UNIVERSIDADE FEDERAL DO MARANHÃO

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

CURSO DE CIÊNCIA DA COMPUTAÇÃO

IVAN MELO AROUCHA JUNIOR

APLICAÇÃO DE REDES MPLS EM UM CONTEXTO DE ENGENHARIA DE TRÁFEGO.

SÃO LUIS

2014

IVAN MELO AROUCHA JUNIOR

APLICAÇÃO DE REDES MPLS EM UM CONTEXTO DE ENGENHARIA DE TRÁFEGO.

Monografia apresentada ao Curso de Ciência da Computação da Universidade Federal do Maranhão **como parte dos requisitos** para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Dr. Mário Antônio Meireles Teixeira

SÃO LUÍS

2014

Aroucha Junior, Ivan Melo

Aplicação de Redes MPLS em um contexto de engenharia de tráfego / Ivan Melo Araucha Junior. – São Luís, 2014.

100f.

Orientador: Prof. Dr. Mário Antônio Meireles Teixeira

Monografia (Graduação) – Universidade Federal do Maranhão, Curso de Ciência da Computação, 2014.

1. Engenharia de tráfego 2. Multiprotocol Label Switching (MPLS) 3. Traffic engineering (TE) 4. Qualidade de Serviços (QoS) I. Título

CDU

IVAN MELO AROUCHA JUNIOR

APLICAÇÃO DE REDES MPLS EM UM CONTEXTO DE ENGENHARIA DE TRÁFEGO.

Monografia apresentada ao Curso de Ciência da Computação da Universidade Federal do Maranhão, **como parte dos requisitos** para obtenção do grau de Bacharel em Ciência da Computação.

Aprovada em: 12 / 12 / 2014 .

BANCA EXAMINADORA

Prof Dr. Mário Antônio Meireles Teixeira (Orientador)
Doutor em Ciência da Computação
Universidade Federal do Maranhão

Profª Msc Maria Auxiliadora Freire
Mestre em Engenharia Civil
Pontífice Universidade Católica - RJ

Profº Dr. Samyr Beiche Vale
Doutor em Ciência da Computação
Universidade Federal do Maranhão

Aos meus pais,

Ivan Melo Aroucha e

Euzanir S. Aroucha

AGRADECIMENTOS

Agradeço primeiramente a Deus, meus pais que sempre me apoiaram nessa jornada acadêmica, aos meus professores pelos conhecimentos e experiência transmitida, ao meu orientador, que me ajudou bastante na conclusão deste trabalho, aos meus colegas de curso, de trabalho que na maioria das vezes me ajudaram e incentivaram a perseverar nos trabalhos e evolução do curso. Sem poder nomeá-los, pois são muitos, apenas deixo meu muito obrigado a todos que de alguma forma fizeram parte desta conquista. Meus sinceros agradecimentos a todos.

"*Tudo tem o seu tempo determinado,*

há tempo para todo o propósito debaixo do céu.

Há tempo de nascer, e tempo de morrer;

tempo de plantar e tempo de

colher o que plantou"

(Salomão Ec 3. 1-2)

RESUMO

Neste trabalho abordaremos o desenvolvimento das tecnologias de comunicação de dados em especial as redes MPLS, uma tecnologia emergente que conta com vantagens econômicas, operacionais, flexibilidade, robustez e segurança, características essas que vem tornando essa tecnologia uma das grandes apostas nesse segmento para o futuro. Para entendermos melhor sobre o MPLS desenvolveremos breves comentários sobre as redes mais comuns existentes, suas vantagens e desvantagens assim como o MPLS podem operar conjuntamente com elas possibilitando a interconexão de múltiplas plataformas e ainda conservando características desejáveis como a possibilidade de QoS e economia de processamento. Vamos nos concentrar na Engenharia de Tráfego que o MPLS proporciona e os protocolos empregados para isso.

Palavras-chave: Engenharia de Tráfego, *Multiprotocol Label Switching* (MPLS), *Resource Reservation Protocol* (RSVP), *Traffic Engineering* (TE), *Qualidade de Serviço* (QoS).

ABSTRACT

In this work we will approach the development of new communication technologies. In special, MPLS networks, an emerging technology that brings flexibility, reliability, strength and security besides huge economics and operational advantages. Those characteristics are raising this technology as one of the greatest investments for this segment's future. For us to understand better about MPLS, we will develop brief comments about the most common existing networks, their advantages and disadvantages as well as their interoperability with MPLS that makes possible the interconnection of multiple platforms and conservation of desired characteristics like the possibility to maintain QoS and CPU economy. We will focus on the Traffic Engineering that MPLS provides and the protocols deployed for that.

Keywords: Traffic Engineering (TE), *Multiprotocol Label Switching* (MPLS), *Resource Reservation Protocol* (RSVP), Quality of Service (QoS), *Virtual Private Network (VPN).*

LISTA DE FIGURAS

LISTA DE SIGLAS

ADSL	-Asymmetric Digital Subscribes Line
AS	*-Autonomous Sytem*
ATM	*-Asynchronous Transfer Mode*
ASON	*-Application-Specific Integrated Circuit*
BGP	*-Border Gateway Protocol*
CE	*-Customer Edge Devices*
CoS	*-Class of Service*
CR-LDP	*-Constrained-based Label Distribution Protocol*
ER	*-Explicit Route*
EXP	*-Experimental*
FEC	*-Forwarding Equivalence Class*
FF	*-Fixed Filter*
FRR	*-Fast Reroute*
FTP	*-File Transfer Protocol*
FIB	*-Forwarding Information Base*
HE	*-Head End*
IETF	*-Internet Engineering Task Force*
IGP	*-Interior Gateway Protocol*
IP	*-Internet Protocol*
IPv4	*-Internet Protocol version 4*
IPv6	*-Internet Protocol version 6*
ISP	*-Internet Service Provider*
LAN	*-Local Area Network*
LDP	*-Label Distribution Protocol*
LER	*-Label Edge Router*
LIB	*-Label Information Base*
LSP	*-Label Switching Path*
LSR	*-Label Switching Router*
MPLS	*-Multi-Protocol Label Switching*
MTU	*-Maximum Transfer Unit*
NSAP	*-Natwork Service Access Point*
OSPF	*-Open Shortest Path First*

PE	*-Provider Edge Routers*
QoS	*-Quality of Service*
RFC	*-Request for Comments*
RRO	*-Record Route Object*
RSVP	*-Resource Reservation Protocol*
RSVP - TE	*-Resource Reservation Protocol with Tunneling Extensions*
SPF	*-Shortest Path First*
TCP	*-Transmission Control Protocol*
TLV	*-Type-Lengh-Value*
TCP/IP	*-Transmission Control Protocol/Internet Protocol*
TTL	*-Time-To-Live*
VPN	*-Virtual Private Network*
WAN	*-Wide Area Network*

SUMÁRIO

1. INTRODUÇÃO

1.1. Motivação

A competitividade no mundo globalizado gerou a necessidade das grandes corporações estarem interligadas, não só trocando informações, mas serviços através de uma rede de dados, podendo realizar controle remoto de equipamento, treinamento e avaliação dos funcionários, soluções em telefonia *VoIP (*Voz *on IP)* e até mesmo videoconferências, porém as soluções mais comuns ou são muito caras ou não atendem as demandas de qualidade que as corporações exigem, para suprir essa lacuna na comunicação de dados surgiu às redes MPLS.

O MPLS foi desenvolvido para resolver o problema de altos fluxos de redes ATM sobre IP. Hoje esta tecnologia é utilizada em muitas operadoras de telecomunicação para promover uma melhor prestação de serviços. Estes serviços podem ser utilizados em conexões nacionais e internacionais (PRETO, 2008).

Daí a necessidade crescente de gerenciar a qualidade e velocidade dos dados que trafegam em uma rede corporativa. O MPLS é o resultado de inúmeros esforços, que a indústria realizou no fim da década de 90, para melhorar a velocidade entre roteadores IP, adotando o conceito de rótulo de tamanho fixo (KUROSE e ROSS, 2006).

Há muito já existe diversas técnicas para garantir um nível mínimo de qualidade de serviço e maximização do tráfego na rede, muitas dessas custosas e inflexíveis.

Embora a grande motivação de uso da tecnologia seja melhorar a velocidade de encaminhamento dos pacotes na rede, apenas esse fator não seria um motivo suficiente para adoção da tecnologia, visto que a capacidade computacional existente nos equipamentos atuais responsáveis pelo roteamento é suficiente para um rápido atendimento ao tráfego. (OSBORNE e SIMHA, 2002).

O MPLS possibilita a melhoria do desempenho do encaminhamento dos pacotes, já que existe uma separação do plano de controle e o plano de dados. Existe um ganho na diminuição da latência, já que não há roteamento e sim uma comutação dos rótulos. (OLIVEIRA, LINS e MENDONÇA, 2012).

Um dos usos mais importantes do MPLS é facilitar a engenharia de tráfego nas redes IP de provedores de serviço de telecomunicação. A principal capacidade que o MPLS traz às redes com engenharia de tráfego é a possibilidade de configurar um circuito virtual *overlay* comutado para o modelo de roteamento da internet. (OLIVEIRA, LINS e MENDONÇA, 2012).

A economia, gerenciamento, segurança e flexibilidade vêm consagrando essas redes como uma boa solução tanto para redes com uma infraestrutura antiga e deficitária como para redes metropolitanas modernas e ágeis. (OSBORNE e SIMHA, 2002).

1.2. Objetivos

1.2.1 Geral

Este trabalho tem a proposta de utilizar os fundamentos da tecnologia das redes MPLS para fundamentar esta como uma ferramenta viável e flexível para um administrador de redes que utiliza engenharia de tráfego para maximizar recursos e minimizar erros nas redes que administra.

1.2.2 Específicos.

a) Discutir a tecnologia através da simulação de uma rede MPLS,

b) Analisar a tecnologia de encaminhamento de rótulos,

c) Aplicar e demonstrar os conhecimentos teóricos na simulação de MPLS

1.3. Metodologia

Coletar ampla literatura sobre MPLS, *site* de provedores da tecnologia, manual de equipamentos que implementam seus protocolos, além de pesquisar e descrever resumidamente as camadas utilizadas nesse trabalho, tecnologias similares a rede abordada, como redes ATM, *Frame Relay* e sistemas modernos de enlace de dados.

Este trabalho está assim organizado: o Capítulo 2, veremos os conceitos e funcionamento das redes MPLS e as tecnologias que as inspiraram. Já no Capítulo 3, temos a Engenharia de Tráfego, onde além dos conceitos, veremos como o MPLS-TE funciona e porque ele é uma

ferramenta flexível para engenharia de tráfego. No capítulo 4 veremos o Estudo de Caso, onde através de uma rede simulada faremos captura dos pacotes e executaremos alguns comandos para demonstrar o que vimos nos capítulos teóricos.

2. MPLS (*MultiProtocol Label Switching*)

Para se compreender a tecnologia MPLS é preciso que alguns conceitos fundamentais sejam discutidos. Este capítulo se propõe a discutir esses conceitos básicos, sem aprofundar muito em detalhes técnicos que não contribuem de forma prática para a compreensão do foco desta monografia, que é apresentar o MPLS como uma ferramenta versátil e útil na Engenharia de Tráfego.

2.1. Histórico

No final da década de 80 o que tínhamos em termos de redes de computadores era basicamente redes de camada 2, onde havia um grande domínio de *broadcast* e um único *gateway* de saída, isso além de acarretar grande fluxo de dados desnecessário demandava um grande esforço para tentar controlar o tráfego e aplicar algum nível de segurança. O que as operadoras fizeram para melhorar esse cenário foi, dividir a rede em subdomínios de *broadcast* e até mesmo criação de *links* diretos ou túneis, esse sim, já com tráfego controlado e baixo nível de tráfego desnecessário. Porém com o crescimento das redes os roteadores passaram a demandar uma carga de trabalho muito alta, além de terem que processar grandes tabelas de roteamento.

Em meados da década de 90 houve uma evolução na velocidade das redes de telecomunicação digital por meio elétrico, óptico e radio, nascia o paradigma cliente/servidor, além da migração da interface de texto para interfaces gráficas, avanços esses que aliados ao crescimento da capacidade computacional e a popularização dos computadores pessoais ajudaram a abrir espaço para redes de alta velocidade com serviços diferenciados, ou seja, redes

com tratamento especial para cada tipo de aplicação. Uma das redes que surgiram nessa época foi a ATM. (MINOLI, SCHINMIDT, 1996)

Ascynchronous Transfer Mode (ATM) são redes orientadas a conexão e operam na camada 2 do modelo OSI, seu propósito era de interligar redes internas das corporações e organizações que utilizavam aplicações de voz, vídeo ou dados, tudo isso sem está atrelado a uma topologia de rede específica. (MINOLI e SCHINMIDT, 1996). E a capacidade destas redes criarem Circuitos Virtuais ou caminhos virtuais, além de conceitos de Engenharia de tráfego inspiraram profundamente a criação das redes MPLS.

Outra rede desse período que contribuiu sobretudo para o formato dos rótulos MPLS foi as redes *Frame Relay,* que são redes que operam na camada 2 do modelo OSI, neste nível são implementadas características como a verificação de *frames* válidos, porém sem a solicitação de retransmissão em caso de erro, desta forma não há a redundância de verificação de *frames* feito no protocolo de aplicação, tornando a velocidade destas redes alta chegando até 1,984 Mbps, com o mínimo de atraso e bom aproveitamento da largura de banda. (KUROSE e ROSS, 2006)

2.2. Objetivos das Redes MPLS.

Essas redes surgiram para suprir a lacuna das redes da época, trazendo o melhor do mundo ATM, *Frame Relay*, mas com a interoperabilidade das redes IP modernas, onde essa tecnologia se destaca por substituir o tradicional roteamento IP por encaminhamento de rótulos.

São redes usadas em *backbones* embora a grande motivação de uso da tecnologia seja a melhora da velocidade de encaminhamento dos pacotes de rede, apenas este fator não seria suficiente para adoção da tecnologia, visto que a capacidade computacional existente nos equipamentos atuais responsáveis pelo roteamento é suficiente para um rápido atendimento ao tráfego. Os algoritmos de encaminhamento de pacotes com alta velocidade agora são implementados em hardware, usando ASICs (*Aplication Specific Integrated*), portanto a pesquisa de 20 bits não é significativamente mais rápida do que uma pesquisa IP de 32 bits (OSBONE e SIMHA, 2002).

Nessas redes como há a separação do plano de dados e de controle, isso possibilita um ganho de desempenho e manutenabilidade e isso nos leva a outro grande objetivo das redes MPLS, a Engenharia de Tráfego, que como vamos ver no capítulo seguinte é muito facilitada

por essa tecnologia.

Apenas para citar outros objetivos do MPLS, temos o AToN, um aplicativo que faz integração com as redes ATM, temos também a possibilidade da criação de VPNs, onde túneis transparentes são criados dentro da topologia MPLS interligando duas redes de forma rápida, segura e escalável. O *QoS* embora não seja o objetivo do MPLS pode ser facilitado tanto por espaços específicos no rótulo como tabelas de equivalência de serviço.

Entre as principais características do MPLS podemos destacar o desacoplamento do roteamento e encaminhamento; melhor integração com os mundos IP e ATM; redução dos custos com túneis baseado em VPN usando protocolo IP; escalabilidade; flexibilidade; garantia de níveis de serviço; e utilização de serviços tais como QoS, VPN e Engenharia de Tráfego. (OLIVEIRA, LINS, MENDONÇA, 2012).

2.3. Terminologias

Para estudar a tecnologia MPLS é necessário conhecer alguns termos definidos pela RFC (*Request for Comments*) 3031. Abaixo estão algumas terminologias (MORGAN e LOVERING, 2008).

1. *Upstream*: E o roteador que está mais perto da origem de um pacote, em relação a outro roteador.
2. *Downstream*: E o roteador que está mais longe da origem de um pacote, em relação a outro roteador.
3. *Cisco Express Forwarding* (CEF): Ou Encaminhamento expresso Cisco é o método de comutação mais recente utilizado no IOS da Cisco.
4. Vinculo de Rótulo: E uma associação de um FEC (prefixo) a um rótulo.
5. *Label Switch Router* (LSR): Ou Roteador de Comutação de Rótulos, é qualquer dispositivo que comuta pacotes com base nos rótulos MPLS.
6. *Label Edge Router* (LER): Roteador de Rótulo de Borda.
7. P/PE e C/CE: Roteadores P e PE são LSRs e LERs no contexto do MPLS-VPN.
8. *Label-Switched Path* (LSP): Caminho de comutação de rótulo é a rota que um pacote rotulado atravessa através de uma rede.
9. *Forwarding Information Base* (FIB): Base de informações de encaminhamento. *Label Information Base* (LIB): Base de informação de rótulos é a tabela onde são armazenados os vínculos de rótulos que um LSR recebe.
10. *Label Distribution Protocol* (LDP): Um dos muitos protocolos existentes para distribuir os vínculos de rótulos.

11. Resource Reservation Protocol (RSVP): Este é o protocolo que faz a reserva de recursos.

2.4. Roteamento IP vs MPLS

Por padrão, o protocolo IP possui como base para encaminhamento de pacotes a análise do endereço IP de destino existente no cabeçalho do pacote da camada de rede. "Este processo também é tradicionalmente chamado de *hop-by-hop packet forward*" (PEPELNJAK e GUICHARD, 2000).

Principalmente devido ao crescimento mundial da Internet (HARNEDY, 2002), a demanda de tráfego requerida pelos provedores desserviços (ISPs) aumentou bastante. Para suprir essa demanda era necessários roteadores de alto desempenho, pois, além de terem que lidar com o aumento de banda, também precisavam rotear cada vez mais nós.

O processo de roteamento é complexo e deve suportar muitos protocolos e tipos de interfaces, diferente dos *switches* (comutadores) que por serem mais simples, tem uma relação custo/desempenho melhor que a dos roteadores.

De acordo com Pepelnjak e Guichard (2000), os *switches* oferecem um desempenho muito superior na comutação de células ou seguimentos que os roteadores para encaminhamento de pacotes. Isso se deve ao fato de que o tipo das informações a serem analisadas pelos *switches* é mais simples, tornando o processo de encaminhamento dos seguimentos muito mais rápido, fato esse que levou a maior parte dos *backbones* IP a serem implementados utilizando uma rede ATM em seu núcleo e como vimos no capitulo 1 essas redes por trabalharem com encaminhamento de pacotes são mais ágeis e flexíveis que as tradicionais redes IP.

O MPLS é uma tecnologia aberta que foi apresentada incialmente como uma solução para melhorar o desempenho das redes IP na função de encaminhamento de pacotes IP, combinando o processo de roteamento camada 3 com comutação de camada 2 para realizar o encaminhamento de datagramas através de pequenos rótulos de tamanho fixo. Tais rótulos são o número utilizado no protocolo MPLS e, através destes, a decisão de qual interface encaminhar o datagrama é tomada (ROSEN et al, 2001).

Rosen et al, 2001, dia que a comutação de rótulos multiprotocolos alia a funcionalidade de roteamento da câmara de rede e a comutação por rótulos, além de oferecer vantagens significativas para as redes como a IP e ATM.

Outra grande vantagem que podemos destacar, diz respeito ao encaminhamento dos datagramas ao longo de um caminho. Em uma rede IP, todos os roteadores todos os roteadores da topologia precisam saber a melhor rota em sua tabela de roteamento para encaminhar o pacote ao seu destino. Já o protocolo MPLS usa o encaminhamento dos pacotes baseado em rótulos, sendo que os roteadores do núcleo da rede (P), não enxergam o endereço IP de destino do pacote, logo não há custo de roteamento no núcleo.

2.5. Cabeçalho MPLS

O cabeçalho MPLS é formado por quatro bytes e está localizado antes do cabeçalho IP. O rótulo do MPLS é formado por um campo de 20 bits. (ODOM; HEALY; METHA, 2008).

O item mais importante para o MPLS é o rótulo (De GHEIN, 2007), está no cerne da tecnologia e através dele que a maior parte das vantagens apresentadas até aqui se tornam possíveis.

Os rótulos contidos no MPLS tem a função de separar as operações de encaminhamento da camada de rede de destinos e informações contidas nos cabeçalhos dos pacotes (MORGAN e LOVERING, 2008).

Também de *label* ou *Shim Header* são partes integrante do MPLS. O rótulo permite o desacoplamento entre roteamento e encaminhamento, geralmente é encapsulado em um pequeno cabeçalho localizado entre a camada 2 e a camada 3, permitindo assim o suporte a vários outros protocolos e qualquer tecnologia da camada de ligação (VEIGA, 2009).

A RFC 3031 define o rótulo como “um identificador curto de tamanho físico e fisicamente contíguo, usado para identificar uma FEC, normalmente com significado local”

O quadro MPLS é utilizado para descrever que tipo de encapsulamento que será utilizado nas interfaces que estão sendo usadas para a comunicação dos roteadores (MORGAN e LOVERING, 2008). Se a interface de saída está habilitada com MPLS, o roteador deverá colocar o rótulo e encapsular de acordo com a estrutura da camada de enlace. O roteador

também especifica o tipo do protocolo de roteamento, conforme está configurado e encontra seus vizinhos.

MPLS pode operar em dois modos da camada de enlace: **Frame** e **Célula**. O modo frame é o termo que se usa quando um pacote é encaminhado com *label* inserido na frente do cabeçalho da camada 3 (O cabeçalho IP é um exemplo). Um pacote pode ter vários rótulos, transportados no que chamamos de pilha de rótulos, onde em cada salto da rede, apenas o mais externo é considerado.

O rótulo de 20 bits é codificado da seguinte forma: Rótulo (20 bits), EXP (3 bits), P (1 bit), TTL (8 bits), tudo isso quantifica um total de 32 bits chamado de entrada de pilha de *label* ou rótulo.

- EXP – Experimental, pode conter *flags* QoS, normalmente uma cópia direta dos bits do pacote IP, ou pode ser usado como bit de precedência quando há um enfileiramento de rótulos.
- P – Final de Pilha, É comum ter mais de um rótulo no pacote e o ultimo da pilha é marcado com 1, para indicar o fim daquela pilha.
- TTL – *Time To Live*, as vezes são uma cópia do TTL do cabeçalho TTL IP. Eles são decrementados a cada salto na rede a fim de evitar loops e assim não sobrecarrega a rede. Mas ele pode ser usado quando um operador de rede deseja esconder sua topologia de rede de *pings* vinda dos *tracerouters*.

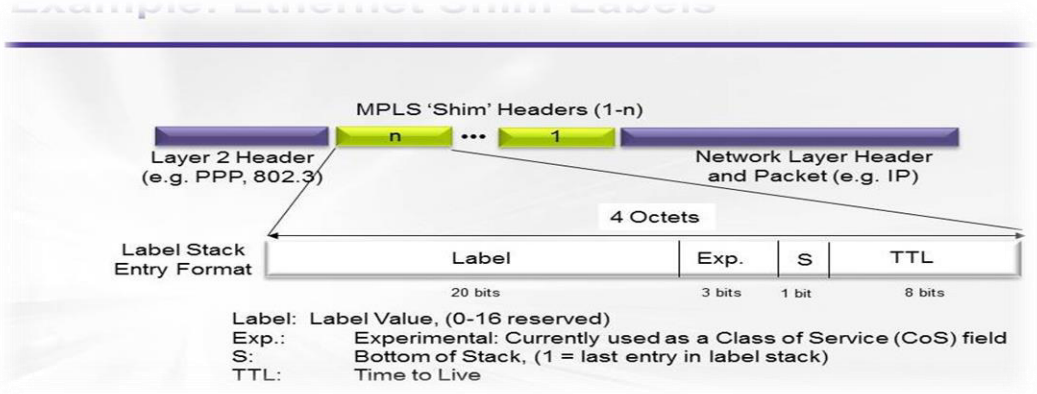


Figura 1: Detalhamento de um rótulo MPLS.
Fonte: *Exetreme Network, Mikael Holmberg EMEA*

A figura 1 ilustra o que acabamos de ver, o rótulo inserido em um pacote IP e o detalhamento de seus campos.

O modo célula é o termo usado quando se tem uma rede onde os LSRs ATM utilizam

MPLS no plano de controle para trocar informações VPI/VCI em vez de usar sinalização ATM. Por isso diz-se que no modo célula o rótulo está codificado nos campos de VPI/VCI de uma célula.

2.5.1. Anuncio dos Rótulos

Assim que os LSRs tiverem estabelecidos um relacionamento LDP com um vizinho, eles começam a anunciar rótulos um para o outro.

Um LSR envia mensagens de endereço para anunciar os endereços de interface aos quais ele está ligado. As mensagens de endereço não são mensagens de anuncio de rótulo LDP, porém as mensagens de endereço também são uma forma de anuncio, e por isso foram incluídas aqui.

A mensagem de endereço é a forma como a associação entre espaço de rótulo e um *salto* seguinte é feito. Sem ela, o LSR não sabe em que código LDP deve ouvir se quiser enviar um pacote a determinado *salto* adiante.

2.5.2. Empilhamento de rótulos

As pilhas de rótulos podem ser comparadas como o encapsulamento IP dentro do IP, existe dois cabeçalhos, mas apenas o primeiro é utilizado para tomar as decisões de roteamento (MORGAN e LOVERING, 2008).

No encaminhamento baseado em MPLS, depois que o LER de ingresso na borda da rede realiza a classificação, ele empilha um rótulo no pacote de dados que corresponde à FEC desse pacote. Esse processo é chamado “colocação de rótulo ou empilhamento”. (OSBORNE e SIMHA, 2002).

Os LSRs no núcleo da rede não são obrigados a reclassificar o pacote. Quando um roteador no núcleo recebe um pacote rotulado, ele primeiramente realiza uma pesquisa do rótulo sobre o rótulo que chega, depois encontra a interface de saída e o rótulo de saída para esse pacote, após isso troca o rótulo de entrada pelo rótulo de saída e o envia pela interface de saída encontrada anteriormente. Esse processo é chamado de “troca de rótulo”.

O modo como um LSR sabe que o LSR *downstream* espera é baseado nos vínculos de

rótulos que são trocados no plano de controle, usando um protocolo de distribuição de rótulos (LDP, RSVP, BGP e etc) antes do encaminhamento de pacote.

Quando um pacote chega ao final da rede, o rótulo mais externo do pacote é removido e o restante do pacote é encaminhado ao próximo salto. O ato de remover um rótulo é chamado de “retirada ou descarte de rótulo”.

Se os rótulos se tornarem obsoletos, eles serão descartados do cabeçalho. O processamento de rótulos é sempre baseado no rótulo superior. Cada um dos rótulos tem uma denominação, o inferior é o rótulo de nível 1, o segundo de nível 2, e assim sucessivamente. O pacote sem rótulo possui uma profundidade zero.

As três operações fundamentais com rótulos (empilhar, trocar e descartar) são tudo que o MPLS precisa para fazer o encaminhamento de pacotes numa rede.

Essas operações estão intimamente ligadas à economia de processamento que é normalmente feita nos encaminhamentos convencionais, deixando que o maior trabalho seja feito pelos roteadores de borda, deixando os do núcleo ou nuvem apenas com a tarefa de encaminhar os pacotes.

2.5.3. Distribuição de rótulos

O MPLS não adiciona *overhead* na comunicação adicional entre os roteadores. São usados recursos significativos para a propagação de prefixos de rotas e a manutenção da LIB e LFIB, juntamente com a tabela de adjacência

(MORGAN e LOVERING, 2008).

A distribuição de rótulos é realizada pelo LDP. O MPLS admite duas formas de propagar informações em sua arquitetura. Uma delas é utilizar as funcionalidades dos protocolos existentes e a outra é criar novos protocolos à tarefa de troca de rótulos. O LDP está implementado no plano de controle e os rótulos de troca estão armazenados na LIB.

A decisão de distribuir um rótulo especial a uma FEC é feita pelo LSR em cada salto ao longo do caminho. No tráfego MPLS, os rótulos são propagados nos dois sentidos. A distribuição de rótulos pode acontecer de duas maneiras:

- Atualizações não solicitadas

- Atualizações por demanda.

Assim como ocorre nas tabelas de roteamento, o LFIB também pode formar uma estrutura para saber qual é o roteador de próximo salto. Este detalhe é visto na figura 2, pode ser notado que cada roteador sabe qual é o próximo roteador que tem que enviar os pacotes.

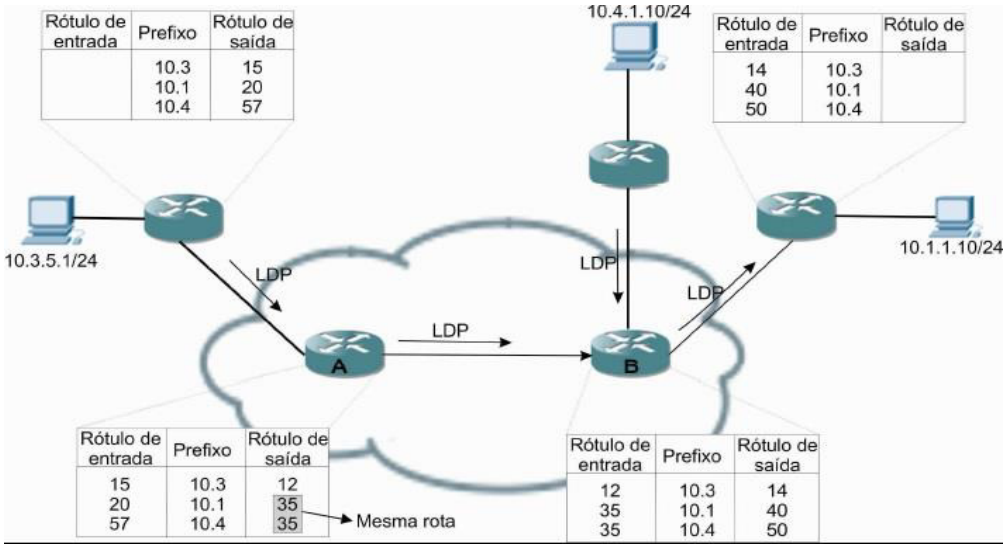


Figura 2: Troca de rótulos entre roteadores.

Fonte: CCNP ISCW, MORGAN e LOVERING, (2008)

Ainda pensando na distribuição de rótulos, quando utilizamos essas redes MPLS no modo Frame, LSRs ATM agem como roteadores no plano de controle, ou seja, eles necessariamente trocam informações de roteador por meio de protocolos IGP (*Interior Gateway Protocol*) ou protocolo de roteamento interno, como OSPF e precisam executar um protocolo de distribuição de rótulo, como TDP ou LDP.

2.6. Componentes da arquitetura MPLS

Já vimos anteriormente alguns componentes MPLS, agora vamos detalha-los e mostrar sua integração em uma rede.

A arquitetura subjacente da tecnologia MPLS foi separada em dois mecanismos tradicionais de roteamento (MORGAN e LOVERING, 2008).

- **Plano de Controle:** É onde ficam as informações de roteamento e outras informações de controle, como vínculos de rótulos que são trocados entre os LSRs. O MPLS se

baseia no plano de controle, isso significa que as trocas de informações de controle devem existir antes do encaminhamento do primeiro pacote. (OSBORNE e SIMHA, 2002)

- **Plano de Dados**: também conhecido como plano de encaminhamento e é ele quem direciona as informações com base nos endereços ou rótulos de destino.

O Plano de Controle trabalha com as questões envolvendo roteamento em geral. Incluindo os protocolos OSPF (*Open Shortest Path First*), EIRGP (*Enhanced Interior Gateway Routing Protocol*), IS-IS (*Intermediate System To Intermediate System*), BGP (*Border Gateway Protocol*), entre outros protocolos utilizados.

E no plano de controle onde há a classificação dos pacotes, por exemplo quando os pacotes IP destinados à mesma sub-rede chegam em um roteador de ingresso (LER), a classificação para todos esses pacotes é a mesma – ela é baseada na pesquisa da correspondência mais longa na FIB. (OSBORNE e SIMHA, 2002).

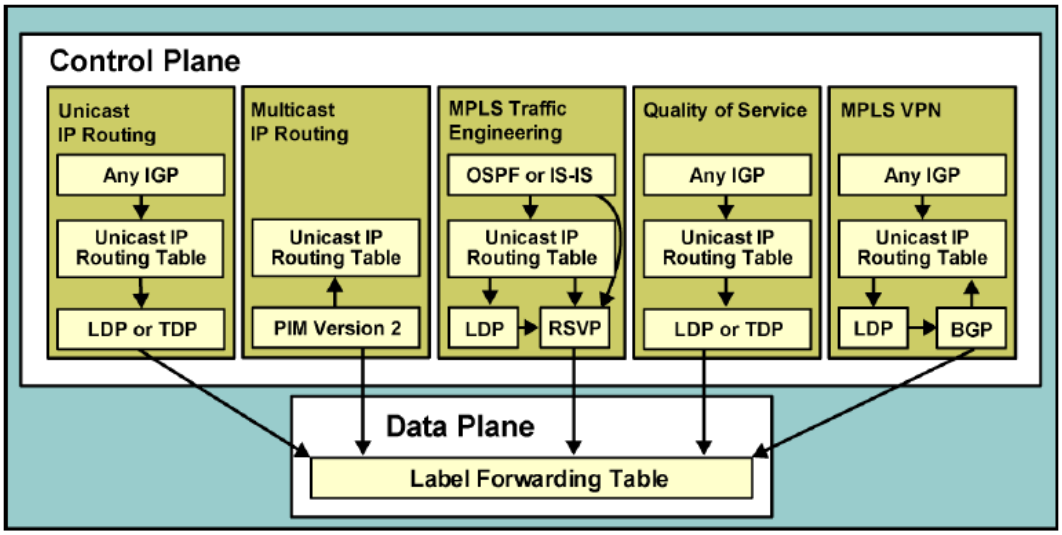


Figura 3: Interação entre os planos

Fonte: Curso MPLS no 20° SCI/RNP (2014)

Além dos protocolos de roteamento tradicionais, existem rótulos equivalentes baseados em protocolo de roteamento. O TDP (*Tag Distribution Protocol*) e o LDP (*Label Distribution Protocol*), este protocolo é proprietário da *Cisco System*. Outro protocolo presente na tecnologia é o RSVP (*ReSource reserVation Protocol*), utilizado no mecanismo de engenharia de tráfego do MPLS, este permite a reserva da largura de banda (MORGAN e LOVERING, 2008).

Para que qualquer pacote de dados passe por uma rede, primeiramente o mecanismo do plano de controle precisam está configurado.

Para uma rede IP isso se daria da seguinte forma:

- *Interior Gateway Protocol* (IGP): Normalmente, OSPF ou IS-IS nas redes de provedor de serviços. Também pode ser EIGRP, RIP ou apenas o roteamento estático.
- *Border Gatway Protocol* (BGP): Usado para anunciar rotas que são descobertas a partir dos vizinhos externos, em redes da vida real, um *Router Reflector* (RR) provavelmente seria utilizado. O ponto importante aqui é que todos dos roteadores precisam descobrir a rota a partir de um vizinho em comum.

Para uma rede MPLS os mecanismos do plano de controle funcionam assim:

- O IGP atua como se estivesse em uma rede apenas IP. Se a rede MPLS estivesse usando engenharia de tráfego, o IGP teria que ser um protocolo com estado de enlace, seja OSPF ou IS-IS.
- Protocolo de distribuição de rótulos: Os três principais protocolos de distribuição de rótulos em uma rede MPLS são: TDP, LDP e RSVP.

O RSVP é usado para a engenharia de tráfego, e não será considerado nesse exemplo. TDP e LDP são na verdade duas versões da mesma coisa, o TDP é mais antigo e o LDP é padronizado. Assim, considere que LDP é utilizado para distribuir rótulos.

Adentrando ainda mais nesse conceito de distribuição de rótulos, podemos dizer que é um vínculo de rótulos que faz a associação de um rótulo a um prefixo (rota). LDP trabalha em conjunto com o IGP para anunciar os vínculos de rótulo para todas as rotas não BGP aos seus vizinhos. Os vizinhos LDP são estabelecidos sobre os links ativados para LDP.

- BGP: É aqui que se encontra a principal diferença entre redes MPLS e as outras. Em vez de ter que colocar BGP em cada roteador, ele é necessário apenas na borda da rede. O BGP não se faz necessário no núcleo, pois é um LER de ingresso que precisa ter as rotas BGP completas, conhece o próximo salto para todas as rotas descobertas pelo BGP. Um rótulo é colocado no pacote correspondente ao próximo salto BGP e o pacote são entregues através da rede para esse próximo salto, usando apenas encaminhamento de rótulos. Assim sendo os problemas de escalada devido a grandes malhas iBGP são resolvidos usando refletores ou confederação de rotas.

Abaixo a figura 4 ilustra como esses protocolos interagem com o MPLS, nota-se que o BGP desconhece a topologia da rede MPLS, todo encaminhamento interno é feito pelo LDP.

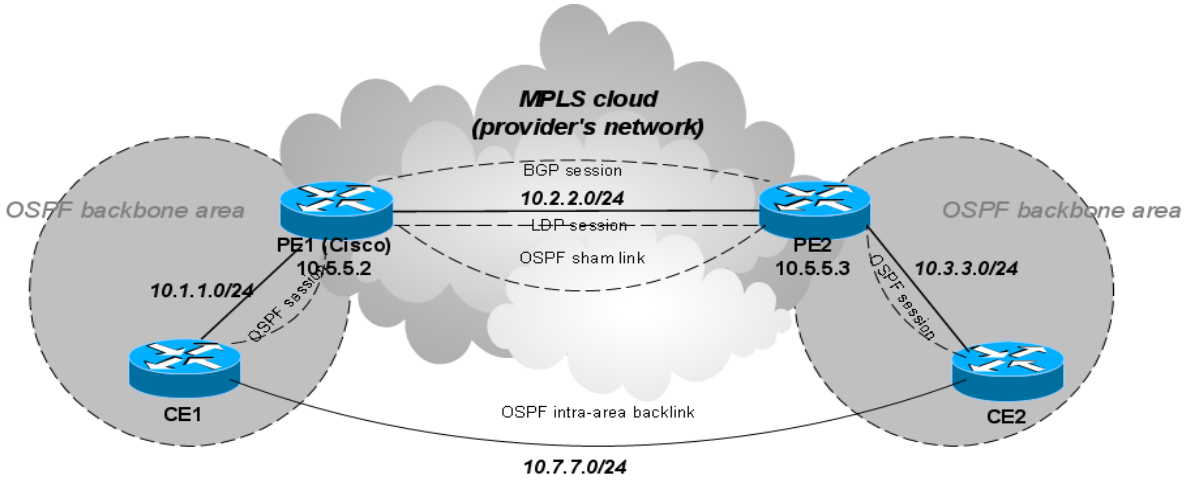


Figura 4: Integração do OSPF, GBP em uma nuvem MPLS.

Fonte: Manual Mikrotik: OSPF as PE-CE *routing protocol*

2.6.1. LDP (*Label Distribuition Protocol*)

Embora já muito mencionado até aqui o LDP sendo um dos principais protocolos da tecnologia MPLS deve ser explicando melhor no que diz respeito ao seu funcionamento, pois é um importante mecanismo usado por administradores de redes na engenharia de tráfego, onde temos que o LDP é descrito e padronizado pela RFC 3036, "*LDP Specification*", o LDP troca os rótulos para rotas IGP e estáticas. A implementação do Cisco para engenharia de tráfego MPLS não é baseada em CR-LDP, que é uma extensão do protocolo LDP para roteamento de base restrita. Porém, conhecer o LDP é importante mesmo em uma rede MPLS-TE, pois na prática as redes preparadas para MPLS utilizam uma mistura de LDP e RSVP em lugares diferentes.

As principais funções do LDP são a descoberta de vizinhos, estabelecimento e manutenção de sessão, anúncio de rótulos e notificação.

Falando particularmente de cada um deles temos a função de descoberta de vinhos, conceito usual para a maioria dos protocolos deste tipo. O LDP usa as portas UDP/TCP 646 para a descoberta de vizinhos e possui dois tipos diferentes de vizinhos:

- Vizinhos conectados diretamente: São aqueles que possuem uma conexão da camada 2. Assim, os roteadores que estão conectados por um enlace de camada 2 são considerados conectados diretamente para o LDP. A semelhança básica por tais conexões é o fato de um vizinho está sempre a um salto de distância do outro.

- Vizinhos conectados indiretamente: Esses vizinhos não possuem conexão de camada 2 entre eles. Mais o interessante é que esses vizinhos estão a vários saltos de distância. Os roteadores que estão conectados um ao outro por túneis de engenharia de tráfego MPLS e que possuem LDP ativados neles são considerados conectados indiretamente. Tal sessão LDP é chamada sessão LDP direcionada.

A diferença entre vizinhos conectados diretamente e indiretamente está no modo como eles descobrem um ao outro. LSRs descobrem vizinhos conectados diretamente enviando mensagens LDP *hello* encapsuladas em UDP para o endereço de *multcast*. Esses pacotes são conhecidos como mensagens *hello*. Veremos em detalhes essas mensagens e a estrutura do pacote LDP na simulação do capítulo 4.

Vizinhos conectados indiretamente não podem ser alcançados por um pacote UDP de *multcast*. Assim as mesmas mensagens *hello* são enviadas como *unicast* (também para a porta UDP). Isso exige que um LSR saiba antes da hora quem ele deseja ter como vizinho conectado indiretamente, o que pode ser feito manualmente.

2.7. Topologia e funcionamento

Conforme já mencionado anteriormente, o MPLS analisa os rótulos, ao invés dos protocolos de camada de rede. Desta maneira o rótulo de um pacote de saída é verificado e comparado com um rótulo do banco de dados. Com a informação encontrada, um novo rótulo é anexado ao pacote e transmitido para a interface de destino (MORGAN e LOVERING, 2008).

Em sessões anteriores vimos muito elementos, siglas, protocolos e tipos diferentes de roteadores, mas como exatamente esses elementos interagem para encaminhar os pacotes através da rede?

A topologia de uma rede MPLS é formada por um conjunto de roteadores de camada três, que são roteadores que podem suportar protocolos de distribuição de rótulos para comutação. Onde estes roteadores se encontram na estrutura da rede e a função que eles desempenham determina o seu tipo (borda ou núcleo). (OSBORNE e SIMHA, 2002).

Os principais elementos de uma rede MPLS são: *Label Switching Routers* (LSR), *Label Switch Path* (LSP), *Forward Equivalence Label* (FEC), *Label Edge Routers* (LER), *Labels* (Rótulos) e *Label Information Base* (LIB). A figura 5 ilustra a distribuição básica de alguns

desses elementos ao longo de uma rede.

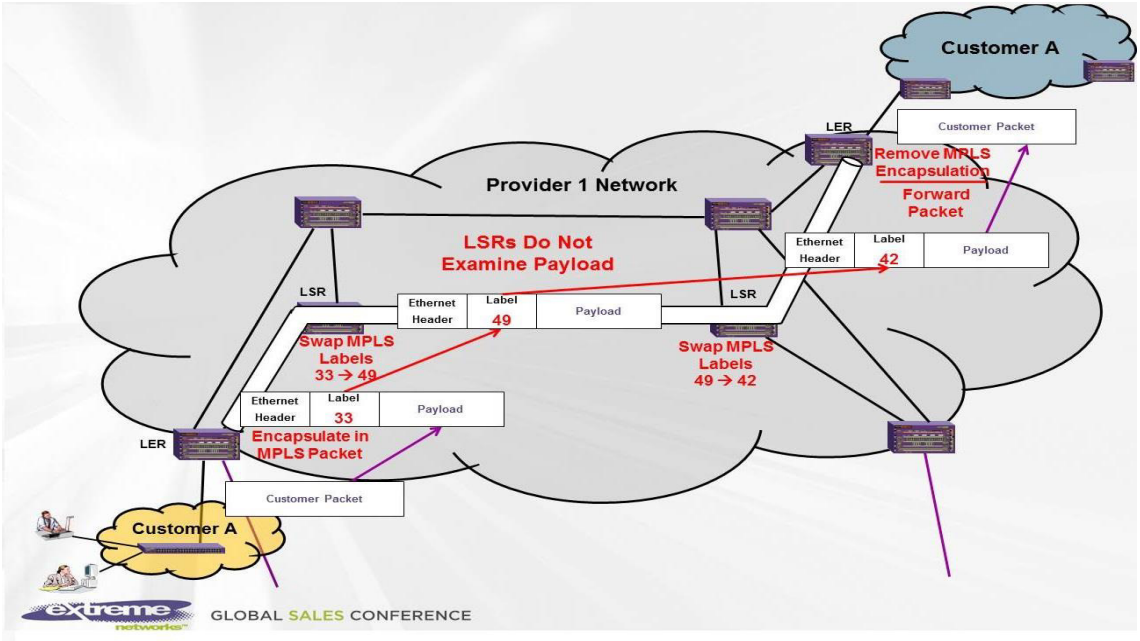


Figura 5: Esquema de troca de rótulos em uma rede MPLS.
Fonte: MPLS Overview - Extreme Networks, Tony Coombs.

Como podemos observar os roteadores que se encontram dentro da rede MPLS ou no núcleo são chamados de LSRs (*Label Switching Router*) e são eles os responsáveis pelo encaminhamento de datagrama de rede através de rótulos MPLS. Ele participa ativamente no estabelecimento de LSP, usando protocolos de sinalização de rótulo, tais como: LDP, RSVP-TE (*Resource Reservation Protocol – Traffic Engineering*) e BGP (*Border Gateway Protocol*), e no encaminhamento de tráfego baseado nos caminhos estabelecidos. Ao receber um pacote, para o próximo roteador e assim por diante. (OLIVEIRA, LINS e MENDONÇA, 2012)

Existem basicamente três tipos de LSRs:

- LSR de Borda de Entrada: É uma LSR (roteador ou *switch* com funções de roteamento) de entrada de uma rede MPLS, ele realiza o processamento e a classificação inicial do pacote e aplica o primeiro rótulo na entrada (*ingress*) do pacote no domínio MPLS. Os *ingress* LSRs analisam as informações do cabeçalho de rede e associam cada datagrama a uma FEC. Toda FEC tem um rótulo associado que será utilizado no encaminhamento para o próximo nó.
- LSR de Trânsito: São LSR intermediários que têm a função de apenas fazer a comutação, ou seja, a troca de rótulos, e encaminhar o datagrama para p próximo nó. Eles oferecem comutação em alta velocidade, sendo essa umas das grandes vantagens

do MPLS, ganho de desempenho, pois não analisam os cabeçalhos IP a cada salto.

- LSR de Borda de Saída: É um LSR responsável pela retirada do rótulo do pacote e encaminhamento ao seu destino final.

Os LSR de entrada (ingresso) e os LRS de Saída (egresso) também são conhecidos como *Edge* LSRs, LER (*Label Edge Router*) ou PE (*Provider Edge*). Já o LSR de trânsito também é chamado de P (*Provider*).

2.7.1. O que acontece na borda?

Depois que o LER de ingresso na borda realiza a classificação, ele empilha um rótulo no pacote de dados que corresponde à FEC desse pacote. Chamamos isso de colocação de rótulo ou empilhamento de rótulo. Os LSRs no núcleo da rede não se envolvem com esse processo de reclassificação, como ocorre nas redes IP, isso gera um alívio de carga de processamento e ganho de desempenho nesses roteadores, que se se ocupam basicamente realizar troca de rótulos que consiste em:

- Realizar a pesquisa do rótulo sobre o rótulo que chega.
- Encontrar a interface de saída e o rótulo de saída para esse pacote.
- Trocar o rótulo recebido (entrada) pelo rótulo de saída adequado e encaminhar à interface de saída.

Quando um pacote chega ao fim da rede, o rótulo mais externo do pacote é retirado e o restante do pacote é encaminhado ao próximo salto, chama-se isso de descarte de rótulo.

E são essas as três operações fundamentais com um rótulo: empilhar, trocar e descartar. Vemos então que a imposição, descarte, um esquema de classificação exige um poder de processamento considerável na borda da rede, entretanto um modesto processamento no núcleo.

2.7.2. Mecanismo de encaminhamento

O mecanismo de MPLS é baseado nos rótulos MPLS e na *Label Forwarding Information Base* (LFIB), diferente do encaminhamento IP baseado apenas no IP de destino e FIB. Tanto o encaminhamento IP como o MPLS são feitos salto a salto, porém no IP há a

reclassificação do pacote a cada salto enquanto no MPLS apenas no LSR de ingresso.

A **tabela LIB** (*Label Information Base*): é a tabela que contém os diversos vínculos de rótulos que um LSR de ingresso recebe sobre o protocolo LDP, ou seja, uma tabela que apresenta informações correlacionando os rótulos às interfaces do roteador.

A **tabela FIB** (*Forwardind Information Base*) é a tabela que controla a decisão de encaminhamento de um roteador. Para todo possível endereço IP de destino, uma pesquisa de prefixo longo é executada pela FIB. Se um endereço é localizado na tabela, o roteador saberá para qual interface de saída o pacote deve ser encaminhado. Se nenhum endereço é encontrado há o descarte do pacote. O conteúdo da FIB reflete o estado atual da topologia IP que cerca o roteador, como determinado pelos protocolos IP de roteamento, por exemplo OSPF ou BGP4.

A **LFIB** (*Label Forwarding Information Base*) é uma tabela que indica onde e como encaminhar os pacotes. É criada por equipamentos pertencente a um domínio MPLS. Ela contém uma lista de entradas que consistem de uma subentrada de ingresso e uma mais subentradas de egresso, rótulo de saída e interface de saída, componentes de saída de nível de enlace. É baseada nas informações obtidas pelo LSR através da interação com os protocolos de roteamento. (OLIVEIRA, LINS e MENDONÇA, 2012)

A **FEC** (*Forwading Equivalence Class*), consiste em um grupo de pacotes que podem ser tratados de forma equivalente para proposito de encaminhamento. Uma FEC é representada por um rótulo e cada LSP (*Label Swtich Path*) é associado a uma FEC, quando um LER (*Label Edge Router*) recebe um pacote, verifica qual FEC ele pertence. Logo existe uma associação pacote > rótulo > FEC > LSP. Essa associação é o que possibilita a garante flexibilidade e escalabilidade desse tipo de rede.

Uma consideração cabível aqui é em relação ao tratamento que um pacote sofre para compor uma FEC, onde foram classificados e sofreram modificação em alguns de seus campos do cabeçalho. Essas modificações podem ter a ver com requisitos de QoS, tipo de aplicativo que o pacote está relacionado, identificador AS/VPN, sub-rede de origem ou destino e grupo de *multcast*, gerando um rótulo destino apropriado para cada requisição.

Podemos dizer que a FEC é uma rota ou prefixo encontrada na FIB que foi a melhor correspondência para o pacote recebido, podemos ver na figura 6 a associação das FECs e os LSPs.

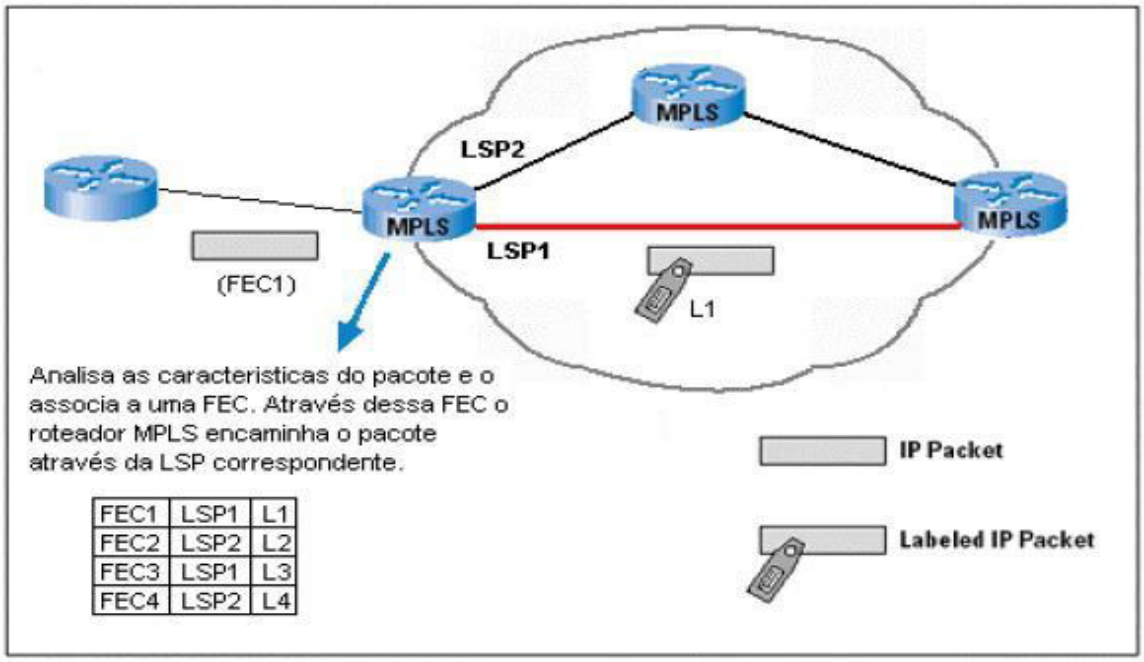


Figura 6: Construção das tabelas FEC.

Fonte: Redes MPLS, Oliveira, Lins e Mendonça, (2012)

O **LDP** (*Label Distribuition Protocol*) já detalhado em sessões anteriores.

Agora que já conhecemos os elementos básicos de uma rede MPLS e qual o papel de cada uma delas, vamos ver como elas interagem passo a passo.

Etapa 1: Construção da tabela de roteamento. Através dos protocolos de roteamento tais como OSPF e IS-IS, são construídas as tabelas de roteamento, que irão determinar os melhores caminhos para atingir as redes de destinos por toda a rede do provedor. Nesta etapa também há a atuação do protocolo LDP, que irá fazer o mapeamento entre os rótulos e IP de destino. Os rótulos serão atribuídos automaticamente, de acordo com os valores dos elementos do rótulo (EXP, P, TTL).

Etapa 2: Ingresso dos pacotes na rede. Os roteadores de borda LSR de ingresso recebe os pacotes que irão entrar na rede, executando serviços de camada 3 e valor agregado, tais como QoS, e em seguida acrescenta o rótulo aos pacotes.

Etapa 3: Encaminhamento dos pacotes na rede. O LSR encaminha 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 encaminha, sendo essa ação repetida por todos os roteadores no núcleo do *backbone*.

Etapa 4: Saída do pacote na rede. O roteador de borda LSR de saída remove o rótulo

e entrega o pacote IP para seguir seu restante do caminho. Na figura 7 abaixo podemos observar um resumo gráfico de tudo o que falamos até aqui.

É importante salientar a existência de uma técnica conhecida com PHP (*Penultimate Hop Popping*) (ROSE et al, 2001), que consiste na configuração da retirada do cabeçalho MPLS no penúltimo LSR, e não no LSR de saída. Esta técnica não compromete o funcionamento de um LSP e propicia um ganho de desempenho nos roteadores de borda que sem o uso desta técnica, fariam duas analises do cabeçalho: a análise do valor do rótulo ao receber o pacote rotulado e a análise do próximo cabeçalho MPLS ou do cabeçalho da rede. Porem com o uso do PHP é feito apenas uma análise do cabeçalho.

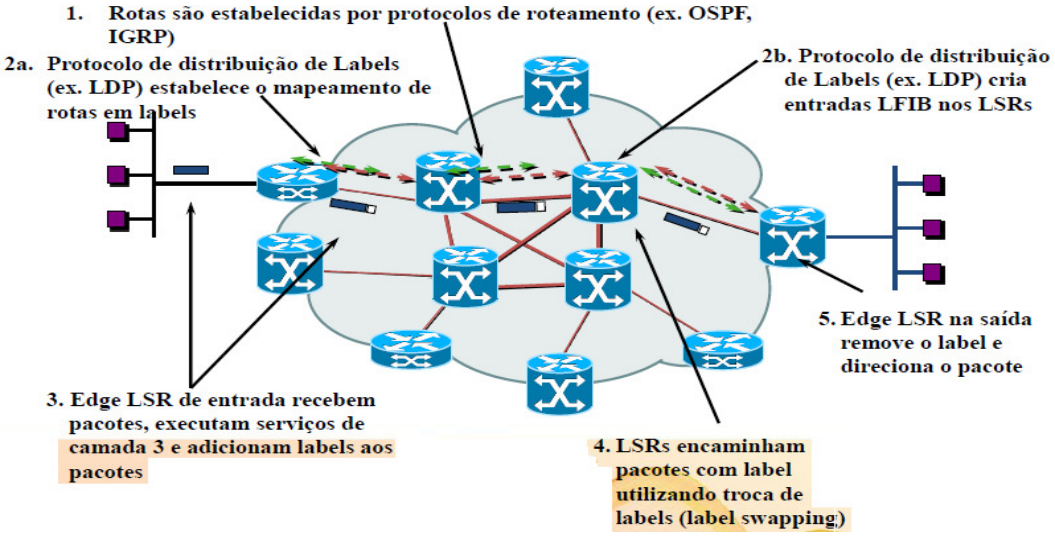


Figura 7: Resumo do encaminhamento de rótulos MPLS

Fonte: Curso de MPLS do 20°SCI/RNP (2014)

3. ENGENHARIA DE TRÁFEGO

Este capítulo tratará da engenharia de tráfego, área importante dentro do contexto de redes e uma das principais motivações para a criação e manutenção das redes MPLS, objeto deste trabalho. Abordaremos os principais conceitos, importância e aplicação nas redes MPLS além de um breve histórico de como esse trabalho era feito antes do surgimento destas redes.

3.1. O que é engenharia de tráfego?

A engenharia de tráfego é a utilização de princípios tecnológicos e científicos para a medição, caracterização, modelagem e controle do tráfego com o objetivo de avaliação e otimização do desempenho das redes IP (AWDUCHE *et al.*, 2000).

Diante deste crescimento e desenvolvimento das redes de computadores tanto em complexidade quanto em importância dos dados, surgiu à necessidade do gerenciamento dessa estrutura, visando a melhoria da qualidade do tráfego nas redes e é neste panorama surge duas vertentes, a Engenharia de Redes e a Engenharia de Tráfego.

A primeira delas se concentra na manipulação das redes para se ajustar ao tráfego. Isso é, com base em projeções feita acerca da carga de dados que fluirá pela rede o engenheiro de redes na busca de satisfazer essas demandas faz uso de roteadores, comutadores e afins, tudo isso é planejado, adquirido e instalado em uma escala de tempo relativamente longa, semanas, meses e até anos. Ou seja, esses ramos da engenharia lida com hardware, projeções e implantação de meios físicos para o bom funcionamento das redes, chamaram essa vertente de engenharia de tráfego proativa. (OSBORNE e SIMHA, 2002).

A Engenharia de Tráfego é um importante serviço na operação de grandes *backbones*, permitindo direcionar o tráfego da rede para caminhos diferentes dos que foram estabelecidos por um roteamento IP convencional, assim distribuir melhor o tráfego na rede, evitando pontos de congestionamentos e otimizando a utilização de recursos de rede. (OLIVEIRA, LINS e MENDONÇA, 2012)

Não importa o quanto você tente prever o futuro de uma rede, ela nunca corresponderá 100% com suas previsões, pois muitas vezes a taxa de crescimento excede muitas vezes as previsões feitas, assim como aconteceu em na década de 90 com a popularização da internet e as redes ainda não estavam prontas para tamanha expansão de volume de tráfego. Para suprir essa incapacidade de prever e equipar uma rede o engenheiro de tráfego pode fazer mudanças como, por exemplo, uma simples mudança das rotas de uma rede a migrando enlaces congestionadas para outros menos congestionados. (OSBORNE e SIMHA, 2002).

Mas dependendo da tecnologia adotada pela rede esse pode ser um procedimento penoso e até mesmo impossível. As populares redes IP, por exemplo, carregam uma dificuldade imensa em se alterar suas rotas de trafego quando utilizam algoritmos de roteamento baseados em custo, tal problema chama-se problema do peixe e em resumo é quando uma rota que tenha o menor custo em relação à outra é sobrecarregada enquanto a de maior custo fica ociosa ou com pouco tráfego. Na figura 8 abaixo podemos ver um esquema de uma rede com seus roteadores onde

o problema do peixe é visualizado.

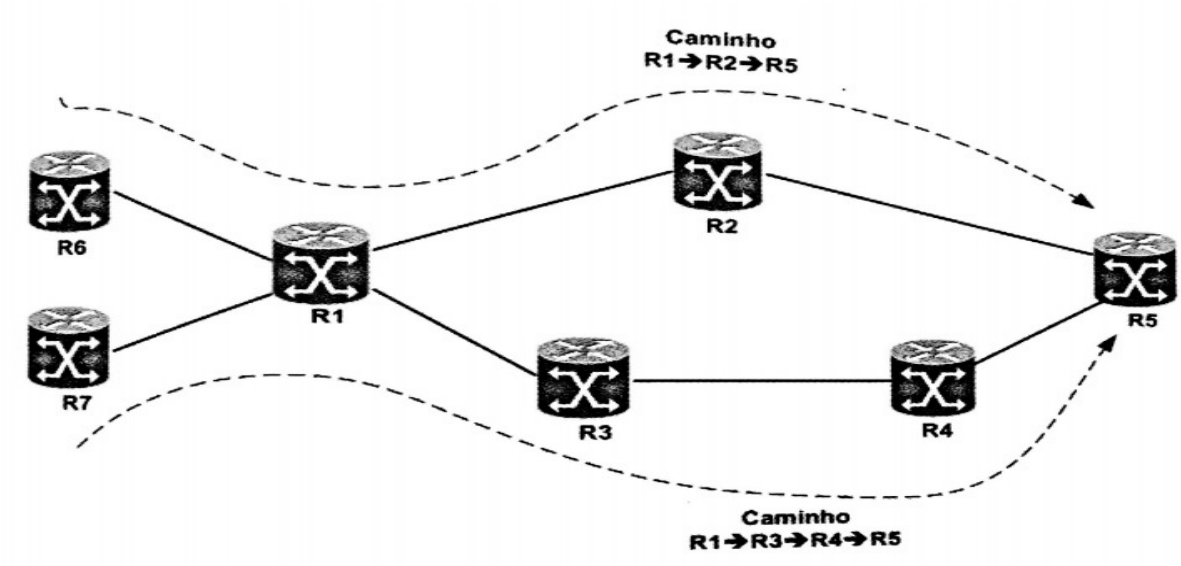


Figura 8: Rede exigindo roteamento explícito.
Fonte: Redes MPLS, Oliveira, Lins, Mendonça, 2012

Nessa figura existem dois caminhos para se mover de R2 a R6; R2- R5 – R6 e R2- R3- R4- R6

Todos os enlaces possuem o mesmo custo (15), e como todos os encaminhamentos são baseados em destino, todos os pacotes vindos de R1 ou de R7 e destinados a R6 são encaminhados pela mesma interface, passando por R2 e R5, pois o custo superior e mais baixo que o do caminho abaixo, logo ver-se uma sobrecarga do enlace superior em detrimento ao inferior.

Se fosse uma rede ATM, a resolução do problema seria mais trivial, bastando estabelecer dois PVCs de R2 a R6 e definir seus custos como sendo os mesmos. O problema estaria resolvido, pois haveria um balanceamento de cargas entre os dois circuitos. Entretanto sabemos que as redes dominantes atualmente são as redes IP e chegaram a esse patamar não por seus problemas, mas por estes serem pequenos quando comparados a praticidade e aplicabilidade às tecnologias atuais.

No MPLS-TE há encaminhamento de pacotes, enquanto no ATM isso é feito por células, ou seja, para se usar a solução ATM interligada a redes IP seriam necessários servidores de tradução IP/ATM o que acarreta custo e problemas de risco de falhas já mencionados. Mesmo que o engenheiro de redes quisesse usar a solução ATM precisaria fazer uma malha completa de adjacências o que não é necessário no MPLS, logo a solução MPLS se mostra mais econômica, viável e tecnicamente mais completa.

Pode-se dizer, então, que a TE (*Traffic Engineering*) visa sempre evitar congestionamentos na rede. Logo, não se pode haver uma parte da rede com sua banda sobrecarregada enquanto outras estão livres. Vale lembrar que o objetivo principal da TE é o uso contínuo da rede, e não de "*Flash Crowds*" (um significativo aumento no uso da rede por um período muito pequeno de tempo).

Para que as características descritas acima sejam possíveis, deve haver um elemento na rede que seja responsável pela medição do uso e controle de seus recursos.

Uma das aplicações do roteamento explícito é na engenharia de tráfego, onde o objetivo é apresentar como é possível garantir que os diversos caminhos possam ser utilizados para o envio do tráfego sem sobrecarregar um determinado caminho, deixando o outro subutilizado. Uma boa engenharia de tráfego é essencial para a eficiência dos *backbones* das operadoras de telecomunicação. A capacidade de transmissão das redes deve ser bastante robusta, de forma que possam suportar falhas de enlaces ou de um roteador. (OLIVEIRA, LINS e MENDONÇA, 2012)

O MPLS-TE (*acrônimo de MultiProtocol Label Switching – Traffic Engineering*) é uma tecnologia que implementa a engenharia de trafego em redes IP ao permitir o estabelecimento de caminhos alternativos nessas redes - diferentes dos caminhos definidos pelo protocolo IGP – com base em critérios disponíveis, métrica sensível ao atraso ou, por exemplo, características físicas do enlace com velocidades diferentes.

O MPLS-TE pode trazer benefícios para todas as tecnologias e/ou aplicações que requerem banda, atrasos ou verificação dos níveis de eficiência no mapeamento de fluxos de recursos. A aplicação do MPLS-TE não cria banda e não reduz os problemas com insuficiência de recursos na rede, mas ajuda no mapeamento mais eficiente desses recursos, como, por exemplo, o mapeamento de caminhos redundantes. O MPLS-TE permite um esquema de engenharia de tráfego onde o roteador conhecido como *head-end* (HE) do LSP pode calcular a rota de forma mais eficiente através da rede em direção ao roteador conhecido como *tail end*. O *head-end* pode fazer isso se ele conhecer a topologia da rede e a banda disponível de todos os enlaces na rede. É necessário habilitar o MPLS nos roteadores para estabelecimento do LSP fim-a-fim. O fato da comunicação de rótulos serem utilizada, e não o encaminhamento baseado em IP é o que permite roteamento baseado em origem em vez do roteamento baseado em IP de destino (De Ghein, 2007)

3.2. O MPLS-TE

Entre meados da década de 90, os artigos de revistas sobre redes falavam a respeito de um novo paradigma no mundo IP – a comutação IP. E a princípio parecia que a necessidade de roteamento IP havia sido eliminada e poderíamos simplesmente comutar pacotes IP. A empresa que iniciou isso foi a *Ipsilion*. Outras empresas como a *Toshiba*, passaram para o ATM como meio de comutação IP em seus *Cell-Switched Router* (CSR). A *Cisco System* apareceu com sua própria resposta a esse conceito – comutação de *labels*. As tentativas de se padronizar essas tecnologias através do IETF resultaram na combinação de várias tecnologias, gerando o *Multiprotocol Label Switching* (MPLS). (OSBORNE e SIMHA, 2002).

As políticas de roteamentos e balanceamento de carga baseada no encaminhamento dos pacotes podem ser empregadas no TE e é possível utilizar outros parâmetros, mas isso não ocorre em redes de alto volume de tráfego devido às limitações de desempenho.

Há algumas limitações distintas do modo como a engenharia de tráfego pode ser realizada usando basicamente o protocolo IP. Se as regras de encaminhamento forem modificadas, então os roteadores na rede terão de ser mantidos sincronizados e todos deverão operar com o mesmo nível de função, ou então poderão acontecer *loops* e maior congestionamento. O roteamento baseado na origem IP é limitado tanto pela quantidade de novos enlaces (*hops*) quanto pelo fato de que nem todos os roteadores admitem o roteamento baseado na origem de uma maneira consistente. Como solução para esses problemas, o MPLS apresenta o roteamento explicito. (OSBORNE e SIMHA, 2002).

A figura 9 abaixo ilustra uma típica situação de roteamento baseado em IP de destino, onde não há qualquer mecanismo de balanceamento de cargas por caminhos redundantes. Nesse encaminhamento tem-se uma sobrecarga dos enlaces principais e de maior banda; já os enlaces redundantes são subutilizados.

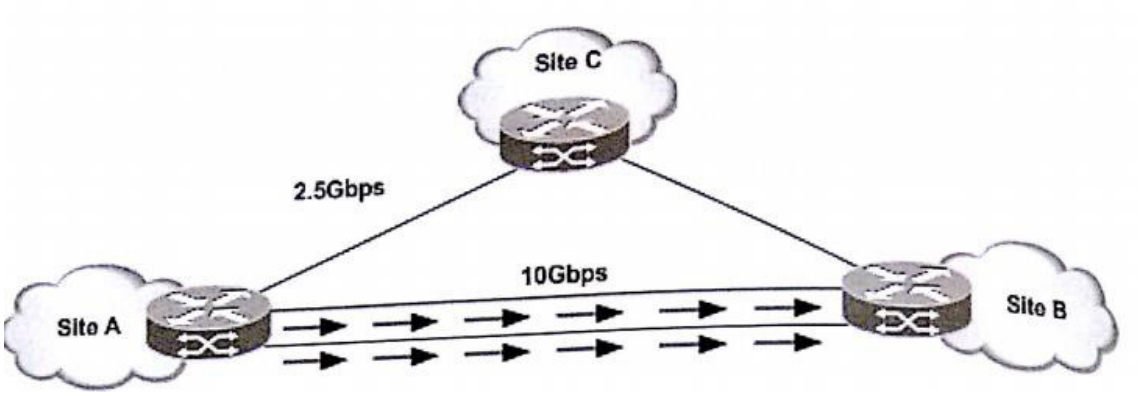


Figura 9: Encaminhamento IP tradicional.

Fonte: Redes MPLS, José Oliveira, Rafael Lins, Roberto Mendonça, 2102

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 10 abaixo. Dessa forma, a engenharia de tráfego está utilizando cada vez mais o MPLS para atender as suas necessidades de tunelamento.

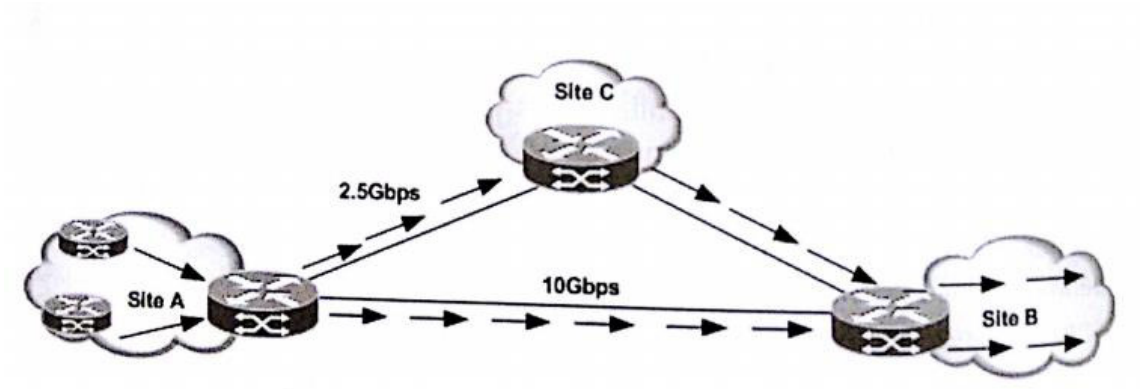


Figura 10: Balanceamento de carga com MPLS-TE

Fonte: Redes MPLS, José Oliveira, Rafael Lins, Roberto Mendonça, 2012

A motivação inicial a criação do MPLS era de melhorar a velocidade de encaminhamento dos pacotes, mas isso acabou não se mostrando uma vantagem realmente expressiva, pois as pesquisas de rótulos de 20 bits do MPLS não eram significativamente mais rápidas do que a pesquisa de IP de 32 bits. Entretanto o MPLS se mostrou interessante quando se analisa as aplicações que ele permite.

O MPLS possui muitos componentes que o tornam interessante para o uso em uma rede com engenharia de tráfego, entre eles estão:

- O MPLS tem a capacidade de estabelecer um LSP que segue um caminho diferente do oferecido como “preferido” pelo protocolo de roteamento.
- Os recursos dentro da rede podem ser reservados dinamicamente, conforme os LDPs são estabelecidos, e podem ser atualizados dinamicamente, conforme mudam as necessidades dos LSPs, para que esses fluxos de tráfego possam ter garantia de nível e qualidade de serviço.
- O tráfego pode ser ordenado para LSPs “paralelos”, ou seja, vários LSPs podem ser estabelecidos de origem e destino, e o tráfego pode ser distribuído entre os LSPs de acordo com qualquer número de algoritmos. Os LSPs “paralelos” podem tomar caminhos significativamente diferentes por meio da rede.
- Os recursos de rede podem ser automaticamente gerenciados como novos LSPs, configurados para atender as exigências imediatas da rede e com recursos liberados novamente quando os LSPs antigos não são mais necessários.
- Procedimentos de recuperação podem ser definidos, descrevendo como o tráfego pode ser transferido para LSPs alternativos no caso de uma falha e indicando como e quando LSPs de *backup* e espera devem ser configurados e roteados.

Na engenharia de tráfego (TE) é determinado o caminho por meio da rede que diversos fluxos de dados surgirão. Como TE as operadoras de telecomunicações podem oferecer um *backbone* para seus clientes com mais eficiência.

3.3. Protocolos envolvidos na TE

Para a TE muitos protocolos usuais ganharam extensões para que possam trabalhar no intuito de colaborar, medir e compartilhar métricas importantes na construção de uma rede que usa TE.

3.3.1. Extensões do OSPF para TE

A RFC 3630 define as extensões do protocolo OSPF versão 2 para engenharia de tráfego aplicáveis a redes IP, sendo também totalmente válido para o MPLS. O OSPF-TE (*Open*

Shortest Path First- Traffic Engineering) incluir o conceito de LSAs (*Link State Advertisements*) opacos. Eles permitem que os roteadores compartilhem informações privadas ou proprietárias pela rede de uma maneira interoperável. Foram definidos três tipos de LSAs opacos:

1. LSA opaco tipo 8 – Abrange apenas um enlace;
2. LSA opaco tipo 10 – Abrange uma área;
3. LSA opaco tipo 11 – Abrange um sistema autônomo OSPF.

Os roteadores que não "entendem" os LSAs opacos não precisam examinar nem os usar em seus cálculos de caminho. Esses roteadores necessitam apenas de armazenar e reencaminhar os LSAs recebidos. Isso provê um modo elegante de acrescentar função a uma rede de engenharia de tráfego ao OSPF, de modo que os roteadores cientes da engenharia de tráfego possam descobrir e atuar sobre a informação de TE em cooperação com roteadores mais antigos, que continuam a implementar o OSPF padrão (FARREL, 2005). A RFC 3630 engloba apenas o LSA opaco 10, ou seja, restringe a sua aplicabilidade ao interior de uma área OSPF (ENNE, 2009).

Dentro do LSA opaco 10 foi definido TE LSA, identificado pelo código 1. Esse LSA descreve roteadores ponto a ponto e conexões para redes com múltiplos acessos, de forma similar a um roteador LSA do OSPF convencional.

O OSPF-TE descreve e define uma forma de distribuição de atributos de enlaces estendidos (*extended links atributes*) que se baseia em roteamento baseado em restrição (*constraint based routing*). Ao contrário do OSPF convencional, onde cada salto realiza o roteamento de pacotes com base em tabela de roteamento local, o OSPF-TE centraliza as informações em base de dados localizada no *head-end* LSR, no caso do MPLS-TE, denominado base de dados de TE (TE *databese*). (OLIVEIRA, LINS e MENDONÇA, 2012)

Existe a possibilidade da utilização conjunta da métrica do OSPF convencional e de uma métrica TE no MPLS-TE para diferentes classes de tráfego. Uma aplicação de voz pode utilizar a métrica OSPF-TE relativa a retardo e a *jitters* na rede, enquanto uma transferência de grandes arquivos pode utilizar uma métrica OSPF convencional.

3.3.2. Extensões do IS-IS para TE

Para que o MPLS-TE funcione sobre uma rede com um protocolo IS-IS (*Intermediate System to Intermediate System*), preexistente, é preciso atualiza-lo para uma nova versão de IS-IS; já com OSPF não é necessária a transição.

As extensões de TE para IS-IS estão descritas nas RFC 3784.

Os procedimentos no IS-IS-TE são semelhantes ao do OSPF-TE, com algumas pequenas diferenças. Por exemplo: o período padrão para *reflooding* periódico de informação de roteamento, que é de meia hora para o OSPF-TE, assume o valor de quinze minutos para o IS-IS-TE.

Tanto o OSPF quanto o IS-IS são considerados protocolos de *link-stage* ou seja, eles guardam e distribuem o status dos enlaces e isso é muito útil para reserva de recursos e gerenciamento de tráfego feito por outros protocolos.

3.3.3. Protocolo RSVP-TE

O RSVP-TE (*Resource Reservation Procol – Traffic Enginnering*) é o protocolo apropriado para sinalização de rótulos em uma rede MPLS com engenharia de tráfego, baseado no RSVP (*Resource reServation Protocol*). O RSVP é adequado para a extensão ao mundo MPLS porque lida com reservas de recursos fim-a-fim para o fluxo de dados de forma semelhante com o MPLS com TE. Por outro lado, ele não atende a todas as exigências necessárias para o MPLS principalmente a distribuição de rótulos e controle de caminhos por meio de rotas explícitas (FARREL, 2005).

O RSVP foi inicialmente estendido para esse tipo de aplicação pela *Cisco System* quando ela estava desenvolvendo a comutação por TAG. Desde então, o IETF tem publicado o RSVP-TE.

RSVP-TE não é um protocolo de roteamento. Quaisquer decisões de roteamento são feitas pelo IGP e pelo CSPF (*Constrained Shortest Path First*). A única tarefa do RSVP-TE é sinalizar e manter reserva de recursos para uma rede MPLS-TE, o RSVP-TE reserva largura de banda na camada do plano de controle; não existe policiamento de tráfego no plano de encaminhamento. Quando usado para outros propósitos (como reservas VoIP), RSVP pode ser usado para reserva para montar SVCs ATM. (OSBORNE e SIMHA, 2002)

RSVP possui três funções básicas:

- Configurações e manutenção de caminho
- Encerramento de caminho
- Sinalização de erro

RSVP é um protocolo com estado flexível, isso significa que ele precisa atualizar suas reservas de redes periodicamente, sinalizando novamente sobre possíveis alterações. O RSVP-TE consegue reutilizar o RSVP de maneira bastante completa. Todas as sete mensagens RSVP encontram um uso no RSVP-TE, embora o *ResvConf*, que é a mensagem para reserva de recurso ao longo do caminho, seja o menos significativo do que quando usado para o RSVP.

Depois que um *head end* do túnel completa o seu CSPF (C*onstrained Shortest Path First*) para determinado túnel, ele terá que sinalizar essa solicitação para a rede. O *head end* faz isso enviando uma mensagem de *PATH* ao nó do salto seguinte, junto com o caminho calculado até o destino. O roteador que enviou a mensagem *PATH* é chamado roteador *upstream*, e o roteador que recebeu a mensagem é chamado de roteador *downstream*. O roteador *upstream* às vezes é chamado salto anterior ou *phop*. (OSBORNE e SIMHA, 2002)

Depois que um roteador *downstream* recebe uma mensagem *PATH*, ele faz algumas coisas. Ele verifica o formato da mensagem para confirmar que estar tudo correto e depois a quantidade de largura de banda que a mensagem *PATH* solicita, chamamos isso de controle de admissão.

Se o controle de admissão tiver sucesso e a mensagem *PATH* tiver permissão para reservar a largura de banda que deseja, o roteador *downstream* cria uma nova mensagem *PATH* e envia ao salto seguinte no *Explicit Route Object* (ERO), isso se repete nó a nó até o fim do túnel.

No fim do túnel é feito o controle de admissão sobre o *PATH*, assim como qualquer outro roteador *downstream*. Quando o ultimo nó observa que tem um túnel definido ele responde com uma mensagem *RESV*. Essa mensagem seria como um ACK de volta ao roteador *upstream*, ela não apenas tem a confirmação de reserva das solicitações para a criação do túnel, mas contém o rótulo de chegada que o roteador *upstream* deverá usar para encaminhar os pacotes ao longo do LSP TE até o final do túnel. O *RESV* mensagem inclui o *flowspec* objeto de dados que identifica os recursos que o fluxo precisa.

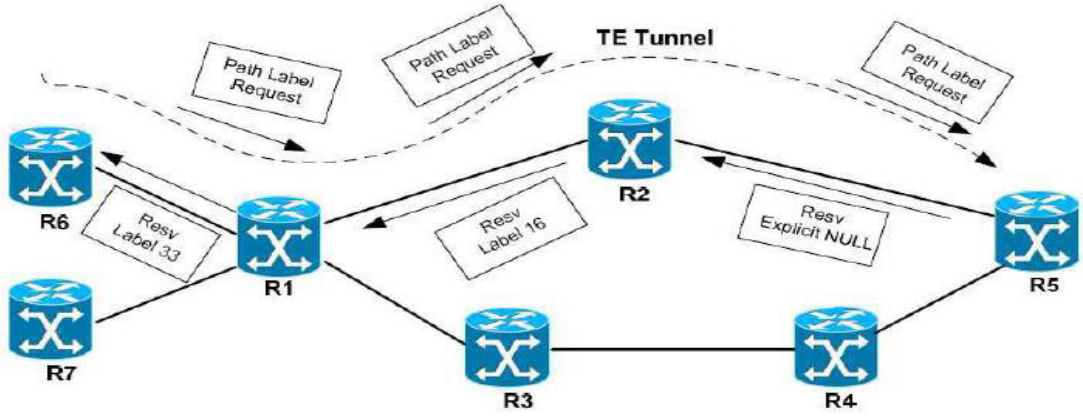


Figura 11: Troca de pacotes RSVP.
FONTE: Curso de MPLS no 20° SCI –RNP

A figura 11 acima ilustra o funcionamento básico do RSVP-TE, as solicitações de reserva de recurso assim com as mensagens de volta.

3.4. PCALC (*Path Calculation*)

Em um protocolo de roteadores de estado de enlace, cada roteador sabe a respeito de todos os outros roteadores em uma rede e dos enlaces que conectam esses roteadores. Em OSPF, essa informação é codificada como anúncio de estado de enlace (*LSA - Link Satate Advertisements*); no IS-IS, essa informação está em pacotes de estado de enlace (LSPs – *Link-State Packets*). (OSBORNE e SIMHA, 2002).

Assim que um roteador sabe a respeito de todas as outras rotas de enlaces, ele executa o algoritmo *Dijkstra Shortest Path First* para determinar o caminho mais curto entre o roteador que realiza o cálculo em todos os outros roteadores na rede.

Como todos os roteadores executam o mesmo cálculo sobre os mesmos dados, cada roteador possui a mesma imagem da rede, e os pacotes são roteadores de modo coerente em cada salto.

Entender o SPF (*Shortest Path First)* é fundamental para entender o CSPF da engenharia de tráfego MPLS, que é baseado no algoritmo de SPF básico de *Dijkstra*.

Por exemplo, em uma rede depois que cada roteador tiver inundado suas informações na rede, todos os roteadores saberão que os outros roteadores sabem. Assim, o banco de dado

de enlace em cada roteador tem as informações de cada par de roteador e o custo entre eles.

No cálculo do SPF, cada roteador mantém duas listas e usa essas informações para executar seus cálculos.

- Uma delas tem os nós que são conhecidos como estando no caminho mais curto até o destino, essa lista é chamada de PATH. É importante entender que a única coisa que há nessa tabela é o caminho mais curto até o destino.
- Outra lista contém os saltos seguintes, que podem ou não está no caminho mais curto até um destino. Essa lista é chamada lista de tentativas, ou lista TENT.

As rotas de melhores caminhos são calculadas pelo PCALC que é um algoritmo SPF (*Shortst Path First*), ou seja, prefere o menor caminho primeiro. Como o OSPF e o IS-IS foram estendidos para distribuir outros critérios para a elaboração do caminho mais curto o PCALC pode calcular um caminho não só com base no caminho mais curto, mas também com base nesses recursos.

O processo que gera um caminho para um túnel TE é diferente do processo normal SPF, mas não muito. Existem duas diferenças principais entre SPF normal, feito por protocolos de roteador, é o CSPF, executando pela engenharia de tráfego MPLS.

Por um lado, o processo de determinação do caminho não é preparado para encontrar a melhor rota, apenas para a extremidade do túnel. Isso torna o algoritmo SPF ligeiramente diferente, pois ele para assim que o nó alvo é achado na lista PATH.

Além disso, agora há mais de uma métrica em cada nó. Em vez de apenas um único custo para o enlace entre dois vinhos, há também:

- Largura de banda
- Atributos do enlace
- Peso Administrativo.

Outro detalhe sutil da CSPF é que, como você está procurando um único caminho até um nó final, não existe compartilhamento de carga. Existem algumas formas de desempate quanto dois caminhos possuem os mesmos atributos: largura de banda mínima no caminho, medição IGP (*Interior Gateway Protocol*) mais baixa até um caminho de contagem de saltos mais baixo do caminho.

A Largura de Banda é fundamental, pois um caminho não é considerado elegível para uso por um túnel MPLS-TE específico se ele não tiver a largura de banda exigida.

Os Atributos de Enlace são semelhantes à largura de banda, do ponto de vista do CSPF são bits de afinidade que são definidos pelo gerente de redes, onde quando esses bits não coincidem com os bits de afinidade do túnel esses enlaces não são eleitos.

O Peso Admirativo também é muito simples, embora seja usado de modo um pouco diferente. O peso admirativo é o que é propagado pelo IGP quando ele inunda informações de engenharia de tráfego. Por isso com SPF regular é possível que o PCALC execute pedido de rotas explicitas manipulando manualmente esses pesos e este caminho, que não é nada mais que uma sequência de endereços IP, onde cada acesso representa uma interface do roteador.

3.5. Proteção e Restauração

As redes são projetadas com um alto nível de redundância para garantir que oferta dos serviços disponíveis aos clientes. No entanto, muitas vezes a falha em um circuito de comunicação faz com que a recuperação de um serviço gaste um tempo na ordem de dezenas de segundos, dado a quantidade de protocolos envolvidos na convergência. Este tempo de convergência é resultante, principalmente, do tempo de propagação do protocolo IGP, responsável por fazer o novo roteamento rápido para contornar as falhas, efetuando a convergência na rede. Dependendo do tamanho da rede, este tempo pode levar de cinco a dez segundos. Durante esta convergência há perdas de pacotes e, consequentemente, uma indisponibilidade do serviço oferecido ao usuário, o que pode afetar o SLA (*Service Level Agreement*) acordado entre o usuário e o provedor. (OLIVEIRA, LINS e MENDONÇA, 2012)

Fast Reroute (FRR) é uma ferramenta integrante do MPLS-TE. Ela permite que circuitos e roteadores sejam protegidos pelos túneis do MPLS-TE com rápido tempo de convergência. A proteção dos circuitos é denominada *Link Protection* e a dos roteadores, *Node Protection*.

Ambos os modos de proteção são conhecidos como proteção local, isso porque os túneis de *backup* protegem apenas um segmento do caminho. A figura 12 abaixo exibe a proteção local entre R3 e R5, denominada de proteção de enlace, e a proteção de nó R5, denominada de proteção de nó. Para a proteção do enlace, o *head-end* do túnel de *backup* é o R3, que será PLR (*Point of Local Repair*), e o fim do túnel é o roteador R5 (*Merge Point*). Já para a proteção do nó, o *head-end* (HE) do túnel é o R3, e o fim do túnel é o roteador R7.

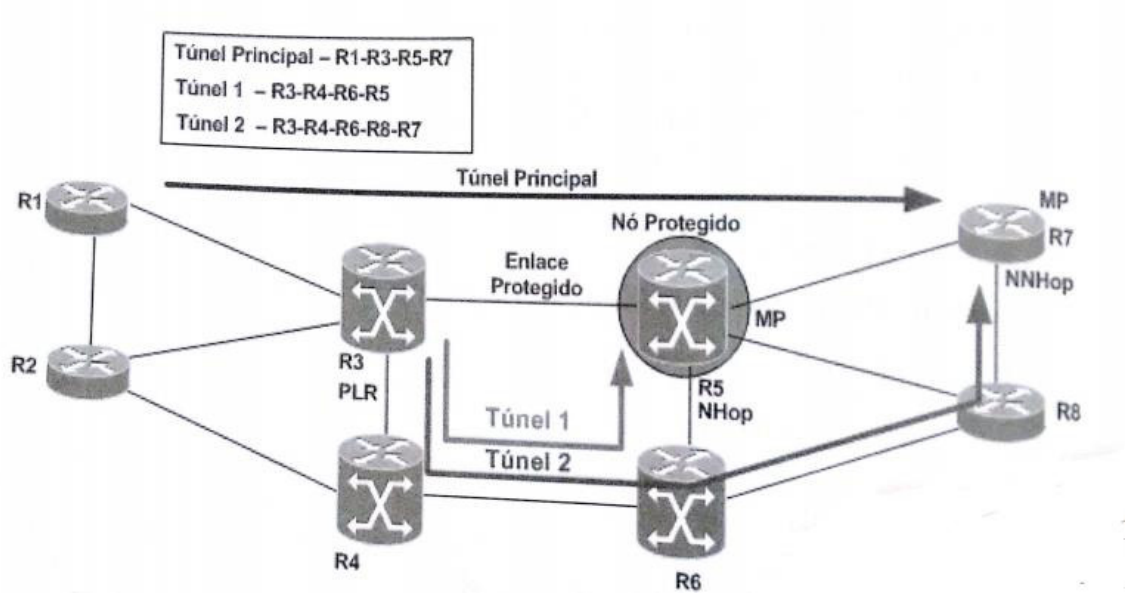


Figura 12: Proteção de enlace e proteção de nó.

Fonte: Adaptado de (OSBORNE e SIMHA, 2002) pg 94

O enlace R3-R5 é considerado o enlace crítico sobre o qual o túnel primário é sinalizado. Esse enlace será o enlace protegido e, para sua proteção e proteção do túnel principal, um túnel de backup é sinalizado em torno do enlace. A proteção do enlace usa túneis de backup NHop (*Next Hop Router*) e conta com o fato que embora o enlace protegido tenha sido rompido, o roteador na outra ponta desse enlace protegido ainda está ativo; portanto a proteção do enlace protege de uma falha no enlacem mas não contra uma falha de nó (OSBORNE e SIMHA, 2002).

A proteção do nó é semelhante à proteção do enlace, porém ela difere porque o MP não é NHop, e sim NNHop (*Next Next Hop Router*). No caso da figura 12, o túnel principal faz o uso do caminho R1-R3-R5-R7. O enlace R3-R5 está protegido pelo Túnel 1, e o roteador R5 está protegido pelo Túnel 2.

No caso de falhas da conexão R3-R5, o tráfego ocorrerá pelo Túnel 1 até que o túnel principal seja reestabelecido. Já em caso de falha do roteador R5, o tráfego será transmitido através do Túnel 2 até que o principal seja reestabelecido.

3.6. Tratamento de Congestionamento

A otimização da utilização de sua rede é chamada de Método Estratégico de implantação do MPLS-TE. Ela também pode ser chamada de técnica da malha completa. A ideia é montar

uma malha completa de LSPs MPLS-TE entre determinado conjunto de roteadores, dimensione as rotas de acordo com a largura de banda que passa por cada par de roteador e deixe o LSP encontrar o melhor caminho na sua rede, desde de que atenda a demanda de largura de banda que deseja. Isso permite evitar congestionamentos ao máximo possível, espelhando LSP pela rede. Essa técnica não substitui um bom planejamento de uma rede, mas ela permite obter o máximo que a infraestrutura já existente pode oferecer, retardando assim um *upgrade* de emergência na largura de banda e novos roteadores.

Outra forma de tratar os congestionamentos usando MPLS-TE é a técnica "tática", ou "conforme a necessidade". Em vez de montar uma malha completa, essa tática permite que o IGP encaminhe o tráfego como precisar, montando um TR-LSPs somente depois que um congestionamento for detectado. Isso é útil quando ocorre uma grande demanda na rede por um novo serviço, ou um *site* com promoções da *Black Friday*, onde é gerado um congestionamento em alguns enlaces da rede enquanto deixa outros vazios. Pode até criar túneis MPLS-TE para contornar parte do congestionamento, usando enlaces não escolhidos pelo IGP, isso lhe garante um tempo a mais para levantar esses serviços.

3.7. Atributos de um túnel MPLS-TE

Muito se tem falado sobre túneis MPLS-TE e para esclarecer melhor quais são seus atributos citaremos os mais relevantes. Alguns deles têm a mesma natureza que os atributos dos enlaces distribuídos pelo protocolo IGP estendidos para TE. Alguns outros atributos dos túneis MPLS-TE são configurados pelos administradores da rede, transparentemente ao protocolo de roteamento utilizado.

Os atributos são listados a seguir:

- Endereço do *tail end* LSR;
- Largura de banda desejada;
- Atributos de preempção;
- Atributos de reotimização;
- *Fast rerouting*

3.8 Outras contribuições na ET

Ainda no contexto do uso do MPLS na Engenharia de Tráfego, falaremos sucintamente de outras contribuições dessas redes, muito embora algumas dessas características não sejam os alvos deste trabalho, mais é relevante para se compreender a importância desta tecnologia para as redes modernas.

Suas principais aplicações são:

- *VPNs MPLS*
- *Quality of service* (QoS) MPLS
- *Any Transport over MPLS* (AtoM)

VPNs não é nenhuma invenção do MPLS, já existem desde 1990, eram usados pelo *Frame Relay* e ATM como meio de interligação entre empresas e suas filiais. As VPNs MPLS vieram com a proposta de focar em padrões, como o IP privado, intranet, extranet além é claro da conectividade com a internet, tudo isso de forma escalável.

O QoS também longe de ser um legado dessas redes, mas tão somente uma possibilidade de oferecer um serviço semelhante ao que o QoS de redes IP já previam, ou seja *Differentiated Service* (*DiffServ*), onde no cabeçalho MPLS são representados por 3 bits que representarão a classe de serviço daquele pacote.

Já o AtoM é uma aplicação que facilita o transporte de dados a nível de camada 2, como no *Frame Relay*, Ethernet e ATM.

Após a descrição das facilidades e flexibilidade, comparações e integrações com outras redes, alguns pontos devem ficar claros para que não ocorra equívocos. O MPLS não é uma rede ATM ou um *Frame Relay* moderno, embora tenha herdado muitas funcionalidades destas tecnologias e sua estrutura propicie uma integração com as mesmas o MPLS não pode ser considerado uma evolução delas ou suas versões aprimoradas. O MPLS embora possibilite a aplicação de QoS não é um protocolo de Qualidade de Serviços, então essa nunca deve ser a motivação principal para adotar tais redes.

O MPLS-TE traz soluções para problemas de Engenharia de Tráfego que o IP não pode oferecer, como já dito anteriormente o MPLS conhece sua demanda de trafego e os recursos que lhe estão disponíveis, por isso pode tratar o tráfego de sua rede forma otimizada,

além de gerenciar possíveis congestionamentos ou falhas no enlace e nós.

4. ESTUDO DE CASO

A última parte deste trabalho é destinada à implantação de uma rede para a simulação do MPLS. Nesta simulação será verificada toda a configuração de todos os roteadores envolvidos na rede, os protocolos envolvidos assim como as interfaces e modelos de roteadores usados. Será verificada a convergência de rede e se o protocolo MPLS corresponde conforme foi estudado.

No decorrer da simulação a teoria já vista será mencionada onde for oportuno, mostrando na prática onde esses conceitos são utilizados dentro de uma rede MPLS.

4.1. Metodologia

Foi utilizado um ambiente de simulação para os testes através do *software* emulador GNS3. Esse software foi utilizado pois atende a todos os requisitos necessários para a emulação das funcionalidades que serão exibidas. Trata-se de um emulador gráfico que é fortemente utilizado com *o Dynamipis* (um emulador Cisco IOS) e o *Dynagem* (um *front-end* para *Dynampis* baseado em texto).

Algumas características do GNS3:

- Cada roteador virtual criado é de fato uma emulação completa de um roteador Cisco, suportando todos os protocolos e RFCs que um roteador Cisco real suportaria.
- Várias instâncias de roteadores virtuais podem ser criadas e executadas em um mesmo PC.
- Permite a comunicação entre elementos emulados e elementos físicos.
- Trata-se de um *software* de domínio público.
- Pode ser utilizado em qualquer tipo de computador e sob os mais diversos sistemas operacionais.

4.2. Topologia

A topologia completa será a base para a implementação do teste e é apresentada na figura 14. Essa figura não reflete as dimensões de um *backbone* de um grande provedor de serviços, onde normalmente se encontram centenas de roteadores, mas usamos uma topologia suficiente para exibição dos serviços aqui propostos.

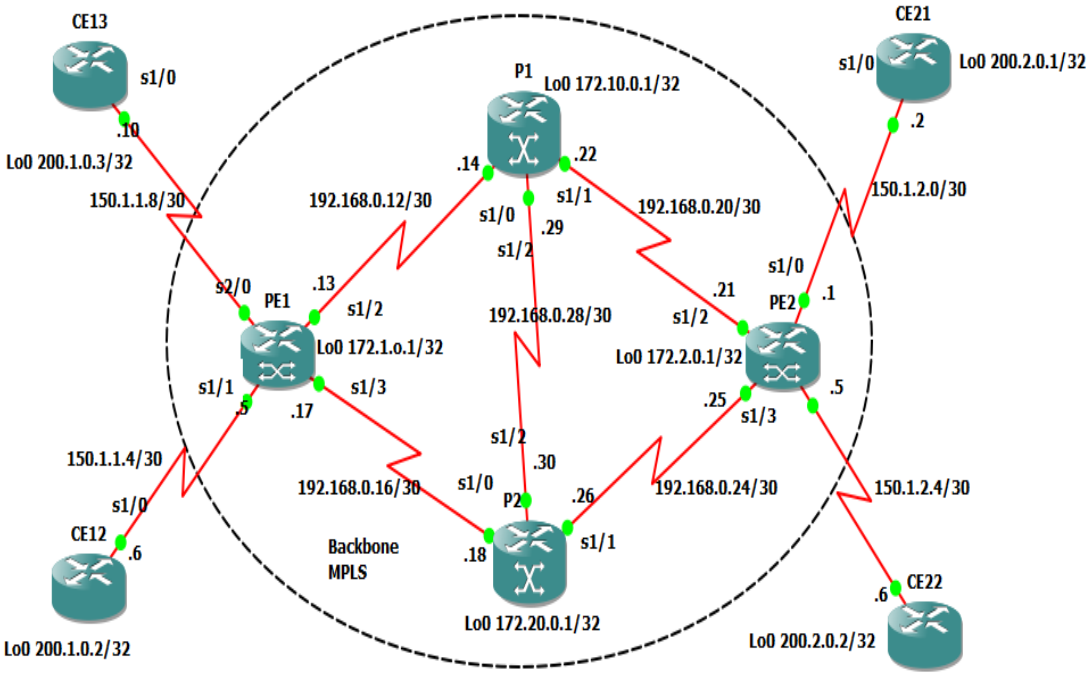


Figura 13: Topologia da simulação

Fonte: Próprio autor

4.1. Recursos utilizados

- Hardware: Quatro roteadores, modelo 7206. Estes farão a função de PE e P da rede MPLS. Cinco roteadores modelo 3640. Estes farão a função de CE.
- Versões de software: Levando em conta todas as características necessárias para implementar todos os serviços usamos para os roteadores 7206 o Sistema Operacional (IOS) 12.4-7a. Já para os 3640, usamos 12.4-13b.
- *WireShark* um serviço de monitoração e análise de pacotes disponível dentro do GNS3. É um programa que analisa o tráfego de rede, e o organiza os protocolos.

As funcionalidades do *Wireshark* são semelhantes ao do *tcpdump*, mas com uma interface gráfica, com mais informação e com a possibilidade da utilização de filtros.

4.3. Protocolos IGP/EGP e esquema de endereçamento IP.

Para a utilização do MPLS, os protocolos IGPs (*Interior Gateway Protocols*) é recomendado o OSPF (*Open Shortest Path First*) ou IS-IS (*Intermediate System to Intermediate System*).

Os dois são excelentes protocolos de roteamento de *link-state*, estáveis e escaláveis, no entanto por questões de habilidade na configuração, será usado o OSPF.

São esses protocolos os responsáveis por passar informações como tamanho da banda e restrições dos enlaces, além de promover a distribuição da informação para o TE *database*.

A TE *database* é formada por informações dos protocolos *link-stage* como OSPF ou IS-IS, que fazem isso através de um algoritmo chamado *path calculation* (PCALC) que calcula o melhor caminho entre um *head end* LSR até um *tail end* LSR.

Esta base de dados também contém todos os *links* que estão habilitados com MPLS-TE além de outros atributos.

4.4. Protocolo BGP

O BGP (*Border Gateway Protocol*) é um protocolo robusto e escalável, pois isso é o protocolo mais utilizado na internet. Para alcançar isso o BGP usa diversos parâmetros, chamados de atributos, que definem políticas de roteamento e mantêm a estabilidade do ambiente. Além disso, o BGP utiliza CIDR (*Classless Inter-Domain Routing*) para reduzir o tamanho das tabelas de roteamento.

Os vizinhos BGP trocam todas as informações de roteamento após o estabelecimento de uma sessão TCP entre eles. Depois, quando uma alteração na tabela é detectada, os vizinhos somente trocam as informações novas. Não há uma troca periódica de informações, e as atualizações que ocorrem somente anunciam o melhor caminho existente para a rede destino.

O BGP possibilitou a adição de extensões no protocolo criando o MP-BGP (*Multi Protocol* BGP). Estas extensões permitem e facilitam a troca de informações associadas aos clientes MPLS VPN entre os roteadores PEs do Backbone. Assim, é possível trocar informações de diferentes protocolos através de uma única sessão BGP entre os PEs. Esses protocolos são: IPV4 e IPV6, VPNv4 entre outros conhecidos como *Address Families.*

Sistema Autônomo (AS).

Os sistemas autônomos utilizados no *backbone* MPLS simulado foram de âmbito privado. De acordo com a recomendação da RFC 1930, o intervalo a ser usado para o sistema autônomo privado está entre 64512 e 65535, aqui foi usado 65500.

4.5. Configurações do MP-iBGP

A configuração do MP-BGP consiste em dois elementos:

- Configuração geral das sessões, como: *Neighbor address, Source interfaces, Remote AS number.*
- Configuração e ativação do *Addres Families* de VPNv4, incluindo as políticas associadas (*route-maps, filters,* etc).

Os vizinhos BGP precisam ser explicitamente ativados, pois não há uma descoberta automática de adjacência como no IS-IS. Por isso os vinhos BGP não precisam ser diretamente conectados. Para a ativação da sessão BGP segue:

- Configuração do processo BGP com o AS 65500: *router bgp 65500*
- O endereço de IP do vizinho e o número de *AS* remoto. O IP utilizado será o de *loopback* 0, e o número do AS é 65500: *neighbor x.x.x.x remote-as 65500.*
- Por padrão, o IOS utiliza o endereço IP da interface de saída em direção ao vizinho como IP de origem. Como utilizaremos para ambos vizinhos da mesma sessão um endereço de *loopback*, é preciso explicitamente configurar o comando a seguir, senão a sessão não se estabelece: *neighbor x.x.x.x update-source*

loopback 0

4.6. Configuração do *Address Family* VPNv4

Como já foi dito anteriormente, os prefixos de VPNv4 consistem em 32 bits do endereço IPV4 mais 64 bits do campo *route distinguisher* – RD (<*route-distinguisher*><*ip-address*>). A adição do RD permite a sobreposição de endereços IPs em VPNs distintas.

Essa atualização do *Address Family* além do prefixo de VPNv4 contem também um rótulo MPLS, que é o rótulo VPN, chamado de *inner label*; e alguns atributos de BGP *extended community*, como por exemplo os *route targets*, que são usados pelos roteadores PEs para construírem a topologia da VPN.

Os comandos a seguir são necessários para ativar a *Address* Family de VPNv4 para um vizinho. Todos eles devem ser executados dentro do *address-family* vpn4, no modo de configuração BGP.

- Ativar o vizinho dentro do *Address Family:neighbor x.x.x.x activete*.
- Habilitar o envio de atributo de *extended community* para os vizinhos: *neighbor x.x.x.x send-community extended*

4.7. Testes e analises

A seguir veremos todos os testes e configurações realizadas para a simulação proposta.

4.7.1. Configurações

Segue as configurações dos equipamentos de *backbone*:

Habilitar CEF	*Router(config) #ip cef [distributed]*

Configurar OSPF	*router ospf 1* *log-adjacency-changes* *network 172.10.0.1 0.0.0.0 area 0* *network 192.168.0.12 0.0.0.3 area 0* *network 192.168.0.20 0.0.0.3 area 0* *network 192.168.0.28 0.0.0.3 area 0*
Configurar BGP	*router(config) #router bgp autonomous-system*
Protocolo distribuição *label*	*router(config-router) #neighbor {ip-addres | peer-group-name} remote-as number*
Configurar interface MPLS	*router(config) #mpls label protocol ldp* *router(config) #interface interface-type number* *router(config-if) #mpls ip*

Tabela 1: Configurações dos protocolos em P1

Passo 1: Habilitar o CEF

O CEF é o acrômio para *Cisco Express Forwarding* (BOLLAPRAGADA et al, 2000). É basicamente utilizado para acelerar o processo de comutação dos roteadores, diminuindo a carga de processamento nos roteadores. É uma componente chave da arquitetura *Tag Switching* da Cisco System e passa a ser fundamental a sua utilização nos roteadores da Cisco ao se fazer uso da tecnologia MPLS. Em todos os roteadores do *backbone* devemos habilitar o CEF através do comando "ip cef" ou "*ip cef distributed*".

Passo 2: Configurar OSPF

É necessário configurar o protocolo OSPF em todos os roteadores do *backbone* MPLS. Como no exemplo a seguir temos a configuração para o PE1:

```
router ospf 1
log-adjacency-changes
networks 172.1.0.1 0.0.0.0 area 0
networks 192.168.0.12 0.0.0.3 area 0
networks 192.168.0.16 0.0.0.3 area 0
```

Passo 3: Configurar o BGP

Segue o exemplo das configurações de BGP para o roteador PE1:

```
router bgp 65500
no synchronization
redistribuited static
neighbor 172.2.0.1 remote-as 65500
neighbor 172.2.0.1 update-source loopback0
neighbor 172.2.0.1 next-hop-self
```

O comando "*redistributed static*" é utilizado sempre que houver rotas estáticas entre os CEs e os PEs, sendo necessária a redistribuição do tráfego para dentro do *backbone* MPLS. (OLIVEIRA, LINS e MENDONÇA, 2012).

Já o comando "*next-hop-self*" obriga o BGP a usar o seu próprio endereço BGP como próximo salto, em vez de deixar que o protocolo escolha. O comando *"no synchronization*" desativa a sincronização do protocolo BGP, assim o roteador anuncia externamente suas rotas vizinhas aprendidas pelo IBGP (*Interior Border Gatway Protocol).*

Passo 4: Definir o protocolo de distribuição de rótulos.

O LDP precisa ser configurado em todos os LSRs, segue a configuração apenas do PE1:

```
mpls label protocol ldp
```

Passo 5: Configurar MPLS na interface:

É preciso habilitar o comando para o encaminhamento do rótulo nas interfaces entre os PEs e o s Os através do comando "*mpls ip*" para a interface serial1/2 do PE1:

```
interface serial1/2
mpls ip
```

4.7.2. Teste de conectividade:

A seguir a figura 14 faz um teste de *ping* enviando pacotes ICMP do roteador CE13 para o CE21, comprovando assim que um pacote está atravessando uma parte de rede, no caso o LSP compreendido pelos nós PE1, P1 e PE2

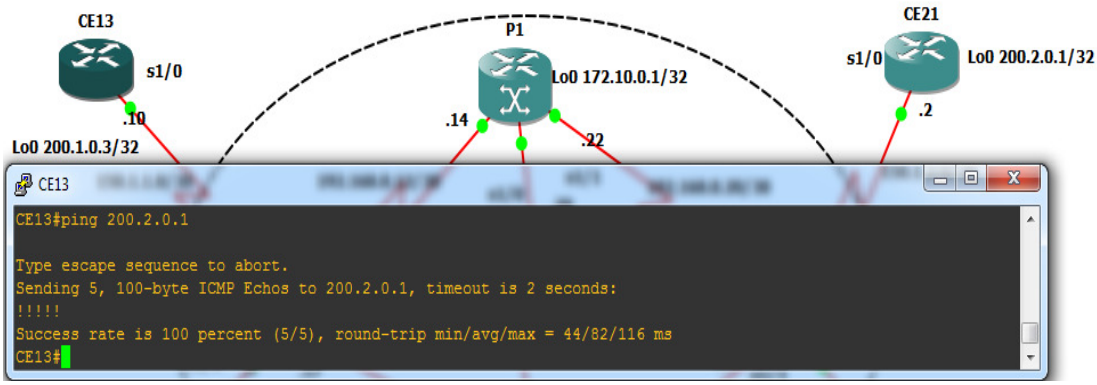


Figura 14: Teste de ping

FONTE: Próprio autor

4.7.3. Analise de Pacotes

Depois de validarmos a conectividade da rede, vamos capturar alguns pacotes no roteador P1 e verificar os tipos de protocolo rodando na rede e fazer algumas considerações

levando em conta a teoria apresentada até aqui.

Novamente fizemos um teste de *ping* entre o CE1 e o CE2 e ao capturar os pacotes da interface s1/1 do roteador P1, daí temos a figura 15 abaixo.

	Time	Source	Destination	Protocol	Length	Info
14	14.281030	192.168.0.22	224.0.0.2	LDP	66	Hello Message
15	15.241031	172.1.0.1	172.2.0.1	RSVP	212	PATH Message. SESSION: IPv4-LSP, Destination 172.2.0.1, Tunnel ID 0,
16	16.351033	192.168.0.21	224.0.0.5	OSPF	84	Hello Packet
17	17.086034	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 14, returned sequence 12
18	17.206034	192.168.0.21	224.0.0.2	LDP	66	Hello Message
19	18.046035	N/A	N/A	CDP	321	Device ID: P1 Port ID: Serial1/1
20	19.246037	192.168.0.22	224.0.0.2	LDP	66	Hello Message
21	20.576039	192.168.0.22	224.0.0.5	OSPF	84	Hello Packet
22	21.036040	192.168.0.21	224.0.0.2	LDP	66	Hello Message
23	23.671045	192.168.0.22	224.0.0.2	LDP	66	Hello Message
24	24.131046	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 13, returned sequence 14
25	24.581046	172.1.0.1	172.2.0.1	ICMP	104	Echo (ping) request id=0x0000, seq=0/0, ttl=254 (reply in 26)
26	24.601046	172.2.0.1	172.1.0.1	ICMP	108	Echo (ping) reply id=0x0000, seq=0/0, ttl=255 (request in 25)
27	24.651047	172.1.0.1	172.2.0.1	ICMP	104	Echo (ping) request id=0x0000, seq=1/256, ttl=254 (reply in 28)
28	24.671047	172.2.0.1	172.1.0.1	ICMP	108	Echo (ping) reply id=0x0000, seq=1/256, ttl=255 (request in 27)
29	24.691047	172.1.0.1	172.2.0.1	ICMP	104	Echo (ping) request id=0x0000, seq=2/512, ttl=254 (reply in 30)
30	24.701047	172.2.0.1	172.1.0.1	ICMP	108	Echo (ping) reply id=0x0000, seq=2/512, ttl=255 (request in 29)
31	24.731047	172.1.0.1	172.2.0.1	ICMP	104	Echo (ping) request id=0x0000, seq=3/768, ttl=254 (reply in 32)
32	24.741047	172.2.0.1	172.1.0.1	ICMP	108	Echo (ping) reply id=0x0000, seq=3/768, ttl=255 (request in 31)
33	24.771047	172.1.0.1	172.2.0.1	ICMP	104	Echo (ping) request id=0x0000, seq=4/1024, ttl=254 (reply in 34)
34	24.781047	172.2.0.1	172.1.0.1	ICMP	108	Echo (ping) reply id=0x0000, seq=4/1024, ttl=255 (request in 33)
35	25.701049	192.168.0.21	224.0.0.2	LDP	66	Hello Message
36	25.711049	172.2.0.1	172.10.0.1	LDP	62	Keep Alive Message
37	25.941049	172.10.0.1	172.2.0.1	TCP	44	53147 > ldp [ACK] Seq=1 Ack=19 Win=3724 Len=0
38	26.251049	192.168.0.21	224.0.0.5	OSPF	84	Hello Packet
39	26.351049	172.10.0.1	172.2.0.1	LDP	62	Keep Alive Message

Figura 15: Panorama geral de captura de pacotes pelo *wireshark*.

Fonte: Próprio autor, captura de *wireshark*

- LDP – *Label Distribuition Protocol*, como vimos ele permite que os roteadores se comunicam através do MPLS para troca de informações sobre rótulos. Durante a fase de descoberta, pacotes "*hello"* são enviados pela porta UDP 646 para "todos os roteadores da sub-rede" através do endereço de grupo de *multicast*, essa mensagem é possível ver na captura do pacote. Na linha 36 e 39 o LDP manda uma mensagem de "*Keep Alive*" para manter a conexão estabelecida.

- RSVP - O RSVP (*Resource reSerVation Protocol*), é um protocolo para a arquitetura de serviços integrado, usado para fazer reservas de recursos. O RSVP permite que os receptores individuais mudem livremente de canal e maximizem o uso da largura de banda ao mesmo tempo em que elimina o congestionamento.

- OSPF – *Open Shortest Path First* – é um protocolo de roteamento para redes IP, vemos que ele também usa um pacote de "hello" para descobrir seus vizinhos.

- SLARP - *Serial Line Address Resolution Protocol*, é um pacote do protocolo de camada de enlace de dados da Cisco.

- CDP – *Cisco Discovery Protocol*, é um protocolo proprietário de camada 2 desenvolvido pela Cisco System, sua principal função é a descoberta de equipamentos na rede, facilitando a compressão da topologia da rede e de sua arquitetura. Nesse caso notamos informações acerca do roteador onde ele está rodando, nome do roteador P1, e interface que está sendo monitorada Serial1/1.
- ICMP – *Internet Control Message Protocol*, é um protocolo típico de redes IP e é utilizado para gerar relatórios de erros à fonte original, nesse caso foi acionado pelo *ping* inicial que foi feito para o teste.

Conforme o objetivo proposto nesse trabalho, abordaremos em mais detalhes os protocolos específicos do MPLS-TE capturados pelo *wireshark*.

LDP

O LDP depende da informação de roteamento provida por um protocolo de roteamento interno para encaminhar os rótulos de pacote. O roteador através de uma FIB é responsável por determinar o caminho salto a salto. Ao contrário dos caminhos obtidos por engenharia de tráfego, que utilizam restrições e rotas explicitas para estabelecer um *Label Switched Paths* (LSPs) fim-a-fim, o LDP é utilizado apenas para sinalizar os caminhos (LSPs) de melhor custo/benefício.

Podemos observar isso na figura 16, e o id do LSR com melhor custo x benefício.

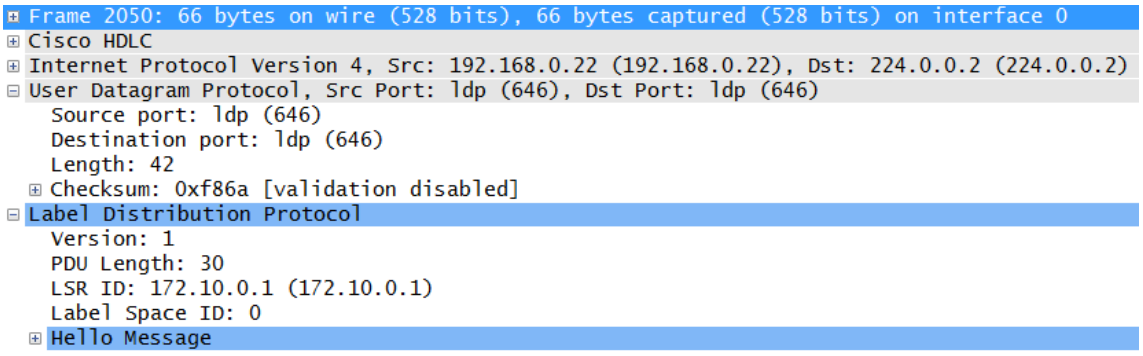


Figura 16: Estrutura do pacote LDP vista pelo *WireShark*

Fonte: Autor

RSVP-TE

Talvez um dos mais importantes protocolos de sinalização do MPLS-TE. Como já foi mencionado ele permite fazer reservas de recursos fim-a-fim para os fluxos de tráfego individuais.

O RSVP tem como suas principais mensagens:

- *Path*: Solicita um *Label* para uma FEC, incluindo restrições como: Rota explicita e Banda reservada ao longo do caminho. (Ingresso).
- *Resv*: Anuncia o *Label* caso a reserva possa ser atendida. (Egresso)

Já o RSVP-TE estende outras além dessas:

- O objeto "*Label Request*" na mensagem *Path*.
- O Objeto "*Label*" na mensagem *Resv*
- E dois novos tipos de classes: IPV4 LSP *Tunnel* e IPV6 LSP *Tunnel*.
- "Rota explícita" na mensagem de *Path*.
- "Registro de rota" na mensagem Resv ou *Path*
- "Atributo de Sessão" inclui prioridade na mensagem *Path*
- E mensagens de "*Hello*" trocadas entre os LSRs adjacentes para manter a conectividade.

Vamos poder ver no cabeçalho que tipo de mensagem é, no caso deste exemplo o *PATH*, a solicitação explicita de uma rota, no caso a 192.168.0.21 entre outros objetos que solicitam reserva de recursos, essa informação é enviada ao *tail head* SLP, ou seja, ao último roteador MPLS da borda de saída, e este envia uma resposta confirmando ou negando a reserva de recurso.

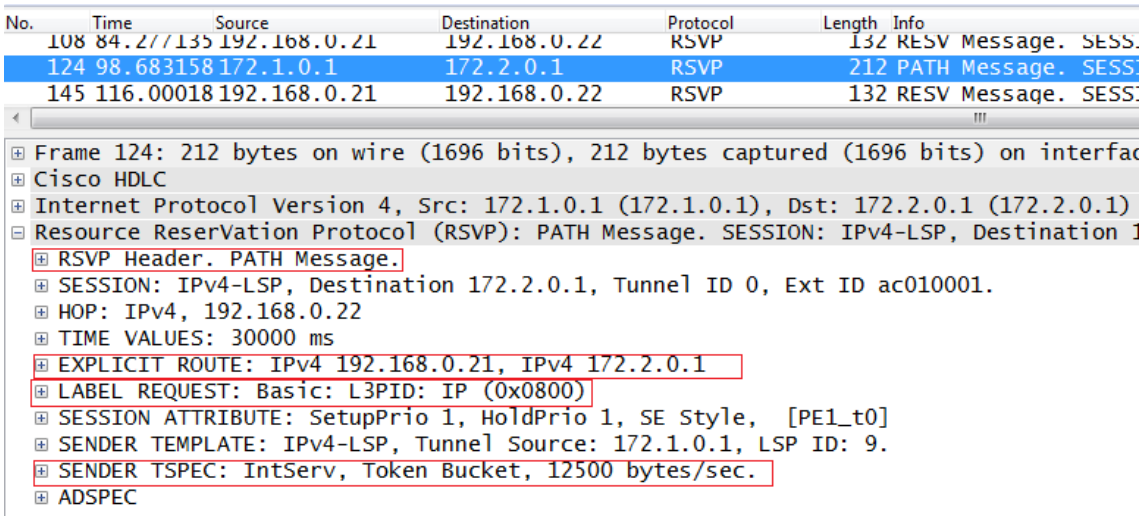


Figura 17: Detalhe do RSVP – PATH visto pelo *WireShark*

FONTE: Próprio autor

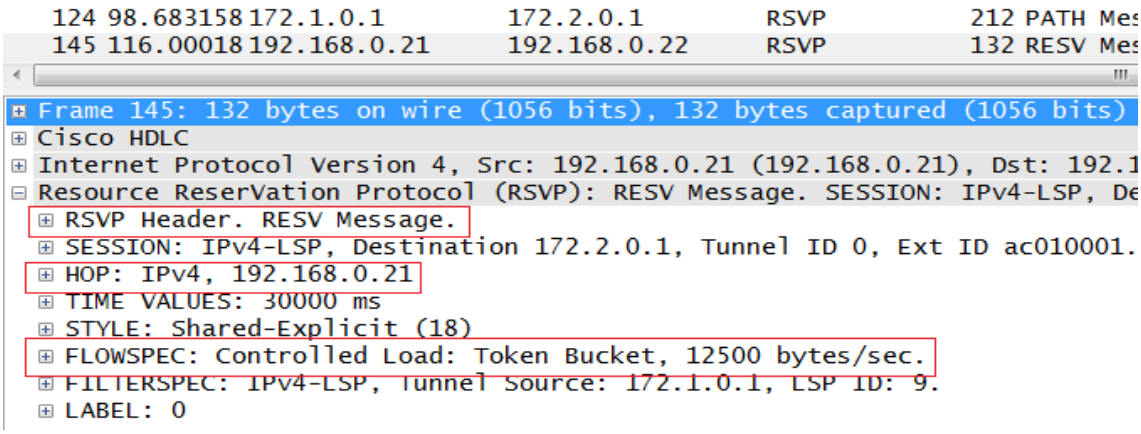


Figura 18: Detalhamento do RSVP-RESV no *WireShark*

FONTE: Próprio autor

Acima vermos que o tipo da mensagem é RESV, ou seja, a resposta da solicitação de PATH, já se encontra reservado o HOP solicitado o 192.168.0.21 e demais recursos reservados conforme solicitados.

Uma reserva em RSVP é caracterizada pela estrutura de dados chamada *FLOWSPEC* e esta é composta por dois elementos definidos na RFC 2210 e são opacos para o RSVP, são eles:

- Rspec (*Reserve Spec*) – Indica a classe de serviço desejada.
- Tspec (*Traffic Spec*) – Indica o que será transmitido.

O modelo utilizado pelo RSVP é o *Token Bucket*, este modelo é um método que é executado para definir uma taxa de transmissão variável com atraso limitado.

Assumindo o *Token Bucket Model, Tspec é* definido da seguinte forma:

- r – taxa média de bytes/s
- b – tamanho do *bucket* (bytes)
- p – taxa de pico
- m – tamanho mínimo do pacote
- M – MTU (tamanho máximo do pacote)

Regra: $T < rT + b$

Assumindo o *Token Bucket Model, Rspec* é definido da seguinte forma:

- R – taxa desejável – taxa média solicitada.
- s – Saldo (slack) de retardo – Valor excedente do atraso que pode ser

usado pelos nós intermediários.

Dentro do *FLOWSPEC* ainda podemos destacar o *Service Class* que indica o tipo de Serviço Garantido (REC2212- Há reserva de banda) ou Serviço de Carga de Controlada (RFC2211 – Não há reserva de banda).

A figura também revela outro objeto o *Filter Spec* que identifica os pacotes que devem receber o benefício da reserva, lá nós observamos o protocolo de transporte e a porta com o IP de origem.

Em nível de ilustração temos na figura 19 abaixo em uma mensagem RESV do protocolo RSVP-TE esses objetos em detalhes na simulação.

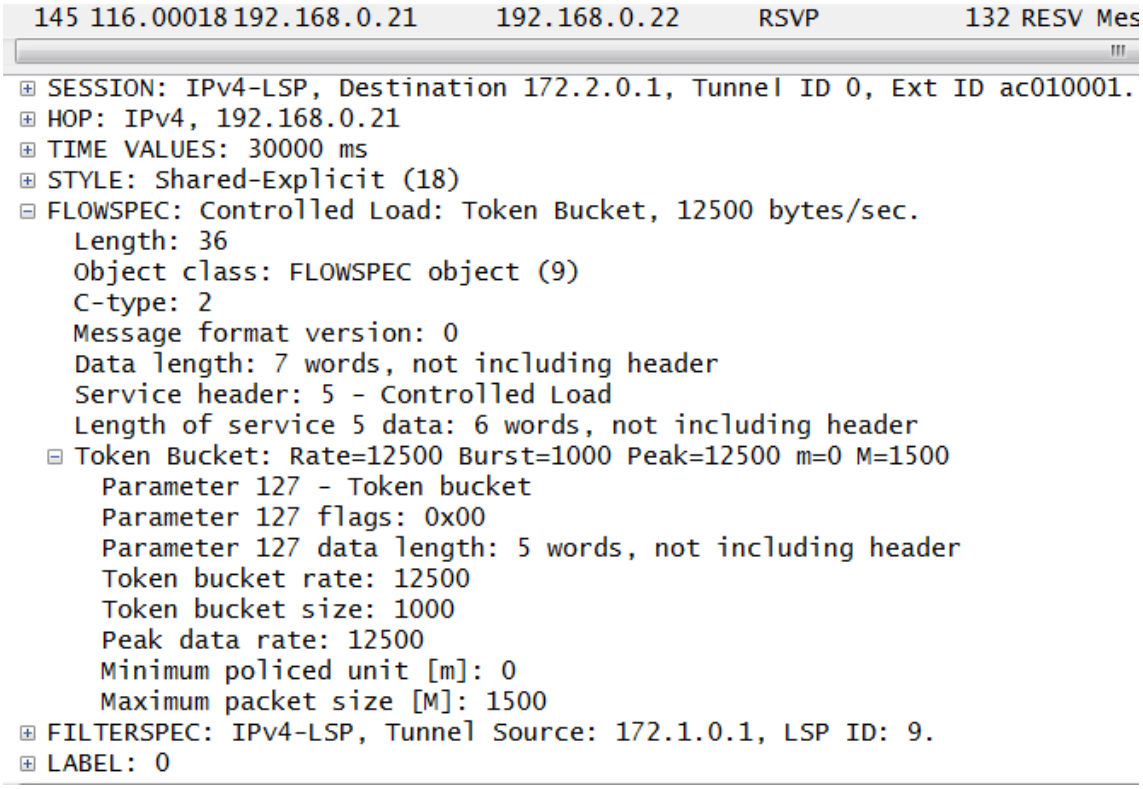


Figura 19: Detalhamento do RSVP – Flowspec e Token Bucket

Fonte: Próprio Autor

Na figura 19 podemos ver o objeto *FlowSpec* e o Modelo *Tokem Buck*et com todos seus parâmetros de resposta à solicitação de reserva.

CDP

Outro protocolo de camada 2 muito importante dentro do MPLS que podemos ver na captura inicial dos pacotes. O *Cisco Discovery Protocol* vem habilitado por padrão em todos os dispositivos da marca. É esse protocolo que tem o objetivo de descobrir informações sobre seus

vizinhos, dentre essas informações essas são as mais relevantes:

- **Identificação do Dispositivo:** Aqui conhecemos o nome ou o *hostname* do equipamento vizinho.
- **Interface Local:** Mostra por qual interface este dispositivo vizinho está conectado.
- **Plataforma:** Apresenta qual é a plataforma do dispositivo conectado, podemos ter plataforma 2500, 1700, 2950 entre outras.
- **Capacidade:** Mostra qual é exatamente o tipo de dispositivo ou sua função, como por exemplo, podemos ter roteadores, switches, bridges ou repetidores.
- **Identificação da Porta:** Qual o nome da porta do dispositivo vizinho.

Vamos agora verificar o tempo de atualização para a versão deste protocolo. Para isso usaremos o comando > Show cdp

O resultado é apresentado na figura abaixo.

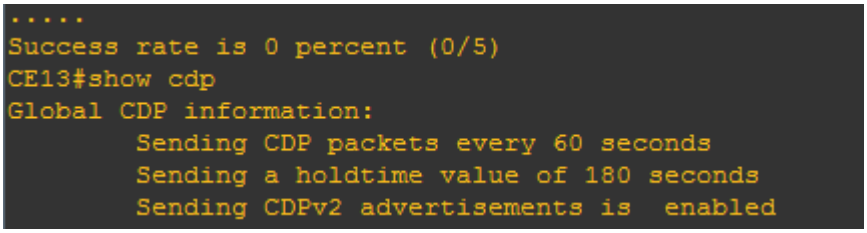


Figura 20: Print do comando Show cdp

Fonte: Próprio autor

Aqui vemos que a cada 60 segundo um pacote CDP é enviado.

Para visualizar os vizinhos do roteador P1 usamos o comando > *show cdp neghbors*

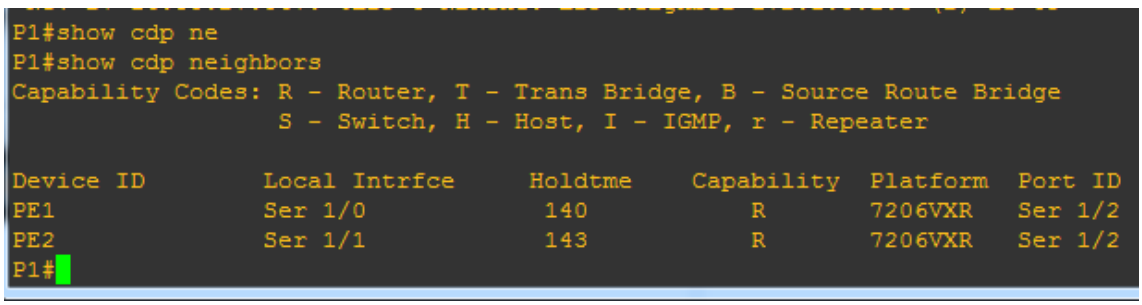


Figura 21: Vizinhos vistos pelo comando *cdp neghbor*

Fonte: Próprio autor

Na figura 21 acima vemos os vizinhos de P1 que são PE1 e PE2, suas respectivas interfaces e portas conectadas. P2 apesar de conectado diretamente a P1 está como *link backup*, sem tráfego e sem conexão no momento.

É possível utilizarmos o protocolo CDP para verificarmos o tráfego entre os dispositivos diretamente conectados, desta forma identificaremos algum problema relacionado à perda de pacotes neste link. O comando > ***show cdp traffic*** possui esta finalidade, veja a figura 21 abaixo:

```
P1#show cdp tra
P1#show cdp traffic
CDP counters :
        Total packets output: 494, Input: 490
        Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
        No memory: 0, Invalid packet: 0, Fragmented: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 494, Input: 490
P1#
```

Figura 22: Trafico entre dois vizinhos

Fonte: Próprio autor

Observamos que não há qualquer tipo de perda ou atraso na distribuição dos pacotes, considerando assim um enlace saudável. Vemos também que é feito testes de *checksum* (método para garantir a integridade dos dados baseado em um *hash*).

Também podemos monitorar este tráfego, o comando acima apresentado apenas lista a quantidade de pacotes enviados, recebidos e os erros que possam ter ocorrido naquele momento. Com o comando debug podemos certamente monitorar o tráfego de acordo com o tempo de atualização do CDP. Vale ainda lembrar que o *Cisco Discovery Protocol* envia suas atualizações a cada 60 segundos.

Na figura 22 abaixo temos a expansão de um dos protocolos LDP capturados pelo W*ireShark*, nele podemos ver que são enviadas informações bem específicas como modelo, marca, versão do software do equipamento, assim como as portas e interfaces a ele ligado e como já visto o *cheksum* e o ID do equipamento em questão. Informações importantíssimas para um gerente de redes que admitira um grande *backbone* heterogêneo, ou seja, que possua diversos modelos de equipamentos e versões de softwares.

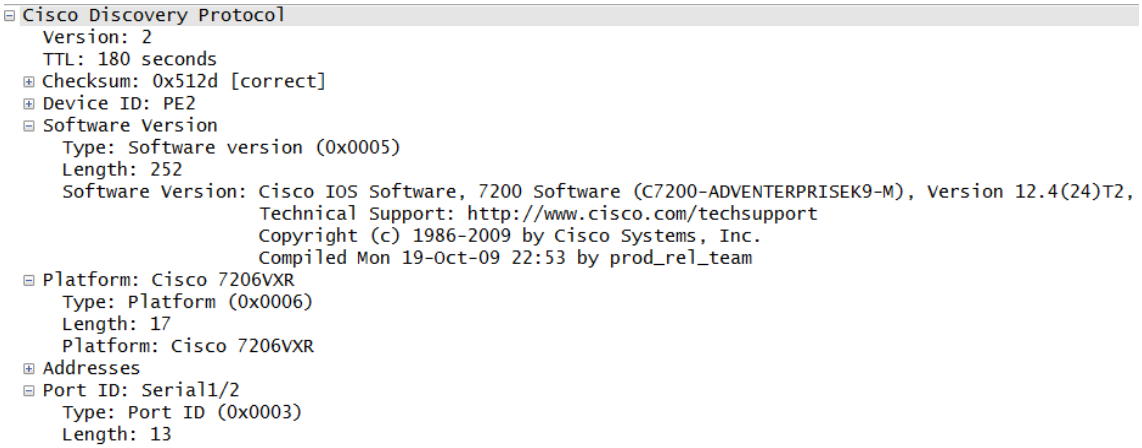


Figura 23: Informações vistas no LDP.

Fonte: Próprio Autor.

ICMP

Mesmo esse não sendo um protocolo do MPLS, vamos usá-lo para ilustrar o encapsulamento do pacote usando *labels* MPLS.

Na figura 23 a seguir vamos notar que a camada do MPLS precede as informações do TCP/IP, verificamos que o *label* deste pacote é o 18, depois segue as informações do datagrama IP e seus campos usuais.

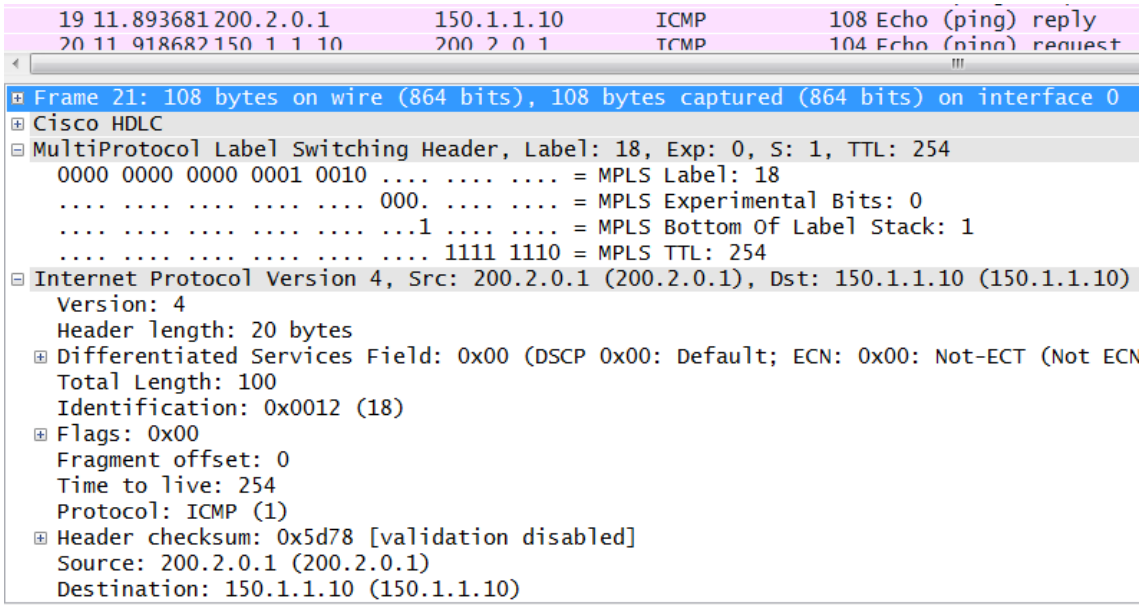


Figura 24: Pacote ICMP já com rótulos MPLS

Fonte: Próprio autor.

Apenas para fazer a comparação, fizemos uma captura dos mesmos pacotes ICMP no

CE21 já fora da nuvem MPLS e verificamos que estes já estão sem os rótulos, o que aconteceu no PE2.

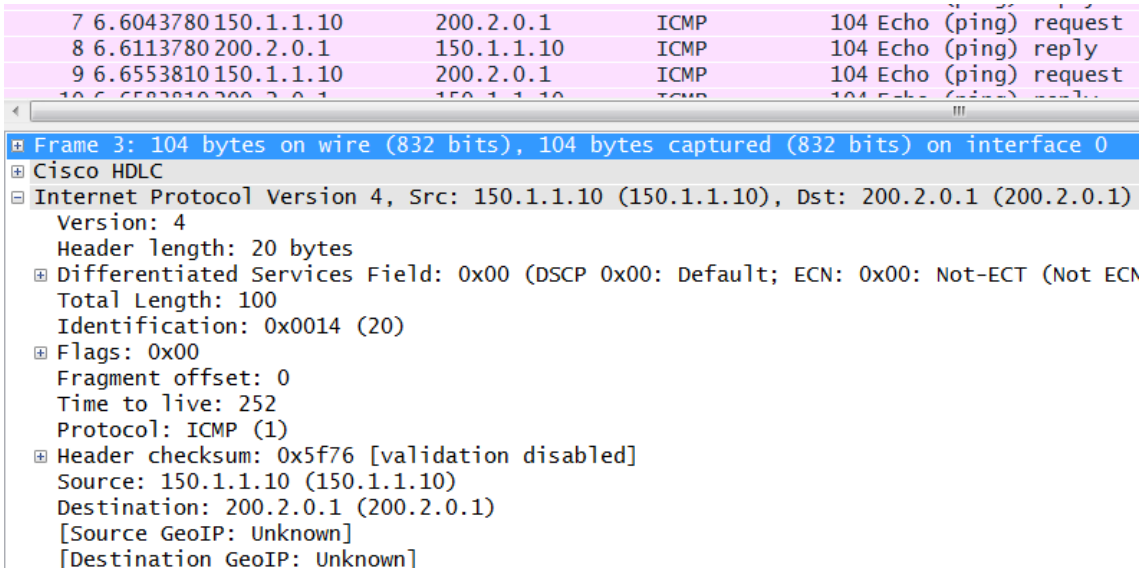
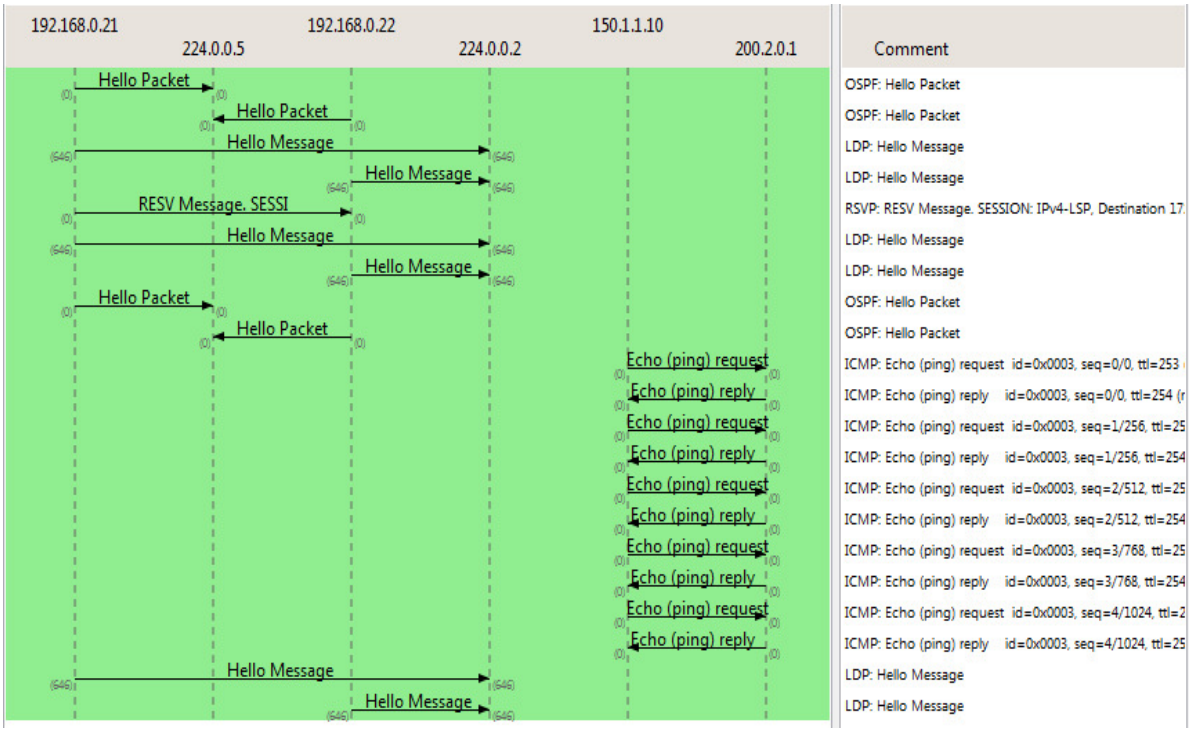


Figura 25: Pacote ICMP sem o rótulo MPLS

Fonte: Próprio autor

4.9. Conclusão da Análise

Veremos a seguir um resumo gráfico que o *WireShark* proporciona dos eventos abordados nessa simulação:



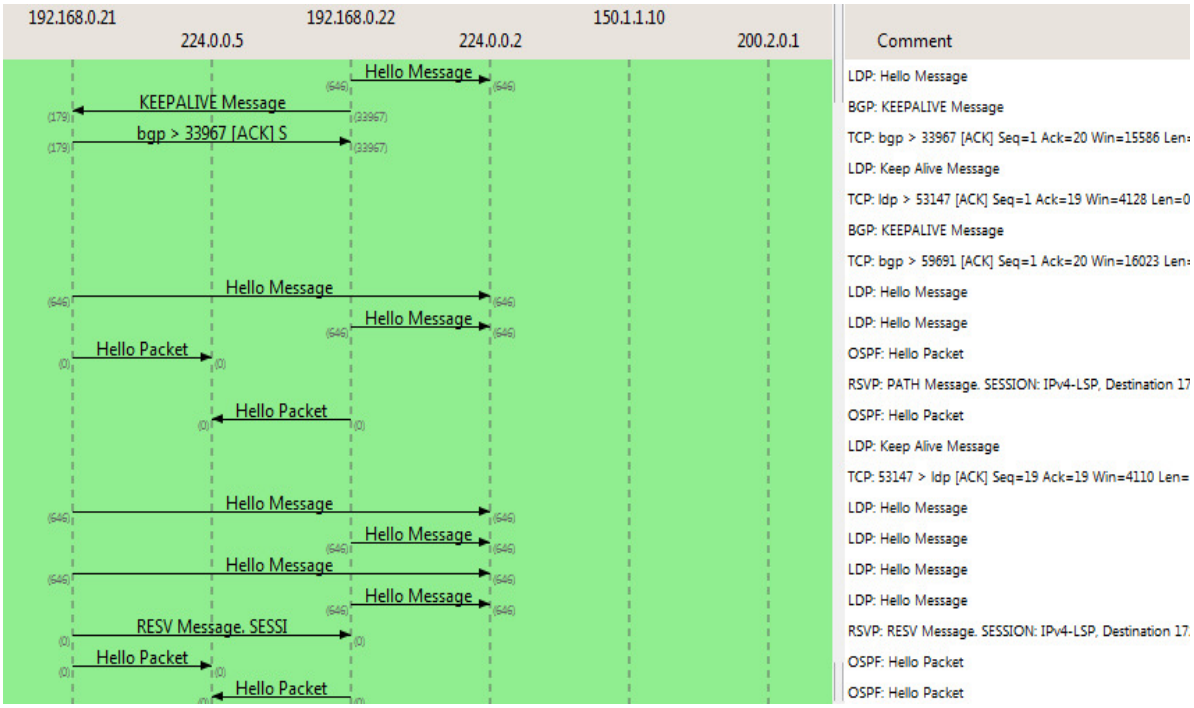


Figura 26: Troca de pacotes na simulação

Fonte: Próprio autor

Podemos ver que primeiramente o OSPF se estabelece trocando mensagens de *Hello*, depois o LDP descobrindo seus vizinhos com mensagens semelhantes, com os dados da topologia, estado dos enlaces promovidos pelo OSPF e LDP entra em cena o protocolo de sinalização RSVP que tenta abrir uma sessão, os ICMP se referem ao *ping* feito no teste, depois de algumas mensagens de "*keep alive*" tanto do OSPF quanto do LDP vemos que o RSVP finalmente manda uma solicitação de reserva de recurso usando a mensagem PATH, que tempos depois é respondida com uma mensagem de RESV, estabelecendo assim uma conexão MPLS-TE.

5. CONCLUSÃO

Este trabalho procurou apresentar inicialmente os conceitos básicos das Redes, os tipos e modelos que elas operam, os protocolos do Frame Relay e ATM, e os conceitos de roteamento e comutação. A seguir apresentou um breve histórico do surgimento do MPLS, e apresentou a Arquitetura MPLS, detalhando suas principais características e seu funcionamento, após esse embasamento teórico vimos o MPLS-TE, suas características, limitações e é claro, vantagens

dessa tecnologia no emprego das técnicas de Engenharia de tráfego, para respaldar esses conceitos, concluímos com sucesso uma simulação simples, porém que ampla o suficiente para que as características e protocolos dessa tecnologia fossem observados na prática.

Sem ter a pretensão de ter esgotado a discursão sobre o tema proposto, vimos que o MPLS possibilita a melhoria do desempenho no encaminhamento dos pacotes, já que existe uma separação do plano de controle do plano de dados. Existe um ganho na diminuição da latência, já que há roteamento e sim a comutação.

No MPLS há possibilidades de criações de tuneis. Tal mecanismo é importante para que muitos LSPs sejam tratados da mesma forma no núcleo da rede sem perder sua individualidade nas bordas. Dessa forma, tem-se um ganho na escalabilidade dos LSRs do núcleo.

Um dos usos mais importantes do MPLS é facilitar a engenharia de tráfego nas redes IPs de provedores de serviços de telecomunicações. A principal capacidade que o MPLS traz às redes com engenharia de tráfego é a possibilidade de configurar um circuito virtual *overlay* comutado para o modelo de roteamento de internet.

Porém a tecnologia MPLS possui algumas desvantagens como o aumento das informações de controle ocasionado pela adição de rótulos, como consequência disso há redução de carga útil das informações. Há também a desvantagem é que a conexão com o cliente e o provedor passa por uma conexão camada 3, herdado com isto suas vulnerabilidades. Por exemplo, a tabela de rotas do cliente pode ser vista no *backbone* MPLS.

Por isso é importante avaliar as necessidades da corporação os benefícios e as desvantagens da tecnologia, ai então decidir se é viável implantar ou não esse tipo de redes e a partir daí verificar a melhor abordagem para um projeto de redes, execução e manutenção como rege os princípios de qualquer tipo de engenharia.

5.1 Trabalhos Futuros

Para o futuro vemos que o MPLS caminha para um novo paradigma o GMPLS, (*Generalized Multi-Protocol Label Switching*) que é um conjunto de protocolos que se estende do MPLS para gerenciar novas classes de interfaces e de comutação diferente das interfaces de pacotes e comutação, tais como tecnologias de multiplexação por divisão de tempo, camada 2 comutação, comprimento de onda de comutação e comutação de fibras

O MPLS Generalizado é um conjunto de extensões aos protocolos de sinalização de engenharia de tráfego MPLS e aos protocolos de roteamento de engenharia de tráfego, como o objetivo de promover um conjunto padronizado e comum para controlar as redes de núcleo. GMPLS é desenvolvido sobre o MPLS porque as noções de comutação são muito semelhantes e devido à vantagem de potencializar a reconhecida tecnologia MPLS (Farrel, 2005).

Como toda tecnologia o MPLS ainda está em evolução e tenta acompanhar as tendências do mercado, sobretudo quanto aos novos meios de transmissão, tenteando contornar seus pontos frágeis e ficar cada vez mais transparente para o usuário final e mais prático e versátil para o gerente de redes.

REFERÊNCIAS

AWDUCHE, D. et al. ***Requirements for Traffic Engineering over MPLS***. RFC 2702, 1999.

BRENT D. Stewart. **CCNP BSCI – Official Exam Certification Guide**. 4ª ed. Indianápolis: Cisco Press, 2008.

B. FILHO, Huber. ***Asynchronous Transfer Mode*** **(ATM).** Teleco. Disponível em: **www.teleco.com.br**
Acesso em: 5 jul 2014.

ENNE, Antônio José Figueiredo. **TCP/IP sobre MPLS.** Rio de Janeiro: Ciência Moderna Ltda, 2009

FARREL, Adrian. **The Internet and Its Protocols**: a comparative approach. Massachusetts:

Morgan Kaufmann, 2005

GNS3. Disponível em: <htttps://www.gns3.org>. Acesso: 12/jan/2014

MORGAN, Brian; LOVERING, Neil. CCNP ISCW: ***Official Exam Certification Guide***. Indianapolis, USA: Cisco Press, 2008. 682 p.

MINOLI Daniel, SCHIMITED Andrew, **Internet Architectures**, ed: Wiley, 1998 (pg 241)

OLIVEIRA Jose; LINS Rafael; MENDONÇA Roberto, **Redes MPLS, Fundamentos e Aplicações** 2012: Brasport

OSBORN Eric, SIMHA Ajay, **Engenharia de tráfego com MPLS**, 2002: Ciscopress.

PRETO, Gerson. **Rede MPLS, Tecnologias e Tendências de Evoluções Tecnológicas.** Novembro 2008. Disponível em http://www.lume.ufrgs.br/bitstream/handle/10183/15971/000695253.pdf?sequence=1 Acesso em 22 de Fev. 2014.

RICCI, Bruno. **Redes Seguras: VPN Linux**. 1 ed. Ruio de Janeiro: Ciência Moderna, 2007

SUARES Luiz Fernando G., COLCHER Sergio, **Redes de computadores: Das LANS às Redes ATM**, 1995, Editora CAMPUS

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet: uma abordagem top-down**. 3. ed. São Paulo, SP: Pearson Addison-Wesley, 2006.

VEIGA, Miguel Ângelo. **Simulação de redes MPLS: Uma perspectiva pedagógica.** 2009 Dissertação (Mestrado em Engenharia Eletrônica e Telecomunicações) – Departamento de Eletrônica, Telecomunicações e Informática. – Universidade de Aveiro, Portugal 2009.

WIRESHARK. Disponível em: https://www.wireshark.org Acesso: 25 de out 2014

http://docwiki.cisco.com/wiki/Frame_Relay Acesso 12 jul 2014