Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Sérgio Ricardo Polizer

Engenharia de tráfego em redes de computadores com MPLS: análise comparativa com OSPF.

São Paulo

2005

Sérgio Ricardo Polizer

Engenharia de tráfego em redes de computadores com MPLS: análise comparativa com OSPF.

Dissertação apresentada ao Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT, para obtenção de título de Mestre em Engenharia de Computação.

Área de concentração: Redes de Computadores.

Orientador: Dr. Cláudio Luiz Marte

São Paulo

Outubro de 2005

Ficha Catalográfica
Elaborada pelo Centro de Informação Tecnológica do
Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT

P769e **Polizer, Sérgio Ricardo**

Engenharia de tráfego de redes de computadores com MPLS: análise comparativa com OSPF. / Sérgio Ricardo Polizer. São Paulo, 2005.
91p.

Dissertação (Mestrado em Engenharia de Computação) - Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Área de concentração: Redes de Computadores.

Orientador: Prof. Dr. Cláudio Luiz Marte

1. Tráfego de redes (computadores) 2. Internet (redes de computadores) 3. Comunicação de dados 4. Multiprotocol Label Switching – MPLS 5. Open Shortest Path First - OSPF 6. Protocolo de roteamento 7. Tese I. Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Centro de Aperfeiçoamento Tecnológico II.Título

05/67 CDU 004.724(043)

Agradecimentos

À Deus pela proteção, força e benção durante toda minha vida.

À minha querida esposa Renata e filho Gustavo pelo apoio e compreensão pelos momentos que lhes furtei.

Aos meus pais pela estrutura que me proporcionaram, incentivo e exemplo de caráter.

Ao Dr. Cláudio Luiz Marte pela confiança e orientação e ao Dr. Antônio Luiz Rigo e Dra. Regina Melo Silveira pelas sugestões.

A todos integrantes da secretaria do Cenatec no IPT, especialmente ao Adilson pela colaboração.

Resumo

Esta dissertação aborda o problema de alocação de tráfego de pacotes com protocolo IP *(Internet Protocol)* em redes de comunicação de dados, voz e imagem.

As técnicas de encaminhamento alternativas ao modo baseado em rotas de menor métrica[1], resultado do processo de roteamento IP, são discutidas. Dentre essas técnicas, freqüentemente denominadas de engenharia de tráfego, estão a alteração das métricas dos protocolos de roteamento IP, utilização de circuitos virtuais e MPLS *(Multiprotocol Label Switching)*.

São apresentados os motivos que fazem da engenharia de tráfego com MPLS, uma técnica que proporciona o melhor controle de tráfego de pacotes com protocolo IP. Por isso, MPLS é abordado em profundidade nesta dissertação.

Além de uma abordagem teórica, esta dissertação apresenta uma implementação prática para demonstrar diferentes modelos de controle de tráfego em computadores funcionando com Linux. Eles foram conectados entre si para simular um grupo de roteadores em uma rede. Os softwares que possibilitaram OSPF *(Open Shortest Path First)* e *MPLS*, através do RSVP-TE (*Reservation Protocol for Traffic Engineering)*, permitiram que computadores trabalhassem como roteadores para avaliar engenharia de tráfego em cada modelo.

Palavras-chave: Computadores, Redes de comunicação de dados, Engenharia de tráfego, Protocolo de roteamento, MPLS.

[1] Custos das rotas em um roteador para atingir os destinos declarados em cada uma. Estes custos são calculados pelo protocolo de roteamento de acordo com seus critérios de avaliação. A banda total do link é um deles.

Abstract

Networking Traffic Engineering with MPLS: comparative study with OSPF.

This thesis focus the IP (Internet Protocol) traffic allocation problem in data, voice and image networks.

It was evaluated some forwarding methods, that are not similar than traditional basis, provided by IP routing protocols. Examples of these methods, used named as traffic engineering, are IP routing protocol metrics changing, virtual circuit switching and MPLS *(Multiprotocol Label Switching).*

It was observed that traffic engineering powered by MPLS is a technical that provide the best advantages for IP traffic control. Therefore, MPLS is studied with more criteria in this thesis.

Besides the theoretical discussion, this thesis shows a practical implementation to demonstrate the different traffic control models within computers running Linux. They were interconnected themselves to simulate a set of routes in a network. The OSPF *(Open Shortest Path First)* process and MPLS patches, like *Reservation Protocol for Traffic Engineering* (RSVP-TE), allowed the computers to work as routers for evaluation of the traffic engineering on each model.

Keywords: Computers, Networking, traffic engineering, routing protocols, MPLS.

Lista de Ilustrações

Lista de tabelas

Lista de Abreviaturas e Siglas

ADM	Add-Drop Multiplex
ATM	Asynchronous Transport Mode
BE	Burst exceed
CSPF	Constraint-Based Short Path First
VC	Virtual Circuit
DiffServ	Differentiated Services
DSCP	Diffserv Code Protocol
EXP	Experimental. Campo usado para marcação de QoS no pacote MPLS.
FEC	Forwarding Equivalent Class
IETF	Internet Engineering Task Force
IGP	Internal Gateway Protocol
IP	Internet Protocol
ISIS	Intermediate System to Intermediate System
ISIS-TE	Intermediate System to Intermediate System estendido para engenharia de tráfego.
LAN	Local Area Network
LDP	Label Distribution Protocol
LER	Label Edge Router
LSA	Link State Advertisement
LSP	Label Switch Path
LSR	Label Switch Router
MAN	Metropolitan Area Network
MPLS	Multiprotocol Label Switching
OSPF	Open Shortest Path First
OSPF-TE	Open Shortest Path First estendido para engenharia de tráfego

POS	Packet Over SDH/Sonet
PVC	Permanent Virtual Circuits
PWE3	Pseudo Wire Emulation Edge-to-Edge
QoS	Quality of Service
RFC	Request for Comments
RSVP	Reservation Protocol
RSVP-TE	Reservation Protocol estendido para engenharia de tráfego
SONET	Synchronous Optical Network
SDH	Synchronous Digital Hierarchical
SE	Shared Explicit
SLA	Service Level Agreement
SPF	Short Path First
TDM	Time Division Multiplex
TLV	Type Length Value
TOS	Type of Service
VPLS	Virtual Private LAN Services
VPN	Virtual Private Network
VRF	Virtual Routing Forwarding
WAN	Wide Area Network

Sumário

1 Introdução

Os roteadores encaminham pacotes de protocolo IP *(Internet Protocol)* em redes de comunicação de dados, voz e imagem, através da escolha de rota de menor custo para enviar o pacote IP em direção ao endereço de destino, indicado nele próprio. A escolha da rota é realizada entre todas as opções disponíveis em sua tabela de roteamento. A operação é repetida em cada roteador pelo qual o pacote passa, até que ele atinja o destino final.

Essa característica faz da operação de encaminhamento do protocolo IP, uma operação simples que, entre outras coisas, justifica seu sucesso, já que dispensa a presença de tabelas das rotas de todo o trajeto na origem e no destino do pacote. Por outro lado, faz com que muitos pacotes percorram juntos, seqüências de trechos idênticos da rede, formando grandes fluxos de tráfego.

Esse comportamento é observado com freqüência porque todos os pacotes são encaminhados em rotas de menor custo, rotas estas que tendem a ser as mesmas quando os destinos dos pacotes estão localizados num mesmo local, como servidores de aplicações e interfaces de conexão a outras redes, reunidos num mesmo prédio, ou quando originam e terminam em diferentes extremidades da rede, criando coincidências de trajeto no centro dela. Neste caso, o cenário é causado pelo provimento de túneis *VPN (Virtual Private Network)* ou quando a rede de um provedor de Internet funciona apenas como rede de trânsito a outro provedor, ou ainda, em trechos de redes de interligação entre grandes núcleos de tráfego, como capitais estaduais, por exemplo.

Com o aumento da quantidade de tráfego, foram observados comportamentos indesejáveis que precisavam ser amenizados. Por isso, a alteração das métricas dos protocolos de roteamento e a utilização de circuitos virtuais de tecnologias como *Frame-Relay* e ATM *(Asynchronous Transport Mode),* têm sido opções de alteração do sentido do tráfego. A técnica ficou conhecida como engenharia de tráfego e possibilita formas de encaminhar o tráfego em caminhos diferentes dos eleitos pelos protocolos de roteamento como os melhores para encaminhamento do tráfego, amenizando assim, os efeitos provocados pela característica de trajetos idênticos de grandes fluxos de tráfego de protocolo IP.

A engenharia de tráfego, em redes de comunicação de dados, sempre foi buscada com o objetivo de reduzir custos, utilizar melhor os recursos existentes sem, contudo, impor atraso às aplicações críticas existentes (Swallow, 1999). O alto custo dos ativos de rede e a grande competição por menores preços na prestação de serviços enfatizam sua aplicabilidade.

A realização de engenharia de tráfego tem sido feita através das tecnologias de camada de enlace *Frame-Relay*, ATM e por meio da manipulação de métricas de rotas em protocolos de roteamento como o *Open Shortest Path First - OSPF*. Este último, protocolo de roteamento interno de redes, é muito empregado em todo o mundo, pois sua capacidade de crescimento, rápida convergência e característica hierárquica baseada em áreas, fizeram dele um protocolo muito poderoso e implementado mundialmente.

Contudo, através do emprego de um conjunto de protocolos que formam o *Multiprotocol Label Switching – MPLS,* é possível realizar engenharia de tráfego de uma forma mais eficiente (Awduche *et al.* 1999), possibilitando inclusive, adicionar valores táticos e estratégicos a essas redes (Boyle *et al.*, 2002).

Esta dissertação aborda engenharia de tráfego e suas formas de obtenção, utilização, benefícios e limitações dentro de redes autônomas, ou seja, sob domínio e gestão de um grupo de pessoas, empresas ou organizações, ao contrário de redes como a Internet, por exemplo. Além disso, foca a engenharia de tráfego com MPLS em detalhes de funcionamento, protocolos e demonstrações de experiências em laboratório. A engenharia de tráfego conseguida com OSPF é comparada com a obtida com MPLS, teórica e experimentalmente.

Motivação

A arquitetura MPLS tem sido uma opção de implementação em redes de provedores de serviços de telecomunicações e Internet para possibilitarem o fornecimento de valor agregado aos serviços de conectividade e acesso a Internet que oferecem. O principal diferencial para o usuário final, está no fato de que parte de seu tráfego de informações terá qualidade de serviço nos nós comutadores durante seu trajeto e alta disponibilidade dos meios de transmissão de informações.

Entretanto, MPLS possibilita vantagens também para a própria provedora de serviços. Com a possibilidade de aplicar engenharia de tráfego, ter capacidade de continuidade nos negócios durante e após a transição de versão do protocolo IP e integração de diferentes redes em uma única, através da migração de redes de switches Frame-Relay e redes de roteadores interligados com linhas privadas ponto a ponto para uma única rede MPLS, as provedoras de serviços podem diminuir seus custos operacionais e aumentar a disponibilidade de recursos financeiros e humanos para se tornarem mais competitivas.

Quando a motivação de migração para MPLS é apenas a engenharia de tráfego, questiona-se sua real necessidade devido à existência de técnicas como através da alteração das métricas do protocolo de roteamento, utilização de circuito virtuais *Frame-Relay* ou ATM. A motivação desta dissertação está em colaborar com a clarificação desta questão destacando as vantagens e desvantagens de cada técnica e estudar melhor a arquitetura MPLS.

Outra motivação importante foi aplicar de forma prática o conteúdo teórico desta dissertação em uma rede de roteadores, representados por computadores com sistema operacional de código livre. Com isso, procurou-se incentivar o emprego de MPLS de forma didática em redes com computadores, tendo em vista que arquitetura MPLS é empregada apenas em roteadores comerciais de médio e grande porte, com sistemas proprietários e de alto custo de aquisição.

Objetivos

Os objetivos desta dissertação são:

- Dissertar sobre engenharia de tráfego com MPLS, utilizando-se de comparações com outras técnicas, em especial, com a técnica de alteração da métrica banda do OSPF.

- Demonstrar experimentalmente as características de controle de tráfego IP, utilizando engenharia de tráfego através da alteração das métricas do OSPF e através do MPLS.

- Gerar um procedimento prático e didático para apoio em aulas sobre MPLS.

A Metodologia utilizada foi baseada na constatação da melhor técnica de engenharia de tráfego, através de uma exploração teórica das características e demonstração prática do comportamento das principais delas.

Benefícios

Este trabalho pretende colaborar com o meio científico, na condição de prover uma dissertação sobre engenharia de tráfego em redes de comunicação. Ele está centrado na apresentação, abordagem e demonstração prática de técnicas de engenharia de tráfego com o objetivo de clarificar esse assunto a leitores interessados em melhor explorá-los ou aplicar nas redes sobre sua administração ou desenvolvimento, meios de maximizar a banda disponível, evitar congestionamentos e garantir cumprimento de acordos de nível de serviço.

Além disso, esta dissertação prove um procedimento prático e didático, com software livre, para apoio em aulas de redes de computadores sobre engenharia de tráfego.

A abordagem desse assunto é relevante pois o número de provedores de serviço de comunicação é grande, o que obriga cada um a aplicar técnicas de engenharia de tráfego que reduzam ou adiem custos de ampliação das redes, e por conseqüência, os custos dos serviços prestados, capacidade de recuperação rápida de falhas, controle granular sobre o tráfego e alternativa para descongestionamento de links[1] com objetivo de se tornarem mais competitivos em preço e serviços.

Outros Trabalhos Correlatos

A engenharia de tráfego tem sido objeto de estudo há algum tempo. Entre os trabalhos e pesquisas já publicados, estão:

a) *Achieving Near-Optimal Traffic Engineering Solutions for Current OSPF/IS-IS Networks* (Sridharan, 2003) Neste artigo publicado pelo IEEE, o autor propõe e

[1] Enlace de interligação de dois nós de rede.

avalia uma proposta de alteração no mecanismo de encaminhamento de pacotes de roteadores a fim de considerar não só a rota com menor custo mas um grupo de rotas para o mesmo destino. Conforme o autor, essa alteração é capaz de realizar otimização da distribuição do tráfego sem alterações nos protocolos de roteamento.

b) *Projeto Tequila* (Tequila, 2002). O objetivo desse projeto é estudar, especificar, implementar MPLS em computadores com Linux e validar uma série de serviços e ferramentas de engenharia de tráfego para obter garantia de qualidade de serviço através de um cuidadoso planejamento, dimensionamento e controle dinâmico das técnicas de gerenciamento de tráfego.

c) *Projeto MPLS-Linux* (Sourceforge, 2004). Trata-se de um grupo de desenvolvimento e implementação de MPLS em Linux. O grupo também trabalha para tornar os protocolos de sinalização associados a arquitetura MPLS também portáveis a Linux.

d) *Multipath based traffic engineering in MPLS Networks* (Hökelek, 2002). Essa dissertação de mestrado propõe uma arquitetura de engenharia de tráfego com MPLS que consiste em estabelecer dois *Label Swicth Path* (LSP) entre cada roteador de uma rede MPLS. A idéia consiste em dividir o tráfego crítico do tráfego comum entre esses LSP de acordo com os recursos de rede disponíveis em cada momento.

e) *The online and offline Properties of rounting algorithms in MPLS* (Wong, 2002). Trata-se de uma dissertação de mestrado onde o autor estudou como otimizar o estabelecimento de LSP. Para isso ele avaliou cinco algoritmos de roteamento teoricamente e experimentalmente através de processos computacionais.

f) *Internet Traffic Engineering* (Mortier, 2002). Essa tese de doutorado apresenta formas de realizar engenharia de tráfego entre diferentes provedores de serviço na Internet. Declara ainda que é possível resolver os problemas enfrentados e aumentar a eficiência das redes.

g) *Renewed Focus on Profitability Bodes well for deployment of MPLS in Traffic engineering* (RHK, 2002). Trata-se de recomendações de uma empresa analista de mercado, especialista na indústria de telecomunicações. Em termos gerais, apóia e recomenda a implementação de engenharia de tráfego com MPLS em core de redes de provedores de serviço.

h) *Traffic Engineering with Traditional IP Rounting Protocols* (Fortz, 2002). Nesse artigo publicado no pelo IEEE, os autores abordam engenharia de tráfego com utilização apenas de protocolos de roteamento, em especial, OSPF.

Esta dissertação se posiciona no contexto global de trabalhos já publicados, adicionando um estudo que reúne em uma única dissertação, mais de uma técnica de engenharia de tráfego que inclui comparações e demonstrações práticas e didáticas sobre o assunto.

Organização da Dissertação

Essa dissertação esta organizada da seguinte forma:

No capítulo 2, “Engenharia de tráfego”, além de ser definida, apresenta o que a difere da engenharia de rede, exemplificando e declarando os motivos e vantagens de realizá-la. Ainda neste capítulo, as formas de se obter engenharia de tráfego, com exceção do modo com MPLS, são apresentadas e adicionadas de características observadas em vivência prática de operação.

O capítulo 3, “MPLS”, apresenta o funcionamento da arquitetura MPLS, explicando os termos importantes para compreensão da engenharia de tráfego com tal arquitetura. Outras aplicações do MPLS como VPN e QoS, também são explicadas.

No capítulo 4, "Engenharia de tráfego com MPLS", inicialmente os benefícios, forma de funcionamento e protocolos participantes, como OSPF-TE e RSVP-TE, tem suas extensões para engenharia de tráfego explicadas a fim de verificar suas vantagens e interação entre si e com os nós participantes da rede MPLS. O capítulo termina com uma análise comparativa entre engenharia de tráfego com MPLS e sem a utilização de MPLS, abordado no capítulo 2.

A “Parte Prática” apresentada no capítulo 5, abordou as experiências de engenharia de tráfego implementadas em laboratório. Procurou-se iniciar com os componentes necessários para preparação da infra-estrutura, seguido das experiências realizadas. Os comentários explicativos e resultados são apresentados ao longo das experiências.

A dissertação termina com a conclusão no Capítulo 6, seguido da bibliografia e glossário.

Nos anexos, encontra-se o procedimento experimental didático para auxílio em aulas sobre MPLS, engenharia de tráfego ou OSPF, além dos procedimentos de instalação dos softwares utilizados na parte experimental.

2 Engenharia de Tráfego

Alterações nos elementos de rede ou no trajeto do tráfego de pacotes IP sempre foram realizadas a fim de evitar congestionamentos e utilização melhor dos recursos de redes de comunicação de dados, voz e imagem. Este capítulo inicia apresentando essas formas de alterações, denominadas engenharia de rede e de tráfego, seguido das formas de obtenção e termina com uma análise de engenharia de tráfego no protocolo IPv6.

A decisão de encaminhamento de um pacote IP é feita nó a nó. Quando um pacote chega a um roteador, este compara o endereço de destino no cabeçalho do pacote IP com a tabela de roteamento do *Internal Gateway Protocol* - IGP ou um conjunto de rotas manualmente configuradas, na inexistência de protocolo de roteamento para determinar qual nó vizinho apresentará o caminho de menor métrica para alcançar seu destino. Na ausência de rota correspondente àquele destino, o pacote é descartado. Quando o pacote chega ao próximo nó, toda esta operação é repetida até que o pacote chegue ao seu endereço destino.

Em virtude deste comportamento, à medida que há crescimento do tráfego de pacotes, alguns trechos de uma rede tendem a ficar super utilizados porque todo o tráfego sempre será encaminhado para o caminho de menor métrica para atingir seu destino. Ocorre ainda que, estes trechos são normalmente pouco diversificados em grandes redes. Por exemplo, um único local em uma rede WAN pode ser um destino muito procurado pelo tráfego, pois pode possuir inúmeros servidores de aplicações diferentes, *gateway* para a Internet, ou uma grande concentração de usuários da rede. Da mesma forma, um trecho de rede que interliga dois grandes centros urbanos também pode ser muito utilizado por apresentar uma boa métrica, acarretando uma concentração demasiada de tráfego neste local.

Por isso, haverá momentos em que serão necessárias aquisições de novos equipamentos e infra-estrutura de rede ou a realização de alterações no sentido do tráfego. Será necessária nova estrutura para que a rede atual continue a suportar o tráfego e principalmente, as aplicações com suas peculiaridades como tempo máximo de atraso, perda máxima de pacotes, entre outros.

2.1 Diferenças entre engenharia de rede e engenharia de tráfego

À medida que há crescimento e expansão de redes, ocorrem dois tipos de engenharia envolvidos: engenharia de redes e engenharia de tráfego (Osborne, Simha, 2002).

Na engenharia de redes, manipula-se os elementos e a infra-estrutura de rede, como links, roteadores e switches *LAN* e *WAN,* para se adaptarem ao tráfego. Os gestores da rede procuram fazer a melhor estimativa de crescimento do tráfego e iniciam o processo de aquisição dos elementos de rede necessários para atenderem

esse tráfego antecipadamente, pois o tempo para adquirir e instalar links e equipamentos pode ser longo.

Na engenharia de tráfego manipula-se o tráfego para ajustá-lo à rede. Em geral, é difícil estimar precisamente o crescimento de um tráfego IP. No final dos anos 90 o crescimento do tráfego nas redes de todo o mundo foi tão rápido que foi impossível atualizar as redes existentes na mesma velocidade. Exemplos de situações onde a previsão de crescimento do tráfego é difícil de ser feita, são: as coberturas de eventos de grande interesse popular por sites da Internet relacionados a esportes, escândalos políticos, atentados terroristas, promoções, etc. ou por falhas em roteadores ou quedas de links de trechos principais da rede.

Como freqüentemente são encontrados links em redes IP com baixa utilização, eles poderiam ser usados pela engenharia de tráfego. O trabalho nestes casos é manipular o tráfego de links congestionados para links sem utilização, da forma mais eficaz possível, para atender os objetivos operacionais desejados. Esta alternativa, portanto, aumenta a banda disponível pois utiliza melhor os recursos existentes.

Sob a perspectiva de crescimento, a decisão de encaminhamento de um pacote IP feita nó a nó é ótima, pois seria impraticável manter todas as rotas na origem e no destino do pacote. Mas sob a perspectiva de engenharia de tráfego, o encaminhamento do pacote IP baseado no endereço destino, é pouco otimizado. Formas de compensar este comportamento foram criadas e são apresentas a seguir.

2.2 Engenharia de tráfego com alteração das métricas dos protocolos de roteamento

Em um roteador, os protocolos de roteamento assumem valores, conhecido como custo ou peso, para cada interface habilitada para ser reconhecida pelo protocolo, baseado em critérios próprios de cada tipo, como tamanho da banda do link conectado a esta interface, como acontece no OSPF. Esses custos são associadas aos endereços de redes da interface a que pertencem e são distribuídos entre os roteadores vizinhos participantes. Cada roteador utiliza os endereços de rede e respectivo custo associado obtido dos outros roteadores, para calcular e decidir qual interface apresentará o trajeto de menor custo para que o pacote atinja seu destino final.

A engenharia de tráfego neste cenário é obtida alterando-se manualmente o custo de uma ou mais interfaces do roteador, para um valor diferente do assumido pelo protocolo, a fim de influenciar a escolha da interface eleita pelo protocolo de roteamento para o roteador encaminhar os pacotes.

Essa implementação tem sido feita com sucesso em protocolos como OSPFv2 e ISIS *(Intermediate System to Intermediate System*), descrita também em *Traffic Engineering with traditional IP routing protocols* (Fortz, B.,2002), porém apresenta as seguintes limitações:

a) Todo o tráfego caminha agregado nos roteadores, portanto não é possível uma definição do trajeto por tipo do tráfego (voz, Internet, vídeo, etc.) ou cliente;

b) A quantidade de tráfego enviado em caminhos diferentes para um mesmo destino é sempre uma razão 1/n, onde n é o número de caminhos, impossibilitando uma divisão proporcional à banda disponível em cada um deles. A Figura 1, O problema de alocação de tráfego com protocolo OSPF, exemplifica que, para custo de valor 15 em cada trecho, do ponto de vista de R2 para R6 ou vice-versa (através de R5), o custo é 1,5 vezes menor, do que através de R3R4. Entretanto, isso não significa que a quantidade de tráfego enviada por R2 e R6 no trecho R2R5R6 será 1,5 vezes maior que no trecho R2R3R4R6, na verdade, R2 e R6 escolherão a rota de menor custo.

Para utilizar todos os recursos disponíveis da rede do exemplo é necessário manipular a métrica das interfaces dos roteadores administrativamente para que os trechos apresentem custos idênticos, e o tráfego seja dividido entre os dois caminhos possíveis.

Contudo, isso pode levar a outros problemas. Caso um dos trechos no caminho R2R3R4R6, como por exemplo, R3R4, possua banda inferior ao do outros trechos do caminho em virtude da existência de um link de menor capacidade ou por apresentar alta utilização devido a um tráfego originado em R3 ou R4, haverá descartes de pacotes neste trecho. O evento irá impor atrasos nos pacotes das aplicações que se utilizarem deste caminho, ou seja, 50% de todo o tráfego, pois o tráfego foi balanceado igualmente entre R2R5R6 e R2R3R4R6.

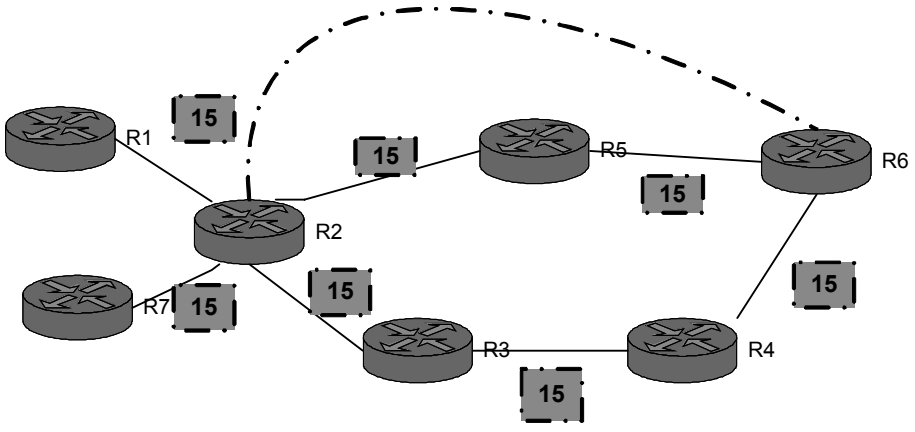


Figura 1. O problema de alocação de tráfego com protocolo OSPF
(Osborne, 2002)

c) A alteração administrativa das métricas das interfaces em grandes redes, quando o número de nós entre origem e destino for grande, pode gerar instabilidade ou efeitos imprevisíveis no processo de roteamento no caso quedas de links e/ou nós. Geralmente com a troca do custo de um link em um ponto da rede o trajeto do tráfego pode ser afetado em outros pontos da rede;

d) Outro problema causado por falha de link e/ou nós de rede é o relacionado ao tempo de interrupção de encaminhamento de pacotes. Em grandes redes de roteadores funcionando com IGP como OSPF, esse tempo pode variar de cinco até quinze segundos, até que o protocolo de roteamento perceba a queda de mais um dos caminhos, avise seus vizinhos e faça sua convergência para estabelecer o encaminhamento por outro caminho da rede.

e) Nenhum objetivo de desempenho é incorporado pelo processo de roteamento dos protocolos OSPF ou ISIS em resposta a alterações na topologia das redes, como falhas de elementos, ou em resposta a alterações no tráfego.

Com a RFC2740, *OSPF for IPv6*, (Coltum, 1999) conhecida também como OSPFv3, o protocolo passou a suportar o IPv6. Entretanto, seus mecanismos fundamentais como calculo da rota de menor custo, permaneceram inalterados.

2.3 Engenharia de tráfego com utilização de circuitos virtuais

O uso de circuitos virtuais ATM, soluciona algumas limitações causadas pela alteração das métricas dos protocolos de roteamento. A figura 2, por exemplo, ilustra como a mesma rede do exemplo anterior pode interligar R2 e R6 por dois *Permanent* V*irtual Circuits - PVC's*, estabelecidos pelos *switches* SW5 e SW3SW4. Os *switches* dão a impressão que R2 e R6 estão diretamente conectados do ponto de vista do protocolo de roteamento, pois não há elementos de camada de rede (Internation Organization for Standardization, 1987) entre eles. Isso permite divisão de carga entre os links, redundância, limitação da banda de cada *virtual circuit* (VC) e compartilhamento da rede do provedor de serviço com vários clientes através de vários VC.

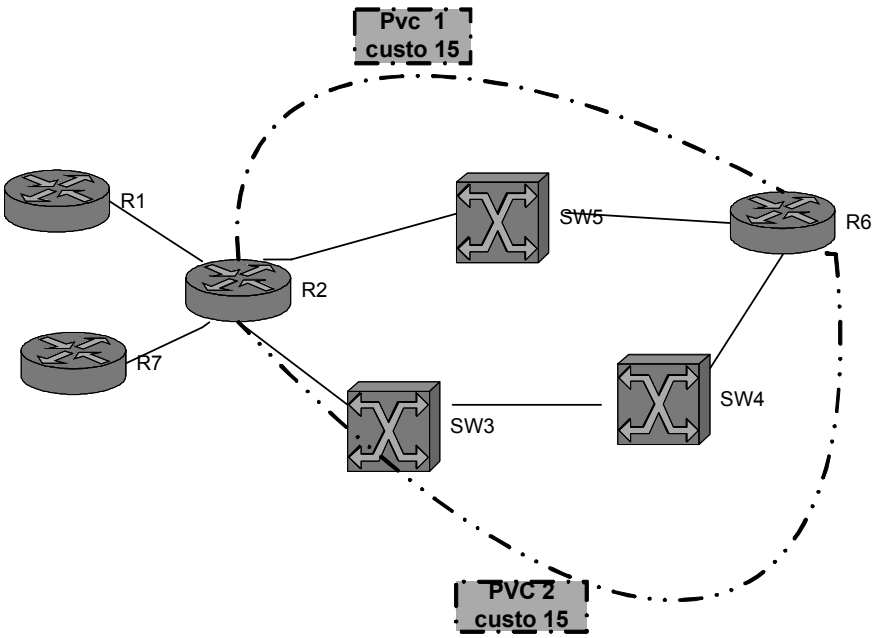


Figura 2. O problema de alocação de tráfego, resolvido com arquitetura ATM (Osborne, Simha, 2002)

Entretanto, apesar desse e outros benefícios descritos (Awduche, 1999), esse modelo também possui algumas limitações:

a) Em uma implementação de tecnologias de camada de enlace para realização de engenharia de tráfego, os roteadores IP são interligados por PVC através dos switches ATM ou Frame-Relay. Estes, por sua vez, são interligados entre si e aos roteadores por meio de links físicos, como do tipo E1/E3/STM-1, para transportarem os *Permanent Virtual Circuits*. Entretanto, protocolos de roteamento como do tipo *link state*, podem passar por uma grande convergência e congelar a rede por alguns segundos se uma falha em um link ou uma queda de um nó ocorrer, ocasionando queda de dezenas de VC. Isso significa gerar, em grandes redes, instabilidade no processo de roteamento após a oscilação de um link ou nó;

b) O roteador desconhece a topologia física neste tipo de solução. Ele visualiza o roteador vizinho como diretamente conectado a ele através do VC. Portanto, no caso de haver mais de um VC entre dois roteadores, e um deles passar a percorrer um trajeto muito mais longo dentro da nuvem de switches do que o outro, os pacotes que tomarem este caminho apresentarão maior atraso que os que tomarem o caminho do outro VC. Na prática, haverá uma aplicação que ora tem tempo de resposta rápida, ora tem resposta longa, pois todo o tráfego esta sendo balanceado entre os dois VC;

c) Essa solução se caracteriza por exigir mais equipamentos de rede, cabos para interligação, espaço em *racks*, energia e pessoas especializadas em diferentes arquiteturas de equipamento. Também é uma solução que apresenta dificuldade de identificação de problemas, maior número de peças de reposição devido a maior variedade de equipamentos. Por outro lado, essa solução foi muito adotada e continua sendo utilizada em empresas pois esta em processo de amortização.

d) Como os modelos de QoS das tecnologias de circuitos virtuais e do IP são diferentes, a combinação dos dois é difícil e configura uma limitação;

e) O período de restabelecimento de um circuito virtual em um link diferente do qual ele trafegava é alto em comparação com o que a engenharia de tráfego no MPLS implementa. *Fast-reroute* é uma característica de proteção do MPLS contra falhas de links que diminui a interrupção na comunicação entre dois pontos quando um link ou nó se torna inoperante, pois pode realizar a comutação alternativa em até 50 milésimos de segundo (Boyle *et al*., 2002), (Swallow, 2004), (Laurence, 2003).

f) Muitos nós comutadores de circuitos virtuais impossibilitam a definição de trajeto de VC, pois somente o estabelecimento entre a origem e o fim do VC é considerado no software. Por isso, para utilizar melhor links da rede, é necessária uma alteração manual nos VC durante o início da operação e depois de qualquer alteração no estado dos links da rede, o que gera uma intensa administração de operadores na rede;

g) Na utilização de circuitos virtuais, assim como na alternativa de alteração de métricas, todo o tráfego caminha agregado nos roteadores, portanto é não é possível uma separação por tipo e/ou cliente;

Ajustando-se as métricas de interfaces ou encaminhando o tráfego por circuitos virtuais a fim de influenciar a decisão de roteamento, é possível atuar somente no fluxo agregado, mudando seu trajeto de todo o tráfego ou realizando uma divisão de carga entre caminhos paralelos. Para otimizar o roteamento, utilizar melhor a banda disponível e evitar o congestionamento, há necessidade de controlar o tráfego em quantidade, tipo e seu trajeto dentro da rede.

2.4 Engenharia de tráfego com IPv6

A nova versão do protocolo de Internet, *Internet Protocol version 6 - IPv6* (Deering & Hinden, 1998), traz alterações no cabeçalho do protocolo IPv4 (Information Sciences Institute, 1981) em categorias relacionadas a extensão da capacidade de endereçamento, simplificação do cabeçalho do pacote, melhoria no suporte às extensões e opções, capacidade de marcação de fluxo de tráfego e autenticação. A Figura 3, Cabeçalho do protocolo IPv6 ilustra o formato do cabeçalho.

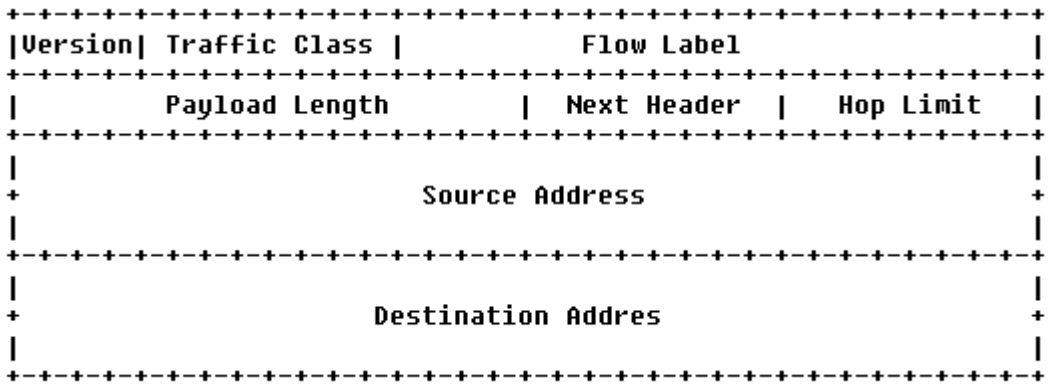


Figura 3. Cabeçalho do protocolo IPv6 (Deering & Hinden, 1998)

Dentre as alterações realizadas, uma poderá ter aplicações de engenharia de tráfego e implementar a característica de encaminhamento de tráfego de protocolo IP diferente do modelo de rota de menor custo. O campo *Flow Label* do cabeçalho do protocolo IPv6, que ainda passa por estudos de aplicação até a data de produção desta dissertação, poderia ser utilizado para identificar que o pacote precisa ser roteado de maneira diferente de todo o restante do tráfego. A existência de 20 bits neste campo garantiria capacidade de sinalização de diferentes tipos de roteamento. Porém, essa alteração é somente de uma sugestão particular feita pelo autor desta dissertação, podendo ser objeto de estudo futuro.

Outra opção para alteração da forma de roteamento de pacotes baseadas apenas no endereço destino, é a utilização dos campos possibilitados pelo *Next Header* do cabeçalho do protocolo IPv6. Neste campo são encontradas extensões como, *Hop-by-Hop Options Header, Destination Options Header* e *Routing Header.* Eles podem ser combinados de forma a permitir que um ou mais nós intermediários

sejam alcançados numa seqüência predefinida no trajeto do pacote até seu destino ou usados como túneis de outros pacotes IPv6.

Por outro lado, os protocolos de roteamento com suporte a IPv6, como o *OSPF for IPv6* (COLTUN, 1999), conhecido também como OSPFv3, continuam a utilizar os mesmos algoritmos para eleição de rotas de encaminhamento de pacotes que utilizavam nas versões de suporte a IPv4. Portanto, o comportamento anterior com o IPv4 permanecerá caso nenhum recurso seja adicionado.

Toda via, assim como ocorreu com o IPv4, o protocolo IPv6 possui campos ainda sem utilização que tendem a ser aprimorados a medida que o protocolo é empregado para melhorar seu funcionamento, como por exemplo, relacionado a engenharia de tráfego.

A utilização do MPLS e seu conjunto de protocolos estendidos, como recurso de tecnologia de comutação de pacotes possibilita ferramentas de engenharia de tráfego com IPv6, mas também é uma alternativa para o processo de transição de IPv4 para IPv6. Redes MPLS possibilitam domínios IPv6 isolados se comunicarem entre si sob uma rede com core IPv4 ou vice-versa. Essa implementação é possível pois o encaminhamento é baseado em label ao invés de cabeçalho do pacote IP.

3 MPLS

Para uma melhor compreensão da engenharia de tráfego com Multiprotocol Label Switching - MPLS, este capítulo procura apresentar uma introdução a essa arquitetura, fornecendo base para compreensão mais completa da dissertação. Um resumo das aplicações com MPLS encerra o capitulo.

O Multiprotocol Label Switching é uma arquitetura padronizada pelo *Internet Engineering Task Force - IETF* na RFC3031 (Rosen, 2001). Ele é empregado industrialmente e responsável pelo encaminhamento do tráfego de pacotes baseado em um rótulo (*label*) que é adicionado a cada pacote que entra em uma rede configurada nesta arquitetura. Os elementos dessa rede, roteadores e switches, encaminham os pacotes rotulados de acordo com as informações de roteamento, como no modo clássico, ou de uma forma manipulada, implementando então um novo modo de escolha de interface de saída para encaminhar um pacote IP.

O *label* é um conceito antigo. *Asynchronous Transport Mode - ATM*, *Frame-Relay* e X25 têm usado encapsulamento com *label* desde sua concepção. MPLS, entretanto, implementa o conceito genérico onde os *labels* são amarrados a nenhuma tecnologia de camada de enlace (Open Systems Interconnection, 1987).

A parte “MP” do MPLS significa que o protocolo pode transportar outros protocolos de camada de enlace, como *Ethernet* e *Frame-Relay*, e de rede, como IPv4 e IPv6. Em outras palavras, MPLS é um protocolo de encapsulamento. Já à parte “LS” indica que os protocolos que estão sendo transportados são rotulados diferentemente em cada nó de rede que ele atravessa.

3.1 Fundamentos do MPLS

Origem

O grupo de trabalho para desenvolver MPLS surgiu em dezembro de 1996, a partir da união de esforços e de listas de discussão de empresas que buscavam realização de switch com pacotes IP. Entre as propostas estavam (Gray, 2001):

- Tag Switching, da Cisco Systems
- ARIS (Aggregated Route-based IP Switching) da IBM
- Cell Switched Router, da Toshiba.

Inicialmente, o objetivo era tornar o roteamento de pacotes IP tão veloz quanto a comutação de pacotes realizada em camada de enlace, ou camada 2. Entretanto, com o aumento de esforços na pesquisa e definição de padrões para interoperabilidade surgiram outros benefícios que tornaram esta arquitetura vantajosa. Entre as padronizações estão a criação dos protocolos como LDP, CR-

LDP, RSVP-TE, MP-BGP e definição de termos como LSP, LSR e LER entre outros que serão abordados a seguir.

Label

O label é parte principal do MPLS. Ele permite a decomposição do processo de roteamento para um processo de encaminhamento. Ele trata-se de um pacote de 32 bits que é inserido antes do cabeçalho de um pacote de camada de rede como pode ser ilustrado pela Figura 4, O pacote MPLS e modelo de referência OSI. Esse label portanto, será usado pelos elementos de rede para determinar qual interface de saída e qual o novo label a ser substituído ou adicionado.

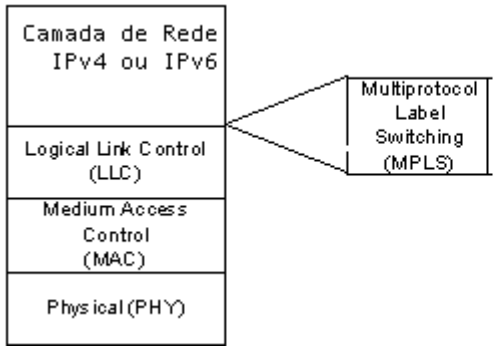


Figura 4. O pacote MPLS e modelo de referência OSI (Chowdhury, 2001)

Um pacote IP pode ter múltiplos labels, ou seja, um label inserido após o outro, processo conhecido como pilha de labels. Entretanto, em cada roteador da rede, apenas o label inserido por último é considerado, os label anteriores não tem referencias nas tabelas de encaminhamento destes roteadores até que os label superiores sejam retirados. A Figura 5, "Composição do pacote MPLS", ilustra o objeto em estudo.

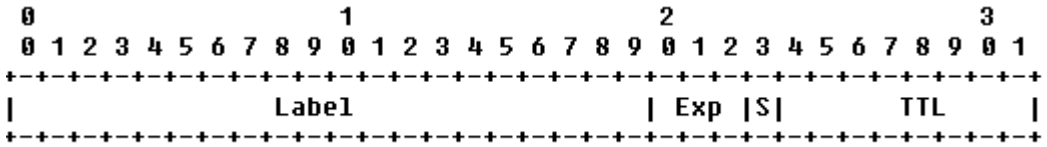


Figura 5. Composição do pacote MPLS (Rosen, 2001)

O label do pacote MPLS possui 20 bits. Portanto, ele pode assumir $2^{2°}$, ou 1.048.576 possíveis valores em uma única interface do roteador.

O campo Exp., denominado *Experimental*, com três bits, é utilizado como um indicador de Qualidade de Serviço. Ele freqüentemente baseia-se no campo IP *Precedence* ou *DiffServ Code Point* (DSCP) do pacote IP.

O campo S, chamado de *bottom-of-stack,* de um (1) bit, indica fim da pilha. Como há possibilidade de utilizar múltiplos labels, ele é usado para indicar se o próximo campo trata-se de um outro label ou se é o campo da camada de rede.

O campo TTL, denominado *Time To Live,* é uma cópia direta do campo IP TTL do cabeçalho IP. Ele é decrementado a cada roteador para evitar *lopping* da mesma forma que seu uso no pacote IP. Os valores em TTL também podem ser configurados para qualquer valor diferente do encontrado no pacote IP para impossibilitar a identificação dos endereços IP dos roteadores da rede MPLS através de comandos *traceroute* gerados de fora da rede.

Componentes

Um *Label Switch Router* (LSR), representado também pela letra "P" de *Provider*, é o nome dado aos roteadores que se encontram no centro de uma rede MPLS. Cada LSR tem função de comutar labels entre suas interfaces trocando, adicionando ou retirando labels.

Um outro tipo de roteador é um *Label Edge Router* (LER), representado também pelas letras "PE" de *Provider Edge*. Ele é localizado na extremidade da rede MPLS fazendo fronteira com o cliente. Cada LER é responsável por associar redes IP que contenham as mesmas características de roteamento, como mesmo prefixo de endereço de rede destino, requisitos[1] de roteamento, ou mesma interface de entrada no roteador a um único label. Além disso, um LER também é responsável por manter armazenadas as redes dos clientes conectados a ele, e transporta-las aos outros PE participantes.

O "CE" ou *Customer Edge*, é um outro elemento de uma rede MPLS. Ele é caracterizado como o roteador do cliente e desconhece configurações MPLS. Tem como função apenas encaminhar os pacotes para um PE com opção de marcação de classe de serviço. A figura 6, Elementos de uma rede MPLS, ilustra os componentes.

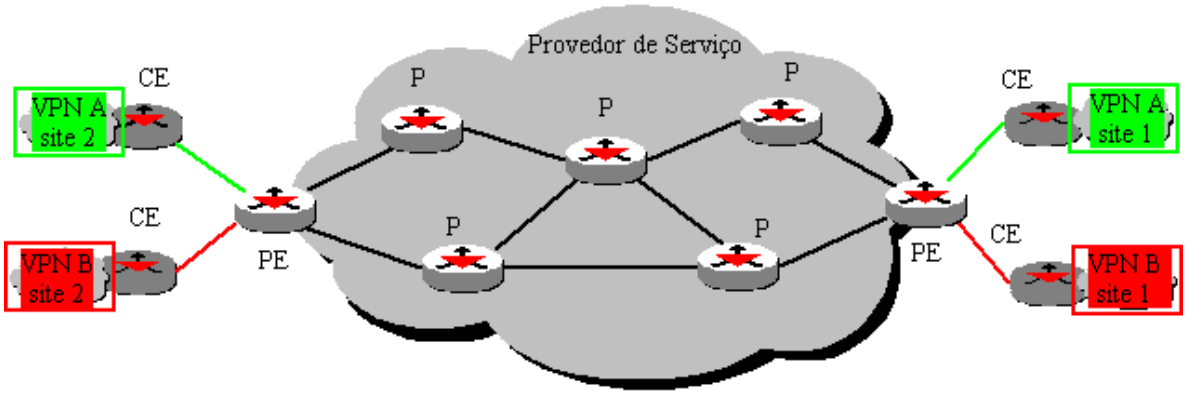


Figura 6. Elementos de uma rede MPLS

[1] Compreendem requisitos de roteamento: banda mínima, nós obrigatórios ou proibidos no trajeto e características de recuperação a falhas de rede,

FEC

Qualquer propriedade que associe grupo de pacotes de entrada num roteador a um mesmo label de saída são chamados de *Forwarding Equivalent Class* (FEC). Elas existem em todos os nós MPLS e genericamente, uma FEC é equivalente a várias rotas. Por exemplo, todos pacotes destinados para algum endereço IP dentro de 10.0.0.0/8 coincidem com uma mesma FEC. A característica principal esta no fato que uma FEC pode ser formada por pacotes com semelhanças de classe de serviço, interfaces de entrada no roteador, endereços IP de origem, tipos de protocolos e características de recuperação a falhas.

Essas associações são realizadas para os pacotes de cada FEC receberem um mesmo label, caracterizando um *Label Switch Path* que será discutido adiante, para então, receberem roteamento, reserva de banda ou recuperação a falhas diferentes de outras FEC.

LDP

O *Label Distribution Protocol* (LDP) padronizado na RFC3036 (Andersson, L.,2001) é um protocolo que tem como funções descobrir nós MPLS vizinhos, estabelecer e manter sessões entre os nós descobertos, trocar rotas dinâmicas e estáticas rotuladas com label e notificar erros. Ele requer absoluta confiabilidade na entrega de mensagens para evitar perda de eventos, por isso ele é transportado por protocolos como *Transmission Control Protocol* (TCP) e *Border Gateway Protocol (BGP).*

O LDP é conhecido como *downstream-unsolicited label distribution protocol* pois realiza distribuição de labels a todas as rotas presentes em cada roteador. Este protocolo é utilizado em aplicações como MPLS-VPN, que será abordado adiante neste capítulo.

Operações com Label

A operação dinâmica de uma rede MPLS consiste na imposição de labels aos pacotes que entram na rede, comutação baseada no label e retirada do mesmo .

O processo se inicia com o descobrimento das rotas IP e nós da rede por protocolos de roteamento como OSPF e IS-IS. A figura 7, Rede de roteadores com protocolo de roteamento IP, exemplifica esta etapa.

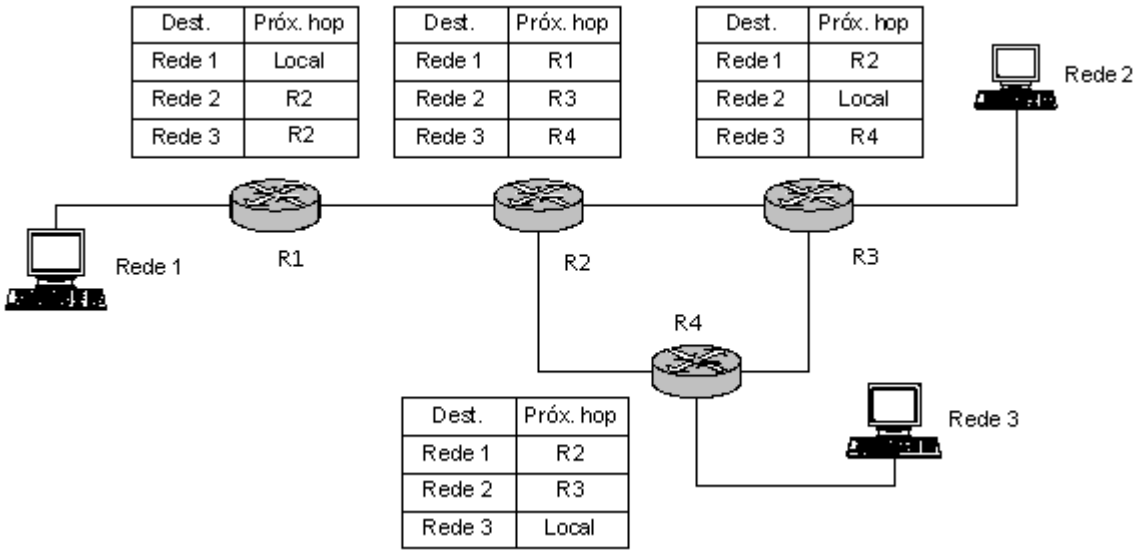


Figura 7. Rede de roteadores com protocolo de roteamento IP (Chowdhury, 2001)

Em seguida, o protocolo LDP em cada LSR ou LER, por exemplo, R1, aloca um label por FEC e distribui esta informação com os nós MPLS vizinhos, por exemplo, R2.

O roteador R2 por sua vez, consulta sua tabela de roteamento e determina a interface de saída, cria sua própria FEC, aloca um novo label e realiza uma associação do label e interface de entrada com um novo label e interface de saída determinado por ele. Além disso, refaz o mesmo processo feito por R1 com suas FEC, distribuindo-as aos nós vizinhos. A figura 8, Rede de roteadores com suas tabelas de roteamento associadas à labels MPLS, ilustra a explicação.

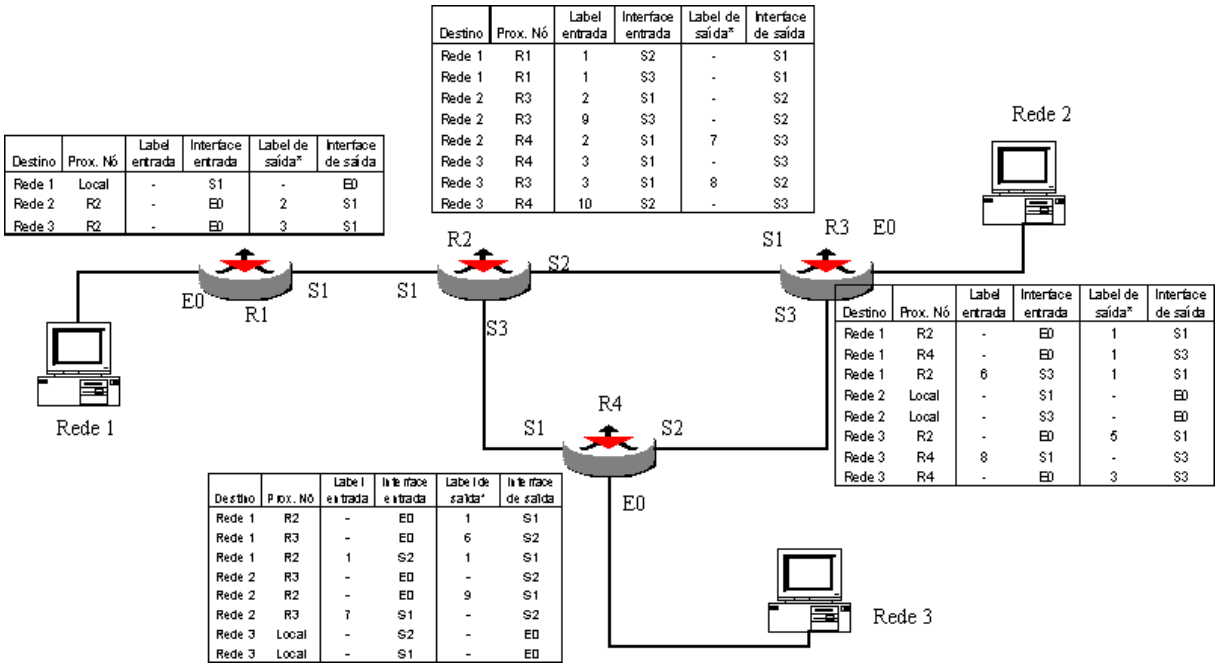


Figura 8. Rede de roteadores com suas tabelas de roteamento associadas a label MPLS (Adaptado. Chowdhury, 2001)

Terminado o processo de associação de labels a interfaces, assim que um pacote IP ingressar no R1, este realiza o processo de determinação de uma FEC, através da operação de roteamento e verificação de parâmetros de classe de serviço, tipo de protocolo, etc. para descobrir qual label inserir e que interface encaminhar este pacote, Figura 8. Em seguida, o encaminha ao R2, que apenas comutará o pacote entre as interfaces e trocará o label conforme associação de labels e interfaces realizadas anteriormente.

O processo continua com o pacote sendo comutado através do label até seu destino final. Assim que o penúltimo nó do trajeto na rede MPLS reconhecer que comutará o pacote ao último nó da rede, ou seja, um roteador PE, o label é retirado e o pacote é encaminhado na mesma forma que ingressou na rede MPLS para que o PE não tenha que retirar o label antes de realizar o roteamento tradicional para encaminha-lo a interface de saída.

LSP

O trajeto que um pacote rotulado com label percorre através da rede, tendo seu label imposto e substituído a cada roteador até sua retirada, é chamado de *Label Switch Path* (LSP).

Um LSP é unidirecional e seu trajeto pode ser definido pelo protocolo de roteamento em aplicações como VPN, ou determinado manualmente em aplicações como engenharia de tráfego.

O LSP determina o trajeto dos pacotes, portanto, ele precisa ser estabelecido antecipadamente.

3.2 Aplicações com MPLS

Engenharia de Tráfego

A engenharia de tráfego é proporcionada pelo protocolo RSVP-TE. Ele provê extensões ao RSVP para suportar estabelecimento de LSP ao longo da rede MPLS com possibilidade de determinar nós intermediários obrigatórios no trajeto. Além disso, reutiliza outra característica, a de reserva de banda para LSP.

Foram definidas na RFC3630 as seguintes funções do RSVP-TE: estabelecer túneis LSP, com opção de atendimento aos requisitos de roteamento, identificar e alterar dinamicamente seu trajeto, distinguir, mantê-los e diagnosticá-los. Além de aplicar políticas de prioridade e, principalmente, apresentar capacidade de realizar alocação de *labels* por demanda.

O RSVP-TE é utilizado para permitir controle do tráfego IP sobre uma rede sem influência das rotas determinadas pelos protocolos de roteamento. Este controle proporciona utilização de links de rede que apresentarem maior custo que outras alternativas, encaminhamento de tráfego prioritário por caminhos de rede descongestionados, reserva de banda por classe de serviço de LSP e redundância.

Outras características e funcionamento são abordados no Capítulo 4, Engenharia de Tráfego com MPLS.

MPLS-VPN

As *Virtual Private Networks* (VPN) são proporcionadas por tecnologias de interligação de redes desde os anos 90, através de linhas dedicadas, circuitos virtuais do Frame-Relay ou do ATM, com o objetivo de conectar escritórios de corporações. Os túneis IPSec também são usados para possibilitar acesso a *Intranet* sobre uma rede pública ou compartilhada.

As VPNs em redes MPLS podem ser proporcionadas através de camada de enlace, conhecidas como *Layer 2 Transport* ou *Layer 2 Encapsulation* e as VPNs de camada 3, conhecidas como Layer 3 VPNs.

As Layer 2 VPN, descritas na RFC3985 (Bryant, S.,2005) como *Pseudo Wire Emulation Edge-to-Edge* (PWE3), abrangem a emulação de serviços Frame-Relay, ATM, Ethernet, TDM e SONET/SDH com comutação de pacotes usando redes MPLS. Este benefício tem sido considerado pelos provedores de serviço para convergirem os serviços de outras redes para uma única rede MPLS, a fim de reduzirem custos operacionais. A figura 9, reproduz a opinião de 200 provedores de serviço questionados em 2004, sobre a importância em migrar serviços Frame-Relay para redes MPLS (HEAVY READING, 2004), por exemplo.

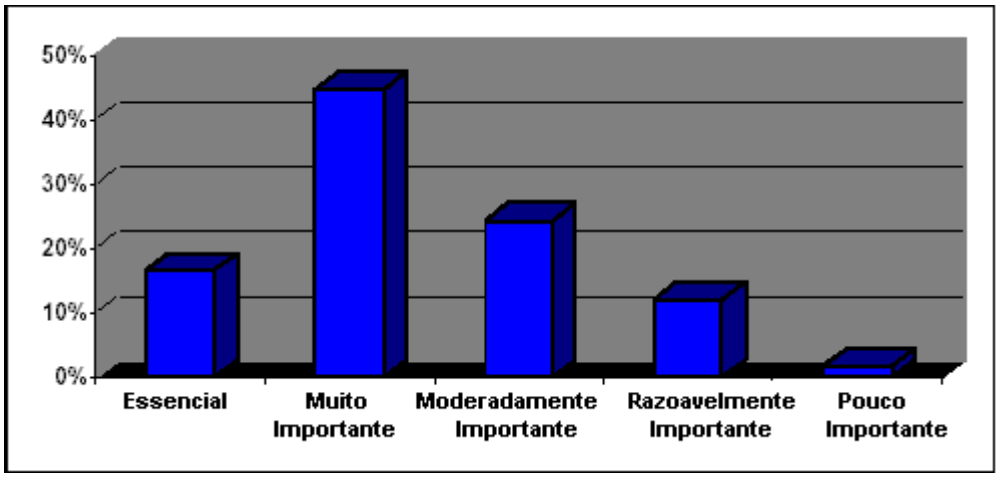


Figura 9. Opinião dos provedores de serviço em migrarem serviços legados para redes MPLS (Heavy Reading Report, 2004)

As Layer 3 VPN, proporcionadas por MPLS apresentam uma série de vantagens as VPN tradicionais, como podem ser citadas a seguir:

- Seguem o mesmo motivo de sucesso da Internet com o protocolo IP, ou seja, não são orientadas a conexão. Com essa característica elas eliminam complexidade e possibilitam escalabilidade.

- Apesar de funcionar em uma rede compartilhada entre várias VPN, há possibilidade de fornecimento de serviços privados a um grupo de usuários representados por uma VPN como *multicasting,* para aplicações como videoconferência, qualidade de serviço, telefonia IP, acesso a DataCenter remoto.

- A segurança proporcionada pelas VPN tradicionais como Frame-Relay, tem o mesmo nível que as proporcionadas por MPLS-VPN.

- MPLS-VPNs permitem que clientes desta rede, continuem a usar seu endereçamento sem tradução com *Network Address Translation* (NAT) e definir sua própria regras de conexão de sites, acesso a Internet, Intranet e Extranet.

Com VPN Layer 3, cada roteador de extremidade da rede MPLS (PE) age como um agregado de roteadores virtuais. O provedor de serviço configura cada membro de uma VPN de acordo com a interface de conexão ao CE como pode ser observado na Figura 10, Componentes de uma rede MPLS-VPN. Como resultado, apenas os pacotes provenientes desta interface pertencem a VPN especificada e nenhum outro consegue acessá-la. A interface entre um PE e um CE é realizada através de roteamento tradicional IP, por isso há rotas estáticas ou protocolos de roteamento como RIP, OSPF ou BGP em ambos os lados.

O provedor da rede MPLS estabelece conectividade entre os PE que necessitaram se comunicar, para proporcionar uma VPN. Os PE adicionam cada endereço externo IP que foi aprendido, em uma *Virtual Routing Forwarding* (VRF), e os transmitem para todos os outros PE envolvidos na VPN usando uma forma estendida do BGP capaz de transportar labels (MP-BGP). Além disso, criam uma FEC e adicionam um outro label capaz de identificar a VRF remota.

Desta forma, um pacote com dois label é encaminhado para um LSR ou P, o primeiro e mais externo label será usado para comutação, assim como apresentado anteriormente no item LDP, e o segundo será utilizado apenas no PE destino que identificará através deste label qual VRF ele pertence e em seguida qual interface de saída. A figura 9, apresenta um diagrama dos componentes de uma rede MPLS-VPN.

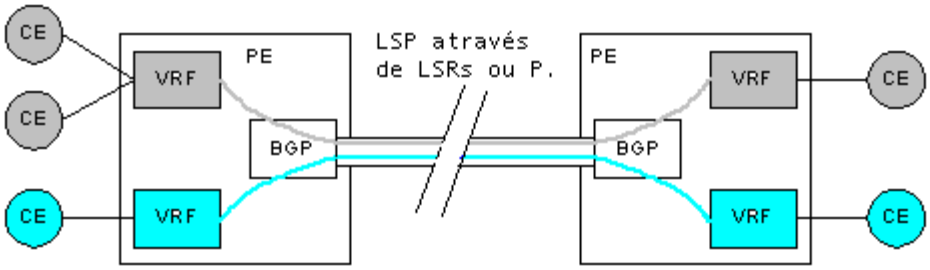


Figura 10. Componentes de uma rede MPLS-VPN

QoS

A qualidade de serviço (QoS) esta associada a performance da rede, ou seja, controle de perda de pacote, jitter e latência. Em MPLS o QoS é inicialmente possibilitado através do campo Exp presente no label. Ele é mapeado conforme campo do pacote IP, responsável por indicar classes de serviço, o DSCP, definido na RFC3168 (Ramakrishnan, 2001).

Os pacotes IP que chegam a um roteador PE com o DSCP configurado, recebem um label com o campo Exp também configurado, e são encaminhados em LSP até atingirem algum roteador P, onde são agrupados em filas também conhecidas como *buffers*, de acordo com a classe de serviço identificada no campo Exp. A figura 10 ilustra os pacotes rotulados com classe de serviço diferentes em um mesmo LSP.

Os nós LSR propiciam a qualidade de serviço encaminhando preferencialmente para o próximo destino, os pacotes das filas mais priorizadas ou reservando banda nos links e nos buffers específicos para classes de serviço priorizado (Fineberg, 2003).

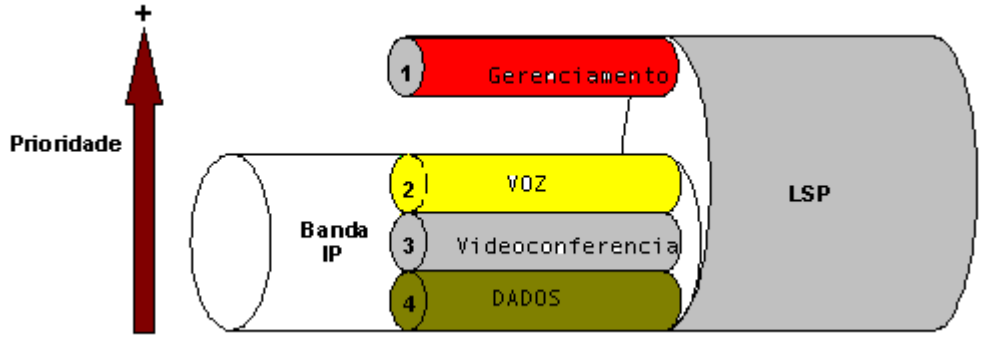


Figura 11. Exemplo de um LSP com pacotes classificados com classe de serviço

A engenharia de tráfego com MPLS colabora com uma política de QoS porque, como o tráfego é carregado em LSP, há reserva de banda. Além disso, quando o tráfego é separado por tipo ou grupo de tipos de aplicação e em seguida encaminhado em LSP relativo a cada grupo, a engenharia de tráfego com MPLS pode forçar o LSP que carregar as aplicações mais críticas, a percorrer um trajeto dentro da rede de menor distância ou livre de congestionamentos.

Essas características, assim como *fast-reroute* do RSVP-TE, são ferramentas do MPLS, para garantir atendimento dos acordos de nível de serviço, *Service Level Agreetment* (SLA).

3.3 Considerações Parciais

O MPLS tem obtido destaque nos últimos anos. Esta arquitetura tem sido empregada com sucesso em um grande número de redes e tem sido usada para oferecer Internet e serviços de *Virtual Private Networks* (VPN) em redes de todo o mundo. Um estudo sobre planos dos provedores de serviço para redes IP, MPLS e ATM realizado em 2003, através de entrevistas com executivos de 21 provedores de serviço nos Estados Unidos, Europa e leste da Ásia mostrou que, 62% dos provedores de serviço estavam engajados de alguma forma com redes de dados convergentes[1] sobre IP ou IP/MPLS em 2003, e 86% estariam em 2004 (Michell, 2003).

Outra pesquisa, com funcionários de 200 provedores de serviço sobre atitudes relacionadas a IP/MPLS em 2004, indicavam que dos provedores que responderam esta questão, 18% pretendiam oferecer em 2004 os serviços pesquisados sobre a sua rede MPLS e aproximadamente 82% o fariam em 2005 (Heavy Reading, 2004). A mesma pesquisa, identificou que mais de 30% dos provedores de serviços *Frame-Relay*, esperam em 2005, 25% de lucratividade vinda dos serviços *Frame-Relay* convergidos em sua rede MPLS através de MPLS-VPN (Heavy Reading, 2004).

No Brasil, até agosto de 2005, seis operadoras de telefonia fixa já ofertavam serviços de VPN com qualidade de serviço através de redes MPLS. Já com relação as operadoras de telefonia celular, apenas uma já utilizava rede MPLS para trafegar dados de Internet dos celulares de seus clientes.

A motivação para implementar MPLS nas redes atualmente tem sido as aplicações que ele possibilita, pois elas seriam difíceis ou quase impossíveis de serem implementadas ou operadas em redes IP tradicionais. Neste trabalho foram abordadas suas aplicações com engenharia de tráfego, por isso o próximo capítulo abordará um pouco melhor este tema.

[1] Consideram-se redes convergentes, redes de diferentes tecnologias como, por exemplo, *Frame-Relay* , ATM ou IP (fornada somente por roteadores interligados através de links), convertidas para uma única rede.

4 Engenharia de tráfego com MPLS

Neste capítulo, além das características e benefícios da engenharia de tráfego com MPLS, serão apresentados a estrutura de funcionamento, definição de termos importantes e seus componentes. São eles: o componente responsável pelo levantamento da topologia da rede e estado de utilização de seus recursos, Open Shortest Path First estendido para engenharia de tráfego (OSPF-TE) e o componente responsável pelo estabelecimento, manutenção e remoção de túneis, Reservation Protocol estendido para engenharia de tráfego (RSVP-TE). O capítulo termina com uma análise comparativa com a técnica de engenharia de tráfego através da alteração das métricas do OSPF.

A engenharia de tráfego é essencial para provedores de serviço ou corporações que possuem uma larga rede de comunicações porque otimiza os elementos de rede empregados, atende os requisitos de qualidade de serviço das aplicações dos clientes e as protege de falhas de links e nós. Foi a primeira aplicação do MPLS em redes IP, passando a interagir posteriormente com outras aplicações, como MPLS-VPN, por exemplo.

A engenharia de tráfego com MPLS é possível graças ao modo de encaminhamento de tráfego baseado em label, aos protocolos de sinalização de LSP e aos responsáveis pela obtenção, atualização e distribuição das redes e da banda disponível nos links aos nós da rede. Por isso, os pacotes de diferentes clientes, protocolos, aplicações, endereçamentos iguais, classes de serviço e segurança podem ser transportados dentro de uma mesma rede, com tratamento diferenciado a cada fluxo, como mudança de trajeto e reserva de banda, se necessário.

4.1 Funcionamento e Benefícios

Para que o trajeto possa ser determinado, atendendo assim uma das características da engenharia de tráfego, os protocolos RSVP (Braden *et al.*, 1997) e LDP (Andersson, 2001) tiveram suas padronizações estendidas, formando *Reservation Protocol* (Awduche, 2001) e *Constraint-Based Label Distribution Protocol* (Jamoussi, 2002), para serem opções de estabelecimento, remoção e manutenção de túneis ao longo da rede MPLS. Características adicionais como limitação de banda e mecanismos de proteção contra falhas tornaram esses protocolos ainda mais funcionais.

Contudo, para que nós MPLS estabeleçam túneis ao longo da rede, de forma que tenham seus requisitos de banda e prioridade atendidos, um protocolo precisa obter, atualizar e distribuir informações sobre a topologia de rede e recursos disponíveis dos elementos participantes para todos os nós. Por isso, os protocolos OSPF e *Intermediate System to Intermediate System* (ISIS) também foram estendidos, formando OSPF-TE (Katz, Yeung & Kompella, 2003) e ISIS-TE (Smit,

2004) para serem opções na escolha de um protocolo de roteamento com objetivos de engenharia de tráfego.

Em redes MPLS os nós podem tomar decisão de encaminhamento de pacote nó a nó *(hop by hop routing)* ou trabalhar com a opção de seleção de rota explícita *(explicit routing)* (Rosen, Viswanathan & Callon, 2001). O fato da decisão ser baseada no *Label* do pacote MPLS ao invés do endereço destino do pacote IP, proporciona aos nós *Label Switch Router - LSR* a implementação de serviços como engenharia de tráfego através de *explicit routing,* ou a possibilidade de trabalhar num modo de escolha de rota feita nó a nó como no modelo clássico de encaminhamento IP, *hop by hop routing*.

Ao ingressar em elementos de rede participantes da rede MPLS, os pacotes IP são classificados em classes de encaminhamento equivalentes, *Forwarding Equivalent Class - FEC*. Em seguida, as FECs são mapeados para *Label Switch Path - LSP* de forma a permitir que o tráfego IP seja agregado e tratado unido, evitando problemas de crescimento como os encontrados nos modelos como *Intserv* (Mortier, 2002), por exemplo.

A engenharia de tráfego em redes MPLS consiste num controle rígido de variáveis do LSP por meio de uma explícita sinalização. Entre eles estão, os controles dos nós intermediários entre a origem e término, comportamento em caso de interrupção no trajeto, reserva de banda, prioridade, política de policiamento em caso de super utilização da banda e afinidades[1]. Essas variáveis podem ser determinadas e ativadas em uma rede através de métodos táticos, ou estratégicos on-line e off-line (Osborne, Simha, 2002).

As informações associadas a LSP são:

- Nós de origem e término

- Banda requerida

- Prioridade

- Nós intermediários desejados ou indesejados no trajeto

- Opção de inclusão de Afinidades no trajeto

- Parâmetros de recuperação em caso de falha (*fast-reroute*)

Todas essas informações potencializam a capacidade de controlar o trajeto do tráfego por tipo, prioridade ou cliente. Entre as vantagens apresentadas, estão:

a) Controle de congestionamento;

b) Melhor utilização dos recursos existentes;

[1] Afinidades podem ser usadas para implementar vários tipos de regras: rotas preferenciais, inclusão ou exclusão de grupos de links de um caminho de LSP. (Awduche, 2001) fornece maiores detalhes sobre este assunto.

c) Implementação de requisitos de roteamento;

d) Proteção contra falhas na rede;

e) Reserva de banda.

a) Controle de congestionamento

Com objetivo de diminuir a utilização de links congestionados, a engenharia de tráfego pode ser utilizada para rotear uma parte desse tráfego para links menos utilizados da topologia. Essa técnica é viável quando segmentos da rede estão congestionados, enquanto outras partes estão pouco ou inutilizadas.

Ela pode ser empregada taticamente, para reagir no momento do congestionamento, ou estrategicamente, para evitar períodos de congestionamento na rede.

Os fatores que podem causar congestionamento são: falhas em nós de rede, cordões de fibras ou em equipamentos da infra-estrutura responsável por prover o link, além de falta de energia, manutenções programadas, surtos de tráfego inesperados na rede em virtude de acontecimentos especiais, atraso na instalação de novos links, etc.

b) Melhor utilização dos recursos existentes

Na prática, muitas redes de provedores de serviço IP contêm múltiplos links dispostos paralelamente entre dois pontos. Links como n x E1 (onde n é um número de links), n x E3 ou n x STM-1 podem estar ligando dois roteadores simultaneamente, criando conexões de diferentes métricas na visão dos protocolos de roteamento destes roteadores. Como IGP elege caminhos de menor métrica, eles podem utilizar uma única conexão ou parte das existentes, mantendo outras inutilizadas.

MPLS pode ser usado com a finalidade de criar túneis LSP para controlar a proporção de demanda em cada link, configurando rotas explícitas, para esses túneis LSP distribuírem o tráfego através dos links paralelos. Essa solução também pode ser utilizada para redes que empreguem links como n x STM-4/16/64;

c) Implementação de requisitos de roteamento

Algumas vezes é desejável restringir certos tipos de tráfego de pacotes IP em certos tipos de links, ou explicitamente excluir certos segmentos da rede do trajeto de alguns tipos de tráfego para atender algumas aplicações específicas, acordos de nível de serviço, *Service Level Agreement – SLA,* ou características de segurança.

d) Proteção contra falhas na rede

As redes falham. Mais precisamente, pedaços de redes falham. Uma quantidade grande de variáveis pode falhar em uma rede. Podem falhar devido a um mau contato em conectores, até o rompimento de fibras, problemas em infra-estrutura, equipamentos como *Add/Drop Multiplexer - ADM*, falta de energia, falhas ou manutenções programadas em roteadores entre outras causas. Contudo, uma rede de comunicações deve manter seus serviços, mesmo quando sua topologia se altera.

A característica do MPLS de rápida otimização, após uma falha (*fast reroute)*, proporciona determinação do comportamento dos LSPs antes mesmo da constatação pelo usuário final de uma falha na rede ou diminuição dos recursos disponíveis.

O tempo gasto para restabelecimento de uma aplicação ou comunicação que utiliza um trecho de uma rede que apresenta uma falha, como uma queda de link ou nó, pode ser longo. O tempo para um IGP descobrir que houve uma falha em um link ou nó, recalcular seu banco de dados, informar os nós vizinhos e determinar uma nova rota pode ser suficiente para comprometer uma aplicação e/ou um nível de serviço acordado. Por isso, sinalizações através do protocolo RSVP (estendido para engenharia de tráfego) podem diminuir o tempo de interrupção da comunicação para ordem de milésimos de segundo, graças a característica de túneis *Shared Explicit* do RSVP-TE (Macre-Crane, Makam & Owens, 2003).

A característica de túneis *Shared Explicit* do RSVP proporciona o estabelecimento de dois túneis com mesma origem e destino, por caminhos diferentes e com a opção de reserva de banda nos dois trajetos. Isso evita o tempo gasto com sinalização, formação dos novos túneis e cálculo do algoritmo OSPF caso ocorra falha em algum deles, tornando a interrupção invisível para o protocolo de roteamento nos nós onde o túnel LSP se origina e termina.

e) Reserva de banda

A vantagem na utilização de RSVP para estabelecer túneis LSP está na possibilidade de reserva de banda no seu trajeto. Isto é realizável, porque o tráfego possui labels, o que permite aos roteadores identificar através deles o LSP desejado e aplicar a reserva configurada.

Durante o estabelecimento de um LSP o originador da mensagem realiza uma consulta pela disponibilidade de banda, nó a nó, até o destino desejado utilizando mensagens do RSVP-TE. Contudo, a confirmação considera não só a quantidade de banda desejada em relação a disponível, mas também as prioridades e afinidades configuradas de cada LSP.

Estas características possibilitam a garantia de banda a LSP e, consequentemente, ao tráfego que transportam, honrando os compromissos assumidos com os clientes.

A reserva de banda também é utilizada para fast-reroute. Neste caso, dois túneis com mesma origem e destino, mas com um ou mais trechos intermediários diferentes, são estabelecidos com reserva de banda para proporcionarem, na ocorrência de falha de algum elemento do trajeto principal, garantia de continuidade do serviço, além da rápida comutação.

4.2 Protocolo de roteamento para engenharia de tráfego: OSPF-TE

Com a utilização do MPLS e sua característica de implementação de labels nos pacotes IP, é possível transportar dentro de uma mesma rede MPLS fluxos de tráfego IP de diferentes clientes com mesmo endereçamento e com classes de serviço e trajetos diferentes. Entretanto, para que nós MPLS possam enviar e comutar esses fluxos no sentido mais adequado ao atendimento de seus requisitos de roteamento, um protocolo precisa obter, distribuir e manter a topologia da rede MPLS atualizada inclusive com informações relativas ao estado de utilização dos links em cada nó. Nessa seção, são estudadas as extensões do protocolo OSPF para engenharia de tráfego.

As extensões no protocolo OSPF e ISIS, caracterizando OSPF-TE (Katz, Yeung & Kompella, 2003) e ISIS-TE (Smith, 2004), respectiamente, foram feitas com o objetivo de adicionar, à base de dados da topologia da rede, informações atualizadas sobre o estado de utilização dos links entre cada roteador.

As extensões do protocolo OSPF foram escolhidas para serem abordados com mais detalhes neste trabalho, pois ele é um protocolo de roteamento IP muito empregado em redes IP em todo o mundo. Porém, também é valida a analogia com ISIS-TE .

OSPF-TE

No protocolo OSPF, as extensões são usadas para construir um banco de dados estendido, ou seja, um banco de dados de engenharia de tráfego. Dessa forma, um dispositivo participante de uma área[1] OSPF (Moy, 1998) cria um banco de dados de engenharia de tráfego e troca constantemente com seus vizinhos, informações sobre estado de utilização dos links da área que participa.

Essas informações têm sido úteis aos nós participantes do estabelecimento de LSP para poderem realizar o roteamento baseado em restrições, *constraint-based routing* (Awduche, 1999) de cada LSP.

O algoritmo de escolha de rota no OSPF, *Short Path First (SPF),* é utilizado no OSPF-TE para eleger uma rota de estabelecimento de LSP entre rotas capazes de atender seus requisitos de roteamento como, banda mínima, nós proibidos no trajeto, prioridade de estabelecimento em comparação com outros LSP e fast-

[1] Requisitos para engenharia de tráfego entre áreas OSPF (Le Roux *et al*, 2005) foram definidos, mas em entre Automonous System diferentes não foram completamente definidos (Zhang, 2004) até a data de conclusão deste material.

reroute, por exemplo. O processo consiste em desconsiderar rotas incapazes de atender esses requisitos e executar SPF nas rotas restantes. Por este motivo, o algoritmo do OSPF-TE foi chamado de *constraint-based routing* SPF (CSPF).

Existem outros algoritmos em desenvolvimento, principalmente no meio acadêmico, como por exemplo, métodos heurísticos, (EL-HAWARDY *et al.*, 2003) (Blanchy, Mélon & Leduc, 2003) (Banerjee & Sidhu, 2002).

O OSPF-TE, baseia-se na utilização de um *Link-state advertisement - LSA*, chamado de Opaque LSA (Coltun *et al.*, 1998). Assim como outros tipos de LSA, um Opaque LSA também possui um escopo de abrangência e, como foram criados três tipos, cada um tem uma abrangência diferente. O Opaque LSA tipo 10, por exemplo, é utilizado para permitir engenharia de tráfego dentro de uma área OSPF, pois denota um escopo de área local. O Opaque LSA consiste num cabeçalho do LSA, padrão do OSPF, seguido por um campo de informação de engenharia de tráfego conforme ilustra a Figura 12.

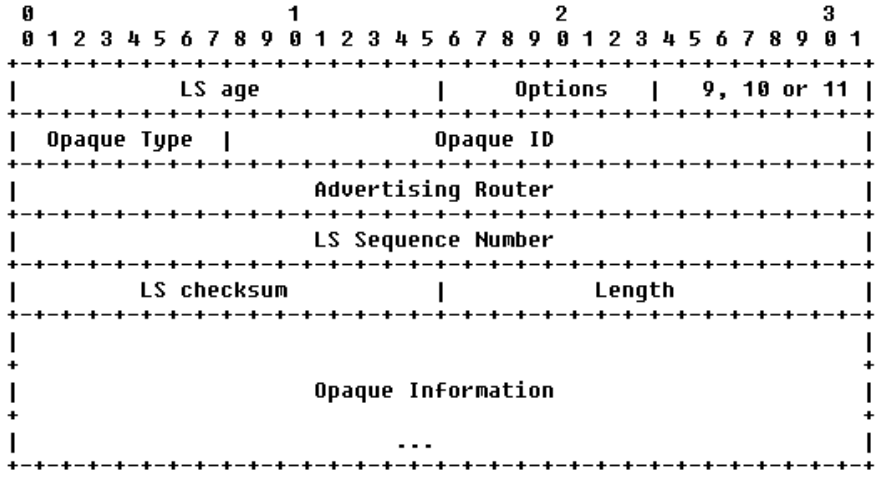


Figura 12. Formato do protocolo Opaque LSA (Coltun, 1998)

O campo de informação de engenharia de tráfego, Opaque Information, consiste em um ou mais modelos Type/Length/Value - TLV. O formato desse modelo pode ser visto na Figura 13, Formato do campo TLV do protocolo Opaque LSA.

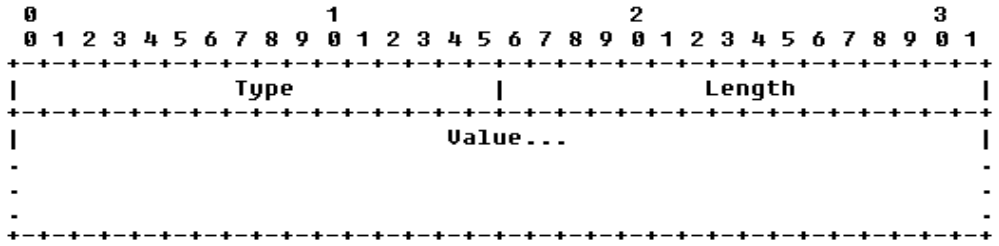


Figura 13. Formato do campo TLV do protocolo Opaque LSA (Coltun, 1998)

O TLV é utilizado por um nó LSR com o objetivo de divulgar/requisitar informações de roteamento com extensões para engenharia de tráfego.

O Opaque LSA é encaminhado em toda rede (*flooding*) utilizando os mecanismos padrões de encaminhamento que os outros tipos de LSA do OSPF utilizam. Entretanto, quando encaminhado em uma interface que o leva a um dispositivo participante do processo OSPF, mas desconfigurado para compreender este tipo de LSA, ele é descartado e, por conseqüência, inelegível para receber atualizações relacionadas a engenharia de tráfego. Porém, este nó estabelecerá vizinhança OSPF se houver resposta a outros tipos de LSA encaminhados. A tabela 1, ilustra a importância das informações de engenharia de tráfego obtidas durante atualizações pelo Opaque LSA.

Tabela 1 - Importância da informações obtidas pelo protocolo Opaque LSA

Informação	**Importância**
Endereço IP (loopback)	Identificar um roteador originador da mensagem
Tipo de link:	Distinguir links Point-to-Point de Multi-access.
Identificação do link	Identificar nó interligado pelo link
Endereço IP da interface local	Identificar links paralelos
Endereço IP da interface remota	Identificar links paralelos
Métrica de engenharia de tráfego	Possibilitar Interferência administrativa
Banda máxima	Informar capacidade real do link
Banda máxima reservada	Limitar uso do link ou aumentar a capacidade de alocação de banda estatística, como é feito com *burst exceed* (BE) do *Frame-Relay.*
Banda disponível	Limitar quantidade de banda disponível por nível de prioridade de túneis LSP.
Grupo administrativo	Associar interfaces de nós, a diferentes grupos de engenharia de tráfego.

Fonte Própria

Como podem ser observadas na tabela 1, as informações obtidas pelo Opaque LSA adicionam, à topologia da rede já formada pelo conteúdo de outros tipos de LSA, informações sempre atualizadas dos recursos existentes, de forma que os LSP tenham seus requisitos de roteamento atendidos.

4.3 Protocolo de sinalização para engenharia de tráfego: RSVP-TE

Com a capacidade dos pacotes serem comutados através de cabeçalhos comuns MPLS (labels) através de uma rede cuja forma e recursos disponíveis é conhecida, resta ao RSVP a tarefa de estabelecer, manter e remover os túneis ao longo da rede, manipulando os labels em cada trecho a fim de que o tráfego possa

ser transportado. Nesta seção, o papel do RSVP e suas extensões para engenharia de tráfego serão apresentados.

As redes MPLS, aplicadas à engenharia de tráfego, têm *labels* distribuídos entre os nós participantes feitos por demanda, ao invés de uma distribuição automática de label a todas as rotas conhecidas em um nó, como ocorre com o protocolo LDP empregado em aplicações MPLS com VPN.

A requisição de *labels* por demanda ocorre depois que o trajeto de um LSP é determinado, objetivando sempre atender seus requisitos de roteamento. Isso é necessário para que um nó saiba qual *label* ele deve adicionar ao pacote MPLS de modo que ao encaminhá-lo ao próximo nó, no trajeto do destino do túnel, este reconheça o pacote e dê continuidade ao encaminhamento até o destino final. Além disso, um LSP precisa ter sua quantidade de banda reservada e sua disponibilidade verificada constantemente, por isso foram definidos dois protocolos, apresentados a seguir, para realizar estas funções chamadas genericamente de sinalizações ao longo de todo seu trajeto.

O grupo de trabalho da arquitetura MPLS, para atender os objetivos de engenharia de tráfego (*explicit routing*), definiu inicialmente dois protocolos, o *Reservation Protocol*, RSVP-TE e o *Constraint-Based* (LDP - CR-LDP) baseado no LDP.

Desde então, sucederam-se esforços para desenvolvimento dos dois protocolos e o estabelecimento de padrões, mas sem uma definição pelo grupo de trabalho MPLS do caminho a ser seguido. Contudo, em fevereiro de 2003, de acordo com Smith (2004), "*The Multiprotocol Label Switching (MPLS) Working Group decision on MPLS signaling protocols*" documenta o consenso do grupo de trabalho do MPLS na decisão de continuar a desenvolver o RSVP TE (Awduche *et al*., 2001) como protocolo de sinalização para aplicações de engenharia de tráfego em implementações em MPLS, e também, a opção em dispensar esforços relacionados ao CR-LDP.

Paralelo à esta posição do IETF, os fabricantes de equipamentos com suporte a MPLS, já haviam demonstrado sua preferência pelo emprego do RSVP-TE nos anuais congressos internacionais de MPLS e nos eventos de interoperabilidade organizados pelo *MPLS and Frame Relay (MPLS and FRAME RELAY ALLIANCE*, 2004).

Nesta dissertação foi levado em consideração a mesma opção do IETF e dos fabricantes de equipamentos com suporte a MPLS, ou seja, focou-se o RSVP-TE.

RSVP-TE

O RSVP é um mecanismo de sinalização usado para reservar recursos através da rede. Foi definido a ele seu próprio tipo de protocolo de camada de transporte, o 46, sendo assim possível de ser roteado pelo IP (Braden *et al*,1997). Portanto, todas as decisões de roteamento são tomadas por IGP com extensões para engenharia de tráfego como o protocolo OSPF-TE, visto na seção 4.2.

O RSVP-TE suporta o estabelecimento de E*xplicity Routed LSPs*, com ou sem reserva de recursos, além de suportar também rápida mudança de trajeto de LSPs e detecção de *looping*. Essa característica é uma das mais importantes e responsáveis para a engenharia de tráfego, pois permiti a determinação exata do trajeto de um LSP, reserva de banda e rápida recuperação a falhas.

As funções do RSVP-TE são: estabelecer túneis LSP com opção de atendimento de requisitos de roteamento, identificar e alterar dinamicamente seu trajeto, distinguir e diagnosticá-los, aplicar políticas de prioridade e, principalmente, apresentar capacidade de realizar alocação de *labels* por demanda.

Para realizar estas funções foram adicionados outros objetos aos já existentes na especificação do RSVP. Entretanto, todos são aplicados a um ou mais tipos de mensagens RSVP, ilustradas na Tabela 2:

Tabela 2 - Mensagens e correspondente importância do protocolo RSVP-TE

Tipo de mensagem	**Importância dos objetos**
Path	Estabelecer e manter reservas ao longo da rede, informar o tipo de trajeto, prevenir *loopings*, identificar sessões LSP e especificar prioridades e afinidades.
Resv	Confirmar a mensagem Path, divulgar o label a ser utilizado e informar o modo de reserva escolhido Fixed Filter (FF) ou Shared Explicit (SE) (Awduche *et al*., 2001).
PathTear	Remover reservas da rede
ResvTear	Confirmar a mensagem PathTear
PathErr	Reportar erros em mensagens Path
ResvErr	Reportar erros em mensagens Resv ou interrupções na reserva de banda em algum link.
ResvConf	Confirmar ao originador de Resv que os recursos foram reservados (opcional)
Hello[1]	Detecção rápida de falhas de nós vizinhos (opcional).

Fonte Própria

Cada uma das mensagens acima utiliza o cabeçalho padrão do RSVP, ilustrado na Figura 14, diferenciado entre si pelo campo *Msg Type*, seguido por um objeto de tipo, classe, tamanho e conteúdo variável, ilustrado na Figura 15.

[1] A mensagem Hello é a única que foi criada na RFC 3209, com o objetivo de adicionar capacidade de detecção de falha de links e nós a fim de permitir rápida comutação para um caminho alternativo

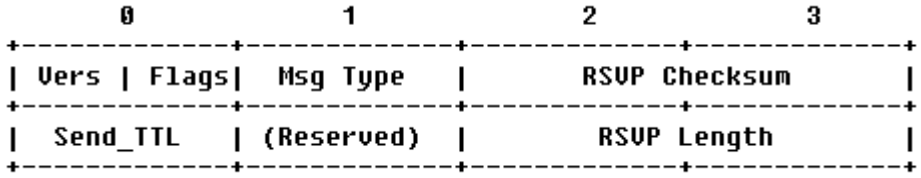


Figura 14. Formato do cabeçalho do protocolo RSVP (Braden,1997)

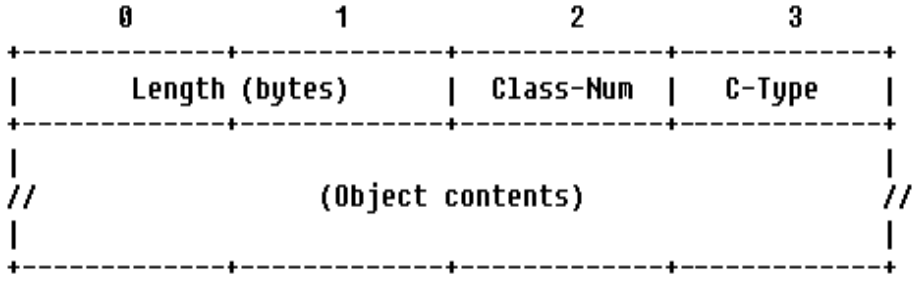


Figura 15. Formato do protocolo RSVP (Braden,1997)

Os novos objetos das mensagens RSVP, carregados no formato da Figura 15 (Awduche *et al*., 2001), adicionam campos[1] para requisição e transporte de labels, identificação da seqüência de nós que um túnel deverá passar, identificação de um túnel, estabelecimento de um túnel redundante com a finalidade de realizar a comutação entre eles sem interrupção na transmissão dos pacotes, possibilidade de reservar banda em cada túnel, além de oito possíveis níveis de prioridade para privilegiar o estabelecimento de alguns túneis sobre outros e capacidade de detecção rápida de falha de nós ou link através de mensagens HELLO.

Para melhor compreensão do funcionamento de um LSP, a seguir são descritos os processos de:

a) Estabelecimento;

b) Manutenção;

c) Remoção;

d) Sinalização de erros;

e) Fast-reroute.

a) Estabelecimento

Para que um túnel seja estabelecido, o nó originador do túnel define o trajeto de acordo com as características de roteamento que o túnel exigir, como rota

[1] Todos os campos adicionados na RFC3209, possuem aplicabilidade em engenharia de tráfego para redes com protocolo IPv4 e IPv6.

explícita, banda, afinidades e custos administrativos, e através de CSPF inicia o processo enviando uma mensagem *Path* em direção ao primeiro roteador no trajeto até o nó destino.

Ao receber e checar a integridade da mensagem *Path*, o nó executa um processo de controle de admissão para verificar se a quantidade de banda solicitada pela mensagem pode ser disponibilizada - campos de prioridade também são verificados nesta mensagem. Em caso negativo, uma mensagem de erro é dada como resposta, fazendo com que o originador do túnel procure um outro trajeto.

Entretanto, se houver recursos e o nó for intermediário, ou seja, estiver entre a origem e o destino do túnel, este não confirma ainda ao nó originador da mensagem *Path* a alocação de banda. Por enquanto, cria uma nova mensagem *Path,* como solicitação de recursos e *label*, e o envia ao próximo nó a fim de alcançar o destino final do túnel, de acordo com o trajeto definido pelo nó originador e descrito no objeto *explicit routing* presente na mensagem *Path,* repetindo o procedimento realizado pelo nó anterior.

Todo este procedimento é repetido pelos nós intermediários até que o destino final do túnel responda com uma mensagem *Resv,* confirmando a alocação de recursos com *label* com o qual o nó anterior a ele (o gerador da mensagem *Path*) deverá usar para utilizar este túnel.

Cada nó ao receber a mensagem *Resv*, realiza o mesmo procedimento, confirmando a alocação de recurso ao nó que lhe enviou a mensagem *Path,* e lhe informa qual *label* usar para utilizar este túnel. Este procedimento novamente é seguido até que alcance o nó originador do túnel.

Essa característica do RSVP-TE é conhecida como distribuição de *labels* por demanda, do termo em inglês *Downstream-on-demand Label Distribution*.

b) Manutenção

O RSVP-TE é um protocolo que após estabelecer seus túneis, realiza sinalizações periódicas em cada túnel estabelecido – semelhante aos pacotes de *hello* do OSPF (Moy, 1998) – a fim de detectar ocasionais falhas em nós vizinhos ou mudança no estado de links ao longo do caminho de um túnel LSP. Essa característica é conhecida como *Soft-State Protocol*.

Para a manutenção de um túnel, um nó envia mensagens *Path*, em intervalos de poucos segundos, em direção ao vizinho que confirmou o estabelecimento do LSP, a fim de informar que deseja que os recursos continuem sendo mantidos. Se este nó, enviar quatro mensagens de *Path*, e não receber uma mensagem *Resv* durante este tempo, este túnel será considerado inexistente.

Entretanto, nesta etapa as mensagens *Path* e *Resv* são enviadas independentemente e sem sincronismo entre dois vizinhos. A mensagem *Resv*, por exemplo, é usada para informar que os recursos continuam sendo alocados.

c) Remoção

Se um nó, geralmente o originador de um túnel, decidir que a reserva de banda será desnecessária naquele caminho, uma mensagem *PathTear* é enviada no mesmo sentido que *Path,* e uma mensagem de confirmação de remoção de recursos, *ResvTear*, é respondida, da mesma forma que a mensagem *Resv*. Entretanto, as mensagens *PathTear* não percorrem todo o caminho do túnel para terem efeito. Se um nó enviar uma *PathTear* ao seu nó vizinho, este responderá imediatamente com um *ResvTear*, e repetirá o procedimento com seu outro vizinho participante do estabelecimento do túnel.

d) Sinalização de erros

Ocasionalmente erros podem ser encontrados na manutençãos de túneis. Se um erro for detectado por uma mensagem *Path*, ele será sinalizado como *PathErr*, e para erros detectados em mensagens de *Resv*, o erro será sinalizado com *ResvErr*.

e) Realizando *Fast Reroute*

O mecanismo de detecção de falhas do RSVP-TE através do envio e recebimento de Path e Resv são insuficientes para acusar com rapidez a falha em um link ou nó da rede por onde o LSP está estabelecido.

Mensagens do tipo *hello,* figura 16, foram implementados de forma opcional, para tornar o mecanismo de detecção a falhas mais eficiente. Pacotes *hello* são enviados e confirmados em intervalos de milésimos de segundo (Awduche *et al*., 2001) (Boyle *et al*., 2002), (Swallow, 2004), (Laurence, 2003). A falta de confirmação de um determinado número de *hellos* enviados, implica em consideração de uma falha de nó ou link de rede.

Além do mecanismo de *hello*, interfaces de rede MPLS, ligadas diretamente a equipamentos *Add-drop Multiplexer – ADM* e denominadas interface *Packet Over SDH/Sonet - POS*, podem se utilizar do mecanismo de alarmes dessa tecnologia para informar falhas na rede a nós MPLS já que a detecção em nível físico é muito rápida.

Após a descoberta de uma falha na rede, o nó originador é notificado para que altere o trajeto do LSP. Técnicas definidas na (Awduche *et al*., 2001) como *Make Before Break*, de estabelecimento de duplos LSP, com mesma origem e destino, mas trechos do trajeto distintos são utilizados para tornarem a interrupção do tráfego ainda menor.

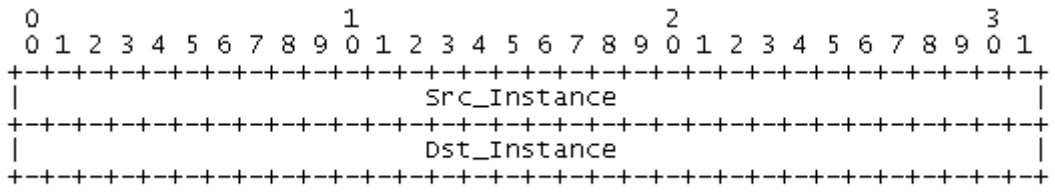


Figura 16. Formato da mensagem Hello

4.4 Considerações Parciais

O protocolo de roteamento OSPF e sua característica hierárquica, rápida convergência e baixo tráfego de atualizações de roteamento, ao contrário dos protocolos de roteamento do tipo *distance-vector*, fizeram dele um protocolo utilizado em larga escala por ser eficaz em médias e grandes redes.

Características de engenharia de tráfego não foram previstas no OSPF, por isso técnicas como alterações das métricas são utilizadas para mudança do sentido do tráfego ou para realizar balanceamento de carga com outros caminhos disponíveis. Esses recursos são utilizados, certamente, em muitas redes OSPF, mas a competição por preços e compromisso com nível de serviço, tem exigido busca por outras alternativas.

Nota-se pelas vantagens disponibilizadas e estudadas no item 2.3 - Engenharia de tráfego com utilização de circuitos virtuais, e 4.1 - Funcionamento e Benefícios da engenharia de tráfego com MPLS, que tal operação é melhor executada quando sai da responsabilidade do protocolo de roteamento. Cronologicamente, a utilização dos circuitos virtuais do Frame-Relay e depois do ATM, tiraram da camada de rede, responsável pelo roteamento do pacote IP, a execução da engenharia de tráfego que passou a ser feita em camada 2. Mais adiante, com a criação da arquitetura MPLS e extensão dos protocolos RSVP-TE e OSPF-TE, a engenharia de tráfego pode ser melhor executada do que em qualquer técnica anterior, conforme vantagens apresentadas neste capítulo.

Contudo, como o aprimoramento dos protocolos é constante. A utilização dos campos *Flow Label* e *Next Header* do IPv6, como citadas no item 2.4 - Engenharia de Tráfego com IPv6, unidos com a utilização do OSPFv3, que é compatível com IPv6, pode trazer novamente aos IGP a responsabilidade de executar engenharia de tráfego. Por outro lado, como os provedores de serviço precisam de uma solução de engenharia de tráfego imediata para suas redes, a opção mais eficiente até o momento, é através do MPLS.

5 Parte Prática

Neste capítulo será apresentada uma demonstração prática de engenharia de tráfego utilizando MPLS e alteração das métricas do OSPF. O capítulo termina com uma análise dos resultados.

5.1 Objetivo

O objetivo da parte prática desta dissertação é demonstrar a capacidade de controle do tráfego IP possibilitada pelos recursos de engenharia de tráfego do MPLS e desenvolver um procedimento didático de estudo prático com MPLS que possibilite alunos de redes de computadores melhorarem sua compreensão desse assunto.

5.2 Introdução

Os conjuntos de protocolos que formam as redes MPLS foram desenvolvidos para adicionarem maior controle do tráfego e novas aplicações IP em núcleos de grandes redes, onde são empregados elementos de grande capacidade de processamento e de conectividade a outros equipamentos. Por isso, o alto custo de aquisição desse nível de equipamento, dificulta a implementação de MPLS em laboratório.

Simulações de redes MPLS têm sido feitas, com o software *Network Similator - NS* (NS2, 2004), simulador de elementos de rede, baseado em modelos matemáticos, que pode funcionar em um único computador. Entretanto, implementações práticas tem sido feitas com MPLS-Linux (VA Linux Systems, 2004) ou *RSVP-TE Daemon for DiffServ over MPLS under Linux* (INTEC, 2004) que são alterações em kernel de sistemas operacionais LINUX para fazer um computador se comportar como um roteador MPLS. Graças a esse tipo de implementação o MPLS é melhor compreendido, pois permite interação prática com a arquitetura e com baixo investimento para realizá-la.

A demonstração de protocolos de redes MAN e WAN em laboratório apresentam dificuldades de implementação devido à dificuldade de obtenção dos equipamentos e meios de interligação. Entretanto, com os recursos utilizados nesta dissertação, essa arquitetura pôde ser demonstrada e estudada em laboratório com computadores interligados através de interfaces Ethernet e FastEthernet. A idéia é válida, pois a arquitetura MPLS é também empregada em redes MAN *Gigabit Ethernet*.

A implementação nesta dissertação foca os benefícios adicionados a engenharia de tráfego IP com os recursos disponibilizados pelo MPLS, enquanto submete o interessado num procedimento de melhor compreensão da arquitetura. Para isso, optou-se pela alternativa de implementação em código aberto Linux com

kernel alterado, *RSVP-TE Daemon for DiffServ over MPLS under Linux,* porque disponibiliza ferramentas de estabelecimento e encaminhamento de tráfego específico em túnel LSP, ou seja, realizando engenharia de tráfego.

A alternativa de implementação com MPLS-Linux permite configurações com *Label Distribution Protocol* (LDP) e estabelecimento de túneis LSP de nó a nó manualmente. Por isso, segue a linha didática de outra aplicação MPLS, o VPN, onde, em conjunto com MP-BGP, permitem o compartilhamento de uma única rede IP por várias outras redes. O item 3.2 - Aplicações com MPLS, aborda melhor o assunto.

5.3 Software Utilizados

5.3.1 RSVP-TE Daemon for Diffserv over MPLS under Linux

O *RSVP-TE Daemon for Diffserv over MPLS under Linux* foi desenvolvido baseado na arquitetura MPLS (RFC3031) do IETF. Ele estabelece túneis MPLS com suporte a DiffServ, padrão RFC2475, utilizando RSVP-TE, padrão RFC2205.

O *RSVP-TE Daemon* consiste na combinação de determinado kernel com *patches*, que possibilitam computadores fornecer labels MPLS, configurar LSP, comutá-los de acordo com os labels, reservar banda e aplicar diferentes tipos de tráfego a cada LSP.

Para desenvolver este código foi reutilizado o *Nistswitch version 2* para Free BSD (Nist, 2000) que por sua vez, foi baseado em *ISI RSVP implementation* (ISI, 1999) porém, todos sem prosseguimento em seus projetos à algum tempo. Além disso, o *RSVP-TE Daemon* reutiliza alguns conceitos do projeto MPLS-Linux.

5.3.2 Zebra

O Zebra (ZEBRA, 2004) é um software livre que gerencia protocolos de roteamento TCP/IP de forma modular. Entre os protocolos válidos estão RIPv2, BGP-4, OSPFv2 e ISIS. Todo seu desenvolvimento foi baseado em padrões do IETF e por isso tem interoperabilidade com roteadores comerciais.

5.3.3 Gerador de Tráfego JTG

O gerador de tráfego JTG (Manner, 2005), é um software livre desenvolvido para Linux por Jukka Manner da Universidade de Helsinki, Finlândia. A característica principal é possibilitar a transmissão de diferentes tipos de tráfego ao mesmo tempo com características diferentes uns dos outros em um mesmo computador.

Ele é utilizado durante a experiência 4 no item 5.4, a fim de gerar tráfego UDP com port 6000 e 6001 para que o RSVP-TE possa aplicá-los em LSP diferentes.

5.4 Experiências

Mesmo com objetivo didático, procurou-se formular experiências e um diagrama de rede que ilustrasse situações reais. Nesta linha, destacam-se as seguintes características:

- O diagrama de rede, figura 17, apresenta computadores diretamente conectados por cabos *crossover* uns aos outros através de interfaces FastEthernet, simulando roteadores MPLS conectados por interfaces Gigabit Ethernet numa rede metropolitana.

- A disposição dos computadores representa a rede de um provedor de serviço, com elementos de núcleo de rede, também chamado de Core, elementos de borda e clientes conectados em diferentes pontos da rede.

- Todo endereçamento IP e máscaras aplicadas são baseados em implementações reais.

- A rede possui protocolo de roteamento OSPF, para possibilitar aos nós participantes condições de estabelecimento de túneis LSP.

- O protocolo OSPF assim como os protocolos RSVP-TE e MPLS empregados nos computadores com Linux foram desenvolvidos conforme padrões do IETF.

- A configuração dos softwares que possibilitam OSPF e RSVP-TE possui lógica semelhante a utilizada em roteadores comerciais.

A Figura 17, Diagrama de laboratório, ilustra o diagrama de laboratório implementado e utilizado para desenvolvimento do procedimento.

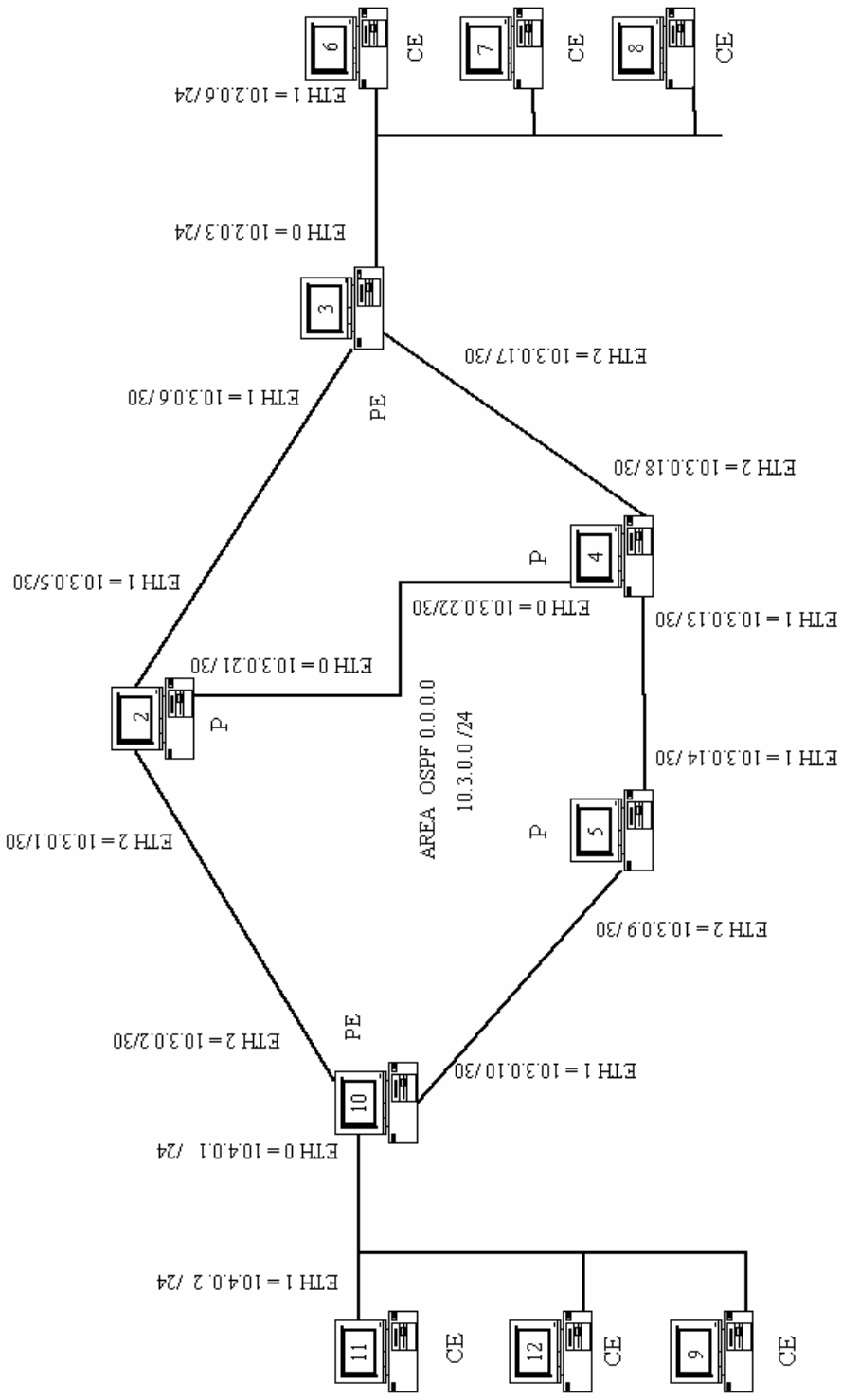


Figura 17. Diagrama de laboratório

5.4.1 Procedimento experimental

Um procedimento experimental foi desenvolvido para atender os dois objetivos planejados, ou seja, demonstrar a melhoria de controle de tráfego IP, a medida que submete o aluno a uma experiência prática com MPLS.

A seguir, o procedimento é apresentado com os resultados da experimentação e a análise teórica de cada item. No Anexo A, "Experiências de engenharia de tráfego: procedimento de laboratório", encontra-se a forma como poderia ser apresentado em aulas sobre o assunto, pois possui desenvolvimento didático, seguido do Procedimento de instalação do RSVP-TE no Anexo B e do Procedimento de instalação do OSPF, no Anexo C.

1º Parte Configurando a rede

Após instalação dos softwares nos computadores do laboratório, de acordo com os procedimentos nos Anexos B e C, cada um deles foi associado a um elemento do diagrama de rede e tiveram suas interfaces, endereços de rede e mascarás configurados no kernel de acordo com a proposta do diagrama. Por exemplo, no computador 10, foram utilizados os comandos descritos na figura 18, Configuração da Rede.

```
ifconfig eth0 10.4.0.1 netmask 255.255.255.0

ifconfig eth2 10.3.0.2 netmask 255.255.255.252

ifconfig eth1 10.3.0.10 netmask 255.255.255.252
```

Figura 18. Configuração da rede

Os computadores classificados no diagrama, como CE, puderam funcionar em qualquer sistema operacional, pois desempenhavam o papel de clientes, ou seja, geravam tráfego IP e não recebiam as mensagens do RSVP-TE ou OSPF. Os computadores P e PE, representaram um provedor de serviço, e por isso receberam as configurações apresentadas nos itens a seguir.

2º Parte Configurando Zebra

Na segunda parte da experiência, o Zebra foi utilizado para possibilitar protocolo de roteamento OSPFv2. Este aplicativo funciona de forma modular, dividindo as tarefas de configuração e gerenciamento de interfaces e rotas estáticas num módulo e de roteamento de protocolos como OSPF, RIP, BGP em outros módulos. Nesta etapa, concentrou-se no primeiro módulo, ou seja, onde apenas foram declaradas as interfaces e endereços IP utilizados no diagrama, Figura 19.

```
! Zebra configuration saved from vty
!   2005/05/13 18:58:48
!
hostname Router3-z
password zebra
enable password zebra
!
interface eth0
 bandwidth 10000
 ip address 10.2.0.1/24
!
interface eth1
 bandwidth 10000
 ip address 10.3.0.6/30
!
interface eth2
 bandwidth 10000
 ip address 10.3.0.17/30
!
interface lo
!
interface teql0
!
ip forwarding
!
line vty
 exec-timeout 0 0
!
```

Figura 19. Configuração do Zebra - 1º Parte

A composição do custo entre dois nós participantes de um processo OSPF é baseado na soma dos custos dos enlaces existentes entre eles. Por sua vez, o OSPF calcula o custo de cada enlace dividindo-se um valor constante, 100.000.000, pela banda total do link. Por isso, foi declarado nas interfaces dos computadores, que a banda disponível em cada enlace seria de 10.000.000 bits por segundo, com o comando bandwidth[1] 10.000, com o intuito de aplicar a todas as interfaces dos computadores, Ethernet ou FastEthernet, um custo de 10.

3º Parte Configurando OSPF

Nesta etapa o modulo OSPF do Zebra foi configurado. A figura 20, apresenta um exemplo de configuração que foi aplicada a todos os computadores P e PE, ou seja, aqueles que representavam a rede do provedor de serviços.

[1] O comando bandwidth considera os valores em kpbs.

```
! Zebra configuration saved from vty
!   2005/05/10 18:43:07
!
hostname ospfd
password zebra
log stdout
!
interface eth0
!
interface eth1
!
interface eth2
!
interface lo
!
interface teql0
!
router ospf
 redistribute connected
 network 10.3.0.0/24 area 0.0.0.0
!
line vty
 exec-timeout 0 0
```

Figura 20. Configuração do Zebra - 2º Parte

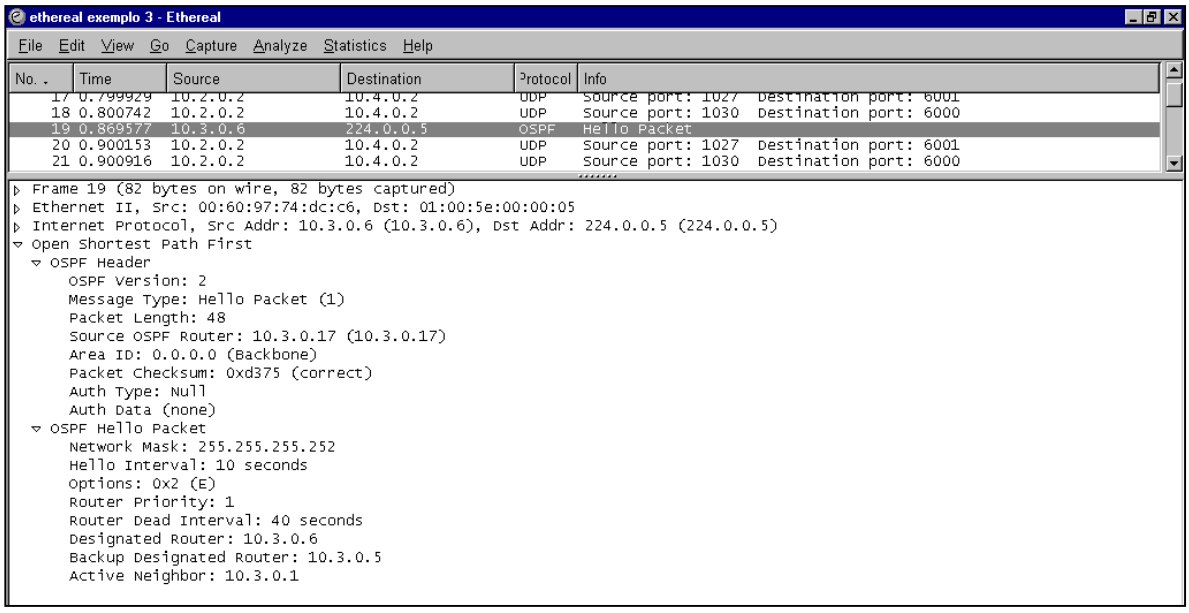


Figura 21. Pacote OSPF no Analisador de Protocolos

Entre as configurações da figura 20, destaca-se a referente a da área OSPF. Nesta linha declarou-se a rede participante e que área ela pertencia, pois indicou aos computadores qual rede possibilitaria estabelecimento de vizinhança OSPF com outros computadores. A linha "*redistrubute connected*", foi adicionada com o objetivo de indicar aos computadores que redistribuíssem aos seus vizinhos, redes que

estavam conectadas a eles e diferentes de 10.3.0.0/24. Por exemplo, a rede dos clientes 10.4.0.0/24 e 10.2.0.0/24.

A figura 21, ilustra um pacote OSPF do tipo *Hello packet tipo 1*, capturado pelo analisador de protocolos. Pacotes como esse, são enviados por um nó OSPF nas interfaces com endereço IP declaradas como pertencentes a área OSPF, a cada 10 segundos, para comprovar que o link e o nó vizinho continuam funcionando.

A figura 22, apresenta as rotas descobertas e as redistribuídas pelo OSPF no computador 3.

```
ospfd# show ip ospf route
============ OSPF network routing table ============
N    10.3.0.0/30           [20] area: 0.0.0.0
                           via 10.3.0.5, eth1
N    10.3.0.4/30           [10] area: 0.0.0.0
                           directly attached to eth1
N    10.3.0.8/30           [30] area: 0.0.0.0
                           via 10.3.0.5, eth1
                           via 10.3.0.18, eth2
N    10.3.0.12/30          [20] area: 0.0.0.0
                           via 10.3.0.18, eth2
N    10.3.0.16/30          [10] area: 0.0.0.0
                           directly attached to eth2
N    10.3.0.20/30          [20] area: 0.0.0.0
                           via 10.3.0.5, eth1
                           via 10.3.0.18, eth2

============ OSPF router routing table =============
R    10.3.0.2              [20] area: 0.0.0.0, ASBR
                           via 10.3.0.5, eth1

============ OSPF external routing table ===========
N E2 10.4.0.0/24           [20/20] tag: 0
                           via 10.3.0.5, eth1
```

Figura 22. Tabelas de rotas do processo OSPF

O kernel dos computadores funciona como mecanismo de encaminhamento dos pacotes. Eles são configurados através dos comandos *make menuconfig* ou make xconfig ou *make config* no diretório /usr/src/linux-x.x.x, por exemplo. Além disso, recebe todas as atualizações de rotas do processo OSPF, como pode ser observado comparando as figuras 22 e 23.

```
[root@Router3 root]# ip route
10.3.0.0/30 via 10.3.0.5 dev eth1  proto zebra  metric 20
equalize
10.3.0.4/30 dev eth1  proto kernel  scope link  src 10.3.0.6
10.3.0.8/30  proto zebra  metric 30 equalize
        nexthop via 10.3.0.5  dev eth1 weight 1
        nexthop via 10.3.0.18  dev eth2 weight 1
10.3.0.12/30 via 10.3.0.18 dev eth2  proto zebra  metric 20
equalize
10.3.0.16/30 dev eth2  proto kernel  scope link  src 10.3.0.17
10.3.0.20/30  proto zebra  metric 20 equalize
        nexthop via 10.3.0.5  dev eth1 weight 1
        nexthop via 10.3.0.18  dev eth2 weight 1
10.2.0.0/24 dev eth0  proto kernel  scope link  src 10.2.0.1
10.4.0.0/24 via 10.3.0.5 dev eth1  proto zebra  metric 20
equalize
127.0.0.0/8 dev lo  scope link
```

Figura 23. Tabela de rotas do kernel do computador 3

Experiência 1 - Obtenção do trajeto do tráfego em condições normais da rede

Como o protocolo OSPF escolhe rotas para o destino de acordo com o menor custo a partir da origem, um tráfego IP entre computadores CE (11 e 6), representando um cliente, foi submetido à rede para obter o trajeto que o protocolo OSPF determinaria.

Como pode ser observado na Figura 24, o trajeto determinado entre os CE, foi através do computador 2, pois apresentou o menor custo, ou seja, total de 20.

```
[root@Router3 root]# traceroute 10.4.0.2
traceroute to 10.4.0.2 (10.4.0.2), 30 hops max, 38 byte
packets
 1  10.3.0.5 (10.3.0.5)  3.189 ms  1.244 ms  7.946 ms
 2  10.3.0.2 (10.3.0.2)  6.022 ms  32.824 ms  0.718 ms
 3  10.4.0.2 (10.4.0.2)  1.318 ms  0.983 ms  0.973 ms
```

Figura 24. Trajeto do tráfego entre os CE 11 e 6

Experiência 2 - Realização de balanceamento do tráfego entre os dois nós.

A alteração do custo de um encale da rede através do comando *bandwidth*, pode alterar o trajeto do tráfego entre CE. Por exemplo, um aumento do custo do enlace entre os computadores 3 e 2 para 20, proporcionou o aparecimento, na tabela de roteamento do computador 3, de uma segunda rota para o computador 11, Figura 25.

```
ospfd# show ip ospf route
============ OSPF network routing table ============
N    10.3.0.0/30           [30] area: 0.0.0.0
                           via 10.3.0.5, eth1
N    10.3.0.4/30           [20] area: 0.0.0.0
                           directly attached to eth1
N    10.3.0.8/30           [30] area: 0.0.0.0
                           via 10.3.0.18, eth2
N    10.3.0.12/30          [20] area: 0.0.0.0
                           via 10.3.0.18, eth2
N    10.3.0.16/30          [10] area: 0.0.0.0
                           directly attached to eth2

============ OSPF router routing table =============
R    10.3.0.2              [30] area: 0.0.0.0, ASBR
                           via 10.3.0.5, eth1
                           via 10.3.0.18, eth2

============ OSPF external routing table ===========
N E2 10.4.0.0/24           [30/20] tag: 0
                           via 10.3.0.5, eth1
                           via 10.3.0.18, eth2
```

Figura 25. Tabela de roteamento OSPF - Experiência 1

A presença no kernel dos computadores de duas rotas para um mesmo destino, como pode ser observado na Figura 25, indicou que o computador utilizará as duas rotas para encaminhar o tráfego para o destino especificado. Este comportamento caracteriza, portanto, um objetivo buscado pela engenharia de tráfego.

Entretanto, observou-se que o balanceamento de tráfego, realizado pelos computadores Linux desse laboratório, foi realizado unidirecionalmente por aplicação. Por exemplo, mensagens ECHO do comando ping enviados do computador 6 (CE) para o computador 11 (CE) foram encaminhados por uma rota, enquanto as mensagens de ECO REPLY do mesmo comando retornavam pelo outro trajeto, pois o destino, 11, também possuía rotas para balanceamento de carga. O mesmo ocorreu com mensagens OPEN do comando *telnet.* Elas foram encaminhadas por uma rota enquanto as mensagens de confirmação vieram por outra rota.

Considerando que aplicações de computadores possuem quantidade de tráfego de transmissão (tx) diferente do tráfego de recepção (rx), este comportamento indica um aspecto negativo para a engenharia de tráfego em computadores com Linux e OSPF, pois implica em um balanceamento de carga desproporcional entre as rotas disponíveis.

Roteadores comerciais que apresentam a opção de balanceamento de tráfego por pacote, não possuem este problema, pois dividem pelas rotas disponíveis, todos os pacotes de todas as aplicações. Contudo, limitações como

incapacidade de controle do trajeto do tráfego por endereço de origem, protocolo, port ou prioridade e por quantidade de tráfego enviada por rota, entre outras abordadas no capítulo 2 - Engenharia de Tráfego, comprovaram as limitações deste modelo.

O OSPF-TE, utilizado em redes MPLS com aplicação em engenharia de tráfego e abordado no capítulo 4, distribui entre nós participantes, além do custo dos enlaces, a taxa de ocupação dos LSP e reserva de banda por classe de tráfego. Entretanto, continua a apresentar o mesmo comportamento do OSPF comprovado acima.

Há a necessidade de que um protocolo realize exatamente os trajetos determinados e negocie reserva de banda entre outras funções, por isso o protocolo RSVP-TE é utilizado.

4º Parte Iniciando RSVP-TE daemon

O *RSVP-TE Daemon* é um programa de computador que possibilita o estabelecimento de túneis LSP em trajetos predeterminados com opção de reserva de banda, fast-reroute, marcação e administração dos labels em filas de QoS. Redes MPLS com aplicações em VPN, utilizam-se de outro protocolo para requisição e alocação de labels, o *Label Distribution Protocol* (LDP). A principal diferença é que este aloca label a todas as rotas presentes no roteador, ao contrário do RSVP-TE, que aloca os labels por demanda, ou seja, a medida que os túneis são estabelecidos.

Nesta etapa, o RSVP-TE foi iniciado em cada computador representante de um provedor de serviço, para permitir alocação de labels e o estabelecimento de túneis LSP.

Experiência 3 - Estabelecimento de túneis LSP.

Com o objetivo de alocar o tráfego em um trajeto diferente do determinado pelo protocolo OSPF, foram estabelecidos dois túneis entre as interfaces dos computadores 10 e 3. O túnel 100 (LSPID[1]=100) seguiu o mesmo trajeto do tráfego determinado pelo OSPF, ou seja, através da interface com endereço IP 10.3.0.5 do computador 2, e o segundo túnel (LSPID=200) seguiu através dos computadores 4 e 5, interfaces com endereço IP 10.3.0.18 e 10.3.0.14, respectivamente.

A figura 26, apresenta o protocolo RSVP-TE capturado pelo analisador de protocolo *Ethereal*. Nota-se que o label utilizado é 21680 para o LSPID 100 no enlace de rede 10.3.0.4/30. A mensagem capturada também apresenta que a manutenção do estabelecimento do túnel ocorre a cada 30 segundos, conforme observado no campo TIME VALUE. Este campo conclui que a manutenção do estabelecimento de um túnel MPLS torna a capacidade de diagnóstico de falhas muito lenta. Essa característica exige a presença da mensagem de hello do RSVP-

[1]. LSPID corresponde ao identificador de um Label Switch Path (LSP).

TE, conforme apresentada no item 4.3, Protocolo de sinalização para engenharia de tráfego, para permitir rápida detecção de falhas.

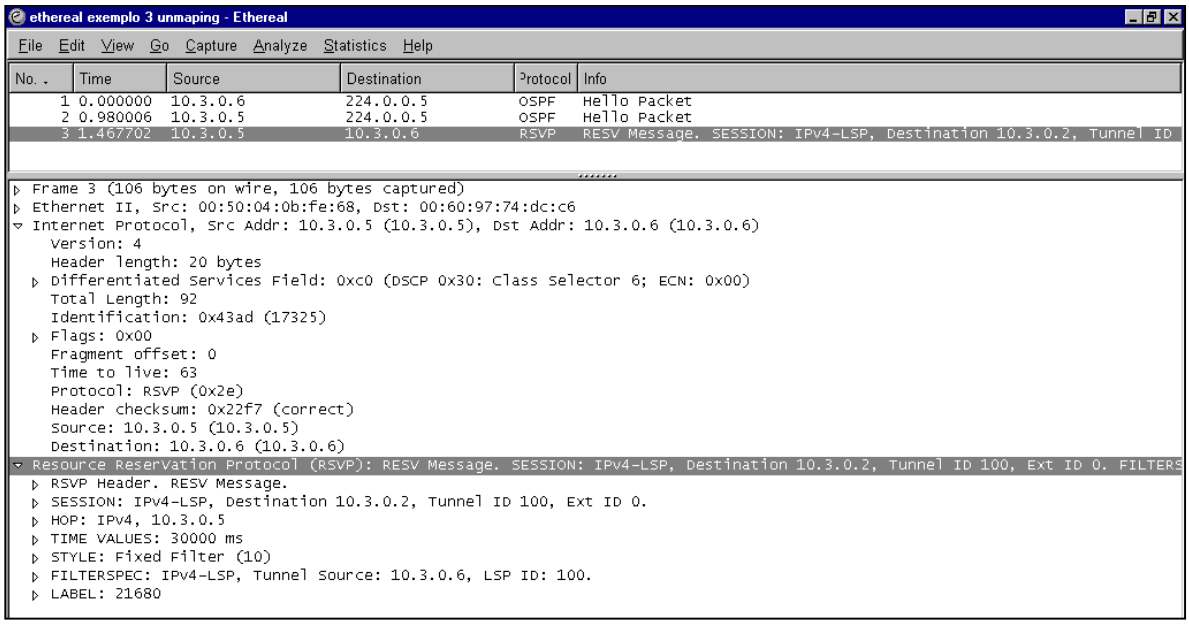


Figura 26. Protocolo RSVP-TE no Analisador de Protocolos

Os comandos na figura 27, foram utilizados para estabelecer os túneis LSP de número 100 e 200. Destaca-se, por exemplo, que o LSP 100 apresenta apenas um nó intermediário, denominado hop, antes do campo responsável pela identificação de fim de hop, ":0", ao contrário do LSP 200 que apresenta dois nós antes desse campo.

Destino	Origem	LSPID	Diffspec	hops	fim_de_hops	reroute
10.3.0.2	10.3.0.6	100	0 0	10.3.0.5	:0	0
10.3.0.10	10.3.0.17	200	0 0	10.3.0.18 10.3.0.14	:0	0

Figura 27. Comandos para estabelecimento de LSP

O tráfego IP em redes MPLS-TE é transmitido entre os nós de rede da forma tradicional até que um dos nós adicione o primeiro label, ou em outras palavras, submeta o tráfego sob o túnel LSP. Nesta lógica, os computadores 10 e 3, representando nós de extremidade com o cliente, realizaram esta operação.

Experiência 4 - Alteração da métrica do OSPF para verificação de mudança de trajeto do tráfego.

Com o objetivo de demonstrar a capacidade de manipulação do tráfego, independente da rota que o protocolo OSPF indicava, diminuiu-se manualmente o *bandwidth* entre os computadores 2 e 3 de 10.000 para 1.000 fazendo com que o trajeto de 6 para 11 fosse realizado através dos computadores 4 e 5, e demostrado pela figura 28.

```
ec2-06:~# traceroute 10.4.0.2
traceroute to 10.4.0.2 (10.4.0.2), 30 hops max, 38 byte packets
 1  10.2.0.1 (10.2.0.1)  0.724 ms  0.469 ms  0.352 ms
 2  10.3.0.18 (10.3.0.18)  0.816 ms  0.622 ms  0.479 ms
 3  10.3.0.14 (10.3.0.14)  1.634 ms  0.977 ms  0.781 ms
 4  10.3.0.10 (10.3.0.10)  1.480 ms  1.277 ms  1.026 ms
 5  10.4.0.2 (10.4.0.2)  1.629 ms  1.565 ms  1.177 ms
```

Figura 28. Demonstração I do trajeto do tráfego

Experiência 5 - Alteração do tráfego

Em seguida, optou-se por submeter todo o tráfego do computador 3 para o 11, através do túnel 100, figura 29, contrariando a rota determinada pelo OSPF.

```
[root@Router3 labeltest]# ./tunnel -m -a -d 10.4.0.2/32 -l100

Adding fwmark 1 table 1 rule
Add gw T21680eth1 to table 1
LSPID:100
```

Figura 29. Comando para submeter o tráfego sob um LSP

O comando para submeter o tráfego em LSP, utilizou as seguintes opções:

-m, para significar que esta mapeando o tráfego em um túnel MPLS.

-a, com o objetivo de incluir todos os protocolos a este mapeamento.

-d, para incluir o endereço IP do destino.

-l, a fim de indicar sob qual LSP mapear o tráfego com destino e tipo declarado.

Como resultado, um traceroute do computador 6 para o 11 voltou a apresentar o trajeto pelo computador 2, contrariando a rota determinada pelo protocolo OSPF.

```
ec2-06:~# traceroute 10.4.0.2
traceroute to 10.4.0.2 (10.4.0.2), 30 hops max, 38 byte packets
 1  10.2.0.1 (10.2.0.1)  0.994 ms  0.483 ms  0.352 ms
 2  10.3.0.5 (10.3.0.5)  0.967 ms  0.768 ms  0.628 ms
 3  10.3.0.2 (10.3.0.2)  1.266 ms  1.084 ms  0.856 ms
 4  10.4.0.2 (10.4.0.2)  1.618 ms  1.353 ms  1.176 ms
```

Figura 30. Demonstração II do trajeto do tráfego

A alocação foi retirada, apenas alterando a opção -m para -u (unmap), a fim de retirar o mapeamento realizado, Figura 31.

```
[root@Router3 labeltest]# ./tunnel -u -a -d 10.4.0.2/32 -l100
LSPID:100
```

Figura 31. Comando para retirar o tráfego sob um LSP

Entretanto, para demostrar que o controle de tráfego com MPLS-TE consegue ser ainda mais preciso, submeteu-se um tráfego UTP com port 6000 e 6001, provenientes do gerador de tráfego JTG (Manner, 2005) a partir do computador 6 para o computador 11, em dois LSP diferentes através da opção "-p" do comando de mapeamento de tráfego em túneis MPLS, Figura 32.

```
[root@Router3 labeltest]# ./tunnel -m -p udp/6000 -d 10.4.0.2/32 -l100
LSPID:100
[root@Router3 labeltest]# ./tunnel -m -p udp/6001 -d 10.4.0.2/32 -l200
LSPID:200
```

Figura 32. Comando para submeter um tráfego de port específico sob um LSP

Desta forma, o resultado de um *traceroute* entre os computadores 6 e 11, volta à apresentar o trajeto através dos computadores 4 e 5 pois a alteração do custo OSPF entre os computadores 2 e 3 realizada na experiência 4 ainda estava presente e o comando que submetia todo o tráfego pelo túnel 100 foi alterado para submeter apenas tráfego com port 6000.

```
ec2-06:~# traceroute 10.4.0.2
traceroute to 10.4.0.2 (10.4.0.2), 30 hops max, 38 byte packets
 1  10.2.0.1 (10.2.0.1)  2.837 ms  0.494 ms  0.354 ms
 2  * 10.3.0.18 (10.3.0.18)  1.012 ms  0.711 ms
 3  10.3.0.14 (10.3.0.14)  1.266 ms *  0.981 ms
 4  10.3.0.10 (10.3.0.10)  1.529 ms  1.244 ms  1.028 ms
 5  10.4.0.2 (10.4.0.2)  1.834 ms  1.623 ms  1.304 ms
```

Figura 33. Demonstração do trajeto do tráfego

O tráfego do protocolo UDP com port 6000 e 6001 apresentou-se nos túneis 100 e 200, respectivamente. A figura 34, porém, ilustra o tráfego unido, pois no enlace de rede entre os computadores 6 e 3 ele ainda não havia sido submetido ao túneis.

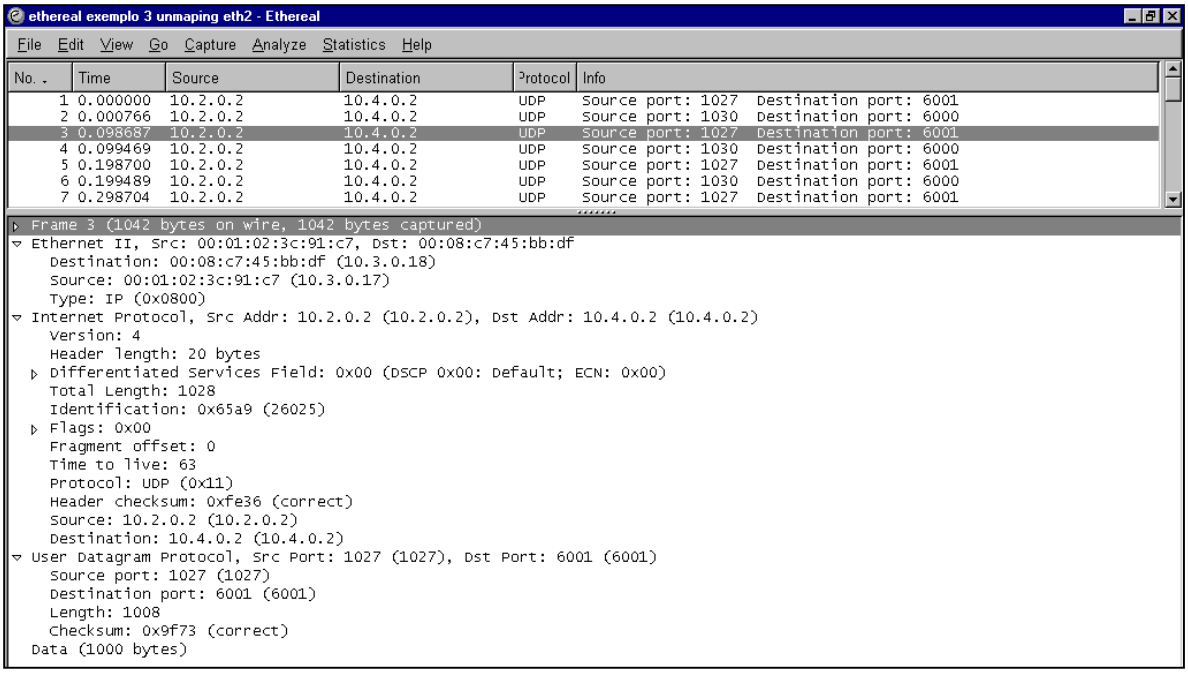


Figura 34. Tráfego de port 6000 e 6001 sem label

A figura 35, ilustra o tráfego no enlace de rede entre os computadores 3 e 2.

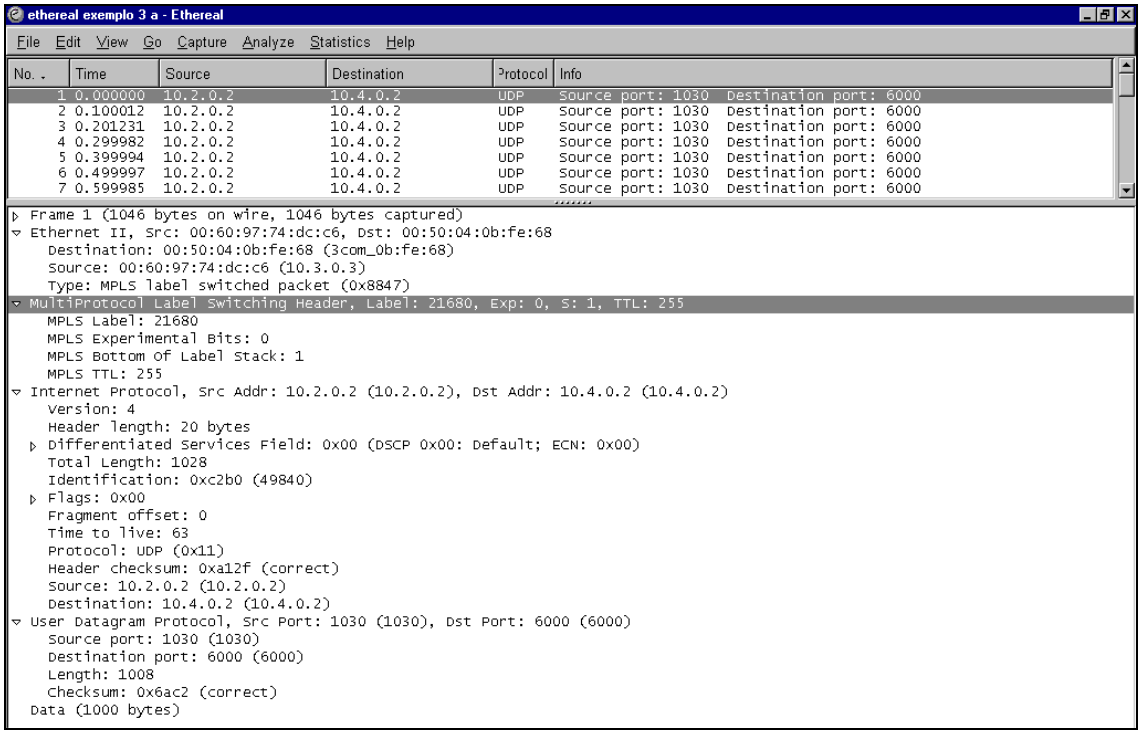


Figura 35. Tráfego de port 6000 submetido ao túnel 100

Observa-se que só há a presença do tráfego UPD 6000 com label MPLS, pois ele foi alocado ao túnel 100 que percorre o trajeto entre os computadores 3 e 10 através do computador 2.

A figura 36, ilustra o tráfego no enlace de rede entre os computadores 3 e 4. Observa-se que só há a presença do tráfego UPD 6001 com label MPLS, pois ele foi alocado ao túnel 200 que percorre o trajeto entre os computadores 3 e 10 através dos computadores 4 e 5.

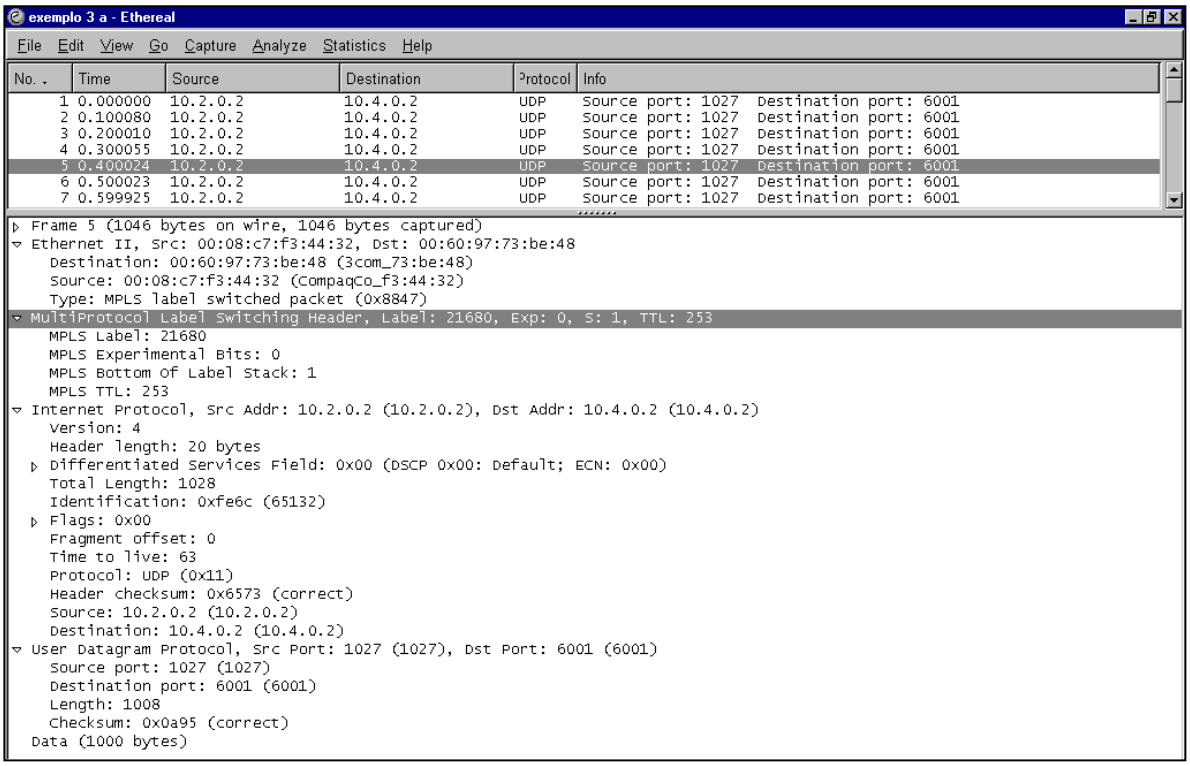


Figura 36. Tráfego de port 6001 submetido ao túnel 200

Da mesma forma que um tráfego UDP com port 6000 foi alocado a um LSP, um tráfego IP com campo DSCP configurado também poderia ser. Essa operação é realizada quando se deseja reservar banda e enviar o tráfego de classe especial por um trajeto específico.

O pacote MPLS pode ainda ser configurado para possibilitar priorização de pacotes MPLS sobre outros pacotes MPLS, através da marcação do campo Experimental Bits de seu cabeçalho. O item 3.1, Aplicações com MPLS fornece maiores detalhes.

Para retornar todo tráfego IP ao trajeto original, os comandos da figura 32, tiveram a opção "-m" substituída por "-u", a fim de retirar o tráfego do LSP, e a alteração do custo no enlace entre os computadores 2 e 3 foi desfeita, retornando o comportamento do tráfego entre o computador 6 e 11 para seu trajeto normal, Figura 37.

```
ec2-06:~# traceroute 10.4.0.2

traceroute to 10.4.0.2 (10.4.0.2), 30 hops max, 38 byte packets
 1  10.2.0.1 (10.2.0.1)  0.643 ms  0.688 ms  0.377 ms
 2  10.3.0.5 (10.3.0.5)  1.049 ms  0.862 ms  0.669 ms
 3  10.3.0.2 (10.3.0.2)  1.214 ms  1.138 ms  0.911 ms
 4  10.4.0.2 (10.4.0.2)  1.460 ms  1.233 ms  1.042 ms
ec2-06:~#
```

Figura 37. Demonstração III do trajeto do tráfego

5.5 Considerações Parciais

Demonstrou-se que a engenharia de tráfego com MPLS conseguiu alterar o sentido de todo o tráfego e de uma aplicação específica, representada por *port* diferente, independente das decisões do protocolo de roteamento OSPF. Sabe-se inclusive, que o mesmo poderia ter sido feito em função do endereço IP destino, tipo de protocolo e campo DSCP através das opções do comando "/tunnel", apresentado na Experiência 5.

A engenharia de tráfego com alterações das métricas do OSPF, por outro lado, conseguiu alterar todo tráfego ou permitiu um balanceamento de carga entre o número de rotas disponíveis.

Contudo, devido as redes atualmente trafegarem aplicações com requisitos de desempenho bem contrastantes, como Voz sobre IP e as provenientes de *backup* de informações em DataCenter, por exemplo, os provedores de serviço necessitam de uma engenharia de tráfego com ferramentas de controle granular, como as proporcionadas pelo MPLS, para otimizarem seus recursos e obterem maior retorno financeiro pelo que já foi investido, sem contudo, comprometer os compromissos assumidos com seus clientes através de *Service Level Agreement* (SLA) e sem apresentarem custos elevados de operação, para continuarem competitivos em preço no mercado que atuam.

Do ponto de vista didático, as realizações das experiências proporcionaram um contato prático com protocolo de roteamento e seu processo de configuração, obtenção das redes vizinhas e eleição das rotas de melhor métrica, mas principalmente, proporcionaram contato com o estabelecimento de túneis LSP, configuração dos parâmetros de label e controle do tráfego. Desta forma, o conceito de engenharia de tráfego, suas vantagens e características puderam ser melhor apresentadas, compreendidas e formatados em um procedimento de aula.

6 Conclusão

6.1 Considerações Finais

A engenharia de tráfego é realizada de forma mais eficiente com MPLS do que através da alteração das métricas do protocolo de roteamento OSPF devido a possibilidade de determinação específica do trajeto do tráfego, reserva de banda, opção de rápida recuperação a falhas e alteração do roteamento em função de variáveis como endereço destino, tipo de tráfego, interface de entrada e prioridade.

Por outro lado, sua implementação e operação são mais complexas devido a grande quantidade de configurações e protocolos. Contudo, a exigência por serviços de transporte de pacotes IP com qualidade de serviço, como VoIP por exemplo, competitividade por preços baixos e alta disponibilidade requeridas pelos clientes leva os provedores de serviço a encontrarem no MPLS uma arquitetura capaz de atender estas exigências.

O protocolo IPv6 pode ser desenvolvimento para apresentar variáveis próprias de configuração eficiente de engenharia de tráfego, pois possui condições suficientes para incorporar esta característica. O OSPFv3 com extensões para engenharia de tráfego, apresenta suporte a IPv6, mas permanece com a mesma forma de eleição de rotas, o que indica a continuidade da técnica de alteração das métricas ou utilização de outras técnicas se o objetivo for obter engenharia de tráfego.

É possível implementar MPLS e realizar experiências com engenharia de tráfego em computadores com sistema operacional Linux para fins didáticos. A experimentação demonstrou o modo do MPLS de controlar o tráfego, e a possibilidade de levar alunos a praticarem configurações e análise de funcionamento do OSPF e de roteadores MPLS.

A implementação da parte prática deste trabalho demonstrou também que a operação de um computador Linux para rotear pacotes se assemelha a um roteador tradicional em termos didáticos, pois permite alterações no mecanismo de encaminhamento de pacotes, através do kernel, como a possibilidade de configuração de balanceamento de carga.

6.2 Trabalhos Futuros

A realização desta dissertação despertou a possibilidade de aprofundamento de estudo nos seguintes temas:

- **Engenharia de tráfego com IPv6**

O protocolo IPv6 poderia apresentar meios de realizar engenharia de tráfego sem depender de outros protocolos, através da utilização de parte dos 20 bits do campo

do cabeçalho *Flow Label.* Por isso, poderia ser desenvolvida uma proposta de utilização e regras.

- **Automatização da Engenharia de tráfego com MPLS**

Com o objetivo de tornar as decisões de alteração do trajeto do tráfego automáticas e pró-ativas a alterações na rede, um sistema computacional poderia capturar informações de estado da rede em tempo real e utilizar um banco de dados para tomar decisões de engenharia de tráfego sem interferência humana.

Informações como elementos da rede existentes e requisitos de qualidade de serviço de cada aplicação, com origem e destino configurados, fariam parte deste banco de dados.

- **Estudo do MPLS como arquitetura de integração e coexistência de redes IPv4 e IPv6.**

A arquitetura MPLS permite o aprofundamento de estudo em várias vertentes. Dentre elas, sua aplicação durante a integração e coexistência de redes IPv4 e IPv6 é uma das mais interessantes. Portanto, poderia ser realizado um estudo de aplicação teórico e prático, também através de Linux.

- **Experiências de engenharia de tráfego com alteração da métrica TOS do OSPF.**

Este trabalho abordou a alteração da métrica banda no protocolo de roteamento OSPF. Como ampliação, experiências de engenharia de tráfego podem ser feitas com alteração da métrica TOS (*Type of Service*) do OSPF. Além disso, outras métricas como, por exemplo, atraso, quantidade de *hops* e carga de utilização do link podem ser usados caso outros protocolos de roteamento sejam estudados.

6.3 Dificuldades Encontradas

A arquitetura MPLS é aplicada em núcleo de médias e grandes redes de roteadores, portanto, realizar implementações com MPLS em laboratório sem utilização de nenhum equipamento proprietário é um desafio.

O projeto RSVP-TE Daemon (INTEC, 2004) possibilitou a implementação de MPLS com engenharia de tráfego em computadores com Linux. Contudo, erros de código e procedimentos incompletos de compilação do kernel e configuração do software, consumiram dezenas de horas para instalação de uma única máquina, até que se atualizasse o procedimento de instalação e o adaptasse a versão 8.0 do RedHat. Esse procedimento encontra-se no Anexo B.

Além disso, a lista de discussão deste projeto não possuía movimentação há algum tempo o que impossibilitou a solução de *bugs* encontrados durante a tentativa de ativação de reserva de banda e fast-reroute de um LSP que o Daemon possui.

De qualquer forma, foi possível a demonstração das características de engenharia de tráfego planejadas.

Bibliografia

ANDERSSON, L. et al. **RFC 3036**: LDP Specification. IETF, jan. 2001. Disponível em: <ftp://ftp.rfc-editor.org/in-notes/rfc3036.txt>, data de acesso: 09/03/2004.

AWDUCHE, D. et al. **RFC 3209**: RSVP-TE: extensions to RSVP for LSP tunnels. IETF, abr. 1998. Disponível em: <ftp://ftp.rfc-editor.org/in-notes/rfc3209.txt >, data de acesso: 12/03/2004.

AWDUCHE, D. et al. **RFC 2702**: Requirements for traffic engineering over MPLS. IETF, set. 1999. Disponível em: <ftp://ftp.rfc-editor.org/in-notes/rfc2702.txt >, data de acesso: 17/02/2004.

AWDUCHE, D.; HANNAN, A.;XIAO, X. **RFC 3210**: Applicability statement for extensions to RSVP for LSP-Tunnels. IETF, dez. 2001. Disponível em: <ftp://ftp.rfc-editor.org/in-nots/rfc3210.txt>, data de acesso: 18/02/2004.

AWDUCHE, D. et al. **RFC 3630**: RSVP-TE: Extensions to RSVP for LSP Tunnels. IETF, dez. 2001. Disponível em: <ftp://ftp.rfc-editor.org/in-notes/rfc3630.txt >, data de acesso: 25/02/2004.

AWDUCHE, D. et al. **RFC 3272**: Overview and principles of internet traffic engineering. IETF, maio 2002. Disponível em: <ftp://ftp.rfc-editor.org/in-notes/rfc3272.txt >, data de acesso: 17/04/2004.

BANERJEE, G. SIDHU, D. Comparative analysis of path computation techniques for MPLS traffic engineering. **Computer Networks**, p. 149-165, n.40, set. 2002.

BLANCHY, F. MÉLON, L.; LEDUC, G. Decentralized local backup LSP calculation with efficient bandwidth sharing. **IEEE** INTERNATIONAL CONFERENCE ON TELECOMMUNICATIONS, 10., fev. 2003, Papeete. **Proceedings**… Papeete: IEEE Press, p.253-260, 2003. Disponível em: <ftp://ftp.run.montefiore.ulg.ac.be/pub/RUN-PP03-02.pdf>, data de acesso: 27/03/2004.

BOYLE, J. et al. **RFC 3346**. Applicability Statement for Traffic Engineering with MPLS. IETF**,** ago. 2002. Disponível em: <ftp://ftp.rfc-editor.org/in-notes/rfc3346.txt >, data de acesso: 11/11/2003.

BRADEN, R. et al. **RFC 2205**: Resource ReSerVation Protocol - RSVP. IETF, set. 1997. Disponível em: <ftp://ftp.rfc-editor.org/in-notes/rfc2205.txt >, data de acesso: 20/11/2003.

BRYANT, S. PATE, P. **RFC3985**: Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture. IETF, mar. 2005. Disponível em <ftp://ftp.rfc-editor.org/in-notes/rfc3985.txt >, data de acesso: 02/08/2005.

CHORWDHURY, D. **Unified IP Internetworking.** New York, Springer-Verlag ed., 2001.

COLTUN, R. et al. **RFC 2370**: The OSPF Opaque LSA Option. IETF, jul. 1998. Disponível em: <ftp://ftp.rfc-editor.org/in-notes/rfc2370.txt>, data de acesso: 19/05/2003.

COLTUN, R. FERGUNSON, D. MOY, J. **RFC2740.** OSPF for IPv6.IETF, dez. 1999. Disponível em: <ftp://ftp.rfc-editor.org/in-notes/rfc2740.txt>, data de acesso: 19/12/2004.

DEERING, S. HINDEN, R. **RFC 2460**: Internet Protocol, Version 6 (IPv6) Specification. IETF, dez. 1998. Disponível em: <ftp://ftp.rfc-editor.org/in-notes/rfc2460.txt >, data de acesso: 01/06/2004.

EL-HAWARY, M. F.; EL-DERINI, M. N.; H. H. ALY , H. **Egypt heuristics for rerouting of label switched paths in MPLS based IP networks**. Alexandria University, Egito, julho 2003. Disponível em: <http://csdl.computer.org/comp/proceedings/iscc/2003/1961/00/19610957abs.htm>, data de acesso: 15/06/2004.

FINEBERG, V. **QoS Support in MPLS Networks**. MPLS/Frame Relay Alliance Forum, maio 2003. Disponível em: <http://www.mplsforum.org>, data de acesso em: 10/05/2004

FORTZ, B; REXFORD, J.; THORUP, M. **Traffic engineering with traditional routing protocols**. IEEE COMMUNICATION MAGAZINE, 40 (10), 2002. Disponível em: <http://www.research.att.com/~jrex/papers/ieeecomm02.pdf >, data de acesso: 07/08/2005.

GNV **ZEBRA**. Software de roteamento: Zebra. Disponível em: www.zebra.org., data de acesso: 07/11/2004. Distribuição gratuita.

GRAY, E. **MPLS: Implementing the Technology.** Boston, Addison-Wesley, 2001.

RAMAKRISHNAN, H. FLOYD, S. BLACK, D. **RFC 3168**: The Addition of Explicit Congestion Notification (ECN) to IP. IETF, sep.2001. Disponível em: <ftp://ftp.rfc-editor.org/in-notes/rfc3168.txt >, data de acesso: 10/08/2005.

HEAVY READING. Survey of carrier attitudes toward IP/MPLS backbones and VPN. **Heavy Reading Report**, v.2, n.4, jan. 2004. 40p.

HöKELEK, I. **Multipath based traffic engineering in MPLS networks**. Bilkent University. Sep., 2002.

INFORMATION SCIENCE INSTITUTE. **RFC 791**: Internet protocol. IETF, set. 1981. Disponível em: <ftp://ftp.rfc-editor.org/in-notes/rfc791.txt>, data de acesso: 13/04/2004.

INTEC / GHENT UNIVERSITY /IMEC. **RSVP-TE daemon for TE for DiffServ over MPLS under Linux**, 2002. Projeto Disponível em: <http://dsmpls.atlantis.rug.ac.be.>, data de acesso: 05/05/2004.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Open Systems Interconnection. **ISO 8602**. 1987. Disponível em: <www.isso.org/isso/em/cataloguelistpage> , data de acesso: 03/05/2004.

ISI. **Project Home Page.** Information Sciences Institute, março, 1999. Disponível em http://www.isi.edu/div7/rsvp, data do acesso: 03/05/2004.

JAMOUSSI, B. **RFC 3212**: Constraint-Based LSP Setup using LDP. IETF, jan. 2002. Disponível em: <ftp://ftp.rfc-editor.org/in-notes/rfc3212.txt>, data de acesso: 04/05/2004

KATZ, D.; YEUNG. D.; KOMPELLA, K. **RFC 3630**: Traffic Engineering Extensions To OSPF. RFC 3630. IETF, set. de 2003. Disponível em: <ftp://ftp.rfc-editor.org/in-notes/rfc3630.txt>, data de acesso: 11/11/2003.

LAURENCE, J.; LADAM, M. Network Protection and MPLS Path Recovery **Stratecast Partners**, v.3, n.4, p.11-12 , mar. 2003.

LE ROUX, J.L.; VASSEUR, J.P.; BOYLE, J. **RFC 4105** Requirements for Inter-area MPLS traffic engineering. IETF, 2005. Disponível em: <: <ftp://ftp.rfc-editor.org/in-notes/rfc4105.txt >, data de acesso: 20/08/2005.

MANNER, J. **JTG Generator.** Página do projeto. University of Helsinki. Site disponível em <www.cs.helsinki.fi/u/jmanner/>, data do acesso, 10/05/05.

MACRE-CRANE, B., MAKAM, S.; OWENS, K. **RFC 3469**: framework for multi-protocol label switching (MPLS)-based recovery. IETF, fev. 2003. Disponível em: <ftp://ftp.rfc-editor.org/in-notes/rfc3469.txt>, data de acesso: 21/01/2004.

MICHELL, K. Service Provider Plans for IP, MPLS, and ATM Networks, North America and Europe 2003. **Infonetics Research** , Disponível em: <www.channelminds.com/article.php3?id_article=1374>, data de acesso: 14/06/2004.

MORTIER, R. **Internet Traffic Engineering**. Dissertação para obtenção do grau de doutor em Filosofia na Universidade de Cambridge, Churchill College, p.26, abr. 2002.

MOY, J. **RFC 2328**: OSPF. IETF, v.2, abr. 1998. Disponível em: <ftp://ftp.rfc-editor.org/in-notes/rfc2328.txt>, data de acesso: 19/05/2004.

MPLS AND FRAME RELAY ALLIANCE. **Workgroup Home Page**. Site disponível em <www.mplsforum.org>, data de acesso: 27/07/2004

NS2. **Network Simulator 2**. Página do projeto disponível em: <www.isi.edu/nsnam/ns>, data de acesso: 18/05/2004.

NIST, 2000. **Projetc Home Page**. National Institute of standards and technology. Software livre disponível em http://snad.ncsl.nist.gov/nistswitch/, data do acesso: 03/05/2004.

OSBORNE, E., SIMHA, A. **Traffic Engineering with MPLS**. Indianapolis, Cisco press, 2002.

RHK. **Renewed Focus on Profitability Bodes Well for Deployment of MPLS in Traffic Engineering.** RHK Telecommunications Industry Analysis, Insight, jan, 2002.

ROSEN, E., VISWANATHAN, A.; CALLON, R. **RFC 3031**: Multiprotocol label switching architecture. IETF, jan. 2001. Disponível em: <ftp://ftp.rfc-editor.org/in-notes/rfc3031.txt>, data de acesso: 26/01/2004.

SRIDHARAN, A.; GUÉRIN, R.; DIOT, C. **Achieving Near-Optimal Traffic Engineering Solutions for Current OSPF/IS-IS Networks**. Dept. of Elec. Eng., Univ. of Pennsylvania, Philadelphia, 2003.

SMIT, H. T. Li. **RFC 3784:** ISIS Extensions for Traffic Engineering. IETF, jun. 2004. Disponível em: <ftp://ftp.rfc-editor.org/in-notes/rfc3784.txt>, data de acesso: 06/12/2003.

SOURCEFORGE. **MPLS-Linux**. Disponível em: <http://mpls-linux.sourceforge.net>, data de acesso: 03/06/2004

SWALLOW, G. MPLS Advantages for Traffic Engineering. **IEEE Communications Magazine**, p.54-57, dez. 1999.

SWALLOW, G.; PAN, P.; ATLAS, A. **(draft-lsp-fastrerote):** Draft-ietf-mpls-rsvp-lsp-fastreroute-05. IETF, maio 2004. Disponível em: <http://www.ietf.org/internet-drafts/draft-ietf-mpls-rsvp-lsp-fastreroute-05.txt>, data de acesso: 05/05/2004.

TEQUILA. **Project Home Page,** January, 2002. Disponível em: www.ist-tequila.org; data do acesso: 10/04/2005.

ZEBRA, 2004. **Software Home Page,** abril, 2003. Disponível em <http://www.zebra.org>, data do acesso 12/12/2003.

ZHANG, R.; VASSEUR, JP. **(draft-ietf-interas-mpls-te)** MPLS inter-AS traffic engineering requirements. IETF, 2004. Disponível em: <http://www.ietf.org/internet-drafts/draft-ietf-tewg-interas-mpls-te-req-06.txt>, data de acesso: 20/08/2005.

WONG, S. **The on line and offline Properties of Routing Algorithms in MPLS.** University of Toronto. July, 2002.

Glossário

O glossário a seguir apresenta o significado de alguns termos nesta dissertação.

Buffer - Área de memória responsável por armazenar temporariamente pacotes IP.

Constraint-based routing - Roteamento baseado em restrições.

Crossover - Cabo *Ethernet* que encaminha o sinal de transmissão do pino de uma das pontas do conector para os pinos de recepção da outra ponta e vice-versa com os pinos de recepção. Ele pode ser usado para conectar duas placas de rede, por exemplo.

Daemon - É um programa de computador que funciona sem intervenção humana, com o objetivo de realizar uma tarefa específica.

Downstream on demand label distribution - Distribuição de label por demanda.

Explicit routing - Roteamento explícito.

Fast-reroute - Característica de reação a falhas de links e nós do RSVP-TE.

Fixed explicit - Tipo de estabelecimento de LSP do RSVP-TE que indica túnel de trajeto único e fixo.

Flow label - Campo disponível no cabeçalho do protocolo IPv6 para requisição de QoS.

FreeBSD - É um sistema operacional descendente do Unix com código fonte aberto e livre de licenças. Ele funciona em computadores com processadores Intel x86, UltraSPARC e AMD64.

Hop by hop routing - Escolha de rota para encaminhamento do pacote IP realizada independentemente em cada nó.

Jitter - Variação do atraso no recebimento de uma quantidade de pacotes IP.

Kernel - Série de programas em linguagem C e Assembly que constituem o núcleo do sistema operacional de um computador.

Label - Rótulo que é adicionado a cada pacote que entra em uma rede configurada com arquitetura MPLS.

Link - Enlace de interligação de dois nós de rede.

Looping - Trajeto de um LSP quando passa pelo mesmo nó duas vezes.

Loose source - Campo do cabeçalho do IPv4 para definição de roteamento livre.

Make before break - Característica de um LSP, que se estabelece por dois caminhos diferentes, um principal, que recebe tráfego e o secundário que permanece vazio. Ao primeiro sinal de falha encontrado ao longo do caminho principal, todo o tráfego é encaminhado para o LSP secundário.

Patch - É uma atualização de software para corrigir problemas em um programa de computador ou melhorar sua apresentação e performance.

Path - Trajeto de um LSP em uma rede.

Requisitos de roteamento - Exigências de banda mínima, nós obrigatórios ou proibidos no trajeto de um LSP e características de recuperação a falhas de rede,

Routing Header - Campo do cabeçalho do IPv6 que permite que um ou mais nós intermediários sejam alcançados numa seqüência predefinida no trajeto do pacote até seu destino.

Shared explicit - Tipo de estabelecimento de LSP do RSVP-TE que permite que dois túneis com mesma origem e destino se formem por caminhos diferentes.

Soft State protocol - Protocolo com a característica de verificação periódica do estado de estabelecimento de suas conexões.

Anexo A

Experiências de engenharia de tráfego: procedimento de laboratório

Experiências de engenharia de tráfego: procedimento de laboratório

Assunto: MPLS

v2.0

Objetivo: Estudar MPLS e suas aplicações de forma prática, através da implementação de RSVP-TE e OSPF em computadores com Linux, distribuição RedHat 8.0.

Introdução:

A figura, Topologia de laboratório, apresentada no final deste procedimento, pretende amostrar uma rede de provedor de serviços de comunicação. Por isso, apresenta computadores, representando roteadores, de centro de rede (Core), de fronteira com o cliente e propriamente o cliente. Há diversos caminhos para interligação dos nós e endereçamento de rede nos enlaces com mascará 255.255.255.252 (/30), assim como em redes reais, para evitar o desperdício de endereçamento.

A demonstração de protocolos de redes MAN e WAN em laboratório, apresenta dificuldades de realização devido a dificuldade de obtenção dos equipamentos e meios de interligação. Entretanto, com daemons que permitem que computadores com sistema operacional Linux implementem protocolos de redes MPLS, essa arquitetura pode ser demonstrada e estudada em laboratório com computadores. A idéia é válida, pois, redes MPLS são também empregadas em redes MAN Gigabit Ethernet, por isso um laboratório de computadores interligados com interfaces Ethernet e FastEthernet se aproxima do real.

Parte Prática:

1º Parte - Configurando a rede

1) Inicie seu computador na partição Red Hat 8.0 onde o daemon RSVP-TE e Zebra se encontram instalados. Inicie o modo gráfico para melhor gerenciamento das janelas de terminal e utilização do sniffer Ethereal.

Os computadores classificados como *Customer Edge* (CE) podem funcionar em qualquer sistema operacional.

2) Descubra o número de seu computador e localize-o na topologia de rede anexado a este procedimento.

3) Configure os endereços IP nas interfaces correspondentes, conforme topologia. As interfaces não utilizadas devem ser desabilitadas.

4) Nos computadores CE, nº 11, por exemplo, adicione uma rota default para a interface diretamente conectada ao PE (Provider Edge).

5) Teste a conexão com o computador vizinho.

6) Permita que seu computador realize encaminhamento de pacotes entre as interfaces, digitando o comando: echo 1 > /proc/sys/net/ipv4/ip_forward.

Os clientes, representados pelos computadores CE, devem desconhecer qualquer configuração MPLS, no máximo, marcar o campo DSCP para que sejam priorizados na rede. Por isso, os computadores CE não terão as próximas etapas de configuração. Porém, serão usados para gerar tráfego e estudarmos as alterações ocorridas na rede MPLS.

2º Parte - Configurando Zebra

O Zebra é um software livre que gerencia protocolos de roteamento TCP/IP de forma modular. Entre os protocolos válidos estão RIPv2, BGP-4, OSPFv2 e IS-IS. Todo seu desenvolvimento é baseado em RFC do IETF e por isso tem interoperabilidade com roteadores comerciais.

1) Inicie digitando "zebra";

2) Em outra janela de terminal ou na mesma, digitando (Shift+Ctrl+T), realize um telnet para seu próprio computador com port 2601: telnet localhost 2601

3) Programe os endereços IP em cada interface no Zebra e a banda do link . Para isso, entre com a senha de visualização "zebra". Entre em modo privilegiado digitando "enable" e novamente "zebra". Entre em modo de configuração com comando "configure terminal" e em seguida, digitando "interface eth0". Insira o endereço ip desta interface digitando, "ip address X.X.X.X/Y" (onde X e Y estão no diagrama anexado). E então, entre com "bandwidth 10000".

O protocolo OSPF, como você sabe, escolhe rotas para o destino de acordo com o menor custo a partir da origem. A composição deste custo é baseado no tamanho da banda total do link. Portanto, declarando bandwidth 10000, estamos nivelando as interfaces Ethernet e FastEthernet dos computadores do lab. Em redes MPLS com aplicação em engenharia de tráfego (MPLS-TE), o OSPF, estendido para engenharia de tráfego (OSPF-TE), distribui entre nós participantes, além das rotas e custo, a taxa de ocupação e reserva da banda por classe de tráfego.

1) Digite "exit" e entre nas outras interfaces que deverão ser configuradas.

2) Ao final, digite "end" confira as configurações com show run e salve com "wr".

3) Verifique suas rotas com "show ip route".

3º Parte - Configurando OSPF

1) Inicie digitando "ospfd";

2) Em outra janela de terminal, realize um telnet para seu próprio computador com port 2604: telnet localhost 2604

3) Configure a rede IP da área OSPF zero, que deve compreender todas os enlaces dessa área, digitando em modo de configuração, "router ospf", em seguida, "network 10.3.0.0/24 area 0.0.0.0"

    3.1) Nos computadores 3 e 10, adicione também "redistribute conneted", a fim de redistribuir nos roteadores da área 0, as redes conectadas e não compreendidas através de "network X.X.X.X/24 area 0.0.0.0.

Em redes MPLS, há sempre um protocolo de roteamento IGP (Internal Gateway Protocol) responsável pelo levantamento da topologia da rede, pois os roteadores originadores do túnel devem ter a uma visão de todas as rotas e trajetos da rede.

1) Saia do modo de configuração e verifique sua tabela de roteamento com "show ip ospf route".

2) Realize traceroute para os computadores 3 e 10, analise o trajeto com reação ao diagrama e custos OSPF.

4º Parte - Iniciando RSVP-TE daemon

O RSVP-TE daemon trata-se de um aplicativo que possibilita o estabelecimento de túneis MPLS em trajetos predeterminados com ou sem reserva de banda, além de políticas de rápida recuperação a falhas. Redes MPLS com aplicações em VPN, utilizam-se de outro protocolo para requisição e alocação de labels, o Label Distribution Protocol (LDP). A principal diferença é que este aloca label a todas as rotas presentes no roteador, ao contrário do RSVP-TE, que aloca os labels por demanda, ou seja, a medida que os túneis são estabelecidos.

1) Inicie rsvpd em /home/rsvp/rsvpd/rsvpd com o comando ./rsvpd -D

2) Os computadores 3 e 11 deverão estabelecer dois túneis entre eles, cada um através por um caminho diferente.

Lembrando que túneis MPLS são unidirecionais, portanto devem ser estabelecidos dois túneis num mesmo trajeto para que o tráfego possa ser alocado nos dois sentidos.

3) Para estabelecer cada túnel, o *RSVP-TE Daemon* exige um terminal aberto no destino em /home/rsvp/rsvpd/labeltest/ e com o comando ./rapirecv_auto digitado e na origem, um terminal aberto em /home/rsvp/rsvpd/labeltest com o comando ./rtest2.

4) Assim que digitar ./rtest2 você será questionado pelo end. IP da interface de entrada no nó destino, a de saída na origem e o LSPID. Digite um por vez e tecle enter ao finalizar.

Label Switch Path (LSP) trata-se do túnel MPLS que o RSVP estabelecerá e o manterá ao longo da rede. LSPID trata-se do identificador ou label MPLS que designará o túnel.

5) Em seguida, você será questionado por nós intermediários, digite o end. da interface de entrada que o túnel utilizará, um por vez, de acordo com o trajeto para atingir o destino, ao terminar, digite 0.

6) 2.3 “Verifique o sucesso do estabelecimento dos túneis através do comando “./tunnel -L" realizado em /home/rsvp/rsvpd/labeltest em outra janela de terminal.

7) Os computadores intermediários poderão verificar as mensagens de sinalização do protocolo RSVP no terminal que foi habilitado o *RSVP-TE Daemon* e através do programa Ethereal, que pode ser iniciado através do menu de programas, System Tools.

Em Ethereal, selecione uma única interface de captura para melhor visualização.

8) Nos computadores 6 e 11, observe o trajeto do tráfego entre eles com traceroute, ele é determinado pelo protocolo de roteamento que escolhe a rota de menor custo. Ou observe nos computadores "P" com Ethereal, o trajeto de um tráfego ping, telnet <end. Ip destino> 2604 e ftp que você pode gerar.

Alocaremos os tráfego transmitidos pelos CE's, nos roteadores PE, ao túnel de maior trajeto. Desta forma, pretende-se observar que alteraremos o modo com que o tráfego é encaminhado ao longo da rede.

9) Sincronize com seus colegas de laboratório o momento de alocar o tráfego transmitido por 6 e 10 ao túnel de trajeto mais longo, e até então, não utilizado pelo OSPF, nos computadores 3 e 10 com o comando:

   ./tunnel -m -a -d <end. Ip destino> -L <nº do tunel>

10) Realize traceroute e compare o resultado com o da parte 3.

Observe que a quantidade de hops mudou. Qual a aplicação desta operação?

11) Retire a alocação de tráfego acima como o mesmo comando, mas com -u no lugar de -m, e experimente as seguintes possibilidades:

12) Alterando o campo EXP do protocolo MPLS:

./tunnel -m -a -d <end. Ip destino> -L<nº do tunel>/3

onde:

-m => map, -a => all, -d => dest., -L => LSPID, -u => unmap, -p => protocol

13) Qual a aplicação para este tipo de marcação do label?

14) Retire novamente a alocação acima repetindo o comando, mas substituindo -m por -u e aloque apenas um tipo de tráfego, como o ping por exemplo, a um túnel.

./tunnel -m -p icmp -d <end. Ip destino> -L<nº do tunel>/3

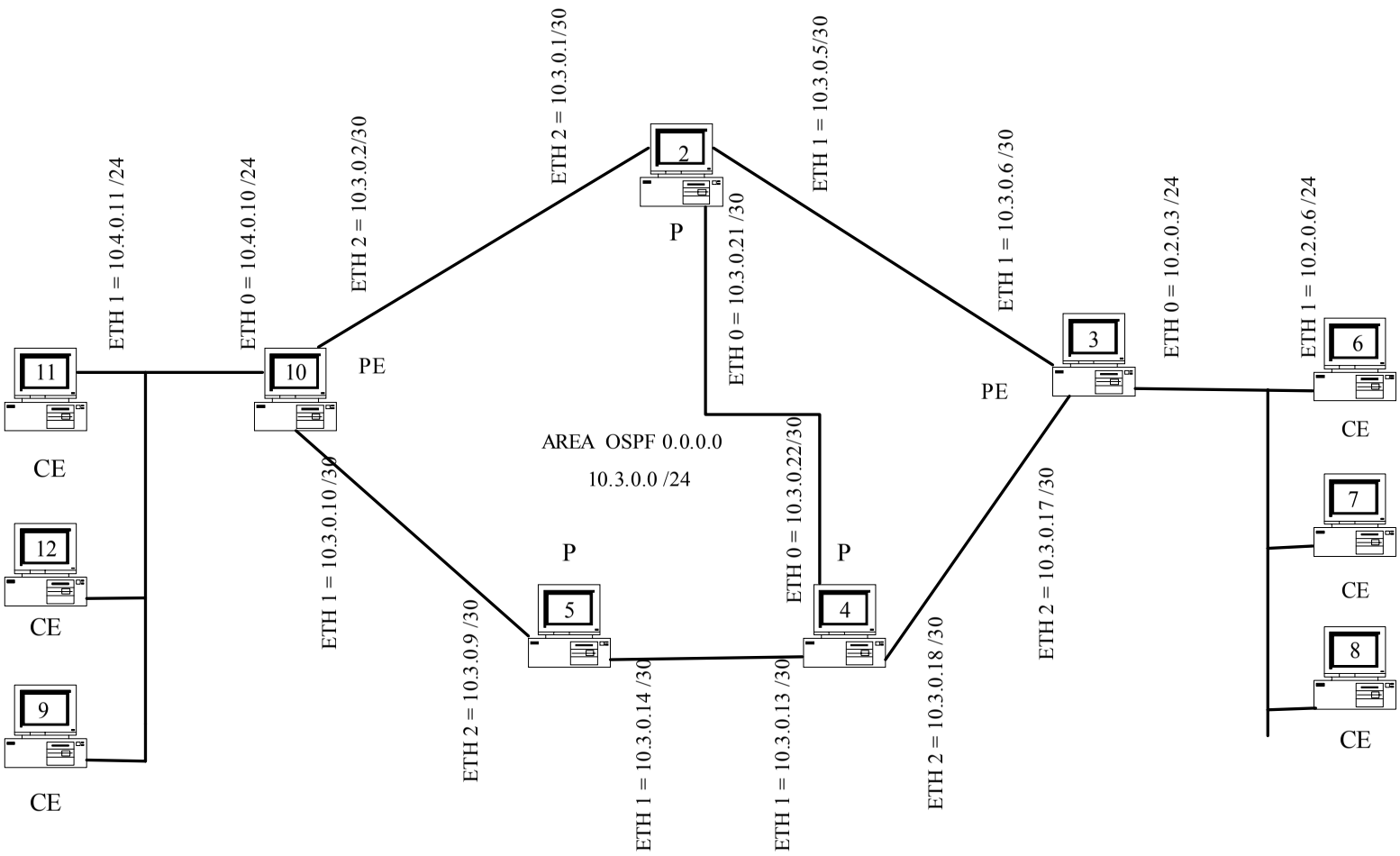
15)Qual a aplicação deste tipo de separação de tráfego?

Referências:

http://dsmpls.atlantis.ugent.be

http://www.zebra.org

http://sourceforge.net/projects/mpls-linux



Topologia de laboratório - TCP -IP
MPLS-TE

Anexo B

Procedimento de Instalação do RSVP-TE *Daemon*

Procedimento de Instalação do RSVP-TE daemon

Instalação do RSVP-TE daemon para DiffServ sobre MPLS em Linux.

Autores: Heuven, Pim Vam; Pierotti, Daniela; Zhou Bin 12/06/03

Corrigido e atualizado por Sérgio Polizer 01/07/05

Pacotes necessários:

RedHat 8.0

www.hedhat.com

Linux-2.4.19.tar.bz2

http://ftp.kernel.org/pub/linux/kernel/v2.4/linux-2.4.19.tar.bz2

KERNEL_2.4.19_MPLS172.patch

http://dsmpls.atlantis.ugent.be/files/KERNEL_2.4.19_MPLS172.patch

iptables-1.2.4-0.2-dscp.tgz

http://dsmpls.atlantis.ugent.be/files/iptables-1.2.4-0.2-dscp.tgz

DSMPLS+IP.patch

http://dsmpls.atlantis.ugent.be/files/DSMPLS+IP.patch

iproute2-current.tar.gz

http://ftp.cdut.edu.cn/pub/linux/new/iproute2-current.tar.gz

rsvpd.0.70-rc2.tgz

http://dsmpls.atlantis.ugent.be/files/rsvpd.0.70-rc2.tgz

iproute2_rsvpd.0.60.patch

http://dsmpls.atlantis.ugent.be/files/IPROUTE2_rsvpd0.60.patch

Procedimento:

Nota: "edit" é um termo genérico para qualquer editor (vi, pico, gedit, etc.)

1. Preparação:

Instalação do Linux Kernel:

- A localização do kernel deverá ser /usr/src/linux-2.4.19. Por isso, uma cópia do kernel 2.4.19 (linux-2.4.19.tar.bz2) deverá ser copiada para o diretório /usr/src/. Este será o ponto de partida para as próximas operações.

- Caso este diretório contenha um link simbólico para um antigo kernel, retire este link.

- Descomprima o kernel com:

~ /usr/src> tar -xjvf linux-2.4.19.tar.bz2

- Em seguida, entre no diretório criado e gere a dependência de links:

~ cd linux-2.4.19

~ make oldconfig (ou make xconfig ou make menuconfig).

2. Adicionado o patch MPLS:

- Mova KERNEL_2.4.19_MPLS172.patch para o diretório /usr/src e digite o comando:

~ /usr/src/linux-2.4.19> patch -p1 < ../KERNEL_2.4.19_MPLS172.patch

3. Adicionando o patch DSMPLS+IP:

- Mova DSMPLS+IP para o diretório /usr/src e digite o comando:

~ /usr/src/linux-2.4.19> patch -p0 < ../DSMPLS+IP.patch

4. Instalação de iptable-1.2.4:

- Crie a pasta rsvp, com ~mkdir rsvp

- Mova iptables-1.2.4-0.2-dscp.tgz para o diretório /home/rsvp/ e descomprima-o:

~ /home/rsvp> tar -zxvf iptables-1.2.4-0.2-dscp.tgz

- Enter no diretório iptables-1.2.4-dscp e faça:

~ /home/rsvp/iptables-1.2.4-dscp> make patch-o-matic

Caso seja questionado por patches a serem instalados, opte apenas por "dscp.patch" e "ftos.patch". Depois da confirmação, de ftos.patch, escolha 'q' para sair de patch-o-matic.

- Em seguida, compile e instale:

~ /home/rsvp/iptables-1.2.4-dscp> make

~ /home/rsvp/iptables-1.2.4-dscp> make install

5. Instalação do kernel do linux:

- Para configurar o kernel, entre em /usr/src/linux-2.4.19 e digite:

~ /usr/src/linux-2.4.19>make menuconfig (ou make xconfig or make config ou se houver um .config: make oldconfig)

Compile o kernel com as seguintes opções de no item "Networking":

- Enable Prompt for development and/or incomplete code/drivers
- Em Networking Options:
- Network packet filtering
- TCP/IP networking
- Advanced router
- Policy routing
- Use netfilter MARK value as routing key
- MPLS support
- Netfilter Configuration (em Networking options)
- IP tables support (habilite todas as subseções. Certifique-se que "DSCP match" and "MPLS target" estão presentes, caso contrário refaça o item 2.)
- QoS and/or fair queuing (habilite todas as subseções).
- Network Device Options (Habillite os drives de placas de rede existentes no computador)

- Edite o arquivo mpls_in_info.c em /usr/src/linux-2.4.19/net/mpls/, acrescentando uma chave "}" de fechamento na última linha do arquivo.

- Compile e instale o kernel:

~ /usr/src/linux-2.4.19>make dep && make clean && make bzImage && make modules && make modules_install

- Mova o novo arquivo bzImage and System.map para o diretório /boot e crie o novo link simbólico para System.map:

~ /usr/src/linux-2.4.19>cp arch/i386/boot/bzImage /boot/vmlinuz-2.4.19

~ /usr/src/linux-2.4.19>cp System.map /boot/System.map-2.4.19

[Opcional]

~ /usr/src/linux>cd /boot

~ /boot>rm vmlinuz

~ /boot>ln -s vmlinuz-2.4.19 vmlinuz

~ /boot>rm System.map

~ /boot>ln -s System.map-2.4.19 System.map

[/Opcional]

- Edit o "Grub", se desejar que o computador inicie no novo kernel toda vez que entrar na partição do RedHat.

- Check o kernel:

#dmesg | grep -i mpls

6. Instalação de iproute2:

- Descomprima e aplique os seguintes patches:

~ /home>tar -zxvf iproute2-current.tar.gz

~ /home>patch -p0 < iproute2_rsvpd.0.60.patch

~ /home>cd iproute2

- Habilite diffserv:

~ /home/iproute2>edit Config

Substitua-a 'n' por 'y' na linha para diffserv , mas deixe 'n' para ATM. Salve e saia.

- Atualize o diretório de compilação do arquivo Make:

~ edit Makefile

Altere a 5º linha para KERNEL_INCLUDE=/usr/src/linux-2.4.19/include

- Compile.

~ /home/iproute2>make clean

~ /home/iproute2>make

- Copie o diretório ip para /sbin e tc para /usr/local/bin

~ /home/iproute2>cd ip

~ /home/iproute2/ip>cp ip /sbin

~ /home/iproute2/ip>cd ../tc

~ /home/iproute2/tc>cp tc /usr/local/bin

7. Instalação de RSVP-TE:

- Recomenda-se:

~cd /usr/include/

~mv linux linux.old

~ln -s /usr/src/linux-2.4.19/include/linux linux

check that:

#ls -ld /usr/include/linux

lrwxrwxrwx 1 root root 28 Nov 21 18:14 /usr/include/linux

-> /usr/src/linux-2.4.19/include/linux

- Coloque o arquivo rsvpd.0.70-rc2.tgz em /home/rsvp e execute com o comando:

~ /home/rsvp> tar -zxvf rsvpd.0.70-rc2.tgz

~ /home/rsvp> cd rsvpd

- Agora compile:

~ /home/rsvp/rsvpd>make clean

~ /home/rsvp/rsvpd>make

O daemon esta compilado e pode ser encontrado no diretório /home/rsvp/rsvpd/rsvpd. As ferramentas estão no /home/rsvp/rsvpd/labeltest.

- Copie o executável mplsadm de /home/rsvp/rsvpd/labeltest para /usr/local/bin:

~ cp labeltest/mplsadm /usr/local/bin

- Antes de iniciar o daemon faça:

~ /home/rsvp/rsvpd>edit label.conf

-Compare os nomes das interfaces com os nomes correspondentes no seu computador, altere se necessário e salve em /etc/label.conf.

~ /home/rsvp/rsvpd>edit ds_config

Compareo nome da interface na linha:

IFACES='xxx yyy'

Anexo C

Procedimento de Instalação do Zebra

Procedimento de Instalação do Zebra

Instalação do Zebra

v.1

Objetivo: Instalação do Zebra em Linux, distribuição RedHat 8.0, a fim de se obter o módulo de roteamento OSPF.

Software

quagga-0.98.3.tar.gz

http://www.quagga.net/download/quagga-0.98.3.tar.gz

Procedimento:

1. Preparação:

Descomprima o Zebra

~ tar -zxvf

Entre no diretório criado

~ cd quagga

Personalize a configuração, por exemplo:

~./configure --disable-ipv6 & --disable-ripd & --disable-bgpd & --disable-bgp-announce & --enable-opauqe-LSA & --enable-ospf-te & --enable-multpath=0 & --enable-user=root & --enable-group=root

Configure os módulos e usuário do Zebra com o seguinte comando:

~ make

- Instale o software

~ make install

- Habilite o processo Tenet no computador editando a linha correspondente a "DISABLE" para o valor "NO" no arquivo:

~ /etc/xinetd.d/telnet

Execute o comando abaixo para finalizar

~ chkconfig telnet on

Siga o procedimento do Anexo A para configurar o Zebra.