UNIVERSIDADE FEDERAL DO MARANHÃO

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

CURSO DE CIÊNCIA DA COMPUTAÇÃO

FILIPE HILUY LIMA

A IMPORTÂNCIA DO MPLS NA ENGENHARIA DE TRÁFEGO PARA SERVIÇOS TRADICIONAIS E DIFERENCIADOS EM UMA REDE CORPORATIVA

São Luís

2012

FILIPE HILUY LIMA

A IMPORTÂNCIA DO MPLS NA ENGENHARIA DE TRÁFEGO PARA SERVIÇOS TRADICIONAIS E DIFERENCIADOS EM UMA REDE CORPORATIVA

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

Orientadora: Prof. Msc. Maria Auxiliadora Freire

São Luís

2012

Lima, Filipe Hiluy.

A importância do MPLS na engenharia de tráfego para serviços tradicionais e diferenciados em uma rede corporativa / Filipe Hiluy Lima. – São Luís, 2012.

69 f.

Impresso por computador (Fotocópia).

Orientadora: Maria Auxiliadora Freire.

Monografia (Graduação) – Universidade Federal do Maranhão, Curso de Ciência da Computação, 2012.

1. Engenharia de tráfego. 2. MPLS. 3. RSVP. I. Título.

CDU 004.41

FILIPE HILUY LIMA

A IMPORTÂNCIA DO MPLS NA ENGENHARIA DE TRÁFEGO PARA SERVIÇOS TRADICIONAIS E DIFERENCIADOS EM UMA REDE CORPORATIVA

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

Aprovada em: _____/_____/_____.

BANCA EXAMINADORA

_____

Profª Maria Auxiliadora Freire (Orientadora)
Mestre em Ciência de Engenharia
Universidade Federal do Maranhão

_____

Profº Carlos Eduardo Portela Serra de Castro
Mestre em Informática
Universidade Federal do Maranhão

_____

Profº Gedson Rios Lopes
Especialista em Redes de Computadores
Universidade Federal do Maranhão

Aos meus queridos avós,
Salma Chear Murad Hiluy e
Jamil Daud Murad Hiluy.

AGRADECIMENTOS

A Deus, pela oportunidade de crescimento intelectual dada e pela força e esperança para superar tantos obstáculos e alcançar mais esta meta.

À minha mãe, Jacira Hiluy Lima, por todo o incentivo, dedicação e esforço dispensados a mim durante todos os anos da minha vida.

Ao meu pai, Afonso Henrique Lima, pela disciplina ensinada e por sempre acreditar na minha vitória.

Ao meu irmão, Afonso Henrique Hiluy Lima, pelo sentimento de segurança que eu sinto ao seu lado.

À minha companheira, amiga, cúmplice, meu amor, Huaína Guimarães Vieira Ribeiro, por toda a prosperidade, alegria, incentivo, razão, tranquilidade e felicidade que ela me traz.

À minha tia Myriam de Viana Carvalho, por todo o apoio dado à minha família.

À minha amiga Rafisa Moscoso Lobato, pela consideração e sincera amizade.

Ao amigo Mauro Antônio Rocha da Silva, pela presteza, presença, cumplicidade e ensinamentos a mim repassados.

À minha orientadora, Maria Auxiliadora Freire, pelo apoio, receptividade ao tema, orientação e paciência dispensada.

Ao meu amigo e coordenador de curso, Carlos Eduardo Portela Serra de Castro, pela paciência e compreensão.

Aos amigos de curso, em especial a Guilherme Amoury Tesch, João Vitor Segalla e Fabrício Martins Monteiro Rocha, pelo apoio, consideração e participação nesta difícil e exaustiva jornada.

Ao meu mestre Hélio de Sá Almeida, pelos ensinamentos de como ser um capoeira na roda da vida.

E a todas as pessoas que acreditaram e torceram por mim em todos esses anos de graduação.

“De que serve ter riqueza,
sendo pobre de talento,
mendiga a alma de impureza
e a carcaça de avarento?

O valor do homem está
na força do seu talento,
com o qual conseguirá
o que for de seu intento.”

(Jamil Jorge)

RESUMO

Com a automação dos processos corporativos e um aumento significativo no número dos recursos humanos, cada vez mais dependentes de um computador com acesso à rede de comunicação da empresa corporativa, é perceptível a importância na utilização de forma eficiente deste recurso. Por isso, há uma necessidade constante de se implementar uma engenharia de tráfego de informações para que se possa garantir agilidade de transações, disponibilidade e economia. Atualmente, o crescente uso do protocolo MPLS pelos provedores, favoreceu o desenvolvimento de outro protocolo chamado RSVP-TE, capaz de reservar recursos da rede através de elementos da arquitetura daquele protocolo, atingindo os objetivos da engenharia de tráfego. Esta monografia irá abordar o funcionamento agregado dos dois protocolos e apresentará como se dá a configuração diante de um cenário corporativo.

Palavras-chave: Engenharia de Tráfego, *Multiprotocol Label Switching* (MPLS), *Resource Reservation Protocol* (RSVP), *Virtual Private Network* (VPN), *Traffic Engineering* (TE).

ABSTRACT

With the automation of business processes and a significant increase in the number of human resources increasingly dependent on a computer with network access to corporate communications company, is perceived the importance of using this resource efficiently. Therefore, there is a constant need to implement traffic engineering information so that we can guarantee a streamlined transaction, availability and economy. Currently, the increasing use of the MPLS protocol providers, favored the development of another protocol called RSVP-TE, able to reserve network resources through elements of the architecture of that protocol, reaching the goals of traffic engineering. This monograph will address the aggregate function of the two protocols and present how the setting is in a corporate scenario.

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

LISTA DE FIGURAS E ILUSTRAÇÃO

LISTA DE ABREVIATURAS E SIGLAS

BGP	*-Border Gateway Protocol*
CE	*-Customer Edge Devices*
CoS	*-Class of Service*
CR-LDP	*-Constrained-based Label Distribution Protocol*
DS	*-Differentiated Services*
DSCP	*-Differentiated Services Code Point*
ER	*-Explicit Route*
EXP	*-Experimental*
FEC	*-Forwarding Equivalence Class*
FF	*-Fixed Filter*
FRR	*-Fast Reroute*
FTP	*-File Transfer Protocol*
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*
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*
SLA	*-Service Level Agreement*
TCP	*-Transmission Control Protocol*
TLV	*-Type-Lengh-Value*
UDP	*-User Datagram Protocol*
TCP/IP	*-Transmission Control Protocol/Internet Protocol*
TTL	*-Time-To-Live*
VPN	*-Virtual Private Network*
VRF	*-Virtual Routing and Forwarding*
WAN	*-Wide Area Network*
WF	*-Wildcard Filter*

SUMÁRIO

1 INTRODUÇÃO

Com o avanço da tecnologia e uma competição comercial cada vez mais acirrada, percebe-se que atualmente, quase a totalidade de processos das grandes corporações estão totalmente dependentes de uma disponibilidade maior de acesso à rede de comunicação e dados. Empresas de grande porte que possuem unidades de negócios em várias regiões do país ou até mesmo em regiões internacionais, precisam estreitar essas longas distâncias fazendo com que a única rede controladora e compartilhadora dessas informações pareça única e local.

A rede de comunicação de uma empresa corporativa se torna ferramenta fundamental para implementações de padrões, divulgação de políticas internas, treinamento de funcionários e até mesmo sistemas que controlam máquinas que operam *full-time*. Com todo esse aumento exponencial de informações trafegando por toda essa rede, é imprescindível que haja um planejamento mínimo na hora de sua construção para que todas as "vias" por onde passarão essas informações, obtenham o maior rendimento possível, traduzindo-se em rapidez de resposta, balanceamento do tráfego, boa escalabilidade, menor número de colisões e maior economia financeira para a empresa. Para que uma informação ou um dado chegue ao seu destino a partir de sua origem, é percorrido um trajeto que possui vários equipamentos de rede (cabos, fibras ópticas, *hubs, switchs*, roteadores), por isso, a melhor disposição desses equipamentos ao longo da malha (caminho) lógica, acarretará maior aproveitamento da infraestrutura desta empresa. Apesar da existência de vários protocolos de encaminhamento de dados, a CiscoSystems[1] implementa em seus equipamentos (roteadores), um mecanismo padronizado pela IETF[2] de livre utilização chamado MPLS (*Multi Protocol Label Switching*) que possui diversas aplicações na engenharia de tráfego, que se mostra eficaz para alcançar os objetivos acima expostos.

O protocolo MPLS possui uma arquitetura que proporciona a agregação de outras tecnologias de forma otimizada, pois sua utilização compreende na formação de vários componentes ou elementos ao longo da rede que propiciaram a abertura

---

[1] *Cisco Systems, Inc.* é uma companhia multinacional sediada em São José Califórnia, Estados Unidos da América. A atividade principal da Cisco é o oferecimento de soluções para redes e comunicações quer seja na fabricação e venda.

[2] *Internet Engineering Task Force* é uma comunidade internacional ampla e aberta (técnicos, agências, fabricantes, fornecedores, pesquisadores) preocupada com a evolução da arquitetura da Internet e seu perfeito funcionamento.

de um ambiente capaz de ser utilizado por outros protocolos, garantindo um melhor rendimento e um novo paradigma na engenharia de tráfego. Por isso foi criado o protocolo RSVP-TE (*Resource Reservation Protocol – Traffic Engineering*) que se utiliza de um desses elementos do MPLS para criar túneis virtuais, fundamentais na implementação da engenharia de tráfego de redes.

1.1 Justificativa

Devido às constantes implementações de melhoria para que a rede corporativa de informações opere sempre em um nível de serviço aceitável para a acirrada concorrência e com um mínimo de segurança desses dados, uma engenharia lógica de tráfego se faz necessária. Por isso, há uma razão direta entre os aspectos da engenharia de tráfego adotada e maior rendimento produtivo e financeiro da corporação.

1.2 Objetivos

1.2.1 Objetivo Geral

A proposta da realização desta monografia é a utilização de um protocolo no desenvolvimento da engenharia de tráfego em um determinado cenário real corporativo, a fim de garantir maior qualidade de serviço.

Apresentar a importância do MPLS no desenvolvimento de uma engenharia de tráfego de uma rede corporativa para garantir certos níveis de serviços de forma agregada com o protocolo RSVP-TE, específico na criação de túneis virtuais em uma topologia de grandes redes corporativas.

1.2.2 Objetivos Específicos

e) Apresentar as necessidades de utilização das ferramentas GNS3 e *Wireshark* para a construção de topologias utilizadas como estudo de caso;

f) Configurar os equipamentos de rede para possibilitar a captura dos pacotes necessários para a constatação da utilização do protocolo estudado.

1.3 Estrutura do texto

Esta monografia encontra-se estruturada em 5 (cinco) capítulos. Apresentou-se no capítulo 1 a introdução necessária ao restante dos capítulos que compõe o trabalho.

No capítulo 2, apresenta-se uma fundamentação teórica sobre engenharia de tráfego em redes, bem como as diversas gerências onde ela é aplicada.

No capítulo 3, explica-se o funcionamento dos protocolos MPLS e RSVP-TE, bem como a utilização agregada dos dois para o desenvolvimento da engenharia de tráfego.

No capítulo 4, é demonstrado o estudo de caso, onde faz-se referência à uma empresa de grande porte que possui uma estrutura consolidada em tecnologia da informação, capaz de desenvolver constantemente a engenharia de tráfego em sua rede de comunicação através da tecnologia apresentada no capítulo 3. Além disso, são apresentados os cenários construídos e as análises dos pacotes capturados após a configuração dos equipamentos necessários.

No capítulo 5, por fim, apresentam-se as considerações finais conclusivas e as sugestões de trabalhos futuros referentes a esta pesquisa.

2 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).

Com o crescimento e desenvolvimento de uma determinada empresa que possui uma rede de informação, como área estratégica de maior produção, cresce também a necessidade de um maior rendimento e eficácia dessa rede. Com isso, a engenharia de tráfego dessas informações que passarão na rede se torna alvo de constante planejamento, execução e otimização para alcançar resultados mais positivos e rentáveis para a empresa.

O principal objetivo da engenharia de tráfego é controlar e otimizar o fluxo de informações, uniformemente, por todos os caminhos que a rede possui, para que os recursos implantados sejam melhores aproveitados. A figura 2.1(a) demonstra uma situação que evidencia a não implementação da engenharia de tráfego na rede, cujos pacotes seguem por uma única alternativa de caminho pré-estabelecido. Já a situação mostrada na figura 2.1(b), de forma simples, há uma implementação de engenharia de tráfego, cujos pacotes possuem opções de tráfego dos pacotes. As ações de engenharia de tráfego podem ser construídas, em longo prazo, como planejamento de crescimento contínuo de uma rede, mas poderá ter ações em tempo real, como recuperação de um caminho bloqueado por um tráfego intenso gerado por um sistema online.

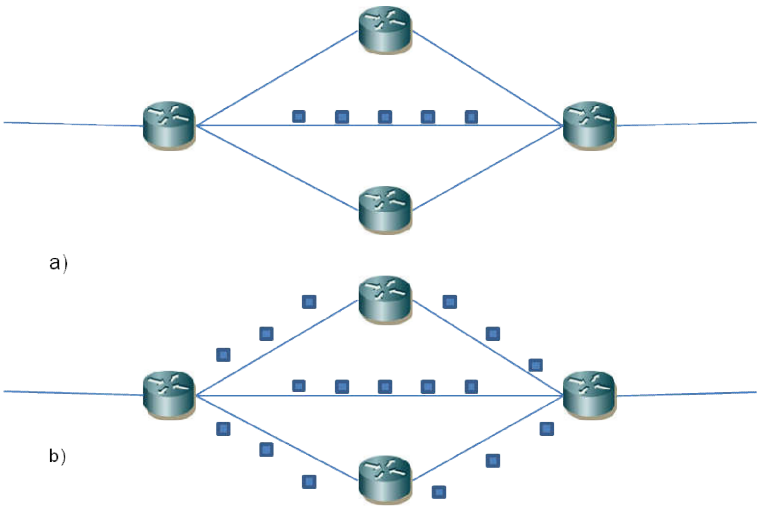


Figura 2.1 – a) Topologia sem engenharia de tráfego; b) Topologia com implementação de engenharia de tráfego.

2.1 Visão geral da engenharia de tráfego

Há alguns anos, a percepção dos usuários acerca do tempo de resposta da rede passava a ser o principal parâmetro de desempenho considerado pelos gerentes da rede. Porém, a cada dia, é notório o aparecimento de vários outros parâmetros de análise para o provedor desse serviço, como, por exemplo, o maior tempo de disponibilidade para que um determinado processo alocado, solicitado pela empresa possa ser executado.

Desde o planejamento de implantação de redes locais ou metropolitanas, a principal meta dessas redes, principalmente para grandes empresas, é transmitir os pacotes de dados a partir de nós de ingresso (onde se originam) até os nós de egresso (onde encontram seu destino) de forma rápida, eficaz, econômica e sem perdas. Além disso, atualmente as empresas de grande porte estão utilizando tecnologias cada vez mais dependentes de uma boa infraestrutura em suas redes, separadas por várias classes de serviços como o *Diffserv*[3]. Por isso, em um ambiente que possui os pacotes de informação pertencentes a diferentes classes, é natural que ocorra uma concorrência de recursos tornando-se necessário obter uma configuração na qual esses pacotes enfrentem um menor número de possíveis interferências advindas dessa competição pelos serviços.

Como consequência do contínuo dinamismo que a rede possui, o processo de engenharia de tráfego perdura por toda sua existência dentro da corporação. Com isso, surge a necessidade de criação de políticas adequadas para a realização de certas mudanças estruturais e lógicas que causam impacto significativo no desempenho da rede, trazendo vantagens ao prover certas habilidades de controle da rede como um todo, ao invés de controlar interfaces e dispositivos individualmente. Porém, qualquer decisão a ser tomada em sentido de gerenciamento de controle por uma empresa dependente da rede lógica, é necessário um estudo prévio, sobretudo da topologia alocada aos componentes, englobando a rede na sua total extensão, analisando o fluxo conjunto com as funções de comutação e roteamento de pacotes.

[3] *Diffserv* é um serviço de rede disponível capaz de separar os pacotes de dados em determinadas classes e prioridades através de identificações contidas no cabeçalho do protocolo IP.

O controle e o gerenciamento da rede corporativa na engenharia de tráfego assumem papel de fundamental importância, tendo em vista este dinamismo do fluxo dos pacotes, alternando as fontes de possíveis gargalos e conseqüentes degradações nos recursos aplicados. Por isso, empresas de grande porte seguem duas principais linhas para controle do tráfego: o controle pró-ativo e o reativo.

No caso do controle pró-ativo, há um controle preventivo no sentido de poder prever possíveis eventos desfavoráveis inesperados ou até minimizar os eventos já previstos. Isso pode ser feito com a constante análise da rede como um todo, verificando as origens de tráfego mais significantes, os sistemas mais críticos juntamente com a sobrecarga gerada em algum ponto da rede com a finalidade de saná-la a curto ou longo prazo.

Para restringir o acesso a recursos da rede que estejam congestionados e/ou regular a demanda para diminuir a situação de sobrecarga, devem ser definidas certas políticas para a aceitação, estabelecimento e manutenção de conexões (AWDUCHE; REKHTER, 2001 apud MAIA, NILTON 2006).

No caso do controle reativo, como o nome já diz, reage de forma a corrigir eventos desfavoráveis, ou falhas que já aconteceram na rede em curto prazo.

2.2 Tipos de gerência de redes

Para se conseguir uma eficiência razoável na engenharia de tráfego de dados em uma rede, a gerência dela se torna uma grande aliada a partir do momento em que são feitas medições, análises de pacotes, *delay* de atraso em equipamentos, porcentagem de disponibilidade etc.

Com todas essas informações disponibilizadas, é possível traçar metas de intervenções cada vez mais adaptativas para maior eficiência da engenharia de tráfego.

No contexto de uma empresa de grande porte, o gerente de rede se torna o principal responsável pelo desempenho e pela eficácia da manutenção da engenharia de tráfego, possuindo total poder de decisão em relação a mudanças.

Apesar de cada empresa possuir sua metodologia de gerência de rede diferente, é possível separá-la em três grandes domínios de ação: Gerência de Desempenho e Planejamento, Gerência de Incidentes ou Falhas/Segurança, Gerência de Configuração.

2.2.1 Gerência de desempenho e planejamento

O principal objetivo da gerência de desempenho é a avaliação de desempenho da rede como um todo, com o objetivo de buscar uma melhor performance, ou seja, envolve atividades a fim de obter uma maior otimização do fluxo dos dados.

Um bom gerenciamento de desempenho de uma rede pode ser obtido através do gerenciamento e planejamento da capacidade desta rede, analisando-a por completo juntamente com seu contínuo tráfego. O gerenciamento de planejamento da capacidade da rede inclui um estudo dos recursos computacionais a serem implantados como largura de banda dos enlaces, configurações dos servidores, *buffers* etc. Em redes corporativas, esse gerenciamento se torna muito importante com análises muito frequentes, pois o crescimento da demanda é muito grande, o que pode comprometer o desempenho se não houver uma melhora constante.

O gerenciamento de tráfego atua basicamente nos nós da rede (roteador, *hubs, access points, swicths*) que são responsáveis pelo transporte de pacotes. Esse controle pode ser efetivado por medições ou funções que demonstram o rendimento de cada um desses nós, apontando o atraso e eficácia de transmissão dos pacotes, possibilitando uma análise mais detalhada de pontos ou trechos da rede que são candidatos a ter congestionamentos, o que significa uma antecipação na resolução de problemas de indisponibilidade dos recursos.

2.2.2 Gerência de incidentes ou falhas/segurança

Uma boa engenharia de tráfego engloba também uma gerência de falhas devido à dependência de uma constante monitoração em busca de qualquer evento que impeça a disponibilidade da rede.

O objetivo da gerência de falha é descobrir a raiz do problema, coletando os dados monitorados e que se mostram potencialmente capazes de gerar alguma falha no transporte normal ou ótimo do fluxo de pacotes. Identificado o problema, é importante tomar uma decisão para saná-la de forma que posteriormente seja possível solucioná-lo definitivamente sem muita transparência para os usuários da rede.

Outro ponto importante para o impedimento de falhas em uma rede é a implementação de uma segurança robusta, ou seja, quanto menor as chances de pontos de ataques em uma grande malha lógica, menor será a quantidade de falhas geradas por algum agente externo ou mesmo internas. Como toda e qualquer rede empresarial possui um caráter privado, ou seja, não há permissão de conexões externas com seus servidores ou com qualquer nó, normalmente quando se percebe uma ameaça ativa, poderá ser acionado um *plugin* específico para tentar impedir de alguma forma a vulnerabilidade que o ataque proporcionou, degradando o desempenho normal.

Por isso, tanto as falhas que acontecem de forma natural ou aquelas ocasionadas por fatores externos, devem ser gerenciadas ao longo do processo da engenharia de tráfego para garantir acordos de disponibilidade firmados. Por outro lado, faz-se necessário incluir como parâmetro o intervalo temporal que cada falha diferente necessita para ser corrigida. Isto decorre das diferentes políticas que cada empresa implementa.

2.2.3 Gerência de configuração

A última das principais gerências e não menos importante é a gerência de configuração. Ela se caracteriza pela uniformidade de configuração que alguns ou todos os equipamentos relacionados da rede possuem. Configuração de uma rede corporativa pode se dá em nível topológico, em que se mantém um mapa da arquitetura que, como os nós (equipamentos), estão interligados uns aos outros e em nível lógico, onde todas as configurações feitas no sistema operacional de cada equipamento são guardadas a fim de que facilite operações de mudanças, recuperação de enlaces comprometidos e otimizando o processo de escalabilidade. Essas informações são melhores administradas, acumulando-as em uma base de dados chamada *baseline*.

É muito importante tornar a consulta à *baseline* confiável e atualizada, ou seja, qualquer modificação feita, como novo padrão adotado pela empresa, ela deverá ser atualizada.

Por isso, uma gerência de configuração dos dispositivos da rede demonstra-se como um grande aliado na hora em que se precisa tomar medidas ou intervenções na otimização da engenharia de tráfego.

2.3 Modelagem, análise e medição

Atualmente, há um crescente aumento de padronização no gerenciamento de serviços de TI, porém de forma que o gerente tenha grande liberdade de implementação dentro da sua área de negócio. Por isso, cada empresa adota uma política ou modelo para que se desenvolva uma engenharia de tráfego de dos seus dados na rede.

Os principais parâmetros norteadores para que se consiga implementar uma engenharia de tráfego são disponibilizados através de processos experimentais, como a medição de fluxos, velocidade de respostas, capacidade de transportes etc. A partir dessas informações, é necessário que seja feita uma análise para que se tenha uma conclusão no comportamento dessa rede.

2.3.1 Modelagem para engenharia de tráfego

Atualmente não existe um modelo de processo padrão para o desenvolvimento de uma engenharia de tráfego em redes computacionais. Por isso, cada empresa possui um modelo próprio dependendo de suas características e objetivos. Apesar dessa falta de um modelo, cada qual possui etapas para sua construção que se assemelham bastante e se destacam por ter as seguintes características:

a) A primeira etapa possui uma característica de definição de políticas de controle mais amplo, dependendo de parâmetros, como objetivos da empresa, atividade de negócio, custo estrutural da rede, níveis de serviço, restrições, permissões etc.
b) A segunda fase consiste basicamente em uma aquisição de dados de *feedback* para a análise através da rede operacional. Dependendo da política de segurança da empresa, esses dados poderão ser de difícil acesso, necessitando-se de uma análise feita com simuladores, o que reflete o comportamento da rede estimando valores bem aproximados da realidade.
c) A terceira e mais trabalhosa fase consiste na investigação de pontos críticos, pontos potenciais de gargalos, pontos problemáticos existentes e também na investigação do equilíbrio existente das concentrações dos fluxos de dados e sua distribuição.

d) A quarta fase é a otimização da rede. Uma empresa pode possuir técnicas próprias para alcançar a melhor performance no fluxo de dados de uma rede. Isto pode ser feito em nível topológico, parâmetros de roteamento em determinado trecho, mudanças dinâmicas para atender certo gargalo em um ponto, métricas de protocolos configurados etc. Uma boa otimização tem seu início desde planejamento da topologia até as configurações de equipamentos que visam o crescimento atual e futuro da empresa.

2.3.2 Análise e medições

A análise pormenorizada de uma rede corporativa começa a partir da coleta de dados específicos, através de medições feitas com sistemas apropriados para tal fim e que ajudam a dar suporte à engenharia de tráfego em grandes redes IP corporativas, de forma a assegurar aspectos dessa engenharia, como planejamento, dimensionamento, gerenciamento (controle) e otimização de desempenho.

As bases para uma medição de rede podem ser os fluxos, interfaces, desempenho dos equipamentos, topologia da rede, enlaces etc. A partir dessas bases, há a formação das entidades de medição que se identificam pelos resultados ou desempenho do funcionamento das bases utilizadas como parâmetro. Essas entidades podem ser o atraso dos pacotes em algum enlace, retardo de processamento de algum equipamento, banda disponível e utilizada em alguma parte da topologia, tempo gasto em algum fluxo específico e utilização dos recursos.

É importante notar que essas informações em conjunto com outras, como por exemplo, as configurações da *baseline* e outros dados estatísticos obtidos com as entidades de medição são importantes para se obter uma melhor engenharia de tráfego.

Atualmente, há alguns *frameworks* capazes de identificar componentes de medição para a engenharia de tráfego. Dentre esses componentes, alguns apresentam maiores relevâncias para uma análise mais eficaz, tais como escalas de tempo, bases para medição, interfaces, medição baseada em MPLS[4] e entidades de medição*,* as quais comentaremos a seguir:

[4] *MPLS* (*Multiprotocol Label Switching)* é um protocolo de roteamento baseado em pacotes rotulados, onde cada rótulo representa um índice na tabela de roteamento do próximo roteador.

- Escalas de tempo: para cada tipo de gerenciamento existente na rede, pode-se atribuir uma escala de tempo diferente. Como exemplo, a gerência de planejamento de rede possui uma escala de tempo grande ou muito grande, pois uma mudança na configuração requer uma constante avaliação, cuja alteração dure dias ou meses a fim de não ocorrer impactos significativos ou perda de desempenho.

Já na gerência de capacidade, onde os *SLA's*[5] (*Service Level Agreement*) entram em evidência, há uma necessidade de obter uma rotina de análises, cujas alterações acontecem em um espaço de tempo não muito longo a fim de atender demandas estratégicas da corporação ou reverter algumas falhas toleráveis. Possuindo uma gerência de controle, há informações que se modificam muito rapidamente, necessitando de mudanças cujas alterações possuem um tempo muito menor do que nos outros tipos de gerências, objetivando a recuperação de falhas e perdas de dados importantes em serviços diferenciados obtidas por falhas de infra-estrutura, reequilibrando a carga e retornando o funcionamento de todos os nós e enlaces o mais rápido possível.

- Bases para a medição: é importante notar que, dentre vários pontos da rede, haverá uma diferença enorme na coleta de dados entre esses pontos devido ao maior e menor fluxo de dados que passarão nas mais diferentes interfaces de coletas. Por exemplo, em roteadores de borda ou concentração (roteadores responsáveis pela entrada de todos os dados em uma determinada rede) haverá um fluxo muito grande de dados, porém, em roteadores de qualquer outro ponto, haverá uma quantidade menor e um fluxo totalmente diferente. Por isso, o fluxo de um dado ponto da rede, compreendendo uma origem e um destino, servirá como base de medição para uma engenharia de tráfego.
- As interfaces e nós alocados por toda a extensão da rede podem servir também como base de medição na engenharia a partir do momento em que esses equipamentos detêm todas as rotas definidas dos pacotes que por eles ultrapassarem. Daí se torna necessária uma análise estatística da quantidade

[5] *SLA(Service Level Agreement)* ou acordo de nível de serviço é a parte do contrato de serviços entre duas ou mais entidades no qual o nível da prestação de serviço é definido formalmente

perdida e processada desses pacotes, contribuindo como informação relevante nas medições.

- Medição baseada em caminhos MPLS. De forma semelhante ao do fluxo, o caminho sugere uma análise de uma forma mais abrangente pelo fato de que, por esse caminho MPLS, poderão percorrer diversos fluxos, ou seja, de um nó de origem para um nó de destino, não se observa apenas um fluxo simples, mas é necessário considerar o conjunto deles.
- Entidades de medição: definidas as bases de medição, a análise pode ser iniciada com as medições propriamente ditas, possuindo nomenclaturas e unidades diferentes. Dentre essas entidades, as mais conhecidas são a vazão (*throughput)*, a variação de retardo (*jitter*) e a matriz de tráfego[6].

Por isso, qualquer valor estatístico observado por um tempo e que possui uma unidade caracterizadora de uma rede lógica, poderá servir como uma entidade de medição na engenharia de tráfego. Obviamente que serão determinados limiares norteadores sobre a operacionalidade normal da rede em questão.

[6] *Throughput* é a taxa a que os dados são enviados entre dois pontos da rede em um período determinado de tempo; *Jitter* é o tempo médio de um determinado enlace, perda de pacotes por qualquer motivo, banda disponível em um determinado caminho e etc; Matriz de tráfego é o conjunto de informações existentes a respeito de análises feitas da rede obtidos pelas medições.

3 MPLS *(Multiprotocol Label Switching) e TE (Traffic Engineering)*

Com a crescente exigência de aplicações de tempo real, voz e vídeo, houve uma motivação em agilizar o processo de roteamento para suportar o tráfego cada vez maior. Como esse processamento era feito baseado nos pacotes IP, o tempo de roteamento se tornava muito elevado para esta tecnologia. A partir dessa necessidade, o IETF padronizou o MPLS, baseado na combinação de três tecnologias apresentadas por três principais empresas, Ipsilon (tecnologia *IP Switching*), Toshiba (tecnologia *Cell Switching Router*) e a Cisco (tecnologia *Tag Switching*), demonstrando o conceito de comutação dos pacotes IP de forma mais rápida que os processos anteriores.

O principal objetivo desta tecnologia é a solução dos problemas de redes atuais como velocidade, escalabilidade, qualidade dos serviços e engenharia de tráfego (TE). Por isso, uma das vantagens, está na relação do aumento no rendimento da rede, uma vez que existe uma facilidade de implementação dessa engenharia, escolhendo caminhos com maior velocidade e prioridades para distribuição da carga de um enlace congestionado.

O MPLS é utilizado principalmente em *backbones*[7] e sua principal aplicação consiste na utilização em conjunto com a tecnologia IP, o que se torna possível a interoperabilidade de roteamento dos pacotes com a comutação de circuitos. Outra aplicação muito significativa que esta tecnologia pode implementar é a construção de *Virtual Private Network – VPN's* de grande abrangência, onde os dados conseguem trafegar pelo túnel MPLS de forma segura em uma rede aberta, sem serem descobertos por terceiros.

Por tudo isso, esta tecnologia se torna responsável por dar suporte a diversas aplicações que necessitam de um serviço diferenciado com qualidade sobre a infraestrutura de redes.

[7] *Backbone* significa "espinha dorsal", e é o termo utilizado para identificar a rede principal pela qual os dados de todos os clientes passam.

3.1 Elementos de uma rede MPLS

Para o entendimento do funcionamento de uma rede de domínio MPLS, é necessário conhecer o significado e o papel de cada elemento pertencente a essa rede. Fisicamente, uma rede MPLS é formada por um conjunto de roteadores camada três, ou seja, roteadores que suportam o protocolo de distribuição de rótulos para comutação.

Dependendo da topologia e da localização de cada um desses roteadores dentro da rede, pode-se ter uma denominação e um conceito diferente para cada um deles. 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 3.1 ilustra a distribuição desses elementos ao longo de uma rede.

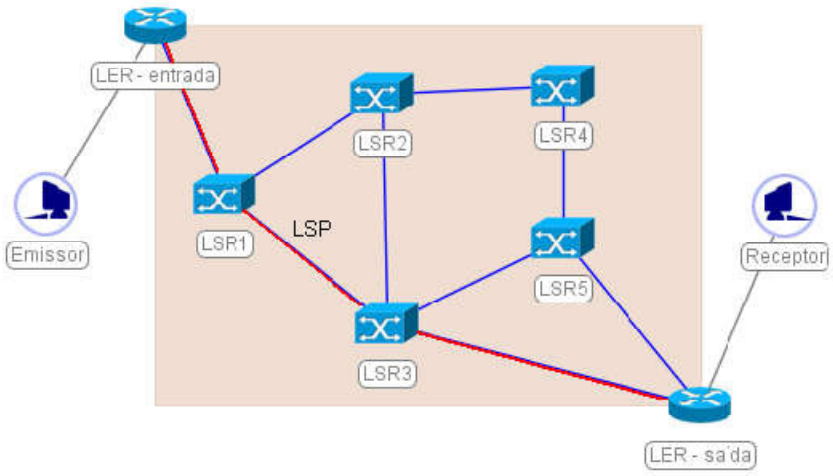


Figura 3.1 – Elementos de uma rede MPLS

Os LSR's são roteadores que se encontram no interior da rede e são fundamentais para a comunicação com outros roteadores, aonde irão se certificar de informações sobre os enlaces, efetuando a expedição de pacotes com seus rótulos a um ritmo de níveis elevados, gerando um caminho chamado LSP (*Label Switching Path*), ligando a origem (roteador localizado na borda de entrada do fluxo) ao destino (roteador localizado na borda de saída do fluxo). Na fronteira da rede MPLS, estão os roteadores chamados LER's que, por se localizarem na entrada e saída da rede, implementam as políticas de acesso determinadas pelo administrador da rede, além

de inserir os rótulos (roteadores de entrada) e retirar rótulos (roteadores de saída) nos pacotes que trafegam por esta rede.

Uma FEC (*Forward Equivalence Class*) é um conjunto de pacotes que foram tratados pelo roteador de entrada para expedição, no sentido de classificar esses pacotes, aplicando alguns processamentos nos campos de cabeçalho: requisitos de *QoS*, tipo de aplicação, identificador de *AS/VPN*, as sub-redes de origem/destino e grupos de *multicast*, gerando um rótulo distinto apropriado para cada requisição associada.

Algumas características presentes na FEC são importantes para que se faça engenharia de tráfego eficientemente, como por exemplo, a atribuição de várias FEC's associadas ao mesmo caminho LSP e vários caminhos LSP's associados à mesma FEC, gerando assim, uma melhora da agregação dos fluxos desses pacotes. Outra importante característica é a possibilidade de configuração explícita dos caminhos LSP's atribuídos a cada FEC relacionada, executando-se de forma administrativa pelo gerente da rede ou de acordo com as necessidades de recursos requisitadas, baseadas em restrições.

O *Label* ou rótulo MPLS também chamado de *Shim Header*, 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). Dentro de uma rede MPLS os rótulos são pequenos identificadores colocados nos pacotes durante seu tráfego pela rede. Eles são inseridos pelos roteadores de entrada e removidos definitivamente pelos roteadores de saída. Os rótulos possuem a seguinte estrutura:

|-20bits Label-|-3bits CoS-|-1bit Stack-|-8bits TTL-|

Os três bits de *CoS* (*Class of Service*) são usados para determinação de classes de enfileiramento e descarte de pacotes, podendo-se utilizar prioridades para certos pacotes. O bit *Stack* é usado para a criação de uma pilha de rótulos, usada de forma hierárquica, ou seja, durante a movimentação dos pacotes pela rede, os rótulos mais externos dessa pilha, serão removidos e os mais internos, atravessarão os roteadores que formam o caminho LSP até chegar aos roteadores de saída, removendo-os definitivamente.

A *Label Information Base* (LIB), nada mais é do que uma tabela que contém informações acerca dos rótulos de entrada e saída de cada um dos roteadores

localizados no interior da rede, estruturada em campos como índices dos rótulos, interface de entrada e saída, e o IP do próximo *hop* (salto). Assim que um caminho LSP é criado, a relação entre interface e rótulo é armazenada na LIB.

3.1.1 Distribuição de rótulos

Cada roteador localizado no interior de uma rede MPLS irá atribuir um rótulo para cada caminho LSP formado. Por isso, um roteador localizado mais próximo à origem do fluxo do tráfego, deverá conhecer qual o rótulo que o roteador que está localizado mais distante dele utiliza para identificar esse caminho LSP.

O responsável pela distribuição dos rótulos em uma rede MPLS é um protocolo denominado LDP (*Label Distribution Protocol*). O funcionamento deste protocolo se dá com a troca de mensagens entre os roteadores localizados no interior da rede, sobre informações de mapeamento do caminho LSP e a FEC respectiva. Isto é feito de forma bidirecional entre eles, abrindo uma sessão de comunicação, cujas informações de controle e alcance dos rótulos são trocadas. Atualmente o LDP foi modificado para que este consiga suportar o encaminhamento de rótulos com restrições, o que é fundamental para implementação de serviços diferenciados e engenharia de tráfego de rede. Por serem configurados nos roteadores localizados na fronteira das redes MPLS, os LER's devem possuir um desempenho muito alto devido à distribuição dos rótulos na entrada e a retirada desses na saída da rede.

3.2 Encaminhamento com restrições e MPLS-TE

Os protocolos IGP[8] convencionais implementados dentro da rede MPLS, por si só não atendem todas as necessidades de recursos e nem otimizam os cálculos de métrica escalares (como por exemplo, o número de saltos). Para administrar métricas do IGP no encaminhamento entre dois pontos, se torna bastante difícil na medida em que o estado da ligação e a forma como são manipuladas no domínio MPLS, são diferentes das métricas utilizadas na arquitetura de serviços integrados (arquitetura *IntServ)* de uma rede IP tradicional. Por isso, os protocolos de

[8] IGP protocolos utilizados no interior de uma rede. Composto de três protocolos (RIP, Hello, OSPF).

encaminhamento baseados em restrições, buscam encontrar uma rota que otimize uma certa métrica e ao mesmo tempo não viole alguma restrição solicitada (como por exemplo, largura de banda mínima). Sendo assim, torna-se necessário a sinalização para implementação desses serviços utilizando-se as métricas IGP.

As principais soluções desenvolvidas para esta tarefa de sinalização são: Constraint *Based Label Distribution Protocol* (CR-LDP) e o protocolo *Resource Reservation Protocol* (RSVP) que atualmente já possui extensões de engenharia de tráfego com MPLS, chamando-se *Resource Reservation Protocol with Traffic Engineering* (RSVP-TE).

3.2.1 *Constraint Based Label Distribution* (CR-LDP)

O CR-LDP é construído sobre o LDP, que já é parte do MPLS. Embora os estudos do *IETF MPLS Working Group* tenham sido abandonados, este protocolo possui resultados satisfatórios e não implica a implementação de um novo protocolo, com o consequente aumento na carga de processamento, tal como acontece com o preferido RSVP-TE (VEIGA, 2009).

As principais características do protocolo são: o uso de um esquema de codificação parecida com o LDP tradicional de redes MPLS denominado TLV *(Type-Lenght-Value)* que são mensagens passadas pela rede, possuindo três campos diferentes. O campo *type* (define o tipo da mensagem), o campo *length* (especifica o tamanho em bytes do campo *value*), o campo *value* (codifica a mensagem que é interpretada de acordo com o tipo). Com a manipulação desses três campos, pode-se implementar a engenharia de tráfego na rede MPLS. Outra característica deste protocolo é o suporte explícito de encaminhamentos do tipo *stric* e *loose*, onde no primeiro tipo, o caminho completo a ser seguido se torna fixo e o segundo tipo, somente alguns nós ou routeadores do caminho todo se tornam fixos. Além dessas características, para descobertas de novos nós em uma rede MPLS, o CR-LDP usa o protocolo *User Datagram Protocol* (UDP) e para realização de controle e gestão, mensagens *label request e label mapping*.

3.2.1.1 Funcionamento do CR-LDP

O funcionamento da sinalização usando o CR-LDP se dá basicamente através das mensagens *label request* e *label mapping.* Todo o processo de distribuição e solicitação do estabelecimento de rota se inicia no LSR de borda quando é gerado um *label request* que é o possuidor de campos indicadores dos parâmetros de recursos requeridos. Após a reserva desses recursos requeridos para o novo caminho LSP, a mensagem para estabelecimento de comunicação é encaminhada para o próximo nó (*router*) numa sessão TCP. Este processo é feito de nó em nó até que o LSR de saída pertencente ao LSP receba esta mensagem, e a partir daí é gerado um *label mapping* que fará com que percorra por todos os nós anteriores, chegando ao roteador de entrada que concluirá informações dos recursos reservados para o LSP, alocando-os.

Existem diversos objetos característicos deste protocolo: o ER (*Explicit Route*) é um campo das mensagens CR-LDP que especifica o caminho que um LSP deve tomar no momento em que está a ser estabelecido. É composto por um ou mais *ER-Hops* que constituem a especificação dos *routers* que fazem parte do caminho definido para o LSP (VEIGA, 2009).

Para controlar erros por falta de recursos ou outro tipo de falha no estabelecimento de um CR-LSP, o protocolo possui notificação de mensagens que carregam o campo *Status TLV's* que identificam os eventos sinalizados. Se um LSR receber uma mensagem de notificação, este deverá desalocar todo o recurso previamente alocado para tal caminho e ainda propagar para o LSR anterior se estes recursos estiverem associados a ele. Essas notificações são propagadas até o roteador de entrada, o qual gerou o *label request message*. A figura 3.2 ilustra o funcionamento básico de troca de mensagens entre os roteadores de um caminho LSP implementado com o protocolo CR-LDP.

Apesar das boas referências deste protocolo acima expostas, há uma diferença que motiva a preferência do IETF – *Internet Engineering Task Force* pelo RSVP-TE, presente no fato do CR-LDP ser do tipo *Hard State* caracterizando o fechamento do circuito virtual somente após um pedido expresso de desconexão

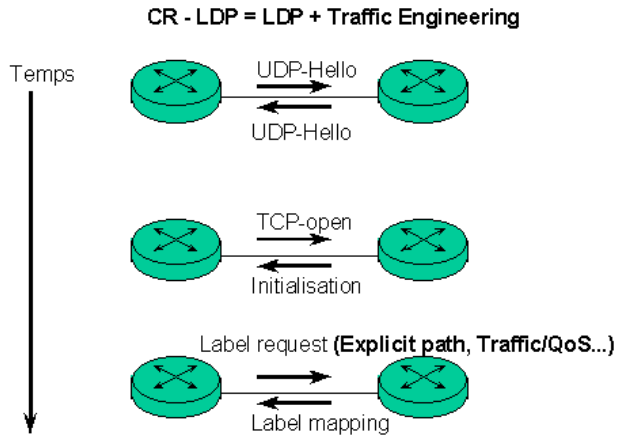


Figura 3.2 – Funcionamento de troca de mensagens do protocolo CR-LDP.

enviado, ao passo que o RSVP-TE é do tipo *Soft State* que se caracteriza por envios de mensagens periódicas acerca do estado operacional dos circuitos virtuais, podendo ser fechados se ultrapassarem algum tempo determinado de resposta.

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

O protocolo RSVPv1 foi desenvolvido para contornar congestionamentos de rede, pela inteligência proporcionada aos roteadores para decidir, antecipadamente, qual o caminho que atenderia às necessidades do fluxo de tráfego de uma aplicação e então reservar os recursos necessários (AMORIM & SILVA, 2007). Assim como o CR-LDP, o RSVP é uma técnica de sinalização usada para reservar recursos através de uma rede, portanto não possui a capacidade de roteamento dos pacotes. O protocolo RSVP-TE é na verdade uma extensão do protocolo RSVP original, suportando o estabelecimento de LSP's que utilizam redes MPLS[9].

O protocolo RSVP-TE possui várias mensagens que são utilizadas nas operações de formação de túneis, são elas: *Path, Resv, PathTear, ResvTear, PathErr, ResvErr, ResvConf, ResvTearConf* (proprietária da *Cisco Systems*) e *Hello*. Para iniciar o

[9] Descrito na *Request for Comments* (RFC3209). RFC é um documento que descreve os padrões para cada protocolo da internet previamente a ser considerado um padrão.

estabelecimento de um caminho, as mensagens *Path message* e *Resv message* se tornam fundamentais para a troca de informações entre origem e destino.

A estrutura do protocolo RSVP-TE é alicerçada com a troca de mensagens e objetos utilizados entre os roteadores definidos para implementação da qualidade de serviço em uma rede MPLS. O quadro 3.1 mostra um resumo das funções definidas que as mensagens do protocolo possuem:

Quadro 3.1 – Resumo das funções definidas

Tipo de Mensagem	Descrição
Path	Usada para configurar e manter reservas
Resv (abreviação de Reservation)	Enviado em resposta a mensagens Path, mas usada para remover reservas da rede.
PathTear	Semelhante a mensagens Path, mas usado para remover reservas da rede.
ResvTear	Enviado para mensagens Resv, mas usado para remover reservas da rede.
PathErr	Enviado por um destinatário de uma mensagem Path, que detecta um erro nessa mensagem.
ResvErr	Enviado por um destinatário de uma mensagem Resv, que detecta um erro nessa mensagem.
ResvConf	Opcionalmente enviado de volta ao emissor de uma mensagem Resv, para confirmar que determinada reserva realmente foi instalada.
ResvTearConf	Uma mensagem proprietária da Cisco para um ResvConf. Usado para confirmar que determinada reserva foi removida da rede.
Hello	Uma extensão definida na RFC 3209, que permite *keepalives* locais do enlace entre dois vizinhos RSVP conectados diretamente.

Fonte: OSBORNE, Eric 2003

Cada tipo de mensagem possui uma identificação única definida previamente para o processo de comunicação. As mensagens *Path* e *Resv* que são trocadas entre a origem e o destino para o estabelecimento do caminho LSP, possuem objetos que são transportados por elas, carregando as informações e características de qualidade de serviço, banda disponível, reservas, possíveis *loops*, rotas explícitas e etc. Além disso, esses objetos fazem parte da constituição de um pacote RSVP-TE juntamente com um cabeçalho (AMORIM & SILVA, 2007).

Os objetos utilizados pelas mensagens *Path Message* e *Resv Message* são: *Label Request Object, Label Object, Flowspec Object, Explicit Route Object, Record Route Object, Session Object, Sender_Template Object, Filter_Spec Object* e *Session_Atribute Object*.

É importante esclarecer que além dos objetos serem separados por classes, dentro de cada classe, há outra separação por tipo de classes, definida no como Tipo C do objeto, criando assim, uma espécie de hierarquia de tipos.

O objeto *Label Request Object* é basicamente utilizado por uma mensagem do tipo *Path Message* para que um router da rede MPLS reserve um *label* de um caminho LSP. Outra característica importante desse objeto está no fato de poder identificar um protocolo de nível 3 como por exemplo o protocolo de roteamento OSPF, BGP-4.

O *Label Object* é utilizado em mensagens do tipo *Resv Message*, confirmando a alocação de um recurso solicitado e posteriormente atualiza a LIB do roteador. Por ter essa característica, na pilha de *labels*, o objeto contém apenas um identificador referenciando o respectivo recurso local da interface onde é percorrido o LSP.

O objeto *Flowspec* é importante pela sua função de especificação da qualidade de serviço que a aplicação requisitará. Alguns requisitos são: nível de QoS, banda a ser alocada, *delay*, taxas de perdas e etc. É claro que, em muitos casos, não se precisa definir esses requisitos por não se tratar de um LSP que necessite desses recursos diferenciados, por isso, caso isso aconteça, o objeto *Flowspec* não possuirá nenhuma informação e o tráfego irá ser associado ao tipo *best effort* (melhor esforço) convencional.

Há situações em que é possível configurar rotas explícitas independente dos protocolos implementados dentro da rede como o IGP. Além disso, existe a possibilidade de manter um nível de QoS nesse caminho LSP através do uso do protocolo RSVP-TE com o objeto *Explicit Route Object* associado a essa rota. Para garantir que isto aconteça, é necessário que a origem conheça todo o caminho por onde irá passar o tráfego (somente por roteadores com o RSVP-TE configurado) e que possui características necessárias para o atendimento desses requisitos de recursos.

O *Explicit Route Object* possui vários sub-tipos de classe, onde é garantido o suporte a vários elementos de rede como o IPv4, IPv6, *Autonomous System Number* e Terminação MPLS LSP.

Outro objeto de grande importância e de fundamental implementação é o *Record Route Object* (RRO), capaz de gravar e identificar cada elemento de rede por onde as mensagens *PATH e RESV Messages* passam, por isso, é utilizado por elas. Porém, o RRO possui um número limitado de elementos a ser gravado e por

isso, quando esse limite for ultrapassado, será enviado um *PathErr* ou um *ResvErr* no intuito de retirar o RRO da mensagem. É possível aplicar este objeto de forma a descobrir loops de roteamento e loops de rotas explicitas que não obtiveram êxito em suas implementações (AMORIM & SILVA, 2007). Esse objeto possui atualmente dois subtipos de classe, sendo uma para o IPv4 tradicional e o novo IPv6.

Há outros tipos de objetos com funções específicas como, por exemplo: *Session Object* utilizado pelo *Path Message* para identificar um LSP; *Sender_Template Object* também utilizado pela Path Message para informar o formato dos dados; *Filter_Spec Object* que define em conjunto com o *Session Object*, o fluxo de dados que possuirá as características definidas pelo *Flowspec Object* e o *Session_Atribute Object* que controla a prioridade do caminho LSP em casos de preempção utilizado pela mensagem *Path Message*, podendo ajustar as sessões baseado nas prioridades antigas e atuais e com valores maiores e menores.

Esse objeto em específico se torna muito importante para implementação de engenharia de tráfego na medida em que há circuitos virtuais com reservas similares de recursos, podendo-se determinar a política e estratégia de utilização da banda em períodos críticos de solicitações.

3.2.2.1 Funcionamento do RSVP-TE

O funcionamento do protocolo é baseado em operações que ocorrem nos túneis LSP's, sendo essencialmente constituídas por troca de mensagens entre a origem e o destino do túnel. As reservas que o protocolo faz, necessita ser atualizada de tempos em tempos, tornando-lhe não rígido. Uma requisição solicitada, somente irá desaparecer se for explicitamente pedido ou tiver seu tempo de vida esgotado.

Com base na figura 3.3 mostra-se uma rede MPLS com seus roteadores de fronteira (LER's) e os de *backbone* (LSR's) configurados com o protocolo RSVP-TE. É importante notificar que, além da arquitetura MPLS, há um protocolo de roteamento (IGP) dentro da rede, responsável por definir caminhos para a comunicação entre as duas estações.

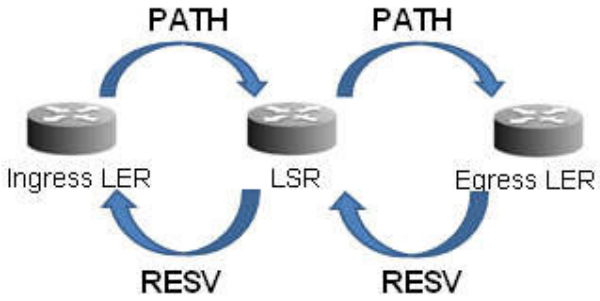


Figura 3.3 – Funcionamento de troca de mensagens do protocolo RSVP-TE.

A estação de origem requisita um caminho com qualidade de serviço para alcançar a estação de destino enviando uma mensagem do tipo *Path Message*, contendo todas as informações referentes ao tipo de recurso, tráfego e qualidade de serviço a ser utilizado.

A mensagem do tipo *Resv Message* é enviada da estação destino para a estação de origem percorrendo o mesmo caminho seguido pela mensagem *Path Message* reservando todos os recursos de QoS requisitados, estabelecendo o caminho de túnel LSP. Por isso, o protocolo RSVP-TE é dito orientado pelo destinatário ou *Receiver Oriented*. Devido à troca de mensagens do tipo *Path Message* e *Resv Message* ser feita periodicamente entre os roteadores, o protocolo é do tipo *softstate*, possibilitando o rápido re-roteamento dos caminhos LSP's.

A verificação da disponibilidade de recursos e a alocação de um *label* para o LSP são duas tarefas que serão realizadas em todos os nós (*routers*) do túnel. Porém, se algumas dessas duas tarefas não puderem ser efetivadas, haverá uma mensagem de erro chamada *PathErr* ou *ResvErr* (dependendo do sentido da requisição) e o túnel não será estabelecido.

Um *PathErr* é enviado quando um label não pode ser alocado para um *Path Message* devido uma indisponibilidade de faixa para alocação. O código padrão para este tipo de procedimento é: *Routing Problem* e com o valor: MPLS *label allocation failure*. Além do formato normal do *label request*, há outros que especificam faixas de valores para VPI e VCI em redes ATM e DLCI para redes *Frame Relay,* demonstrando o poder de utilidade em pacotes de diferentes tecnologias de redes.

Diante dos principais tipos de objetos utilizados no mecanismo de alocação de recursos, há três possibilidades de se reservar tais recursos. A primeira forma é chamada de *Fixed Filter* (FF), como o nome já diz, não há uma mobilidade de

recursos, se trata de uma forma fixa para um único par origem-destino, sem compartilhamentos. A segunda forma é chamada de *Shared Explicit* (SE), permitindo que a origem solicitante do recurso, compartilhe com elementos diferentes e com necessidades diferentes. Nesse modelo de reserva, é utilizado o conceito de *make-before-break* que significa a realocação de recursos de um LSP danificado (com interrupções de tráfego ou queda de performance) para outro LSP antes que o primeiro seja desativado (AMORIM; SILVA, 2007). A terceira forma de reserva é chamada de *Wildcard Filter* (WF) e compartilha apenas um único recurso reservado não podendo assim ter atributos de engenharia de tráfego e por isso não é utilizado pelo RSVP-TE.

3.3 Classes de serviços e MPLS-TE

Um campo de 8 bits chamado DS (*Differentiated Services*), presente no protocolo IP, dá o suporte a arquitetura de serviços diferenciados de forma a inserir informações (classificação) nos pacotes para que sejam analisados. Todas as informações de classificação estão inseridas nos primeiros 6 bits do campo, denominado DSCP (*Differentiated Services Codepoint*). O modelo DiffServ não necessita de um protocolo próprio (como no caso do RSVP, usado no IntServ), pois aqui se utiliza um campo do próprio datagrama IP. Tudo que um roteador precisa fazer é examinar o campo DSCP de cada pacote para determinar qual tratamento a ser dado ao mesmo. (TEIXEIRA, 2000).

A primeira tarefa ao implementar serviços diferenciados é ter a capacidade de classificar os pacotes. Isto nada mais é do que fazer uma análise para saber sobre qual o tipo de regra que cada um deles será executada.

Os pacotes com a tecnologia MPLS são classificados apenas comparando o valor do campo EXP de 3 bits, presente nos rótulos, ou seja, não há forma de comparação distinta, pois o MPLS encapsula o protocolo IP. Além disso, somente os rótulos encontrados no topo da pilha serão comparados, uma vez que são os únicos visíveis para os roteadores, decorrentes de sua hierarquia.

Para que os serviços sejam classificados através desses pacotes, é preciso que seja feito um tratamento na pilha de rótulos, especialmente no campo EXP, uma vez que haverá um encapsulamento de vários rótulos com o campo referido.

O primeiro caso a ser considerado, é observado nos pacotes IP que entram em uma rede MPLS, conhecido como *ip-para-mpls* e normalmente escrito como *ip2mpls*. Quando os pacotes IP entram numa rede MPLS, há uma operação de empilhamento (*push*), ou seja, os rótulo MPLS é empilhado sobre o pacote IP não rotulado.

Por padrão, quando o software da Cisco empilha rótulos sobre um pacote IP, os bits mais significativos no campo DiffServ (os *bits IP Precedence*[10]) são copiados para o campo EXP de todos os rótulos empilhados (OSBORNE, 2003).

O segundo caso a ser considerado, é observado em pacotes MPLS que estão trafegando num domínio MPLS, ou seja, pacotes que já possuem rótulos sendo empilhados por outros rótulos. Isto é conhecido como *mpls-para-mpls* ou *mpls2mpls*. Quando ocorre a operação de empilhamento, o campo EXP do rótulo mais abaixo da pilha é copiado para o rótulo mais acima da pilha. Essa troca é chamada de caminho (*path*) *mpls2mpls*. No entanto, por existir uma pilha de rótulos, três ações são possíveis de ser manipuladas nesse âmbito:

- Empilhar (*Push*): rótulos MPLS são acrescentados a um pacote que já possui rótulo;
- Trocar (*Swap*): rótulos que se localizam no topo da pilha, é trocado por outro rótulo;
- Desempilhar (*Pop*): rótulos mais externos são removidos, mas pelo menos um rótulo ainda permanece na pilha;

O último caso é observado quando a pilha de rótulos é completamente removida, resultando apenas num pacote IP tradicional. Isto é chamado de *mpls-para-ip* ou *mpls2ip*. A única operação presente é a de desempilhar (pop) todos os rótulos da pilha, resultando em um pacote IP tradicional.

O suporte do MPLS para serviços diferenciados possui uma particularidade devido à limitação encontrada nesta tecnologia. Isto se deve ao fato de que o rótulo MPLS, com seu campo EXP (utilizado para marcação de pacotes) de três bits, foi definido anteriormente ao DSCP (utilizado para classificação de serviços em pacotes IP) de seis bits. Em consequência disso, serviços diferenciados sem o uso do MPLS, poderão ter 64 possibilidades de classificação DSCP, e com esta tecnologia,

[10] *IP Precedence* é a referência para os três dos seis *bits* presentes no cabeçalho IP que são copiados para o rótulo.

somente oito possibilidades de classificação. Por isso, foram desenvolvidos dois métodos para aliviar tal problema. O primeiro método chamado de E-LSP possui a ideia de que se a rede possui até oito classificações de serviços diferenciados, o campo EXP do pacote MPLS é suficiente para mapear e transmitir os valores deste campo para essas classificações, utilizando o DSCP normalmente. Porém, se a rede possuir mais de oito classificações de serviços, o método chamado L-LSP utiliza tanto o campo EXP de três bits como o próprio rótulo MPLS para definir essas diferentes classificações.

3.4 Proteção e restauração

Apesar da implementação de toda uma engenharia de tráfego em uma rede corporativa, sempre haverá momentos que tudo ou parcialmente não funcionará devido alguma falha física ou lógica. Partindo para o foco no núcleo dessas redes (roteadores), podemos ter falhas de enlace (caracterizando-se na ligação desses roteadores) e falhas de nó (o próprio roteador). Uma falha no enlace pode ser uma fibra cortada, cabos mal conectados e etc. Já uma falha no nó pode ser representada por falta de alimentação do roteador, problemas administrativos ou desligamentos preventivos.

Acontece que a MPLS-TE e sua capacidade de direcionar o tráfego para fora do caminho mais curto, derivado pelo IGP, ajuda a aliviar a perda de pacotes associadas a falhas de enlace ou nó na rede. A capacidade da MPLS-TE de fazer isso é conhecida como Fast Reroute (FRR) ou simplesmente MPLS-TE *Protection* (OSBORNE, 2003).

A proteção para alguma eventualidade de falha está relacionada à perda mínima de pacotes após esse evento. Os recursos a serem protegidos podem ser físicos (roteadores ou fibras/cabos) e lógicos (caminhos LSP's). O termo proteção deverá estar associado ao fato de que recursos de backup são pré-estabelecidos e não são sinalizados depois que uma falha tenha ocorrido.

Se os recursos de proteção não fossem pré-estabelecidos, eles teriam que ser configurados depois da detecção da falha; nesse caso, seria tarde demais (OSBORNE, 2003).

3.5 VPN/MPLS

Com a crescente expansão de grandes empresas, houve também um espalhamento das extensões dessa empresa, ou seja, escritórios (redes locais – LANs) foram montados em diferentes lugares separados por grandes distâncias. Com isso, gerou-se uma motivação em interligar esses escritórios de forma que todos os usuários pertencentes a cada localidade não pudesse notar essa separação, nascendo assim as redes virtuais privadas de cada empresa.

Este tipo de rede, que interconecta vários sites (redes corporativas), através de uma infraestrutura de rede compartilhada é chamado de VPN (*Virtual Private Network* - rede privada virtual). (DE QUEIROZ, 2000).

Esse tipo de tecnologia é feito geralmente utilizando-se a infraestrutura pública, realizada por provedores de serviços, que no caso é a *Internet* e todo o seu *backbone*.

De acordo com Veiga (2009) as VPN's são túneis de criptografia entre pontos autorizados, criados através da Internet ou de outras redes públicas e/ou privadas para transferência de informações, de modo seguro, entre redes corporativas ou utilizadores remotos. A principal característica ou principal requisito para criação de uma VPN é o estabelecimento de um mecanismo de segurança como a criptografia de dados, ou seja, em uma rede virtual ligando duas ou mais redes locais, há um isolamento dos dados dessas redes pertencentes à VPN, de modo que não haja uma mistura desses dados com os demais de outras redes ou da Internet. Isto é possível, pois em uma rede MPLS, os pacotes percorrem a rede pública através de caminhos estáticos do tipo circuito, regidos pela troca de rótulos. Além disso, este protocolo apresenta vantagens de forma agregada a esses circuitos virtuais, podendo ser implementada a engenharia de tráfego.

A VPN deve dispor de recursos para permitir o acesso de clientes remotos autorizados aos recursos da LAN corporativa, viabilizar a interligação de LANs de forma a possibilitar o acesso de filiais, compartilhando recursos e informações e, finalmente assegurar privacidade e integridade dos dados ao atravessar a Internet e a própria rede corporativa. (Veiga, 2009)**.** Outra principal vantagem do uso de VPN é a redução do custo das comunicações das redes de empresas corporativas, uma vez que o estabelecimento de circuitos virtuais com *links* dedicados de longa distância são substituídos pelo *backbone* da Internet.

3.5.1 Métodos de VPN

Além da possibilidade de uma VPN ser implementada por vários dispositivos, equipamentos específicos ou softwares, ela pode ser executada obtendo-se principalmente duas formações, como LAN-to-LAN (entre redes locais) ou USUÁRIO-to-LAN (acesso remoto).

A solução VPN de ligação entre redes locais, figura 3.4, se dá através da Internet, em substituição a *links* dedicados de longa distância, onde cada rede local possui um *link* dedicado local ao provedor de acesso a Internet, disponibilizado 24h por dia para o tráfego da VPN.

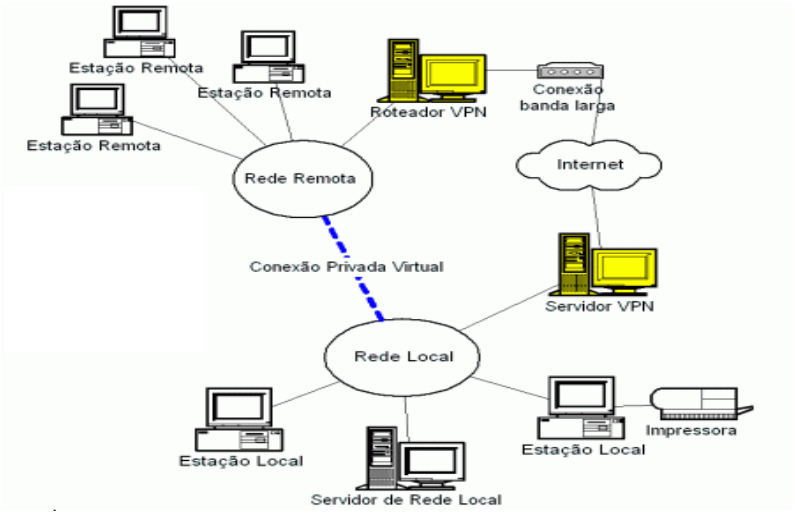


Figura 3.4 – Rede virtual privada.

O acesso remoto se dá através da ligação de um ISP (*Internet Service Provider*) e da rede local, onde a estação que deseja se conectar remotamente, liga-se à Internet e ao software de VPN, que geralmente é instalado na máquina do usuário, cria uma rede virtual privada entre a estação e o servidor corporativo. A figura 3.5 ilustra a arquitetura de um acesso remoto feito através de uma infraestrutura VP.

De um modo geral, o tunelamento virtual de pacotes é uma tecnologia conhecida antes da formação de VPN's e consiste basicamente em encapsular um protocolo dentro de outro protocolo. O processo de tunelamento possui as fases de encapsulamento, transmissão ao longo do caminho lógico e desencapsulamento do

pacote para seu destino final. O protocolo que encapsula o pacote realiza uma adição de um cabeçalho que possui informações de encaminhamento do mesmo, onde será determinado o túnel, que nada mais é do que o caminho lógico a ser percorrido pela rede intermediária entre a origem e o destino.

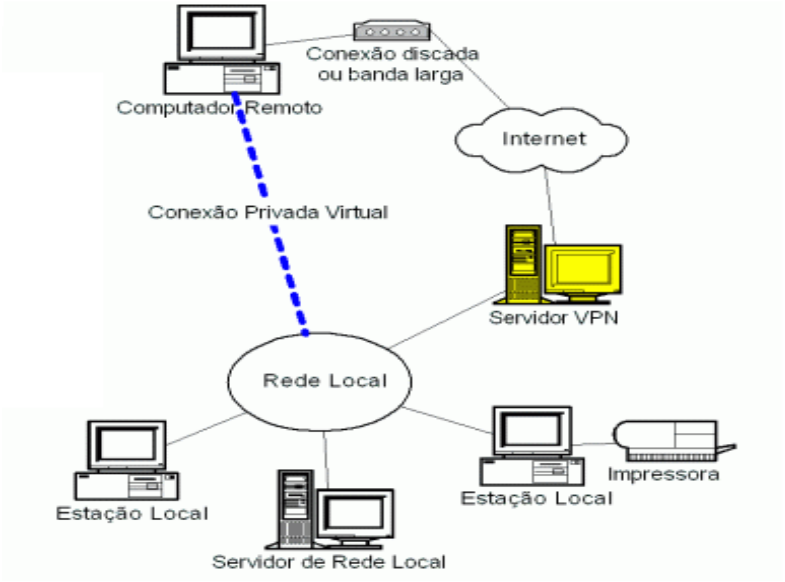


Figura 3.5 – Acesso remoto feito através de uma infraestrutura VP.

3.5.2 Modelos de VPN

As técnicas mais comuns utilizadas para prover o serviço de VPN estavam baseadas no modelo chamado *Overlay* com predominância do protocolo *Frame Relay*, que se caracteriza pela ligação ponto a ponto entre as redes. A figura 3.6 ilustra este modelo de ligação entre as redes. A vantagem deste modelo pode ser identificada a partir do isolamento das redes gerado por essas ligações, o que traz alguma forma de segurança. Esse tipo de modelo, no entanto, possui várias desvantagens ou pontos críticos de escalabilidade, uma vez que se torna complexo o gerenciamento de muitos enlaces no sentido do próprio cliente operar sua VPN, configuração de requisitos de QoS IP, QoS de camada 2 e o mapeamento entre essas duas camadas.

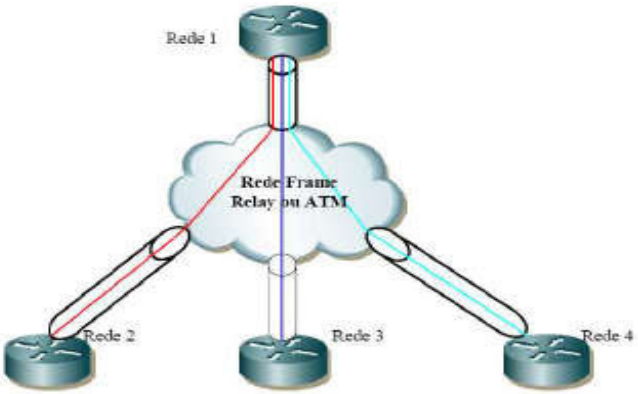


Figura 3.6 – Modelo VPN *Overlay*
Fonte: BOAVA, Adão 2004.

O modelo *Peer-to-Peer* possui a característica de oferecer um serviço de VPN em grande escala, ou seja, pela simplicidade por parte do usuário de trocar informações com um ou poucos roteadores de borda do provedor. A figura 3.7 ilustra este tipo de modelo possuidor de um roteador compartilhado.

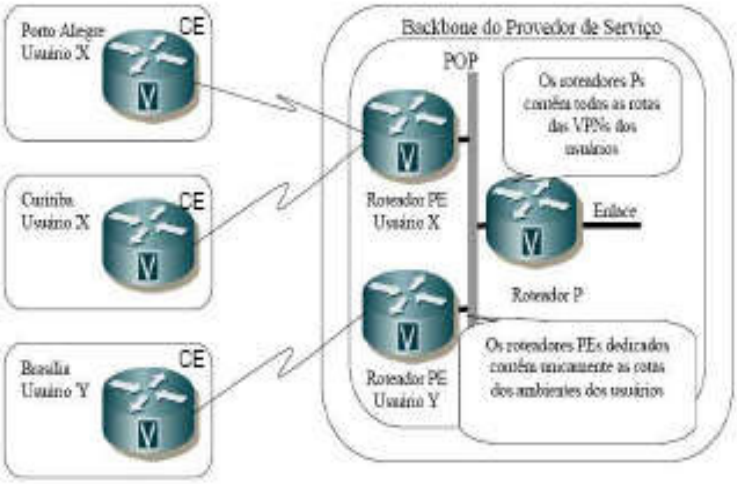


Figura 3.7 – Modelo *Peer-to-Peer* com roteador compartilhado.
Fonte: BOAVA, Adão 2004.

Este modelo se torna mais simples devido os roteadores do provedor possuírem o conhecimento da topologia do cliente, simplificando também o trabalho de incorporação de novas localidades. A partir da figura 3.8, pode-se observar que o roteador de borda do lado provedor pode ser dedicado ou compartilhado por clientes de diferentes VPN's.

Com a introdução do MPLS, que combina os benefícios do *switching* da camada 2 e do *switching* e *routing* da camada 3, tornou-se possível construir uma tecnologia que combina os benefícios do *overlay* VPN (como segurança e isolamento entre clientes) com os benefícios do encaminhamento simplificado que o *Peer-to-Peer* VPN proporciona (VEIGA, 2009).

Por apresentar essas características, há uma RFC 2547bis (*Request for Comments*) na qual define a implementação de soluções VPN BGP/MPLS, utilizando o protocolo BGP responsável pela distribuição e encaminhamento das sessões VPN e o estabelecimento dos circuitos virtuais para o fluxo do tráfego utilizado pelo MPLS.

Os principais objetivos trazidos pela RCF 2547bis são:

- Simplificar os serviços para os clientes utilizando todo o potencial do protocolo IP;
- Prover um serviço com grande escalabilidade e flexibilidade topológica;
- Permitir a implementação de regras na criação de VPN's que poderão ter participação direta dos clientes;

A figura 3.8 demonstra os principais elementos de uma rede que se utiliza do protocolo MPLS na formação de redes virtuais privadas com base na RFC 2547bis.

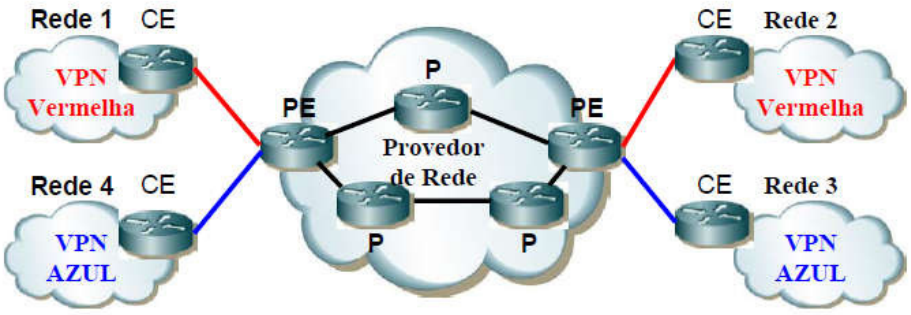


Figura 3.8 – Elementos de uma rede VPN/MPLS
Fonte: BOAVA, 2004.

O caminho LSP (*Label Switched* Path) entre dois roteadores PE's de borda utiliza-se para sua construção, protocolos de sinalização LDP ou RSVP-TE. O roteador de borda PE adiciona dois rótulos como prefixos para cada pacote do tráfego IP do cliente. O “rótulo mais externo” identifica o próximo “salto” ao longo do LSP do provedor de rede, enquanto o “rótulo mais interno” identifica a VPN particular

do cliente, conectada no roteador de destino. A informação do rótulo é trocada durante a sessão de configuração MP-BGP (BOAVA, Adão 2004).

O elemento com a sigla CE (*Customer Edge Devices*), se localiza na borda da rede cliente fazendo a ligação direta com o elemento chamado PE (*Provider Edge Routers*). O CE se apresenta como roteador IP anunciando as rotas dos pontos da VPN local para o roteador PE, aprendendo também as rotas remotas.

O roteador PE (*Provider Edge Routers*), se localiza na borda da rede provedora da VPN trocando informações de roteamento com os roteadores CE's através de rotas estáticas e após isso, há uma troca de informações entre os roteadores PE's com o protocolo BGP. São nos roteadores PE's que se identificam de forma unívoca as informações de encaminhamento de cada VPN.

Outro elemento muito importante e fundamental que compõe uma rede VPN BGP/MPLS são as tabelas de encaminhamento e roteamento dos roteadores PE's. Elas são chamadas de VPN *Routing and Fowarding* (VRF). Cada VPN diferente acessa uma VRF correspondente através de sua interface e todos os pontos que estão conectados ao roteador PE devem fazer parte de uma VRF. Uma VRF se torna fundamental para criação de encaminhamento de pacotes por possuir todas as informações referentes a uma VPN, onde todo o tráfego terá a VRF como principal norteadora do caminho.

Em uma conectividade de rede *Full Mesh*[11], o gerenciamento de largura de banda é feito apenas na entrada e saída de cada acesso VPN, o que simplifica o processo e, além disso, feita a adição de mais um ponto VPN, o único processo a ser realizado para o estabelecimento deste novo acesso VPN é a configuração entre o roteador de borda da rede provedora e o roteador local da empresa. Uma característica importante é que quando foi concebido o protocolo BGP para VPN MPLS, tornou-se necessário uma comunicação direta entre todos os roteadores PE's de forma dois a dois fazendo um *full mesh* de sessões.

[11] *Full Mesh* são redes compostas de várias "células" que se intercomunicam.

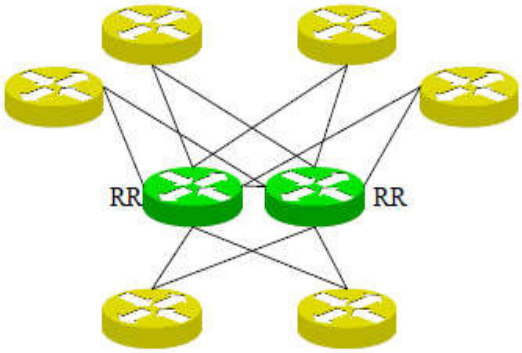


Figura 3.9 – *Route Reflector*.
Fonte: BOAVA, Adão 2004.

Dessa forma, poderia causar problemas de escalabilidade e uma configuração muito complexa, mas foi criado um tipo de roteador atuando como um *Route Reflector* (figura 3.9), agindo como refletores das rotas, onde os elementos PE's estabelecem uma sessão BGP somente com estes roteadores.

4 ESTUDO DE CASO

- ✓ **Estudo da aplicação do MPLS-TE em uma rede corporativa**

No estudo de caso proposto neste trabalho, será apresentada a forma estrutural da área responsável pelo gerenciamento da rede como um todo, englobada por uma área de negócio chamada TI de uma empresa multinacional que possui escritórios em várias localidades do Brasil e do mundo. Além disso, será apresentado o histórico e a evolução da implantação do MPLS para interligar esses sites corporativos, analisando a estrutura atual desta tecnologia, correlacionando com a parte gerencial. Por fim, serão apresentadas duas ferramentas (GNS3 e *WireShark),* utilizadas para demonstrar a emulação dos cenários extraídos da própria realidade da empresa, os serviços implementados com a tecnologia MPLS, suas configurações e as análises de pacotes de tráfego desta rede que serão capturados.

4.1 Evoluções da estrutura de telecomunicações da empresa

Na década de 80, mesmo com unidades de negócios espalhadas geograficamente pelo país, a empresa analisada não possuía meios eletrônicos de comunicação, controlando todos seus processos por meio de documentos oficiais, principalmente através de malotes de correios. Com o advento do avanço na telefonia, passou-se a utilizar um sistema de conexão de máquinas de escrever elétricas a uma rede telefônica, chamado Telex.

Por isso, o único *link* de dados era utilizado através desta ferramenta, o que limitava muito a quantidade de informações que se pretendia trafegar. Paralelo a isso, os links de voz existentes ainda resistiam em serem os principais meios de comunicação e de informações, uma vez que a central de telefonia com toda a sua infraestrutura era gerida e administrada pela própria empresa.

Com o passar do tempo, a empresa se expandiu, tornando-se necessária a colocação dos mainframes de informações em cada localidade, que passaram a ser ligados ponto-a-ponto através de um sistema de rádio de frequência analógico, chamado SHF (*Super High Frequency*). Esse sistema continha uma antena capaz de capturar os sinais analógicos e um multiplexador em cada lado da conexão, distribuindo esses sinais para os modems transformarem em sinais digitais. Por

atravessar por toda essa infraestrutura, as taxas de transmissão para o tráfego eram muito baixas entre as localidades que possuíam esses mainframes.

Por ser utilizada uma estrutura de mainframe principal, ainda não existia a ideia de hosts (computadores pessoais), utilizando-se apenas os terminais burros (terminais com funcionalidades limitadas) que operavam como se estivessem diretamente neles.

Após o sistema de rádio, foi adotada a ligação com fibra óptica na década de 90, quando as antenas responsáveis pela captura dos sinais foram substituídas pelos conversores eletro-ópticos, juntamente com os multiplexadores digitais. Porém os links continuaram a ser diretos e toda essa infraestrutura continuava a ser provida pela própria empresa.

Com o avanço da tecnologia e o oferecimento de uma melhor infraestrutura, a empresa passou a contratar links de telecomunicação, pagando por altos valores para provedores desse serviço (justificados pela novidade tecnológica da época), devido à grande dispersão geográfica dos sites no país. Com isso, foram criadas as redes locais, com servidores locais, em que se rodavam aplicações também locais (não possuíam aplicações padrão para todos os sites) no modelo cliente-servidor, gerando o deslocamento do mainframe de informações para a sede da empresa.

Com o crescimento da empresa e do número de clientes que passaram a utilizar a informática como ferramenta de trabalho, a área de Tecnologia da Informação (TI) ganhou uma importância maior e houve a necessidade de se criar uma área (gerência) que intermediasse todas as necessidades dos empregados, com a implementação de novas aplicações e de novos equipamentos de telecomunicações, a fim de atender a demanda, a qualidade e a continuidade dos serviços.

Em consequência disso, a gerência de projetos de TI alavancou toda a infraestrutura da empresa e o número sistemas, causando um “boom” de mais de 300 novas aplicações, gerando, assim, uma quantidade muito grande de acessos por parte dos empregados aos servidores. Isso era feito de forma desordenada e isolada do resto das unidades de negócios, atendendo apenas as necessidades locais. Em contrapartida, foi observada uma consequente lentidão contínua na rede, justamente por esse crescimento, apontado como principal motivo do gargalo.

Na tentativa de acabar com o gargalo no número de aplicações que eram desenvolvidas de forma separadas, foi feita a adoção e a implantação de um

sistema único, muito grande e segmentado por módulos, em que as principais aplicações de várias áreas de negócios da empresa (recursos humanos, financeiro, sistemas operacionais, voz sobre IP) pudessem ser atendidas por qualquer site distribuído pelo mundo. A partir daí, esse novo sistema passou a ter um nível muito alto de criticidade, pois qualquer falha significaria uma perda considerável de trabalho e de rendimento. Por isso, a área de telecomunicações da empresa passou a ser vista como ponto crítico de seu funcionamento. Porém, como a estrutura do Data Center era centralizada na sede e havia apenas um único canal para acessar essas aplicações, gerou-se um problema de tráfego difícil de ser diagnosticado.

Uma das medidas, para que o problema desse gargalo na rede pudesse ser sanado, foi a adoção de uma política de hostiar as aplicações em um Data Center, ou seja, replicar virtualmente em uma localidade diferente, forçando a distribuição de acesso entre a sede e o novo centro de processamento. Além dessa solução, observou-se a necessidade de ajustar o contrato com a provedora do link de comunicação, com a finalidade de garantir uma qualidade de serviços links específicos, restritos e críticos, indicados pela empresa. Com isso, foi feito um mapeamento de todos os processos prioritários e não prioritários, apontando quais aplicações necessitariam de implementações de qualidade de serviços, a fim de firmar os *SLA's* correspondentes.

Consequentemente à implantação de uma réplica do Data Center, os sites mais distantes geograficamente pelo país passaram a se interligar através da VPN/MPLS (nuvem MPLS), administrada pela provedora. De forma equivalente, os sites localizados em regiões fora do país, se interligam através da nuvem MPLS internacional, administrada por uma empresa provedora internacional.

Atualmente a empresa possui uma infraestrutura de contingência lógica, ou seja, existem dois *links* principais providos por empresas diferentes. Fisicamente, ela ainda não implantou esta redundância, consistindo apenas em um *switch-core*. Como os principais links atualmente são implementados com a tecnologia MPLS, a área gestora de TI monitora todos os enlaces através de um aplicativo gráfico, chamado *Cacti*, analisando todo o volume de tráfego nos feixes de ligações entre os *sites.*

4.2 Ferramentas utilizadas

Atualmente há diversos simuladores e emuladores de redes disponíveis, porém as ferramentas utilizadas, o desenvolvimento da emulação da rede e a sua análise são respectivamente a GNS3 e a Wireshark. A primeira foi escolhida devido tanto à aproximação com a realidade verificada com o uso de IOS's binárias reais dos equipamentos quanto ao suporte da tecnologia MPLS, objeto de estudo desse trabalho.

A segunda ferramenta possui vantagens em capturar pacotes separados por protocolos específicos que trafegam em redes virtuais e reais. Além disso, possui a característica de demonstrar claramente o funcionamento em tempo real de transmissão desses pacotes pelos protocolos, podendo-se tirar conclusões acerca da eficiência deles.

4.2.1 GNS3

O GNS3 é um simulador gráfico de código aberto que permite criar qualquer tipo de topologia de redes, fazendo a emulação dos sistemas operacionais dos equipamentos. Sua arquitetura se baseia na junção de outros projetos, como o Dynamips (emulador de IOS binárias dos sistemas Cisco), Dynagen (ambiente gráfico para o Dynamips) e o Pemu (emulador Pix). A figura 4.1 ilustra o ambiente de emulação da ferramenta.

Com o GNS3, é possível se fazer todas as configurações nos roteadores, switches e Pix Cisco reais, ou seja, este programa é na verdade um emulador, pois utiliza as imagens reais dos equipamentos. Estas imagens correspondem ao sistema operativo dos equipamentos Cisco.

A principal vantagem de se utilizar uma ferramenta como essa é a possibilidade de se testar novas funcionalidades dos IOS's, antes mesmo deles entrarem em produção corporativa.

A escolha dessa ferramenta, para desenvolver este trabalho, se deu pelo fato de ser gratuita e também pela característica de permissão de se poder utilizar a mesma, nos IOS's dos equipamentos reais, o que se aproxima muito de um ambiente real.

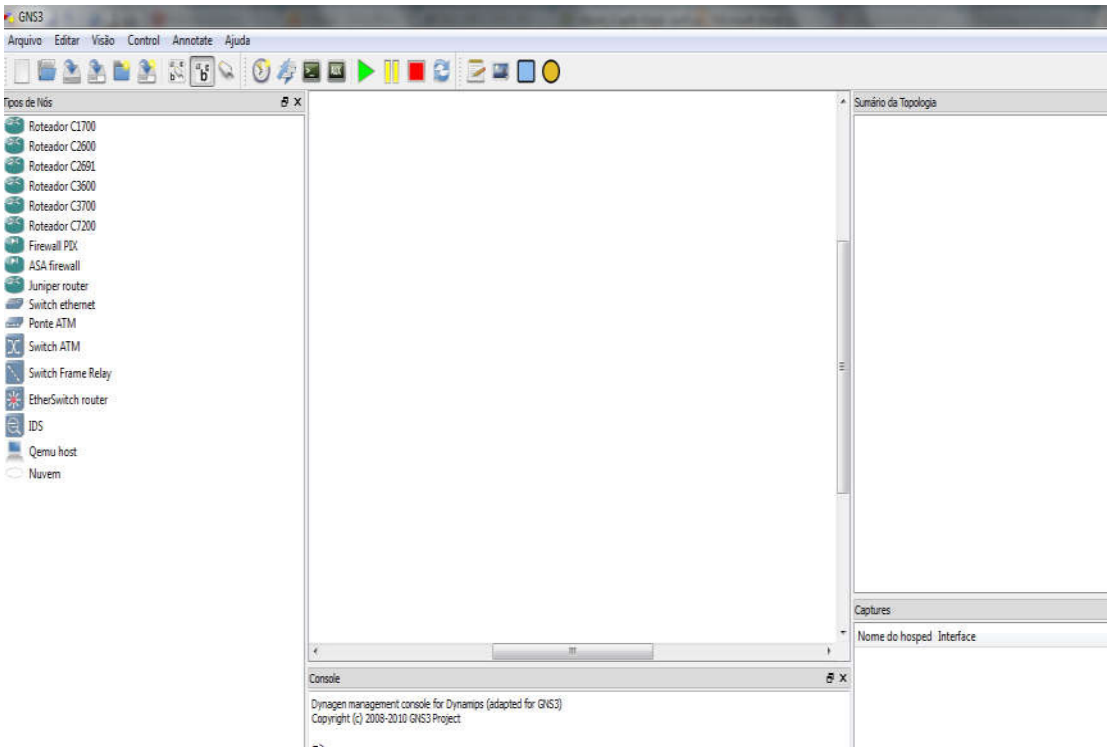


Figura 4.1 - Ambiente de emulação GNS3

Além disso, nem todas as ferramentas encontradas, davam o suporte a MPLS como o GNS3 oferece, podendo aplicar todas as configurações para este tipo de serviço. Por isso, projetistas de redes utilizam esta ferramenta com a possibilidade de implementar grandes redes corporativas com seus *backbones,* qualidade de serviços e engenharia de tráfego, ainda em ambiente de testes.

4.2.2 *Wireshark*

Esta ferramenta apresenta, como principal função, a captura de pacotes em determinada interface de rede. Ela auxilia tanto na resolução de problemas de rede através das análises dos pacotes como também se mostra bastante eficiente para o aprendizado sobre o comportamento de vários protocolos de rede. A figura 4.2 ilustra o ambiente de captura de pacotes em uma determinada rede.

O *Wireshark* faz a captura de todo o tráfego de rede em uma ou mais interfaces de rede. Como o tráfego é muito grande em qualquer interface ativa de rede, diversos protocolos atuantes podem ser encontrados.

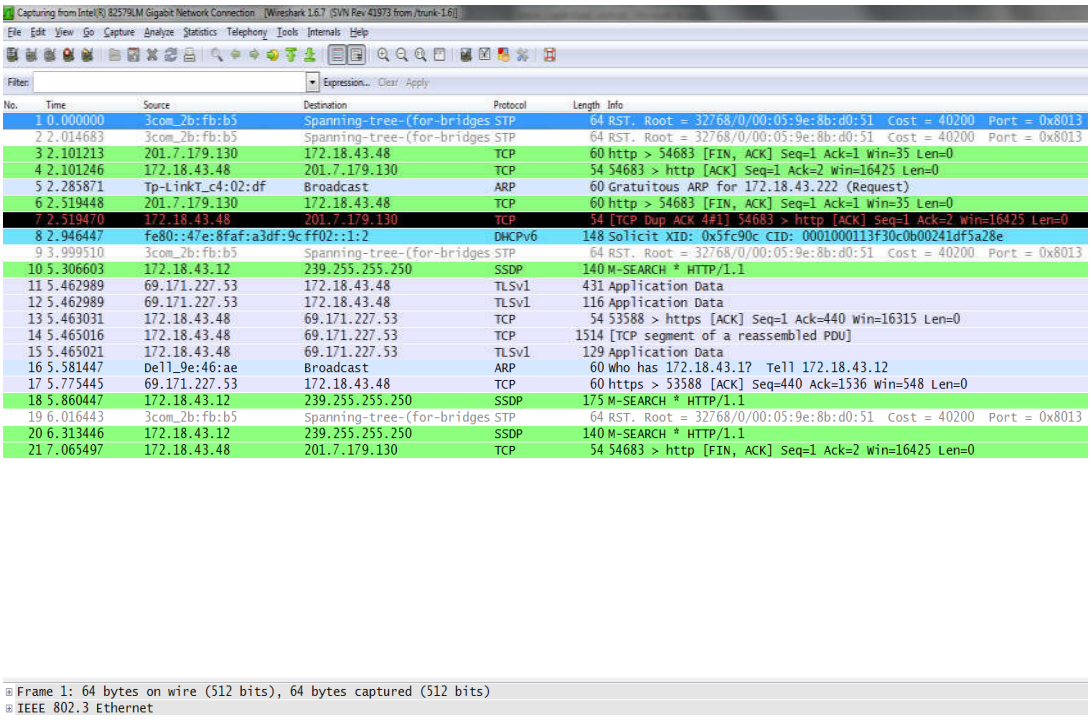


Figura 4.2 - Ambiente de captura de pacotes - Wireshark

Por isso, esta ferramenta possui uma grande vantagem em poder separar a captura por protocolo, o que facilita na análise pormenorizada de determinados processos e tecnologias implementadas ao longo da rede.

Por ser uma ferramenta que possui uma interface gráfica, o processo de filtragem se torna bem intuitivo e fácil de ser analisado. Além disso, esta ferramenta possibilita, de maneira bastante útil, o rastreamento de todas as etapas da comunicação de algum protocolo requisitante do determinado enlace.

O *Wireshark* possibilita uma captura em tempo real dos pacotes de uma grande rede ao depurar algum trecho ou simplesmente salvar todos os dados capturados, exportando ou importando arquivos em vários formatos.

Esta ferramenta foi escolhida por ser uma das mais utilizadas tanto em ambientes acadêmicos quanto corporativos para a captura e análise dos pacotes e protocolos implementados. Além disso, é possível capturar e analisar os pacotes localizados em diferentes segmentos de rede, facilitando a comprovação do uso de determinado protocolo e dos serviços fim-a-fim.

4.3 Cenários utilizados para simulação

Os cenários foram construídos com base nas topologias reais da empresa em estudo, de forma mais simplificada em relação à quantidade de sistemas autônomos e equipamentos de rede. Entretanto, esta possui semelhanças por toda a extensão da malha lógica da rede, não deixando assim, de explorar todas as tecnologias em produção.

4.3.1 Cenário 1: Nuvem MPLS

O primeiro cenário construído neste trabalho refere-se a uma topologia de roteadores que simula uma grande nuvem MPLS, localizada entre os sites de uma grande rede corporativa. O objetivo da elaboração deste primeiro cenário é a comprovação de utilização do protocolo RSVP-TE entre os roteadores sob a gerência dos provedores, capazes de realizar a criação de túneis virtuais nesses links, o que garante uma qualidade de serviço melhor e necessária.

O cenário é composto por quatro roteadores, como ilustrado na figura 4.3. A topologia retrata apenas uma área OSPF, ou seja, apenas um sistema autônomo de roteadores ou uma pequena célula que utiliza o mesmo protocolo para comunicação em uma determinada área.

Em conjunto com os protocolos de roteamento convencionais, usou-se a tecnologia do MPLS-TE antes da ativação do protocolo de reserva de recursos e o RSVP, necessário para geração dos túneis virtuais ao longo dos caminhos LSP's. Por final, foi feita a captura dos pacotes no momento do estabelecimento desses túneis através da ferramenta *Wireshark*, em que são demonstradas e comprovadas as trocas de mensagens que o protocolo RSVP-TE utiliza para tal procedimento.

4.3.2 Cenário 2: Rede Virtual Privada

O segundo cenário constituído refere-se a uma topologia de roteadores que simulam uma rede virtual privada, ou seja, a interligação de redes corporativas locais situadas em outras cidades e países.

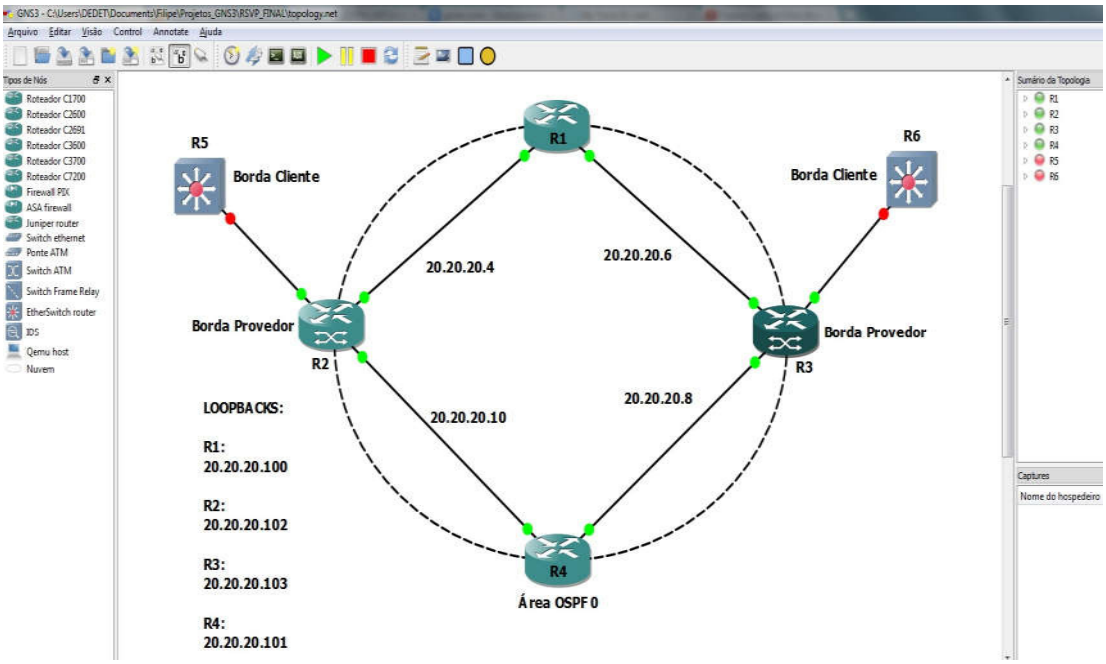


Figura 4.3 – Topologia do cenário 1

O objetivo deste cenário é fazer a comprovação de que, somente a partir de um endereço de destino, o pacote enviado de uma localidade, possa chegar à outra, de forma encriptado e sem ter conhecimento sobre o caminho por onde ele percorreu. Isto é possível, implementando as tabelas de roteamento virtuais nos roteadores localizados ao lado dos provedores. O cenário possui cinco roteadores, ilustrado na figura 4.4, onde são representados os provedores de serviços, a nuvem WAN e os clientes, representados pelas redes locais corporativas.

Os roteadores ditos provedores possuem uma configuração com o protocolo OSPF, pertencentes apenas a uma área de comunicação. Porém as interfaces dos roteadores, que se interligam aos roteadores de borda das redes locais de cada site, são excluídas dessa área, pois, a partir daí, não haverá mais processo de roteamento, distribuindo diretamente os pacotes com destino àquela rede. Por isso, foi implementado o protocolo EIGRP, proprietário da *Cisco Systems*, capaz de descobrir tanto as redes internas quanto as redes externas de uma determinada área. Além disso, o protocolo BGP, presente nas bordas dos provedores, foi implementado para executar o roteamento dinâmico entre os sistemas autônomos, sempre em forma de pares, no caso, os roteadores localizados na borda de cada *site* Vitória e São Luis.

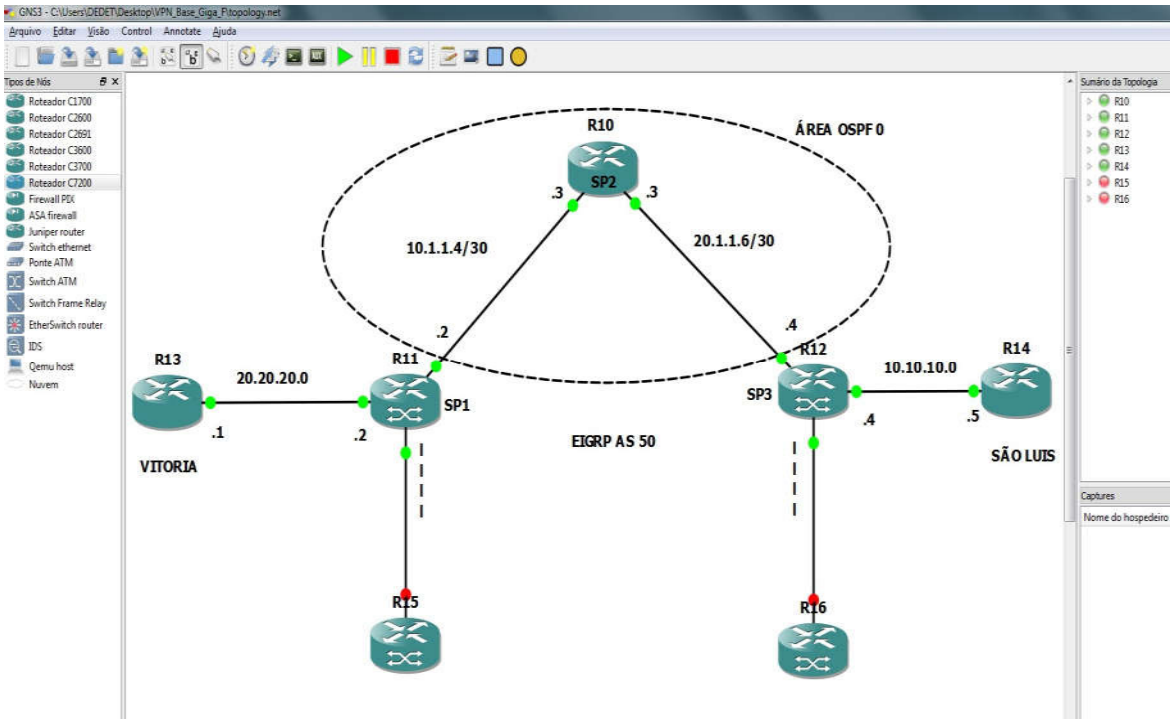


Figura 4.4 – Topologia do Cenário 2

Novamente em conjunto com os protocolos convencionais e as técnicas de encriptação, o MPLS-TE foi configurado para que os pacotes enviados de cada site fossem encapsulados na entrada e desencapsulados na saída do sistema autônomo. Por final, foi feita a verificação de comunicação entre os sites, emulando uma mesma rede separada por uma nuvem MPLS.

4.4 Configurações e Emulação

A configuração nos dois cenários foi realizada tendo como base os roteadores da *Cisco Systems* com o modelo da série C7200 e utilizada a IOS “c7200-jk9o3s-mz.124-19.bin” desse respectivo equipamento.

4.4.1 Configuração do cenário 1

A configuração básica dos roteadores, inicialmente, se dá com a atribuição de endereços IP’s das interfaces reais e de *loopback*. Após isso, foi configurado o

protocolo OSPF área 0 e, em seguida, foi ativado o *Cisco Expedited Forwarding* (CEF) de forma global em cada roteador, responsável por habilitar a ativação da tabela de roteamento entre os vizinhos. Por fim, foi ativado o LDP MPLS em cada interface do roteador. Os comandos utilizados para realização dessas configurações nos roteadores estão indicados no quadro 01, exemplificados para o roteador R3).

Quadro 01 – Configuração básica do roteador

```
Enable
configure terminal                          //Entra no modo global do roteador
ip cef
interface fastethernet 1/0                  //Entra na interface física 1/0
ip route-cache cef                          //Habilita o CEF na interface
ip address 20.20.20.10 255.255.255.0        //Atribui o endereço IP
no shut
interface fastethernet 1/1
ip route-cache cef
ip address 20.20.20.13 255.255.255.0
no shut
interface loopback 0
ip route-cache cef
ip address 20.20.20.103 255.255.255.0
no shut
router ospf 1                               //Habilita o protocolo OSPF
network 20.20.20.6 0.0.0.255    area 0      //Publica as redes vizinhas da área
network 20.20.20.8 0.0.0.255    area 0
network 20.20.20.103 0.0.0.255 area 0
end
config t
interface fastethernet 1/0
mpls ip                                     //Habilita o MPLS na interface
exit
interface fastethernet 1/1
mpls ip
end
write
```

Fonte: Próprio Autor

Nos restantes dos roteadores da Área 0, foram implementadas as mesmas configurações, diferindo apenas os endereços IP's. A partir desse momento, os roteadores já estão trocando rótulos entre si. A seguir será implementado e habilitado o protocolo RSVP entre os roteadores, necessário para serem criados os túneis virtuais. Os comandos utilizados para realização dessas configurações nos roteadores são mostrados no quadro 02, exemplificado para o roteador R3).

Quadro 02 – Habilitação do modo túnel e do protocolo RSVP-TE

```
enable
configure terminal
router ospf 1
mpls traffic-eng area 0                    //Habilita a troca do MPLS-TE na área 0
mpls traffic-eng router-id Lo0             //Atribui um identificador com a loopback
end
write
configure terminal
mpls traffic-eng tunnels
interface fastethernet 1/0
mpls traffic-eng tunnels                   //Habilita o modo túnel MPLS-TE
exit                                       na interface
interface fastethernet 1/1
mpls traffic-eng tunnels
end
configure terminal
interface fastethernet 1/0
ip rsvp bandwidth 512 512                  //Reserva uma quantidade de banda
interface fastethernet 1/1                 para a interface
ip rsvp bandwidth 512 512
end
write
```

Fonte: Próprio Autor

Após a configuração especificada no quadro 02, a mesma foi realizada em todos os outros roteadores, pois é necessária a ativação do RSVP em todos os vizinhos que irão formar o túnel.

A configuração do roteador R3, quadro 03, demonstra a criação dos túneis RSVP. É importante notar que há várias características diferentes ao se criar um túnel, como, por exemplo, túneis estáticos ou dinâmicos, largura de banda de cada túnel, prioridades etc.

Será apresentada a configuração de criação de três túneis estáticos e dois dinâmicos, diferenciando-se apenas pela prioridade de cada um. Os túneis estáticos possuem a seguinte orientação: R3_R1, R3_r1 e R3_R2. Os túneis dinâmicos iniciam-se no roteador R1 e têm como destino o roteador R3.

É importante notar que, entre dois ou mais roteadores CISCO, é possível se criar mais de um túnel RSVP-TE, tanto dinâmico quanto estático. A figura 4.5 ilustra essa ideia.

Quadro 03 – Criação dos túneis RSVP-TE t1 e t2

```
enable
configure terminal
interface tunnel 1
ip unnumbered loopback 0                   //Adiciona um endereço IP
tunnel destination 20.20.20.100            para a interface túnel
```

```
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 1 1                    //Habilita o valor da prioridade
tunnel mpls traffic-eng bandwidth 150                     do túnel
tunnel mpls traffic-eng path-option explicit name R3-R1   //Habilita o caminho pelo túnel
end
config t
interface tunnel 2
ip unnumbered loopback 0
tunnel destination 20.20.20.100                         //Habilita o IP do roteador de
tunnel mode mpls traffic-eng                              destino
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 4 4
tunnel mpls traffic-eng bandwidth 200
tunnel mpls traffic-eng path-option 1 explicit name R3_r1
end
config t
ip explicit-path name R3-R1 enable
next-address 20.20.20.9
ip explicit-path name R3_r1
next address 20.20.20.9
end
write
```

Fonte: Próprio Autor

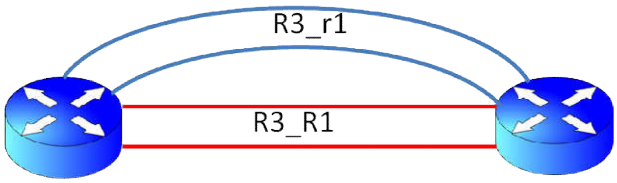


Figura 4.5 - Ilustração de túneis

Para a criação do túnel 5, é feita a configuração no roteador R3, passando pelo roteador R1 até chegar ao roteador de destino R2 (veja quadro 04).

Quadro 04 – Criação do túnel RSVP-TE t5

```
enable
config t
interface tunnel 5
ip unnumbered loopback 0
tunnel destination 20.20.20.102
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 2 2
tunnel mpls traffic-eng bandwidth 300
tunnel mpls traffic-eng path-option 1 explicit name R3_R2
end
write
config t
ip explicit-path name R3_R2 enable
next address 20.20.20.9
next address 20.20.20.5
end
```

Fonte: Próprio Autor

A seguir, foi feita uma configuração no roteador R1, quadro 05, para a criação de dois túneis de forma dinâmica.

Quadro 05 – Criação dos túneis RSVP-TE t3 e t4

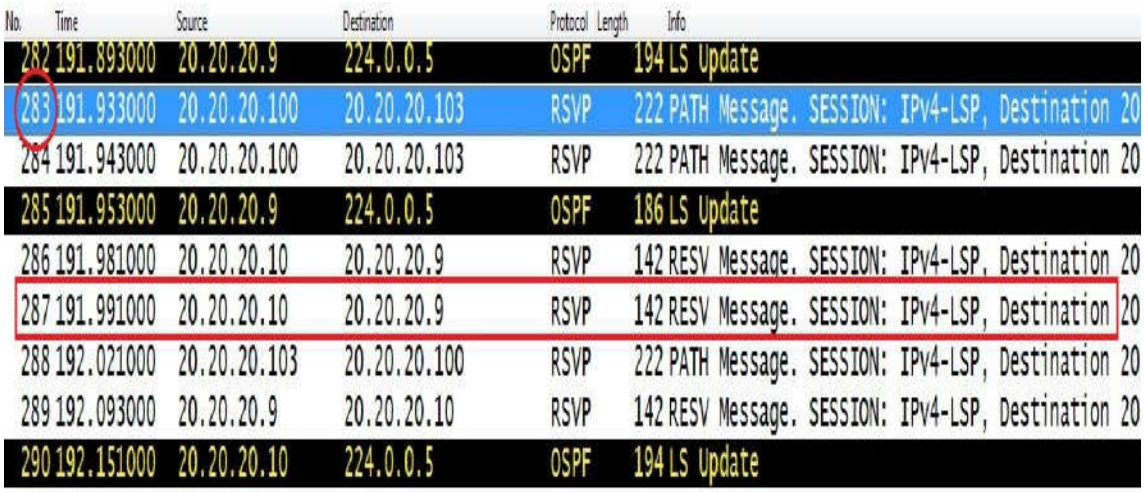
- enable
- config t
- interface tunnel 3
- ip unnumbered loopback 0
- no ip directed-broadcast
- tunnel destination 20.20.20.103
- tunnel mode mpls traffic-eng
- tunnel mpls traffic-eng autoroute announce
- tunnel mpls traffic-eng priority 5 5
- tunnel mpls traffic-eng bandwidth 100
- tunnel mpls traffic-eng path-option 2 dynamic
- end
- config t
- interface tunnel 4
- ip unnumbered loopback 0
- no ip directed-broadcast
- tunnel destination 20.20.20.103
- tunnel mode mpls traffic-eng
- tunnel mpls traffic-eng autoroute announce
- tunnel mpls traffic-eng priority 6 6
- tunnel mpls traffic-eng bandwidth 500
- tunnel mpls traffic-eng path-option 1 dynamic
- end
- write

Fonte: Próprio Autor

Durante a configuração dos túneis, foi realizada uma captura de pacotes com a ferramenta *Wireshark* e constatado o estabelecimento dos mesmos com a comunicação entre os roteadores habilitados com o protocolo RSVP. A figura 4.5 ilustra a captura de pacotes do roteador R1 interface 1/1, com algumas características dos pacotes.

A partir da observação da figura 4.6, pode-se constatar o estabelecimento do túnel feito a partir do encapsulamento das etiquetas MPLS pelo protocolo RSVP (ex. pacote 287). Da análise do pacote 283, é verificado que, dentro do campo RSVP e no objeto SESSION, é referido o protocolo IPv4-LSP. Isto se dá pelo fato do protocolo RSVP atender às necessidades do MPLS-TE.

Além da captura dos pacotes desse túnel, foi realizada a captura dos pacotes no momento do estabelecimento do túnel 5.



No.	Time	Source	Destination	Protocol	Length	Info
282	191.893000	20.20.20.9	224.0.0.5	OSPF	194	LS Update
283	191.933000	20.20.20.100	20.20.20.103	RSVP	222	PATH Message. SESSION: IPv4-LSP, Destination 20
284	191.943000	20.20.20.100	20.20.20.103	RSVP	222	PATH Message. SESSION: IPv4-LSP, Destination 20
285	191.953000	20.20.20.9	224.0.0.5	OSPF	186	LS Update
286	191.981000	20.20.20.10	20.20.20.9	RSVP	142	RESV Message. SESSION: IPv4-LSP, Destination 20
287	191.991000	20.20.20.10	20.20.20.9	RSVP	142	RESV Message. SESSION: IPv4-LSP, Destination 20
288	192.021000	20.20.20.103	20.20.20.100	RSVP	222	PATH Message. SESSION: IPv4-LSP, Destination 20
289	192.093000	20.20.20.9	20.20.20.10	RSVP	142	RESV Message. SESSION: IPv4-LSP, Destination 20
290	192.151000	20.20.20.10	224.0.0.5	OSPF	194	LS Update

Figura 4.6 – Captura de pacotes do roteador R1

A análise desses pacotes se torna interessante pelo fato do túnel ter a necessidade de atravessar mais um roteador para chegar ao seu destino final. O pré-requisito para que isto possa acontecer é a habilitação do RSVP em todos os roteadores do caminho LSP. A figura 4.7 constata que foi feita a comunicação de um roteador, localizado no meio do túnel (roteador R1), com seu destino final.

No.	Time	Source	Destination	Protocol	Length	Info
1325	1204.429000	20.20.20.103	20.20.20.102	RSVP	222	PATH Message. SESSION: IPv4-LSP, Destination 20.20.20.102, Tunnel ID 5,
1326	1205.639000	20.20.20.103	20.20.20.101	LDP	72	Keep Alive Message
1327	1205.679000	20.20.20.101	20.20.20.103	TCP	60	ldp > 52122 [ACK] Seq=415 Ack=433 Win=3930 Len=0
1328	1206.549000	20.20.20.5	224.0.0.2	LDP	76	Hello Message
1329	1208.129000	20.20.20.6	224.0.0.2	LDP	76	Hello Message
1330	1210.199000	ca:00:0b:98:00:1c	CDP/VTP/DTP/PAgP/UDLD	CDP	338	Device ID: R1 Port ID: FastEthernet1/0
1331	1211.110000	20.20.20.5	224.0.0.2	LDP	76	Hello Message
1332	1211.130000	20.20.20.5	224.0.0.5	OSPF	94	Hello Packet
1333	1213.010000	20.20.20.6	224.0.0.2	LDP	76	Hello Message

Figura 4.7 – Captura dos pacotes do roteador R3

A partir da figura 4.7, pode-se perceber que há uma tentativa do estabelecimento do túnel com o seu destino final (pacote 1325), através de um PATH Message. Pelo funcionamento do protocolo RSVP, ocorrerá o envio de um PATH Message do roteador R1 para o roteador R2. Se ocorrer uma comunicação entre eles, a resposta será um RESV Message em sentido contrário. Isto pode ser constatado a partir da figura 4.8.

1339	1215.680000	20.20.20.5	224.0.0.2	LDP	76 Hello Message
1340	1217.230000	20.20.20.6	224.0.0.2	LDP	76 Hello Message
1341	1219.240000	20.20.20.5	20.20.20.6	RSVP	142 RESV Message. SESSION: IPv4-LSP, Destination 20.20.20.102, Tunnel ID 5,
1342	1220.280000	20.20.20.5	224.0.0.2	LDP	76 Hello Message
1343	1221.130000	20.20.20.5	224.0.0.5	OSPF	94 Hello Packet
1344	1221.770000	20.20.20.6	224.0.0.2	LDP	76 Hello Message
1345	1223.440000	ca:00:0b:98:00:1c	ca:00:0b:98:00:1c	LOOP	60 Reply
1346	1223.560000	ca:01:0b:98:00:1c	ca:01:0b:98:00:1c	LOOP	60 Reply
1347	1224.030000	20.20.20.6	224.0.0.5	OSPF	94 Hello Packet
1348	1225.190000	20.20.20.5	224.0.0.2	LDP	76 Hello Message
1349	1225.720000	20.20.20.6	224.0.0.2	LDP	76 Hello Message
1350	1229.631000	20.20.20.103	20.20.20.102	RSVP	222 PATH Message. SESSION: IPv4-LSP, Destination 20.20.20.102, Tunnel ID 5,

Figura 4.8 – Captura de pacotes do roteador R3

Ao se analisar a figura 4.8 e o pacote 1341, pode-se constatar que houve o estabelecimento entre os roteadores R2 e R1, através do objeto RESV Message enviado.

Além de possibilitar a captura de pacotes, a ferramenta Wireshark é capaz de demonstrar como está estruturado o protocolo implementado em determinado pacote. De acordo com a figura 4.9, pode-se observar todas as características estruturais do objeto PATH Message, como prioridades, endereçamento, tempo utilizado, rota explícita etc., configuradas para o estabelecimento do túnel 5.

Outro recurso utilizado pela ferramenta Wireshark é a utilização de um gráfico gerado a partir dos pacotes capturados, chamado *Flow Graph*, onde é possível ver o tempo em que cada requisição foi feita e se essa foi aceita e estabelecida a comunicação. A figura 4.10 demonstra o gráfico mencionado, com a criação dos túneis 3 e 4 em relação ao tempo, em milissegundos gastos para o estabelecimento entre os roteadores.

4.4.2 Configuração do cenário 2

A principal configuração dos roteadores para se formar uma rede virtual privada, se faz nos roteadores chamados de *Service Provider*, pois como eles estão localizados na fronteira limite entre o *site* e o provedor, só haverá um único ponto de entrada e saída das informações da empresa, propiciando o encapsulamento e

```
⊞ Frame 1325: 222 bytes on wire (1776 bits), 222 bytes captured (1776 bits)
⊞ Ethernet II, Src: ca:00:0b:98:00:1c (ca:00:0b:98:00:1c), Dst: ca:01:0b:98:00:1c (ca:01:0b:98:00:1c)
⊞ Internet Protocol Version 4, Src: 20.20.20.103 (20.20.20.103), Dst: 20.20.20.102 (20.20.20.102)
⊟ Resource ReserVation Protocol (RSVP): PATH Message. SESSION: IPv4-LSP, Destination 20.20.20.102, Tunnel ID 5, Ext ID
  ⊞ RSVP Header. PATH Message.
  ⊟ SESSION: IPv4-LSP, Destination 20.20.20.102, Tunnel ID 5, Ext ID 14141467.
      Length: 16
      Object class: SESSION object (1)
      C-type: 7 - IPv4 LSP
      Destination address: 20.20.20.102 (20.20.20.102)
      Tunnel ID: 5
      Extended Tunnel ID: 336860263 (20.20.20.103)
  ⊞ HOP: IPv4, 20.20.20.6
  ⊞ TIME VALUES: 30000 ms
  ⊞ EXPLICIT ROUTE: IPv4 20.20.20.5, IPv4 20.20.20.102
  ⊞ LABEL REQUEST: Basic: L3PID: IP (0x0800)
  ⊞ SESSION ATTRIBUTE: SetupPrio 2, HoldPrio 2, SE Style,  [R3_t5]
  ⊞ SENDER TEMPLATE: IPv4-LSP, Tunnel Source: 20.20.20.103, LSP ID: 18.
  ⊞ SENDER TSPEC: IntServ, Token Bucket, 31250 bytes/sec.
  ⊞ ADSPEC
```

Figura 4.9 – Estrutura do pacote com o protocolo implementado

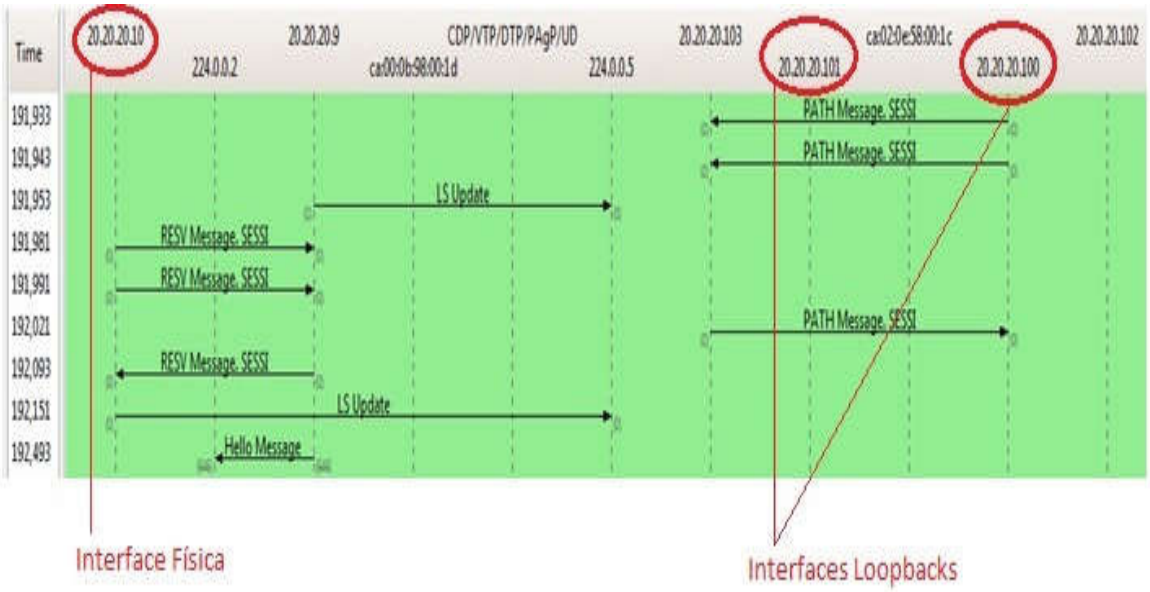


Figura 4.10 – *Flow graph* – Túneis 3 e 4

desencapsulamento dos pacotes pelo MPLS. No cenário criado, esses roteadores foram denominados respectivamente com as siglas SP1 e SP3. Na configuração a seguir do quadro 06, foi feita a criação da VPN CLIENTE com o identificador 100:1 e a seguir foi associada à interface por qual faz ligação direta com este roteador até o roteador de borda do lado da empresa. De forma semelhante, foi feita a mesma

configuração no roteador SP3, mudando-se o endereçamento pertencente à localidade distinta da empresa. (veja o quadro 06).

Quadro 06 - Configuração da criação de uma VPN

```
enable
config t
ip vrf CLIENTE
rd 100:1
route-target both 1:100
exit
interface fastethernet 1/0
ip vrf forwarding CLIENTE
ip address 20.20.20.2 255.255.255.0
exit
end
write
```

Fonte: Próprio Autor

Como o protocolo EIGRP foi implementado entre os *Services Providers* e os roteadores de borda da empresa, é necessário criar um subprocesso dentro deste protocolo para que sejam redistribuídas as rotas dessa VPN anunciadas pelo BGP. São essas rotas que os roteadores clientes receberão. A configuração deste processo e do protocolo BGP entre os roteadores SP1 e SP3 são mostradas a seguir, no quadro 07.

Quadro 07 – Configuração de redistribuição de rotas

```
enable
config t
router eigrp 5
address-family ipv4 vrf CLIENTE
autonomous-system 50
network 20.20.20.0
no auto-sumary
exit
router bgp 1
neighbor 4.4.4.4 remote-as 1
neighbor 4.4.4.4 update-source loopback 0
exit
router eigrp 5
address-family ipv4 vrf CLIENTE
redistribute bgp 1 metric 1500 4000 200 10 1500
end
write
```

Fonte: Próprio Autor

Após a configuração de toda a rede virtual privada foi possível constatar que é possível a comunicação entre duas localidades diferentes, separadas por longa

distância e interligadas por uma nuvem MPLS provedora que distribui os pacotes de forma encapsulada, sem que o cliente conheça o caminho percorrido por este. As figuras 4.11 e 4.12 ilustram os pacotes enviados tanto da localidade Vitória quanto da localidade São Luis, conseguiram a comunicação por meio de uma VPN.

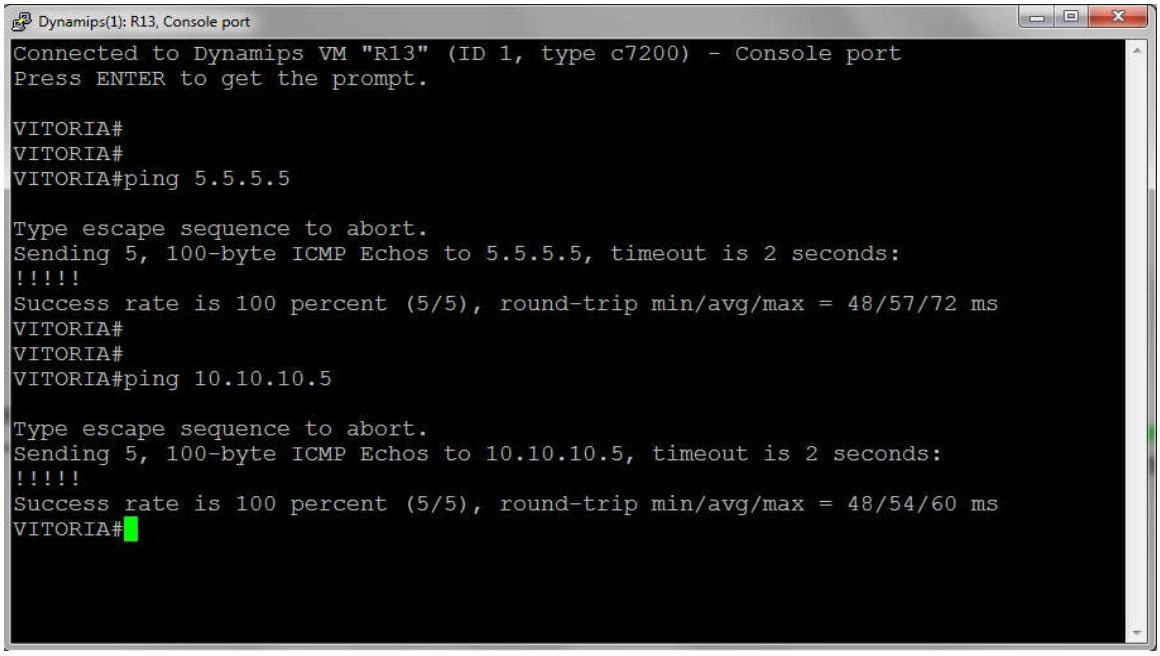


Figura 4.11 – Comunicação de Vitória para São Luis

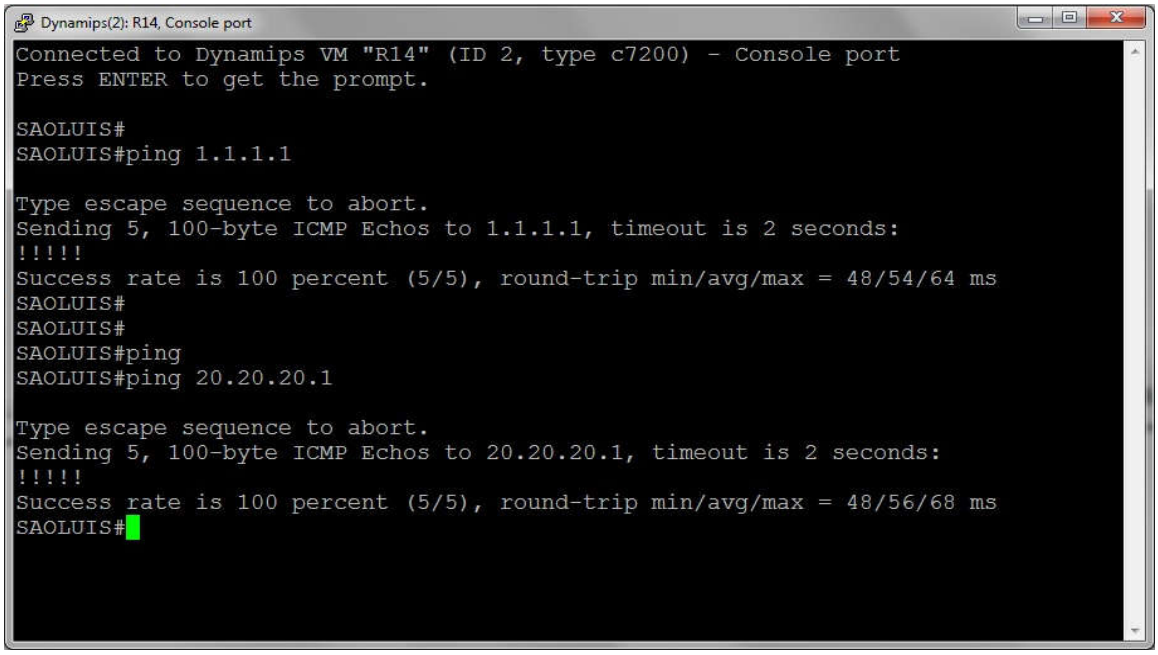


Figura 4.12 – Comunicação de São Luis para Vitória

Durante a ativação do comando “ping” no sentido Vitória - São Luis foi feita uma captura de pacotes na interface 1/1 do roteador SP1. Nela, foi constatado que os pacotes estão encapsulados pelo protocolo de distribuição de rótulos, ativado na entrada do roteador SP1 pela interface 1/0. A figura 4.13 ilustra os pacotes capturados, demonstrando o pacote de número 35 e seus atributos.

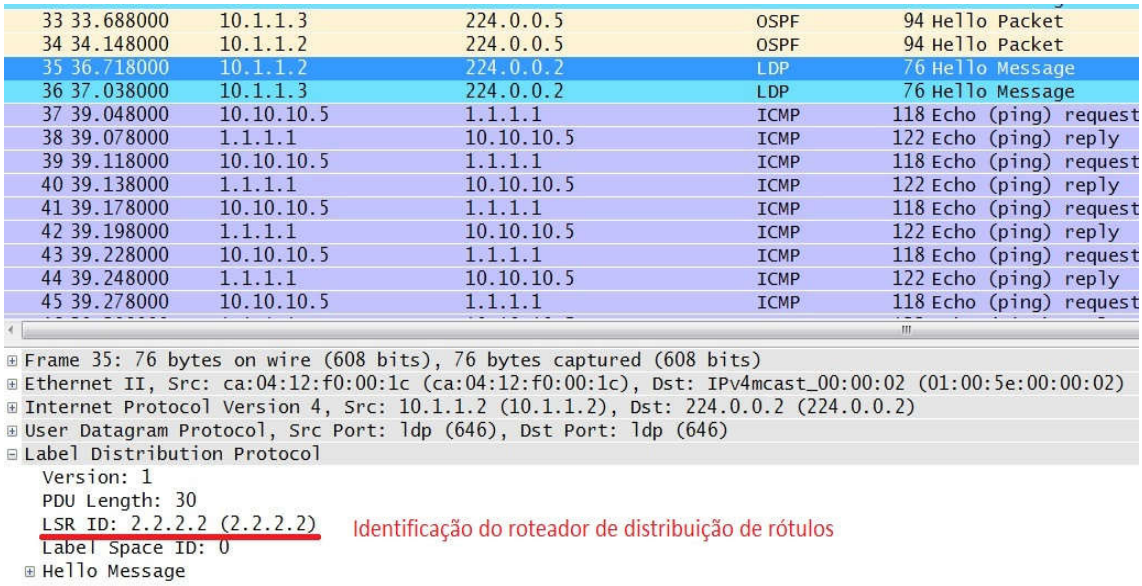


Figura 4.13 – Captura de rótulos do roteador SP1

4.5 Considerações sobre a ferramenta

A ferramenta GNS3 se demonstra bastante robusta quando se pretende copiar ambientes reais de produção. Além da possibilidade de se configurar os equipamentos utilizando todos os recursos oferecidos por eles, é possível que estas configurações fiquem gravadas nas memórias NVRAM’s, não sendo necessária a reconfiguração toda vez que o aplicativo for iniciado. A figura 4.14 ilustra o momento em que se inicia um roteador já configurado, reconhecendo todos os protocolos e vizinhos que fazem parte de alguma rota e os roteadores pertencentes a sua topologia.

Além disso, há a possibilidade de ligação de um equipamento externo ao computador hospedeiro da aplicação através de uma porta de comunicação, configurada nas opções da ferramenta para que este faça parte do ambiente lógico criado. Isso é de grande utilidade pelo fato de não ser necessário a aquisição de

todos os equipamentos pertencente à topologia antes de testá-los e colocá-los em produção.

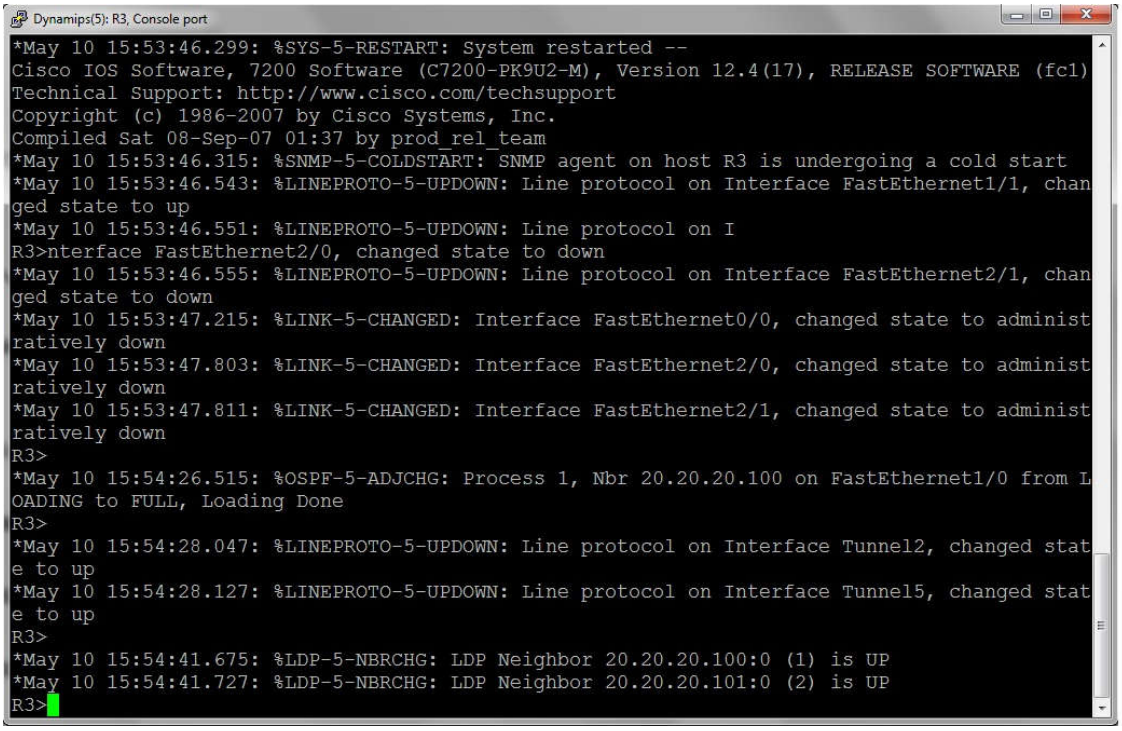


Figura 4.14 – Configurações gravadas e iniciadas

Apesar de vários pontos positivos, a ferramenta ainda se encontra em fase desenvolvimento na implementação melhorias sugeridas pela comunidade. Por isso, uma crítica a ser colocada, é o fato da aplicação não dispor de uma parte gráfica dinâmica, onde seria possível a visualização dos pacotes trocados entre os equipamentos em tempo real, dando maior agilidade na descoberta de possíveis erros.

5 CONCLUSÃO

Atualmente, diversas organizações estão necessitando cada vez mais não apenas de rapidez e disponibilidade de dados “off-line”, mas de serviços diferenciados “online” tais como: videoconferências, apresentações distribuídas, gerenciamento de máquinas remotamente, tecnologia de voz sobre a rede e etc. Por isso, há uma necessidade iminente de aprimoramento da infraestrutura de telecomunicações existente, ao invés da troca por completo da mesma.

Diante de tal necessidade, houve uma concentração nos estudos para a criação de certa tecnologia capaz de dar prioridade a certos serviços e torná-los diferenciados por sua criticidade. O protocolo MPLS foi desenvolvido dentro de uma arquitetura de serviços para conseguiu atingir de forma superior o modelo de melhor esforço no encaminhamento de pacotes pela rede.

A vantagem da criação do MPLS é que dessa arquitetura e de seus elementos, foi possível a criação de um novo protocolo chamado RSVP, no qual o seu esforço se concentra na otimização da distribuição de um desses elementos (rótulos) moldados por aquele protocolo. Além disso, é possível a formação de túneis virtuais com reserva de banda através de outro elemento MPLS, no caso o LSP, manipulando assim, toda uma infraestrutura de antigos paradigmas, sem que ela toda pudesse ser modificada.

Por isso, o protocolo MPLS e toda sua arquitetura se mostram como fundamental para a execução agregada de outro protocolo na implementação da engenharia de tráfego de dados, cujo objetivo é conseguir maior eficácia na transmissão de informações de uma rede corporativa.

Através da elaboração desta monografia foi possível constatar a utilização de pacotes RSVP-TE no momento da criação de túneis virtuais utilizados na engenharia de tráfego de dados, por um provedor de *link* para uma empresa corporativa, sendo capturados e analisados. Outra constatação foi a necessidade de usabilidade do MPLS na formação de redes virtuais privadas, onde houve a comutação de rótulos no núcleo da rede responsável pela ligação dos sites.

Por tudo isso, conclui-se que, com o uso cada vez maior de rótulos MPLS na distribuição de informações pelas provedoras de serviços de comunicação, o protocolo RSVP-TE atualmente se tornou pré-requisito para a implementação de engenharia de tráfego em redes corporativas, uma vez que a utilização dos recursos

de infraestrutura de forma otimizada, traz ganhos econômicos e tecnológicos significativos. Além disso, pode-se concluir que ferramentas de simulação como o GNS3, pode elevar significativamente a porcentagem de eficácia na implantação de uma rede e sua engenharia, pois seus testes se aproximam bastante do cenário real.

5.1 Trabalhos futuros

Como oportunidades para trabalhos futuros, sugere-se a implementação do protocolo de RSVP-TE agregando-se o protocolo IP, versão 6, uma vez que o de versão 4, encontra-se esgotado em sua numeração de distribuição. Além disso, os equipamentos da *Cisco Systems* já estão preparados para aceitar tais configurações daquele protocolo desde o ano de 1996. Outra sugestão seria o estudo de caso sobre o gerenciamento dos túneis virtuais estabelecidos com o protocolo, abrangendo tanto o enlace físico quanto políticas de re-roteamento e criação de túneis passivos. Como a ferramenta GNS3 ainda se encontra em desenvolvimento pela comunidade, sugere-se a elaboração gráfica dos pacotes que trafegam pela topologia lógica, a fim de maior visualização dos possíveis erros encontrados na rede em estudo.

REFERÊNCIAS

AMORIM, Leonardo Gomes; SILVA, Danilo José. **RSVP-TE.** Universidade Federal do Rio Grande do Norte, 2007.

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

DE QUEIROZ, Osmar Leonardo.; **VPN (REDE PRIVADA VIRTUAL): VPN/MPLS.** UNIFACS, 2000 Disponível em: <http:// pt.scribd.com/doc/56980705/Artigo-VPN-Mpls> Acesso em: 18 de maio. 2012.

EVANS, John, Filsfil, Clarence. **Developing IP and MPLS QoS for multiservice networks – Theory and Pratice**: Morgan Kaufman, 2007.

FILIPPETTI, Marco Aurélio. **CCNA 4.1:** Guia completo de estudo. Florianópolis: Visual Books, 2008.

_____. **Blog CCNA**. Disponível em: <http://www.ccna.com.br>.GNS3, Comunidade. Disponível em: <http: //http://www.gns3.net/>.

KUROSE, James F. ROSS, Keith W. **Redes de computadores e a Internet.** 3. ed. São Paulo: Pearson Addinson Wesley, 2006.

LOTITO, Alberto. **Engenharia de tráfego entre domínios de redes distintas.** 119f Dissertação (Mestrado em Engenharia Elétrica) – Pós-Graduação em Gestão de Redes de Telecomunicações. – PUC, Campinas 2007.

OSBORNE, Eric. **Engenharia de tráfego com MPLS.** CiscoPress: Editora Campus, 2003.

SOLIS BARRETO, Priscila. **Uma metodologia de Engenharia de Tráfego Baseada na Abordagem Auto-Similar para a Caracterização de Parâmetros e a Otimização de Redes Multimídias.** Tese (Doutorado em Engenharia Elétrica). – Departamento de Engenharia Elétrica, Universidade de Brasília, 164f, 2007.

TANENBAUM, A. S. **Redes de computadores**. 4 ed. Rio de Janeiro: Editora Campus, 2003.

TEIXEIRA, Mario Antonio Meireles. **Suporte a serviços diferenciados em servidores web: modelos e algoritmos.** São Carlos, SP: 2004. Tese (Doutorado em Ciências: Área Ciências da Computação e Matemática Computacional). Universidade de São Paulo. São Carlos, SP, 2004.

VEIGA, Miguel Ângelo. **Simulação de redes MPLS: Uma perspectiva pedagógica.** 2009 115f Dissertação (Mestrado em Engenharia Eletrônica e Telecomunicações) – Departamento de Eletrônica, Telecomunicações e Informática. – Universidade de Aveiro, Portugal 2009.