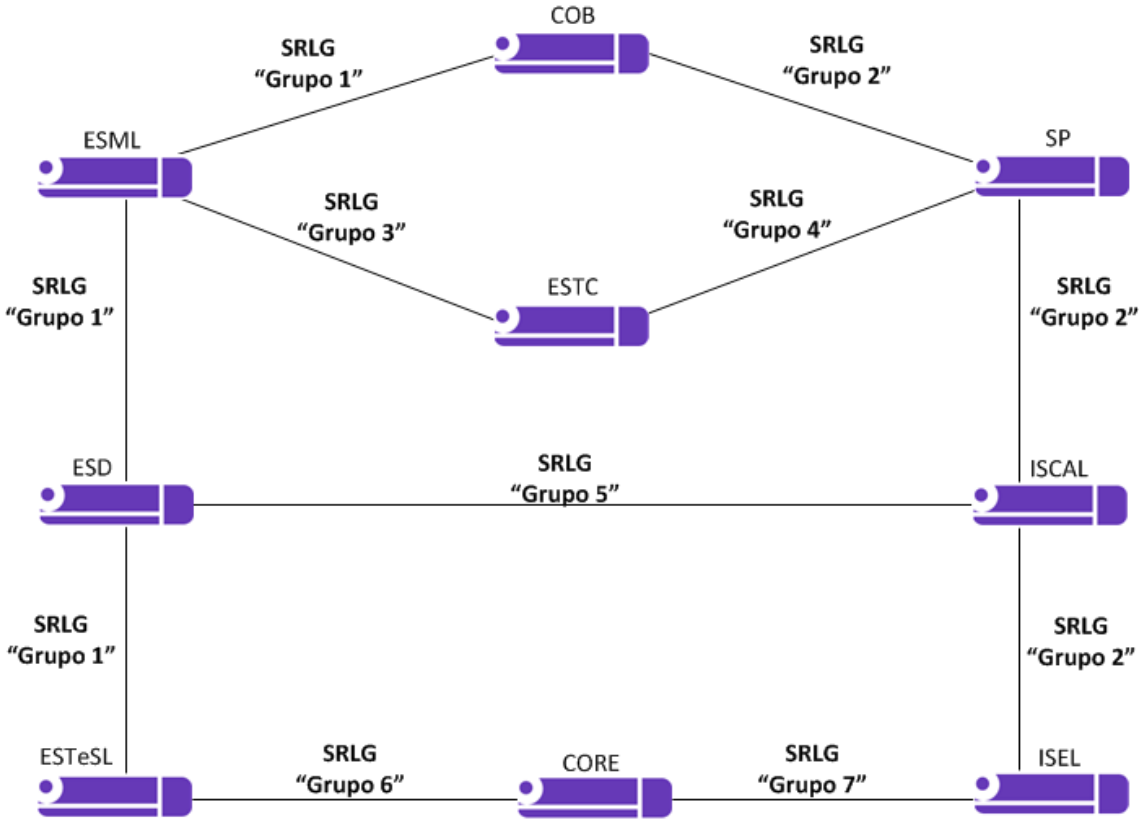

Figura 71 - Proposta de utilização de grupos SRLG na rede MPLS do IPL.

Esta proposta permite que a grande maioria dos LSP se consigam estabelecer pelo caminho mais próximo mantendo a proteção do SRLG. No entanto, alguns LSP apenas terão a proteção SRLG caso se estabeleçam por um caminho alternativo. Este caso aplica-se aos seguintes LSP:

- LSP entre "**ESML <-> ISEL**"
- LSP entre "**ESTeSL <-> SP**"

O caminho mais próximo para estes LSP passaria pela ligação intermédia "ESD <-> ISCAL", como se pode observar na Figura 72. Desta forma o *primary-path* passaria por interfaces atribuídas aos grupos 1, 2 e 5. Tendo mais de metade das interfaces associadas aos grupos 1 e 2, torna-se impossível estabelecer um *secondary-path* quando o *primary-path* utiliza interfaces destes dois grupos em simultâneo.

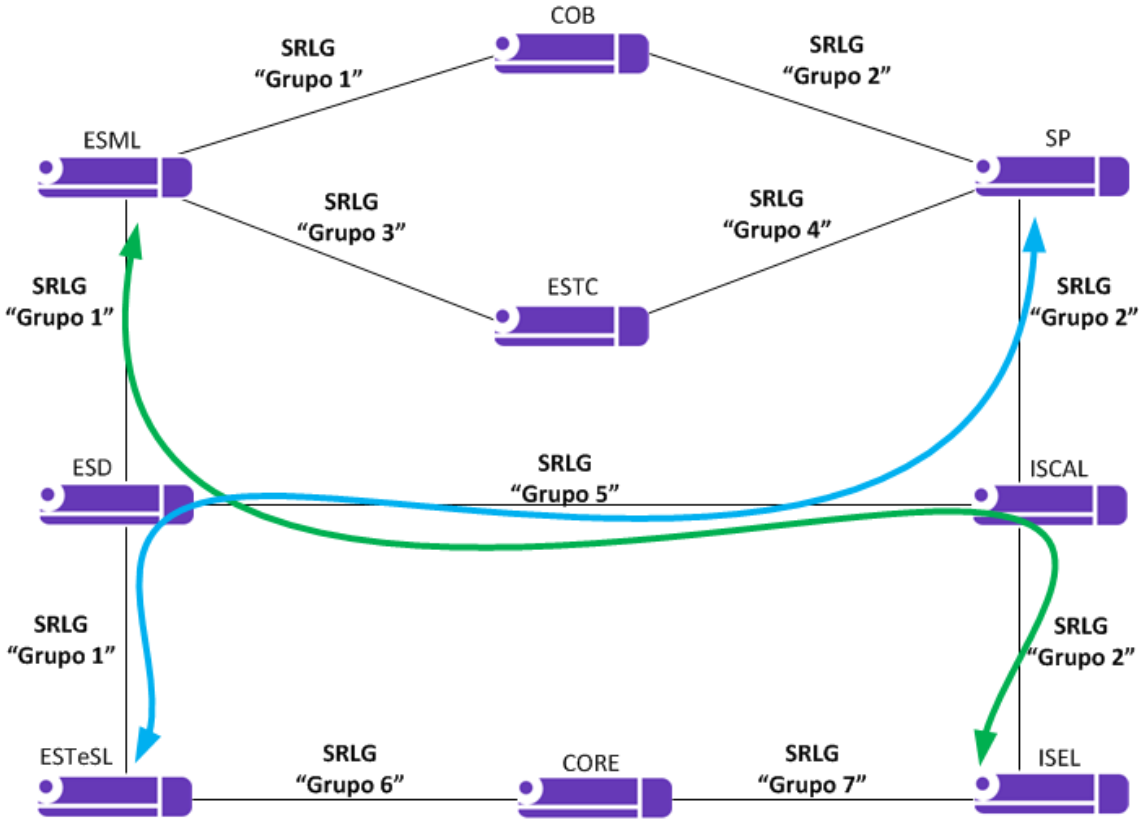

Figura 72 – Caminho mais próximo para os LSP entre "ESML <-> ISEL" e "ESTeSL <-> SP".

Assim, será necessário adicionar uma regra para que o *primary-path* seja forçado a tomar um caminho com ligações associadas apenas ao grupo 1 ou ao grupo 2. Na Figura 73, pode-se observar um exemplo dos caminhos que possibilitam a utilização de SRLG entre os *routers* ESML e ISEL.

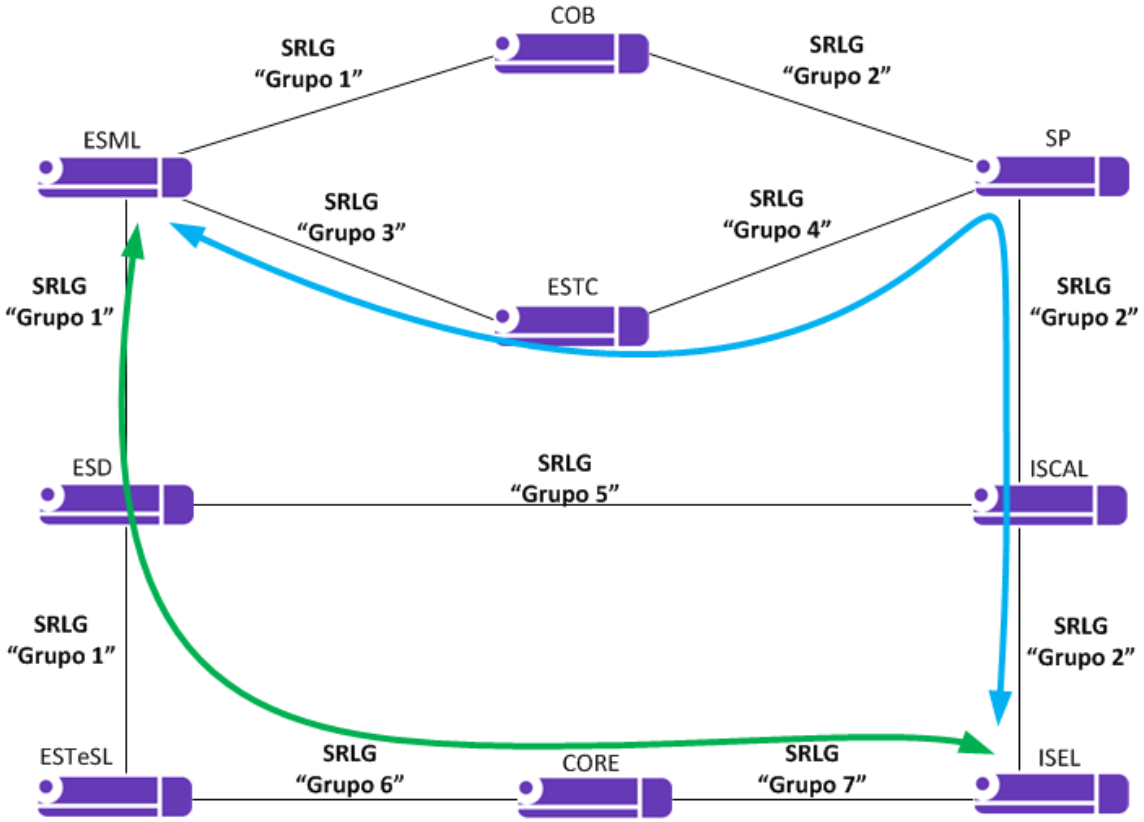

Figura 73 – Caminhos do *primary-path* que possibilitam a utilização de SRLG entre ESML e ISEL.

Outra opção seria atribuir um grupo SRLG a cada ligação, mas isso retiraria toda a eficiência do método e causaria problemas de escalabilidade. Após a exploração de várias opções de planeamento, chegou-se à conclusão que a topologia atual da rede MPLS do IPL não será favorável à aplicação deste método. A formação de vários anéis na topologia da rede dificulta o planeamento dos grupos de SRLG, sendo necessário utilizar outras restrições para resolver os problemas desta implementação. Tendo em conta estas dificuldades o estudo não foi desenvolvido.

3.6.3. Discussão

A utilização do SRLG garante que sejam estabelecidos caminhos alternativos para os *secondary-path* com base no caminho utilizado pelo *primary-path*. O SRLG poderá melhorar as seguintes características QoS dos serviços prioritários:

- ***Availability***: Utilizando um *Hot-standby secondary-path* como método de resiliência garante-se que a rede irá recuperar rapidamente de possíveis falhas e que em conjunto com o SRLG terá um caminho totalmente distinto do *primary-path*.

De uma forma geral a utilização de SRLG como método de resiliência necessita de um planeamento idêntico ao realizado com os *admin-groups*. Este planeamento pode-se tornar complexo dependendo da topologia da rede. Ao contrário dos *admin-groups*, o SRLG não pode ser utilizado como *constraint* para os *primary-path*, necessitando assim

de outros métodos para otimizar a rede. A escalabilidade desta solução depende da topologia da rede, tal como a solução anterior com os *admin-groups*.

O planeamento realizado para a rede MPLS do IPL é complexo e não serve todos os LSP. Assim, este método de resiliência não se enquadra com a topologia atual, no entanto poderá ser útil para responder a casos específicos.

4. Testes e resultados das medidas de QoS nas soluções desenvolvidas

Neste capítulo serão apresentados os testes e os resultados das medidas de QoS das soluções desenvolvidas e da configuração operacional da rede do IPL. Pelos motivos discutidos anteriormente, apenas as soluções dos capítulos 3.3 e 3.5 serão alvo de teste e comparação. Os testes foram realizados no laboratório Alcatel-Lucent do ISEL com a disposição representada na Figura 74.

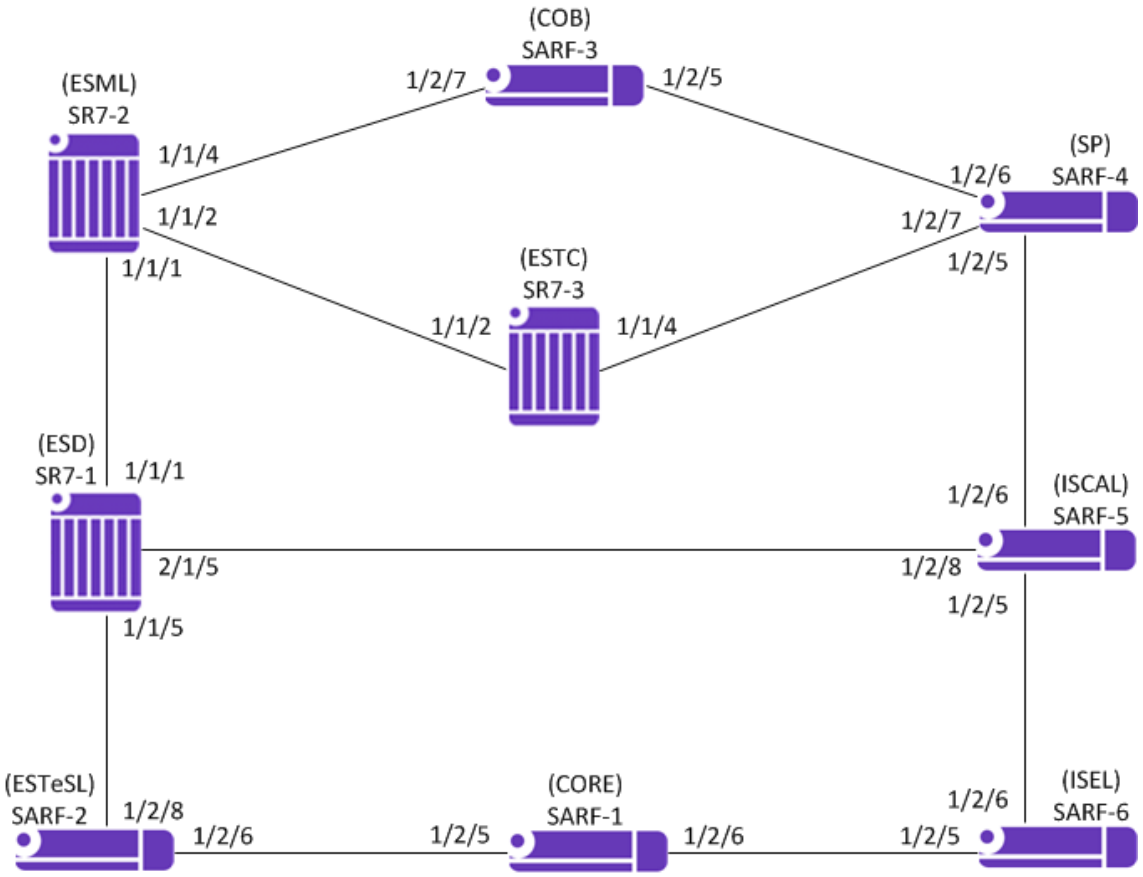

Figura 74 – Representação do cenário de testes no laboratório Alcatel-Lucent do ISEL.

4.1. Configuração base dos testes

A rede operacional do IPL contem uma grande variedade de serviços, no entanto para efeitos de testes será apenas utilizada uma VPLS configurada com o ID 10 e VC-ID 10, como se pode observar no seguinte exemplo de configuração do *router* SARF-1(CORE).

```
A:SARF-1(CORE)# admin display-config
...

#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
    service
      vpls 10 customer 1 create
            stp
                shutdown
            exit
```

```
            sap 1/2/4 create
            exit
            sap 1/2/8:10 create
            exit
            mesh-sdp 2:10 create
            exit
            mesh-sdp 3:10 create
            exit
            mesh-sdp 4:10 create
            exit
            mesh-sdp 5:10 create
            exit
            mesh-sdp 6:10 create
            exit
            mesh-sdp 11:10 create
            exit
            mesh-sdp 12:10 create
            exit
            mesh-sdp 13:10 create
            exit
            no shutdown
```

Tal como foi referido nos capítulos anteriores, todos os equipamentos da rede MPLS do IPL são *routers* PE. Assim, para aproveitar algumas ligações sem utilização entre os *routers* do laboratório, foram criadas 9 VPRN para servir de *Customer Equipment* (CE). Estas VPRN têm como objetivo ajudar a testar a conectividade da VPLS em todos os *routers* PE, como se pode verificar na Figura 75.

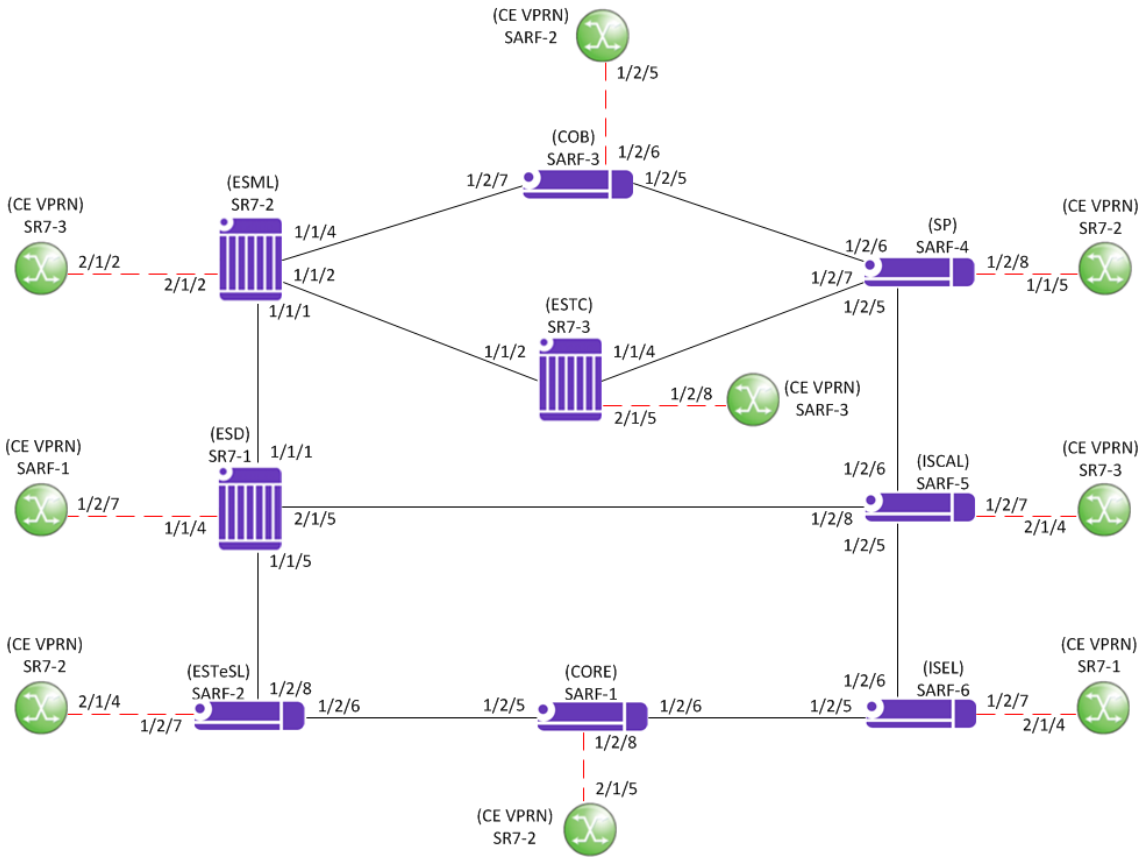

Figura 75 – Cenário de testes com as VPRN a simular os *routers* CE, ligados às portas de acesso dos *routers* PE.

Desta forma, os recursos do laboratório foram aproveitados e reduziu-se o número de equipamentos necessário para testar todas as ligações. Para um melhor entendimento, o *router* virtual CE com ligação ao *router* SARF-1(CORE) na porta de acesso 1/2/8 está virtualizado no *router* SR7-2 na porta de acesso 2/1/5. Na seguinte configuração está representada a VPRN que virtualiza o *router* CE que está ligado ao *router* SARF-1(CORE).

```
A:SR7-2(ESML)# admin display-config
...

#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
    service
        vprn 1001 customer 1 create
            route-distinguisher 1:1
            interface "toSARF1(CORE)" create
                address 10.10.10.1/24
                sap 2/1/5:10 create
                exit
            exit
            no shutdown
        exit
exit
```

As ferramentas para testar as medidas de QoS da rede através dos *routers* virtualizados são limitadas. Assim para melhorar a qualidade dos testes realizados foram adicionadas duas máquinas virtuais Linux Ubuntu 16.04.3 LTS com os *hostname* MPLS-1 e MPLS-2. Estas máquinas têm uma interface *Gigabit Ethernet* dedicada com uma ligação direta ao cenário de teste, como se pode observar na Figura 76.

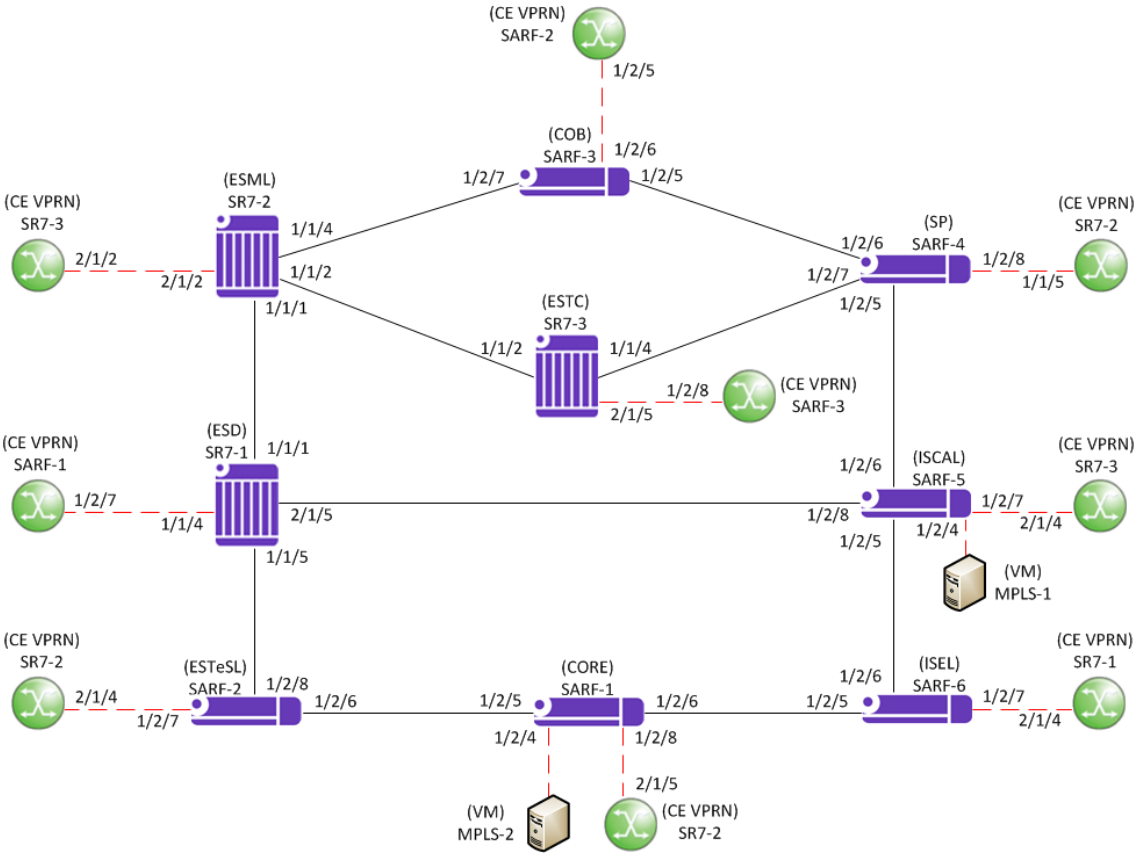

Figura 76 – Cenário de testes com as máquinas virtuais MPLS-1 e MPLS-2.

Em todas as configurações o tráfego entre as máquinas MPLS-1 e MPLS-2 foi transmitido pelos LSP "toSARF5(ISCAL)" e "toSARF1(CORE)", que se estabeleceram pelo *primary-path* representado na Figura 77. Nesta pode-se ainda verificar o caminho do *secondary-path* em caso de falha de rede.

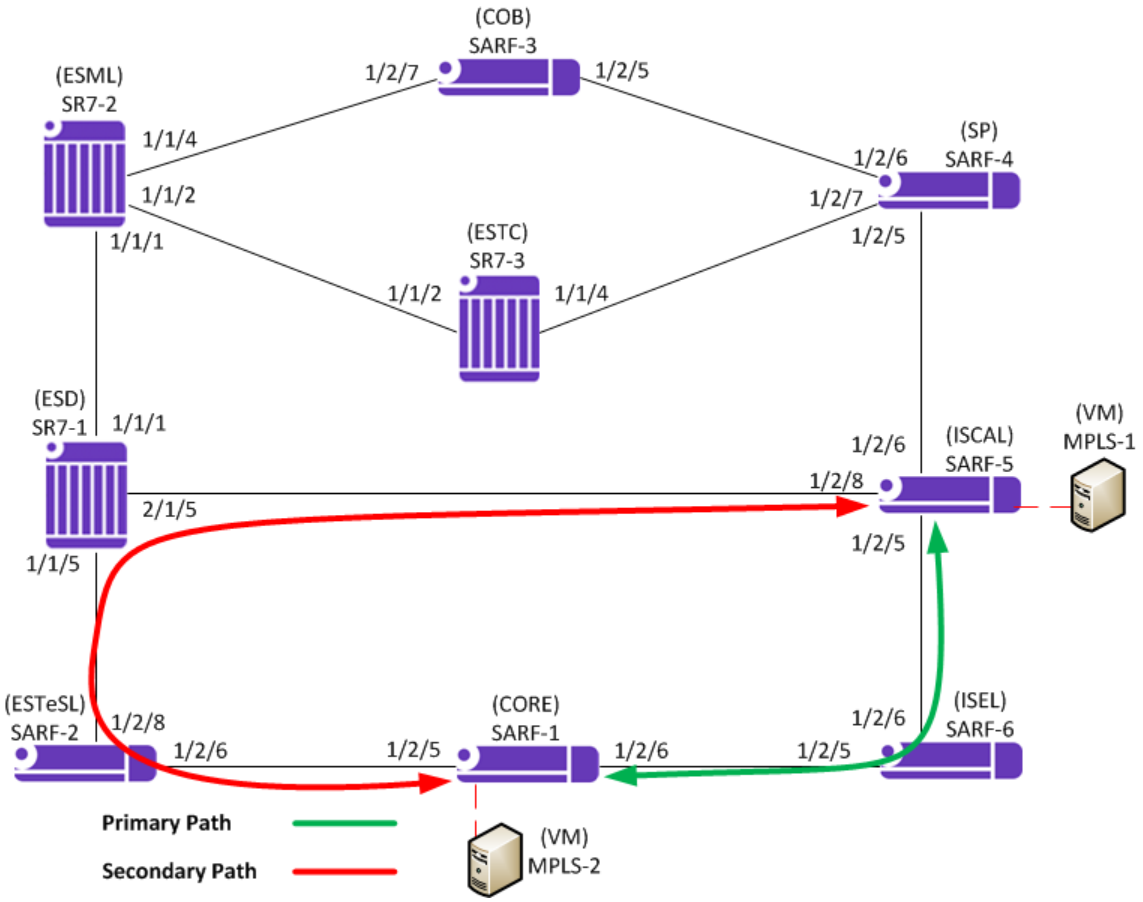

Figura 77 – Representação do caminho utilizado pelo tráfego nos testes realizados.

Na Figura 78 pode-se observar a representação lógica da VPLS sobre a rede MPLS e todos os equipamentos clientes que se ligam a esta através dos *routers* PE.

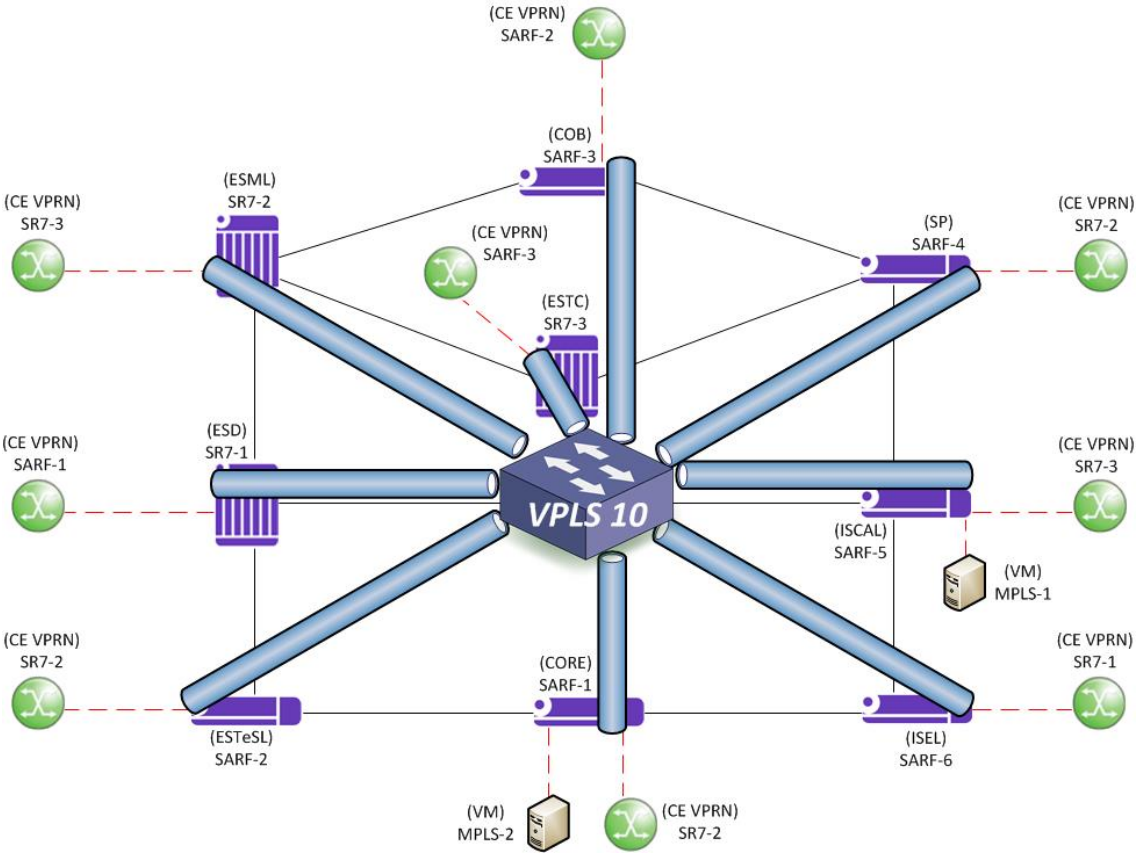

Figura 78 – Representação lógica da VPLS 10 no cenário de testes.

A esta VPLS foi atribuída a rede 10.10.10.0/24. A atribuição dos endereços seguiu a mesma regra que foi utilizada na definição de endereços da rede MPLS. Assim na Tabela 5 pode-se verificar os endereços atribuídos a cada máquina.

Router/Máquina Virtual	**Endereçamento IP**
SARF-1(CORE) CE *router*	10.10.10.1
SARF-2(ESTeSL) CE *router*	10.10.10.2
SARF-3(COB) CE *router*	10.10.10.3
SARF-4(SP) CE *router*	10.10.10.4
SARF-5(ISCAL) CE *router*	10.10.10.5
SARF-6(ISEL) CE *router*	10.10.10.6
SR7-1(ESD) CE *router*	10.10.10.11
SR7-2(ESML) CE *router*	10.10.10.12
SR7-3(ESTC) CE *router*	10.10.10.13
Máquina virtual MPLS-1	10.10.10.100
Máquina virtual MPLS-2	10.10.10.200

Tabela 5 – Atribuição de endereços às máquinas clientes da VPLS 10.

A conectividade entre as máquinas clientes foi verificada em todas as configurações MPLS. Na Figura 79 pode-se observar um exemplo da tabela de endereços MAC da VPLS 10 preenchida com 11 endereços correspondentes às 11 máquinas.

```
*A:SARF-1(CORE)>show>service# fdb-mac

===============================================================================
Service Forwarding Database
===============================================================================
ServId    MAC               Source-Identifier     Type/Age  Last Change
-------------------------------------------------------------------------------
10        00:1a:4a:16:01:52 sdp:5:10              L/79      08/24/2017 22:01:01
10        00:1a:4a:16:01:58 sap:1/2/4             L/45      08/24/2017 22:01:36
10        00:21:05:c9:b6:84 sdp:12:10             L/52      08/24/2017 22:01:28
10        00:21:05:c9:b6:86 sdp:5:10              L/59      08/24/2017 21:48:39
10        00:23:3e:98:2b:67 sdp:2:10              L/73      08/24/2017 21:48:39
10        00:23:3e:98:2b:68 sap:1/2/8:10          L/79      08/24/2017 22:01:01
10        00:23:3e:98:52:d2 sdp:4:10              L/59      08/24/2017 21:48:39
10        00:23:3e:e5:af:48 sdp:3:10              L/73      08/24/2017 22:01:07
10        00:25:ba:30:89:cd sdp:6:10              L/59      08/24/2017 21:48:39
10        38:52:1a:22:d8:60 sdp:13:10             L/50      08/24/2017 22:01:31
10        38:52:1a:30:ae:a1 sdp:11:10             L/55      08/24/2017 22:01:25
-------------------------------------------------------------------------------
No. of Entries: 11
-------------------------------------------------------------------------------
Legend: L=Learned; P=MAC is protected
===============================================================================
```

Figura 79 – Tabela de endereços MAC da VPLS 10.

Note-se que cada SDP e SAP têm um endereço MAC, à exceção do "sdp:5:10" que contem dois endereços MAC. Estes correspondem ao *router* CE com o endereço "00:21:05:c9:b6:86" e à máquina MPLS-1 com o endereço "00:1a:4a:16:01:52". Ambos acedem à VPLS através do "sdp:5:10" no *router* SARF-5(ISCAL).

Os testes de QoS foram realizados entre as máquinas Linux MPLS-1 e MPLS-2, utilizando as ferramentas *Ping*, Iperf e Tcpdump para recolher as medidas pretendidas. Nos próximos capítulos serão apresentados os métodos e os resultados dos testes realizados para cada medida de QoS.

4.2. Largura de Banda

O laboratório Alcatel-Lucent é constituído por algumas ligações *Gigabit Ethernet* sobre fibra e outras *Fast Ethernet* com cabos UTP. Desta forma dependendo do caminho utilizado pode haver mais ou menos largura de banda disponível na rede MPLS. As máquinas de testes MPLS-1 e MPLS-2 têm ambas acesso à rede MPLS através de portas *Fast Ethernet*, logo a largura de banda máxima disponível para testes será de 100 Mb/s. Os LSP utilizados nos testes foram estabelecidos por ligações *Fast Ethernet*, mantendo assim a mesma largura de banda *end-to-end*. Os testes foram realizados com a ferramenta Iperf, que requer uma máquina "Cliente" e uma máquina "Servidor". A máquina cliente transmite o tráfego de teste e a máquina servidor recebe e analisa os resultados. Assim com o intuito de testar a largura de banda foram utilizadas as seguintes opções do Iperf:

- **-u**: Define que o tráfego é enviado com o protocolo UDP.
- **-b**: Define a quantidade de informação a ser transferida por segundo, sendo esta informação apenas referente ao campo Data. Apenas disponível em conjunto com a opção "-u".
- **-t**: Duração do teste em segundos.

- **-l**: Define a quantidade de informação (Data) que é transmitida em cada pacote.
- **-i**: Apresenta resultados no período de segundos definido.

De acordo com as opções apresentadas é possível definir a quantidade de Data que se quer transmitir por segundo e ainda a quantidade de Data que cada pacote pode transportar. A estrutura dos pacotes utilizados nos testes pode ter um mínimo de 60 bytes onde o campo Data contém apenas 18 bytes, ou um máximo de 1514 bytes como está representado na Figura 80.

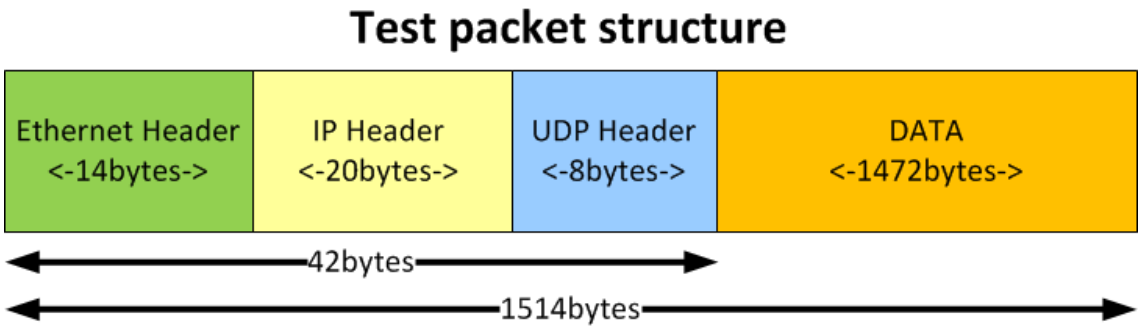

Figura 80 – Representação da estrutura dos pacotes utilizados nos testes realizados.

Para verificar o comportamento da largura de banda e restantes medidas de QoS em função do tamanho de pacotes foram definidos três tamanhos de pacotes, como se pode verificar na Tabela 6.

Tamanho	Cabeçalho	Data	Total
Max	42 bytes	1472 bytes	1514 bytes
Med	42 bytes	727 bytes	769 bytes
Min	42 bytes	18 bytes	60 bytes

Tabela 6 – Tabela com os três tamanhos de pacotes que serão utilizados nos testes.

4.2.1. Largura de banda com o tamanho máximo de pacotes

Numa primeira fase verificou-se a largura de banda máxima com cada tamanho de pacotes numa ligação direta entre as duas máquinas virtuais com um cabo 100BASE-TX. Para definir o valor de largura de banda a utilizar no Iperf com o tamanho de pacotes máximo, realizaram-se os seguintes cálculos:

- **Cálculo da conversão dos valores de bytes para bits.**

  $Inter - frame\ gap = 12 \times 8 = 96\ bits$ [6]

  $Preâmbulo + SFD + FCS = 12 \times 8 = 96\ bits$

  $Header = 42 \times 8 = 336\ bits$

$$Data = 1472 \times 8 = 11776\ bits$$

- **Cálculo do número de pacotes transmitidos por segundo.**

$$nºPacotes = \frac{100\ Mb/s}{96 + 96 + 336 + 11776} = 8127\ Pacotes/s$$

- **Cálculo da largura de banda ocupada pelos cabeçalhos e pelo campo Data**

$$Inter - frame\ gap = 8127 \times 96 = 780\ kb/s$$

$$Preâmbulo + SFD + FCS = 8127 \times 96 = 780\ kb/s$$

$$Header_{LB} = 8127 \times 336 = 2{,}73\ Mb/s$$

$$Data_{LB} = 8127 \times 11776 = 95{,}70\ Mb/s$$

Para testar a largura de banda definiu-se no Iperf um fluxo UDP de 95,7 Mb/s com duração de 20 s e com pacotes de 1472 bytes de Data, como se pode observar na Figura 81.

```
mpls@mpls-tfc-2:~$ iperf -c 10.10.10.100 -u -b 95.7m -t 20 -i 1 -l 1472
------------------------------------------------------------
Client connecting to 10.10.10.100, UDP port 5001
Sending 1472 byte datagrams
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
```

Figura 81 – Comando Iperf para gerar 20 s de fluxos de dados UDP, com ritmo e tamanho de pacotes máximos.

Na Figura 82 pode-se observar que foi possível transmitir uma média de 8127 pacotes/s que dá um total de 99,99 Mb/s.

```
mpls@mpls-tfc-1:~$ iperf -s -u -i 1
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  3] local 10.10.10.100 port 5001 connected with 10.10.10.200 port 39325
[ ID] Interval       Transfer     Bandwidth        Jitter   Lost/Total Datagrams
[  3]  0.0- 1.0 sec  11.4 MBytes  95.6 Mbits/sec   0.119 ms    0/ 8128 (0%)
[  3]  1.0- 2.0 sec  11.4 MBytes  95.3 Mbits/sec   0.122 ms    0/ 8106 (0%)
[  3]  2.0- 3.0 sec  11.4 MBytes  95.6 Mbits/sec   0.126 ms    0/ 8127 (0%)
[  3]  3.0- 4.0 sec  11.4 MBytes  95.6 Mbits/sec   0.120 ms    0/ 8128 (0%)
[  3]  4.0- 5.0 sec  11.4 MBytes  95.6 Mbits/sec   0.123 ms    0/ 8128 (0%)
[  3]  5.0- 6.0 sec  11.4 MBytes  95.6 Mbits/sec   0.120 ms    0/ 8128 (0%)
[  3]  6.0- 7.0 sec  11.4 MBytes  95.6 Mbits/sec   0.121 ms    0/ 8126 (0%)
[  3]  7.0- 8.0 sec  11.4 MBytes  95.6 Mbits/sec   0.121 ms    0/ 8128 (0%)
[  3]  8.0- 9.0 sec  11.4 MBytes  95.6 Mbits/sec   0.121 ms    0/ 8129 (0%)
[  3]  9.0-10.0 sec  11.4 MBytes  95.6 Mbits/sec   0.121 ms    0/ 8128 (0%)
[  3] 10.0-11.0 sec  11.4 MBytes  95.6 Mbits/sec   0.121 ms    0/ 8126 (0%)
[  3] 11.0-12.0 sec  11.4 MBytes  95.6 Mbits/sec   0.122 ms    0/ 8128 (0%)
[  3] 12.0-13.0 sec  11.4 MBytes  95.6 Mbits/sec   0.121 ms    0/ 8128 (0%)
[  3] 13.0-14.0 sec  11.4 MBytes  95.6 Mbits/sec   0.120 ms    0/ 8126 (0%)
[  3] 14.0-15.0 sec  11.4 MBytes  95.6 Mbits/sec   0.121 ms    0/ 8128 (0%)
[  3] 15.0-16.0 sec  11.4 MBytes  95.6 Mbits/sec   0.122 ms    0/ 8129 (0%)
[  3] 16.0-17.0 sec  11.4 MBytes  95.6 Mbits/sec   0.120 ms    0/ 8128 (0%)
[  3] 17.0-18.0 sec  11.4 MBytes  95.6 Mbits/sec   0.120 ms    0/ 8128 (0%)
[  3] 18.0-19.0 sec  11.4 MBytes  95.6 Mbits/sec   0.121 ms    0/ 8126 (0%)
[  3] 19.0-20.0 sec  11.4 MBytes  95.6 Mbits/sec   0.121 ms    0/ 8128 (0%)
[  3]  0.0-20.0 sec   228 MBytes  95.6 Mbits/sec   0.121 ms    0/162602 (0%)
[  3]  0.0-20.0 sec  1 datagrams received out-of-order
```

Figura 82 – Teste de largura de banda entre as duas máquinas virtuais diretamente ligadas, atingindo um total de 99,99 Mb/s.

Realizando o mesmo teste na rede MPLS verificou-se que este obteve perdas de pacotes como se pode observar na Figura 83.

```
mpls@mpls-tfc-1:~$ iperf -s -u -i 1
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  3] local 10.10.10.100 port 5001 connected with 10.10.10.200 port 48371
[ ID] Interval       Transfer     Bandwidth        Jitter   Lost/Total Datagrams
[  3]  0.0- 1.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms    0/ 8014 (0%)
[  3]  1.0- 2.0 sec  11.2 MBytes  94.2 Mbits/sec   0.123 ms    0/ 8011 (0%)
[  3]  2.0- 3.0 sec  11.2 MBytes  94.2 Mbits/sec   0.122 ms    0/ 8012 (0%)
[  3]  3.0- 4.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms    0/ 8013 (0%)
[  3]  4.0- 5.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms    0/ 8013 (0%)
[  3]  5.0- 6.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms    0/ 8011 (0%)
[  3]  6.0- 7.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms    0/ 8013 (0%)
[  3]  7.0- 8.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms   50/ 8063 (0.62%)
[  3]  8.0- 9.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms  135/ 8148 (1.7%)
[  3]  9.0-10.0 sec  11.2 MBytes  94.2 Mbits/sec   0.115 ms  135/ 8146 (1.7%)
[  3] 10.0-11.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms  135/ 8148 (1.7%)
[  3] 11.0-12.0 sec  11.2 MBytes  94.2 Mbits/sec   0.124 ms  136/ 8149 (1.7%)
[  3] 12.0-13.0 sec  11.2 MBytes  94.2 Mbits/sec   0.120 ms  133/ 8145 (1.6%)
[  3] 13.0-14.0 sec  11.2 MBytes  94.2 Mbits/sec   0.120 ms  136/ 8147 (1.7%)
[  3] 14.0-15.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms  134/ 8147 (1.6%)
[  3] 15.0-16.0 sec  11.2 MBytes  94.2 Mbits/sec   0.123 ms  136/ 8149 (1.7%)
[  3] 16.0-17.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms  134/ 8145 (1.6%)
[  3] 17.0-18.0 sec  11.2 MBytes  94.2 Mbits/sec   0.120 ms  136/ 8149 (1.7%)
[  3] 18.0-19.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms  134/ 8146 (1.6%)
[  3] 19.0-20.0 sec  11.2 MBytes  94.2 Mbits/sec   0.122 ms  136/ 8149 (1.7%)
[  3]  0.0-20.4 sec   229 MBytes  94.2 Mbits/sec   0.123 ms 1723/165289 (1%)
```

Figura 83 – Teste de largura de banda na rede MPLS com perdas de pacotes.

Os testes foram realizados nas várias configurações desenvolvidas e na configuração operacional, sendo os resultados iguais em todas uma vez que estes apenas dependem da infraestrutura física. Após este resultado tentou-se verificar onde estavam a ser perdidos os pacotes. Nas estatísticas da interface MPLS por onde o tráfego é encaminhado verificou-se que o número de pacotes transmitidos corresponde ao número de pacotes recebidos na máquina MPLS-1, como se pode observar na Figura 84.

```
*A:SARF-1(CORE)# show router mpls interface toSARF-6 statistics

===============================================================================
MPLS Interface : toSARF-6 (statistics)
===============================================================================
Interface      : toSARF-6
  Transmitted  : Pkts - 163570                Octets - 251894892
  Received     : Pkts - 4                     Octets - 3248
  Invalid      : Labels             - 0
  Invalid      : IPoMPLS Pkts       - 0
  Invalid      : Stack Too Big Pkts - 0
  Invalid      : Other Discard Pkts - 0
  Last Invalid : Label Value        - 0
  Last Invalid : Label Position     - 0
===============================================================================
```

Figura 84 – Estatísticas após teste de largura de banda na interface MPLS no *router* SARF-1(CORE).

Assim, verificou-se as estatísticas da porta de acesso SAP 1/2/4 no *router* SARF-1(CORE), que é a porta de acesso da máquina MPLS-2 à rede do laboratório. Na Figura 85 pode-se observar que o valor de pacotes recebidos está de acordo com os valores anteriores.

```
*A:SARF-1(CORE)# show port 1/2/4

===============================================================================
Ethernet Interface
===============================================================================
Description        : 10/100 Ethernet TX
Interface          : 1/2/4                       Oper Speed       : 100 mbps
Link-level         : Ethernet                    Config Speed     : 100 mbps
Admin State        : up                          Oper Duplex      : full
Oper State         : up                          Config Duplex    : full
Physical Link      : Yes                         MTU              : 1514
Single Fiber Mode  : No
IfIndex            : 37879808                    Hold time up     : 0 seconds
Last State Change  : 09/18/2017 16:58:23         Hold time down   : 0 seconds
Last Cleared Time  : 09/18/2017 20:30:08

Configured Mode    : access                      Encap Type       : null
Dot1Q Ethertype    : 0x8100
Ing. Pool % Rate   : 100                         Egr. Pool % Rate : 100
Net. Egr. Queue Pol: default
Auto-negotiate     : true                        MDI/MDX          : MDX
Config Phy-tx-clock: not-applicable              Oper Phy-tx-clock: N/A
Egress Rate        : Default                     Ingress Rate     : Default
Ingress CBS(bytes) : 130816                      Src-pause        : Disabled
                                                 LACP Tunnel      : Disabled

Down-when-looped   : Disabled                    Keep-alive       : 10
Loop Detected      : False                       Retry            : 120
Use Broadcast Addr : False

Loopback           : none                        Swap Mac Addr    : Disabled
Loopback Time Left : unspecified
Cfm Loopback       : Disabled

Sync. Status Msg.  : Disabled                    Rx Quality Level : N/A
PTP Asymmetry      : 0                           Edge Timestamp   : Disable
Timestamp Capable  : False

Configured Address : 38:52:1a:30:ae:9e
Hardware Address   : 38:52:1a:30:ae:9e
Cfg Alarm          :
Alarm Status       :

===============================================================================
Traffic Statistics
===============================================================================
                                                    Input                Output
-------------------------------------------------------------------------------
Octets                                          248296352                3160
Packets                                            163570                   4
Errors                                                  0                   0
===============================================================================


===============================================================================
Port Statistics
===============================================================================
                                                    Input                Output
-------------------------------------------------------------------------------
Unicast Packets                                    163570                   4
Multicast Packets                                       0                   0
Broadcast Packets                                       0                   0
Discards                                                0                   0
Unknown Proto Discards                                  0
===============================================================================
```

Figura 85 – Estatísticas da porta de entrada da rede do laboratório após teste de largura de banda.

Ainda na continuação destas estatísticas na Figura 86 pode-se observar que nenhum pacote foi descartado.

```
================================================================================
Port Discard Statistics
================================================================================
                                    Input                                Output
Inv L2 Packets    :                     0
Inv IP Packets    :                     0
H.Policed Packets:                      0

CSM Ingress Queues                        CSM Egress Queues
  Hi              :                     0    Common          :                 0
  Medium          :                     0
  Low             :                     0
================================================================================

================================================================================
Port Control Statistics
================================================================================

--------------------------------------------------------------------------------
Ingress Queue CTL              Packets                 Octets
     Forwarded :                 0                       0
     Dropped   :                 0                       N/A

Egress Queue CTL               Packets                 Octets
     Forwarded :                 0                       0
     Dropped   :                 0                       N/A
================================================================================
```

Figura 86 – Continuação das estatísticas na porta de entrada da rede do laboratório após teste de largura de banda.

Conclui-se através destas estatísticas que os pacotes terão sido descartados na máquina MPLS-2 que gerou o tráfego de teste. No entanto a máquina MPLS-2 não apresenta registos de pacotes descartados nas suas estatísticas, como se pode verificar na Figura 87. Nesta é ainda possível verificar que a diferença de o antes e depois de um teste apresenta 165294 pacotes transmitidos. Este valor corresponde ao número de pacotes transmitidos inicialmente pelo Iperf.

```
root@mpls-tfc-2:~# netstat -i ens4
Kernel Interface table
Iface   MTU Met   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
ens3       1500 0    419111      0      5 0       5323216      0      0      0 BMRU
ens4       1500 0    323950      0      0 0      14009374      0      0      0 BMRU
lo        65536 0       166      0      0 0           166      0      0      0 LRU
root@mpls-tfc-2:~# netstat -i ens4
Kernel Interface table
Iface   MTU Met   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
ens3       1500 0    419344      0      5 0       5323388      0      0      0 BMRU
ens4       1500 0    323954      0      0 0      14174668      0      0      0 BMRU
lo        65536 0       166      0      0 0           166      0      0      0 LRU
```

Figura 87 – Estatísticas da interface "ens4" da máquina MPLS-2, antes e depois de gerar o tráfego para um teste de largura de banda.

Tentou-se verificar ainda as estatísticas da carta de rede, no entanto o *driver* instalado não permite recolher estas informações, como se pode observar na Figura 88.

```
root@mpls-tfc-2:~# ethtool -S ens4
no stats available
root@mpls-tfc-2:~# ethtool -i ens4
driver: virtio_net
version: 1.0.0
firmware-version:
expansion-rom-version:
bus-info: 0000:00:04.0
supports-statistics: no
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
root@mpls-tfc-2:~# ethtool ens4
Settings for ens4:
        Supported ports: [ ]
        Supported link modes:   Not reported
        Supported pause frame use: No
        Supports auto-negotiation: No
        Advertised link modes:  Not reported
        Advertised pause frame use: No
        Advertised auto-negotiation: No
        Speed: Unknown!
        Duplex: Unknown! (255)
        Port: Other
        PHYAD: 0
        Transceiver: internal
        Auto-negotiation: off
        Link detected: yes
```

Figura 88 – Estatísticas da carta de rede da máquina MPLS-2.

Apesar de não ser possível confirmar, conclui-se que os pacotes são descartados na máquina virtual MPLS-2, que gerou o tráfego para o teste de largura de banda. A origem deste problema permanece inconclusiva, uma vez que estes problemas não se verificaram nos testes realizados diretamente entre as máquinas virtuais. Desta forma, utilizou-se o método de tentativa e erro para encontrar o valor máximo de largura de banda sem perdas de pacotes. Após algumas tentativas definiu-se um máximo de 94.2 Mb/s de Data, como se pode verificar na Figura 89.

```
mpls@mpls-tfc-1:~$ iperf -s -u -i 1
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  3] local 10.10.10.100 port 5001 connected with 10.10.10.200 port 50217
[ ID] Interval       Transfer     Bandwidth        Jitter   Lost/Total Datagrams
[  3]  0.0- 1.0 sec  11.2 MBytes  94.2 Mbits/sec   0.130 ms    0/ 8014 (0%)
[  3]  1.0- 2.0 sec  11.2 MBytes  94.2 Mbits/sec   0.122 ms    0/ 8013 (0%)
[  3]  2.0- 3.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms    0/ 8013 (0%)
[  3]  3.0- 4.0 sec  11.2 MBytes  94.2 Mbits/sec   0.120 ms    0/ 8011 (0%)
[  3]  4.0- 5.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms    0/ 8012 (0%)
[  3]  5.0- 6.0 sec  11.2 MBytes  94.2 Mbits/sec   0.122 ms    0/ 8013 (0%)
[  3]  6.0- 7.0 sec  11.2 MBytes  94.0 Mbits/sec   0.120 ms    0/ 7995 (0%)
[  3]  7.0- 8.0 sec  11.3 MBytes  94.4 Mbits/sec   0.124 ms    0/ 8028 (0%)
[  3]  8.0- 9.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms    0/ 8013 (0%)
[  3]  9.0-10.0 sec  11.2 MBytes  94.2 Mbits/sec   0.120 ms    0/ 8013 (0%)
[  3] 10.0-11.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms    0/ 8013 (0%)
[  3] 11.0-12.0 sec  11.2 MBytes  94.2 Mbits/sec   0.122 ms    0/ 8011 (0%)
[  3] 12.0-13.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms    0/ 8007 (0%)
[  3] 13.0-14.0 sec  11.2 MBytes  94.3 Mbits/sec   0.123 ms    0/ 8019 (0%)
[  3] 14.0-15.0 sec  11.2 MBytes  94.2 Mbits/sec   0.122 ms    0/ 8012 (0%)
[  3] 15.0-16.0 sec  11.2 MBytes  94.2 Mbits/sec   0.122 ms    0/ 8011 (0%)
[  3] 16.0-17.0 sec  11.2 MBytes  94.2 Mbits/sec   0.124 ms    0/ 8012 (0%)
[  3] 17.0-18.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms    0/ 8013 (0%)
[  3] 18.0-19.0 sec  11.2 MBytes  94.2 Mbits/sec   0.131 ms    0/ 8014 (0%)
[  3] 19.0-20.0 sec  11.2 MBytes  94.2 Mbits/sec   0.130 ms    0/ 8010 (0%)
[  3]  0.0-20.1 sec   226 MBytes  94.2 Mbits/sec   0.121 ms    0/161290 (0%)
```

Figura 89 – Teste de largura de banda de 94.2 Mb/s sem pacotes perdidos e com pacotes de 1514 bytes.

Foram encontradas algumas inconsistências nos valores apresentados pelo Iperf. Este apresenta um total de 161290 pacotes recebidos, mas o somatório dos pacotes recebidos por segundo dá um total de 160247 pacotes. Para confirmar qual destes valores está correto, realizou-se uma captura do tráfego através do comando tcpdump na máquina MPLS-1. Esta captura confirmou que o valor do somatório dos pacotes está correto e que o valor total apresentado pelo Iperf deve-se a um pequeno prolongamento do envio dos pacotes após os 20 s. Através dos seguintes cálculos verificou-se o valor da largura de banda utilizada:

$$nºPacotes = \frac{160247\ Pacotes}{20\ s} = 8012\ Pacotes/s$$

$$LBmax_{Data} = 8012 \times (1472 \times 8) bits = 94{,}35\ Mb/s$$

Com este resultado conclui-se que o Iperf terá uma margem de erro nos resultados apresentados. O valor de 94,35 Mb/s refere-se apenas à informação transmitida no campo Data. Para obter o valor total de largura de banda realizaram-se os seguintes cálculos:

$$LBmax_{Inter-frame\ gap} = 8012 \times (12 \times 8) bits = 769\ kb/s$$

$$LBmax_{Preâmbulo,SFD,FCS} = 8012 \times (12 \times 8) bits = 769\ kb/s$$

$$LBmax_{Header} = 8012 \times (42 \times 8) bits = 2{,}69\ Mb/s$$

Assim no total foram transmitidos:

$$LBmax_{Total} = 0{,}769 + 0{,}769 + 2{,}69 + 94{,}35 = 98{,}58\ Mb/s$$

Verifica-se assim uma diferença de largura de banda de aproximadamente 1,5 Mb/s entre os testes realizados com as máquinas virtuais diretamente ligadas e os testes realizados através da rede MPLS.

4.2.2. Largura de banda com o tamanho médio de pacotes

Os mesmos testes foram realizados com os tamanhos de pacotes médio e mínimo. Com um tamanho de pacote médio verificou-se uma situação idêntica à anterior onde os testes diretos entre as máquinas virtuais tiveram aproximadamente mais 1,5 Mb/s de largura de banda que os testes realizados pela rede MPLS. Na rede MPLS foi utilizado novamente o método de tentativa e erro, tendo os resultados sem perdas de pacotes chegado ao valor de 89.2 Mb/s de Data, como se pode observar na Figura 90.

```
mpls@mpls-tfc-1:~$ iperf -s -u -i 1
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  3] local 10.10.10.100 port 5001 connected with 10.10.10.200 port 59967
[ ID] Interval       Transfer     Bandwidth        Jitter   Lost/Total Datagrams
[  3]  0.0- 1.0 sec  10.6 MBytes  89.1 Mbits/sec   0.084 ms    0/15326 (0%)
[  3]  1.0- 2.0 sec  10.6 MBytes  89.2 Mbits/sec   0.089 ms    0/15337 (0%)
[  3]  2.0- 3.0 sec  10.6 MBytes  89.2 Mbits/sec   0.101 ms    0/15337 (0%)
[  3]  3.0- 4.0 sec  10.6 MBytes  89.2 Mbits/sec   0.099 ms    0/15337 (0%)
[  3]  4.0- 5.0 sec  10.6 MBytes  89.2 Mbits/sec   0.090 ms    0/15334 (0%)
[  3]  5.0- 6.0 sec  10.6 MBytes  89.2 Mbits/sec   0.091 ms    0/15337 (0%)
[  3]  6.0- 7.0 sec  10.6 MBytes  89.2 Mbits/sec   0.085 ms    0/15338 (0%)
[  3]  7.0- 8.0 sec  10.6 MBytes  89.2 Mbits/sec   0.079 ms    0/15337 (0%)
[  3]  8.0- 9.0 sec  10.6 MBytes  89.2 Mbits/sec   0.090 ms    0/15334 (0%)
[  3]  9.0-10.0 sec  10.6 MBytes  89.2 Mbits/sec   0.092 ms    0/15339 (0%)
[  3] 10.0-11.0 sec  10.6 MBytes  89.2 Mbits/sec   0.094 ms    0/15338 (0%)
[  3] 11.0-12.0 sec  10.6 MBytes  89.2 Mbits/sec   0.095 ms    0/15337 (0%)
[  3] 12.0-13.0 sec  10.6 MBytes  89.2 Mbits/sec   0.083 ms    0/15334 (0%)
[  3] 13.0-14.0 sec  10.6 MBytes  89.2 Mbits/sec   0.082 ms    0/15336 (0%)
[  3] 14.0-15.0 sec  10.6 MBytes  89.2 Mbits/sec   0.083 ms    0/15338 (0%)
[  3] 15.0-16.0 sec  10.6 MBytes  89.2 Mbits/sec   0.077 ms    0/15333 (0%)
[  3] 16.0-17.0 sec  10.6 MBytes  89.2 Mbits/sec   0.091 ms    0/15338 (0%)
[  3] 17.0-18.0 sec  10.6 MBytes  89.2 Mbits/sec   0.084 ms    0/15337 (0%)
[  3] 18.0-19.0 sec  10.6 MBytes  89.2 Mbits/sec   0.090 ms    0/15338 (0%)
[  3] 19.0-20.0 sec  10.6 MBytes  89.2 Mbits/sec   0.095 ms    0/15333 (0%)
[  3]  0.0-20.1 sec   213 MBytes  89.2 Mbits/sec   0.081 ms    0/307687 (0%)
```

Figura 90 – Teste de largura de banda de 89.2 Mb/s sem pacotes perdidos e com pacotes de tamanho médio.

Neste teste também foi encontrada uma inconsistência no valor total de pacotes, tendo o somatório de pacotes enviados por segundo um total de 306718 pacotes. O valor total de largura de banda de cada componente pode ser calculado através de:

$$nºPacotes = \frac{306718\ Pacotes}{20\ s} = 15335\ Pacotes/s$$

$$LBmed_{Inter-frame\ gap} = 15335 \times (12 \times 8) bits = 1{,}47\ Mb/s$$

$$LBmed_{Preâmbulo,SFD,FCS} = 15335 \times (12 \times 8) bits = 1{,}47\ Mb/s$$

$$LBmed_{Header} = 15335 \times (42 \times 8) bits = 5{,}15\ Mb/s$$

$$LBmed_{Data} = 15335 \times (727 \times 8) bits = 89{,}19\ Mb/s$$

$$LBmed_{Total} = 1{,}47 + 1{,}47 + 5{,}15 + 89{,}19 = 97{,}28\ Mb/s$$

O valor total de largura de banda obtido com pacotes de tamanho médio é ligeiramente inferior ao valor obtido com pacotes de tamanho máximo. Esta ligeira diferença pode-se justificar com um aumento aproximadamente do dobro do número de pacotes transmitidos.

4.2.3. Largura de banda com o tamanho mínimo de pacotes

O mesmo teste foi ainda realizado para o tamanho mínimo dos pacotes. Neste caso o valor de largura de banda máxima ficou muito a baixo do esperado, tanto nos testes realizados entre as máquinas virtuais diretamente ligadas como nos testes através da rede MPLS. Utilizando o método de tentativa e erro nos testes com ligação direta entre as máquinas virtuais foi possível atingir um valor de 9,96 Mb/s, como se pode observar na Figura 91.

```
mpls@mpls-tfc-1:~$ iperf -s -u -i 1
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  3] local 10.10.10.100 port 5001 connected with 10.10.10.200 port 33171
[ ID] Interval       Transfer     Bandwidth        Jitter   Lost/Total Datagrams
[  3]  0.0- 1.0 sec  1.19 MBytes  9.96 Mbits/sec   0.013 ms    0/69194 (0%)
[  3]  1.0- 2.0 sec  1.19 MBytes  9.96 Mbits/sec   0.015 ms    0/69136 (0%)
[  3]  2.0- 3.0 sec  1.19 MBytes  9.96 Mbits/sec   0.018 ms    0/69144 (0%)
[  3]  3.0- 4.0 sec  1.19 MBytes  9.95 Mbits/sec   0.015 ms    0/69131 (0%)
[  3]  4.0- 5.0 sec  1.19 MBytes  9.95 Mbits/sec   0.014 ms    0/69113 (0%)
[  3]  5.0- 6.0 sec  1.19 MBytes  9.96 Mbits/sec   0.019 ms    0/69151 (0%)
[  3]  6.0- 7.0 sec  1.19 MBytes  9.96 Mbits/sec   0.019 ms    0/69158 (0%)
[  3]  7.0- 8.0 sec  1.19 MBytes  9.96 Mbits/sec   0.017 ms    0/69155 (0%)
[  3]  8.0- 9.0 sec  1.19 MBytes  9.96 Mbits/sec   0.015 ms    0/69151 (0%)
[  3]  9.0-10.0 sec  1.19 MBytes  9.96 Mbits/sec   0.015 ms    0/69158 (0%)
[  3] 10.0-11.0 sec  1.19 MBytes  9.96 Mbits/sec   0.016 ms    0/69155 (0%)
[  3] 11.0-12.0 sec  1.19 MBytes  9.96 Mbits/sec   0.018 ms    0/69171 (0%)
[  3] 12.0-13.0 sec  1.19 MBytes  9.96 Mbits/sec   0.024 ms    0/69154 (0%)
[  3] 13.0-14.0 sec  1.19 MBytes  9.96 Mbits/sec   0.018 ms    0/69151 (0%)
[  3] 14.0-15.0 sec  1.19 MBytes  9.95 Mbits/sec   0.015 ms    0/69107 (0%)
[  3] 15.0-16.0 sec  1.19 MBytes  9.95 Mbits/sec   0.016 ms    0/69102 (0%)
[  3] 16.0-17.0 sec  1.19 MBytes  9.95 Mbits/sec   0.026 ms    0/69102 (0%)
[  3] 17.0-18.0 sec  1.19 MBytes  9.96 Mbits/sec   0.018 ms    0/69143 (0%)
[  3] 18.0-19.0 sec  1.19 MBytes  9.95 Mbits/sec   0.014 ms    0/69109 (0%)
[  3]  0.0-20.0 sec  23.7 MBytes  9.96 Mbits/sec   0.022 ms    0/1382824 (0%)
[  3]  0.0-20.0 sec  1 datagrams received out-of-order
```

Figura 91 – Teste de largura de banda de 9.96 Mb/s sem pacotes perdidos e com pacotes de tamanho mínimo.

No entanto, houve algumas repetições do mesmo teste que obtiveram perdas de pacotes, como se pode observar na Figura 92.

```
mpls@mpls-tfc-1:~$ iperf -s -u -i 1
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  3] local 10.10.10.100 port 5001 connected with 10.10.10.200 port 32864
[  3]  0.0- 1.0 sec  1.18 MBytes  9.94 Mbits/sec   0.020 ms    9/69040 (0.013%)
[  3]  1.0- 2.0 sec  1.19 MBytes  9.95 Mbits/sec   0.023 ms    0/69102 (0%)
[  3]  2.0- 3.0 sec  1.19 MBytes  9.95 Mbits/sec   0.017 ms    7/69109 (0.01%)
[  3]  3.0- 4.0 sec  1.19 MBytes  9.95 Mbits/sec   0.021 ms   14/69116 (0.02%)
[  3]  4.0- 5.0 sec  1.19 MBytes  9.99 Mbits/sec   0.014 ms    7/69370 (0.01%)
[  3]  5.0- 6.0 sec  1.19 MBytes  9.96 Mbits/sec   0.015 ms   33/69166 (0.048%)
[  3]  6.0- 7.0 sec  1.19 MBytes  9.96 Mbits/sec   0.017 ms    0/69193 (0%)
[  3]  7.0- 8.0 sec  1.19 MBytes  9.95 Mbits/sec   0.016 ms   16/69106 (0.023%)
[  3]  8.0- 9.0 sec  1.19 MBytes  9.96 Mbits/sec   0.016 ms    0/69132 (0%)
[  3]  9.0-10.0 sec  1.19 MBytes  9.96 Mbits/sec   0.019 ms    0/69174 (0%)
[  3] 10.0-11.0 sec  1.18 MBytes  9.92 Mbits/sec   0.019 ms   12/68933 (0.017%)
[  3] 11.0-12.0 sec  1.19 MBytes  9.96 Mbits/sec   0.019 ms   16/69175 (0.023%)
[  3] 12.0-13.0 sec  1.19 MBytes  9.96 Mbits/sec   0.015 ms    2/69155 (0.0029%)
[  3] 13.0-14.0 sec  1.19 MBytes  9.95 Mbits/sec   0.016 ms   64/69153 (0.093%)
[  3] 14.0-15.0 sec  1.19 MBytes  9.96 Mbits/sec   0.023 ms    0/69152 (0%)
[  3] 15.0-16.0 sec  1.19 MBytes  9.95 Mbits/sec   0.015 ms    0/69125 (0%)
[  3] 16.0-17.0 sec  1.19 MBytes  9.96 Mbits/sec   0.023 ms    0/69151 (0%)
[  3] 17.0-18.0 sec  1.19 MBytes  9.95 Mbits/sec   0.025 ms    0/69128 (0%)
[  3] 18.0-19.0 sec  1.19 MBytes  9.96 Mbits/sec   0.014 ms    0/69148 (0%)
[  3] 19.0-20.0 sec  1.19 MBytes  9.95 Mbits/sec   0.019 ms    0/69109 (0%)
[  3]  0.0-20.0 sec  23.7 MBytes  9.95 Mbits/sec   0.086 ms  179/1382753 (0.013%)
[  3]  0.0-20.0 sec  1 datagrams received out-of-order
```

Figura 92 – Teste de largura de banda de 9.96 Mb/s com pacotes perdidos e com pacotes de tamanho mínimo.

Este teste obteve um resultado muito inferior aos anteriores, no entanto este valor é justificável devido a uma limitação do número de pacotes que uma máquina virtual consegue enviar por segundo, sendo comum estas atingirem 100 kp/s [17]. Nos testes realizados foi possível atingir mais de 70 kp/s, no entanto estes testes apresentaram alguns pacotes perdidos. Segundo Rizzo *et al.* [17], uma máquina virtual sem otimizações envia um pacote por cada *interrupt*, logo o número de pacotes enviados por segundo está limitado pelo número de *interrupts* que a máquina consegue processar. Note-se que para atingir os 100 Mb/s com este tamanho de pacote seria necessário transmitir 148809 p/s, ou seja mais do dobro do número de pacotes que foi possível transmitir nos testes sem perdas.

Nos testes realizados na rede MPLS verificou-se que apenas foi possível transmitir pacotes sem perdas com a largura de banda de 9 Mb/s, como se pode observar na Figura 93.

```
mpls@mpls-tfc-1:~$ iperf -s -u -i 1
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  3] local 10.10.10.100 port 5001 connected with 10.10.10.200 port 47031
[ ID] Interval       Transfer     Bandwidth        Jitter   Lost/Total Datagrams
[  3]  0.0- 1.0 sec  1.07 MBytes  9.00 Mbits/sec   0.016 ms    0/62490 (0%)
[  3]  1.0- 2.0 sec  1.07 MBytes  9.00 Mbits/sec   0.019 ms    0/62472 (0%)
[  3]  2.0- 3.0 sec  1.07 MBytes  9.00 Mbits/sec   0.024 ms    0/62481 (0%)
[  3]  3.0- 4.0 sec  1.07 MBytes  8.98 Mbits/sec   0.025 ms    0/62336 (0%)
[  3]  4.0- 5.0 sec  1.07 MBytes  9.00 Mbits/sec   0.022 ms    0/62478 (0%)
[  3]  5.0- 6.0 sec  1.07 MBytes  8.99 Mbits/sec   0.023 ms    0/62419 (0%)
[  3]  6.0- 7.0 sec  1.07 MBytes  8.99 Mbits/sec   0.019 ms    0/62456 (0%)
[  3]  7.0- 8.0 sec  1.07 MBytes  8.99 Mbits/sec   0.020 ms    0/62451 (0%)
[  3]  8.0- 9.0 sec  1.07 MBytes  9.00 Mbits/sec   0.021 ms    0/62488 (0%)
[  3]  9.0-10.0 sec  1.07 MBytes  8.99 Mbits/sec   0.026 ms    0/62462 (0%)
[  3] 10.0-11.0 sec  1.07 MBytes  9.00 Mbits/sec   0.023 ms    0/62484 (0%)
[  3] 11.0-12.0 sec  1.07 MBytes  9.00 Mbits/sec   0.022 ms    0/62481 (0%)
[  3] 12.0-13.0 sec  1.07 MBytes  8.97 Mbits/sec   0.024 ms    0/62321 (0%)
[  3] 13.0-14.0 sec  1.07 MBytes  9.00 Mbits/sec   0.018 ms    0/62479 (0%)
[  3] 14.0-15.0 sec  1.07 MBytes  9.00 Mbits/sec   0.022 ms    0/62492 (0%)
[  3] 15.0-16.0 sec  1.07 MBytes  9.00 Mbits/sec   0.017 ms    0/62475 (0%)
[  3] 16.0-17.0 sec  1.07 MBytes  9.00 Mbits/sec   0.017 ms    0/62501 (0%)
[  3] 17.0-18.0 sec  1.07 MBytes  9.00 Mbits/sec   0.025 ms    0/62484 (0%)
[  3] 18.0-19.0 sec  1.07 MBytes  9.00 Mbits/sec   0.016 ms    0/62481 (0%)
[  3]  0.0-20.0 sec  21.4 MBytes  8.99 Mbits/sec   0.024 ms    0/1249184 (0%)
```

Figura 93 – Teste de largura de banda de 9 Mb/s sem pacotes perdidos e com pacotes de tamanho mínimo.

O valor total de largura de banda na rede MPLS sem pacotes perdidos pode ser calculado através de:

$$nºPacotes = \frac{1249184\ Pacotes}{20\ s} = 62459\ Pacotes/s$$

$$LBmin_{Inter-frame\ gap} = 62459 \times (12 \times 8) bits = 5{,}99\ Mb/s$$

$$LBmin_{Preâmbulo,SFD,FCS} = 62459 \times (12 \times 8) bits = 5{,}99\ Mb/s$$

$$LBmin_{Header} = 62459 \times (42 \times 8) bits = 20{,}98\ Mb/s$$

$$LBmin_{Data} = 62459 \times (18 \times 8) bits = 8{,}99\ Mb/s$$

$$LBmin_{Total} = 5{,}99 + 5{,}99 + 20{,}98 + 8{,}99 = 41.95\ Mb/s$$

A largura de banda com pacotes de tamanho mínimo é muito inferior à largura de banda obtida com os outros tamanhos de pacotes, devido à limitação do número de pacotes que as máquinas virtuais conseguem enviar por segundo.

4.2.4. Resultados dos testes de largura de banda

Na Figura 94 pode-se observar uma comparação dos resultados da largura de banda total, obtidos com cada tamanho de pacote para a rede MPLS e para a ligação direta entre máquinas virtuais.

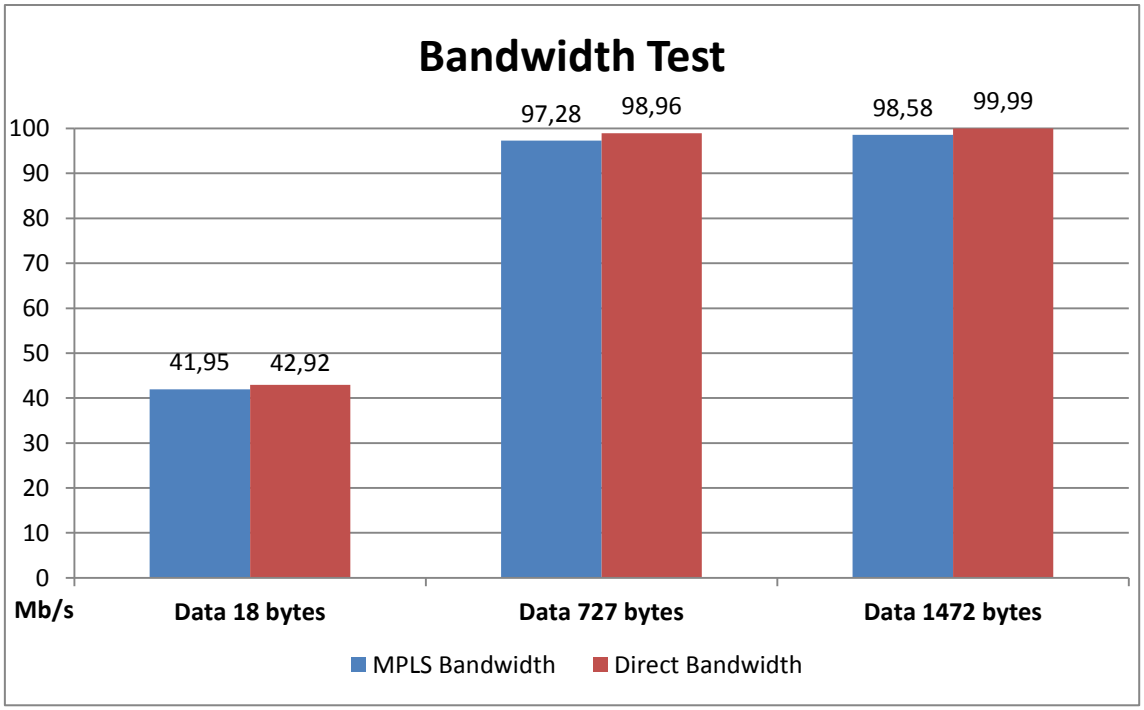

Figura 94 – Comparação dos resultados de largura de banda entre a rede MPLS e as máquinas diretamente ligadas com os três tamanhos de pacotes definidos.

Este estudo teve como principal objetivo a definição de três tamanhos de pacotes e a largura de banda máxima correspondente. Com base nestes valores, foi possível realizar testes com diferentes objetivos para avaliar as restantes medidas de QoS.

4.3. *Delay*

O *delay* pode ser medido apenas numa direção ou no conjunto de ida e volta. A medição do *delay* apenas numa direção implica a sincronização temporal das duas máquinas Linux através de protocolos como o *Network Time Protocol* (NTP). As configurações testadas não influenciam diretamente este parâmetro, por isso optou-se por testar apenas o tempo de ida e volta, também conhecido por *Round-Trip Time* (RTT).

Os testes focaram-se na forma como o *delay* é afetado pela diferença do tamanho dos pacotes e ainda na diferença entre utilizar a rede MPLS ou ligar diretamente as duas máquinas Linux MPLS-1 e MPLS-2. Os testes foram realizados em todas as configurações desenvolvidas e em ambos os sentidos, tendo-se verificado valores idênticos independentemente da configuração ou sentido.

Com os tamanhos de pacotes definido anteriormente, foram realizados testes com a ferramenta *ping* que envia 10 pacotes ICMP. Na Figura 95 está um exemplo do teste realizado da máquina MPLS-1 para a máquina MPLS-2 com o tamanho mínimo de 18 bytes de Data.

```
mpls@mpls-tfc-1:~$ ping 10.10.10.200 -s 18
PING 10.10.10.200 (10.10.10.200) 18(46) bytes of data.
26 bytes from 10.10.10.200: icmp_seq=1 ttl=64 time=0.774 ms
26 bytes from 10.10.10.200: icmp_seq=2 ttl=64 time=0.679 ms
26 bytes from 10.10.10.200: icmp_seq=3 ttl=64 time=0.781 ms
26 bytes from 10.10.10.200: icmp_seq=4 ttl=64 time=0.792 ms
26 bytes from 10.10.10.200: icmp_seq=5 ttl=64 time=0.642 ms
26 bytes from 10.10.10.200: icmp_seq=6 ttl=64 time=0.698 ms
26 bytes from 10.10.10.200: icmp_seq=7 ttl=64 time=0.672 ms
26 bytes from 10.10.10.200: icmp_seq=8 ttl=64 time=0.742 ms
26 bytes from 10.10.10.200: icmp_seq=9 ttl=64 time=0.782 ms
26 bytes from 10.10.10.200: icmp_seq=10 ttl=64 time=0.712 ms
^C
--- 10.10.10.200 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9001ms
rtt min/avg/max/mdev = 0.642/0.727/0.792/0.056 ms
```

Figura 95 – Teste de RTT entre as máquinas Linux MPLS-1 e MPLS-2 com o tamanho mínimo de pacotes.

4.3.1. Resultados do RTT com variação do tamanho dos pacotes

Os resultados do mínimo, máximo e média de RTT obtidos para os diferentes tamanhos de pacotes podem ser observados na Figura 96.

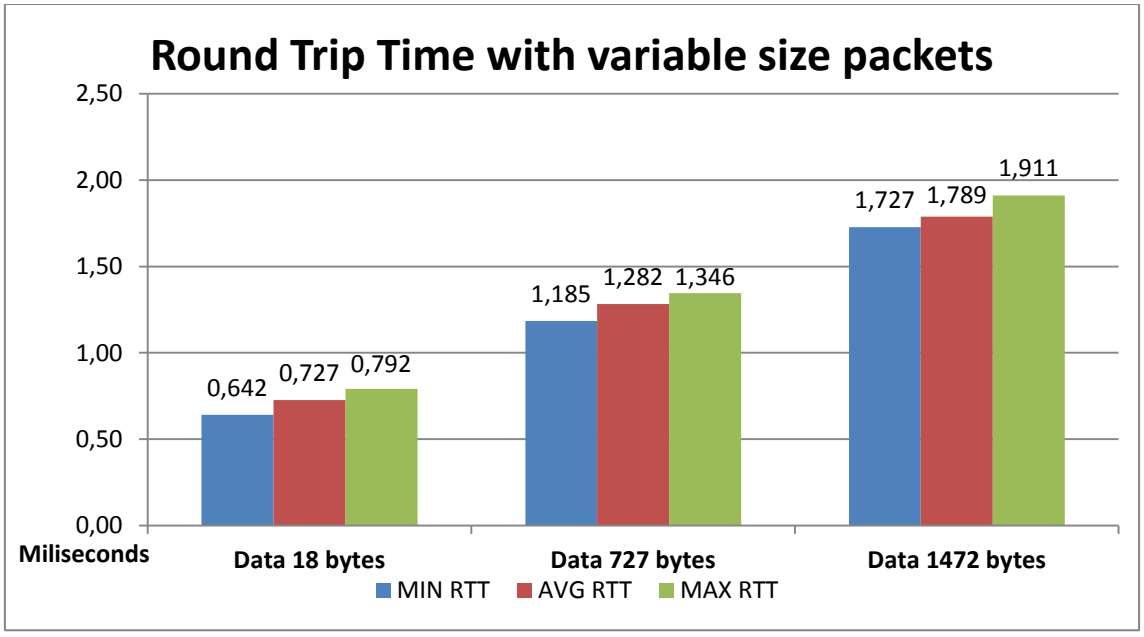

Figura 96 – Resultados do mínimo, média e máximo de RTT para os três tamanhos de pacotes definidos.

Conclui-se que o aumento do tamanho dos pacotes resulta num aumento do *delay*. Os pacotes de maiores dimensões necessitam de mais tempo para serem transmitidos, aumentando assim o *delay* entre pacotes.

4.3.2. Resultados do RTT na rede MPLS *vs* ligação direta

Para realizar esta comparação foi necessário ligar diretamente as duas máquinas MPLS-1 e MPLS-2 e repetir os testes anteriores. Na Figura 97 pode-se observar a comparação da média de RTT para os três tamanhos de pacotes anteriormente definidos.

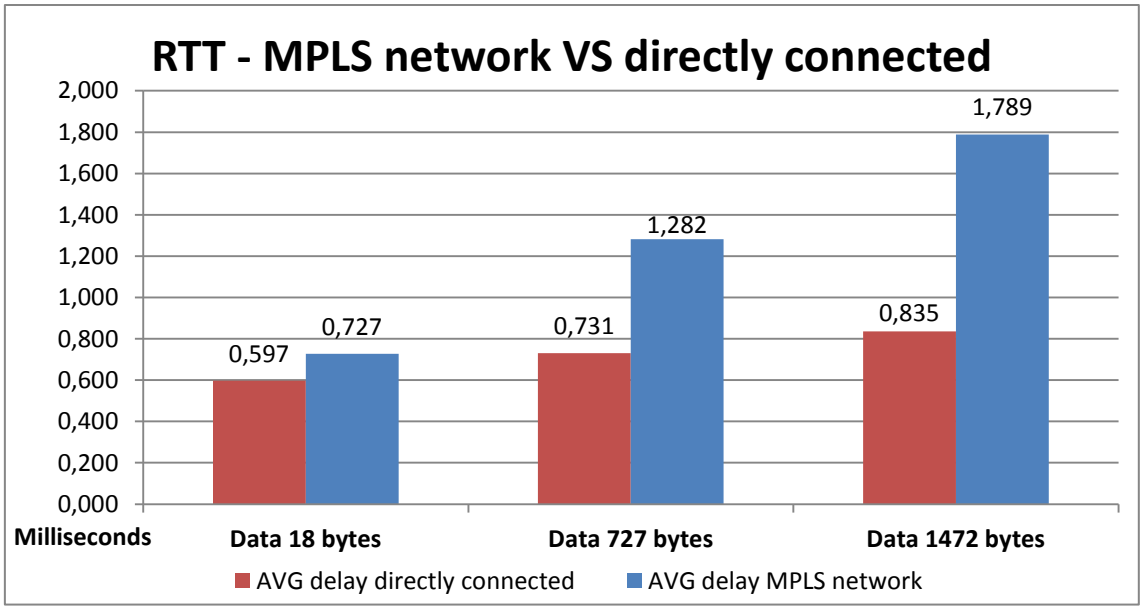

Figura 97 – Resultados da comparação da média de RTT entre uma rede MPLS e duas máquinas diretamente ligadas, com três tamanhos de pacotes.

Os resultados mostram que a ligação direta entre as máquinas MPLS-1 e MPLS-2 tem em média menos *delay*. O *delay* introduzido pela rede MPLS deve-se ao tempo necessário para cada *router* realizar a transmissão, *queuing*, processamento e à propagação dos pacotes. Note-se ainda que com o aumento do tamanho dos pacotes este processo é cada vez mais demorado, aumentando progressivamente a diferença para a transmissão direta entre as duas máquinas.

4.4. *Jitter*

O *Jitter* representa a variação do *delay* entre pacotes. Idealmente o teste ao *jitter* seria feito com vários fluxos de dados com ritmos diferentes e tamanhos de pacotes diferentes [18]. No entanto, os métodos disponíveis são limitados e a ferramenta Iperf apenas permite que sejam transmitidos vários fluxos de dados com o mesmo ritmo e o mesmo tamanho de pacotes. Assim, de forma a testar o *jitter* utilizou-se a ferramenta Iperf para criar três fluxos de dados concorrentes com os três tamanhos de pacotes definidos anteriormente. Os testes focaram-se no impacto da variação do tamanho dos pacotes utilizados e na diferença entre utilizar a rede MPLS ou uma ligação direta entre as duas máquinas MPLS-1 e MPLS-2.

Na Figura 98 pode-se observar o comando Iperf utilizado na máquina cliente, em que "–P 3" define que serão utilizados três fluxos concorrentes. Estes utilizam todos o mesmo tamanho de pacote definido por "-l 1472".

```
mpls@mpls-tfc-2:~$ iperf -c 10.10.10.100 -u -b 31.4m -P 3 -t 20 -i 1 -l 1472
------------------------------------------------------------
Client connecting to 10.10.10.100, UDP port 5001
Sending 1472 byte datagrams
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  5] local 10.10.10.200 port 47222 connected with 10.10.10.100 port 5001
[  3] local 10.10.10.200 port 50934 connected with 10.10.10.100 port 5001
[  4] local 10.10.10.200 port 54828 connected with 10.10.10.100 port 5001
```

Figura 98 – Comando Iperf utilizado na máquina cliente para gerar três fluxos concorrentes.

Na Figura 99 pode-se verificar um exemplo da receção dos fluxos de dados no servidor (MPLS-1).

```
mpls@mpls-tfc-1:~$ iperf -s -u -i 1
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  3] local 10.10.10.100 port 5001 connected with 10.10.10.200 port 36687
[  4] local 10.10.10.100 port 5001 connected with 10.10.10.200 port 34776
[  5] local 10.10.10.100 port 5001 connected with 10.10.10.200 port 52224
[ ID] Interval       Transfer     Bandwidth        Jitter   Lost/Total Datagrams
[  3]  0.0- 1.0 sec  3.74 MBytes  31.4 Mbits/sec   0.138 ms    0/ 2667 (0%)
[  4]  0.0- 1.0 sec  3.74 MBytes  31.4 Mbits/sec   0.160 ms    0/ 2666 (0%)
[  5]  0.0- 1.0 sec  3.74 MBytes  31.3 Mbits/sec   0.197 ms    2/ 2667 (0.075%)
[SUM]  0.0- 1.0 sec  11.2 MBytes  94.1 Mbits/sec
[  3]  1.0- 2.0 sec  3.74 MBytes  31.4 Mbits/sec   0.142 ms    0/ 2666 (0%)
[  4]  1.0- 2.0 sec  3.74 MBytes  31.4 Mbits/sec   0.167 ms    0/ 2667 (0%)
[  5]  1.0- 2.0 sec  3.74 MBytes  31.4 Mbits/sec   0.142 ms    0/ 2667 (0%)
[SUM]  1.0- 2.0 sec  11.2 MBytes  94.1 Mbits/sec
[  3]  2.0- 3.0 sec  3.74 MBytes  31.4 Mbits/sec   0.147 ms    0/ 2667 (0%)
[  4]  2.0- 3.0 sec  3.74 MBytes  31.4 Mbits/sec   0.163 ms    0/ 2666 (0%)
[  5]  2.0- 3.0 sec  3.74 MBytes  31.4 Mbits/sec   0.151 ms    0/ 2666 (0%)
[SUM]  2.0- 3.0 sec  11.2 MBytes  94.1 Mbits/sec
[  3]  3.0- 4.0 sec  3.74 MBytes  31.4 Mbits/sec   0.131 ms    0/ 2666 (0%)
[  4]  3.0- 4.0 sec  3.74 MBytes  31.4 Mbits/sec   0.183 ms    0/ 2668 (0%)
[  5]  3.0- 4.0 sec  3.74 MBytes  31.4 Mbits/sec   0.146 ms    0/ 2666 (0%)
[SUM]  3.0- 4.0 sec  11.2 MBytes  94.1 Mbits/sec
[  3]  4.0- 5.0 sec  3.73 MBytes  31.3 Mbits/sec   0.162 ms    0/ 2658 (0%)
[  4]  4.0- 5.0 sec  3.72 MBytes  31.2 Mbits/sec   0.164 ms    0/ 2657 (0%)
[  5]  4.0- 5.0 sec  3.73 MBytes  31.3 Mbits/sec   0.151 ms    0/ 2658 (0%)
[SUM]  4.0- 5.0 sec  11.2 MBytes  93.8 Mbits/sec
[  3]  5.0- 6.0 sec  3.74 MBytes  31.4 Mbits/sec   0.139 ms    0/ 2671 (0%)
[  4]  5.0- 6.0 sec  3.74 MBytes  31.4 Mbits/sec   0.146 ms    0/ 2671 (0%)
[  5]  5.0- 6.0 sec  3.74 MBytes  31.4 Mbits/sec   0.174 ms    0/ 2671 (0%)
[SUM]  5.0- 6.0 sec  11.2 MBytes  94.2 Mbits/sec
[  3]  6.0- 7.0 sec  3.74 MBytes  31.4 Mbits/sec   0.133 ms    0/ 2671 (0%)
[  4]  6.0- 7.0 sec  3.74 MBytes  31.4 Mbits/sec   0.152 ms    0/ 2670 (0%)
[  5]  6.0- 7.0 sec  3.74 MBytes  31.4 Mbits/sec   0.149 ms    0/ 2670 (0%)
[SUM]  6.0- 7.0 sec  11.2 MBytes  94.2 Mbits/sec
[  3]  7.0- 8.0 sec  3.74 MBytes  31.4 Mbits/sec   0.142 ms    0/ 2668 (0%)
[  4]  7.0- 8.0 sec  3.74 MBytes  31.4 Mbits/sec   0.169 ms    0/ 2668 (0%)
[  5]  7.0- 8.0 sec  3.74 MBytes  31.4 Mbits/sec   0.160 ms    0/ 2668 (0%)
[SUM]  7.0- 8.0 sec  11.2 MBytes  94.1 Mbits/sec
[  3]  8.0- 9.0 sec  3.74 MBytes  31.4 Mbits/sec   0.147 ms    0/ 2666 (0%)
[  4]  8.0- 9.0 sec  3.74 MBytes  31.4 Mbits/sec   0.190 ms    0/ 2667 (0%)
[  5]  8.0- 9.0 sec  3.74 MBytes  31.4 Mbits/sec   0.192 ms    0/ 2667 (0%)
[SUM]  8.0- 9.0 sec  11.2 MBytes  94.1 Mbits/sec
[  3]  9.0-10.0 sec  3.74 MBytes  31.4 Mbits/sec   0.148 ms    0/ 2666 (0%)
[  4]  9.0-10.0 sec  3.74 MBytes  31.3 Mbits/sec   0.146 ms    0/ 2665 (0%)
[  5]  9.0-10.0 sec  3.74 MBytes  31.4 Mbits/sec   0.169 ms    0/ 2666 (0%)
[SUM]  9.0-10.0 sec  11.2 MBytes  94.0 Mbits/sec
[  3] 10.0-11.0 sec  3.74 MBytes  31.4 Mbits/sec   0.154 ms    0/ 2668 (0%)
[  4] 10.0-11.0 sec  3.74 MBytes  31.4 Mbits/sec   0.163 ms    0/ 2668 (0%)
[  5] 10.0-11.0 sec  3.74 MBytes  31.4 Mbits/sec   0.167 ms    0/ 2668 (0%)
[SUM] 10.0-11.0 sec  11.2 MBytes  94.1 Mbits/sec
[  3] 11.0-12.0 sec  3.74 MBytes  31.3 Mbits/sec   0.171 ms    0/ 2665 (0%)
[  4] 11.0-12.0 sec  3.74 MBytes  31.4 Mbits/sec   0.149 ms    0/ 2666 (0%)
[  5] 11.0-12.0 sec  3.74 MBytes  31.4 Mbits/sec   0.155 ms    0/ 2666 (0%)
[SUM] 11.0-12.0 sec  11.2 MBytes  94.0 Mbits/sec
[  3] 12.0-13.0 sec  3.74 MBytes  31.4 Mbits/sec   0.128 ms    0/ 2667 (0%)
[  4] 12.0-13.0 sec  3.74 MBytes  31.4 Mbits/sec   0.180 ms    0/ 2668 (0%)
[  5] 12.0-13.0 sec  3.74 MBytes  31.4 Mbits/sec   0.147 ms    0/ 2667 (0%)
[SUM] 12.0-13.0 sec  11.2 MBytes  94.1 Mbits/sec
[  3] 13.0-14.0 sec  3.73 MBytes  31.3 Mbits/sec   0.149 ms    0/ 2664 (0%)
[  4] 13.0-14.0 sec  3.73 MBytes  31.3 Mbits/sec   0.139 ms    0/ 2663 (0%)
[  5] 13.0-14.0 sec  3.73 MBytes  31.3 Mbits/sec   0.184 ms    0/ 2663 (0%)
[SUM] 13.0-14.0 sec  11.2 MBytes  94.0 Mbits/sec
[  3] 14.0-15.0 sec  3.73 MBytes  31.3 Mbits/sec   0.131 ms    0/ 2663 (0%)
[  4] 14.0-15.0 sec  3.73 MBytes  31.3 Mbits/sec   0.143 ms    0/ 2662 (0%)
[  5] 14.0-15.0 sec  3.73 MBytes  31.3 Mbits/sec   0.165 ms    0/ 2663 (0%)
[SUM] 14.0-15.0 sec  11.2 MBytes  93.9 Mbits/sec
[  3] 15.0-16.0 sec  3.74 MBytes  31.4 Mbits/sec   0.153 ms    0/ 2671 (0%)
[  4] 15.0-16.0 sec  3.74 MBytes  31.4 Mbits/sec   0.158 ms    0/ 2671 (0%)
[  5] 15.0-16.0 sec  3.74 MBytes  31.4 Mbits/sec   0.130 ms    0/ 2671 (0%)
[SUM] 15.0-16.0 sec  11.2 MBytes  94.2 Mbits/sec
[  3] 16.0-17.0 sec  3.74 MBytes  31.4 Mbits/sec   0.146 ms    0/ 2669 (0%)
[  4] 16.0-17.0 sec  3.74 MBytes  31.4 Mbits/sec   0.137 ms    0/ 2670 (0%)
[  5] 16.0-17.0 sec  3.74 MBytes  31.4 Mbits/sec   0.185 ms    0/ 2669 (0%)
[SUM] 16.0-17.0 sec  11.2 MBytes  94.2 Mbits/sec
[  3] 17.0-18.0 sec  3.74 MBytes  31.4 Mbits/sec   0.140 ms    0/ 2667 (0%)
[  4] 17.0-18.0 sec  3.74 MBytes  31.4 Mbits/sec   0.160 ms    0/ 2667 (0%)
[  5] 17.0-18.0 sec  3.74 MBytes  31.4 Mbits/sec   0.149 ms    0/ 2667 (0%)
[SUM] 17.0-18.0 sec  11.2 MBytes  94.1 Mbits/sec
[  3] 18.0-19.0 sec  3.74 MBytes  31.4 Mbits/sec   0.132 ms    0/ 2666 (0%)
[  4] 18.0-19.0 sec  3.74 MBytes  31.4 Mbits/sec   0.155 ms    0/ 2667 (0%)
[  5] 18.0-19.0 sec  3.74 MBytes  31.4 Mbits/sec   0.162 ms    0/ 2667 (0%)
[SUM] 18.0-19.0 sec  11.2 MBytes  94.1 Mbits/sec
[  3] 19.0-20.0 sec  3.74 MBytes  31.3 Mbits/sec   0.157 ms    0/ 2665 (0%)
[  3]  0.0-20.0 sec  74.8 MBytes  31.3 Mbits/sec   0.640 ms    0/53334 (0%)
[  3]  0.0-20.0 sec  1 datagrams received out-of-order
[  4] 19.0-20.0 sec  3.73 MBytes  31.3 Mbits/sec   0.155 ms    0/ 2664 (0%)
[  4]  0.0-20.0 sec  74.8 MBytes  31.4 Mbits/sec   0.150 ms    0/53332 (0%)
[  4]  0.0-20.0 sec  1 datagrams received out-of-order
[  5] 19.0-20.0 sec  3.74 MBytes  31.3 Mbits/sec   0.153 ms    0/ 2665 (0%)
[SUM] 19.0-20.0 sec  11.2 MBytes  94.0 Mbits/sec
[  5]  0.0-20.0 sec  74.8 MBytes  31.4 Mbits/sec   0.436 ms    1/53333 (0.0019%)
[  5]  0.0-20.0 sec  1 datagrams received out-of-order
[SUM]  0.0-20.0 sec   224 MBytes  94.0 Mbits/sec
```

Figura 99 – Exemplo da receção de três fluxos de dados concorrentes para testar o *jitter*.

Os testes foram realizados em todas as configurações desenvolvidas e em ambos os sentidos, tendo-se verificado valores idênticos independentemente da configuração ou sentido. Assim, os resultados tal como no capítulo anterior serão apresentados apenas com referência às três variações no tamanho dos pacotes.

4.4.1. Resultados do *jitter* com variação do tamanho de pacotes

Os resultados dos três fluxos de dados em concorrência com os três tamanhos de pacotes podem ser observados na Figura 100. Estes são ainda comparados com o *jitter* de um fluxo de dados sem concorrência utilizando o respetivo tamanho de pacote.

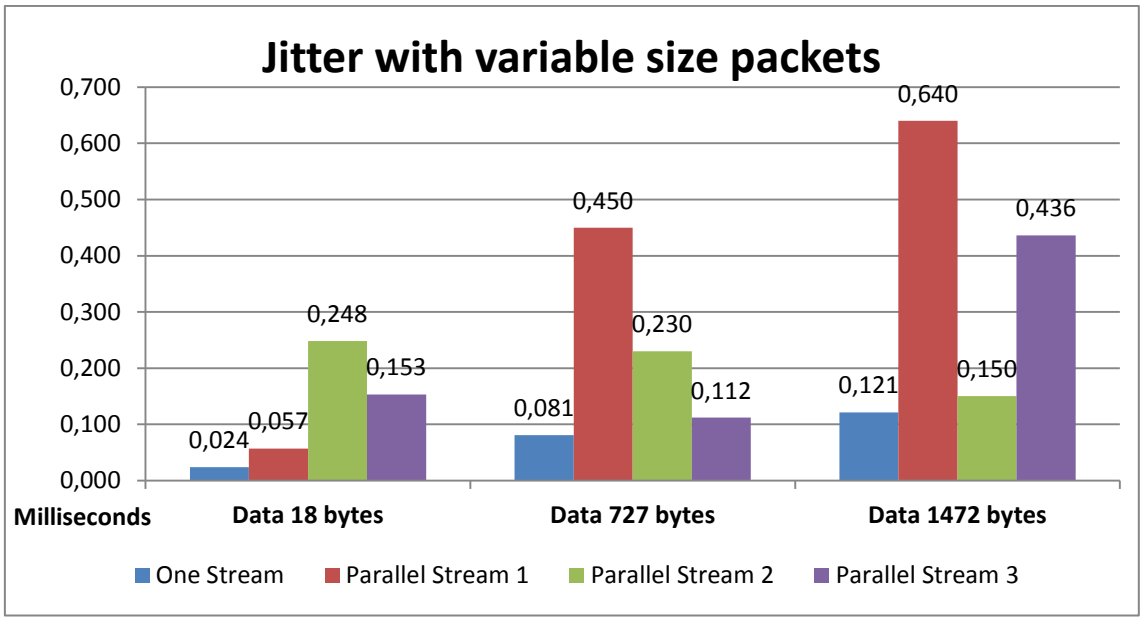

Figura 100 – Comparação do *jitter* entre um fluxo sem concorrência e três fluxos em concorrência, para três tamanhos de pacotes.

Os resultados mostram que os fluxos em concorrência têm um valor de *jitter* maior do que o fluxo sem concorrência, independentemente do tamanho dos pacotes. Conclui-se também que com o aumento do tamanho dos pacotes existe um ligeiro aumento do valor do *jitter*.

4.4.2. Resultados do *jitter* na rede MPLS vs ligação direta

A comparação entre o *jitter* na rede MPLS e o *jitter* numa ligação direta entre as máquinas de testes pode ser verificada na Figura 101, para os três tamanhos de pacotes definidos. Note-se que as três primeiras barras referentes a cada tamanho de pacote representam os três fluxos em concorrência testados na rede MPLS e as restantes três barras representam os fluxos em concorrência na ligação direta entre máquinas.

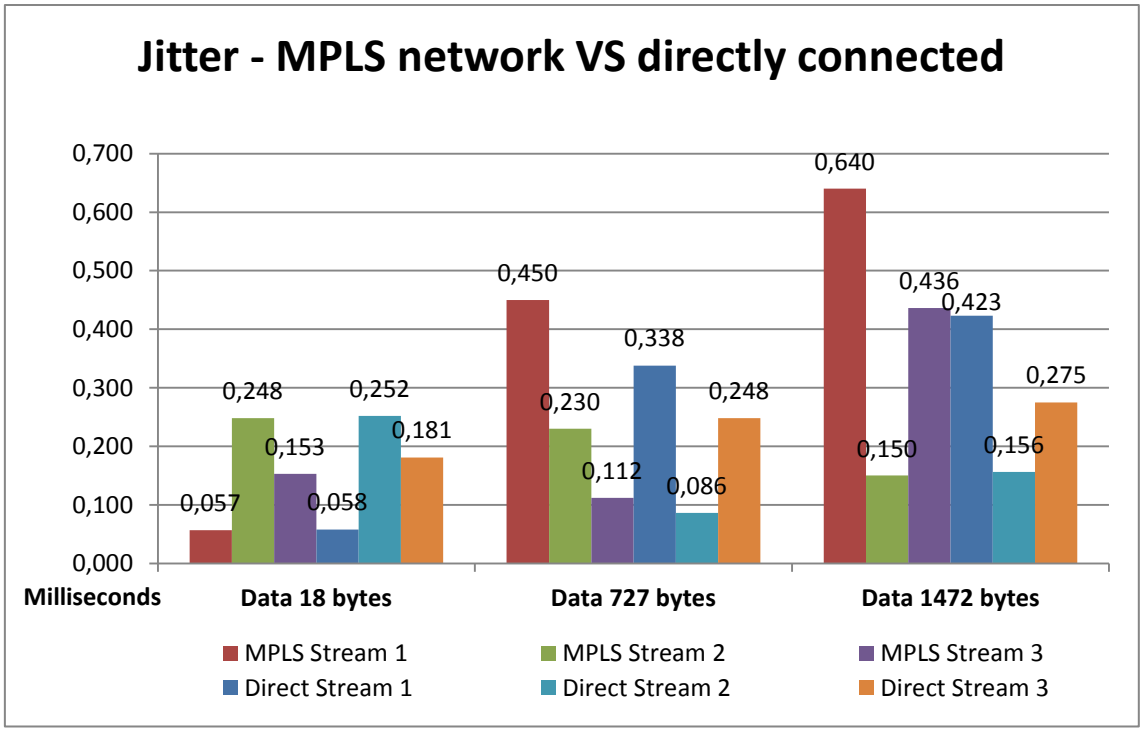

Figura 101 – Comparação do *jitter* na rede MPLS VS ligação direta entre máquinas, para os três tamanhos de pacotes definidos.

Conclui-se através dos resultados que não existe uma diferença significativa de *jitter* entre os dois meios. Como já foi referido anteriormente, alguns tipos de tráfego mais exigentes permitem que o *jitter* tenha valores até aos 20 ms sem que a qualidade do serviço seja afetada. Os valores apresentados são inferiores a 1 ms, logo o *jitter* destes testes não é conclusivo. Os testes realizados não são ideais, pois apesar dos três fluxos de dados estarem em concorrência, estes são gerados e recebidos pelas mesmas máquinas a um ritmo constante e sem variação no tamanho dos pacotes. Devido às limitações impostas pelos recursos disponíveis, não foi possível criar um ambiente de teste propício para esta medida de QoS. No entanto, as configurações desenvolvidas não tiveram como objetivo a melhoria direta do *jitter*, logo prevê-se apenas que a melhoria do balanceamento da rede beneficie indiretamente o *jitter*.

4.5. Resposta a falhas de rede em ligações ponto-a-ponto

As configurações desenvolvidas utilizam métodos de resiliência diferentes da configuração operacional, esperando-se assim diferentes reações às falhas de rede. Assim, de forma a testar a resposta da rede simulou-se uma falha de rede entre os *routers* SARF-1(CORE) e SARF-6(ISEL), recorrendo ao comando "*shutdown*" na porta 1/2/5 no *router* SARF-6(ISEL). Foram utilizadas as máquinas MPLS-1 e MPLS-2 para através da ferramenta Iperf criar um fluxo de dados de teste igual ao utilizado nos testes de largura de banda. Durante esta transmissão é provocada uma falha na rede que permite verificar o número de pacotes perdidos e o tempo que a rede demora a recuperar da falha provocada. Na Figura 102, pode-se observar o caminho utilizado pelo tráfego de testes e o local onde foi provocada a falha de rede.

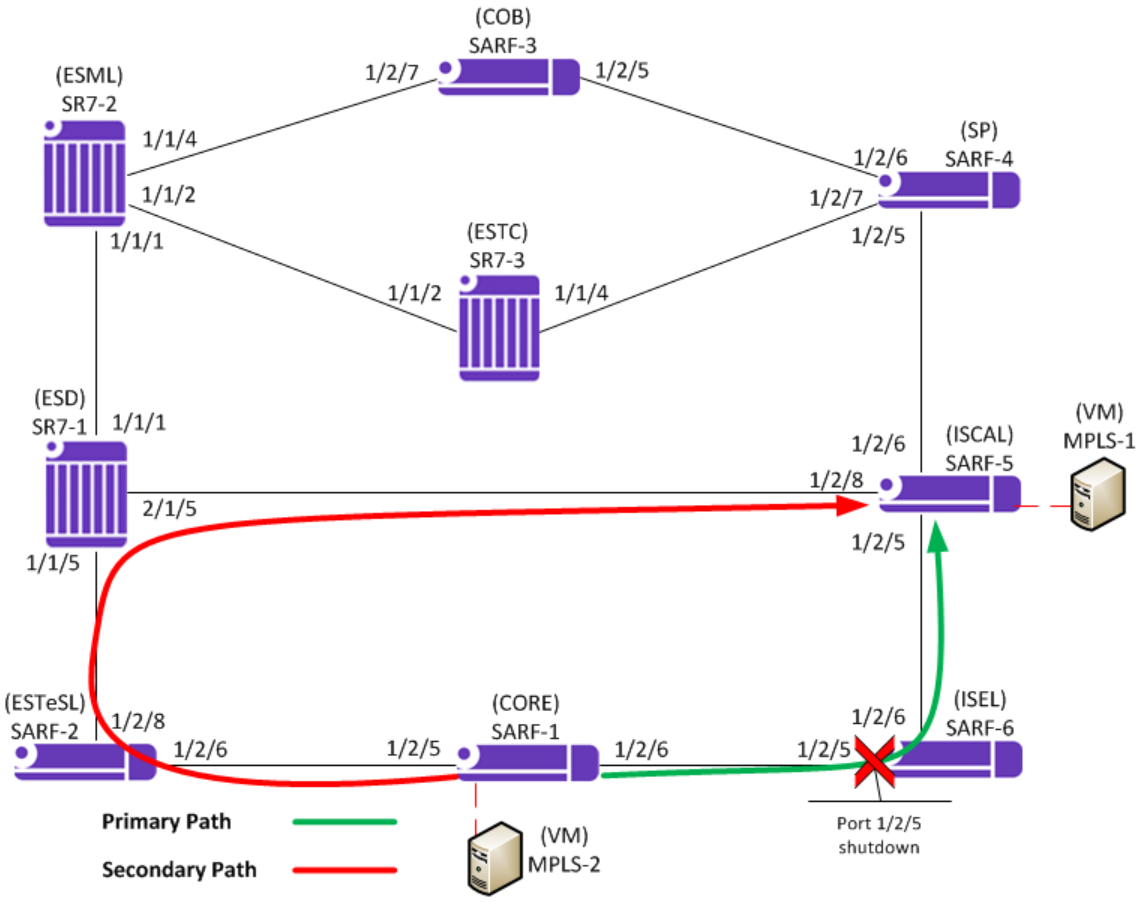

Figura 102 – Representação do *primary-path*, *secondary-path* e da zona de corte que foram utilizados nos testes à resposta da rede a falhas.

Os testes foram realizados em todas as configurações e com os vários tamanhos de pacotes definidos nos testes anteriores. No entanto, para todas as configurações e tamanhos de pacotes foi realizado um teste no sentido contrário que obteve resultados idênticos. Na Figura 103 pode-se observar um exemplo dos resultados obtidos num teste com a configuração operacional do IPL e com o tamanho máximo de pacotes. Nesta o corte de rede é visível pelo número de pacotes perdidos durante o segundo 11 do teste.

```
mpls@mpls-tfc-1:~$ iperf -s -u -i 1
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  3] local 10.10.10.100 port 5001 connected with 10.10.10.200 port 39531
[ ID] Interval       Transfer     Bandwidth        Jitter   Lost/Total Datagrams
[  3]  0.0- 1.0 sec  11.2 MBytes  94.2 Mbits/sec   0.132 ms    0/ 8014 (0%)
[  3]  1.0- 2.0 sec  11.2 MBytes  94.2 Mbits/sec   0.122 ms    0/ 8011 (0%)
[  3]  2.0- 3.0 sec  11.2 MBytes  94.2 Mbits/sec   0.122 ms    0/ 8013 (0%)
[  3]  3.0- 4.0 sec  11.2 MBytes  94.2 Mbits/sec   0.122 ms    0/ 8013 (0%)
[  3]  4.0- 5.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms    0/ 8011 (0%)
[  3]  5.0- 6.0 sec  11.2 MBytes  94.2 Mbits/sec   0.129 ms    0/ 8013 (0%)
[  3]  6.0- 7.0 sec  11.2 MBytes  94.2 Mbits/sec   0.125 ms    0/ 8013 (0%)
[  3]  7.0- 8.0 sec  11.2 MBytes  94.2 Mbits/sec   0.122 ms    0/ 8013 (0%)
[  3]  8.0- 9.0 sec  11.2 MBytes  94.2 Mbits/sec   0.122 ms    0/ 8011 (0%)
[  3]  9.0-10.0 sec  11.2 MBytes  94.2 Mbits/sec   0.122 ms    0/ 8013 (0%)
[  3] 10.0-11.0 sec  5.75 MBytes  48.3 Mbits/sec   0.121 ms    0/ 4104 (0%)
[  3] 11.0-12.0 sec  5.16 MBytes  43.3 Mbits/sec   0.122 ms 8841/12521 (71%)
[  3] 12.0-13.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms    0/ 8013 (0%)
[  3] 13.0-14.0 sec  11.2 MBytes  94.2 Mbits/sec   0.122 ms    0/ 8013 (0%)
[  3] 14.0-15.0 sec  11.2 MBytes  94.2 Mbits/sec   0.126 ms    0/ 8013 (0%)
[  3] 15.0-16.0 sec  11.2 MBytes  94.2 Mbits/sec   0.123 ms    0/ 8011 (0%)
[  3] 16.0-17.0 sec  11.2 MBytes  94.2 Mbits/sec   0.122 ms    0/ 8013 (0%)
[  3] 17.0-18.0 sec  11.2 MBytes  94.2 Mbits/sec   0.132 ms    0/ 8013 (0%)
[  3] 18.0-19.0 sec  11.2 MBytes  94.2 Mbits/sec   0.122 ms    0/ 8013 (0%)
[  3] 19.0-20.0 sec  11.2 MBytes  94.2 Mbits/sec   0.121 ms    0/ 8011 (0%)
[  3]  0.0-20.1 sec   214 MBytes  89.4 Mbits/sec   0.122 ms 8840/161290 (5.5%)
[  3]  0.0-20.1 sec  1 datagrams received out-of-order
```

Figura 103 – Exemplo da receção de pacotes com um corte de rede no segundo 11 do teste.

Desta forma é possível avaliar, em termos de número de pacotes perdidos, o impacto que uma falha de rede tem em cada configuração e ainda as variações dos resultados consoante o tamanho dos pacotes. Para avaliar o tempo que a rede demorou a recuperar desta falha, realizou-se simultaneamente uma captura do tráfego recebido na máquina MPLS-1 através do comando "tcpdump –i ens4 –w NomeCaptura". Os resultados da captura foram posteriormente analisados no programa *Wireshark*. Neste programa foram definidas as opções demonstradas na Figura 104, que permitem verificar para cada pacote quanto tempo passou desde da receção do pacote anterior.

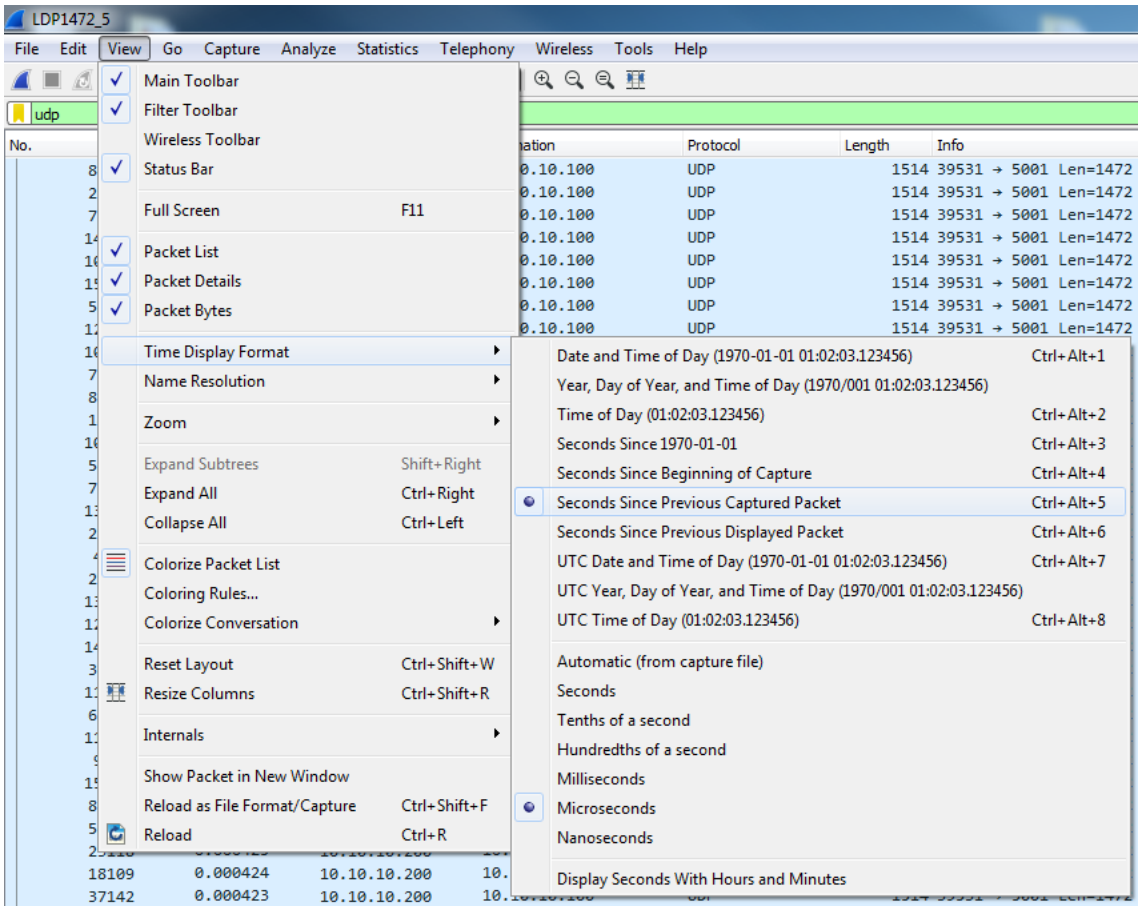

Figura 104 – Opções utilizadas no *Wireshark* para verificar o tempo entre pacotes recebidos.

Ordenando a secção "*Time*" do *Wireshark* de forma decrescente pode-se verificar o tempo mais elevado entre pacotes, que corresponde ao tempo que a rede demorou a recuperar da falha provocada. Na Figura 105 pode-se observar um exemplo desta análise que corresponde à captura realizada durante o teste apresentado na Figura 103.

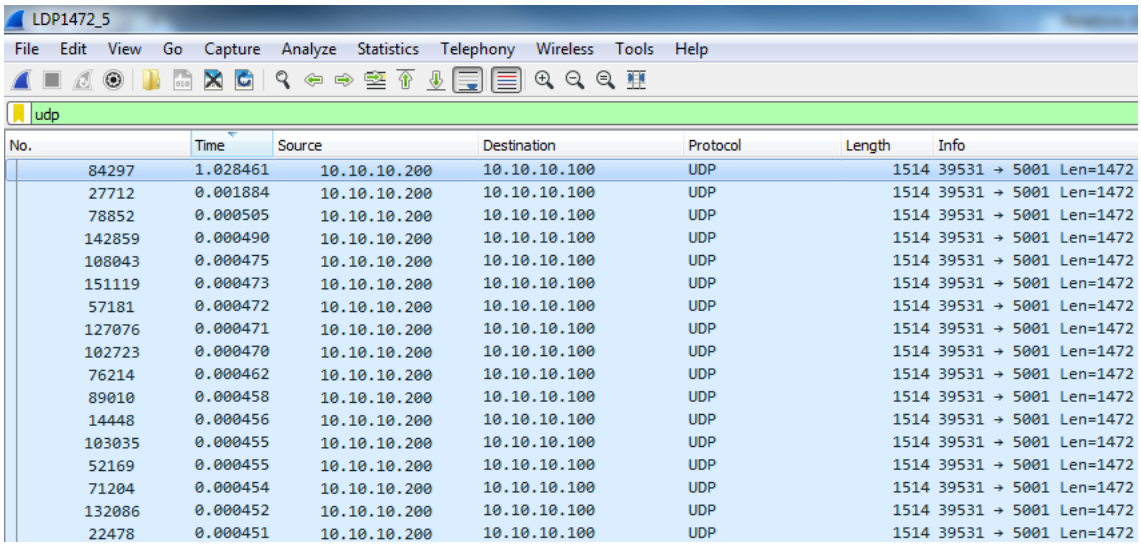

Figura 105 – Exemplo da análise realizada às capturas, de forma a verificar o tempo de recuperação da rede.

Este teste foi realizado com a configuração operacional e apresenta um tempo de recuperação de rede de 1,028 s. Cada configuração foi submetida a este teste por 5 vezes, de forma a criar uma média de valores. Estes testes foram ainda realizados com os três tamanhos de pacotes definidos anteriormente. Assim, para cada configuração foram realizados 15 testes, sendo 5 testes feitos com cada tamanho de pacote.

4.5.1. Resultados da perda de pacotes numa falha de rede

Os resultados apresentam a média da percentagem de pacotes perdidos de cinco testes. Estes estão organizados em três secções que correspondem aos três tamanhos de pacotes utilizados. Na Figura 106 cada barra corresponde ao resultado de uma configuração, sendo a primeira de cada secção o resultado da rede operacional (LDP) e as restantes o resultado das configurações desenvolvidas.

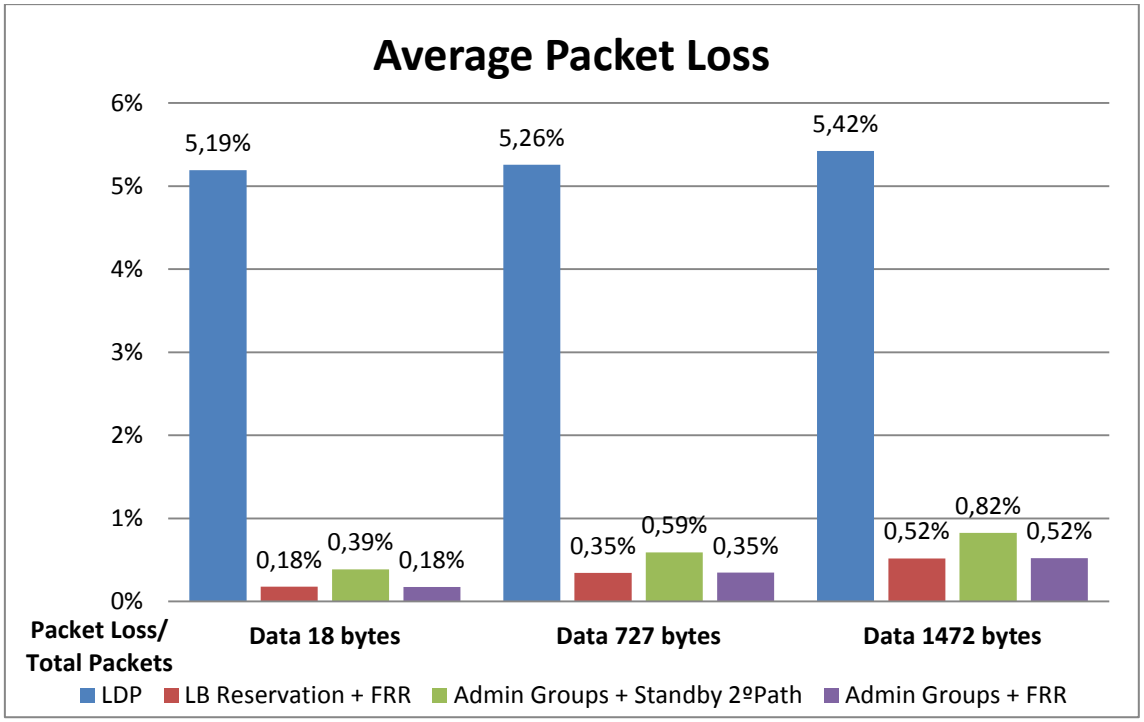

Figura 106 – Comparação da média da percentagem de pacotes perdidos entre a configuração operacional (LDP) e as configurações desenvolvidas durante uma falha de rede, para três tamanhos de pacotes diferentes.

Esta comparação permite concluir que a configuração operacional perde em média quase 5 vezes mais pacotes que as configurações desenvolvidas no processo de recuperação de uma falha de rede, sendo este valor é independente do tamanho do pacote. Conclui-se ainda, que o aumento do tamanho dos pacotes aumenta ligeiramente a relação de pacotes perdidos por pacotes enviados. Nota ainda para a diferença aproximadamente de 0,20% de pacotes perdidos entre as soluções que utilizam FRR e a solução que utiliza *Hot-standby secondary-path*, o que viabiliza a capacidade de recuperação de falhas de rede da solução com o *Hot-standby secondary-path*.

4.5.2. Resultados do tempo de recuperação numa falha de rede

Os resultados apresentam a média de tempos que cada configuração demorou a recuperar do corte de rede provocado. Estes são ainda resultados extraídos dos mesmos testes que forneceram os valores da perda de pacotes apresentados nos resultados anteriores. Na Figura 107 pode-se observar o tempo em segundos que cada configuração demorou a restabelecer o fluxo de dados para cada um dos três tamanhos de pacotes definidos.

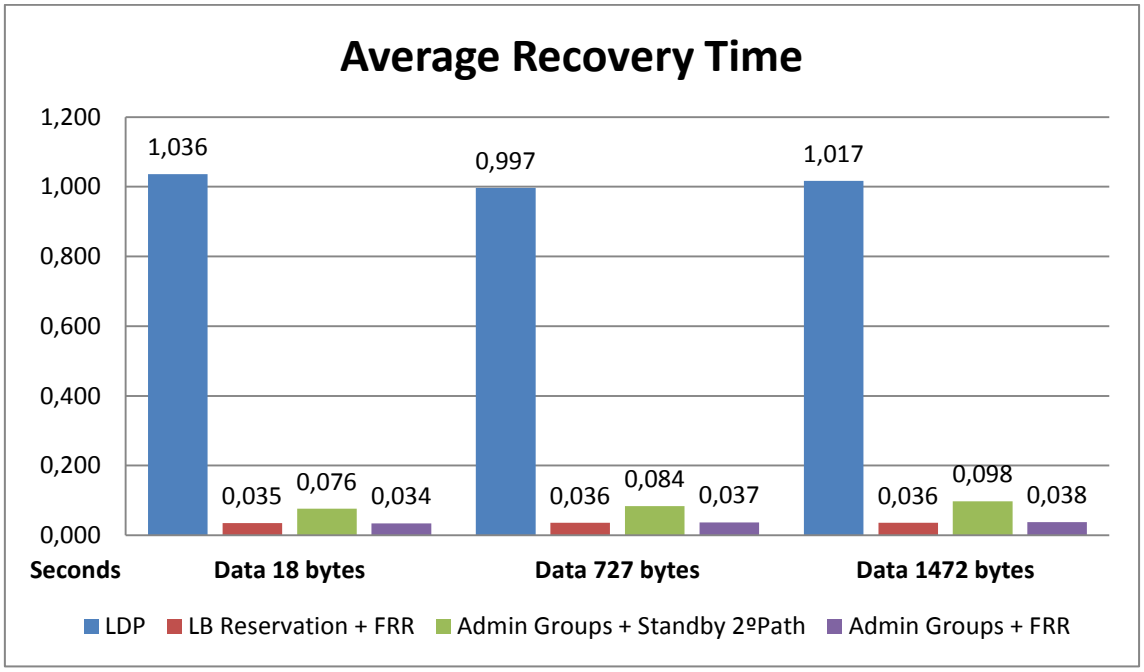

Figura 107 – Comparação da média do tempo de recuperação da rede em segundos entre a configuração operacional (LDP) e as configurações desenvolvidas, com três tamanhos de pacotes diferentes.

Estes resultados estão diretamente relacionados com os resultados anteriores, no entanto são analisados noutra perspetiva. Assim, a configuração operacional necessita em média de 1 segundo para recuperar de falhas, sendo este valor mais de 10 vezes superior ao tempo que as configurações desenvolvidas demoram a recuperar de falhas. Os resultados mostram ainda que esta diferença é independente do tamanho dos pacotes. Por fim, as configurações que utilizam o FRR tiveram em média um tempo de recuperação inferior a 50 ms e a configuração que utiliza o *Hot-standby secondary-path* obteve um valor médio ligeiramente inferior a 100 ms. Conclui-se assim que todas as configurações desenvolvidas apresentam melhorias significativas na recuperação a falhas de rede.

4.5.3. Estudo complementar sobre a resposta a falhas de rede

As configurações desenvolvidas não utilizam todos os métodos disponíveis de resiliência. Assim, de forma a completar este estudo, foram ainda realizados testes diretamente na rede OSPF e ainda na rede MPLS com um *Cold-standby secondary-path*. Os métodos utilizados para a realização destes testes foram iguais aos dos testes anteriores. Sendo este um estudo complementar foram apenas feitas três repetições do mesmo teste. Todos os testes utilizaram o tamanho máximo de pacotes.

Para permitir o teste à rede OSPF foi necessário alterar os endereços das máquinas MPLS-1 e MPLS-2 para que estas estejam em redes diferentes e assim adicionar as novas redes à rede OSPF. Desta forma a máquina MPLS-1 ficou com o endereço 10.10.20.100/24 e a máquina MPLS-2 ficou com o endereço 10.10.10.200/24.

No caso do *Cold-standby secondary-path*, adaptou-se a configuração com *admin-groups* que utiliza um *Hot-standby secondary-path*. Assim no *router* SARF-1(CORE) alterou-se o LSP "toSARF5(ISCAL)" com as configurações do seguinte exemplo.

```
A:SARF-1(CORE)# admin display-config
...

#--------------------------------------------------
echo "MPLS LSP Configuration"
#--------------------------------------------------
        mpls
            path "Loose"
                no shutdown
            exit
            path "LooseALT"
                no shutdown
            exit
            ...

            lsp "toSARF5(ISCAL)"
                to 192.168.0.5
                cspf
                primary "Loose"
                    include "AMARELO"
                    include "VERMELHO"
                exit
                secondary "LooseALT"
                exit
                no shutdown
            exit
```

Desta forma o *secondary-path* passa a estar no modo *Cold-standby* e não tem restrições de *admin-groups*.

4.5.3.1. Resultados do OSPF numa falha de rede

Os resultados mostram a média da percentagem de pacotes perdidos de cada teste. Na Figura 108 pode-se observar a comparação entre a configuração operacional (LDP) e a configuração OSPF, tendo em conta que o valor apresentado para a configuração operacional é o mesmo que foi apresentado nos resultados anteriores.

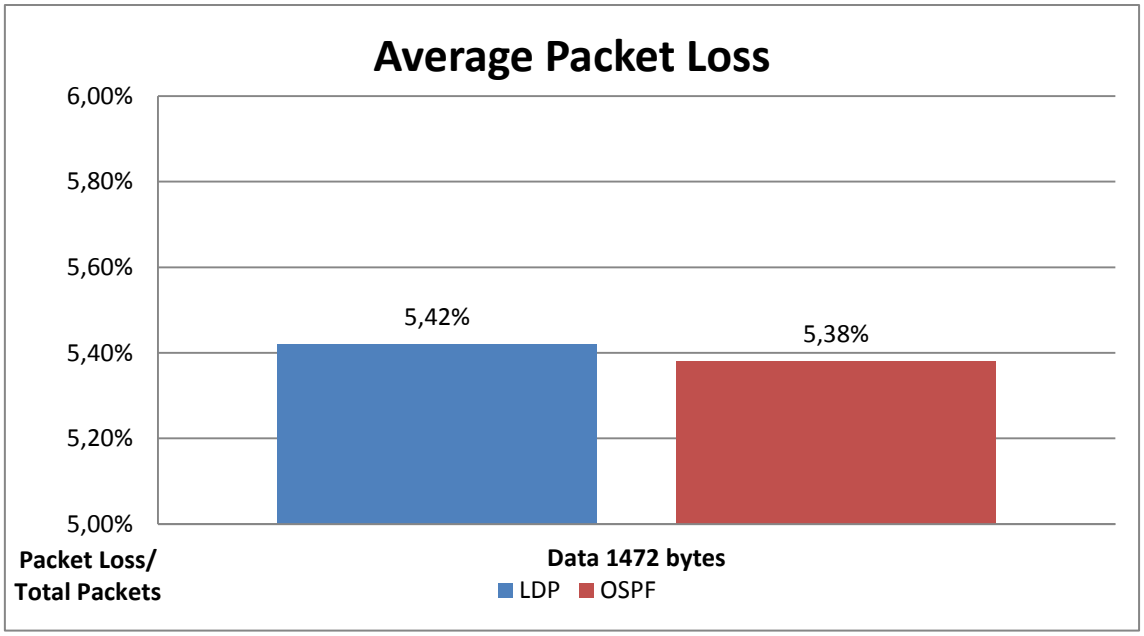

Figura 108 – Comparação da média da percentagem de pacotes perdidos entre a configuração operacional (LDP) e a configuração OSPF, numa falha de rede.

Com estes resultados pode-se concluir que uma rede IP pode apresentar valores de recuperação a falhas de rede semelhantes aos de uma rede MPLS, quando esta utiliza o protocolo LDP. Na Figura 109 pode-se observar ainda que o tempo de recuperação da rede está de acordo com os resultados de perdas de pacotes.

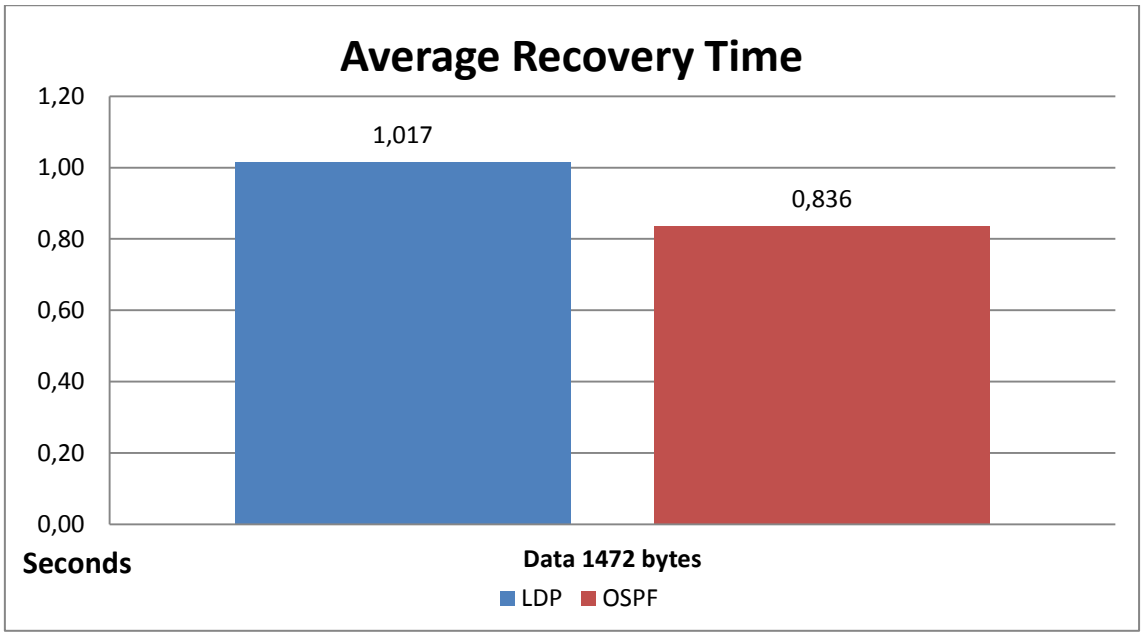

Figura 109 – Comparação da média do tempo de recuperação de uma falha de rede entre a configuração operacional (LDP) e a configuração OSPF.

Estes resultados indicam ainda que o protocolo OSPF poderá ser ligeiramente mais rápido que o protocolo LDP a recuperar de uma falha de rede. Estes valores justificam-se uma vez que o protocolo LDP depende do protocolo IGP, OSPF neste caso, para definir o novo caminho após a falha de rede. Assim, o LDP não consegue ser mais

rápido que o OSPF e as diferenças entre estes correspondem ao tempo necessário para que o LDP preencha a LFIB com as *labels* tendo em consideração o novo caminho calculado pelo OSPF e colocado na tabela de encaminhamento como *next-hop*.

4.5.3.2. Resultados do *Cold-standby secondary-path* numa falha de rede

Neste caso, não foi possível utilizar a duração de referência dos testes de 20 segundos, devido ao tempo de recuperação verificado nos primeiros testes. Assim, a duração deste teste foi aumentada para 60 segundos, para garantir que a recuperação da rede era captada. Com este aumento o número de pacotes enviados e perdidos deixam de ser comparáveis aos testes anteriores. No entanto, na Figura 110 pode-se observar que a média de pacotes perdidos deste método é muito superior à média de pacotes perdidos da configuração operacional.

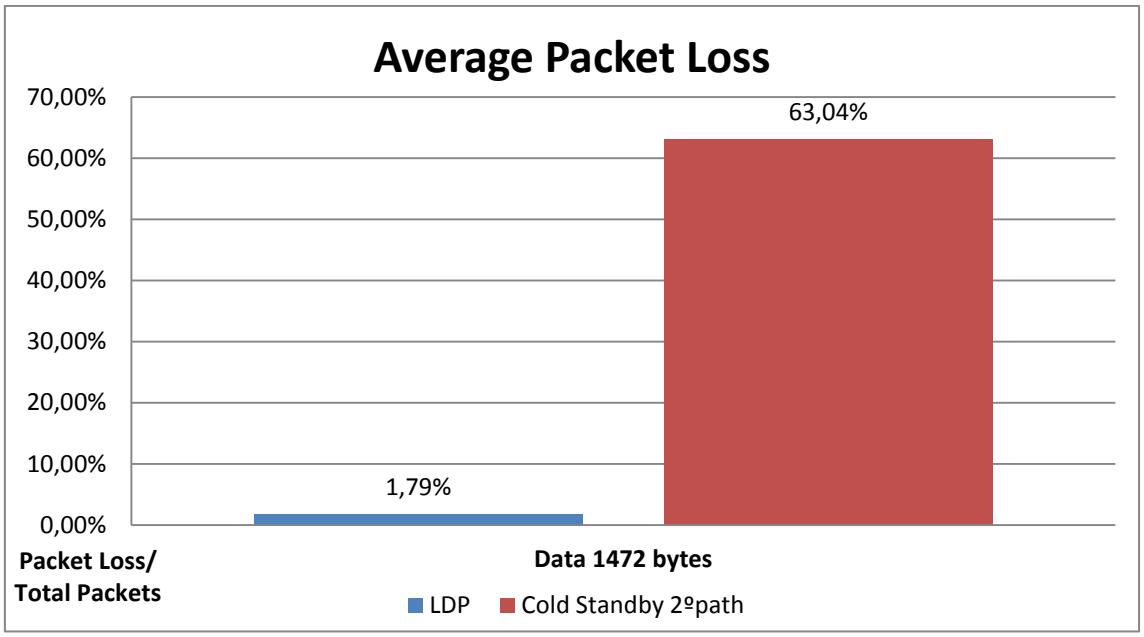

Figura 110 – Comparação da média de pacotes perdidos entre a configuração operacional (LDP) e a configuração *Cold-standby secondary-path*.

Na sequência destes resultados pode-se observar ainda a Figura 111, onde está representada a média do tempo de recuperação da rede após uma falha de rede.

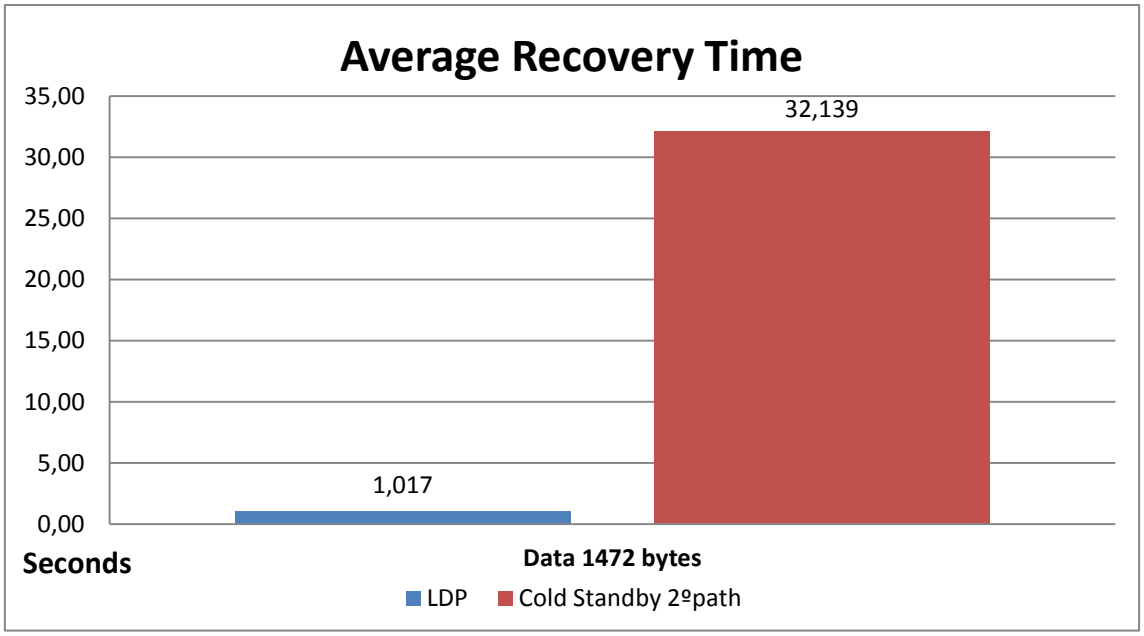

Figura 111 – Comparação da média de tempo de recuperação de uma falha de rede entre a configuração operacional (LDP) e a configuração *Cold-standby secondary-path*.

Através deste conjunto de resultados pode-se concluir que o *Cold-standby secondary-path* é o método de resiliência que demora mais tempo a recuperar de uma falha de rede. No entanto, este método é apenas ativado após o "*Retry-Timer*", que é um temporizador de 30 segundos por omissão. Desta forma, após os 30 segundos será feita uma tentativa de calcular um novo caminho para o *primary-path* de acordo com as restrições aplicadas. Apenas se nenhum caminho for encontrado, será calculado um caminho para o *Cold-standby secondary-path*. Tendo em conta todo este processo, é expectável que na realidade este método precise de menos de 2 segundos para estabelecer o *secondary-path* e reiniciar o fluxo de dados. Note-se que o valor do *Retry-Timer* pode ser reduzido até 1 segundo, sendo assim possível atingir um tempo de recuperação de 3 segundos aproximadamente.

4.6. Resposta a falhas de rede em ligações multiponto

Os testes anteriores mostram apenas a recuperação da rede para falhas em ligações ponto a ponto. Caso as ligações sejam feitas através de equipamentos L2, as falhas ocorridas entre estes equipamentos são apenas detetáveis através dos mecanismos de manutenção de adjacências dos protocolos IGP e RSVP-TE. Assim, dependendo do protocolo a ligação será considerada "desligada" quando o *router* não receber consecutivamente três ou quatro mensagens *Hello* do seu vizinho. No protocolo OSPF estes pacotes são enviados por omissão em períodos de 10 s e a ligação será considerada "desligada" após a perda de quatro mensagens, no entanto neste projeto foram utilizados os valores adotados na rede MPLS do IPL com uma periocidade de mensagens *Hello* de 1 segundo e um *dead-interval* de 3 mensagens. No caso do RSVP, por norma as mensagens *Hello* são enviadas em períodos de 3 segundos e utilizam um *default-timeout* de 3 mensagens, no entanto para que este esteja ao mesmo nível que o OSPF utilizou-se um intervalo de 1 segundo entre mensagens *Hello*. Assim, serão precisos 3 s para ambos os protocolos detetarem uma falha entre equipamentos L2.

No entanto, existem protocolos dedicados a melhorar a deteção de falhas nestes casos, como o *Bidirectional Forwarding Detection* (BFD). Com o objetivo de melhorar a disponibilidade da rede MPLS do IPL neste tipo de ligações, realizou-se um estudo sobre as melhorias que o protocolo BFD pode introduzir nestes casos.

Para testar este tipo de ligações foi necessário fazer alterações ao cenário de testes. Assim, foi adicionado um Cisco *switch* 2950 entre os *routers* SARF-5(ISCAL) e SARF-6(ISEL). Para que apenas um *switch* simule dois equipamentos L2 foi necessário ligar diretamente duas interfaces do *switch* em modo de acesso e com VLAN diferentes, fazendo desta forma o tráfego fluir de uma VLAN para a outra. Esta configuração é apenas possível se o protocolo *Cisco Discovery Protocol* (CDP) for desativado, para que o *switch* não detete a ligação direta entre as suas interfaces. Na Figura 112 pode-se verificar que cada *router* está ligado ao *switch* em VLAN diferentes, obrigando o tráfego a passar pelo cabo em "*loop*" que simula a ligação entre dois equipamentos L2.

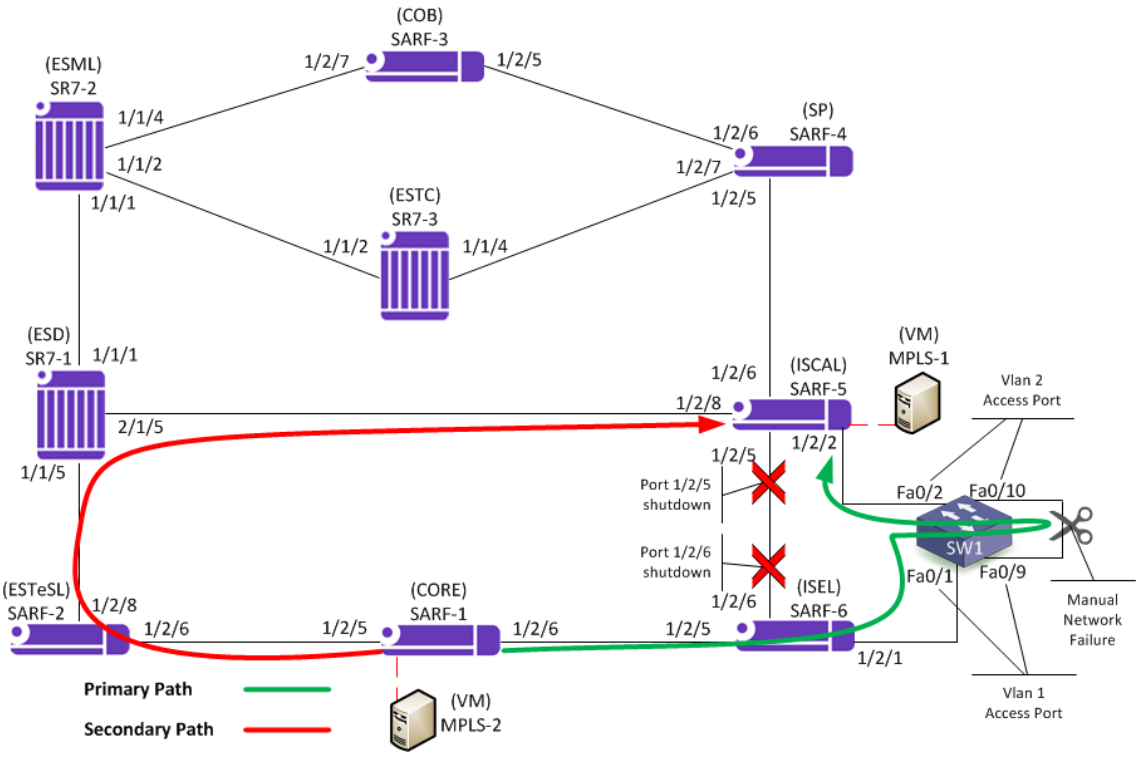

Figura 112 – Cenário para testar o protocolo BFD, com um *switch* entre *routers*.

As falhas foram provocadas retirando fisicamente o cabo da interface "Fa0/10" do *switch*. Os testes foram realizados em todas as configurações com e sem BFD ativo na nova ligação. O BFD foi configurado para enviar pacotes *Hello* num período de 100 ms, bastando 3 pacotes *Hello* perdidos consecutivamente para mudar o estado da interface para "*down*". No seguinte exemplo de configuração pode-se observar as configurações adicionadas à configuração de balanceamento "manual" com FRR.

```
A:SARF-5(ISCAL)# admin display-config
...

#--------------------------------------------------
echo "Router (Network Side) Configuration"
#--------------------------------------------------
```

```
    router
        interface "system"
            address 192.168.0.5/32
        exit
        interface "toSARF-4"
            address 10.4.5.5/24
            port 1/2/6
        exit
        interface "toSARF-6"
            address 10.5.6.5/24
            port 1/2/2
            bfd 100 receive 100 multiplier 3
        exit
        interface "toSR7-1"
            address 10.5.11.5/24
            port 1/2/8
        exit
#--------------------------------------------------
echo "OSPFv2 Configuration"
#--------------------------------------------------
        ospf
            traffic-engineering
            area 0.0.0.0
                interface "system"
                exit
                interface "toSARF-4"
                    interface-type point-to-point
                    hello-interval 1
                    dead-interval 3
                    metric 100
                exit
                interface "toSARF-6"
                    interface-type point-to-point
                    hello-interval 1
                    dead-interval 3
                    metric 100
                    bfd-enable
                exit
                interface "toSR7-1"
                    interface-type point-to-point
                    hello-interval 1
                    dead-interval 3
                    metric 100
                exit
            exit
        exit
#--------------------------------------------------
echo "RSVP Configuration"
#--------------------------------------------------
        rsvp
            interface "system"
            exit
            interface "toSARF-4"
            exit
            interface "toSARF-6"
                hello-interval 1000
                bfd-enable
            exit
            interface "toSR7-1"
            exit
            no shutdown
        exit
```

Na Figura 113 pode-se observar a sessão BFD estabelecida e os protocolos que estão protegidos por esta sessão.

```
A:SARF-5(ISCAL)# show router bfd session

===============================================================================
BFD Session
===============================================================================
Interface                       State                Tx Intvl  Rx Intvl  Multipl
  Remote Address                Protocol             Tx Pkts   Rx Pkts   Type
-------------------------------------------------------------------------------
toSARF-6                        Up (3)               100       100       3
   10.5.6.6                     ospf2 rsvp           1869      1878      iom
-------------------------------------------------------------------------------
No. of BFD sessions: 1
===============================================================================
```

Figura 113 – Exemplo da sessão BFD estabelecida entre os *routers* SARF-5(ISCAL) e SARF-6(ISEL).

Os testes realizados foram idênticos aos anteriores, utilizando o Iperf para gerar tráfego entre as máquinas MPLS-1 e MPLS-2. No entanto, neste caso o *switch* introduziu uma limitação no tamanho máximo dos pacotes, permitindo apenas pacotes com um máximo de 1524 bytes. Para transmitir um pacote de tamanho máximo com 1472 bytes de Data seria necessário permitir 1540 bytes no total, devido ao cabeçalho extra introduzido pelo MPLS. Assim, os testes foram realizados com 1456 bytes de Data e com a constituição dos pacotes apresentada na Figura 114.

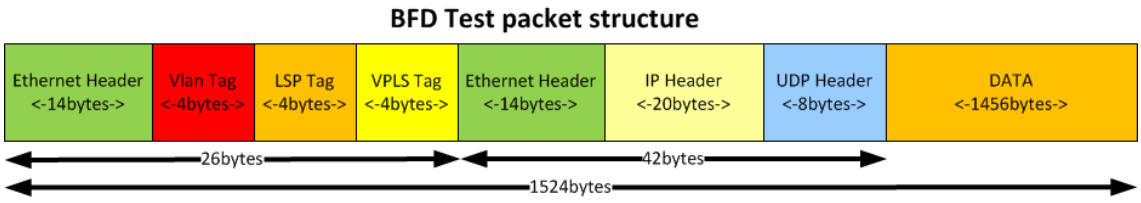

Figura 114 – Estrutura dos pacotes de testes ao passar pelo *switch*.

Todos os testes foram realizados com o mesmo tamanho de pacote durante 20 segundos, sendo a falha de rede provocada manualmente dentro deste intervalo. Cada configuração foi testada três vezes com e sem BFD.

4.6.1. Resultados da resposta dos protocolos BFD vs LDP/RSVP-TE numa falha de rede remota

Na Figura 115 pode-se observar os resultados da média de percentagem de pacotes perdidos em todas as configurações com e sem BFD.

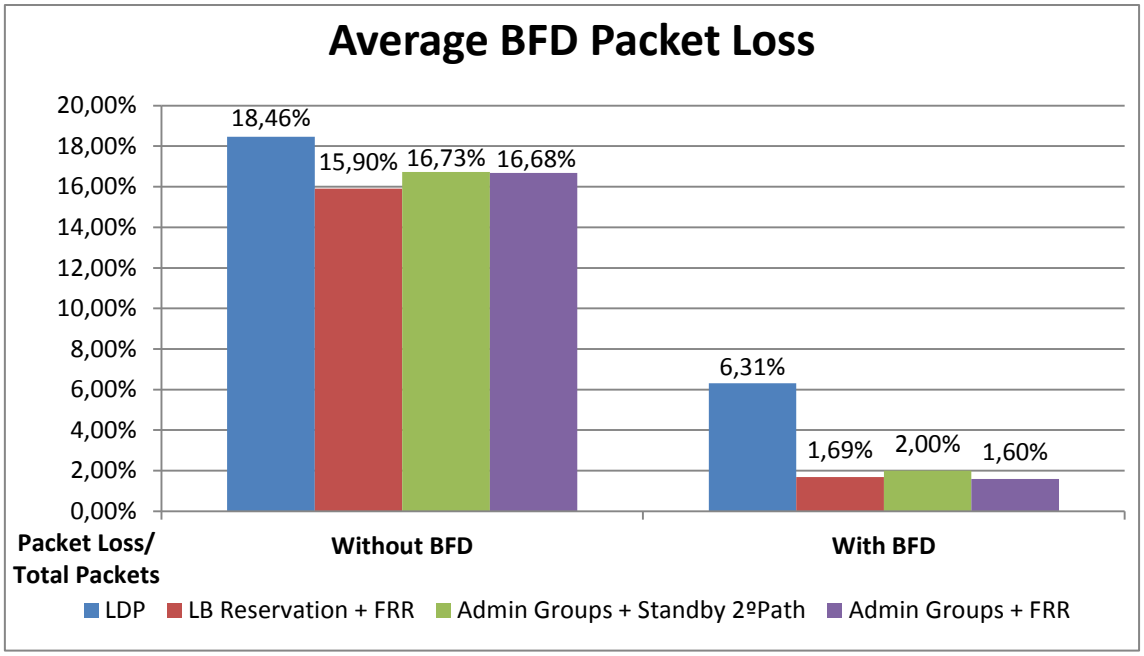

Figura 115 – Comparação dos resultados sem e com BFD da média de percentagem de pacotes perdidos numa falha de rede.

Os resultados apresentam uma diferença percentual de mais de 10% de pacotes perdidos entre as configurações com e sem BFD. Conclui-se que o BFD melhora significativamente a capacidade de resposta da rede em todos os casos. Na Figura 116 pode-se observar os resultados da média do tempo de recuperação da rede com e sem BFD.

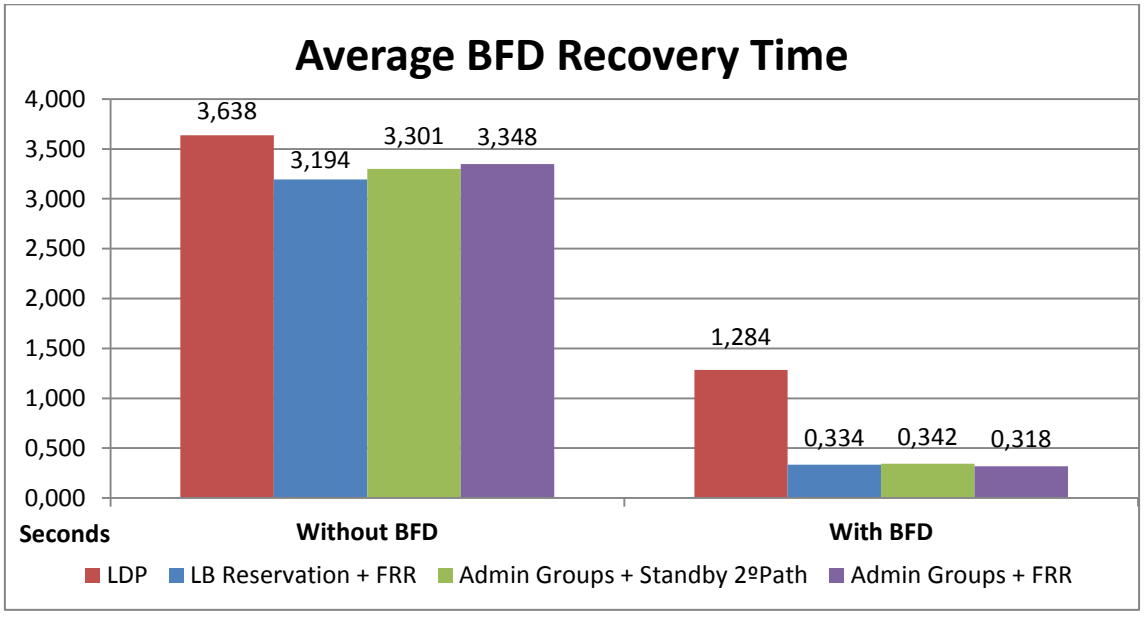

Figura 116 – Comparação dos resultados sem e com BFD da média do tempo de recuperação duma falha de rede.

Através destes resultados é possível comprovar que a recuperação da rede sem BFD necessita de mais de 3 segundos. Estes valores estão de acordo com o tempo necessário para detetar a falha de rede através das mensagens *Hello* do protocolo OSPF ou RSVP. Os resultados com BFD são ligeiramente superiores aos 300 ms

necessários para que este detete a falha de rede. Assim, para este caso a diferença entre as configurações com e sem BFD é de aproximadamente 3 segundos, no entanto esta pode ainda aumentar caso o protocolo BFD seja configurado para o valor mínimo de deteção de falhas de 30 ms. Conclui-se que a utilização do protocolo BFD apresenta uma melhoria significativa no tempo de recuperação da rede e no número de pacotes perdidos, numa falha de rede entre equipamentos L2.

5. Proposta para evolução da topologia da rede MPLS do IPL

Neste capítulo serão sugeridas algumas topologias alternativas à atual, que poderiam ajudar a melhorar o desempenho da rede.

A topologia atual é composta apenas por *routers* PE, o que dificulta o processo de balanceamento da rede e acrescenta ainda uma sobrecarga sobre algumas ligações como foi referido nos capítulos anteriores. De forma a simplificar o processo de balanceamento e consequentemente melhorar o desempenho da rede, serão apresentadas duas topologias alternativas.

5.1. Topologia Anel-Estrela

Esta topologia permite manter algumas das ligações atuais com a utilização de um anel entre todos os *routers* PE, como se pode verificar na Figura 117. Para aumentar a redundância foi acrescentado um *router* P, com ligação a todos os *routers* PE criando a forma de uma estrela. Analisando financeiramente, esta topologia irá precisar de mais 7 ligações face à topologia atual, fazendo um total de 18 ligações e acrescenta ainda um equipamento (P *router*) à atual topologia.

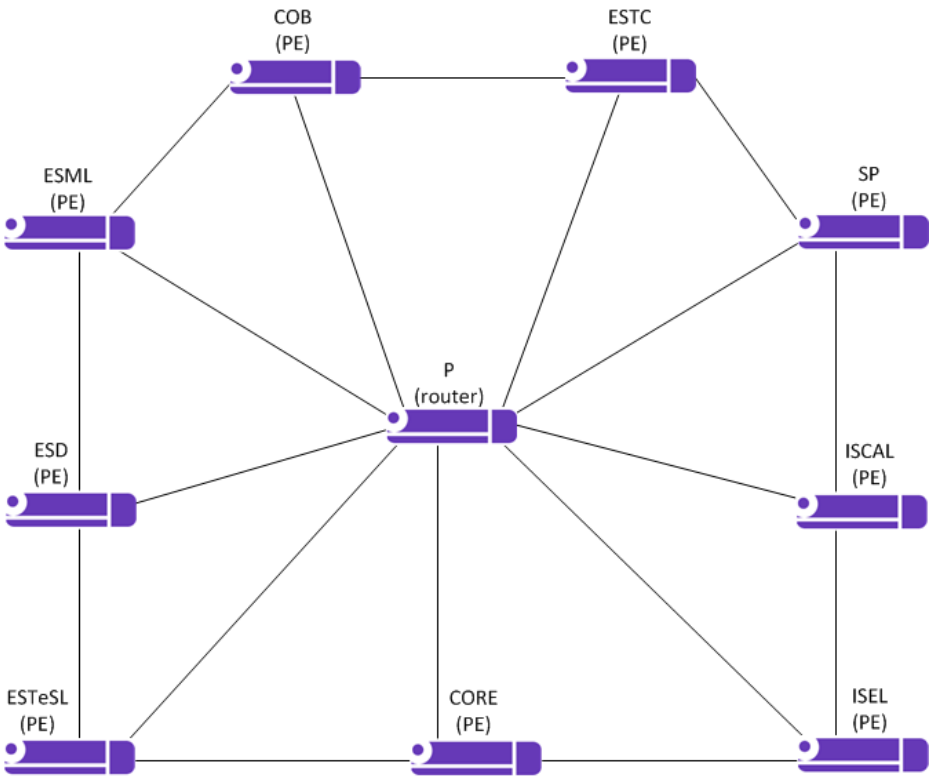

Figura 117 – Topologia alternativa com anel e estrela, para a rede MPLS do IPL.

Desta forma todos os *routers* PE têm três caminhos distintos para comunicar com os restantes PE *routers*. Esta topologia simplifica o planeamento do balanceamento da rede através das técnicas de MPLS-TE desenvolvidas neste projeto. Na Figura 118 pode-se observar um exemplo do planeamento da atribuição de *admin-groups* ou de grupos SRLG, onde apenas seria necessário utilizar dois grupos.

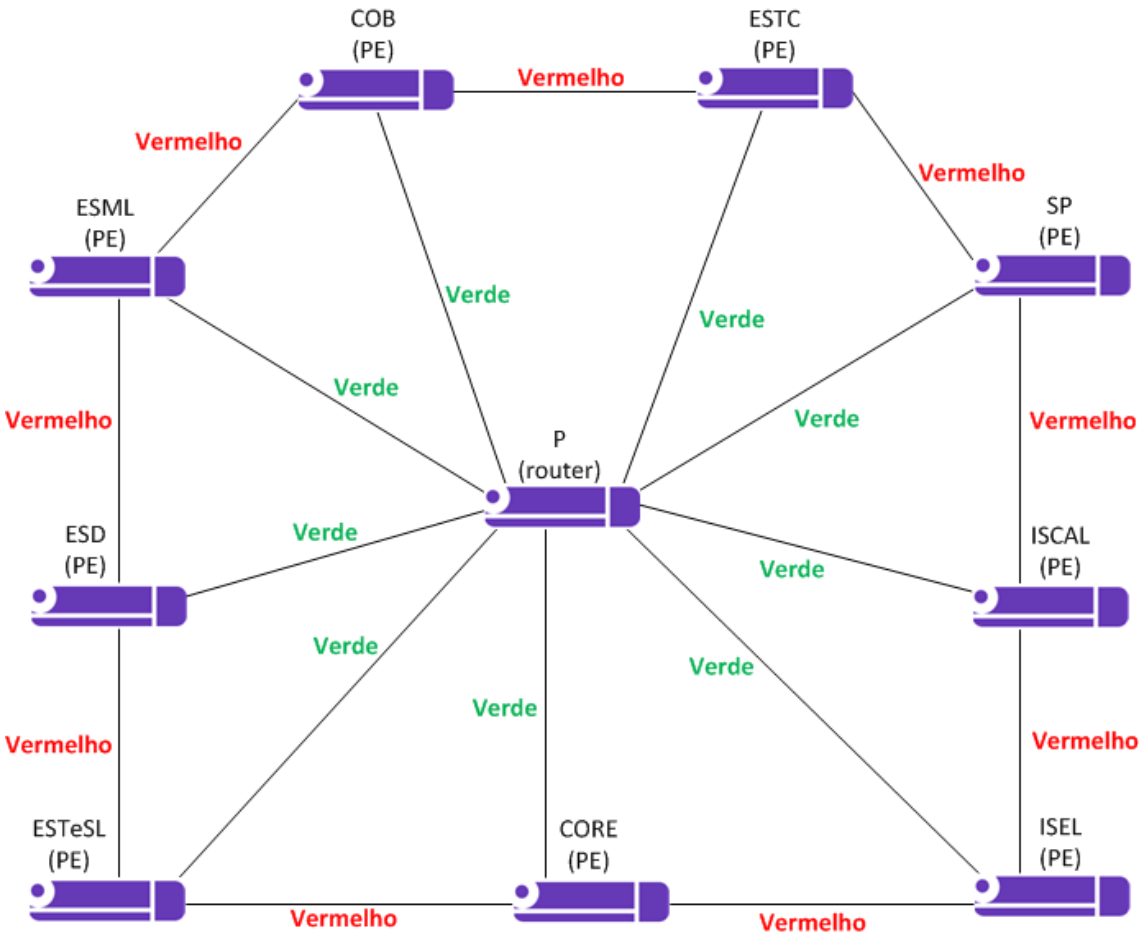

Figura 118 – Topologia alternativa com proposta de atribuição de *admin-groups*.

Esta solução é escalável, tendo facilidade na introdução de novos equipamentos no planeamento MPLS-TE e também na estrutura física. No entanto, um elevado número de equipamentos em anel poderá diminuir a eficiência da solução devido ao número de *hops* a que o tráfego fica sujeito.

5.2. Topologia Duas Estrelas

Esta topologia requer uma mudança total da infraestrutura da rede como se pode verificar na Figura 119, deixando de existir ligações entre *routers* PE e ligando em forma de estrela dois *routers* P a todos os PE *routers*. Analisando financeiramente, esta solução requer 19 ligações novas e ainda dois equipamentos novos (*routers* P1 e P2).

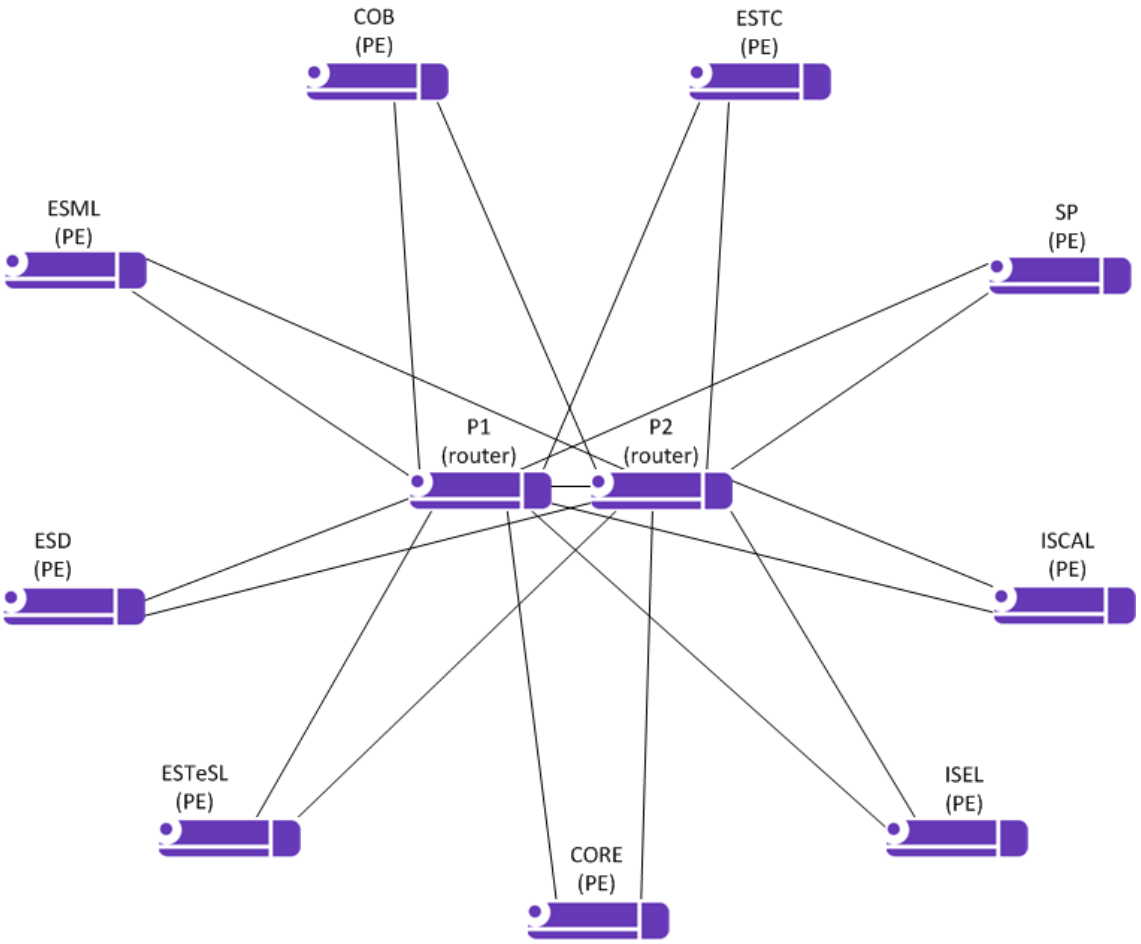

Figura 119 – Topologia alternativa com duas estrelas, para a rede MPLS do IPL.

Esta topologia tal como a anterior garante dois caminhos distintos entre todos os *routers* PE, no entanto para este caso ambos os caminhos estarão apenas um *hop* de distância de todos os *routers* PE. Desta forma, a rede pode ser balanceada entre caminhos idênticos. O planeamento MPLS-TE pode ser aplicado de forma semelhante à proposta anterior. Esta solução é escalável tendo apenas como limite o número de ligações que os equipamentos P1 e P2 suportam.

5.3. Discussão

A solução de duas estrelas permite uma escalabilidade e performance melhor, no entanto esta não permite que a infraestrutura atual seja reaproveitada, criando dificuldades no processo de transição e necessitando de um investimento financeiro maior. A solução anel-estrela apresenta uma melhoria face à topologia atual e reaproveita a infraestrutura existente diminuindo a complexidade do processo de transição e diminuindo o investimento financeiro necessário. Caso se mantenha o número atual de equipamentos, as soluções apresentadas terão uma performance semelhante.

6. Conclusão e Trabalho futuro

Este projeto teve como objetivo a melhoria da qualidade de serviço da rede de MPLS do IPL. Numa primeira análise verificou-se que esta utiliza o protocolo LDP, que não permite a utilização de engenharia de tráfego. A utilização do LDP atribui características de balanceamento e de resiliência semelhantes à de uma rede IP. As soluções apresentadas foram desenvolvidas com engenharia de tráfego, de forma a explorar o potencial da rede MPLS do IPL. As soluções permitem que a rede seja balanceada "manualmente" ou dinamicamente, melhorando a distribuição do tráfego pela topologia. O balanceamento da rede melhora a largura de banda disponível na rede e pode ainda melhorar indiretamente o *delay* e o *jitter*.

As soluções desenvolvidas exploraram também as opções de resiliência do MPLS, focando-se no uso do *Fast Reroute* (FRR) e do *Hot-standby secondary-path*. A resiliência está diretamente ligada à disponibilidade da rede, sendo esta medida de QoS o principal alvo de teste deste projeto. Os resultados dos testes demonstraram que as soluções desenvolvidas introduzem melhorias significativas na rede, tendo capacidade para recuperar de falhas de rede 10 vezes mais rápido que a configuração atual da rede MPLS do IPL. Os resultados demonstraram também que existe uma diferença de 50 ms entre o FRR e o *Hot-standby secondary-path* na recuperação de falhas de rede. Ambos os métodos são opções validas se os requisitos de QoS permitirem falhas de rede até 100 ms, tendo assim à disposição um método dinâmico e outro com a possibilidade de definir manualmente o caminho alternativo. Estes podem ainda ser utilizados em conjunto como foi demonstrado neste projeto, obtendo uma recuperação em menos de 50 ms pelo FRR e encaminhado depois o tráfego para o caminho alternativo desejado no *Hot-standby secondary-path*. Através do estudo de outros métodos como o *Cold-standby secondary-path*, conclui-se ainda que caso sejam utilizadas restrições no *primary-path* e se o principal método de resiliência também falhar pode ser vantajoso configurar um *Cold-standby secondary-path* sem restrições. Desta forma será possível recuperar de uma falha de rede em 32 segundos se existir um caminho disponível. Este valor pode ser diminuído até 3 segundos através da configuração do *Retry-Timer* para 1 s. Note-se que a utilidade deste método de reserva é proporcional ao número de caminhos alternativos disponíveis e às restrições aplicadas ao *primary-path*.

As conclusões anteriores foram obtidas em ligações ponto-a-ponto, no entanto caso exista uma falha de rede entre dois equipamentos L2 será necessário esperar pela deteção da falha através das mensagens *Hello* dos protocolos de IGP ou RSVP. Este processo pode demorar no mínimo 3 segundos. Para que seja possível manter os mesmos níveis de QoS independentemente do tipo de ligação realizou-se um estudo sobre o protocolo BFD. Neste estudo, o BFD foi configurado para detetar falhas em 300 ms, no entanto este permite que sejam detetadas falhas em 30 ms. Os resultados demonstraram que as configurações desenvolvidas em conjunto com o BFD recuperaram da falha de rede em menos de 350 ms, enquanto que sem o BFD a recuperação da falha de rede demorou mais de 3 s.

Por fim, as topologias propostas no capítulo 5 simplificam o planeamento e a implementação das configurações desenvolvidas e melhoram a escalabilidade e

performance da rede. Estas tornam ainda viável a utilização de outros métodos como o SRLG.

O futuro deste projeto passaria pela análise do tráfego da rede MPLS do IPL, de forma a identificar os vários tipos de tráfego e definir prioridades de acordo com o modelo *DiffServ*. O passo seguinte seria realizar um estudo sobre as melhores formas de aplicar estas prioridades e testar em laboratório. Este estudo teria como objetivo diminuir o *delay*, *jitter* e o número de pacotes descartados dos tráfegos prioritários em caso de congestão na rede, concluindo assim a melhoria de todas as medidas de QoS na rede MPLS no IPL.

Um passo seguinte seria a evolução para o SDN (*Software Defined Networks*) para possibilitar uma gestão que permitisse a adaptação dinâmica da rede às necessidades de tráfego.

7. Bibliografia

[1] K. Hundley, *Alcatel-Lucent Scalable IP Networks Sef-Study Guide*. Wiley Publishing, Inc., Indianapolis, Indiana.

[2] H. Lee, M. Kim, J. Hong, and G. Lee, "QoS parameters to network performance metrics mapping for SLA monitoring," *KNOM Rev.*, pp. 42–53, 2002.

[3] S. Thukral and B. Chadha, "A Survey on QoS Behavior in MPLS Networks," *Ijarcce*, vol. 4, no. 3, pp. 289–293, 2015.

[4] S. A. Sharafali, M. M. Al-quzwini, and R. S. Fyath, "Performance Evaluation of MPLS TE Signal Protocols for Voice Applications with QoS Implementation," *Int. J. Networks Commun.*, vol. 5, no. 1, pp. 1–9, 2015.

[5] J. Oubaha and M. Elkoutbi, "802.11 Mobile Networks Combined to QoS IP Networks."

[6] R. Balakrishnan, *Advanced QoS for Multi-Service IP/MPLS Networks*. Wiley Publishing, Inc., Indianapolis, Indiana.

[7] A. M. Sllame and M. Aljafari, "Evaluating the Impact of Routing and Queuing Techniques on the QoS of VoIP Over IP/MPLS Networks," *Int. J. Innov. Res. Comput. Commun. Eng. (An ISO Certif. Organ.*, vol. 3297, no. 12, pp. 7130–7139, 2007.

[8] G. Jain, D. Singh, and S. Verma, "Service level agreements in IP networks," *Inf. Manag. Comput. Secur.*, vol. 10, no. 4, pp. 171–177, 2002.

[9] G. Warnock and A. Nathoo, *Alcatel-Lucent Network Routing Specialist II (NRS II) Self-Study Guide*. Wiley Publishing, Inc., Indianapolis, Indiana.

[10] R. Thaker and R. Q. Shawl, "Analysis of Routing and Signaling Protocols in MPLS," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 4, no. 1, pp. 342–350, 2014.

[11] Z. Xu, *Designing and Implementing IP/MPLS-Based Ethernet Layer 2 VPN Services*. Wiley Publishing, Inc., Indianapolis, Indiana.

[12] N. Kaur, R. Kumar, B. Gupta, "Interpretation of MPLS Enabled Network with QOS Model," Ijiet, vol. 2, no. 1, pp. 130–137, 2013.

[13] R. K. Gupta, A. K. Singh, P. Singh, and O. Singh, "Analyzing Multi Protocol Label Switching Network," Ijarcsse, vol. 3, no. 6, pp. 1757–1762, 2013.

[14] M. N. Alhady and A. G. Elsid, "Improve the QoS by Applying Differentiated Service over MPLS Network," Ijcsmc, vol. 4, no. 9, pp. 84–91, 2015.

[15] Documentação da rede MPLS do IPL

[16] Alcatel-Lucent Software Release Notes "7705 SAR OS Interface Configuration Guide"

[17] L. Rizzo, G. Lettieri, and V. Maffione, “Speeding up packet I/O in virtual machines,” *ANCS 2013 - Proc. 9th ACM/IEEE Symp. Archit. Netw. Commun. Syst.*, pp. 47–58, 2013.

[18] J. Anuskiewicz, “Measuring jitter accurately,” 2008. [Online]. Available: http://www.lightwaveonline.com/articles/2008/04/measuring-jitter-accurately-54886317.html.