UNIVERSIDADE ESTADUAL DO MARANHÃO
CENTRO DE CIÊNCIAS TECNOLÓGICAS
CURSO DE ENGENHARIA DA COMPUTAÇÃO

LORENA TAVARES DA SILVA DE CARVALHO

IMPLEMENTAÇÃO DA TECNOLOGIA MPLS-TE, AVALIANDO SEUS BENEFÍCIOS NO SETOR DE TELECOMUNICAÇÕES

São Luís – MA

2019

LORENA TAVARES DA SILVA DE CARVALHO

IMPLEMENTAÇÃO DA TECNOLOGIA MPLS-TE, AVALIANDO SEUS BENEFÍCIOS NO SETOR DE TELECOMUNICAÇÕES

Trabalho de Conclusão de Curso apresentado ao Curso de Engenharia da Computação da Universidade Estadual do Maranhão, como registro para obtenção do grau de Bacharel em Engenharia da Computação.

Orientador: Prof. Wesley Batista Dominices Araujo.

São Luís – MA
2019

Carvalho, Lorena Tavares da Silva de.
Implementação da tecnologia MPLS-TE avaliando seus benefícios no setor de telecomunicações / Lorena Tavares da Silva de Carvalho. – São Luís, 2020.

82 f.

Monografia (Graduação) – Curso de Engenharia da Computação, Universidade Estadual do Maranhão, 2020.

Orientador: Prof. Me. Wesley Batista Dominices Araújo.

1.MPLS-TE. 2.Engenharia de tráfego. 3. Congestionamento. 4.Perda de pacote. I.Título

CDU: 004.77:656.1/.5

LORENA TAVARES DA SILVA DE CARVALHO

IMPLEMENTAÇÃO DA TECNOLOGIA MPLS-TE, AVALIANDO SEUS BENEFÍCIOS NO SETOR DE TELECOMUNICAÇÕES

Trabalho de Conclusão de Curso apresentado ao Curso de Engenharia da Computação da Universidade Estadual do Maranhão, como registro para obtenção do grau de Bacharel em Engenharia da Computação.

Aprovada em: de dezembro de 2019

BANCA EXAMINADORA

_____

Prof. Wesley Batista Dominices de Araujo (Orientador)
Departamento de Engenharia de Computação
Universidade Estadual do Maranhão

_____

Prof. Lúcio Flávio de Albuquerque Campos (1º Membro)
Departamento de Engenharia de Computação
Universidade Estadual do Maranhão

_____

Prof. Mauro Sérgio Silva Pinto (2º Membro)
Departamento de Engenharia de Computação
Universidade Estadual do Maranhão

AGRADECIMENTOS

Agradeço aos meus pais Dores Tavares da Silva de Carvalho e Domingos Soeiro de Carvalho, que sempre estiveram ao meu lado e batalharam para me dar a melhor educação possível. À minha irmã Julianne Tavares da Silva de Carvalho que me apoiou nos momentos difíceis.

Agradeço à Edimilson Carneiro, Henrique Costa e Michel Neves pelo aprendizado que me passaram, dividindo conhecimento e experiências comigo, tornando possível o desenvolvimento do projeto. Agradeço a André Luís por ter me ajudado na escolha do tema da monografia, além de ter me ajudado em algumas etapas do projeto. Ao meu orientador, Wesley Batista Dominices de Araújo, por sua paciência e dedicação.

Um agradecimento especial aos meus amigos Alexi Lallas, José Pedro, João Francisco, Lays Ribeiro e Paola Lauande pela amizade e apoio ao longo dos anos durante o curso, que compreenderam minhas ausências e torceram por todas as conquistas alcançadas.

“A reação mais comum da mente humana a uma conquista não é satisfação, e sim o anseio por mais.”.

(Yuval Noah Harari)

RESUMO

Este trabalho propõe aplicar a tecnologia *Multiprotocol Label Switching* (MPLS) em conjunto com engenharia de tráfego com o objetivo de fornecer melhor desempenho da rede WAN de um provedor de serviços, utilizando túneis para manipular o tráfego da melhor maneira possível. Foram realizados quatro cenários simulados utilizando o *software* GNS3, mostrando situações comuns em provedores de serviço: falha ponto-a-ponto, falha de enlace, falha de nó e link congestionado. Neles foram aplicadas técnicas do MPLS-TE, como o RSVP-TE e *Fast Reroute*, avaliando se foram capazes de solucionar os problemas propostos e mostrando a visão do provedor e do cliente em um ambiente virtualizado, através do *Oracle VirtualBox*. Para mostrar a eficiência da tecnologia, foi utilizada a ferramenta *Wireshark*, na qual foi possível coletar e analisar os pacotes da rede e comparar com outros protocolos comuns em provedores de serviços.

Palavras-chave: MPLS-TE, Engenharia de Tráfego, Congestionamento, Perda de Pacote.

ABSTRACT

This paper proposes to apply Multiprotocol Label Switching (MPLS) technology in conjunction with traffic engineering in order to provide better performance of a service provider's WAN network, using tunnels to handle traffic in the best possible way. Four simulated scenarios were performed using the GNS3 software, showing common situations in service providers: peer-to-peer failure, link failure, node failure, and congested link. They were applied MPLS-TE techniques, such as RSVP-TE and Fast Reroute, evaluating if they were able to solve the proposed problems and showing the view of the provider and the client in a virtualized environment through Oracle VirtualBox. To show the efficiency of the technology, the Wireshark tool was used, in which it was possible to collect and analyze network packets and compare with other common protocols in service providers.

Keywords: MPLS-TE, Traffic Engineering, Congestion, Packet Loss.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AS	*Autonomous System* (Sistema autônomo)
ATM	*Asynchronous Transfer Mode*
BGP	*Border Gateway Protocol*
CE	*Custumer Edge Equipament*
CoS	*Classes of Service*
CSPF	*Constrained Shortest Path First*
EIGRP	*Enhanced Interior Gateway Routing Protocol*
eBGP	*externa Border Gateway Protocol*
FEC	*Forwarding Equivalency Class*
FTN	*FEC-To-NHLFE*
FRR	*Fast Reroute*
IAP	*Internet Access Provider*
iBGP	*interna Border Gateway Protocol*
IETF	*Internet Engineering Task Force*
IGP	*Interior Gateway Protocols*
IML	*Incoming Label Map*
IP	*Internal Protocol*
IPSec	*Internet Protocol Security*
IPv4	*Internet Protocol version 4*
ISP	*Internet Service Provider*
L2TP	*Layer 2 Tunnelling Protocol*
LDP	*Label Distribution Protocol*
LIB	*Label Information Base*

LSA	*Link-State Advertisement*
LSP	*Label Switch Path*
LSR	*Label Switch Router*
MAC	*Media Access Control*
MP-BGP	*Multiprotocol-Border Gateway Protocol*
MPLS	*Multiprotocol Label Switching*
MPLS-TE	*Multiprotocol Label Switching-Traffic Engineering*
NHLFE	*Next Hop Label Forwarding Entry*
OSI	*Open Systems Interconnection*
OSPF	*Open Shortest Path First*
OSPF-TE	*Open Shortest Path First – Traffic Engineering*
PE	*Provider Edge Equipament*
POP	*Point of Presence*
PPTP	*Point-to-Point Tunneling Protocolo*
QoS	*Quality of Service*
RD	*Router Distinguisher*
RIP	*Routing Information Protocol*
RSVP	*Resource Reservation Protocol*
RSVP-TE	*Resource Reservation Protocol – Traffic Engineering*
SLA	*Service Level Agreement*
TCP	*Transmission Control Protocol*
VPN	*Virtual Private Network*
VPRN	*Virtual Private Routed Network*
VRF	*Virtual Routing and Forwarding*
WAN	*Wide Area Network*

SUMÁRIO

1 INTRODUÇÃO

Um provedor de serviços de internet (ISP) é uma empresa que fornece serviços de acesso à internet permitindo a navegação na *World Wide Web* e acesso a serviços como envio e recebimento de e-mail, as vezes também é chamado de IAP (*Internet access provider*). A rede de um provedor é formada por uma rede de telecomunicações que se estende por uma vasta área geográfica, podendo abranger estados e até mesmo países. Por interligar uma grande quantidade de clientes, o custo para manter a disponibilidade dos enlaces e roteadores da rede são significativos.

Os enlaces geralmente são formados por fibra óptica, que apesar de transportar um grande fluxo de dados em longas distancias, são muito finas, possuindo alguns micrometros de diâmetro. Devido a essa fragilidade, requer muito cuidado no seu manuseio a fim de evitar possíveis falhas que podem comprometer um enlace inteiro.

Os nós da rede geralmente são formados por roteadores e switches de alta capacidade, que possuem grande confiabilidade e com economia de energia, desenvolvidos para atender aos requisitos da rede. Para evitar possíveis falhas elétricas nos POPs (*Point of Presence*), as empresas geralmente utilizam *nobreaks,* dessa maneira, impedindo a indisponibilidade dos clientes por um certo tempo.

O aumento do número de usuários e a implantação de novos aplicativos exigiram a necessidade de melhoria na arquitetura das redes dos provedores de serviços de internet. As redes IP são usadas para troca de dados na internet, e apesar de sua boa funcionalidade, elas não são mais suficientes para fornecer a qualidade de serviço necessária para atender a grandes provedores de internet.

O MPLS (*Multiprotocol Label Switching*) é um padrão IETF de redes de telecomunicação que utiliza “rótulos” ou “etiquetas” (*labels*) como maneira de comutar pacotes (GHEIN, 2007). O protocolo é definido pela RFC 3031 (ROSEN; VISWANATHAN; CALLON, 2001). O MPLS não substitui o roteamento IP, mas funciona juntamente com as tecnologias de roteamento existentes e futuras para fornecer encaminhamento de dados em alta velocidade entre roteadores comutados por etiqueta (LSRs), juntamente com reserva de largura de banda para fluxos de tráfego com diferentes requisitos de Qualidade de Serviço (QoS) (AHMED; IDRIS, 2013).

O encaminhamento de pacotes IP analisa o endereço IP de destino contido no cabeçalho da camada de rede de cada pacote à medida que o pacote é encaminhado ao destino

final. Já o MPLS utiliza o rótulo, na qual o seu valor é alterado a cada salto, diferentemente do cabeçalho IP. Este é justamente uma das características que tornou o MPLS popular, já que o torna uma excelente opção para soluções de VPN (SANTOS, 2003).

Cada vez mais os provedores de serviço estão migrando seus equipamentos de rede para o MPLS, porém segundo Prescott (2014), apesar de ser uma tecnologia difundida e madura, e não possuir um custo grande inicial, já que os equipamentos atualmente já vêm com o protocolo para habilitar, o uso do protocolo MPLS é mais comum em redes de operadoras em comparação aos ISPs.

Atualmente, em provedores de internet, o OSPF é o protocolo preferido entre os IGPs, operando em conjunto com o MPLS para escolher o caminho de menor custo. Porém, o MPLS não encaminha o tráfego para caminhos diferentes daqueles que o próprio roteamento IGP determina, devido a isso, a solução TE baseada em MPLS pode ser uma saída para empresas que necessitam aproveitar melhor os recursos da rede. Muitos engenheiros costumam a fazer engenharia de tráfego com ferramentas que não são do MPLS, modificando o protocolo de roteamento anterior, manipulando a métrica e alterando os custos das interfaces. Entretanto, esse tipo de modificação não influencia apenas a comunicação desejada, mas sim toda a topologia do *backbone*. Sendo assim, esse tipo de abordagem pode resolver o problema em questão, contudo, pode também criar outros.

Segundo Adeyinka A. et al. (2016), alguns problemas associados a uma rede mal projetada incluem: congestionamento, ociosidade de enlaces, desperdício de recursos da rede, links de backup mal projetados, entre outros. Esses problemas resultam em baixa qualidade de serviço ao cliente, podendo gerar perda de pacote, sendo assim, um tempo de indisponibilidade no link do cliente, afetando o acordo de nível de serviço (SLA- *Service Level Agreement*). Contudo, os provedores de serviços não podem prever algumas ocorrências, como o rompimento de fibra óptica em partes do *backbone*. Devido a isso, a infraestrutura deve ser em malha, de forma que possua uma ou mais redundâncias para que os dados possam ser redirecionados caso seja necessário. Em virtude disso, a engenharia de tráfego pode ser utilizada para resolver algumas dessas questões, por meio da implementação de túneis, que vão manipular o fluxo de tráfego pelos enlaces adequados, melhorando o desempenho geral da rede *backbone*. Algumas ferramentas do MPLS-TE como o *Fast Reroute* e RSVP-TE também contribuem para maximizar a qualidade de serviço ao cliente.

Por ser uma tecnologia consolidada, existem vários estudos sobre o emprego do MPLS-TE em redes WAN. Um exemplo desse estudo é o artigo de Adeyinka et al. (2016), que tem como objetivo comparar a performance do MPLS-TE em relação ao MPLS sem a engenharia

de tráfego e a uma rede IP, sem a aplicação MPLS, verificando a latência e a perda de pacote dos cenários. Outro estudo foi o artigo de Ahmed e Idris (2015), na qual implementaram o *Fast Reroute* numa rede MPLS-TE, e verificaram a perda de pacote durante a falha de um enlace e de um nó. Eles também realizaram a comparação com uma rede IP sem o *Fast Reroute*.

1.1 Objetivos

1.1.1 Objetivo Geral

Este projeto tem como objetivo implantar na rede WAN de um provedor de serviços a tecnologia MPLS, explorando a engenharia de tráfego com proposito de melhorar a utilização dos recursos da rede.

1.1.2 Objetivos Específicos

- Implantar o processo de virtualização do enlace, utilizando Virtual Private Network (VPN) junto a tecnologia MPLS;
- Implementação de uma rede MPLS-TE em um ambiente simulado, mostrando seus efeitos durante uma falha de enlace e nó, reduzindo o tempo de recuperação de falha e assim obtendo menor perda de pacote possível;
- Mostrar o comportamento do tráfego diante a enlaces congestionados em um ambiente simulado.

1.2 Estrutura do Trabalho

O presente trabalho está dividido em cinco capítulos, além da Introdução. O segundo é a fundamentação teórica, onde serão conceituados tópicos importantes para a compreensão do trabalho, como o funcionamento e arquitetura do protocolo MPLS, sua aplicação junto à engenharia de tráfego e sobre a tecnologia BGP/MPLS VPN. No terceiro capítulo será descrita a metodologia usada no projeto desenvolvido, com especificações da topologia utilizada e tecnologias, além da explicação da configuração dos protocolos usados.

Em sequência, no capítulo 4, serão abordados os quatro cenários propostos e seus respectivos resultados obtidos, além de explicações sobre os problemas encontrados. Por fim, o último capítulo apresentará as conclusões obtidas.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Engenharia de tráfego

Em provedores de internet o fluxo de pacotes em grande quantidade pode gerar uma alta utilização em algumas partes na rede, se manifestando por meio de congestionamentos, enquanto outra parte da rede tem o efeito contrário, causando ociosidade. A engenharia de tráfego visa manipular o tráfego de acordo com as necessidades da rede, garantindo o caminho mais apropriado, evitando saturação e enlaces ociosos, além de possuir mecanismos contra possíveis falhas na rede.

Segundo Osborne e Simha (2002), a engenharia de tráfego não é de forma alguma algo específico do MPLS, mas sim uma prática geral. Além disso, pode ser implementado em algo simples como ajustar métricas de IP nas interfaces ou algo mais complexo como a execução de um caminho completo de malha e a otimização de caminhos com base nas demandas de tráfego. A engenharia de tráfego com o MPLS é uma tentativa de aproveitar o melhor das técnicas de engenharia de tráfego orientadas a conexão e mesclá-las com o roteamento IP.

2.1.1 SLA

SLA é a sigla de *Service Level Agreement*, na tradução para o português significa Acordo de Nível de Serviço. É um acordo entre a empresa e o cliente, o qual são definidos alguns requisitos contratuais, como a qualidade de serviço que vai ser entregue, o tempo em que o serviço vai ser realizado e as penalidades para o fornecedor em caso do não cumprimento do contrato estabelecido.

Em provedores de internet são acordados parâmetros de serviços, tais como: a limitação de largura de banda do cliente, atrasos, confiabilidade, perda de dados e disponibilidade. Entre eles a perda de dados é a mais crítica. O provedor de serviços precisará ter certeza de que o serviço Ethernet que está sendo fornecido não perderá pacotes quando estes forem transmitidos pela rede (DA COSTA, 2008).

2.2 MPLS

Essa seção será dedicada à discussão sobre alguns pontos ligados à tecnologia MPLS. Para melhor entendimento é necessário ter em mente alguns conceitos essenciais, tais como: o surgimento da tecnologia no mercado, os principais elementos de sua arquitetura e como é o seu funcionamento.

2.2.1 História

Na década de 90, a tecnologia *Asynchronous Transfer Mode* (ATM) era dominante na construção de *backbones*. Naquela época já se sabia que a pilha de protocolos TCP/IP era um padrão muito utilizado no mundo, e que todas as tecnologias que fossem desenvolvidas a partir de então deveriam ser compatíveis com esses protocolos (OLIVEIRA; LINS; MENDONÇA, 2012). Porém, o mapeamento de pacotes IPs no ATM é complexo, pois causa desperdício de banda passante durante o processo de segmentação e remontagem. Além disso, possui um preço elevado, devido à exigência de maior processamento dos roteadores.

Na mesma década devido à natureza da tecnologia ATM se diferir da natureza do protocolo IP, várias empresas criaram tecnologias baseadas na utilização de rótulos. Algumas delas foram: *Aggregate Route-Based IP Switching* da IBM, *Cell Switching Router* da Toshiba e Tag Switching da Cisco (DAVIE; FARREL, 2008). Porém, a fim de padronizar a comutação de pacotes baseada em rótulos, em abril de 1997, a *Internet Engineering Task Force* (IETF) criou um grupo de trabalho para desenvolver um protocolo (OLIVEIRA; LINS; MENDONÇA, 2012). Sendo assim, surgiu o MPLS, uma tecnologia que utiliza comutação de pacotes baseada em *labels* (rótulos) para estabelecer circuitos virtuais LSP (*Label Switch Path*). É considerada uma tecnologia de camada 2.5 do modelo OSI (*Open Systems Interconnection)*, ou seja, está entre a camada de enlace e a camada de rede. De acordo com Ghein (2007) o MPLS possui uma série de benefícios, tais quais:

- Uso de uma infraestrutura de rede unificada;
- Melhor integração de IP sobre ATM;
- *Border Gateway Protocol* (BGP)-*free core*;
- O modelo ponto a ponto da VPN MPLS;
- Fluxo de tráfego otimizado;
- Engenharia de tráfego.

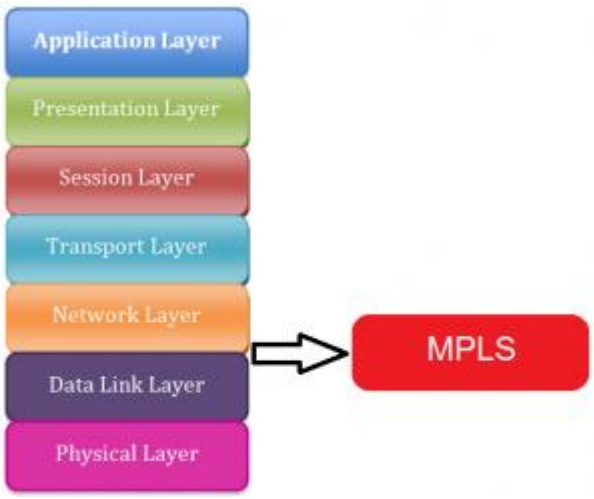
2.2.2 Arquitetura

Essa seção ajuda a entender como o MPLS opera. Serão explicados os principais elementos básicos da tecnologia, além de apresentar algumas nomenclaturas. O item mais importante para o MPLS é o rótulo (GHEIN, 2007). Este capítulo explica para que serve o rótulo, como é usado e como é distribuído em uma rede.

2.2.2.1 Cabeçalho MPLS

O MPLS é uma tecnologia baseada em pacotes rotulados, onde cada rótulo (*label*) apresenta um índice na tabela de roteamento do próximo roteador. Para melhor compreensão sobre o protocolo é importante identificar a localização exata onde será inserido o valor do rótulo no cabeçalho do pacote. A Figura 1 mostra as camadas do modelo OSI e onde o protocolo MPLS está inserido.

Figura 1 - Localização do MPLS no modelo OSI

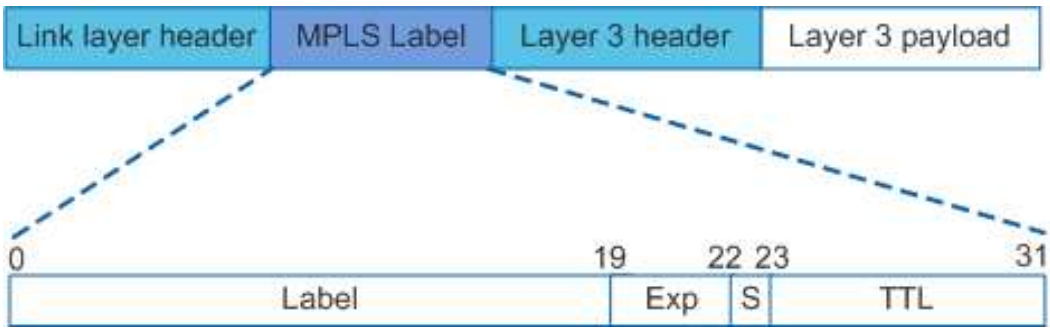


Fonte: Wilfried (2014)

Segundo Mendonça, Lins e Oliveira (2012), o rótulo é um identificador curto, de comprimento fixo de 4 bytes, e com significado local no roteador que é usado para identificar uma FEC (*Forwarding Equivalent Class*), isto é, um grupo de pacotes IPs que são enviados na mesma maneira, sobre o mesmo trajeto e com o mesmo tratamento de transmissão. Os FECs podem ser identificados pela porta de origem, porta de destino, endereço de origem, endereço de destino e VPN.

Um pacote MPLS possui o rótulo MPLS adicional de 4 bytes se comparado com um pacote IP. O MPLS permite o uso de qualquer protocolo da camada de enlace. A Figura 2 mostra a posição de um rótulo MPLS e dos campos no rótulo MPLS.

Figura 2 - Formato de encapsulamento de rótulo MPLS



Fonte: Huawei Technologies Co., Ltd. (2019)

Um rótulo MPLS contém os seguintes campos:

- *Label*: Campo de 20 bits e contém o valor do rótulo MPLS. Os pacotes são encaminhados com base nesse campo;
- Exp (*Experimental Bits*): Composto por 3 bits, é usado como classe de serviço (CoS). Quando há um congestionamento é capaz de alterar os algoritmos de enfileiramento (*queuing*) e descarte, dando prioridade ou desprezando certos pacotes;
- S: Campo de 1 bit, também chamado de BoS (*Bottom of Stack*). Quando o bit é 1 significa que há uma pilha de rótulos e ele fica na parte inferior. Se o bit é 0 significa que só possui um rótulo na pilha ou que ele era o último da pilha;
- TTL (*Time to live*): Campo formado por 8 bits. É igual ao campo TTL presente nos pacotes IP, sendo assim ele especifica um limite de saltos que o pacote deve ter. É usado para evitar possíveis loops na rede, e para isso o valor é decrementado a cada salto e quando chega a zero o pacote é descartado.

2.2.2.2 LSR

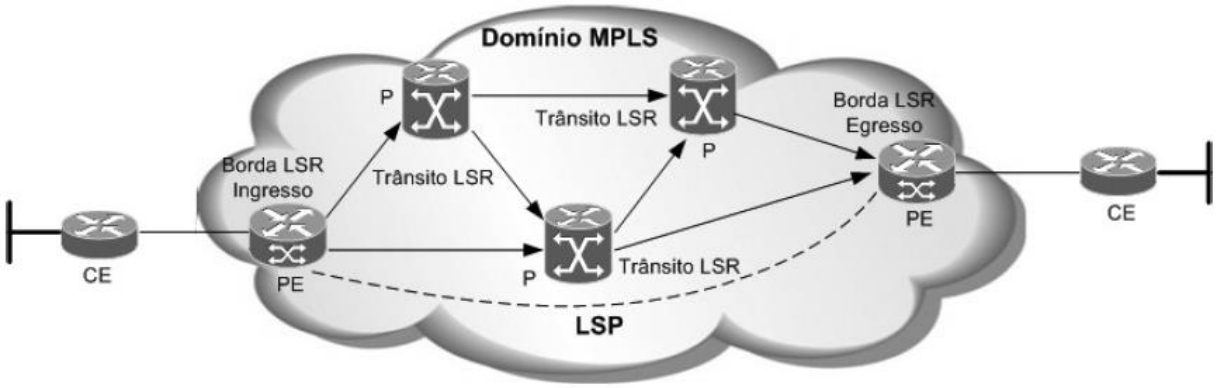
Os *Label Switch Router* (LSR) são roteadores que suportam MPLS. Estes são capazes de interpretar os rótulos MPLS e realizar operações de inserção, retirada ou troca destes rótulos (GHEIN, 2007, p. 29). Existem três tipos de LSRs em uma rede MPLS:

- *Ingress* LSRs - os LSRs do *Ingress* recebem pacotes não rotulados, fazem a inserção do rótulo e enviam estes pacotes através dos devidos links;
- *Egress* LSRs - os LSRs de saída realizam a ação contrária, recebem pacotes rotulados, removem os rótulos e os encaminham a um link de dados. LSRs de entrada e saída são LSRs de borda;
- Intermediate LSRs - os LSRs intermediários recebem um pacote rotulado de entrada, fazem operações de troca de rótulos e encaminham o pacote no link de dados correto.

Os LSRs que possuem as funções *Ingress* e *Egress*, são os roteadores que ficam na borda da rede e também podem ser denominados *Label Edge Router* (LER) (MINEI; LUCEK, 2005). No contexto de VPNs, um LSR intermediário pode ter a nomenclatura de *Provider* (P) e um LER pode também ser chamado de *Provider Edge* (PE) (GHEIN, 2007). Apesar de não fazer parte do domínio MPLS, os roteadores que fazem parte da rede interna do cliente possuem terminologia no ambiente MPLS, sendo chamados de CEs (*Customer Edges*).

Figura 3 mostra os principais elementos da arquitetura MPLS, nela é possível visualizar os LSRs de borda de Ingresso e Egresso, os LSRs intermediários P, e também os CEs, fora do domínio MPLS.

Figura 3 - Componentes da arquitetura MPLS



Fonte: Mendonça, Lins e Oliveira (2012)

Os roteadores de borda serão explicados mais detalhadamente na seção a seguir.

2.2.2.3 LER

Os roteadores *Label Edge Router* (LER) estão localizados da borda do domínio MPLS, onde manipulam tradicionais funções de roteamento e promovem conectividade aos usuários da rede. São classificados como egresso e ingresso. O primeiro analisa os pacotes que estão saindo no domínio para encaminhá-lo ao seu destino. O segundo é quando o pacote entra na nuvem MPLS. É realizado a avaliação do cabeçalho IP, classificando o pacote de acordo com a sua Classe de Encaminhamento Equivalente (FEC - *Forwarding Equivalency Class*) e finalmente adicionando o rótulo ao pacote.

2.2.2.4 FEC

Ao chegar em um LER, o pacote é analisado e são determinadas as FECs. As FECs são as possibilidades de encaminhamento do pacote pela rede e todos os pacotes pertencentes à

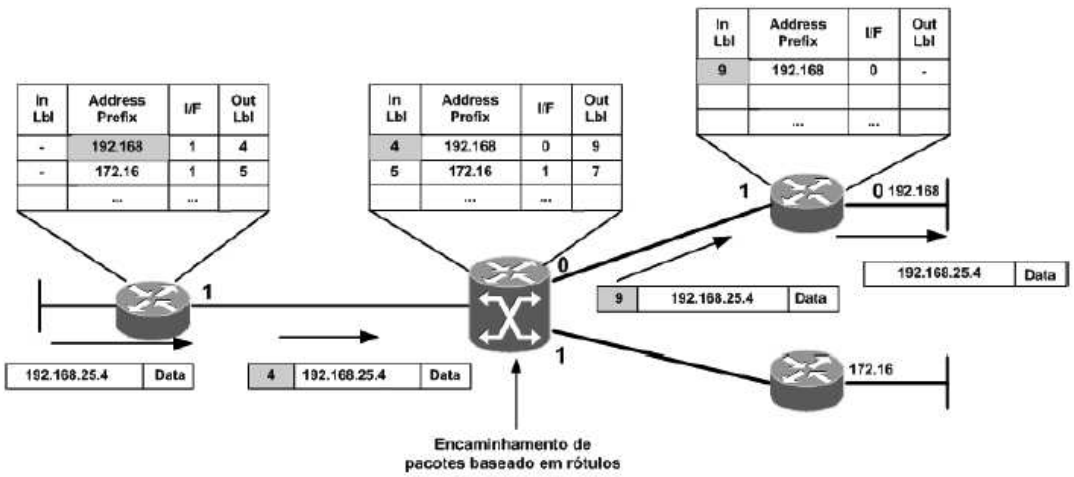
mesma FEC seguirão o mesmo caminho no domínio MPLS. Por exemplo, um grupo de pacotes cujos endereços de origem e destino são iguais.

Uma FEC é representada por um rótulo e cada LSP é associado a uma FEC. Quando um LER recebe um pacote, verifica a qual FEC ele pertence e o encaminha através do LSP correspondente (OLIVEIRA; LINS; MENDONÇA, 2012).

2.2.2.5 LIB

O LIB (*Label Information Base*) é onde contém as informações necessárias para o próximo salto do pacote, correlacionando os rótulos às interfaces do roteador. Nela existe a tabela de encaminhamento do roteador, que contém os diversos vínculos de rótulos que um LSR recebe sobre o protocolo LDP. É através desta tabela que o LSR determina para qual interface deverá encaminhar o pacote recebido (OLIVEIRA; LINS; MENDONÇA, 2012). A Figura 4 mostra a tabela de encaminhamento dos roteadores, apresentando respectivamente o rótulo de entrada, o endereço do próximo salto, interface de saída e rótulo de saída.

Figura 4 - Tabela de encaminhamento



Fonte: Mendonça, Lins e Oliveira (2012)

De acordo com Giladi (2008) há diversas formas de montar uma LIB, normalmente utiliza-se a tabela do ILM (Incoming Label Map), FTN (FEC-To-NHLFE) e NHLFE (*Next Hop Label Forwarding Entry*).

2.2.2.6 NHLFE

O NHLFE é usado ao encaminhar um pacote rotulado, ele contém informações importantes para o LSR determinar o LSP por onde encaminhar o pacote. Segundo Rosen,

Viswanathan e Callon (2001) contêm as seguintes informações: o próximo salto do pacote e a operação a ser executada na pilha de etiquetas do pacote.

A segunda informação pode ser o empilhamento (*PUSH*), substituição (*REPLACE*) e remoção (*POP*) do rótulo que está no topo da pilha. Também pode conter outros dados como o encapsulamento usado na transmissão do pacote, a codificação da pilha de etiquetas e informações necessárias para o descarte adequado do pacote.

A Tabela 1, a seguir, apresenta um exemplo de tabela NHLFE com algumas informações comentadas nesta seção, como o rótulo de saída, a operação a ser realizada, o endereço do próximo salto, o tipo de encapsulamento, como o *NULL* e *SNAP*, e o tipo de codificação usando o método SVC.

Tabela 1- Exemplo de Tabela NHLFE

Rótulo de Saída	Ação	Próximo Salto	Encapsulamento	Codificação
40	POP	80.1.0.0/26	NULL	SVC
16	REPLACE	60.1.0.0/26	SNAP	SVC
27	PUSH	50.1.0.0/26	NULL	SVC

Fonte: Santos et al, 2003

Segundo Santos et al. (2003), caso o próximo salto do pacote seja o atual LSR, então a operação da pilha de rótulo deve ser para ler e retirar um rótulo da pilha de rótulos (*POP the stack*).

2.2.2.7 ILM

O ILM (*Incoming Label Map)* é uma tabela que mapeia cada rótulo de entrada para um conjunto de NHLFEs, permitindo as ações a serem realizadas. É usada somente pelo LSR e LER de egresso.

Se o ILM mapeia um rótulo específico para um conjunto de NHLFEs que contém mais de um elemento, exatamente um elemento do conjunto deve ser escolhido antes do pacote ser encaminhado (ROSEN; VISWANATHAN; CALLON, 2001).

A Tabela 2 apresenta um exemplo de mapeamento feito pelo ILM, na qual o rótulo de entrada utiliza o índice NHFLE para indicar sua devida correspondência na tabela NHFLE (SCHARF, 2017).

Tabela 2 - Exemplo de mapeamento ILM

Rótulo de Entrada	Índice NHFLE
40	8
16	11
27	4

Fonte: Scharf (2017)

O mapeamento de um rótulo pode ser útil em casos de balanceamento de carga em vários caminhos de mesmo custo.

2.2.2.8 FTN

O FTN (FEC para NHLFE), ao contrário do ILM, é utilizado no LER de ingresso. Sendo assim, é usado ao enviar pacotes não rotulados, mas que devem ser rotulados antes de serem encaminhados. Se o FTN mapeia um rótulo específico para um conjunto de NHLFEs que contém mais de um elemento, exatamente um elemento do conjunto deve ser escolhido antes do pacote ser encaminhado (ROSEN; VISWANATHAN; CALLON, 2001).

A Tabela 3 apresenta um exemplo de tabela do FTN. Ela possui duas colunas, a direita refere-se ao endereço de destino e da esquerda ao índice da tabela NHLFE, que corresponde ao índice da tabela NHLFE, onde há as instruções para o encaminhamento do pacote e a inserção do rótulo (SCHARF, 2017).

Tabela 3 - Exemplo de mapeamento "FEC to NHLFE Map (FTN)"

FEC	Índice NHFLE
FEC1	2
FEC2	5
FEC3	4

Fonte: Scharf (2017)

Assim como o ILM, o FTN é útil em casos de balanceamento de carga em vários caminhos de mesmo custo.

2.2.2.6 LSP

O LSP é um caminho através de um ou mais LSRs, sendo o sendo o primeiro um LSR de ingresso e o último um LSR de saída, ou seja, é o caminho entre o nó de ingresso, possíveis

nós intermediários, e o nó de egresso de uma rede MPLS (OLIVEIRA; LINS; MENDONÇA, 2012).

Eles podem ser estáticos ou dinâmicos. O primeiro pode ser alocado rótulos manualmente para configurar LSP estáticos, na qual será válido apenas para o nó local. Possui baixo custo e são indicados para redes simples, de pequena escala. O segundo é estabelecido usando protocolos de distribuição de rótulos. O MPLS pode usar os seguintes protocolos para realizar essa distribuição: LDP, RSVP-TE, MP-BGP. Essas tecnologias serão comentadas mais à frente.

2.2.3 LDP

O LDP (*Label Distribution Protocol*) é o protocolo responsável pela distribuição de rótulos no domínio MPLS. O LDP é usado com o propósito de deixar o rótulo apropriado aos seus pares de distribuição de rótulos quando um LSR intitula um rótulo a uma FEC, dessa maneira tomando conhecimento deste rótulo. Os roteadores LSRs na rede MPLS utilizam o protocolo LDP para o mapeamento das informações de roteamento da Camada 3 para os caminhos comutados da Camada 2 e estabelecer LSPs na rede.

De acordo com Mendonça, Lins e Oliveira (2012), os rótulos são atribuídos a cada prefixo IGP aprendido na tabela de rotas global de um roteador e todos os prefixos anunciados por um mesmo equipamento vizinho recebem o mesmo rótulo, e com isso, os elementos intermediários em uma rede MPLS (elementos conhecidos como P) não precisam conhecer a tabela de roteamento completa da rede.

2.2.3.1 Mensagem LDP

O LDP possui como característica quatro tipos de mensagens: *discovery*, *session*, *advertisement*, e *notification.*

- *Discovery messages:* usada para anunciar e manter um LSR na rede;
- *Session messages*: empregadas para iniciar, manter e terminar sessões entre pares LDP;
- *Advertisement message*: utilizadas para criar, alterar e excluir mapeamentos de rótulos para FECs;
- *Notification messages*: em caso de erro são usadas para fornecer informações consultivas e para sinalizar sobre o incidente.

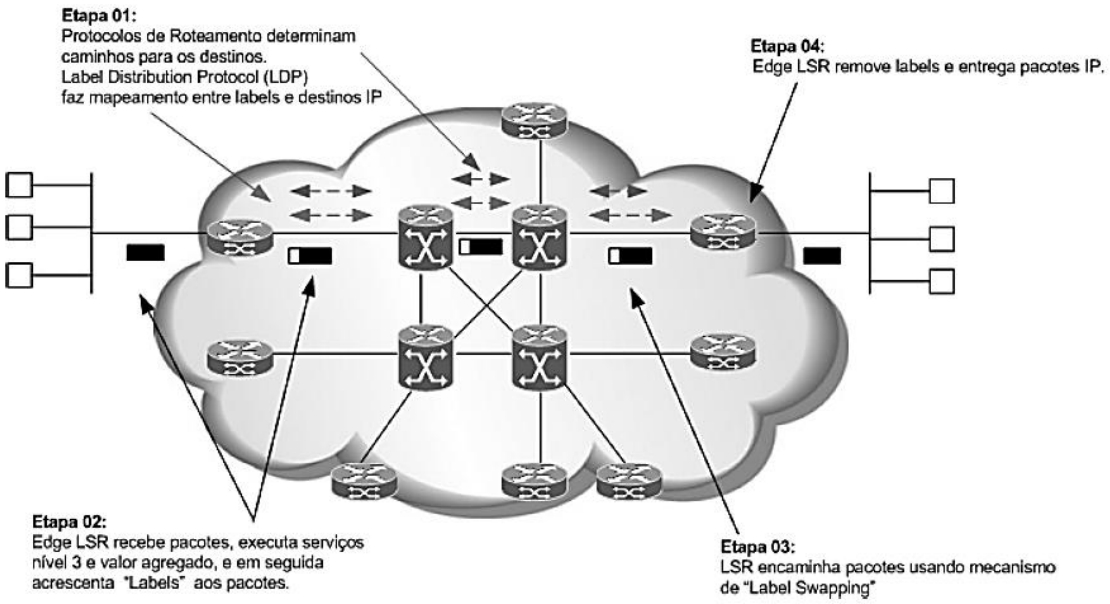
As mensagens de LDP rodam sobre o protocolo TCP para proporcionar fidelidade na entrega das mensagens. As *Discovery messages* possuem um mecanismo para conhecimento

dos vizinhos LSRs na qual enviam uma mensagem *HELLO* periodicamente para um grupo multicast. Este é transmitido como pacote UDP para a porta LDP de todos os roteadores do grupo. Segundo Andersson, Minei e Thomas (2007), quando um LSR decide estabelecer uma sessão com outro LSR aprendido por meio da mensagem *HELLO*, ele usa o procedimento de inicialização do LDP pelo transporte TCP. Após isso, os dois LSRs são pares LDP e podem trocar *advertisement messages*.

2.2.4 Funcionamento

Essa seção mostra uma visão geral do funcionamento de um domínio MPLS. Assim que entram na rede os pacotes são rotulados e são enviados baseados no conteúdo desses rótulos na rede MPLS. Mendonça, Lins e Oliveira (2012) definem a operação do MPLS em quatro etapas, conforme mostra a Figura 5:

Figura 5 - Etapas do funcionamento do MPLS



Fonte: Mendonça, Lins e Oliveira (2012)

- Etapa 1: Construção das tabelas de roteamento. Através dos protocolos de roteamento link-state, tais como OSPF e IS-IS, são feitas as tabelas de roteamento, que serão responsáveis por determinar os melhores caminhos para chegar ao destino por toda a rede do provedor. Há também nessa etapa a utilização do protocolo LDP para estabelecer uma sessão com cada vizinho direto, realizando o mapeamento entre rótulos e IPs de destino;

- Etapa 2: Ingresso dos pacotes na rede. O roteador de borda (Edge LSR) de ingresso recebe os pacotes que irão entrar na rede, executando serviços de nível 3 e valor agregado, e em seguida acrescenta o rótulo aos pacotes;
- Etapa 3: Encaminhamento dos pacotes na rede. O LSR envia pacotes usando o mecanismo de troca de rótulos (Label Swapping). Ao receber o pacote com rótulo, o LSR lê o rótulo, o substitui de acordo com a tabela LFIB e o encaminha, sendo essa ação repetida por todos os roteadores no núcleo do backbone;
- Etapa 4: Saída do pacote na rede. Nessa etapa o roteador de borda (*Edge* LSR) de saída retira o rótulo e entrega pacotes IPs.

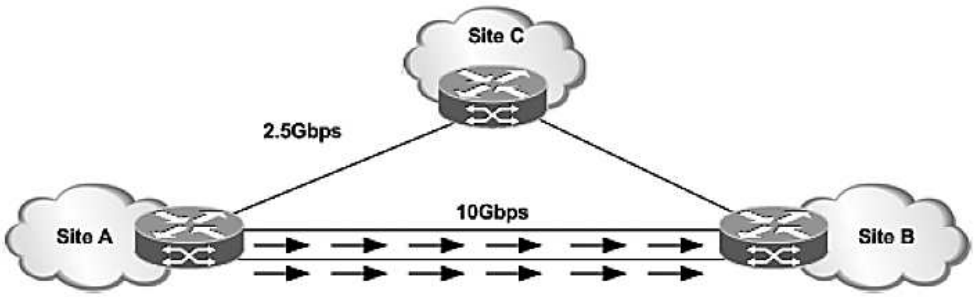
2.3 MPLS-TE

A combinação entre MPLS e engenharia de tráfego permite várias funcionalidades já existentes na TE, estabelecendo o uso de caminhos alternativos com base não só no protocolo IGP, mas também nos recursos disponíveis. Segundo Osborne e Simha (2002), existem três aplicações básicas da vida real para o MPLS-TE: a otimização da utilização da rede, a capacidade de lidar com congestionamentos inesperados e manipulação da rede em caso de falha de link e nó.

- A ideia da otimização da utilização da rede é que construa uma malha completa de LSPs entre um determinado conjunto de roteadores, dimensionando-os de acordo com a largura de banda usada entre um par de roteadores, e permitindo que os LSPs encontrem o melhor caminho na rede atendendo aos requisitos de largura de banda, evitando possíveis congestionamentos;
- Para lidar com congestionamentos inesperados é possível usar o protocolo IGP para encaminhar o tráfego para o melhor caminho. Porém, em caso de grandes eventos na rede (uma grande interrupção, um popular novo site ou serviço, ou algum outro evento que mude drasticamente padrão de tráfego) que congestiona alguns links da rede e deixa outros vazios, podem-se implantar os túneis do MPLS-TE como achar melhor, para remover parte do tráfego dos links congestionados e colocá-lo em caminhos descongestionados que o IGP não teria escolhido.
- Um terceiro uso do MPLS-TE é a rápida recuperação de falhas de links e nós. Existe um componente chamado *Fast Reroute* (FRR) que permite minimizar drasticamente a perda de pacotes quando um link ou nó falha na rede.

O roteamento tradicional baseado no IP de destino não possui mecanismo para balanceamento de carga por caminhos alternativos. Sendo assim os caminhos principais e de maior banda ficam sobrecarregados enquanto a redundância fica subutilizada. A Figura 6 mostra um exemplo onde o enlace primário possui uma banda de 10 Gbps, enquanto o enlace secundário possui banda de 2,5 Gbps. É possível perceber o que roteamento IP tradicional encaminhará o tráfego apenas pelo enlace principal (Site A para o Site B).

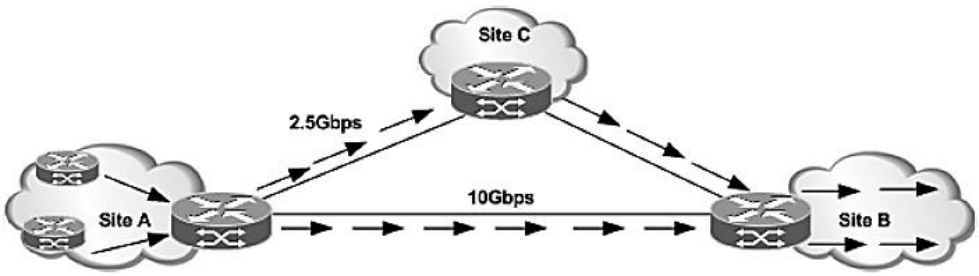
Figura 6 - Encaminhamento IP tradicional



Fonte: Mendonça, Lins e Oliveira (2012)

Segundo Mendonça, Lins e Oliveira (2012) o MPLS pode ser utilizado para criar túneis de engenharia de tráfego com base na análise do tráfego e com objetivo de fornecer balanceamento de carga entre caminhos de diferentes taxas de transmissão, como apresentado na Figura 7.

Figura 7 - Balanceamento de carga com MPLS-TE



Fonte: Mendonça, Lins e Oliveira (2012)

Assim, a engenharia de tráfego está utilizando cada vez mais o MPLS, fazendo com que os recursos da rede sejam bem aproveitados, mapeando os caminhos redundantes e prevenindo possíveis congestionamentos na rede.

2.3.1 OSPF-TE

Os IGPs são protocolos usados para trocar informações de roteamento entre nós de um AS (sistemas autônomos). Existem dois grupos dentro dos IGPs: os protocolos que usam o

vetor distância e os protocolos *link-state*. O primeiro se baseiam na distância entre a origem e o destino, na qual os nós vizinhos se comunicam informando uns aos outros a distância entre eles mantendo assim a tabela de roteamento atualizada. Já os protocolos *link-state* possuem informação sobre toda a rede, em que os nós calculam o melhor nó vizinho para todos os possíveis destinos e caso aconteça alguma alteração na topologia todos os nós na rede são avisados e assim a tabela de roteamento é atualizada. Sendo assim, quando chega um pacote no roteador, o melhor caminho já está pré-estabelecido.

Um dos principais protocolos *link-state* é o OSPF (*Open Shortest Path First*), na qual é baseado no algoritmo SPF (*Shortest Path First*), mais conhecido como algoritmo de Dijkstra, é utilizado para calcular o caminho de menor custo. Os nós da rede possuem todos os dados sobre os links existentes na sua área hierárquica, que são atualizados pelos outros roteadores através de avisos (*Link-State Advertisement - LSA*), informando sobre mudanças dos custos de um enlace. Quando há caminhos de mesmo custo, o OSPF fornece todas as rotas para melhorar a distribuição do tráfego de dados.

O OSPF-TE (*Open Shortest Path First - Traffic Engineering*) utiliza o CSPF (*Constrained Shortest Path First*) para escolher o caminho de menor custo. Ele também usa o algoritmo de Dijkstra para realizar o cálculo da rota, porém se baseia em roteamento baseado em restrições (*constraint-based routing*). Essas restrições são relacionadas ao atributo LSP, que segundo Manayya (2010) são:

- Requisitos de largura de banda;
- Limitações de salto;
- Prioridades;
- Rota explícita;
- Atributos de enlace.

2.3.2 RSVP-TE

O RSVP (*Resource Reservation Protocol*) é um protocolo de sinalização, usado para reservar recursos em uma rede. As decisões de roteamento são tomadas pelo protocolo IGP e CSPF. Segundo Osborne e Simha (2002) após a realização do cálculo do caminho ele precisa ser sinalizado pela rede a fim de estabelecer uma cadeia de rótulos salto a salto que representam o caminho e para consumir quaisquer recursos consumíveis (largura de banda) nesse caminho.

O RSVP-TE (*Resource Reservation Protocol – Traffic Engineering*) além de realizar a reserva de recursos, também é responsável pela distribuição de rótulos. O RSVP é adequado para extensão ao mundo MPLS porque lida com reservas de recursos fim-a-fim para fluxos de tráfego de forma muito semelhante com o MPLS com engenharia de tráfego (OLIVEIRA; LINS; MENDONÇA, 2012).

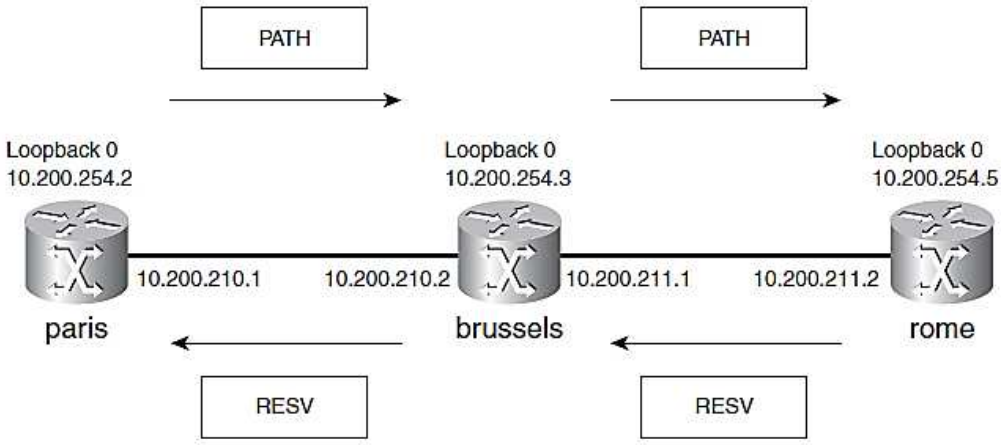
2.3.3.1 Mensagens RSVP

O RSVP é um protocolo soft-state, ou seja, precisa periodicamente atualizar suas reservas na rede. Segundo Braden et al. (1997), o soft-state do RSVP é criado e atualizado periodicamente pelas mensagens Path e Resv, e o *state* é excluído se nenhuma mensagem de atualização correspondente chegar antes da expiração de um intervalo de "tempo limite de limpeza". A seguir são apresentadas as principais mensagens do RSVP e suas respectivas funções:

- Path: Usado para configurar e mandar as reservas. É enviado da origem ao destino;
- Resv: Enviado em resposta às mensagens do Path para configurar e manter reservas. É enviado do destino até a origem;
- PathErr: Enviado por um destinatário de uma mensagem do Path que detecta um erro durante a mensagem;
- ResvErr: Enviado por um destinatário de uma mensagem Resv que detecta um erro durante a mensagem;
- PathTear: Análoga às mensagens Path, usadas para remover reservas da rede em caso de desistência da reserva de recurso;
- ResvTear: Análoga às mensagens Resv, usadas para remover reservas da rede em caso de desistência da reserva de recurso.

A Figura 8 mostra um exemplo de troca de mensagens em um cenário, onde se conseguiu transmitir o fluxo de dados. Caso houvesse finalização do fluxo por parte da origem (Paris) teria a mensagem *PathTear* passando por Paris, Bruxelas e Roma.

Figura 8 - Cenário de RSVP com as mensagens Path e Resv sendo enviadas.



Fonte: Ghein (2007)

Se a finalização fluxo fosse dada pelo destino (Roma) haveria a mensagem *ResvTear* passando por Roma, Bruxelas e Paris. Se Bruxelas não tivesse recursos suficientes mandaria uma mensagem de *ResvErr* para Roma e *PathErr* para Paris.

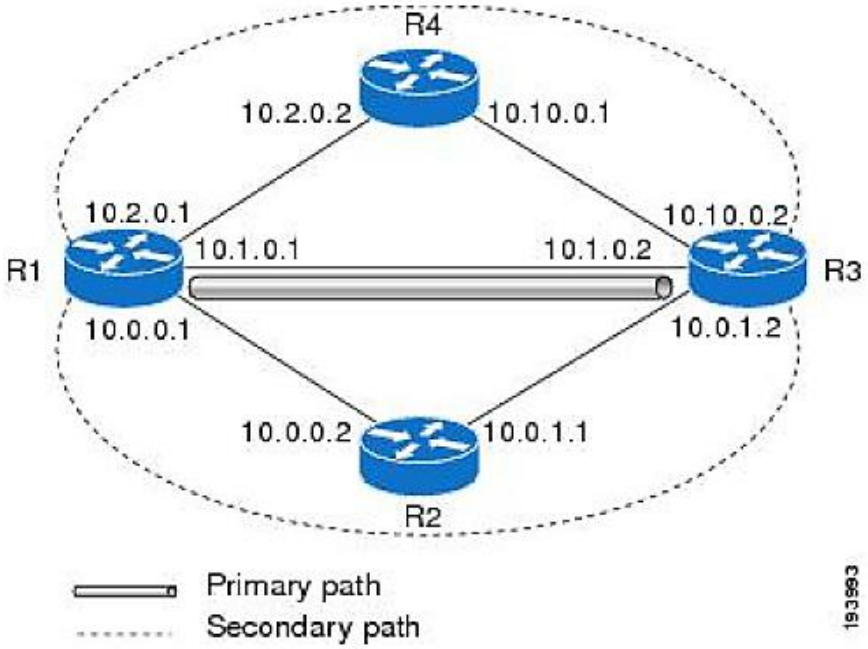
2.3.3 Proteção de caminho

No MPLS-TE a proteção de caminho fornece recuperação de falhas ponto-a-ponto na rede, ou seja, a proteção do caminho completo, da origem até o destino. Antecipadamente, um LSP secundário é estabelecido para garantir proteção contra possíveis falhas do LSP primário. Quando há uma falha no LSP protegido, o roteador *headend* imediatamente permite que o LSP secundário carregue temporariamente o tráfego do túnel, até que a rota primária fique disponível. Caso tenha alguma falha no LSP alternativo, não haverá proteção para o túnel, e até que a falha de um dos caminhos seja removida o túnel ficará indisponível.

Existem vários mecanismos para detecção de falhas que acionam a rota alternativa, entre elas está a sinalização do RSVP, por meio das mensagens PathErr e ResvTear, notificações do RSVP Hello, notificação do BFD (*Bidirectional Forwarding Detection*), notificações do protocolo IGP e pelo LSP.

As opções de rotas primárias e secundárias devem ser apenas explícitas, mesmo que haja apenas uma opção de rota alternativa. A Figura 9 mostra um exemplo de path protection, em que a rota primária é estabelecida de R1 para R3 e as possíveis rotas alternativas podem ser R1, R4 e R3 ou R1, R2 e R3.

Figura 9 – Cenário exemplo de Path Protection



Fonte: Cisco Systems, Inc. (2013)

Pode haver múltiplas rotas de proteção, porém, na configuração das rotas deve haver um grau de prioridade entre elas. Quanto menor o identificador, menor a prioridade.

2.3.4 FRR

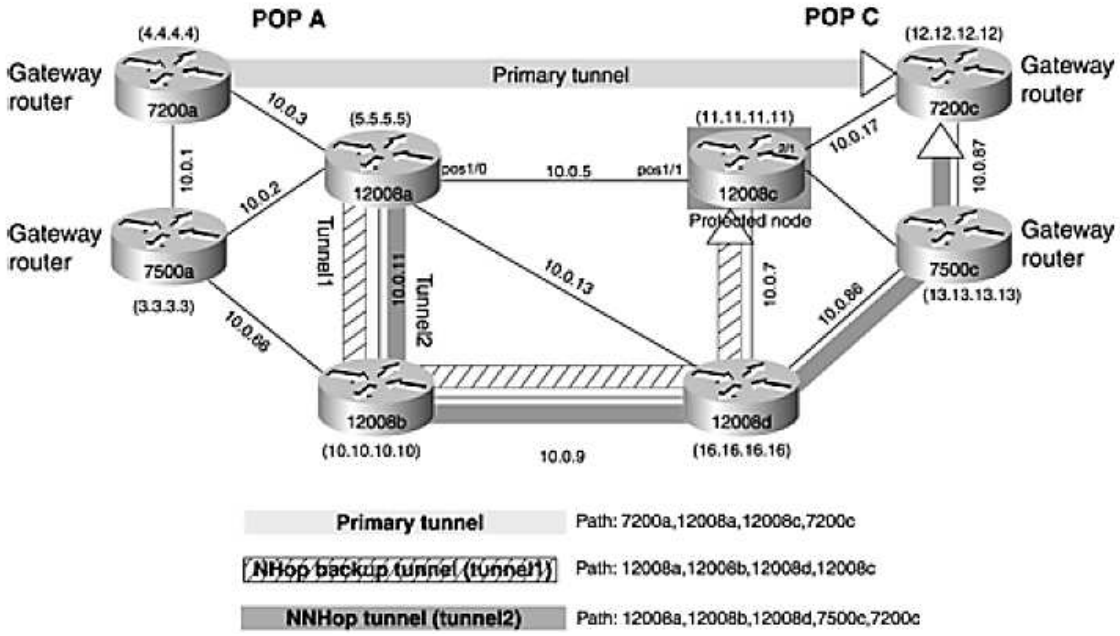
As redes de provedores de serviços são planejadas com alto nível de redundância para garantir o serviço de qualidade aos clientes, dessa maneira, respeitando o SLA acordado entre o cliente e o provedor. Contudo, às vezes a falha de um serviço (enlace ou roteador) faz com que o redirecionamento para a rota backup gaste um tempo maior, dada a quantidade de tráfego e a quantidade protocolos envolvidos. Durante essa convergência pode haver perda de pacote, afetando o SLA do cliente.

O FRR (*Fast Reroute*) é uma ferramenta do MPLS-TE que permite que enlaces e roteadores sejam protegidos por túneis do MPLS-TE, possuindo um tempo de convergência de milisegundos. A proteção de enlace é denominada *Link Protection* e a proteção dos roteadores é denominada *Node Protection*. Nos dois tipos a proteção é local, e o reparo é realizado o mais próximo possível do ponto de falha, sendo configurado um túnel de backup para cada situação com antecedência no roteador mais próximo.

A Figura 10 mostra um cenário de proteção de link e nó. O túnel primário possui caminho 7200a, 12008a, 12008c e 7200c. Em caso de perda de enlace entre 12008a e 12008c, o roteador 12008a ativa o túnel *backup* levando o tráfego para o roteador 12008c. Ou seja, o

head-end do túnel *backup* é o 12008a, que é o PLR (*Point of Local Repair*) e o fim do túnel é o roteador 12008c, que é o MP (*Merge Point*). Nesse caso, o túnel *backup* é chamado de NHOP (*Next Hop Router*).

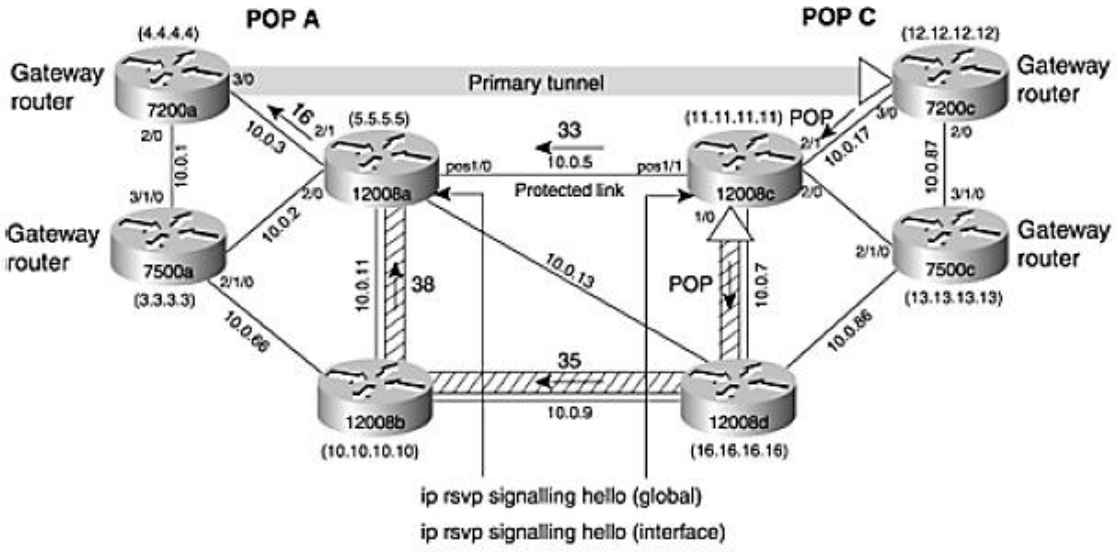
Figura 10 - Cenário exemplo de Proteção de Link e Nó



Fonte: Osborne e Simha (2002)

É importante configurar algum recurso que alertará o 12008a sobre a falha do link. Nesse caso, será usado o RSVP *Hello*, que detectam quando um nó vizinho não está mais acessível. Segundo Osborne e Simha (2002), os *Hellos* permitem que nós RSVP detectem quando um nó vizinho está indisponível e após um certo número de intervalos, os *hellos* percebem que o vizinho não está mais respondendo e deleta o estado. Isso faz com que os recursos do nó sejam liberados para serem reutilizados por outros LSPs. A Figura 11 mostra o mesmo cenário usando o RSVP *Hello State Timer*. O recurso deve ser configurado tanto globalmente quanto na interface dos roteadores.

Figura 11 - Detecção de falha usando RSVP Hellos



Fonte: Osborne e Simha (2002)

Na proteção de nó é semelhante à proteção de enlace, porém o MP não é mais o NHOP, mas sim o NNHop (*Next Next Hop Router*). Isso tem implicações no empilhamento de etiquetas. Na proteção de link, o PLR sabe qual rótulo o MP espera, porque recebe um mapeamento de rótulo diretamente do MP para o túnel primário. Na proteção do nó, no entanto, o rótulo que o MP deseja ver nunca é sinalizado através de RSVP para o PLR. (OSBORNE; SIMHA, 2002). Devido a isso utiliza-se do mecanismo *Label Recording* (gravador de etiquetas), um sinalizador que é ativado sempre que o *Fast Reroute* é configurado no roteador *headend*. Ele registra o rótulo de entrada, usado em cada salto para que o PLR, realizando o *Node Protection*, ao alternar para a rota secundária saiba qual rótulo usar no LSP protegido.

No exemplo da Figura 10, o MP é o 7200c, ou seja, em caso de perda do nó 12008c, o caminho backup será 7200a, 12008a, 12008b, 12008d, 7500c e 7200c. Na proteção de nó é importante também utilizar o recurso RSVP *Hello*.

2.4 BGP/MPLS VPN

Nesta seção serão apresentadas algumas concepções sobre VPN, e como é aplicado junto com a tecnologia MPLS. Será comentado brevemente sobre o protocolo de roteamento BGP e sobre as tabelas VRF.

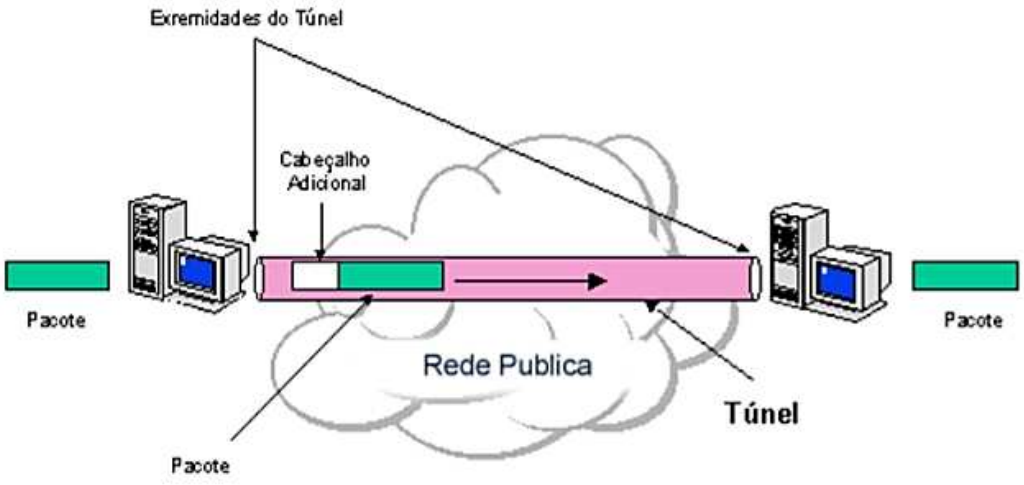
2.4.1 VPN

VPN (*Virtual Private Network*), ou Rede Privada Virtual, é uma rede privada estabelecida sobre a infraestrutura de uma rede pública, normalmente a Internet. A tecnologia propõe solucionar o problema de segurança, usando criptografia e a autenticação para proteger os dados enquanto estiverem em transito.

Empresas geograficamente distribuídas precisam de segurança para a transmissão de dados pela rede. Uma vez que dados privados são trocados pela Internet, que é um meio não muito seguro de transmissão, eles precisam ser protegidos para não sofrerem nenhum tipo de intercepção ou modificação. O uso da VPN é muito comum entre comunicação entre matriz e filiais, mas também pode ser usada como acesso remoto.

Na VPN o pacote criptografado e encapsulado sai da origem até chegar ao destino através da Internet, onde lá é desencapsulado e descriptografado, voltando ao seu estado original. A Figura 12 mostra o processo de tunelamento de três etapas: encapsulamento, encaminhamento e desencapsulamento. A primeira etapa ocorre na origem, onde o pacote é encapsulado e é adicionado um cabeçalho adicional que contém as informações de roteamento. Depois é estabelecido um túnel, onde pacote é encaminhado para o destino, passando pela rede intermediária. Por fim, o pacote chega ao seu destino, realizando o desencapsulamento do pacote.

Figura 12 - Tunelamento VPN e a passagem do pacote por ele



Fonte: Lemos (2007)

O tunelamento pode ocorrer tanto na camada de enlace (L2TP (*Layer 2 Tunnelling Protocol*) e PPTP (*Point-to-Point Tunneling Protocol*)) quanto na camada 3 (IPSec (*Internet Protocol Security*) e BGP/MPLS).

2.4.2 MPLS VPN

O uso de VPNs é uma das implementações mais comuns que fazem o uso do protocolo MPLS. Sua junção chamada MPLS/VPN empregada em provedores de serviços, busca facilitar as operações da rede para os clientes, principalmente aqueles que possuem mais de uma unidade, tal como sede e filial.

MPLS VPN de camada 3 são chamadas de VPRN (*Virtual Private Routed Network*). Nesse tipo de tecnologia o roteador do usuário utiliza algum protocolo de roteamento para se comunicar com os roteadores de borda (LER). Os roteadores de borda conectados ao roteador do cliente utilizam uma tecnologia que seja capaz de montar uma tabela de encaminhamento para cada VPN, chamada de VRF (*Virtual Routing and Forwarding*). Dessa forma, para um cliente que pertença a uma VPN será fornecido a ele apenas o conjunto de rotas contidas na correspondente tabela. Para compartilhar as informações necessárias para a formação das tabelas do VRF é necessário um protocolo de roteamento, o BGP (*Border Gateway Protocol*).

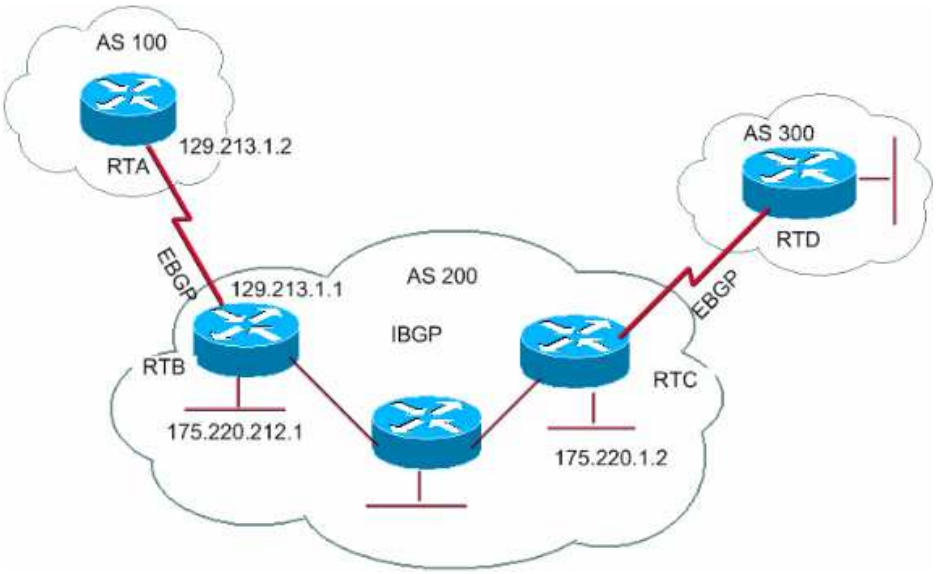
2.4.3 BGP

O BGP (*Border Gateway Protocol*) é um protocolo de roteamento entre AS. A transferência de pacotes é dada baseada em regras, caminhos e políticas de rede que são estabelecidas pelo administrador da rede. Dessa maneira, cada roteador possui uma tabela de roteamento que indica o destino, o roteador vizinho e o caminho até o destino.

O roteamento que ocorre dentro de um mesmo AS é chamado de iBGP (*Internal Border Gateway Protocol*), já um roteamento entre ASs diferentes é chamado de eBGP (*External Border Gateway Protocol*). A divulgação das rotas é realizada entre os roteadores de mesmo AS e entre ASs diferentes, ou seja, tanto em sessões iBGP e eBGP. A troca de informações se dá por uma conexão TCP na porta 179.

A Figura 13 mostra o cenário das duas classes em relação aos ASs, mostrando o eBGP entre dois ASs diferentes: AS 100 e AS 200, e AS 200 e AS 300. É possível também observar o iBGP dentro do mesmo AS, no AS 200.

Figura 13 - Cenário do domínio BGP



Fonte: Cisco Systems, Inc. (2008)

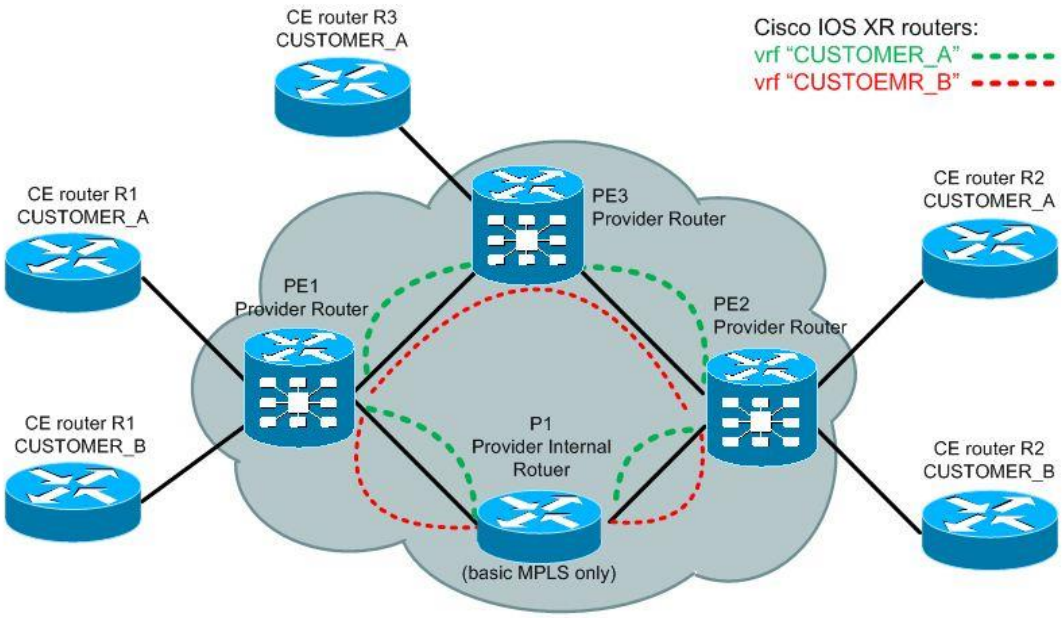
Para estabelecer conexões, trocar informações de rota, informar algum erro e verificar se outro dispositivo BGP está disponível, o protocolo BGP utiliza mensagens.

2.4.4 VRF

VRF (*Virtual Routing and Forwarding*) é uma tecnologia essencial no cenário VPRN, pois possibilita separar as tabelas de encaminhamento e roteamento de cada VPN, isolando VPNs diferentes. Dessa maneira, é possível que rotas equivalentes possam ser encaminhadas para endereços diferentes tendo em base tabelas de roteamentos configuradas de forma separada para cada VRF.

A Figura 14 mostra um exemplo de cenário usando VRF. Nele existem 5 CEs (*Custumer Edge Equipament*), que não estão no domínio MPLS, e eles se conectam com os PEs (*Provider Edge Equipament*), que são os roteadores de borda. Quando o CE encaminha um pacote ao PE, é verificado se pertence a uma VRF (Costumer A ou Costumer B), caso sim, ele verifica a sua tabela de encaminhamento.

Figura 14 - Cenário VRF



Fonte: Havrila (2013)

O BGP é o protocolo responsável por distribuir as rotas das VPNs entre os roteadores PEs. Segundo Mendonça, Lins e Oliveira (2012) para realizar uma VPN MPLS é necessário o conhecimento de alguns atributos utilizados, que são: RD (*Route Distinguisher*) e RT (*RouteTargets*). O primeiro é um identificador único, que é inserido na frente do IPv4 (32 bits do IPv4 + 64 bits do RD), fazendo com que seja único através da rede VPN MPLS. O RT é um atributo que indica quais rotas devem ser importadas e exportadas para outras VRFs.

A junção do IPv4 mais o RD, que forma o endereço com 96 bits no total, é conhecido como endereço VPNv4. Porém, o BGP não possui suporte a essa tecnologia, por isso o MP-BGP (*Multiprotocol-Border Gateway Protocol*) foi escrito para atender a essa necessidade, capacitando a distribuição de endereçamento VPNv4.

2.5 SOFTWARES

Existem vários simuladores e emuladores de redes disponíveis. Ambos possuem propósitos similares, porém trabalham de formas diferentes. Os simuladores visam imitar o comportamento de um sistema, sem necessariamente reproduzir seus componentes reais, entre eles podemos citar o *Packet Tracer*. Os emuladores propõem a possibilidade de reconstruir um sistema a partir do entendimento do funcionamento dos componentes da rede, imitando os recursos de *hardware* de um equipamento real, bem como os recursos de *software*, de forma que o resultado seja o mais próximo possível do original. Como exemplo podemos citar o GNS3, que será abordado neste trabalho.

Existem também ferramentas que auxiliam na virtualização e análise da rede, como o *Oracle VirtualBox* e o *Wireshark,* respectivamente. Esses *softwares* serão explicados nesta seção.

2.5.1 GNS3

O GNS3, abreviação para *Graphical Network Simulator*, é um software de código aberto que simula redes complexas tentando chegar o mais próximo possível do comportamento de redes reais, sem necessitar de um hardware dedicado para isto, como com roteadores e switches (GNS3, 2007). Ele foi lançado em 2005 e vem passando por atualizações desde então. Hoje, o software encontra-se na versão 2.2.3.

Com ele é possível realizar configurações de vários dispositivos diferentes, utilizando imagens reais dos equipamentos, como Mikrotik, Juniper e Cisco. Para carregar e rodar as imagens de roteadores da Cisco, o GNS3 utiliza o Dynamips (GNS3, 2007). É possível utilizar o *VMWare* ou o *Oracle VirtualBox* para emular os softwares de switches e roteadores.

A principal vantagem de se utilizar essa ferramenta é a possibilidade de realizar experimentos, testando novas funcionalidades dos IOS's, antes de colocar em prática em um ambiente real, a fim de evitar possíveis falhas em produções corporativas.

2.5.2 Oracle VirtualBox

O Oracle Virtual Box é um *software open source*, multi-plataforma que permite criar, gerenciar e executar máquinas virtuais (VMs). Foi desenvolvido pela empresa *Innotek* em 2007, depois comprado pela *Sun Microsystems*, que posteriormente foi comprada pela *Oracle*. Atualmente, o software encontra-se na versão 6.0.14.

O *VirtualBox* permite ajustar os recursos de hardware que estarão disponíveis para a máquina virtual, tais como a quantidade de RAM, quantidade de CPUs e tamanho do disco que poderá ser utilizado. É possível também mudar o adaptador de rede.

2.5.3 Wireshark Network Analyzer

Esta ferramenta é usada para captura em tempo real e análise de pacotes em determinada interface de rede, sendo possível monitorar o tráfego de entrada e saída dos equipamentos. Também é capaz de salvar os dados coletados, exportando e importando arquivos em diversos formatos. Sua primeira versão foi lançada em 1998 pela empresa *Gerald Combs*, e atualmente se encontra na versão 3.0.7.

O *Wireshark Network Analyzer* pode ser usado para solucionar possíveis problemas na rede, investigando os pacotes coletados. Também pode ser usado para estudar o comportamento dos protocolos, já que sua interface gráfica possibilita separar a captura por protocolos, facilitando a análise dos processos e tecnologias implementadas.

3 DESENVOLVIMENTO DA REDE MPLS-TE

O trabalho teve como objetivo implantar engenharia de tráfego usando MPLS-TE em um provedor de serviços. A fim de aproveitar os recursos disponíveis na rede, implementou-se um cenário de um *backbone* privado, e nesse cenário foi aplicado as técnicas do MPLS e engenharia de tráfego, avaliando se as técnicas aplicadas foram capazes de solucionar os problemas propostos.

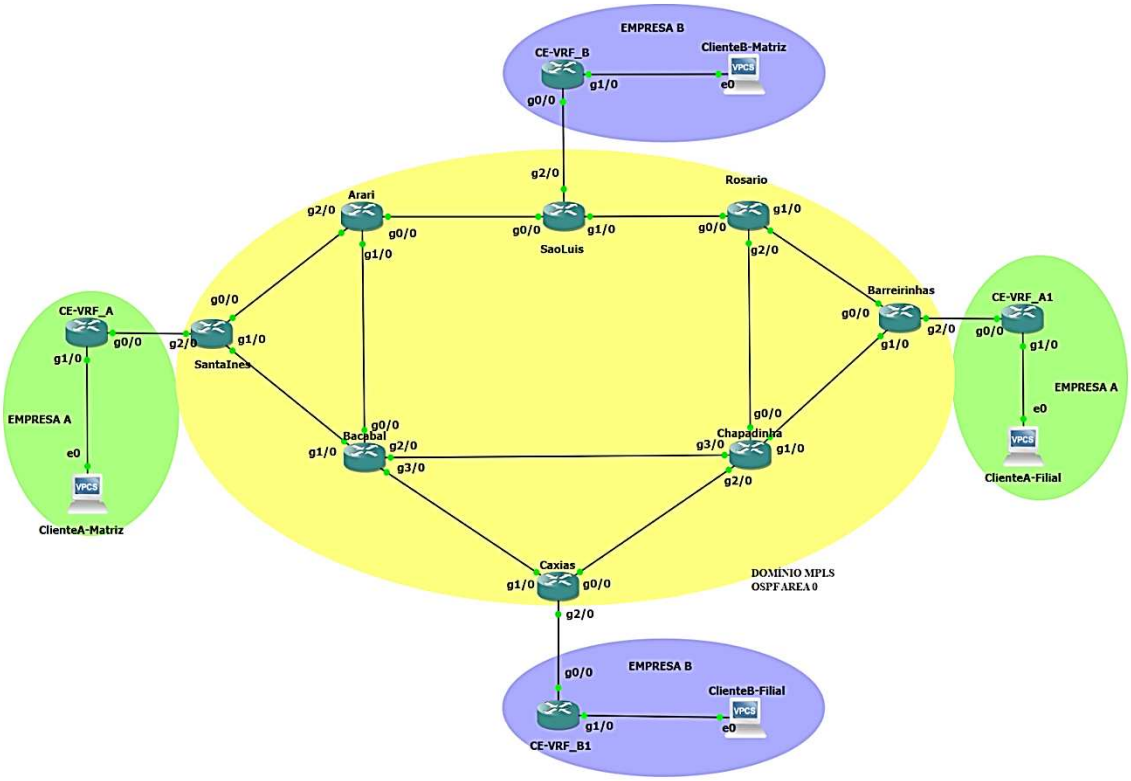
A primeira etapa para a execução do projeto que está sendo proposto foi a montagem da infraestrutura da rede, onde foi estudada uma topologia para atender aos requisitos de um provedor de serviços. Foram escolhidos também os equipamentos que fariam parte da topologia, tanto no *backbone* do provedor, como na rede do cliente. Com a infraestrutura montada, utilizou-se o GNS3 para simular a infraestrutura da rede de telecomunicações, junto ao *Oracle VirtualBox* para virtualizar o ambiente. Depois foi realizada a configuração dos elementos presentes na topologia, implementando OSPF-TE, MPLS, RSVP-TE, MPLS com engenharia de tráfego e as VPNs.

3.1 Infraestrutura

Para mostrar os conceitos teóricos aprendidos, foi montada uma rede utilizando roteadores da Cisco. Para realizar a simulação foi utilizado o GNS3, por ser um *software* gratuito e simular redes complexas, tentando chegar o mais próximo possível do comportamento de redes reais. O *Oracle VirtualBox* foi o programa usado para a virtualização do ambiente. Todos os roteadores presentes na topologia são Cisco da série 7200 e possuem enlace com capacidade de transmissão *GigabitEthernet* (1Gb/s).

Na Figura 15, a seguir, o domínio MPLS está representado de amarelo, a empresa A de verde (matriz e filial) e a empresa B de azul (matriz e filial). Os roteadores receberam nomes das cidades maranhenses que fazem parte da mesorregião norte, centro, leste e oeste, a fim de simular o funcionamento de um provedor do Maranhão.

Figura 15 -Topologia para simulação dos ambientes



Fonte: Autor

Optou-se por essa topologia por ser simples, possuir uma ou mais redundância em todos os equipamentos do *backbone*, possuir vários custos diferentes e por permitir a demonstração de todas as funcionalidades presentes do MPLS.

Na Tabela 4, a seguir, são exibidas as interfaces dos roteadores do *backbone* e seus respectivos endereços IP.

Tabela 4 - Endereço dos equipamentos *backbone* (Provedor)

Equipamento	Gi0/0	Gi1/0	Gi2/0	Gi3/0	Loopback
São Luís	10.200.0.1	10.200.0.5	172.16.1.1	-	10.100.1.1
Rosário	10.200.0.6	10.200.0.9	10.200.0.18	-	10.100.3.1
Arari	10.200.0.2	10.200.0.33	10.200.0.30	-	10.100.2.1
Santa Inês	10.200.0.29	10.200.0.26	172.16.1.1	-	10.100.4.1
Barreirinhas	10.200.0.10	10.200.0.13	172.16.2.1	-	10.100.7.1
Bacabal	10.200.0.34	10.200.0.25	10.200.0.22	10.200.0.42	10.100.5.1
Chapadinha	10.200.0.17	10.200.0.14	10.200.0.37	10.200.0.21	10.100.6.1

Caxias	10.200.0.38	10.200.0.41	172.16.2.1	-	10.100.8.1

Fonte: Autor

A Tabela 5 mostra os equipamentos dos clientes, os computadores e CEs, e seus respectivos endereços. É importante ressaltar que os CEs são roteadores do cliente, portanto não estão dentro do domínio MPLS.

Tabela 5 - Endereço dos equipamentos do cliente

Equipamento	Gi0/0	Gi0/1	Ethernet0
CE-VRF_A	172.16.1.2	192.168.1.1	-
CE-VRF_A1	172.16.2.2	192.168.2.1	-
CE-VRF_B	172.16.1.2	192.168.1.1	-
CE-VRF_B1	172.16.2.2	192.168.2.1	-
ClienteA-Matriz	-	-	192.168.1.2
ClienteA-Filial	-	-	192.168.2.2
ClienteB-Matriz	-	-	192.168.1.2
ClienteB-Filial	-	-	192.168.2.2

Fonte: Autor

Nos roteadores do *backbone* foi atribuído em cada interface de saída e na *Loopback* um endereço IP e uma máscara. As interfaces de *Loopback* são interfaces virtuais que estão sempre *UP*, a menos que estejam com *shutdown* administrativo. Possuem endereçamento IP com prefixo /32, já que não haverá outros hosts diretamente conectados a elas.

Conforme mostrado na Figura 15, existem quatro roteadores de borda (LERs) na topologia simulada: São Luís, Santa Inês, Barreirinhas e Caxias. Existem também quatro LSRs, representados por: Arari, Rosário, Bacabal e Chapadinha. Em termos de configurações, o LER possui uma complexidade maior em relação ao LSR, pois é onde será criado a VPN do cliente, o que inclui VRF, protocolo BGP e VPNv4. É também onde serão configurados os túneis da engenharia de tráfego. Em alguns cenários deste trabalho foi configurado alguns túneis nos roteadores LSRs, porém eles são utilizados como túneis alternativos ou criados para objetivos específicos. As configurações comuns aos dois tipos de roteadores são:

- Configuração dos endereços das interfaces físicas e de *Loopback*;
- Habilitar o MPLS;
- Configurar o protocolo OSPF-TE;

- Habilitar o MPLS-TE;
- Configurar o RSVP-TE;
- Habilitar o RSVP *Hello* nas interfaces.

As configurações citadas acima serão mostradas detalhadamente neste capítulo.

3.2 Configuração MPLS

Uma vez definidos os enlaces e endereçamento do *backbone* e dos clientes, iniciou-se o processo de incorporar a tecnologia MPLS na rede. O MPLS deve ser configurado em todas as interfaces dos roteadores que farão parte do domínio. Em São Luís, Santa Inês, Barreirinhas e Caxias não foi configurado na interface GigabitEthernet2/0 pois está conectada da rede interna do cliente. A Figura 16 a seguir mostra o comando utilizado na interface para habilitar o MPLS.

Figura 16 - Comando para habilitar o MPLS na interface

```
interface GigabitEthernet0/0
mpls ip
```

Fonte: Autor

Para o funcionamento do MPLS, é necessário usar um protocolo IGP para fornecer roteamento para a rede do provedor, computar as rotas do ambiente e assim gerar os rótulos. O protocolo utilizado foi o OSPF, sincronizado com o LDP, que foi o protocolo de distribuição de *labels* escolhido. O LDP é habilitado globalmente por padrão.

Optou-se pelo OSPF por ser um protocolo bem estabelecido, possuindo tempo rápido de convergência e pode ser aplicado junto à engenharia de tráfego. Na configuração do OSPF é necessário adicionar um *Router ID*, na qual é importante utilizar a interface *Loopback*, já que ela está sempre disponível, garantindo que o Router ID seja sempre o mesmo. Caso utilizasse o endereço de uma interface física, no momento que ficasse indisponível o OSPF teria que calcular novamente um novo *Router* ID.

O OSPF é responsável por distribuir as informações sobre o estado da rede, o que inclui a situação dos roteadores da rede e de suas interfaces, e caso haja alguma alteração ele deve atualizar essas informações. Para realizar o cálculo do caminho de menor custo, o OSPF utiliza o CSPF (*Constrained Shortest Path First*).

O comando *show mpls forwarding-table* mostra a tabela de encaminhamento, com as seguintes informações: rótulo de entrada, rótulo de saída, destino, interface de saída e próximo salto. Quando o pacote chega no roteador, é verificado o valor do *label* para saber qual índice da tabela de roteamento o pacote pertence. Com isso, é possível saber qual a operação irá

ocorrer com o rótulo (*POP*, *PUSH* ou *SWAP*) e qual é o destino do pacote. Por fim, enviará o pacote para a interface de saída também listada na tabela de encaminhamento MPLS. Na operação *POP* o rótulo superior é removido e o pacote é encaminhado com a pilha de etiquetas restante ou como um pacote não rotulado.

A Figura 17 abaixo mostra a tabela de encaminhamento do roteador São Luís, mostrando as operações explicadas anteriormente, onde *Local Label* é o rótulo de entrada, *Outgoing Label or VC* é o rótulo de saída, *Prefix or Tunnel Id* é o destino, *Outgoing interface* é a interface de saída e *Next Hop* é o próximo salto.

Figura 17 – Tabela de encaminhamento do roteador São Luís

SaoLuis#show mpls forwarding-table

Local Label	Outgoing Label or VC	Prefix or Tunnel Id	Bytes Label Switched	Outgoing interface	Next Hop
17	22	10.100.7.1/32	0	Gi0/0	10.200.0.6
18	16	10.100.6.1/32	0	Gi0/0	10.200.0.6
19	21	10.100.5.1/32	0	Gi1/0	10.200.0.2
20	16	10.100.4.1/32	0	Gi1/0	10.200.0.2
21	Pop Label	10.100.3.1/32	0	Gi0/0	10.200.0.6
22	Pop Label	10.100.2.1/32	0	Gi1/0	10.200.0.2
23	Pop Label	10.200.0.28/30	0	Gi1/0	10.200.0.2
24	Pop Label	10.200.0.32/30	0	Gi1/0	10.200.0.2
25	17	10.200.0.24/30	0	Gi1/0	10.200.0.2
26	29	10.200.0.40/30	0	Gi1/0	10.200.0.2
27	17	10.200.0.36/30	0	Gi0/0	10.200.0.6
28	28	10.200.0.20/30	0	Gi1/0	10.200.0.2
18		10.200.0.20/30	0	Gi0/0	10.200.0.6
29	19	10.200.0.12/30	0	Gi0/0	10.200.0.6
30	Pop Label	10.200.0.8/30	0	Gi0/0	10.200.0.6
31	Pop Label	10.200.0.16/30	0	Gi0/0	10.200.0.6

Fonte: Autor

A coluna *Bytes label switched* indica o número de bytes do rótulo comutados para esse destino. Quando o contador for zero pode significar que o LSP pode estar enfrentando um problema, ou não está passando tráfego pelas interfaces, como é o caso da Figura 17.

3.3 Configuração MPLS com engenharia de tráfego

Com o MPLS habilitado na rede, é possível utilizar a técnica de túneis para aplicar a engenharia de tráfego. É necessário habilitar o MPLS *Traffic Engineering* em todos os roteadores nos quais deseja participar do MPLS-TE. Entretanto, só a configuração global não altera nada na rede e nem adiciona qualquer túnel, mas o comando deve ser estabelecido, ou a maioria dos outros comandos não funcionará. É necessário também habilitar o comando nas

interfaces dos roteadores para alcançar um túnel TE. A Figura 18 abaixo mostra os comandos utilizados para habilitar o MPLS-TE, tanto global como nas interfaces do domínio.

Figura 18 – Comandos para habilitar o MPLS-TE

```
mpls traffic-eng tunnels

interface GigabitEthernet0/0
 mpls traffic-eng tunnels
```

Fonte: Autor

Não se deve ativar os túneis de engenharia de tráfego nas interfaces voltadas para os clientes, ou seja, em São Luís, Santa Inês, Barreirinhas e Caxias não foi configurado o MPLS-TE na interface GigabitEthernet2/0.

O protocolo IGP também deve ser configurado para suporte a TE, nesse caso foi usado o OSPF. A Figura 19 abaixo mostra os comandos utilizados, em que o *Router ID* deve ser a interface *Loopback*, e *area* é a área na qual deseja-se anunciar esse link, ou seja, a área que a engenharia de tráfego está habilitada.

Figura 19 - Comandos para habilitar o OSPF

```
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
```

Fonte: Autor

Os túneis são criados nos roteadores de borda (LERs) e são unidirecionais. A Figura 20 abaixo mostra a configuração dos parâmetros utilizados pela interface túnel do roteador São Luís. Neste caso, o caminho escolhido para o LSP é feito via CSPF, ou seja, a *path-option* é *dynamic*. Ao escolher a rota dinâmica é calculado o melhor caminho que se encaixa no túnel configurado, verificando os requisitos que atendem ao túnel, como a largura de banda.

Figura 20 - Comandos para habilitar túnel dinâmico MPLS

```
interface Tunnel4
 ip unnumbered Loopback0
 tunnel destination 10.100.8.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 0 0
 tunnel mpls traffic-eng bandwidth 60000
 tunnel mpls traffic-eng path-option 1 dynamic
```

Fonte: Autor

Existe também o *path option* no modo *explicit*, em que é configurado o caminho explícito na rede que o túnel vai passar, sem a utilização do algoritmo CSPF. Esse caminho também precisa corresponder às restrições. A Figura 21 abaixo apresenta as configurações dos

parâmetros utilizados pela interface túnel do roteador Caxias. É possível verificar que existe uma rota secundária (*backup*) também configurada, a fim de proteger a rota principal (*primary*) em caso de falha no enlace.

Figura 21 - Comandos para habilitar túnel explicito MPLS

```
interface Tunnel1
 ip unnumbered Loopback0
 tunnel destination 10.100.1.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 0 0
 tunnel mpls traffic-eng bandwidth 20000
 tunnel mpls traffic-eng path-option 1 explicit name primary
 tunnel mpls traffic-eng path-option protect 1 explicit name backup
```

Fonte: Autor

Para a verificação de falha no enlace ou nó, foi habilitado tanto globalmente como nas interfaces da rede o RSVP *Hello State Timer*. A extensão RSVP *Hello* permite que nós RSVP detectem quando um nó vizinho não está acessível. A Figura 22, a seguir, mostra o comando global e na interface.

Figura 22 - Comandos para habilitar o RSVP *Hello*

```
 ip rsvp signalling hello

interface GigabitEthernet0/0
 ip rsvp signalling hello
```

Fonte: Autor

No MPLS-TE a largura de banda está vinculada ao protocolo RSVP, na qual cada interface dos nós indica qual a largura de banda máxima que o protocolo pode reservar. Como foi visto na seção 2.3.2, o protocolo RSVP-TE é usado para reservar largura de banda devido às restrições dos túneis. Ele realiza a troca de mensagens entre todos os roteadores presentes na rota do túnel, a fim de reservar os recursos requisitados por ele. Caso não tenha banda suficiente para o túnel, o protocolo recomeça o processo para buscar o caminho com o menor custo e que satisfaça as condições do túnel.

A Figura 23 abaixo mostra a configuração do RSVP nas interfaces para sinalização e alocação de recursos para sessões de engenharia de tráfego.

Figura 23 - Comando para habilitar o RSVP

```
interface GigabitEthernet0/0
 ip rsvp bandwidth 100000
```

Fonte: Autor

O comando pode utilizar dois parâmetros: o primeiro é a quantidade de largura de banda máxima reservada na interface em Kbps (no exemplo foi configurado 100 Mbps) e o segundo é quantidade máxima de largura de banda reservada por fluxo, também em Kbps. Esse segundo não foi utilizado pois não é relevante para o MPLS-TE.

3.3.1 Proteção local

A tecnologia MPLS é capaz de recuperar perda de conectividade sem a aplicação de engenharia de tráfego utilizando o protocolo IGP. Segundo Osborne e Simha (2002), o IGP costuma a rotear rapidamente falhas, porém, em uma rede grande pode levar alguns segundos a mais para convergir, levanto até 10 segundos de perda de pacote, além disso, uma falha no link pode levar ao congestionamento de algumas partes da rede, deixando outras partes subutilizadas. Para uma convergência mais rápida que a IGP e minimizar a perda de pacotes durante uma falha, é possível utilizar o FRR (*Fast Reroute*). Essa tecnologia garante proteção de túneis quando há perda de link e nó.

O *Fast Reroute* realiza a proteção local, isso porque os túneis de backup protegem apenas um segmento do caminho, ao contrário do IGP, que realiza a proteção ponto-a-ponto. A falha de link pode ter várias causas, em um provedor de serviços a principal delas é o rompimento de fibra, já que o *backbone* possui vários nós espalhados geograficamente em uma região. Por isso, é recomendável a rede possuir uma ou mais redundâncias. A falha de nó pode ser causada por falha de energia, falha de hardware, manutenção e pela falha dos enlaces, causando isolamento do nó.

Para ter uma proteção de túnel TE, o FRR deve ser configurado explicitamente no túnel do roteador *headend* que deve ser protegido. A seguir, na Figura 24, há a configuração da tecnologia para a interface do túnel que deve ser protegido. Para configurar o *node protection* no roteador *headend* é só colocar *node-protect* depois do comando *tunnel mpls traffic-eng fast-reroute*.

Figura 24 - Configuração do *Fast Reroute* no túnel

```
interface Tunnel2
tunnel mpls traffic-eng fast-reroute
```

Fonte: Autor

O túnel que irá proteger o proteger o túnel principal deve ser configurado no roteador mais próximo da falha. Esse roteador é chamado de PLR (*Point of Local Repair*). Após a criação do túnel, é importante sinalizar o túnel backup na interface que está conectada ao link ou nó da falha. Na Figura 25, o túnel backup Tunnel12 configurado no roteador PLR é

habilitado na interface *GigabitEthernet3/0*, dessa maneira, a interface é informada sobre o túnel backup.

Figura 25 - Configuração túnel backup na interface

```
interface GigabitEthernet3/0
mpls traffic-eng backup-path Tunnel12
```

Fonte: Autor

Para melhorar a eficiência do FRR é necessário utilizar algum recurso para detecção de falhas. Neste caso, será usado o RSVP *Hello* já comentado na seção 2.3.4.

3.4 Rede Privada Virtual

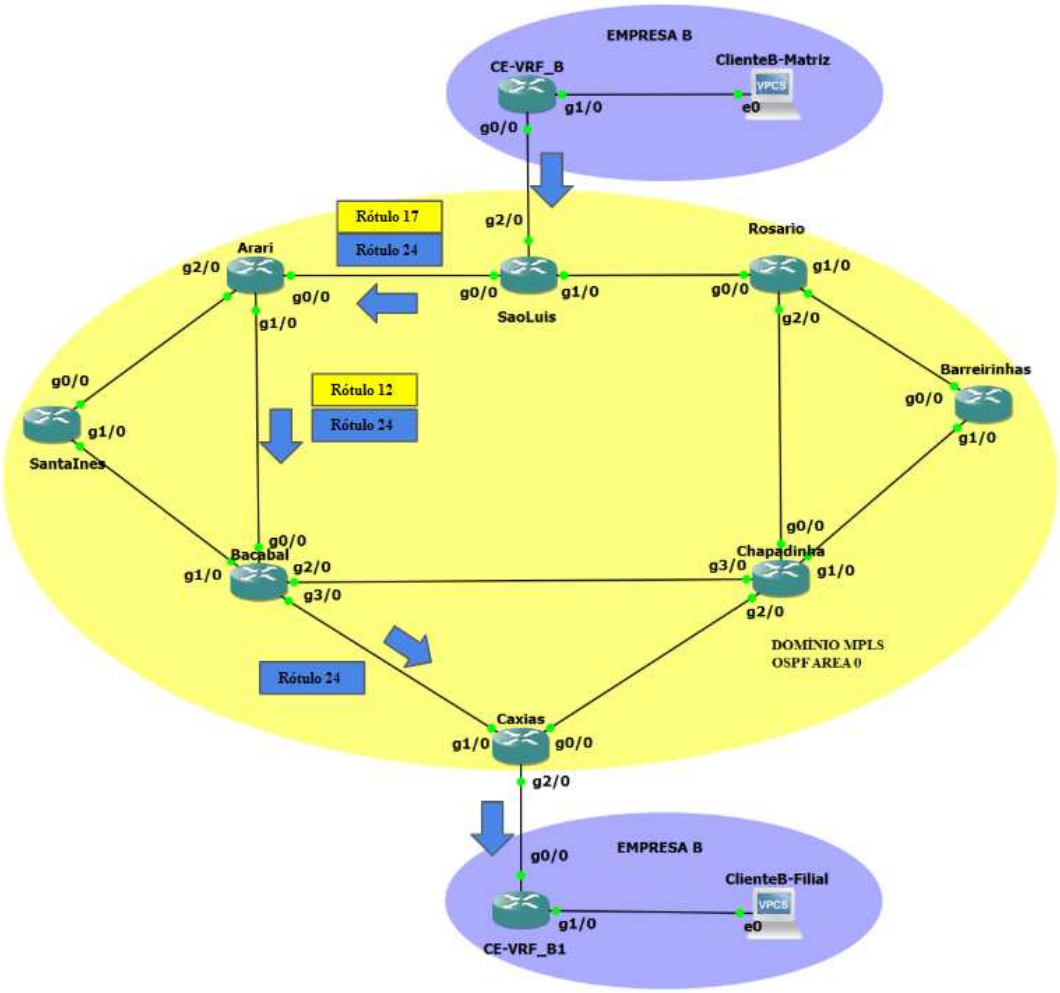
Para simular um ambiente de provedor de serviços foram adicionados dois clientes diferentes que possuíam matriz e filial, fazendo um total de quatro clientes, na qual ambos usavam a mesma nuvem MPLS. Eles estão separados geograficamente e cada par se encontra isolado entre as VPNs. A primeira VPN é a VPN_A na qual está inserida Santa Inês e Barreirinha, respectivamente matriz e filial. A outra é a VPN_B e seus integrantes são São Luís e Caxias, sendo matriz e filial. A Figura 15 mostra como as VPNs estão estabelecidas na rede.

Para a transmissão de tabelas de roteamento distintas, ou VRFs distintas, os roteadores de borda (PEs) conversam MP-BGP entre si, que é o BGP com extensão para MPLS. De acordo com Mendonça, Lins e Oliveira (2012), o MP-BGP é uma extensão que permite e facilita a troca de informações associadas aos clientes MPLS VPN entre os roteadores PEs do backbone, e dessa maneira, é possível trocar informações de diferentes protocolos (IPv4, IPv6, VPNv4) através de uma única sessão BGP entre os PEs. Uma dessas informações trocadas é o valor do rótulo da VPN, no qual ao trafegar pela rede não é modificado.

O pacote ao ser encaminhado por meio de um VPN recebe dois rótulos. O *top label* é o rótulo do IGP e é distribuído pelo LDP entre todos os roteadores Ps (roteadores centrais do fornecedor) e PEs (roteadores de borda) da rede. O *bottom label* é o próprio rótulo da VPN, que é anunciado pelo MP–BGP de PE para PEs. O valor do rótulo da base é sempre o mesmo no decorrer de todo o caminho, sendo assim não há troca de valor do seu rótulo durante o encaminhamento do pacote.

A figura 26 mostra os roteadores Ps usam o rótulo IGP para encaminhando o pacote para o PE de saída correto, e o PE de saída usam o rótulo da VPN para encaminhar o pacote para o CE correto. Quando o pacote entra no domínio MPLS ele recebe dois rótulos: um deles é o rótulo do IGP e o outro é o rótulo da VPN (24).

Figura 26 - Encaminhamento de pacotes na rede VPN MPLS



Fonte: Autor

Quando o *top label* é removido no roteador Bacabal, o *bottom label* fica no topo. Ele é analisado e enviado ao PE de destino, na qual o rótulo é removido e encaminhado para a rede do cliente.

O foco do projeto é o MPLS-TE, a intenção de configurar clientes está relacionada à geração e análise de tráfego, a fim de analisar o comportamento do usuário de um provedor de serviços em situações de falha ou possíveis congestionamentos.

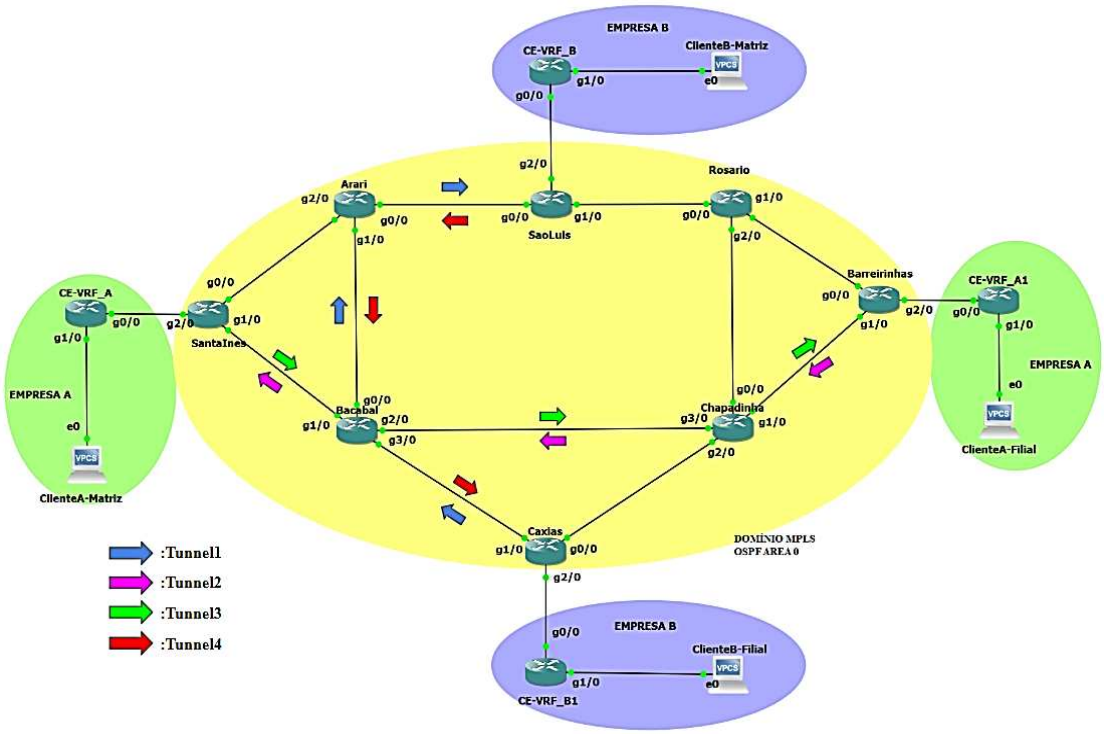
3.5 Cenários simulados

Para mostrar a eficiência do MPLS-TE em provedores de serviço foram elaborados quatro experimentos principais utilizando a topologia da Figura 15. Definiu-se que haveria quatro clientes, sendo duas VPNs, e quatro túneis da engenharia de tráfego, habilitados nos LERs da topologia: São Luís - Caxias, Caxias - São Luís, Santa Inês - Barreirinhas, Barreirinhas - Santa Inês. Cada túnel foi apresentado um cenário, que teve como objetivo

mostrar situações recorrentes em provedores de serviço, analisando o comportamento do *backbone* e dos clientes. Os quatro cenários realizados foram: proteção de caminho (*path protection*), proteção de link (*link protection*), proteção de nó (*node protection*) e link congestionado (*congested link*).

A Figura 27 mostra os túneis principais utilizados nos ambientes de teste, na qual, os túneis Tunnel1, Tunnel2 e Tunnel3 são configurados explicitamente, enquanto o Tunnel4 utiliza o IGP e CSPF para escolher o melhor caminho para o nó de destino.

Figura 27 - Túneis principais da topologia



Fonte: Autor

Os túneis possuem diferentes requisitos de largura de banda e prioridade 0. A largura de banda máxima das interfaces é de 100 Mbps, assim, todos os túneis estabelecidos só podem reservar até essa quantidade que foi delimitada na interface.

Em todos os experimentos realizados foi transmitido tráfego entre os pares de clientes, ou seja, entre a matriz e filial da empresa A e B. E em todos os cenários o tráfego foi gerado através dos próprios *hosts* e pelos clientes da rede. A análise dos dados foi realizada pelo software *Wireshark Network Analyzer*, que analisa o tráfego de rede, e o organiza por protocolos.

4 TESTES E RESULTADOS

Neste capítulo serão apresentados os quatro cenários simulados, mostrando os experimentos realizados, os dados coletados e os resultados encontrados, bem como a topologia usada na implementação da tecnologia MPLS-TE na rede WAN de um provedor de serviços, detalhando os componentes da rede, túneis, VPNs e tecnologias utilizadas.

4.1 Path Protection

No primeiro cenário foi utilizado o Túnel 1, de largura de banda limitada de 20 Mbps, para testar a proteção de caminho (*path protection*) entre Caxias e São Luís, realizando transmissão de pacotes entre a filial e matriz da empresa B.

4.1.1 Testes Path Protection

Para testar como o túnel da engenharia de tráfego se comporta em caso de falha na rede foi transmitido um fluxo de dados entre o host Caxias ⇨ São Luís e entre ClienteB-Filial ↦ ClienteB-Matriz através do comando *ping* e durante a execução foi desligado o link entre Caxias ↦ Bacabal, dessa maneira simulando a perda de caminho entre Caxias ↦ São Luís.

Nesse exemplo, para proteger a rota principal utilizou-se uma rota backup dinâmica, na qual o OSPF efetua o cálculo CSPF (*Constrained Shortest Path First*) e identifica o LSP apropriado. Através do comando *traceroute*, mostrado na Figura 28, foi verificado que o caminho original do túnel era Caxias ↦ Bacabal ↦ Arari ↦ São Luís.

Figura 28 - Traceroute Caxias - São Luís

```
Caxias# traceroute 10.100.1.1 source loopback0
Type escape sequence to abort.
Tracing the route to 10.100.1.1
  1 10.200.0.42 [MPLS: Label 18 Exp 0] 48 msec 84 msec 60 msec
  2 10.200.0.33 [MPLS: Label 24 Exp 0] 120 msec 72 msec 112 msec
  3 10.200.0.1 172 msec 88 msec 108 msec
```

Fonte: Autor

O *traceroute,* mostrado na Figura 29, também foi realizado na máquina na filial do cliente B, e percorria o mesmo caminho.

Figura 29 - Traceroute Filial B para Matriz B

```
PC2_B> trace 192.168.1.2 -P 1
trace to 192.168.1.2, 8 hops max (ICMP), press Ctrl+C to stop
 1   192.168.2.1   17.725 ms  9.023 ms  20.277 ms
 2   172.16.2.1   72.107 ms  60.323 ms  72.400 ms
 3   10.200.0.42   135.676 ms  167.990 ms  176.352 ms
```

4	10.200.0.33	156.740 ms	186.534 ms	177.019 ms
5	172.16.1.1	155.791 ms	155.375 ms	146.607 ms
6	172.16.1.2	166.459 ms	217.753 ms	176.748 ms
7	192.168.1.2	228.013 ms	197.912 ms	177.808 ms

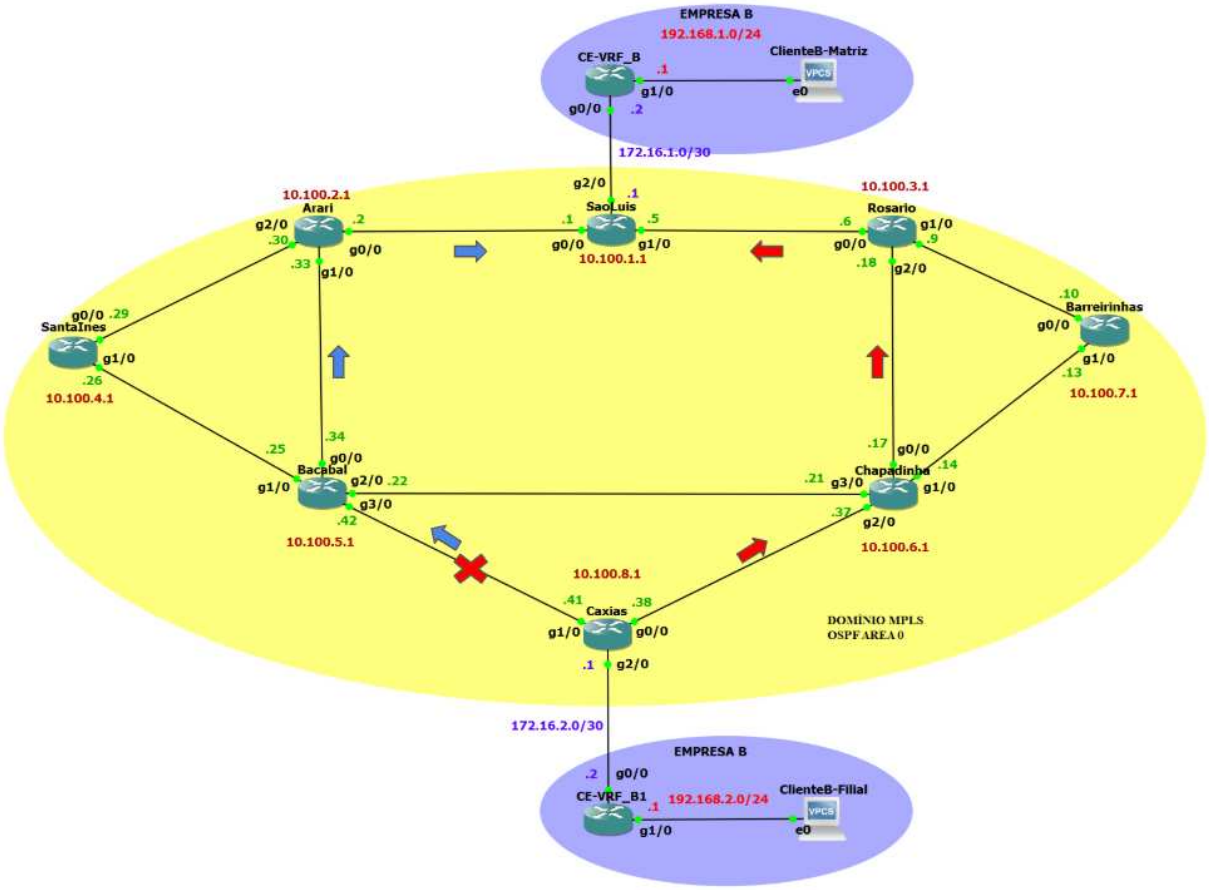
Fonte: Autor

Após realizar *shutdown* na porta *GigabitEthernet3/0* em Bacabal foi observado o comportamento do tráfego. Verificou-se que o túnel é redirecionado em segundos para a rota Caxias ↦ Chapadinha ↦ Rosário ↦ São Luís, calculada pelo protocolo OSPF. Foram realizados testes utilizando uma rota secundária explícita, mas os resultados foram os mesmos encontrados na rota dinâmica.

4.1.2 Resultados Path Protection

A seguir, a Figura 30 mostra a rota explícita antes da perda do caminho, representada por setas azuis, e rota secundária, representada por setas vermelhas.

Figura 30 - Cenário Path Protection



Fonte: Autor

Pode-se comprovar que o túnel continua funcionando (*up*) mesmo após a falha do link através do comando *show mpls traffic-eng tunnels tunnel 1*, como mostrado na Figura 31

abaixo. No campo *Status* pode-se visualizar que o túnel se encontra ativo e que possui duas rotas: a do tipo explicita (primária) e a dinâmica (secundária), na qual está sendo usada. Logo abaixo, em *RSVP Signalling Info* mostra qual rota está sendo *up*, comprovando o uso da rota secundária dinâmica.

Figura 31- Comando para verificar propriedades do túnel

```
Name: Caxias_t1                    (Tunnel1) Destination: 10.100.1.1
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path protect option 1, type dynamic (Basis for Protect, path weight 3)
    path option 1, type explicit primary

  Config Parameters:
    Bandwidth: 20000    kbps (Global)  Priority: 0  0   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute:  enabled   LockDown: disabled  Loadshare: 20000    bw-based
    auto-bw: disabled
  Active Path Option Parameters:
    State: dynamic path option 1 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled


  InLabel  :  -
  OutLabel : GigabitEthernet0/0, 22
  RSVP Signalling Info:
       Src 10.100.8.1, Dst 10.100.1.1, Tun_Id 1, Tun_Instance 570
    RSVP Path Info:
      My Address: 10.200.0.38
      Explicit Route: 10.200.0.37 10.200.0.17 10.200.0.18 10.200.0.6
                    10.200.0.5 10.100.1.1
      Record   Route:   NONE
      Tspec: ave rate=20000 kbits, burst=1000 bytes, peak rate=20000 kbits
    RSVP Resv Info:
      Record   Route:   NONE
      Fspec: ave rate=20000 kbits, burst=1000 bytes, peak rate=20000 kbits
  Shortest Unconstrained Path Info:
    Path Weight: 3 (TE)
    Explicit Route: 10.200.0.38 10.200.0.37 10.200.0.17 10.200.0.18
                  10.200.0.6 10.200.0.5 10.100.1.1
  History:
    Tunnel:
      Time since created: 2 hours, 46 minutes
      Time since path change: 38 seconds
      Number of LSP IDs (Tun_Instances) used: 570
    Current LSP:
      Uptime: 2 minutes, 58 seconds
      Selection:
    Prior LSP:
      ID: path option 1 [569]
      Removal Trigger: path verification failed
      Last Error: PCALC:: Explicit path has unknown address, 10.200.0.42
```

Fonte: Autor

Após a recuperação do link de Caxias ↦ Bacabal, o tráfego volta para a rota primária. Por padrão o tempo para voltar para a rota original da Cisco é de 1 hora, mas para esse experimento o *Periodic reoptimization* foi ajustado para 1 segundo. Observa-se que este cenário simula a perda de link do primeiro salto do *host* Caxias, o comportamento da perda de apenas uma parte da rota será analisado a seguir.

4.2 Link Protection

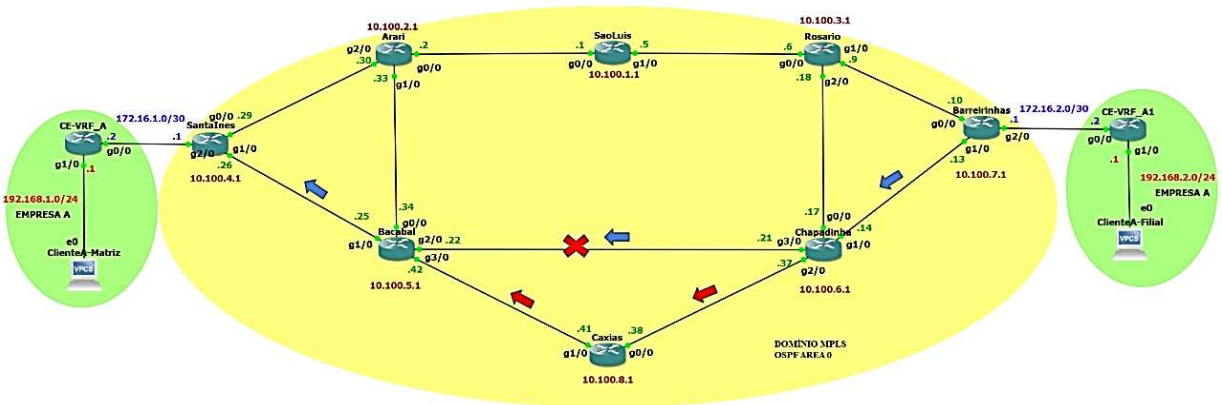
Nesse cenário foi utilizado o Tunnel 2, de largura de banda limitada de 30 Mbps, para testar a proteção de link (*link protection*) do túnel entre Barreirinhas e Santa Inês, ou seja, entre a filial e a matriz da empresa A.

4.2.1 Testes Link Protection

Nesse experimento foi utilizada a técnica comentada na seção 2.3.4, o *Fast Reroute* (FRR), na qual foi simulada a falha do link Chapadinha ↦ Bacabal, na qual o PLR (*Point of Local Repair*) é Chapadinha e o fim do túnel é Bacabal (*Merge Point*). Esse enlace é considerado o enlace crítico, em que possui um túnel backup sinalizado para a sua proteção e proteção do túnel principal de Barreirinhas.

A figura 32 mostra a proteção local entre Chapadinha ↦ Bacabal, na qual mostra a rota principal antes da perda do caminho, representada por setas azuis, e após a perda de enlace, representada por setas vermelhas.

Figura 32 - Cenário Link Protection



Fonte: Autor

Através do comando *traceroute*, mostrado na Figura 33, foi verificado que a rota original do túnel 2 era o caminho explícito de menor custo: Barreirinhas ↦ Chapadinha ↦ Bacabal ↦ Santa Inês.

Figura 33 - Traceroute Barreirinhas - Santa Inês antes da falha

```
Barreirinhas#traceroute 10.100.4.1 source loopback0
Type escape sequence to abort.
Tracing the route to 10.100.4.1
  1 10.200.0.14 [MPLS: Label 16 Exp 0] 92 msec 72 msec 88 msec
  2 10.200.0.22 [MPLS: Label 26 Exp 0] 72 msec 52 msec 72 msec
  3 10.200.0.26 44 msec 136 msec 104 msec
```

Fonte: Autor

Após a perda do enlace Chapadinha ↦ Bacabal a rota utiliza o túnel de proteção criado, chamado de Tunnel 12, direcionando o tráfego para a rota Chapadinha ↦ Caxias ↦ Bacabal. A Figura 34 abaixo mostra o *traceroute* após a perda do link.

Figura 34 - Traceroute Barreirinhas - Links após falha

```
Barreirinhas#traceroute 10.100.4.1 source loopback0
Type escape sequence to abort.
Tracing the route to 10.100.4.1
  1 10.200.0.14 [MPLS: Label 16 Exp 0] 436 msec 132 msec 152 msec
  2 10.200.0.38 [MPLS: Labels 16/26 Exp 0] 140 msec 104 msec 180 msec
  3 10.200.0.42 [MPLS: Label 26 Exp 0] 144 msec 172 msec 148 msec
  4 10.200.0.26 100 msec 136 msec 84 msec
```

Fonte: Autor

4.2.2 Resultados Link Protection

Para verificar se o túnel continua ativo e usando a tecnologia FRR, pode-se usar os comandos *show mpls traffic-eng fast-reroute database* e *show mpls traffic-eng fast-reroute database detail* no roteador PRL. Na Figura 35, é exibido o primeiro comando, na qual mostra que o endereço de origem do LSP primário está sendo protegido (10.100.7.1), também aparece a ID do túnel (2), seu LSP ID (15), a interface do link protegido (Gi3/0), o rótulo que está sendo protegido (16) e o rótulo de saída enviado pelo túnel *backup* (26).

Figura 35 - Verificação do túnel backup

```
Chapadinha#show mpls traffic-eng fast-reroute database
Headend frr information:
Protected tunnel            In-label Out intf/label   FRR intf/label   Status

LSP midpoint frr information:
LSP identifier              In-label Out intf/label   FRR intf/label   Status
10.100.7.1 2 [15]           16       Gi3/0:26         Tu12:26          active
Chapadinha#show mpls traffic-eng fast-reroute database detail
FRR Database Summary:
  Number of protected interfaces: 1
  Number of protected tunnels: 1
  Number of backup tunnels: 1
  Number of active interfaces: 1
LSP identifier 10.100.7.1 2 [15], active
  Input label 16, Output label Gi3/0:26, FRR label Tu12:26
  Role Mid  Head Hop 10.100.7.1 Tail Hop 10.100.4.1
```

Fonte: Autor

Sendo assim, é mostrado que o roteador de Chapadinha está fornecendo uma rota *backup* (Túnel 12) para o Tunnel 2 e que está operante. O segundo comando mostra as mesmas informações de forma mais detalhada.

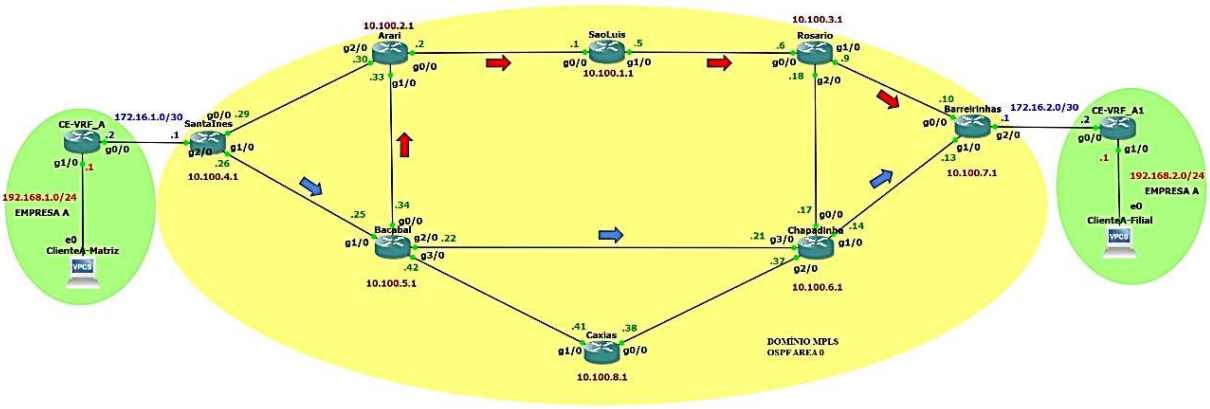
4.3 Node Protection

Nesse experimento também foi usado o *Fast-Reroute* (FRR). Foi criado o Tunnel 3, que possui banda limitada de 30 Mbps, e foi criado um Tunnel 13 em Bacabal para a proteção do roteador de Chapadinha.

4.3.1 Testes Node Protection

A Figura 36 mostra o túnel principal que faz uso do caminho Santa Inês ↦ Bacabal ↦ Chapadinha ↦ Barreirinhas, apresentado por setas azuis e o túnel *backup* Bacabal ↦ Arari ↦ São Luís ↦ Rosário ↦ Barreirinhas, apresentado por setas vermelhas. Em caso de falha do roteador Chapadinha, o tráfego será transmitido através do Tunnel 13 até que o túnel principal (Tunnel 3) seja reestabelecido.

Figura 36 - Cenário Node Protection



Fonte: Autor

Nesse exemplo Bacabal é o PLR e o MP é Barreirinhas, ou seja, o MP não é o NHOP como no *Link Protection*, mas sim o NNHOP. A Figura 37 mostra que ao executar o comando *debug ip rsvp dump-messages* pode-se verificar em SESSION_ATTRIBUTE que o mecanismo *Label Recording* está ativo.

Figura 37 – Label Recording ativado na proteção de nó

```
SantaInes#debug ip rsvp dump-messages
RSVP message dump debugging is on
SantaInes#
*Oct 30 06:12:52.407:  SESSION_ATTRIBUTE    type 7 length 20:
```

```
*Oct 30 06:12:52.407:   Setup Prio: 0, Holding Prio: 0
*Oct 30 06:12:52.407:   Flags: (0x17) Local Prot desired, Label Recording, SE Style
*Oct 30 06:12:52.411:                 Node Prot desired
*Oct 30 06:12:52.411:   Session Name: SantaInes_t3
```

Fonte: Autor

Pelo comando *traceroute*, como mostra a Figura 38, foi verificado que a rota original do Tunnel 3 era o caminho explícito de menor custo: Santa Inês ↦ Bacabal ↦ Chapadinha ↦ Barreirinhas.

Figura 38 - Traceroute Santa Inês - Barreirinhas antes da falha

```
SantaInes#traceroute 10.100.7.1 source loopback0
Type escape sequence to abort.
Tracing the route to 10.100.7.1
  1 10.200.0.25 [MPLS: Label 26 Exp 0] 92 msec 64 msec 92 msec
  2 10.200.0.21 [MPLS: Label 16 Exp 0] 84 msec 92 msec 92 msec
  3 10.200.0.13 96 msec 104 msec 104 msec
```

Fonte: Autor

4.3.2 Resultados Node Protection

A Figura 39 exibe que após a perda do nó Chapadinha, o roteador de Bacabal protege o Tunnel 3, ativando a rota *backup* Bacabal ↦ Arari ↦ São Luís ↦ Rosário ↦ Barreirinhas.

Figura 39 - Traceroute Barreirinhas - Santa Inês após a falha

```
SantaInes#traceroute 10.100.7.1 source loopback0
Type escape sequence to abort.
Tracing the route to 10.100.7.1
  1 10.200.0.25 [MPLS: Label 26 Exp 0] 472 msec 112 msec 140 msec
  2 10.200.0.33 [MPLS: Label 21 Exp 0] 144 msec 136 msec 244 msec
  3 10.200.0.1 [MPLS: Label 19 Exp 0] 140 msec 136 msec 128 msec
  4 10.200.0.6 [MPLS: Label 16 Exp 0] 148 msec 96 msec 104 msec
  5 10.200.0.10 116 msec 132 msec 132 msec
```

Fonte: Autor

Através do comando *show mpls traffic-eng fast-reroute database detail* pode-se verificar que o Tunnel 13 em Bacabal está em uso, protegendo a rota primária.

Figura 40 - Comando mostrando detalhes do FRR

```
Bacabal#show mpls traffic-eng fast-reroute database detail
FRR Database Summary:
  Number of protected interfaces: 1
  Number of protected tunnels: 1
  Number of backup tunnels: 1
```

```
  Number of active interfaces: 1
LSP identifier 10.100.4.1 3 [15], active
  Input label 26, Output label Gi2/0:16, FRR label Tu13:implicit-null
  Role Mid  Head Hop 10.100.4.1 Tail Hop 10.100.7.1
```

Fonte: Autor

É importante sempre habilitar algum recurso para a detecção de falha dos links, nesse caso foi usado o *ip rsvp signal hello*, tanto globalmente como em todas as interfaces da rede.

4.4 Congested Link

Nesse cenário específico o objetivo foi verificar o comportamento do tráfego do Tunnel 4 durante um possível congestionamento na rede. Para isso utilizou-se o RSVP *bandwidth*, configurado nas interfaces para sinalização e alocação de recursos para engenharia de tráfego.

4.4.1 Testes Congested Link

Como dito na seção 3.5, foi reservado 100 Mbps de largura de banda total nas interfaces. O Tunnel 4 foi configurado no roteador de São Luís e seu destino era Caxias, percorrendo o caminho São Luís ↦ Arari ↦ Bacabal ↦ Caxias, como mostra a Figura 41 a seguir. Não foi definido um caminho explícito, o CSPF escolhia o caminho de menor custo.

Figura 41 - Traceroute São Luís - Caxias

```
SaoLuis#traceroute 10.100.8.1 source loopback0
Type escape sequence to abort.
Tracing the route to 10.100.8.1
  1 10.200.0.2 [MPLS: Label 32 Exp 0] 312 msec 124 msec 88 msec
  2 10.200.0.34 [MPLS: Label 32 Exp 0] 64 msec 92 msec 104 msec
  3 10.200.0.41 64 msec 184 msec 92 msec
```

Fonte: Autor

Como mostrado na Tabela 6 a seguir, através do comando *show ip rsvp interface* é possível exibir as informações sobre as interfaces nas quais o RSVP está ativo, incluindo a alocação atual 30M na interface Gi0/0 e 60M na interface Gi1/0 e a largura de banda máxima disponível (100M). O túnel em questão possuía 60 Mbps de largura de banda. Os 30 Mbps são referentes ao cenário *Node Protection* da seção 4.3.

Tabela 6 - Informações de recurso de banda nas interfaces de São Luís

interface	rsvp	allocated	i/f max	flow max	sub max
Gi0/0	ena	30M	100M	100M	0
Gi1/0	ena	60M	100M	100M	0

Fonte: Autor

Para criar um congestionamento na rede foi criado um outro túnel no roteador de Arari de 40 Mbps. Percebe-se pela Tabela 7 que a alocação atual do link entre Arari e Bacabal está usando a largura de banda máxima, sendo assim a interface está no limite, não podendo passar outros túneis ou aumentar a banda dos túneis já existentes.

Tabela 7 - Informações de recurso de banda nas interfaces de Arari

interface	rsvp	allocated	i/f max	flow max	sub max
Gi0/0	ena	50M	100M	100M	0
Gi1/0	ena	100M	100M	100M	0
Gi2/0	Ena	0	100M	100M	0

Fonte: Autor

Para mostrar o comportamento do Tunnel 4, a largura de banda do túnel foi aumentada para 70 Mbps, fazendo com que o link Gi1/0 não suportasse o fluxo atual. Dessa maneira o Tunnel 4 rapidamente escolhia outro caminho com reserva de banda disponível. No experimento o túnel optou, através do CSPF, pela rota São Luís ↦ Rosário ↦ Chapadinha ↦ Caxias, que possui mesmo custo que a rota anterior. O aumento de banda em um túnel pode ter várias causas em um provedor de internet real. É importante ressaltar que o túnel pode encaminhar o trafego de vários clientes conectados no roteador, sendo assim, é possível que haja um *upgrade* de banda de algum cliente, ou até mesmo algum evento grande inesperado como um jogo novo, uma nova série *streaming*, fazendo o tráfego aumentar.

A seguir, a Figura 42 mostra o *traceroute* de São Luís para o destino após o aumento de banda.

Figura 42 - Traceroute de São Luís para Caxias após o upgrade

```
SaoLuis#traceroute 10.100.8.1 source loopback0
Type escape sequence to abort.
Tracing the route to 10.100.8.1
  1 10.200.0.6 [MPLS: Label 21 Exp 0] 212 msec 92 msec 88 msec
  2 10.200.0.17 [MPLS: Label 33 Exp 0] 68 msec 108 msec 60 msec
  3 10.200.0.38 116 msec 196 msec 116 msec
```

Fonte: Autor

Após o aumento de banda no Tunnel 4 o link Gi0/0 chega a seu limite, como mostrado na Tabela 8, abaixo.

Tabela 8 - Informações de RSVP nas interfaces de São Luís após upgrade

interface	rsvp	allocated	i/f max	flow max	sub max
Gi0/0	ena	100M	100M	100M	0
Gi1/0	ena	0	100M	100M	0

Fonte: Autor

A banda alocada na interface Gi1/0 no roteador de Arari diminui, passando apenas 40 Mbps referente ao Tunnel 12 do cenário *Link Protection*. Os 50 Mbps são referentes aos túneis 1 e 13 dos experimentos anteriores.

Tabela 9 - Informações de RSVP nas interfaces de Arari após upgrade

interface	rsvp	allocated	i/f max	flow max	sub max
Gi0/0	ena	50M	100M	100M	0
Gi1/0	ena	40M	100M	100M	0
Gi2/0	Ena	0	100M	100M	0

Fonte: Autor

Através do comando *show mpls traffic-eng tunnels tunnel 4* é possível verificar que o tunnel continua ativo após a troca de rota.

Figura 43 - Comando para verificação do Tunnel4

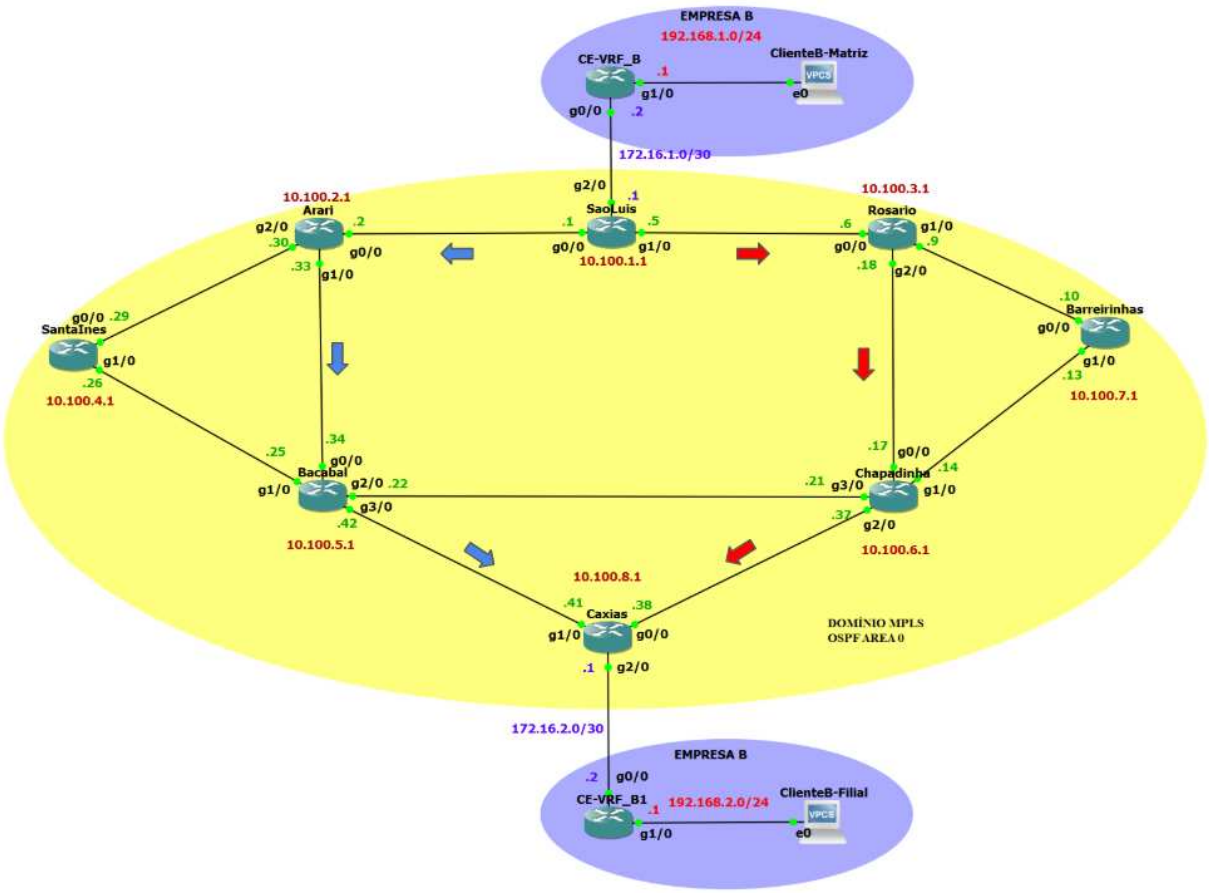
```
SaoLuis#show mpls traffic-eng tunnels tunnel 4

Name: SaoLuis_t4                    (Tunnel4) Destination: 10.100.8.1
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 1, type dynamic (Basis for Setup, path weight 3)

  Config Parameters:
    Bandwidth: 70000    kbps (Global)  Priority: 0  0   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute:  enabled   LockDown: disabled  Loadshare: 70000    bw-based
    auto-bw: disabled
  Active Path Option Parameters:
    State: dynamic path option 1 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled


  InLabel  :  -
  OutLabel : GigabitEthernet0/0, 21
  RSVP Signalling Info:
       Src 10.100.1.1, Dst 10.100.8.1, Tun_Id 4, Tun_Instance 43
    RSVP Path Info:
      My Address: 10.200.0.5
      Explicit Route: 10.200.0.6 10.200.0.18 10.200.0.17 10.200.0.37
                  10.200.0.38 10.100.8.1
      Record   Route:   NONE
      Tspec: ave rate=70000 kbits, burst=1000 bytes, peak rate=70000 kbits
    RSVP Resv Info:
      Record   Route:   NONE
      Fspec: ave rate=70000 kbits, burst=1000 bytes, peak rate=70000 kbits
  Shortest Unconstrained Path Info:
```

```
  Path Weight: 3 (TE)
  Explicit Route: 10.200.0.1 10.200.0.2 10.200.0.33 10.200.0.34
                  10.200.0.42 10.200.0.41 10.100.8.1
History:
  Tunnel:
    Time since created: 2 hours, 39 minutes
    Time since path change: 41 minutes, 41 seconds
    Number of LSP IDs (Tun_Instances) used: 43
  Current LSP:
    Uptime: 41 minutes, 44 seconds
    Selection: reoptimization
  Prior LSP:
    ID: path option 1 [42]
    Removal Trigger: configuration changed
```

Fonte: Autor

A Figura 44 mostra o caminho do link primário, e o caminho após o possível congestionamento do link Gi1/0 de Arari para Bacabal, representado por setas vermelhas.

Figura 44 - Cenário Congested Link



Fonte: Autor

É importante ressaltar que após a banda do Tunnel 4 retornar para 60 Mbps o túnel não retorna para o primeiro caminho, pois os dois possuem mesmo custo e está configurado dinamicamente. A fim de explorar esse aspecto, foi criado um terceiro túnel nesse cenário.

O Tunnel33, de banda limitada de 40 Mbps, foi criado no roteador de Rosário com destino à Chapadinha, com o intuito de mostrar que após a banda do Tunnel 4 voltar para 60 Mbps, o túnel retornava ao caminho original. Esse *host* foi escolhido estrategicamente pois já fazia parte da rota *backup* do túnel e não possuía túneis passando sobre a interface *GigabitEthernet2/0* em nenhum dos cenários já mostrados. A seguir mostra-se as informações das interfaces de Rosário após a adição do Tunnel 33.

Tabela 10 - Informações de RSVP nas interfaces de Rosário

interface	rsvp	allocated	i/f max	flow max	sub max
Gi0/0	ena	0	100M	100M	0
Gi1/0	ena	30M	100M	100M	0
Gi2/0	Ena	40M	100M	100M	0

Fonte: Autor

4.4.2 Resultados Congested Link

A Figura 45, a seguir, mostra o caminho percorrido pelo Tunnel4 após a criação do Tunnel33, percorrendo São Luís ↦ Arari ↦ Santa Inês ↦ Bacabal ↦ Caxias.

Figura 45 - Traceroute São Luís - Caxias após adição do túnel 33

```
SaoLuis#traceroute 10.100.8.1 source loopback0
Type escape sequence to abort.
Tracing the route to 10.100.8.1
  1 10.200.0.2 [MPLS: Label 35 Exp 0] 144 msec 152 msec 148 msec
  2 10.200.0.29 [MPLS: Label 34 Exp 0] 288 msec 112 msec 380 msec
  3 10.200.0.25 [MPLS: Label 21 Exp 0] 512 msec 364 msec 284 msec
  4 10.200.0.41 140 msec 148 msec 84 msec
```

Fonte: Autor

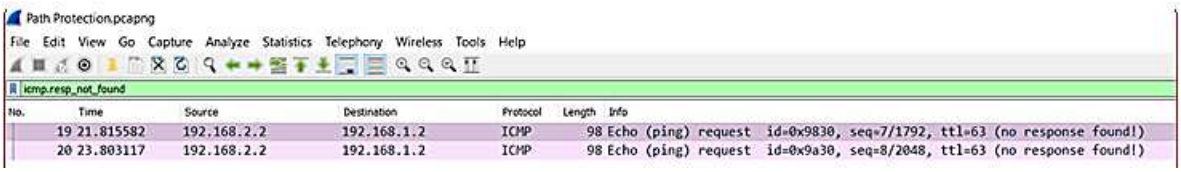
Após realizar o *downgrade* da banda para 60 Mbps novamente, verificou-se que o túnel rapidamente voltava para a rota original percorrida.

4.5 Análise dos resultados

Nesta seção serão abordados os resultados obtidos nos cenários simulados. Primeiramente foi realizada uma análise detalhada sobre a perda de pacote dos cenários. Por fim, todos os dados coletados foram analisados para ter uma visão geral de todos os testes e comparados com outras tecnologias.

Para verificar a perda de pacote dos cenários foi utilizado o software *Wireshark*. Os pacotes foram capturados tanto no *backbone* quanto na rede do cliente (entre o CE e o PE) e a análise de pacotes foi analisada baseada em TCP e ICMP usando respectivamente os filtros tcp.analysis.retransmission e icmp.resp_not_found no *Wireshark* (*Wireshark*, 2012). Na Figura 46 pode-se visualizar o funcionamento do filtro do ICMP para verificação dos pacotes de solicitação que não obtiveram nenhuma resposta, o exemplo utilizado é o do cenário *Path Protection*. É possível ver outras informações, como a origem, o destino e o tamanho do pacote.

Figura 46 - Filtro ICMP no Wireshark



Fonte: Autor

A tabela 11 apresenta a perda de pacote durante a convergência da rota primária para a secundária em cada cenário. Foram enviados cerca de mil pacotes para o destino e foi monitorado tanto no *backbone* como na rede do cliente. Não existe um protocolo de roteamento equivalente ao MPLS ou à tecnologia TE, porém para melhor visualização do comportamento foi comparado com um protocolo de roteamento vetor distância (RIP), com protocolo híbrido (EIGRP) e o com o MPLS, que utiliza protocolo *link-state* (OSPF), porém sem os túneis.

Tabela 11 - Resultados

Packet Loss	RIP	EIGRP	MPLS	MPLS-TE
Path Protection	88	7	4	2
Link Protection	97	8	5	0
Node Protection	86	7	5	0
Congested Link	-	-	-	0

Fonte: Autor

Através da tabela 11 é possível confirmar que o MPLS-TE obteve melhores resultados em todos os cenários, com menor perda de pacote durante a falha e com melhor tempo de convergência.

Em todos os cenários utilizou-se a mesma topologia, entretanto, a ferramenta utilizada pelo *Link Protection* e *Node Protection*, o FRR, é do MPLS-TE, por isso não foi utilizada pelos outros protocolos. Sendo assim, a proteção dos demais protocolos foi ponto-a-ponto. Também não foi possível testar o comportamento da rede dos demais protocolos durante um possível congestionamento do link, devido à falta de compatibilidade com a tecnologia RSVP.

Não houve diferença no resultado entre os pacotes TCP e ICMP na rede do cliente, nos dois protocolos usados a perda de pacote foi a mesma encontrada no *backbone*. Dessa maneira, nos cenários de proteção de link, proteção de nó e de link congestionado do MPLS-TE, o cliente não sentiu indisponibilidade no link. Já na proteção de link, tanto no enlace do provedor quanto do cliente houve perda de dois pacotes em todos os testes.

Inicialmente foi planejado comparar a latência dos protocolos em cada cenário, mas devido à grande variação em todos os cenários, optou-se por mostrar apenas os resultados referentes à perda de pacote.

5 CONCLUSÃO

A tecnologia MPLS é uma tecnologia que resolve com sucesso os problemas comuns enfrentados pelas redes atuais. Este trabalho apresentou uma proposta de como aplicar o MPLS-TE em um provedor de serviços visando honrar o SLA entre o cliente e o fornecedor. Com o intuito de reproduzir uma rede real, foi realizada a simulação de uma infraestrutura com *hosts* situados em localidades distintas, fornecendo *link* à clientes interligados por meio de VPN.

Os túneis da engenharia de tráfego do MPLS eram estabelecidos de acordo com: destino, largura de banda e nível de prioridade. Os fluxos de dados eram transmitidos pela rede através dos túneis da engenharia de tráfego, com o objetivo de evitar o congestionamento de certos enlaces e subutilização em outros. Nos ambientes simulados os roteadores estabeleceram túneis seguindo rotas dinâmicas e pré-configuradas. Nas rotas dinâmicas o melhor caminho era determinado pelo menor custo até o destino e pela reserva de banda. As rotas explícitas foram determinadas estrategicamente para mostrar algumas funcionalidades como tempo de recuperação e balanceamento de carga.

A fim de apresentar as vantagens da tecnologia TE do MPLS, mostrou-se uma das características mais importantes que deve ser seguida para manter a integridade do serviço: a capacidade de manter o tráfego em execução após falha do nó ou do link. Para isso, foi implementada a tecnologia FRR (*Fast Reroute*), que realiza a proteção local de enlaces e roteadores, na qual mostrou-se capaz de recuperar a conectividade na rede em milissegundos.

Também foi implementada a proteção ponto-a-ponto, mostrando ser mais eficiente em relação a outros protocolos de roteamento. Outra aplicação do MPLS-TE importante para um provedor de serviços de internet, é a manipulação do tráfego no *backbone*. Para isso, o trabalho mostrou o comportamento do túnel em um cenário de congestionamento de link, onde o túnel conseguia calcular rapidamente a melhor rota usando o OSPF de acordo com as restrições de largura de banda impostas.

Sendo assim, os objetivos específicos do trabalho foram alcançados, utilizando um simulador conseguiu-se implementar a tecnologia MPLS-TE com sucesso. Foram testados quatro cenários recorrentes em provedores de acesso à internet, mostrando o comportamento da rede MPLS-TE em cada ambiente e seus resultados. O protocolo forneceu os requisitos desejados de diminuir a vulnerabilidade de falha e facilitou o processo de implantação de VPNs, obtendo melhor uso dos recursos da rede e consequentemente clientes mais satisfeitos.

5.1 Trabalhos futuros

Para trabalhos futuros sugere-se:

- Aplicar os mecanismos apresentados neste trabalho em um provedor de serviços real;
- Atestar a eficiência da utilização do *Fast Reroute*, em um provedor de serviços real, a fim de comparar com os resultados dos ambientes simulados.

REFERÊNCIAS

ADEYINKA A., Adewale et al. **A Comparative Simulation Study of IP, MPLS, MPLS-TE for Latency and Packet Loss Reduction over a WAN**. International Journal of Networks and Communications, 2016.

AHMED, Mohammed Elfatih Eltyeb; IDRIS, Dr. Hala Eldaw. **Implement MPLS Traffic Engineering over Network System**. International Journal of Science and Research (IJSR), Sudan, 2013.

ANDERSSON, L; MINEI, I; THOMAS, B. **LDP Specification**. 2007.

BRADEN, R et al**. Resource ReSerVation Protocol (RSVP)**. 1997.

CISCO SYSTEMS, INC.. **Cisco 7200 Series Routers**. Cisco. 2012. Disponível em: https://www.cisco.com/c/en/us/products/routers/7200-series-routers/index.html. Acesso em: 10 Set. 2019.

CISCO SYSTEMS, INC.. **BGP Case Studies**. Cisco. 2008. Disponível em: https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html. Acesso em: 16 Nov. 2019.

CISCO SYSTEMS, INC.. **Cisco Gigabit Ethernet Port Adapter**. 2012. Disponível em: https://www.cisco.com/c/en/us/products/interfaces-modules/gigabit-ethernet-port-adapter/index.html. Acesso em: 10 Set. 2019.

CISCO SYSTEMS, INC.. **MPLS Traffic Engineering: Path, Link, and Node Protection: Configuration Guide, Cisco IOS Release 15S**. San Jose: Cisco Systems, Inc., 2013.

DA COSTA, Giovani Hoff . **Métricas para Avaliação de Desempenho em Redes QoS sobre IP**. Porto Alegre, 2008. Tese - Universidade Federal do Rio Grande do Sul.

DAVIE, Bruce; FARREL, Adrian. **MPLS: next steps**. 1. ed. Morgan Kaufmann, 2008.

GHEIN, Luc De. **MPLS Fundamentals**. Indianapolis: Cisco Press, 2007.

GILADI, Ran. **Network processors: architecture, programming, and implementation**. Morgan Kaufmann, 2008.

GNS3. **Graphical Network Simulator: GNS3**. GNS3. 2007. Disponível em: https://www.gns3.com/. Acesso em: 10 Set. 2019.

HAVRILA, Peter**. Configuring MPLS L3 VPN on IOS XR**. NETWORKGEEKSTUFF. 2013. Disponível em: https://networkgeekstuff.com/networking/configuring-mpls-l3-vpn-on-ios-xr/. Acesso em: 17 Nov. 2019.

HUAWEI TECHNOLOGIES CO., LTD.. **Configuration Guide - MPLS: CloudEngine 8800, 7800, 6800, and 5800 Series Switches**. Shenzhen: Huawei Technologies Co., Ltd., 2019.

LEMOS, Flávio. **Metodologia de Organizações Virtuais Aplicada ao Desenvolvimento do Produto em Empresas de Grande Porte**. São Paulo, 2007. Tese (Engenharia Automotiva) - Escola Politécnica da Universidade de São Paulo.

MANAYYA, KB**. Constrained Shortest Path First**. 2010.

MINEI, Ina; LUCEK, Julian. **MPLS-Enabled Applications: Emerging Developments and New Technologies**. Chichester: John Wiley & Sons, 2005.

OLIVEIRA, José Mario; LINS, Rafael Dueire; MENDONÇA, Roberno. **Redes MPLS: Fundamentos e Aplicações**. Rio de Janeiro: Brasport, 2012.

OSBORNE, Eric; SIMHA, Ajay**. Traffic Engineering with MPLS**. Indianapolis: Cisco Press, 2002.

PRESCOTT, Roberta. **Pouco adotado por ISPs, protocolo MPLS beneficia provedores de Internet**. 2014. Disponível em: http://www.abranet.org.br/Noticias/Pouco-adotado-por-ISPs,-protocolo-MPLS-beneficia-provedores-de-Internet-388.html?UserActiveTemplate=site#.Xeg6_ehKiMo. Acesso em: 4 Dez. 2019.

ROSEN, E; VISWANATHAN, A; CALLON, R. **Multiprotocol Label Switching Architecture**. 2001.

SANTOS, Renato Cesconetto. **Um estudo do Uso da Tecnologia MPLS em Backbones no Brasil**. Florianópolis, 2003. Dissertação (Ciências da Computação) - Universidade Federal de Santa Catarina.

SCHARF, Ana Luiza. **Implantação de engenharia de tráfego com MPLS-TE em rede WAN**. São José, 2017. Trabalho de Conclusão de Curso (Engenharia de Telecomunicações) - Instituto Federal de Santa Catarina.

WILFRIED. **MPLS: all you need to know about**. 2014. Disponível em: http://mysc.altervista.org/mpls/. Acesso em: 16 Nov. 2019.

APÊNDICE A – CONFIGURAÇÃO DOS ROTEADORES

Configuração do roteador São Luís:

```
hostname SaoLuis
ip vrf VPN_B
 rd 65500:2
 route-target export 65500:2
 route-target import 65500:2
ip cef
mpls traffic-eng tunnels

interface Loopback0
 ip address 10.100.1.1 255.255.255.255
interface Tunnel4
 ip unnumbered Loopback0
 tunnel destination 10.100.8.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 0 0
 tunnel mpls traffic-eng bandwidth 60000
 tunnel mpls traffic-eng path-option 1 dynamic
interface GigabitEthernet0/0
 ip address 10.200.0.5 255.255.255.252
 mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello
interface GigabitEthernet1/0
 ip address 10.200.0.1 255.255.255.252
 mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello
interface GigabitEthernet2/0
 ip vrf forwarding VPN_B
 ip address 172.16.1.1 255.255.255.252

router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
network 10.100.0.0 0.0.255.255 area 0
 network 10.200.0.0 0.0.255.255 area 0

router bgp 65500
 bgp log-neighbor-changes
 neighbor 10.100.8.1 remote-as 65500
 neighbor 10.100.8.1 update-source Loopback0
 address-family ipv4
  redistribute static
  neighbor 10.100.8.1 activate
  neighbor 10.100.8.1 next-hop-self
  auto-summary
  no synchronization
 exit-address-family
 address-family vpnv4
  neighbor 10.100.8.1 activate
  neighbor 10.100.8.1 send-community extended
```

```
  neighbor 10.100.8.1 next-hop-self
 exit-address-family

 address-family ipv4 vrf VPN_B
  redistribute connected
  redistribute static
  no synchronization
 exit-address-family

ip route vrf VPN_B 192.168.1.0 255.255.255.0 172.16.1.2
ip rsvp signalling hello
end
```

Configuração do roteador Rosário:

```
hostname Rosario
ip cef
mpls traffic-eng tunnels

interface Loopback0
 ip address 10.100.3.1 255.255.255.255
interface Tunnel33
 no ip address
tunnel destination 10.100.6.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 0 0
 tunnel mpls traffic-eng bandwidth 40000
 tunnel mpls traffic-eng path-option 1 dynamic
interface GigabitEthernet0/0
 ip address 10.200.0.6 255.255.255.252
mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello
interface GigabitEthernet1/0
 ip address 10.200.0.9 255.255.255.252
 mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello
interface GigabitEthernet2/0
 ip address 10.200.0.18 255.255.255.252
 mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello

router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
network 10.100.0.0 0.0.255.255 area 0
 network 10.200.0.0 0.0.255.255 area 0

ip rsvp signalling hello
end
```

Configuração do roteador Arari:

```
hostname Arari
ip cef
mpls traffic-eng tunnels

interface Loopback0
 ip address 10.100.2.1 255.255.255.255
interface Tunnel22
 ip unnumbered Loopback0
 tunnel destination 10.100.5.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 0 0
 tunnel mpls traffic-eng bandwidth 40000
 tunnel mpls traffic-eng path-option 1 explicit name tunnel-primary
interface GigabitEthernet0/0
 ip address 10.200.0.2 255.255.255.252
 mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello
interface GigabitEthernet1/0
 ip address 10.200.0.33 255.255.255.252
mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hell
interface GigabitEthernet2/0
 ip address 10.200.0.30 255.255.255.252
 mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello

router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 network 10.100.0.0 0.0.255.255 area 0
 network 10.200.0.0 0.0.255.255 area 0

ip rsvp signalling hello

ip explicit-path name tunnel-primary enable
 next-address 10.200.0.34
 next-address 10.100.5.1
end
```

Configuração do roteador Santa Inês:

```
hostname SantaInes
ip vrf VPN_A
 rd 65500:1
 route-target export 65500:1
 route-target import 65500:1
ip cef
mpls traffic-eng tunnels

interface Loopback0
 ip address 10.100.4.1 255.255.255.255
```

```
interface Tunnel3
 ip unnumbered Loopback0
 tunnel destination 10.100.7.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 0 0
 tunnel mpls traffic-eng bandwidth 30000
 tunnel mpls traffic-eng path-option 1 explicit name primary
 tunnel mpls traffic-eng fast-reroute node-protect
interface GigabitEthernet0/0
 ip address 10.200.0.29 255.255.255.252
mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
interface GigabitEthernet1/0
 ip address 10.200.0.26 255.255.255.252
 mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello
interface GigabitEthernet2/0
 ip vrf forwarding VPN_A
 ip address 172.16.1.1 255.255.255.252
 negotiation auto

router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
network 10.100.0.0 0.0.255.255 area 0
 network 10.200.0.0 0.0.255.255 area 0

router bgp 65500
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.100.7.1 remote-as 65500
 neighbor 10.100.7.1 update-source Loopback0
 neighbor 10.100.7.1 next-hop-self
 no auto-summary
 address-family vpnv4
  neighbor 10.100.7.1 activate
  neighbor 10.100.7.1 send-community both
 exit-address-family

 address-family ipv4 vrf VPN_A
  redistribute connected
  redistribute static
  no synchronization
 exit-address-family

ip route vrf VPN_A 192.168.1.0 255.255.255.0 172.16.1.2

ip rsvp signalling hello

ip explicit-path name primary enable
 next-address 10.200.0.25
 next-address 10.200.0.21
 next-address 10.200.0.13
 next-address 10.100.7.1
end
```

Configuração do roteador Barreirinhas:

```
hostname Barreirinhas
ip vrf VPN_A
 rd 65500:1
 route-target export 65500:1
 route-target import 65500:1
ip cef
mpls traffic-eng tunnels

interface Loopback0
 ip address 10.100.7.1 255.255.255.255
interface Tunnel2
 ip unnumbered Loopback0
 tunnel destination 10.100.4.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 0 0
 tunnel mpls traffic-eng bandwidth 30000
 tunnel mpls traffic-eng path-option 1 explicit name primary
 tunnel mpls traffic-eng fast-reroute
interface GigabitEthernet0/0
 ip address 10.200.0.10 255.255.255.252
mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello
interface GigabitEthernet1/0
 ip address 10.200.0.13 255.255.255.252
 mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello
interface GigabitEthernet2/0
 ip vrf forwarding VPN_A
 ip address 172.16.2.1 255.255.255.252

router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 network 10.100.0.0 0.0.255.255 area 0
 network 10.200.0.0 0.0.255.255 area 0

router bgp 65500
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.100.4.1 remote-as 65500
 neighbor 10.100.4.1 update-source Loopback0
 neighbor 10.100.4.1 next-hop-self
 no auto-summary

 address-family vpnv4
  neighbor 10.100.4.1 activate
  neighbor 10.100.4.1 send-community both
 exit-address-family

 address-family ipv4 vrf VPN_A
  redistribute connected
  redistribute static
  no synchronization
```

```
 exit-address-family

ip route vrf VPN_A 192.168.2.0 255.255.255.0 172.16.2.2

ip rsvp signalling hello

ip explicit-path name primary enable
 next-address 10.200.0.14
 next-address 10.200.0.22
 next-address 10.200.0.26
 next-address 10.100.4.1
end
```

Configuração do roteador Bacabal:

```
hostname Bacabal
ip cef
mpls traffic-eng tunnels

interface Loopback0
 ip address 10.100.5.1 255.255.255.255
interface Tunnel13
 ip unnumbered Loopback0
 tunnel destination 10.100.7.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 0 0
 tunnel mpls traffic-eng bandwidth 30000
 tunnel mpls traffic-eng path-option 1 explicit name primary
interface GigabitEthernet0/0
 ip address 10.200.0.34 255.255.255.252
mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello
interface GigabitEthernet1/0
 ip address 10.200.0.25 255.255.255.252
 mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello
interface GigabitEthernet2/0
 ip address 10.200.0.22 255.255.255.252
 mpls traffic-eng tunnels
 mpls traffic-eng backup-path Tunnel13
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello
interface GigabitEthernet3/0
 ip address 10.200.0.42 255.255.255.252
mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello

router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
network 10.100.0.0 0.0.255.255 area 0
 network 10.200.0.0 0.0.255.255 area 0
```

```
ip rsvp signalling hello

ip explicit-path name primary enable
 next-address 10.200.0.33
 next-address 10.200.0.1
 next-address 10.200.0.6
 next-address 10.200.0.10
 next-address 10.100.7.1
end
```

Configuração do roteador Chapadinha:

```
hostname Chapadinha
ip cef
mpls traffic-eng tunnels

interface Loopback0
 ip address 10.100.6.1 255.255.255.255
interface Tunnel12
 ip unnumbered Loopback0
 tunnel destination 10.100.5.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng backup-bw 30000
 tunnel mpls traffic-eng priority 0 0
 tunnel mpls traffic-eng bandwidth 30000
 tunnel mpls traffic-eng path-option 1 explicit name backup1
interface GigabitEthernet0/0
 ip address 10.200.0.17 255.255.255.252
 mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello
interface GigabitEthernet1/0
 ip address 10.200.0.14 255.255.255.252
 mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello
interface GigabitEthernet2/0
 ip address 10.200.0.37 255.255.255.252
mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello
interface GigabitEthernet3/0
 ip address 10.200.0.21 255.255.255.252
 mpls traffic-eng tunnels
 mpls traffic-eng backup-path Tunnel12
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello

router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
network 10.100.0.0 0.0.255.255 area 0
 network 10.200.0.0 0.0.255.255 area 0
```

```
ip rsvp signalling hello

ip explicit-path name backup1 enable
 next-address 10.200.0.38
 next-address 10.200.0.42
end
```

Configuração do roteador Caxias:

```
hostname Caxias
ip vrf VPN_B
 rd 65500:2
 route-target export 65500:2
 route-target import 65500:2
ip cef
mpls traffic-eng tunnels

interface Loopback0
 ip address 10.100.8.1 255.255.255.255
interface Tunnel1
 ip unnumbered Loopback0
 tunnel destination 10.100.1.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 0 0
 tunnel mpls traffic-eng bandwidth 20000
 tunnel mpls traffic-eng path-option 1 explicit name primary
 tunnel mpls traffic-eng path-option protect 1 explicit name backup
interface GigabitEthernet0/0
 ip address 10.200.0.38 255.255.255.252
 mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello
interface GigabitEthernet1/0
 ip address 10.200.0.41 255.255.255.252
 mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 100000
 ip rsvp signalling hello
interface GigabitEthernet2/0
 ip vrf forwarding VPN_B
 ip address 172.16.2.1 255.255.255.252

router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 log-adjacency-changes
 network 10.100.0.0 0.0.255.255 area 0
 network 10.200.0.0 0.0.255.255 area 0

router bgp 65500
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.100.1.1 remote-as 65500
 neighbor 10.100.1.1 update-source Loopback0
 neighbor 10.100.1.1 next-hop-self
 no auto-summary
 address-family vpnv4
  neighbor 10.100.1.1 activate
```

```
  neighbor 10.100.1.1 send-community both
 exit-address-family
 address-family ipv4 vrf VPN_B
  redistribute connected
  redistribute static
  no synchronization
 exit-address-family

ip route vrf VPN_B 192.168.2.0 255.255.255.0 172.16.2.2
ip rsvp signalling hello

ip explicit-path name primary enable
 next-address 10.200.0.42
 next-address 10.200.0.33
 next-address 10.200.0.1
 next-address 10.100.1.1

ip explicit-path name backup enable
 next-address 10.200.0.37
 next-address 10.200.0.18
 next-address 10.200.0.5
 next-address 10.100.1.1
end
```

Configuração do roteador CE-VRF_A

```
hostname CE-VRF_A
ip dhcp pool host1
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1 255.255.255.0
interface GigabitEthernet0/0
 ip address 172.16.1.2 255.255.255.252
interface GigabitEthernet1/0
 ip address 192.168.1.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 172.16.1.1
end
```

Configuração do roteador CE-VRF_A1

```
hostname CE-VRF_A1
ip dhcp pool host1
   network 192.168.2.0 255.255.255.0
   default-router 192.168.2.1 255.255.255.0
interface GigabitEthernet0/0
 ip address 172.16.2.2 255.255.255.252
interface GigabitEthernet1/0
 ip address 192.168.2.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 172.16.2.1
end
```

Configuração do roteador CE-VRF_B

```
hostname CE-VRF_B
ip dhcp pool host1
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1 255.255.255.0
interface GigabitEthernet0/0
 ip address 172.16.1.2 255.255.255.252
interface GigabitEthernet1/0
```

```
 ip address 192.168.1.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 172.16.1.1
end
```

Configuração do roteador CE-VRF_B1

```
hostname CE-VRF_B1
ip dhcp pool host1
   network 192.168.2.0 255.255.255.0
   default-router 192.168.2.1 255.255.255.0
interface GigabitEthernet0/0
 ip address 172.16.2.2 255.255.255.252
interface GigabitEthernet1/0
 ip address 192.168.2.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 172.16.2.1
end
```