

**UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ  
DEPARTAMENTO ACADÊMICO DE INFORMÁTICA  
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES**

**ANDRÉ GIACOMELLI ZANON**

**COMPARATIVO ENTRE AS TÉCNOLOGIAS FRAME RELAY E MPLS  
VPN EM CAMADA 3**

**TRABALHO DE CONCLUSÃO DE CURSO**

**PATO BRANCO  
2015**

**ANDRÉ GIACOMELLI ZANON**

**COMPARATIVO ENTRE AS TÉCNOLOGIAS FRAME RELAY E MPLS  
VPN EM CAMADA 3**

Trabalho de Conclusão de Curso, apresentado ao II Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes, da Universidade Tecnológica Federal do Paraná, câmpus Pato Branco, como requisito parcial para obtenção do título de Especialista

Orientador: Prof. MSc. Adriano Serckumecka

**PATO BRANCO  
2015**

## TERMO DE APROVAÇÃO


### Comparativo entre as Tecnologias Frame Relay e MPLS VPN em Camada 3

por

**Andre Giacomelli Zanon**

Esta monografia foi apresentada às 16h00min do dia 27 de outubro de 2015, como requisito parcial para obtenção do título de ESPECIALISTA, no II Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes, da Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. O acadêmico foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho **aprovado**.

Banca Examinadora



---

Prof. M.Sc. Adriano Serckumecka  
Orientador / UTFPR-PB



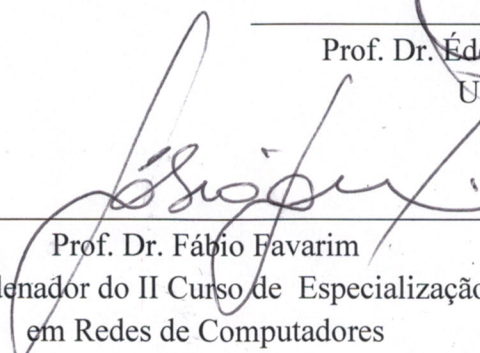
---

Prof. Dr. Fábio Favarim  
UTFPR-PB



---

Prof. Dr. Éden Ricardo Dosciatti  
UTFPR-PB



---

Prof. Dr. Fábio Favarim  
Coordenador do II Curso de Especialização  
em Redes de Computadores

Dedico este trabalho às pessoas mais importantes da minha vida: meus pais Olga e Aldo e a meu irmão Tiago, que confiaram no meu potencial para esta conquista. Não conquistaria nada se não estivessem ao meu lado. Obrigado, por estarem sempre presentes a todos os momentos, me dando carinho, apoio, incentivo, determinação, fé, e principalmente pelo Amor de vocês.

## **AGRADECIMENTOS**

Agradeço à Deus por todas as oportunidades que me proporciona para prosseguir a missão de minha vida.

Agradeço à minha família, especialmente meus pais Olga e Aldo Zanon que com muito carinho e apoio, não mediram esforços para que eu chegasse até esta etapa de minha vida.

Agradeço à meu orientador prof. Adriano, pelas palavras de sabedoria e paciência que me guiou nesta trajetória.

Agradeço à todos os professores do curso, que foram tão importantes na minha vida acadêmica e no desenvolvimento desta monografia.

Agradeço a todos os colegas, pela convivência, amizade e companheirismo.

E, agradeço à todos que contribuíram, mesmo indiretamente para a conclusão desta especialização.

Temos o destino que merecemos. O nosso destino está de acordo com nossos méritos.

Albert Einstein

## RESUMO

ZANON, André Giacomelli. Comparativo entre as tecnologias Frame Relay e MPLS em camada 3. 2015. 52 f. Monografia de Trabalho de Conclusão de Curso (II Curso de Especialização em Redes de Computadores), Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. Pato Branco, 2015.

Com o avanço das redes de computadores na utilização de aplicações avançadas, surgiu a necessidade de uma tecnologia capaz de fornecer velocidade, escalabilidade, gerenciamento de qualidade de serviço (QOS) e engenharia de tráfego por um melhor custo/benéfico, comparando com tecnologias de Rede Núcleo como Frame Relay. A tecnologia MPLS (*Multi-protocol Label Switching*) é capaz de garantir que cada pacote de dados seja entregue ao seu destino com sua devida prioridade, aproveitando o máximo os recursos da rede. Este trabalho tem como objetivo abordar o conceito de MPLS, suas vantagens e desvantagens, uma breve comparação com outras tecnologias como Frame Relay e finalmente demonstrar a aplicação prática usando o simulador de redes GNS3 com foco em MPLS VPN (*Virtual Private Networks*).

**Palavras-chave:** MPLS, VPN, Multi-protocol Label Switching, MPLS VPN.

## ABSTRACT

ZANON, André Giacomelli. Comparing the technologies Frame Relay and MPLS Layer 3. 2015. 52 f. Monografia de Trabalho de Conclusão de Curso (II Curso de Especialização em Redes de Computadores), Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. Pato Branco, 2015.

With the advancement of computer networks in advanced applications, the need for a technology to provide speed, scalability, quality of service management (QoS) and traffic engineering for a better cost / benefit compared to network technologies core as Frame Relay. The MPLS (*Multi-protocol Label Switching*) is able to ensure that each data packet to be delivered to its destination with its due priority, taking advantage of the maximum network resources. This paper aims to address the concept of MPLS, its advantages and disadvantages, a brief comparison with other technologies such as Frame Relay and finally demonstrate the practical application using the simulator GNS3 networks focusing on MPLS VPN (*Virtual Private Networks*).

**Keywords:** MPLS, VPN, Multi-protocol Label Switching, MPLS VPN.

## LISTA DE FIGURAS

FIGURA 1 - ROTEAMENTO IP TRADICIONAL .....	12
FIGURA 2 - VPN FIM A FIM .....	15
FIGURA 3- ENCAPSULAMENTO (RÓTULO MPLS) .....	19
FIGURA 4 - ESQUEMA DE FUNCIONAMENTO DE UMA ASSOCIAÇÃO FEC A UM PACOTE.....	20
FIGURA 5 - OPERAÇÃO DO MPLS.....	22
FIGURA 6 - FRAME RELAY .....	23
FIGURA 7 - TOPOLOGIA FULL-MESH.....	24
FIGURA 8 - TOPOLOGIA HUB-AND-SPOKE .....	25
FIGURA 9 - PROTOLOCOS DE ROTEAMENTO EM L3 VPN.....	26
FIGURA 10 - ARQUITETURA MPLS VPN .....	27
FIGURA 11- CENÁRIO MPLS/VPN L3 GNS3.....	35

## LISTA DE QUADROS

QUADRO 1 - TIPOS DE ROTEAMENTO IP .....	17
QUADRO 2 - CRIAR VRF.....	37
QUADRO 3 - ATRIBUIR VRF .....	37
QUADRO 4 - ROTEAMENTO BGP .....	38
QUADRO 5 - VERIFICAR BGP .....	38
QUADRO 6 - VERIFICAR MP-BGP.....	39
QUADRO 7 - ROTEAMENTO OSPF.....	40
QUADRO 8 - ROTAS VRF .....	41
QUADRO 9 - REDISTRIBUIÇÃO DE ROTAS .....	42
QUADRO 10 - ROTAS CLIENTE A.....	42
QUADRO 11 - REDISTRIBUIÇÃO BGP NO OSPF.....	43
QUADRO 12 - ROTAS VRF CLIENTE A E B .....	43
QUADRO 13 - TESTE PING.....	44
QUADRO 14 -TESTE TRACEROUTE.....	44

## LISTA DE ABREVIATURAS E SIGLAS

QoS	<i>Quality of Service</i>
TE	<i>Traffic Engineering</i>
MPLS	<i>Multiprotocol Label Switching</i>
VPN	<i>Virtual Private Network</i>
WAN	<i>Wide Area Network</i>
ATM	<i>Asynchronous Transfer Mod</i>
CE	<i>Customer Edge</i>
PE	<i>Provider Edge</i>
P	<i>Provider</i>
SLA	<i>Service Level Agreement</i>
CoS	<i>Class of Service</i>
EIGRP	<i>Enhanced Interior Gateway Routing Protocol</i>
OSPF	<i>Open Short Path First</i>
BGP	<i>Border Gateway Protocol</i>
LSP	<i>Label Switch Path</i>
TTL	<i>Time To Live</i>
LDP	<i>Label Distribution Protocol</i>
LSR	<i>Label Switch Router</i>
LFIB	<i>Label Forwarding Information Base</i>
FEC	<i>Forwarding Equivalence Class</i>
RD	<i>Route Distinguisher</i>
RT	<i>Route-Target</i>
DTE	<i>Data Terminal Equipments</i>
DCE	<i>Data Communication Equipments</i>

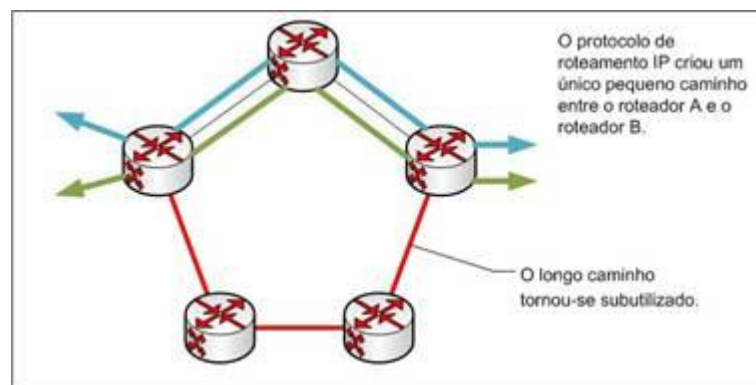
## SUMÁRIO

1 INTRODUÇÃO .....	12
1.2 OBJETIVOS .....	13
1.2.1 Objetivo Geral.....	13
1.2.2 Objetivos Específicos .....	13
1.3 JUSTIFICATIVA .....	14
1.4 ESTRUTURA DO TRABALHO.....	15
2 REFERENCIAL TEÓRICO.....	16
2.1 UM BREVE HISTÓRICO DO SURGIMENTO DA TECNOLOGIA .....	16
2.2 CONCEITO MPLS.....	17
2.3 CABEÇALHO E COMPONENTES DO MPLS.....	18
2.4 FRAME RELAY .....	23
2.5 MPLS VPN .....	25
2.6 MPLS VPN CAMADA 3.....	26
2.7 CARACTERÍSTICAS FRAME RELAY E MPLS – PRINCIPAIS OPERADORAS	28
2.8 COMPARATIVO ENTRE AS TECNOLOGIAS FRAME RELAY E MPLS. ....	32
3 MATERIAIS E MÉTODO .....	33
3.1 MATERIAIS .....	33
3.2 MÉTODO.....	34
4 RESULTADOS .....	35
5 CONCLUSÃO.....	47
REFERÊNCIAS.....	49

## 1 INTRODUÇÃO

Com o avanço crescente das redes de computadores e aplicações que exigem cada vez mais desempenho com qualidade de serviço (QoS) e mecanismos confiáveis de engenharia de tráfego (TE) como por exemplo em transmissão de áudio e vídeo foi necessário o desenvolvimento de uma nova tecnologia que pudesse resolver alguns problemas dos roteadores IP tradicionais que trabalham com uma forma de roteamento ineficiente, pois a medida que a rede cresce para definir o próximo salto (*hop*) do pacote, cada roteador precisa analisar mais informações do que realmente é necessário, além do mais cada roteador realiza o mesmo processo que muitas vezes é semelhante para todos os roteadores, isso se torna ineficiente devido ao fato que a grande parte dos pacotes IP pertencem a fluxos de pacotes com o mesmo destino e origem.

A Figura 1 demonstra o funcionamento de um roteador IP tradicional que utiliza o caminho mais curto, porém não identifica se é o menos congestionado ou melhor, subutilizando o caminho mais longo.



**Figura 1 - Roteamento IP Tradicional**

Fonte: ROCHA (2015).

O MPLS (*Multiprotocol Label Switching*) é uma tecnologia recente que tem como objetivo encaminhar dados através de comutação de rótulos, os roteadores de borda, verificam os pacotes, criando rótulos (*labels*) que são utilizadas para enviar os pacotes de dados até o destino final. Assim a maior parte do processamento dos pacotes é feito nas bordas da rede, diminuindo o processamento do núcleo (AIRES 2004).

Segundo Melo Filho et al (2008), o Frame Relay, é uma tecnologia consolidada no Brasil, visto que está em uso desde a década de 90, porém com o avanço da Internet e redes de computadores foi necessária uma maior disponibilidade de banda, com escalabilidade e maior qualidade de serviços como QoS.

Logo, o MPLS vem se tornando uma tecnologia de comutação atrativa para uso de VPNs em operadoras de telecomunicações que desejam separar os tipos de dados de usuários comuns do tráfego complexo.

## 1.2 OBJETIVOS

O objetivo desse trabalho é apresentar o conceito da tecnologia MPLS, suas vantagens e desvantagens, uma breve comparação com a tecnologia Frame Relay com foco principal em MPLS VPN, demonstrando na prática como funciona uma VPN utilizando a rede MPLS e quais suas principais características.

### 1.2.1 Objetivo Geral

Analisar a tecnologia MPLS e comparar com Frame Relay, implementando no simulador GNS3 um cenário de MPLS VPN.

### 1.2.2 Objetivos Específicos

Para alcançar o objetivo geral, os seguintes objetivos específicos foram definidos:

- Analisar as funcionalidades da tecnologia MPLS e sua aplicabilidade à VPNs.
- Comparar MPLS VPN com Frame Relay VPN, levantando suas vantagens, desvantagens e as principais características.

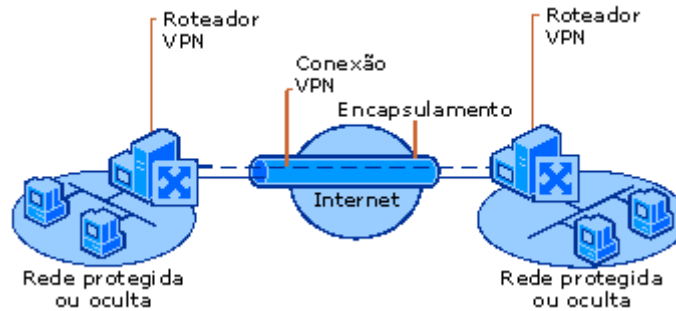
- Elaborar um protótipo para interligação de pontos entre matriz e filiais através de MPLS VPN.
- Realizar uma simulação do protótipo elaborado, através do simulador GNS3, demonstrando seu funcionamento.

### 1.3 JUSTIFICATIVA

O Frame Relay foi um meio barato para conectar redes WAN difundindo no início da década de 90 e utilizando até hoje. No entanto, com a chegada de redes óticas de transporte, virtualização e VPN, combinado com o próprio favorecimento de IP de próxima geração (protocolo Internet) houve a necessidade de buscar novas tecnologias capaz de atender às diversas necessidades dos usuários de redes, desde pequenas empresas que utilizam a rede para negociar com clientes e fornecedores, até as grandes que estejam implementando uma VPN global, assim o MPLS tem como objetivo resolver os problemas atuais como: velocidade, escalabilidade, gerenciamento de qualidade de serviço (QoS) e a necessidade de engenharia de tráfego.

A tecnologia MPLS reduz significativamente a necessidade de tecnologia de camada de enlace de dados, tais como frame relay, modo de transferência assíncrona (ATM) e Ethernet. A tecnologia de camada de enlace de dados é significativamente complexa e caro em comparação com a tecnologia MPLS VPN, que permite às empresas ter uma conexão direta com os locais geográficos sem a aquisição de quaisquer circuitos físicos para ele.

O problema das VPN's é a limitação da topologia física e a base de circuito virtuais (*tuneis fim a fim*), conforme mostra a Figura 2, entre cada par de roteadores de cliente para cada VPN, encontramos grande dificuldades na questão de gerenciamento e flexibilidade, assim como no crescimento da rede, pois cada novo ponto, precisa ser conectado a todos os demais existentes e ao longo do tempo o gerenciamento de tudo ficaria muito complicado.



**Figura 2 - VPN fim a fim**

Fonte: MICROSOFT (2015).

No MPLS VPN todos os pontos de uma VPN, são conexões IP que fazem parte de uma "nuvem" em que apenas membros da mesma VPN tem acesso. Essas "nuvens" são implementadas através de caminhos LSP'S criados no mecanismo de rótulos. Além disso, permite as operadoras criar serviços de VPN com garantia de segurança e privacidade.

#### 1.4 ESTRUTURA DO TRABALHO

Este trabalho está dividido em cinco capítulos, dos quais este apresentou a introdução os objetivos e a justificativa.

O Capítulo 2 contém o Referencial Teórico, o qual fundamenta o tema proposto, com um breve histórico da tecnologia, bem como conceito e componentes, além de uma comparação entre MPLS VPN e Frame Relay, com suas principais características, vantagens e desvantagens.

O Capítulo 3 apresenta os matérias e métodos utilizados para o desenvolvimento desse projeto.

No Capítulo 4 são apresentados as configurações e resultados obtidos através dos métodos utilizados para elaborar o trabalho.

Por último, no Capítulo 5 são apresentadas as conclusões.

## 2 REFERENCIAL TEÓRICO

### 2.1 UM BREVE HISTÓRICO DO SURGIMENTO DA TECNOLOGIA

Quando foi lançada a tecnologia ATM na década de 90, se tornou dominante, principalmente por ter um alto desempenho e velocidade, porém não era compatível com o TCP/IP, padrão que logo se popularizou nas redes de computadores. Nessa mesma época começaram as pesquisas da chamada "comutação IP".

Alguns pesquisadores de fabricantes chegaram à conclusão que não era necessário rotear pacotes IPS no núcleo da rede e além do mais, era possível adquirir qualidade de serviço por meio de comutação de pacotes IP, que seria feita através de rótulos adicionado a cada pacote. (OLIVEIRA, LINS e MENDONÇA, 2012).

Logo começaram a ser criadas, diversas tecnologias de comutação de pacotes, entre elas: IP Navigator (Ascend) (Davie e Rekhter, 2000), CSR – Cell Switched Router (Toshiba), IP Switching (Ipsilon) (Newman et al, 1996) e Tag Switching Architecture (Cisco) (Rekhter et al, 1997), No final de 1996 a IETF (*Internet Engineering Task Force*) grupo de padronização internacional, entrou em cena para desenvolver uma tecnologia padrão de comutação de dados, onde qualquer fabricante poderia implementar.

Assim surgiu o MPLS, com objetivo de padronizar a comutação de pacotes em troca de rótulos, usando o mesmo esquema de endereçamento IP de roteamento nas redes e dos hosts, melhorando a eficiência de fluxos de tráfegos através da rede e interligação de redes com tecnologias distintas.

## 2.2 CONCEITO MPLS

O MPLS é definido como um conjunto de características que são adicionadas a um processo de roteamento.

O MPLS é uma tecnologia aberta que foi apresentada inicialmente como uma solução que possibilitava melhorar o desempenho das redes IPs na função de encaminhamento de pacotes IPs, combinando o processo de roteamento de nível 3 com a comutação de nível 2 para realizar o encaminhamento de data gramas através de pequenos rótulos de tamanho fixo. Tais rótulos são números utilizados no protocolo MPLS e, através destes, a decisão de qual interface encaminhar o data grama é tomada (Rosen et al, 2001a).

O MPLS usa a técnica de comutação de rótulos para encaminhar dados na rede. Um cabeçalho de formato fixo é adicionado em cada pacote que entra na rede MPLS. Em cada salto (*hop*) o pacote é encaminhado com base no rótulo de entrada e enviado por uma interface de saída com o novo valor do rótulo.

O Quadro 1 apresenta um comparativo entre as tecnologias de roteamento IP tradicionais e baseados em rótulos, demonstrando as características de cada uma.

<b>Tipos de roteamento IP</b>		
	<b>Convencional</b>	<b>Baseado em rótulos</b>
<b>Análise de todo cabeçalho IP</b>	Verificação dos pacotes a cada salto em todo caminho na rede.	Verificação dos pacotes apenas uma vez no ingresso do caminho virtual.
<b>Suporte para dados Unicast e Multicast</b>	Necessita de roteamento especial para Multicast e algoritmos de encaminhamento.	Necessita de somente um algoritmo de encaminhamento.
<b>Decisão de roteamento</b>	Baseado no endereço de destino no cabeçalho do pacote IP.	Baseado em vários parâmetros: endereço de destino no cabeçalho IP, QoS, tipo de dados, etc.

**Quadro 1 - Tipos de roteamento IP**

Fonte: (OLIVEIRA, LINS e MENDONÇA, 2012)

Cada pacote que entra na rede MPLS é examinado para determinar qual caminho por onde os pacotes irão passar em uma rede MPLS (LSP (*Label Switch Path*)), vai ser associado e qual rótulo adicionado no pacote. Esta decisão é feita com base em fatores como: estado atual da rede, qualidade de serviço ou endereço de destino. (OSBORNE, 2002).

Uma rede MPLS não tem como objetivo a conexão direta a sistemas finais, mas sim o transporte de pacotes entre pontos de entrada e saída.

### 2.3 CABEÇALHO E COMPONENTES DO MPLS

#### Label (Rótulo)

O rótulo é definido na RCF 3031 "*Multiprotocol Label Switching Architecture*" como "um identificador curto, de tamanho fixo (32 bits) e localmente significativo que é utilizado para identificar uma FEC" isto é, um grupo de pacotes IPs que são enviados na mesma maneira, sobre o mesmo trajeto e com o mesmo tratamento de transmissão (OLIVEIRA, LINS e MENDONÇA, 2012, p.29).

O rótulo MPLS deve ser inserido em um pacote de dados, depois de qualquer cabeçalho de camada dois e antes de um cabeçalho de camada três (ABREU, 2004).

A estrutura de encapsulamento MPLS possui os seguintes campos (KAKIHARA, 2006):

Um rótulo de 20 bits; Existem alguns valores que são reservados ao protocolo e têm significados especiais (Rosen et al, 2001b).

- 0 – *IPv4 Explicit NULL Label*: indica que o rótulo deve ser retirado, e, desse ponto em diante, o roteamento será feito com base no endereço de rede.
- 1 – *Router Alert Label*: indica que o datagrama deve ser analisado pelo software local. O encaminhamento seguinte é definido pelo próximo rótulo da pilha MPLS.

- 2 – *IPv6 Explicit NULL Label*: mesma funcionalidade do valor 0, mas aplicada ao protocolo IPv6.
- 3 – *Implicit NULL Label*: valor utilizado pelos LSRs (*Label Switch Routers*) para a distribuição de rótulos (*LDP – Label Distribution Protocol*).
- 4 a 15 – Reservados para definições futuras.
- 16 a (220 -1) – Rótulos utilizáveis para roteamento.

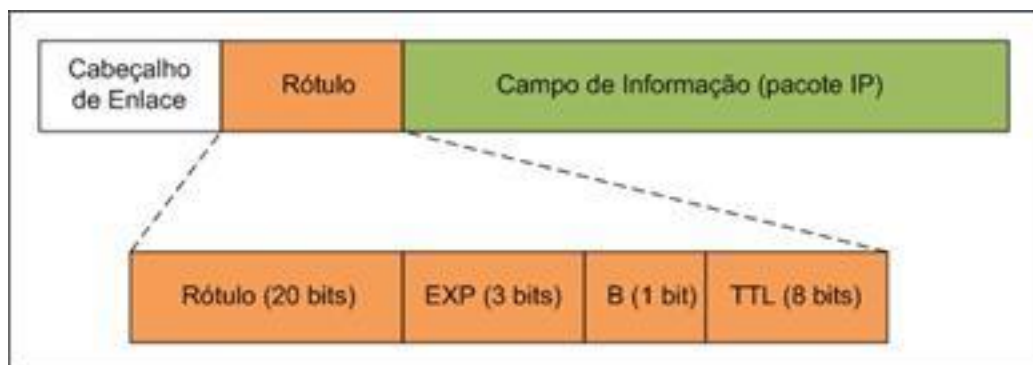
EXP (*Experimental Bits*): Um campo experimental de 3 bits, utilizado para classes de serviço.

TTL (*Time To Live*): Um campo TTL (*Time to Live*) de 8 bits, que fornece funcionalidades de TTL IP (*Time To Live*) convencional.

BoS (*Bottom of Stack*): Um campo B de 1 bit, utilizado para suportar uma pilha hierárquica de etiquetas, informando se o cabeçalho ao qual ele pertence é o último da pilha MPLS.

Todos os cabeçalhos MPLS devem ter esse bit em 0, e através desse campo um roteador de saída tem condições de decidir se o próximo encaminhamento será baseado em MPLS ou IP (OLIVEIRA, LINS e MENDONÇA, 2012, p. 30).

A Figura 3 demonstra os campos de um rótulo MPLS.



**Figura 3 - Encapsulamento (Rótulo MPLS)**

Fonte: ROCHA (2011).

## Componentes do MPLS

LDP (*Label Distribution Protocol*): Tem como função distribuir rótulos para os prefixos IP da rede MPLS.

Oliveira et al, (2012), descreve que todos os prefixos anunciados por um mesmo equipamento vizinho recebem o mesmo rótulo.

Assim, os elementos intermediários em uma rede MPLS não precisam conhecer a tabela de roteamento completa da rede. Um pacote IP com rótulo é encaminhado para o próximo enlace (*next-hop*) baseado somente no rótulo externo, isto é, aquele alocado pelo LDP com base na tabela de roteamento, e isso ocorre até a chegada à rede de destino.

**LIB (*Label Information Base*):** Tabela onde se armazenam os vínculos de rótulos que um LSR (*Label Switch Router*) recebe do LDP, ou seja, relaciona rótulos às interfaces do roteador e também é através desta tabela que é determinado qual interface o LSR deverá enviar o pacote recebido.

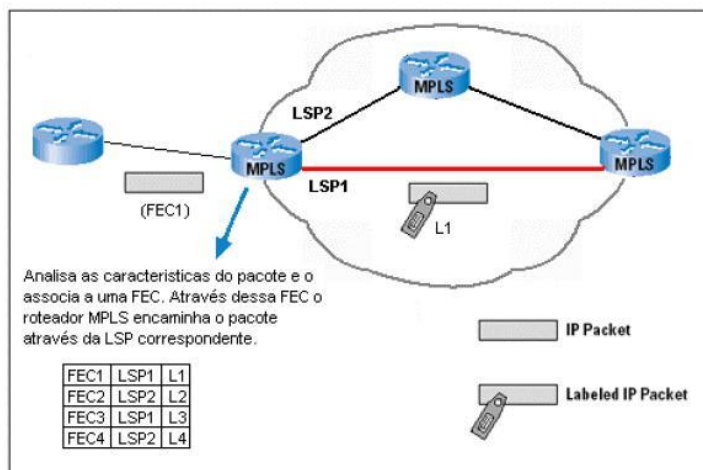
**FIB (*Forwarding Information Base*):** É uma tabela responsável por controlar a decisão de encaminhamento de pacotes de um roteador, através de busca pela tabela é possível saber qual interface o roteador deverá enviar o pacote. O conteúdo desta tabela depende do protocolo IP que está sendo usado, por exemplo OSPF, BGP.

**LFIB (*Label Forwarding Information Base*):** Tabela que tem como objetivo informar como e onde encaminhar os pacotes, através de uma lista de entrada, baseada nas informações obtidas pelo LSR através da interação com protocolos de roteamento (OLIVEIRA, LINS e MENDONÇA, 2012).

**FEC (*Forwarding Equivalence Class*):** Uma FEC é um conjunto ou grupo de pacotes equivalentes, que podem ser tratados da mesma forma, por exemplo, grupo de pacotes que o endereço de origem e destino é os mesmos (OLIVEIRA, LINS e MENDONÇA, 2012).

Todos os pacotes pertencentes a mesma FEC tem o mesmo rótulo e cada LSR constrói uma tabela chamada LIB (*Label Information Base*) com especificação de como o pacote deve ser enviado (NOGUEIRA, 2008).

A Figura 4 demonstra como é feita a análise de características de um pacote e associada a uma FEC.



**Figura 4 - Esquema de funcionamento de uma associação FEC a um pacote**

Fonte: TAFT (2010).

LSR (*Label Switch Router*): Encaminha datagramas de rede através de rótulos MPLS. Participa no estabelecimento de LSP, usando protocolo de sinalização de rótulo, como por exemplo o BGP. Ao receber um pacote, cada LSR troca de rótulo existente por outro, encaminhando o pacote para o próximo roteador e assim sucessivamente.

Podemos classificar o LSR basicamente em LSR de Borda de Entrada ou Edge: é um 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 (ingresso) do pacote no domínio MPLS. Os ingressa 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 (OLIVEIRA, LINS e MENDONÇA, 2012).

LSR de Trânsito ou P (*Provider*): são LSRs intermediários que têm a função de apenas fazer a comutação, ou seja, a troca de rótulos, e encaminhar o datagrama para o próximo nó.

Eles oferecem comutação em alta velocidade, sendo este um processo que mais contribui para o ganho de desempenho na utilização do protocolo MPLS, já que não precisam mais analisar cabeçalhos da camada de rede (IP). (OLIVEIRA, LINS e MENDONÇA, 2012).

LSR de Borda de Saída ou PE (*Provider Edge*): é um LSR responsável pela retirada do rótulo do pacote e encaminhamento ao seu destino final.

Apesar de não fazer parte do domínio MPLS, os roteadores que fazem parte do ambiente dos clientes possuem uma nomenclatura no cenário MPLS, sendo conhecidos como CEs (*Customer Edges*). Tais elementos não têm conhecimento da tecnologia MPLS, e o tráfego gerado é baseado apenas nos protocolos roteáveis, dos quais destacamos o protocolo IP (OLIVEIRA, LINS e MENDONÇA, 2012).

**LSP (*Label Switched Path*):** um LSP é uma sequência ordenada de LSRs, sendo o primeiro um LSR de ingresso e o último um LSR de saída, ou seja, é o caminho entre o nó de ingresso, possíveis nós intermediários, e o nó de egresso de uma rede MPLS. É similar a um circuito virtual ATM ou Frame Relay, sendo unidirecional no sentido da origem para o destino, podendo ser estático ou dinâmico (OLIVEIRA, LINS e MENDONÇA, 2012).

**VRF (*Virtual Routing and Forwarding*):** permite criar tabelas de roteamentos virtuais que trabalham de forma independente das demais, assim cada cliente tem sua própria VRF trazendo mais segurança e flexibilidade. Um roteador PE tem uma instancia de VRF para cada cliente conectado a ele, logo é como se existisse roteadores dedicados para cada cliente dentro do provedor de serviços, porém, é compartilhado o uso de CPU, largura de banda e memória com outros roteadores virtuais que fazem parte do mesmo PE.

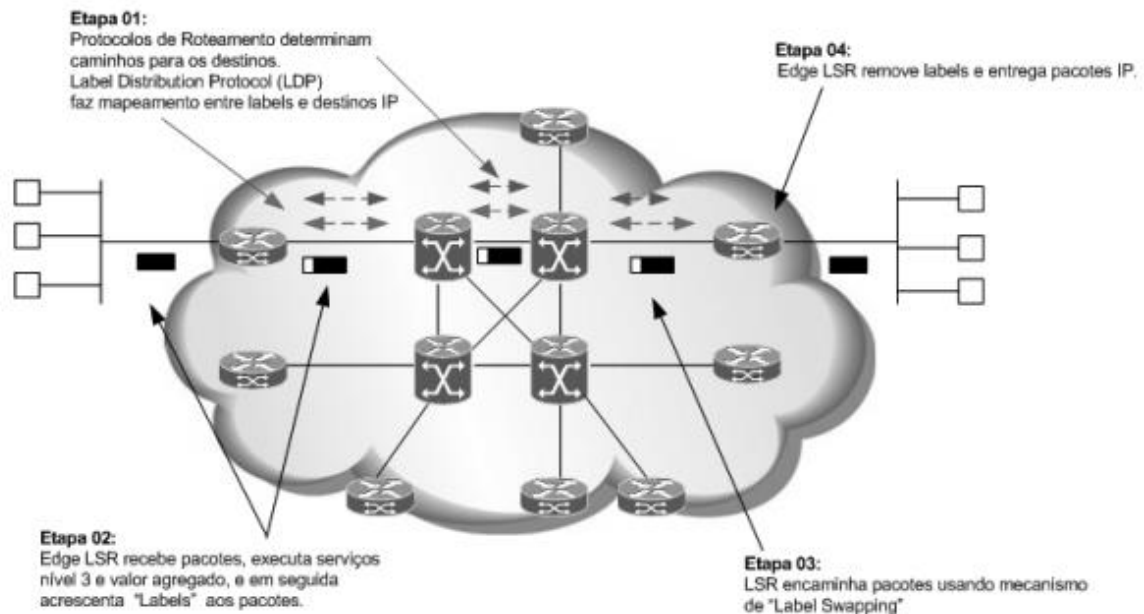
Podemos comparar com uma tabela de roteamento global, mas ela contém todas as rotas que pertencem para uma VPN específica (OLIVEIRA, LINS e MENDONÇA, 2012).

**RD (*Route Distinguisher*):** quando utilizamos os processos de roteamentos entre VRFs no mesmo roteador, deve se configurar o RD, que tem como função o controle de quais rotas pertencem a cada cliente, adicionando um identificador nas rotas para torná-las únicas, assim podemos identificar cada rota e para qual VRF pertence. O Valor do RD é carregado junto com uma rota no MP-BGP quando o roteador faz a troca de rotas VPN com outros roteadores PE.

**RT (*Route-Target ou VPN-target*):** configurado junto com o RD, o RT é uma comunidade BGP que indica o membro de uma VPN, tem como objetivo controlar a importação e exportação de rotas das VRFs no processo de redistribuição.

Há alguns formatos para o RD/RT, sendo que sua forma mais comum consiste em ASN de 16 Bits + Número de 32 Bits ; Ex.: 65000:100.

A Figura 5 apresenta o funcionamento de uma rede MPLS, demonstrando todas as suas etapas.



**Figura 5 - Operação do MPLS**

Fonte: (OLIVEIRA, LINS e MENDONÇA, 2012).

## 2.4 FRAME RELAY

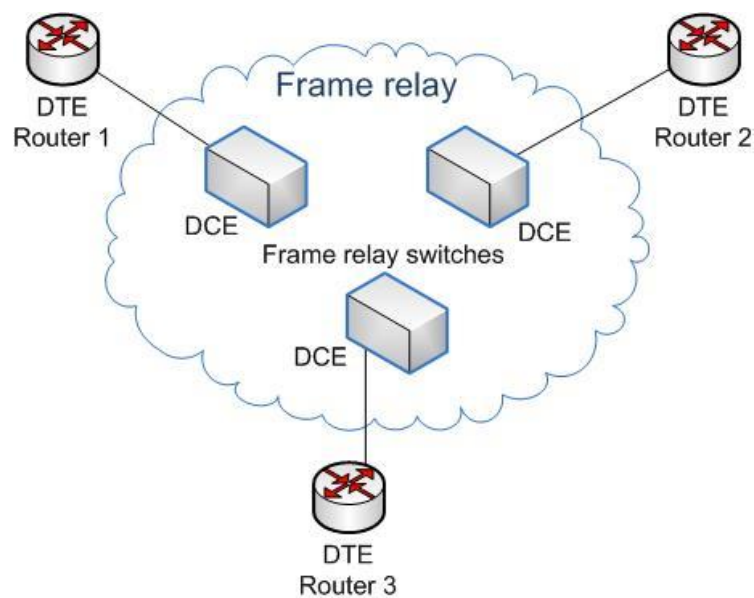
Segundo Enne (1998), o Frame Relay é um protocolo baseado em redes comutadas de pacotes, orientado à conexão, que serve para conectar redes locais e de longa distâncias, operando na camada de enlace, nível 2 do modelo de referência OSI.

No Frame Relay a comunicação é feita através de pares de dispositivos DTE'S (*Data Terminal Equipments*), utilizando "túneis" virtuais, conhecido como CV's (*Circuits Virtual*), passando por vários DCE's (*Data Communication Equipments*) na rede da operadora de serviço. Cada CV (*Circuito Virtual*) conta com um identificador de conexões, o DLCI (*Data Link Connection Identifier*), cuja função é associar circuito virtual entre o DTE e o DCE. A comutação dos caminhos virtuais pode ser (SVC's – *Switched Virtual Circuits*) ou permanentes (PVC's – *Permanent Virtual Circuits*) onde a operadora configura uma conexão entre dois pontos de acordo com

o plano que o cliente contratou gerando um link dedicado entre lado A e lado B, logo se o objetivo é trabalhar com redes full mesh, será necessário, um alto custo de investimento.

A Figura 6 demonstra o esquema de uma rede Frame Relay.

A entrega de frames ou quadros não é garantida no Frame Relay, pois quando ocorre erros ou congestionamento na rede pode descartar parte deles, também não existe nenhum tipo de mecanismo de controle de fluxo e erros, assim essa atividade deve ser configurada nos equipamentos roteadores do usuário.



**Figura 6 - Frame Relay**

Fonte: RUWANINDIKA (2008).

## 2.5 MPLS VPN

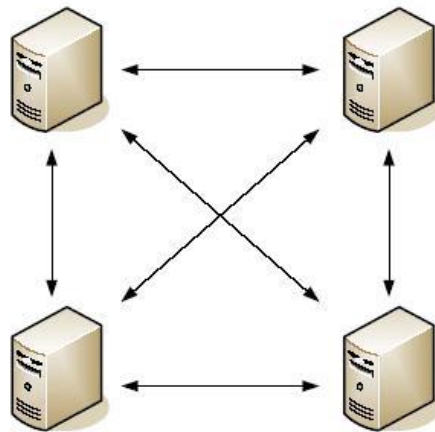
Segundo Rocha (2012), uma das principais utilidades do MPLS é o uso no serviço de VPN (Virtual Private Network), usada para interligar localizações remotas através de uma rede pública. A topologia lógica pode ser Full-Mesh ou Hub Spoke. O MPLS permite dois tipos de serviços: VPN's Camada 3 e VPN's Camada 2 (SANTOS, 2005). Nesse trabalho foi utilizado o VPN na camada 3.

## TOPOLOGIAS DE VPN:

A Topologia Full-Mesh é quando todos os nós da rede estão ligados diretamente, ou seja, o roteador utilizado no centro da rede não precisa mais comutar o tráfego entre filiais e centralizar as informações de roteamento (GERSON, 2008).

A Figura 7 apresenta o esquema de uma topologia Full-Mesh.

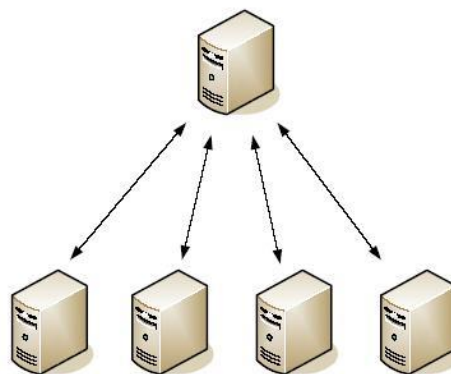
A topologia Hub-and-Spoke: se utiliza normalmente quando deseja implementar um maior nível de segurança, forçando o tráfego entre filiais a passar pela matriz (GERSON, 2008).



**Figura 7 - Topologia Full-Mesh**

Fonte: SILVA (2015).

A Figura 8 demonstra a topologia de uma rede Hub-and-Spoke.



**Figura 8 - Topologia Hub-and-Spoke**

Fonte: SILVA (2015).

## 2.6 MPLS VPN CAMADA 3

Segundo Rocha (2012), a MPLS VPN Camada 3 utiliza uma extensão do BGP, chamada MP-iBGP (*Multi-Protocol internal BGP*) para distribuir as informações de roteamento através do backbone do provedor de serviço. Essas VPN's podem ser: do tipo *PE-based* (provedor é responsável pelo encaminhamento e rotas dentro da rede) e do tipo *CE-based* (onde o contratante desse tipo de rede junto ao provedor é responsável pelo encaminhamento e rotas dentro da rede) (KUROSE; KEITH, 2007).

Numa MPLS VPN Camada 3 o roteador do cliente envia ao LER, informações de roteamento da rede privada que está por traz dele, essas informações são armazenadas em uma tabela virtual de encaminhamento e roteamento (*VRF-Virtual Routing and Forwarding*), sendo cada VRF uma rede IP privada.

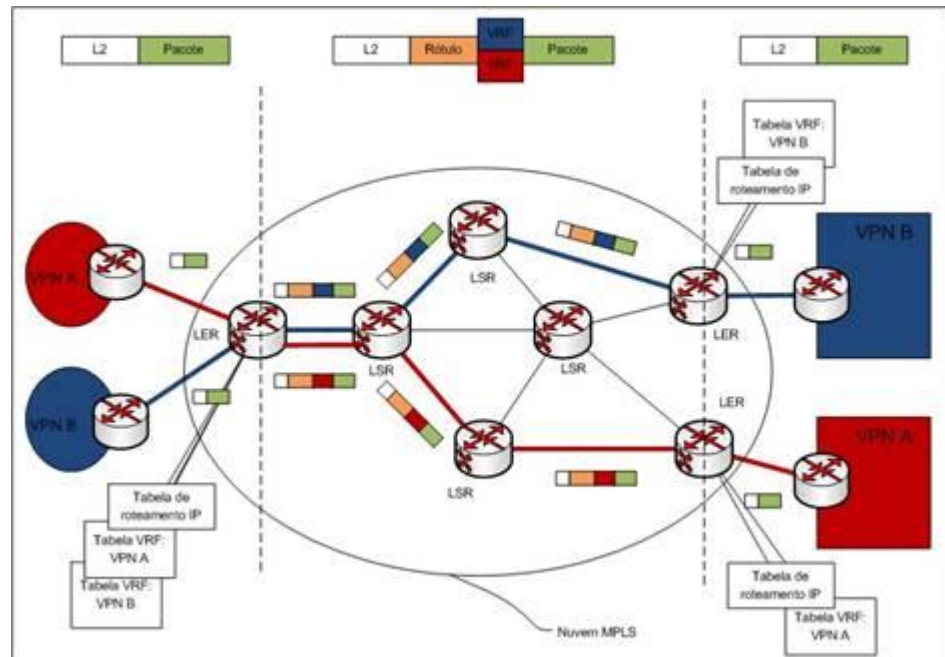
Para se ter um isolamento e segurança, a LER aloca uma tabela VRF separada para cada VPN, assim os usuários tem acesso apenas aos sites e hosts que fazem parte da sua VPN.

No LER também fica armazenado as informações de roteamento necessárias para efetuar o encaminhamento do tráfego em toda a rede pública (por exemplo, a Internet) (IXIA, 2015).

Logo que os roteadores do cliente (*CE*) iniciam a troca de protocolos de roteamento com o backbone, esse identifica o endereçamento IP do cliente, definindo o melhor caminho de um site a outro (GERSON, 2008).

Os pacotes que vão de um site para outro seguem o melhor caminho no backbone, direto para o endereço IP destino não passando, necessariamente pela matriz (GERSON, 2008).

A Figura 9 demonstra um esquema de MPLS VPN Camada 3.



**Figura 9 - Protocolos de roteamento MPS VPN Camada 3**

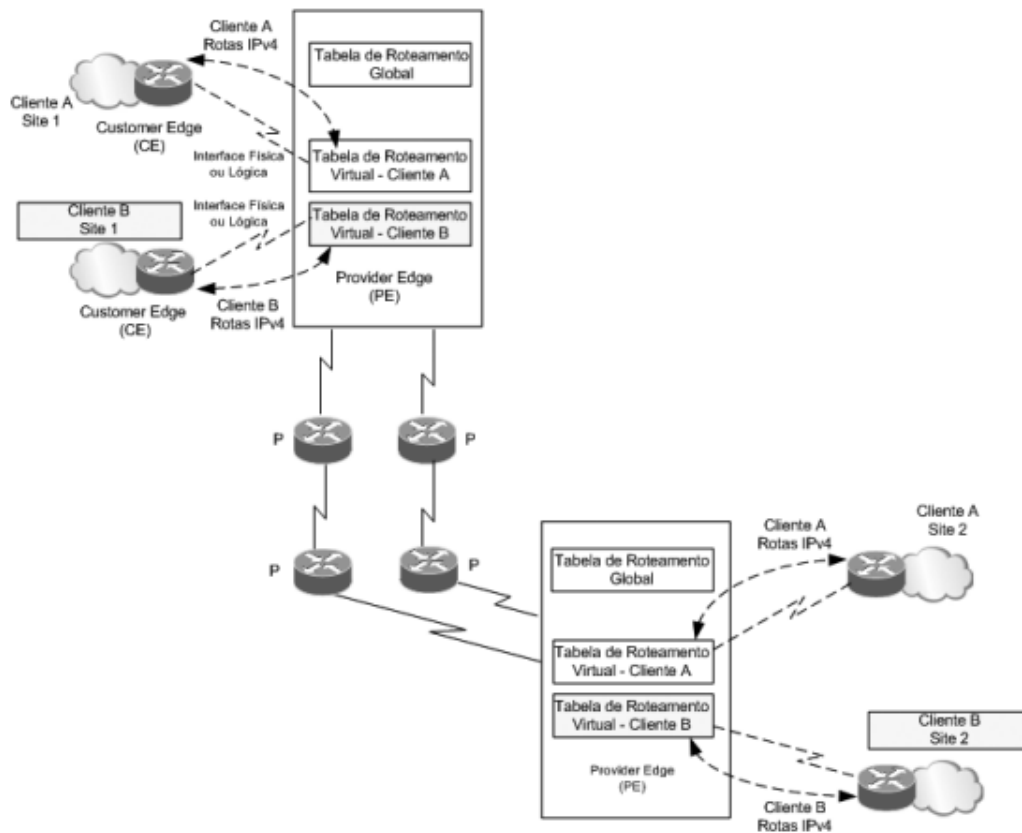
Fonte: ROCHA (2012).

Como vantagens na utilização de MPS VPN Camada 3, pode-se citar:

- O endereçamento IP do cliente é gerido pela operadora de serviço.
- Facilidade para a operadora adicionar e gerir novos sites VPN.
- Suporte a autodescoberta para distribuição de rotas VPN aproveitando a capacidade de roteamento dinâmico do BGP.

A desvantagem é suportar apenas o tráfego dos clientes baseados em encapsulamento IP (IXIA, 2015).

A Figura 10 demonstra a arquitetura de uma MPS VPN Camada 3.



**Figura 10 - Arquitetura MPLS VPN**

Fonte: (OLIVEIRA, LINS e MENDONÇA, 2012).

## 2.7 CARACTERÍSTICAS FRAME RELAY E MPLS – PRINCIPAIS OPERADORAS

Nesta seção será apresentado um comparativo demonstrando características, vantagens e desvantagens dos serviços de Frame Relay e MPLS oferecidos por duas das principais operadoras do Brasil.

### CARACTERÍSTICAS, VANTAGENS E DESVANTAGENS DOS SERVIÇO DE FRAME RELAY DA EMBRATEL E VIVO/TELEFÔNICA

O Frame Relay é um serviço de transmissão de dados de 64 Kbps a 2 Mbps, que interliga redes corporativas (*LANs* e *WANs*) e possibilita a transmissão de informações - voz, dados e imagens - entre unidades de negócio fisicamente distantes, através de quadros (*frames*).

## Características

Algumas características do serviço comuns em ambas às operadoras são: Rede por pacotes, Interligar matriz x filial por backbone's ponto a ponto, Frame Relay gerencia (controla) os pacotes na rede gerenciando o tráfego, Melhor uso da banda, ABRANGÊNCIA - cobertura nacional (todas as principais cidades) e internacional.

A VIVO/TELEFONICA através do serviço FRAME RELAY DEDICADO oferece alguns diferenciais como: Utilização - Intercâmbio de informações em tempo real por meio da transmissão, em alta velocidade, de grande volume de dados, voz e imagem, Aplicações - Serviço bastante apropriado para Transferência Eletrônica de Fundos - TEF, criação de intranet e construção de bases de dados distribuídas (gestão de estoque, movimentação de vendas, controle de faturamento, etc.), Tarifa única por velocidade sem franquia de tráfego e SLA de reparo de 4 horas.

## Vantagens

As principais vantagens comuns entre as duas operadoras são:

- Rede Segura - Garantidas por um tratamento de "grupo fechado" para a topologia de rede definida pelo cliente.
- Redução de custo com telecomunicação.
- Interligar matriz x filial.
- Suporte a aplicações cliente x servidor.

A VIVO/TELEFONICA oferece como diferencial: gerenciamento ininterrupto, possibilitando, inclusive, roteamento alternativo para a transmissão em momentos de pico de tráfego (sem custo adicional).

## Desvantagens

As principais desvantagens em ambas são:

Maior custo operacional e porta até 2 Mb/s, sendo assim quando há necessidade de maior velocidade é necessário contratar mais portas, aumentando o seu custo.

## CARACTERÍSTICAS, VANTAGENS E DESVANTAGENS DOS SERVIÇOS DE MPLS DA EMBRATEL E VIVO/TELEFÔNICA

A solução MPLS interliga e cria uma rede para agilizar suas transferências de informação entre matriz e filias. Com ela, as empresas podem integrar as suas aplicações de dados, voz e vídeo usando uma única infraestrutura, ganhando qualidade e economia na condução dos seus negócios. O serviço permite integrar múltiplos sites a múltiplos destinos, com garantia de 100% da banda, alta disponibilidade e gestão centralizada, utilizando o MPLS (*Multiprotocol Label Switching*), que é o recurso mais avançado e flexível para a construção de VPN's com CoS (Classes de Serviços), possibilitando a priorização de tráfego de dados, voz e vídeo.

### Características

As principais características do serviço VIVO/TELEFONICA - VIVO VPN IP MPLS são: Ligações seguras entre todos os pontos da rede corporativa, com 100% de banda garantida e priorização de tráfego crítico, Solução voltada a criação de intranet e extranet, Conexões de 64kbps à 1Gbps, com SLA (nível de serviço) a partir de 99,0% de acordo com a solução contratada, É indicado para empresas que necessitam de uma comunicação segura, flexível, escalável, abrangente e que priorize as aplicações - QoS (Qualidade de Serviço); todos esses recursos baseados no protocolo TCP/IP (*Transmission Control Protocol/ Internet Protocol*).

No serviço da EMBRATEL – REDE ÚNICA DE DADOS MPLS podemos cita como características: um método de classificação e priorização denominado *DiffServ*, resultando em QoS (qualidade de serviço) com até seis classes de serviços: Voz/Vídeo; Missão Crítica; Interativa; Bulk; *Network Control* e *Best Effort* e Com as redes interligadas, você poderá falar a vontade com seus funcionários, sem custos com DDD/DDI. Além disso, você realiza videoconferências e transmite todas as aplicações corporativas com as devidas priorizações (e-mail, CRM, ERP etc).

## Vantagens

A VIVO/TELEFONICA - VIVO VPN IP MPLS tem como principais vantagens, permitir flexibilidade de crescimento e integração entre os sites das empresas, assim como aumento da disponibilidade da rede da sua empresa, Gestão baseada na rede IP da Telefônica, a mais completa plataforma de integração de serviços.

Na EMBRATEL – REDE ÚNICA DE DADOS MPLS podemos destacar algumas vantagens, tais como: Todo o isolamento do tráfego é implementado e realizado no backbone IP/MPLS da Embratel, Redução de custos - Com o uso da estrutura IP/MPLS sua empresa terá garantida uma formação de rede segura com baixos custos, A distância entre os pontos da VPN ou sua configuração (topologia) não provocam impacto no custo total, garantindo, assim, o melhor custo e benefício na solução de formação de redes, Custo x benefício, Tratamento do tráfego - A função da Qualidade de Serviço (QoS) é otimizar os recursos da rede de sua empresa. Com até seis classes diferentes, você pode escolher quais aplicações devem ser tratadas, Gerência - Se a sua empresa precisa de uma gerência simplificada, com menor grau de complexidade da rede, a Rede Única Dados MPLS atende a sua necessidade, Escalabilidade, Qualidade - SLA (*Service Level Agreement*) que assegura a qualidade do backbone IP/MPLS da Embratel, Opções de topologia - adequação da topologia lógica da rede ao perfil de tráfego em cada ponto, seja ela full mesh (malha), hub-and-spoke (estrela) ou mista e Serviços personalizados.

## Desvantagens

Cria grande dependência com relação à operadora.

## 2.8 COMPARATIVO ENTRE AS TECNOLOGIAS FRAME RELAY E MPLS.

Em uma rede Frame Relay se trabalha em uma nuvem central dentro da camada 2, onde se encontra diversas conexões (*PVC e Circuitos Virtuais*) e cada ponto (site) é pago um PVC a operadora, tornando assim um alto custo em infraestrutura (BUNN, 2010).

No MPLS, a operadora cobra apenas o plano da nuvem roteada, logo vamos ter uma rede *full mesh* IP conectada entre todos os pontos remotos, o que torna uma tecnologia ideal para empresas com grande número de filiais.

O circuito MPLS não está dentro da rede internet, embora é utilizando os mesmos equipamentos no backbone, outro ponto positivo em relação ao Frame Relay, é não se preocupar mais com o CIR, pois ele não existe no MPLS, eliminando os problemas de notificações de congestionamento e afunilamento de informações.

No Frame Relay todas as informações de destino são armazenadas dentro do pacote DLCI (*Data Link Connection Identifier*), assim as informações de IP não passa pelos switches, diferente do MPLS onde os switches verificam a origem do IP e envia ao destino.

Quando se trabalha com MPLS é formado uma rede full mesh entre todos os pontos, para isso é necessário utilizar um protocolo de roteamento estático ou dinâmico, os mais recomendados são: EIGRP, OSPF ou BGP, sendo a melhor opção um protocolo dinâmico, para que todos os pontos (sites) possam aprender sobre suas LAN's.

Outro motivo para escolher o protocolo dinâmico, é que o roteamento fica sob responsabilidade da operadora, sempre que adicionado um novo roteador, toda a rede deve identifica-lo, para que aprenda todas as rotas da nuvem e consiga encaminhar todos os seus pacotes para o destino de maneira correta.

Quando falamos em nuvem, se trata de um grande roteador (forma figurada), como sabemos, os roteadores de borda estão interconectados em redes de alta velocidade, espalhados dentro do país, fazendo parte desse grande roteador (BUNN, 2010).

## 3 MATERIAIS E MÉTODO

### 3.1 MATERIAIS

Para simular a rede MPLS foi utilizado o GNS3, com 3 modelos de roteadores diferentes, sendo eles:

- Cisco 7200, para roteadores da borda do provedor.
- Cisco 3725, nos roteadores MPLS, onde é feita grande parte das configurações e principal responsável por encaminhar os pacotes até os roteadores de clientes.
- Cisco 2691, roteadores utilizados nos clientes, não há nenhuma configuração MPLS, recebe as rotas OSPF e pacotes dos roteadores MPLS.

#### Simulador GNS3

O GNS3, disponível no site [www.gns3.com](http://www.gns3.com), é um software gratuito (*open source*) capaz de simular redes altamente complexas, sem precisar ter um hardware dedicado como roteadores e switches. Funciona usando imagens IOS da Cisco reais, que são emuladas através de um programa chamado *Dynamips*.

Um dos pontos levado em consideração para escolha do GNS3 foi a possibilidade de emular roteadores reais, além de se comunicar diretamente com a máquina hospedeira (computador onde está rodando).

Outro ponto importante é a quantidade de CPU e memória RAM utilizado, sendo assim, é necessário um computador com certa robustez.

## 3.2 MÉTODO

A primeira etapa para o desenvolvimento desse trabalho foi o levantamento bibliográfico sobre MPLS que teve como objetivo principal, aprimorar os conhecimentos sobre redes MPLS com foco em MPLS VPN Camada 3 e identificar as referências que poderiam ser utilizadas para buscar os resultados esperados no decorrer do trabalho. Para isso utilizou-se como referencial, as principais obras disponíveis sobre o assunto.

A segunda etapa foi a realização de um levantamento da infraestrutura necessária para simular um cenário de MPLS VPN Camada 3. Nesta etapa foi planejada toda a topologia do projeto.

Na terceira etapa foi feito um levantamento sobre ferramentas e equipamentos compatíveis com a tecnologia MPLS. Para isso realizou-se uma pesquisa de materiais na Internet, buscando informações em documentações oficiais disponibilizados no site da Cisco e em muitos sites que tratavam do assunto como, por exemplo, fóruns e blogs.

Na quarta etapa foi configurado todos os equipamentos, bem como versões do IOS em roteadores virtuais, através de um ambiente simulado, com objetivo de recriar a estrutura proposta no projeto.

Na quinta etapa foi desenvolvida a implantação de um cenário de MPLS VPNS Camada 3, com objetivo de demonstrar o funcionamento de uma rede MPLS.

## 4 RESULTADOS

Este capítulo tem por objetivo descrever os passos para implantação de uma rede MPLS VPN Camada 3, assim como, apresentar os resultados obtidos. Será descrito de forma geral todas as configurações necessárias das ferramentas para implantação desse projeto. Também será apresentada como resultado a comparação entre as tecnologias Frame Relay e MPLS:

- Frame Relay
  - Nuvem Central dentro da camada 2.
  - Diversas conexões (PVC e Circuitos Virtuais).
  - Cada ponto é pago um PVC a operadora.
  - Alto custo em infraestrutura.
  
- MPLS
  - Cobra apenas o plano da nuvem roteada.
  - Rede full mesh conectada entre todos os pontos remotos.
  - Ideal para empresas com grande numero de filiais.
  - Não esta dentro da rede internet, mas utiliza os mesmo equipamentos.
  - Não se preocupar com CIR, pois não existe no MPLS, eliminando os problemas de notificações de congestionamento e afunilamento de informações.
  
- Informações de destino:
  - No Frame Relay são armazenadas dentro do pacote DLCI.
  - Informações de IP não passa pelos switches.
  - No MPLS os switches verificam origem do IP e envia ao destino.
  
- Rede Ful Mesh
  - O MPLS precisa utilizar um protocolo estatico ou dinamico (EIGRP, OSPF).

- Quando adiciona um novo roteador toda rede identifica e aprende sua rota.

#### 4.1 ESTRUTURA PROPOSTA

Na Figura 11, segue a topologia para desenvolvimento do cenário:

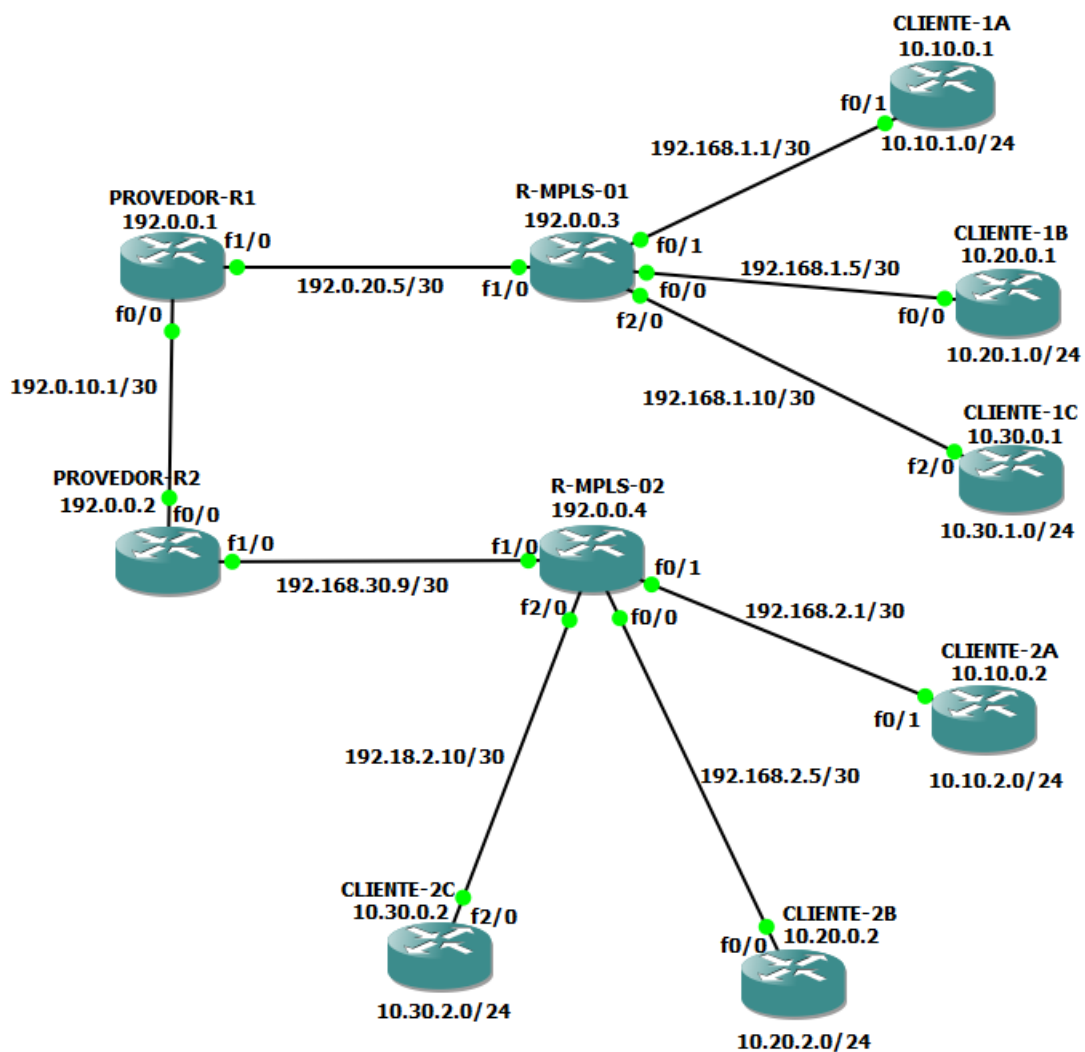


Figura 11 - Cenário MPLS/VPN L3 GNS3

Fonte: Adaptado de STRETCH (2011).

## 4.2 – CENÁRIO

Na figura 11 podemos observar o cenário de uma rede MPLS VPN Camada 3, sendo os roteadores Provedor R1 e R2 modelo Cisco 7200, chamados de P (*Provider*) cuja o qual representa o roteador de núcleo do ISP, que não se conecta diretamente ao cliente, logo depois diretamente conectado vamos ter os R-MPLS-01 e R-MPLS-02, conhecidos como PE (*Provider Edge*), modelo Cisco 3725, são conectados a sites de clientes e forma a borda de uma VPN, onde fica a rede do Cliente a MPLS da operadora, e por último os roteadores CLIENTE-1A até 1C e CLIENTE-2A até 2C ou CE (*Customer Edges*), modelo Cisco 2691, que são os roteadores de clientes, não é necessário rodar MPLS, pois são divulgadas para os R-MPLS-01 utilizando protocolos de roteamento.

### ATIVAR MPLS

O primeiro passo depois de conectar todos os roteadores é ativar o MPLS em todos os roteadores P (*Provider*) e PE (*Provider Edge*). Para isso se utiliza o comando ***ip mpls*** em todas interfaces conectadas ao roteador.

### CRIAR E ATRIBUIR VRFS

O próximo passo é criar VRFs (tabelas de roteamentos virtuais) em nossos roteadores PE, criando estancias VRFs independentes e permitindo que todos os clientes utilizem endereços de rede iguais, pois ao contrario o tráfego entre as sub-redes de todos os clientes da operadora iriam compor uma única tabela de roteamento.

Para configurar os VRFs é necessário adicionar um RD(*Route Distinguisher*) um identificador nas rotas para torna-las únicas e também o RT(*Route Target*) configurado junto com o RD, o RT é uma comunidade BGP que indica o membro de uma VPN, tem como objetivo controlar a importação e exportação de rotas das VRFs no processo de redistribuição.

Em nosso cenário, vamos utilizar o exemplo: ASN de 16 Bits + Número de 32 Bits; Ex.: 65000:100.

No Quadro 2 é dado um exemplo de código dessa configuração.

O comando **route-target** é usado para simplificar os comandos **route-target import** (importação) e **route-target export** (exportação).

Agora vamos as interfaces a sua respectiva VRF e adicionar seus endereços IPs, esse processo é feito apenas nos roteadores PE, já que nos roteadores dos clientes não é necessário habilitar o MPLS.

No quadro 3 são exibidos os comandos dessa configuração.

Exemplo de código:

```
// Ativar e criar um nome para VRF.
PE1(config)# ip vrf Cliente_A
// Criar um identificador na rotas para torna-las únicas.
PE1(config-vrf)# rd 65000:1
// Identificar o membro de uma VPN, permitindo que rotas sejam importadas e
exportadas das VRFs no processo de redistribuição.
PE1(config-vrf)# route-target both 65000:1
PE1(config-vrf)# ip vrf Cliente_B
PE1(config-vrf)# rd 65000:2
PE1(config-vrf)# route-target both 65000:2
```

#### Quadro 2 - Criar VRF

Fonte: Adaptado de STRETCH (2011).

Exemplo de código:

```
PE1(config)# interface f0/1
// Configure os detalhes de encaminhamento das respectivas interfaces utilizando
o comando ip vrf forwarding e logo após defina o endereço ip da interface.
PE1(config-if)# ip vrf forwarding Cliente_A
% Interface FastEthernet0/1 IP address 192.168.1.1 removed due to enabling VRF
Cliente_A
PE1(config-if)# ip address 192.168.1.1 255.255.255.252
```

#### Quadro 3 - Atribuir VRF

Fonte: Adaptado de STRETCH (2011).

Para anunciar as rotas VRF de um roteador PE para outro, devemos configurar o MP-BGP (*Multiprotocol BGP*), um pouco diferente do conhecido BGP, ele suporta várias famílias de endereços, como IPv4 e IPv6, além de suporte a anuncio de rotas VPN, onde adicionamos um RT(*Route Target*) na configuração do VRF.

O MP-BGP é executado apenas nos roteadores PE, os roteadores P dependem apenas do IGP e MPLS para encaminhar o trafego através da rede do provedor enquanto os roteadores CE (Clientes) não têm conhecimento de rotas fora do seu VRF.

Em nosso cenário vamos configurar os dois roteadores PE usando a AS 65000.

No quadro 4 são exibidos os comandos dessa configuração.

Exemplo de Código:

```
// criar roteamento BPG
PE1(config)# router bgp 65000
// Adicionar uma entrada à tabela de vizinho BGP, no caso o roteador PE2
PE1(config-router)# neighbor 192.0.0.4 remote-as 65000
// Habilitar as seções BGP a utilizar a interface loopback.
PE1(config-router)# neighbor 192.0.0.4 update-source loopback 0
// Inserir o modo de configuração da família de endereços.
PE1(config-router)# address-family vpnv4
// enviar o atributo de comunidade a um vizinho bgp.
PE1(config-router-af)# neighbor 192.0.0.4 activate
```

#### Quadro 4 - Roteamento BGP

Fonte: Adaptado de STRETCH (2011).

Podemos verificar a configuração BGP usando o comando **show running-config | section router bgp**.

No quadro 5 são exibidos os comandos dessa configuração.

Exemplo de Código:

```
PE1# show running-config | section router bgp
router bgp 65000
```

```

no synchronization
bgp log-neighbor-changes
neighbor 192.0.0.4 remote-as 65000
neighbor 192.0.0.4 update-source Loopback0
no auto-summary
!
address-family vpnv4
neighbor 192.0.0.4 activate
neighbor 192.0.0.4 send-community extended
exit-address-family
!
address-family ipv4 vrf Cliente_B
no synchronization
exit-address-family
!
address-family ipv4 vrf Cliente_A
no synchronization
exit-address-family

```

#### Quadro 5 - Verificar BGP

Fonte: Adaptado de STRETCH (2011).

Podemos verificar no código acima que foi criado **address-family** para os dois clientes VRFs automaticamente. Além disso a comunidade vpn4 é adicionada as configurações dos **neighbor** (vizinhos).

Para verificar o MP-BGP entre P1 e P2, utilizamos o comando **show bgp vpnv4 unicast all summary**.

No quadro 6 são exibidos os comandos dessa configuração.

#### Código de Exemplo

```

PE1# show bgp vpnv4 unicast all summary
BGP router identifier 192.0.0.3, local AS number 65000
BGP table version is 1, main routing table version 1

Neighbor      V  AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down

```

State/PfxRcd								
192.0.0.4	4	65000	12	12	1	0	0 00:06:05	0

#### Quadro 6 - Verificar MP-BGP

Fonte: Adaptado de STRETCH (2011).

Ainda não há rotas na tabela BGP, pois não especificamos nada para ser anunciando ou redistribuído, vamos fazer isso nos próximos passos.

### CONFIGURAR OSPF PE-CE

Depois de configurar o MP-BGP entre os dois roteadores PE. Agora precisamos configurar um IGP entre cada roteador PE com seu respectivo CE, para troca de rotas com os sites de clientes. Nesse trabalho optei por usar OSPF, mas pode ser usado qualquer outro protocolo de roteamento, de preferencia dinâmico, tais como: EIGRP ou RIP.

Nessa etapa vamos configurar um processo OSPF adicional para cada roteador CE em cada roteador PE. Cada roteador PE terá, então, três processos OSPF no total: uma para a rede do provedor, e um para cada roteador CE.

Considerando que o processo OSPF existe na tabela de encaminhamento global, os dois processos CE irão ser atribuído a cada um dos respectivos clientes VRFs.

No quadro 7 são exibidos os comandos dessa configuração.

Exemplo de Código
<pre>// Ativar roteamento OSPF nas VRFs para os roteadores CE respectivos. PE1(config)# router ospf 2 vrf Cliente_A // CE1A PE1(config-router)# router-id 192.168.1.1 PE1(config-router)# interface f0/1 PE1(config-if)# ip ospf 2 area 0 PE1(config-if)# router ospf 3 vrf Cliente_B // CE1B PE1(config-router)# router-id 192.168.1.5 PE1(config-router)# interface f0/1</pre>

```
PE1(config-if)# ip ospf 3 area 0
```

#### Quadro 7 - Roteamento OSPF

Fonte: Adaptado de STRETCH (2011).

Agora vamos verificar se cada roteador PE conhece seus roteadores CE conectados através do OSPF, as rotas dos clientes devem aparecer nas tabelas VRF dos roteadores PE.

No quadro 8 são exibidos os comandos dessa configuração.

#### CONFIGURAR DISTRIBUIÇÃO DE ROTA

Agora que o MPLS e MP-BGP está instalado e funcionando e todos os roteadores CE estão enviando rotas para os roteadores PE dentro de suas VRFs.

Código de Exemplo:

```
PE1# show ip route vrf Cliente_A
Routing Table: Cliente_A
...
10.10.0.0/16 is variably subnetted, 2 subnets, 2 masks
O   10.10.1.0/24 [110/11] via 192.168.1.2, 00:04:21, FastEthernet0/1
O   10.10.0.1/32 [110/11] via 192.168.1.2, 00:04:21, FastEthernet0/1
   192.0.0.0/30 is subnetted, 1 subnets
C   10.10.0.0 is directly connected, FastEthernet0/1
PE1# show ip route vrf Cliente_B

Routing Table: Cliente_B
...
10.20.0.0/16 is variably subnetted, 2 subnets, 2 masks
O   10.20.1.0/24 [110/11] via 10.0.1.6, 00:03:03, FastEthernet0/0
O   10.20.0.1/32 [110/11] via 10.0.1.6, 00:03:04, FastEthernet0/0
   192.0.0.0/30 is subnetted, 1 subnets
C   192.168.1.4 is directly connected, FastEthernet0/0
```

#### Quadro 8 - Rotas VRF

Fonte: Adaptado de STRETCH (2011).

O último passo é configurar a redistribuição de rotas. Primeiro é necessário configurar a redistribuição de rotas CE em cada VRF no MP-BGP, isso é feito sob a família de endereços IPv4 BGP para cada VRF.

No quadro 9 são exibidos os comandos dessa configuração.

#### Exemplo de Código

```
PE1(config)# router bgp 65000
PE1(config-router)# address-family ipv4 vrf Cliente_A
// redistribuir rotas OSPF
PE1(config-router-af)# redistribute ospf 2
PE1(config-router-af)# address-family ipv4 vrf Cliente_B
PE1(config-router-af)# redistribute ospf 3
```

#### Quadro 9 - Redistribuição de Rotas

Fonte: Adaptado de STRETCH (2011).

Isso permite a redistribuição de rotas OSPF em BGP para o transporte em toda a rede provedor entre os dois sites. Podemos verificar através do comando **show ip bgp vpnv4 vrf** que as rotas aprendidas a partir dos locais de clientes agora aparecem nas tabelas de BGP para seus respectivos VRFs.

No quadro 10 são exibidos os comandos dessa configuração.

#### Exemplo de Código

```
PE1# show ip bgp vpnv4 vrf Cliente_A
...
Network      Next Hop      Metric LocPrf Weight Path
Route Distinguisher: 65000:1 (default for vrf Cliente_A)
*> 192.168.1.0/30  0.0.0.0      0      32768 ?
*>i192.168.2.0/30  10.0.0.4     0      100    0 ?
*> 10.10.0.1/32   10.0.1.2     11     32768 ?
*>i10.10.0.2/32   10.0.0.4     11    100    0 ?
*> 10.10.1.0/24   10.0.1.2     11     32768 ?
*>i10.10.2.0/24   10.0.0.4     11    100    0 ?
```

#### Quadro 10 – Rotas Cliente A

Fonte: Adaptado de STRETCH (2011).

O último passo para configurar uma MPLS VPN Camada 3 é completar a redistribuição em sentido oposto: a partir do BGP nos processos OSPF de clientes. (Não precisamos especificar quaisquer informações VRF na declaração de redistribuição porque cada processo OSPF do cliente já está atribuído a um VRF).

No quadro 11 são exibidos os comandos dessa configuração.

Exemplo de Código
<pre>PE1(config)# router ospf 2 // redistribuir rotas BPG no OSPF PE1(config-router)# redistribute bgp 65000 subnets PE1(config-router)# router ospf 3 PE1(config-router)# redistribute bgp 65000 subnets</pre>

**Quadro 11 - Redistribuição BGP no OSPF**

Fonte: Adaptado de STRETCH (2011).

## TESTES

Para verificar se tudo está funcionando, devemos confirmar a conectividade de ponta a ponta entre os roteadores CE dentro de cada VRF. Os dois roteadores para cada cliente devem ter tabelas de roteamento completas.

No quadro 12 são exibidos os comandos dessa configuração.

Exemplo de Código
<pre>PE1# show ip route vrf Cliente_A Routing Table: Cliente_A .. 10.10.0.0/16 is variably subnetted, 2 subnets, 2 masks O   10.10.1.0/24 [110/11] via 10.0.1.2, 00:04:21, FastEthernet0/1 O   10.10.0.1/32 [110/11] via 10.0.1.2, 00:04:21, FastEthernet0/1    192.0.0.0/30 is subnetted, 1 subnets C   192.168.1.0 is directly connected, FastEthernet0/1 PE1# show ip route vrf Cliente_B Routing Table: Cliente_B ...</pre>

```

10.20.0.0/16 is variably subnetted, 2 subnets, 2 masks
O   10.20.1.0/24 [110/11] via 10.0.1.6, 00:03:03, FastEthernet0/0
O   10.20.0.1/32 [110/11] via 10.0.1.6, 00:03:04, FastEthernet0/0
    192.0.0.0/30 is subnetted, 1 subnets
C   192.168.1.4 is directly connected, FastEthernet0/1

```

#### Quadro 12 - Rotas VRF Cliente A e B

Fonte: Adaptado de STRETCH (2011).

Devemos ser capazes de executar ping de um roteador CE para outro.  
No quadro 13 são exibidos os comandos dessa configuração.

#### Exemplo de Código

```

CE1A# ping 10.10.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.0.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/21/32 ms

```

#### Quadro 13 - Teste Ping

Fonte: Adaptado de STRETCH (2011).

Podemos realizar um traceroute para verificar o caminho tomado, bem como os rótulos MPLS utilizados para percorrer a rede do provedor.

No quadro 14 são exibidos os comandos dessa configuração.

#### Exemplo de Código

```

CE1A# traceroute 10.10.0.2

Type escape sequence to abort.
Tracing the route to 10.10.0.2

 1 192.168.1.1 4 msec 4 msec 8 msec
 2 192.0.20.5 [MPLS: Labels 19/22 Exp 0] 16 msec 12 msec 24 msec
 3 192.0.10.2 [MPLS: Labels 19/22 Exp 0] 24 msec 20 msec 16 msec

```

4	192.168.2.1 [MPLS: Label 22 Exp 0]	20 msec	16 msec	24 msec
5	192.168.2.2	16 msec	*	36 msec

**Quadro 14 - Teste Traceroute**

Fonte: Adaptado de STRETCH (2011).

Enfim, os resultados obtidos demonstram que a utilização da tecnologia MPLS para VPN se demonstra muito eficaz e segura, através das VRFs (tabelas de roteamentos virtuais) é possível criar redes isoladas para cada grupo de VPN, assim cada cliente tem acesso apenas a seus sites (pontos), além da facilidade para adicionar novas VPNs, visto que utilizando um roteamento dinâmico, como OSFP, cada novo ponto adicionado é reconhecido por toda a rede.

## 5 CONCLUSÃO

O MPLS é uma tecnologia relativamente nova, que tem como objetivo solucionar alguns dos principais problemas enfrentados nas redes atuais, como velocidade, escalabilidade, gerenciamento de QoS e engenharia de tráfego. Através do modelo de encaminhamento de pacotes baseados em rótulos é possível seu mapeamento com as principais tecnologias de rede existentes.

Em comparação com o Frame Relay, o MPLS é uma novidade que surge para oferecer vários benefícios, tais como: Redução de custo com a utilização de VPN baseada no protocolo IP, segurança das informações trafegadas na rede através do confinamento do tráfego e da utilização de uma infraestrutura dedicada, gerenciamento da rede, garantindo privacidade e integridade dos dados e priorização de tráfego de dados de modo mais eficiente.

Nas redes Frame Relay há um maior custo operacional, pois, cada ponto (site) oferece uma porta com velocidade máxima de 2mb/s, assim quando há necessidade de velocidades maiores é necessário contratar mais portas, aumentando seu custo, além disso, essa tecnologia impossibilita fazer um controle de fluxo de erro nó a nó (essa função deve ser implementada em um nível mais alto), sendo assim a rede de transporte deve ser virtualmente a prova de falhas.

O MPLS permite integrar múltiplos sites e múltiplos destinos, com garantia de 100% de banda, priorização de tráfego crítico, conexões de 64kbps à 1Gbps e SLA, tornando-se uma tecnologia atrativa para empresas que necessitam de uma comunicação segura, flexível, escalável, abrangente e que priorize as aplicações.

Embora o MPLS, tenha suas vantagens o Frame Relay é uma tecnologia consolidada usada até hoje, assim toda a tecnologia tem suas vantagens e desvantagens, ou seja, haverá projetos de redes que o Frame Relay atende suas necessidades, enquanto outros sejam mais atraentes a utilização de MPLS.

Nos testes feitos através do simulador de redes GNS3, foi possível verificar que o MPLS demonstra ser uma ótima solução para criação de VPN em camada 3, cada roteador PE possui VRF (tabelas de roteamento virtuais) com um RD, identificador nas rotas para torná-las únicas, assim é possível ter endereços IPs

repetidos, também podemos destacar o total isolamento entre VPNs, sendo possível acessar, enxergar e pingar somente CEs da mesma VRF.

Por fim, o MPLS aparece como alternativa viável para implantação de VPNs onde há necessidade de comunicação com integridade, confiabilidade e segurança entre matriz com múltiplas filiais, oferecendo melhor desempenho das redes, por ser flexível. Para provedores é uma solução ideal para agregar serviços, pois utilizando MPLS é possível isolar tráfego de clientes de tráfego complexo na rede.

## REFERÊNCIAS

ABREU, L. H. *Arquitetura MPLS para Formação de VPN. 87f. Monografia* (Trabalho de Conclusão de Curso) – Faculdade de Ciências Aplicadas de Minas, Uberlândia, 2004.

AIRES, D. M.. *MPLS: Multiprotocol Label Switching RFC 3031. Monografia* (Trabalho de Conclusão de Curso) - Universidade Federal do Paraná, Curitiba, 2004.

BUNN, A. R.. *Migração de rede Frame Relay para MPLS* - Pontifícia Universidade Católica do Paraná, Curitiba, 2010.

ENNE, A F. *Frame Relay – Redes, Protocolos e Serviços*. Rio de Janeiro: Axcel Books. 1998.

GERSON, P. *Rede MPLS, Tecnologias e Tendências de Evoluções Tecnológicas. Monografia* (Trabalho de Conclusão de Curso) - Universidade Federal do Rio Grande do Sul, 2008.

IXIA - *MPLS: Conformance and Performance Testing*. Disponível em <[https://www.ixiacom.com/sites/default/files/resources/test-plan/mpls\\_0.pdf](https://www.ixiacom.com/sites/default/files/resources/test-plan/mpls_0.pdf)>. Acesso em: 10 ago. 2015.

KAKIHARA, C. M. *Avaliação e comparação de desempenho entre a arquitetura IP e a arquitetura IP sobre MPLS*. 2006. Tese (Mestrado em Engenharia de Produção) - Programa de Pós-Graduação em Física Aplicada, Instituto de Física de São Carlos, São Carlos.

KUROSE, J.; ROSS, K. *Redes de Computadores e a Internet: uma abordagem top-down*. [S.l.]: Pearson Education - Br, 2007.

MELO FILHO, I. J. et al. *Estudo comparativo para contratação de serviços de telecomunicações convergentes*. In: CONGRESSO DE PESQUISA E INOVAÇÃO DA

REDE NORTE NORDESTE DE EDUCAÇÃO TECNOLÓGICA, 5, 2010, Maceió. **Anais eletrônicos...** Maceió: IFAL, 2010. Disponível em: <<http://connepi.ifal.edu.br/ocs/index.php/connepi/CONNEPI2010/paper/view/1219/743>>. Acesso em: 10 ago. 2015.

MICROSOFT - *TechNet Library* Disponível em: <[https://technet.microsoft.com/ptbr/library/Cc731954\(v=WS.10\).aspx](https://technet.microsoft.com/ptbr/library/Cc731954(v=WS.10).aspx)>. Acesso em: 11 ago. 2015.

NOGUEIRA, R. F. *Aplicação de QoS sobre MPLS em equipamentos Cisco*. 33f. Monografia (Trabalho de Conclusão de Curso) - Universidade Federal do Rio Grande do Sul, 2008.

OLIVEIRA, J. M.; LINS, R. D.; MENDONÇA, R. *Redes MPLS: Fundamentos e Aplicações*. São Paulo: Brasport, 2012.

OSBONE, E.; SIMHA, A. *Traffic Engineering with MPLS*. Indianapolis: Cisco Press, 2002.

EMBRATEL - *Rede Única de Dados Frame Relay*. Disponível em <<http://portal.embratel.com.br/mge/rede-unica-dados-frame-relay.php>>. Acesso em: 28 ago. 2015.

ROCHA, A. S. *Estudo Básico do MPLS (Multi Protocol Label Switching)*. Teleco, 24, jan. 2012. Disponível em: <[http://www.teleco.com.br/tutoriais/tutorialmplseb1/pagina\\_3.asp](http://www.teleco.com.br/tutoriais/tutorialmplseb1/pagina_3.asp)>. Acesso em: 11 jun. 2015.

ROSEN, E.; VISWANATHAN, A.; CALLON, R. *RFC 3031: MultiProtocol Label Switching Architecture*. The Internet Society, 2001.

ROSEN, E.; TAPPAN, D.; FEDORKOW, G.; REKHTER, Y.; LI, T.; CONTA, A. *RFC 3032: MPLS Label Stack Encoding*. The Internet Society, 2001.

RUWANINDIKA. *Basic Network Diagram of a Frame Relay network, Drawn Manually Using MS Visio*. Wikimedia, 28, set. 2008. Disponível em: <[https://commons.wikimedia.org/wiki/File:Frame\\_relay.jpg](https://commons.wikimedia.org/wiki/File:Frame_relay.jpg)>. Acesso em: 11 jun. 2015.

SILVA, B. C. *Entendendo as topologias de replicação DFS*. Disponível em: <<http://www.linhadecodigo.com.br/artigo/2305/entendendo-as-topologias-de-replicacao-dfs.aspx>>. Acesso em: 25 ago. 2015.

STRETCH, J. *Creating an MPLS VPN*. Disponível em: <<http://packetlife.net/blog/2011/may/16/creating-mpls-vpn/>>. Acesso em: 28 set. 2015.

TAFT, B. P. *MPLS*. GTA/UFRJ, 25, out. 2010. Disponível em: <[http://www.gta.ufrj.br/grad/04\\_2/MPLS/conceitos.htm](http://www.gta.ufrj.br/grad/04_2/MPLS/conceitos.htm)>. Acesso em: 11 jun. 2015.

VIVO - *VPN IP MPLS*. Disponível em <[http://www.vivo.com.br/portalweb/appmanager/env/web?\\_nfpb=true&\\_nfls=false&\\_pageLabel=empSolSTSDVpnIpMplsPage#](http://www.vivo.com.br/portalweb/appmanager/env/web?_nfpb=true&_nfls=false&_pageLabel=empSolSTSDVpnIpMplsPage#)>. Acesso em: 23 ago. 2015.

VIVO - *Descritivo do Serviço Acesso Frame Relay Dedicado com Opção de Equipamento de Comunicação de Dados*. Disponível em <<http://www.vivo.com.br/portalweb/servlets/SearchContentServlet?did=63112>>. Acesso em: 29 ago. 2015.