UNIVERSIDADE FEDERAL DE UBERLÂNDIA

FACULDADE DE ENGENHARIA ELÉTRICA

PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

UM ESTUDO SOBRE A APLICABILIDADE DO MODELO MPLS/CBR NO PROVIMENTO DE QoS NUMA REDE IP

Dissertação apresentada por Nelcileno Virgílio de Souza Araújo à Universidade Federal de Uberlândia para obtenção do título de Mestre em Engenharia Elétrica aprovada em 07/07/2003 pela Banca Examinadora:

Professor Einstein Lemos de Aguiar, Dr. (UFMT)

Professor Paulo Roberto Guardieiro, Dr. (UFU) - Orientador

Professor Jamil Salem Barbar, Dr. (UFU)

UM ESTUDO SOBRE A APLICABILIDADE DO MODELO MPLS/CBR NO PROVIMENTO DE QoS NUMA REDE IP

NELCILENO VIRGÍLIO DE SOUZA ARAÚJO

Dissertação apresentada por Nelcileno Virgílio de Souza Araújo à Universidade Federal de Uberlândia como parte dos requisitos para obtenção do título de Mestre em Engenharia Elétrica.

Prof. Dr. Paulo Roberto Guardieiro
Orientador

Prof. PhD. Alcimar Barbosa Soares
Coordenador do Curso de Pós-Graduação

DEDICATÓRIA

Aos meus queridos pais por todo amor e incentivo que sempre demonstraram.

AGRADECIMENTOS

A conclusão desta dissertação só foi possível devido à ajuda e apoio de várias pessoas e instituições. Então, eu gostaria de agradecer:

À Deus pela vida e por mais esta oportunidade.

À Faculdade de Engenharia Elétrica na Universidade Federal de Uberlândia pelos recursos oferecidos para a execução deste trabalho.

À CAPES, Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, pela ajuda financeira recebida no decorrer do meu trabalho de pós-graduação.

Ao meu orientador Paulo Roberto Guardieiro, por sua orientação e dedicação na realização do curso de mestrado. Ele, que sempre me deu atenção, conselho e um melhor direcionamento nos momentos em que precisei.

A minha família que muito contribuíram com essa conquista, através da paciência, dedicação e carinho nos momentos mais difíceis durante a realização do curso de mestrado.

A todos os amigos e todas as pessoas que indiretamente me deram força e apoio.

RESUMO

Um Estudo sobre a Aplicabilidade do Modelo MPLS/CBR no Provimento de QoS numa Rede IP

O rápido crescimento dos usuários corporativos e da quantidade de aplicações de tempo real na Internet tem exigido das redes IP a criação de outros modelos de serviço de entrega de dados que possam garantir uma diferenciação de tráfego dos usuários e forneça qualidade de serviço no transporte dos pacotes. Seguindo esta tendência, o IETF tem apresentado diversas padronizações de modelos de serviço, tais como: serviços integrados, serviços diferenciados, MPLS, roteamento baseado em restrição e engenharia de tráfego, além do já existente serviço do melhor esforço. Contudo, a implementação isolada destes modelos tem se mostrado complexa e, ás vezes, ineficaz para determinadas situações. Por isso, a interoperação de modelos de serviço tem sido aconselhada, já que desta forma retira-se de cada modelo, a funcionalidade mais importante para gerar um modelo híbrido. Neste sentido, este trabalho apresenta e discute um modelo de serviço que combina o roteamento baseado em restrição e a tecnologia MPLS. Para avaliar o desempenho deste modelo híbrido em oferecer QoS foram analisados três parâmetros: banda passante, retardo e variação de retardo experimentado pelos tráfegos. Os resultados obtidos nos cenários simulados mostraram a viabilidade do modelo MPLS/CBR na construção de caminhos com garantias de QoS.

Palavras-Chave - Internet, MPLS, Roteamento Baseado em Restrição, Modelos de QoS Híbridos

ABSTRACT

An Study about Applicability of MPLS/CBR Model for Providing QoS in IP Networks

The fast growth of the corporative users and the amount of real time applications in the Internet has demanded IP networks the creation of others service models that can guarantee a differentiation of users traffic and supply quality of service in the transport of the packets. Following this trend, the IETF has presented diverse standardizations of service models, such as integrated services, differentiated services, MPLS, constraint based routing and traffic engineering, beyond the best effort service. However, the isolated implementation of these models it has shown complex and, sometimes, inefficacious for determined situations. Therefore, the interoperation of service models has been advised, since it gets each model, the most important functionality to generate a hybrid model. In this direction, this work presents and argues a service model that combines CBR and technology MPLS. To evaluate the performance of this hybrid model in offering QoS, three parameters had been analyzed: throughput, delay and jitter. The results gotten in the simulated scenes had shown the viability of model MPLS/CBR in the construction of paths with QoS guarantees.

Keywords - Internet, MPLS, Constraint Based Routing, QoS Hybrid Models

UM ESTUDO SOBRE A APLICABILIDADE DO MODELO MPLS/CBR NO PROVIMENTO DE QoS NUMA REDE IP

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

AF	*Assured Forwarding*
ARIS	*Aggregated Route Based IP Switching*
ATM	*Asynchronous Transfer Mode*
AS	*Autonomous Systems*
BA	*Behavior Aggregate*
BE	*Best Effort*
BGP	*Border Gateway Protocol*
BGP4	*Border Gateway Protocol version 4*
BPTM	Balde de Permissões de Taxa Máxima
CBR	*Constraint Based Routing*
CBQ	*Class Based Queueing*
CBS	*Commited Burst Size*
CDR	*Committed Data Rate*
CoS	*Class of Service*
CR-LDP	*Constraint Routing – Label Distribution Protocol*
CR-LSP	*Constraint Routing – Label Switching Path*
CSPF	*Constrained Shortest Path First*
CSR	*Cell Switching Router*
CU	*Currently Unused*
DiffServ	*Differentiated Service*

DLCI	*Data Link Connection Identifier*
DS	*Differentiated Service*
DSCP	*Differentiated Service CodePoint*
EF	*Expedited Forwarding*
ER	*Edge Router*
ERB	*Explicit Route Information Base*
ER-Hop	*Explicit Route – Hop*
ER-LSP	*Explicit Routing – Label Switching Path*
ER-TLV	*Explicit Route – Time-Length-Value*
ERO	*Explicit Route Object*
FEC	*Forwarding Equivalence Class*
FIB	*Forwarding Information Base*
FR	*Frame Relay*
FTN	*FEC-to-NHLFE*
FTP	*File Transfer Protocol*
GSMP	*General Switch Management Protocol*
HBT	*High Priority Best Effort Traffic*
HTTP	*Hypertext Transfer Protocol*
IBM	*International Business Machines*
IntServ	*Integrated Service*
IETF	*Internet Engineering Task Force*
IF_{in}	Interface de Entrada

IF_{out}	Interface de Saída
IP	*Internet Protocol*
IPv4	*Internet Protocol version 4*
IPv6	*Internet Protocol version 6*
IS-IS	*Intermediate Station to Intermediate Station*
ISP	*Internet Service Provider*
LAN	*Local Area Network*
LDP	*Label Distribution Protocol*
LER	*Label Edge Router*
LIB	*Label Information Base*
LSR	*Label Switching Router*
LSP	*Label Switching Path*
LSPID	*Label Switching Path Identification*
MAC	*Medium Access Control*
MF	*Multi-Field*
MNS2	*MPLS Network Simulator Version 2*
MPLS	*Multiprotocol Label Switching*
NAM	*Network Animator*
NHLFE	*Next Hop Label Forwarding Entry*
NS-2.1b6	*Network Simulator Version 2.1b6*
OSPF	*Open Shortest Path First*
OTCL	*Oriented Tool Command Language*

PBS	*Peak Burst Size*
PDR	*Peak Data Rate*
PHB	*Per Hop Behavior*
PHB BE	*Per Hop Behavior Best Effort*
PHB AF	*Per Hop Behavior Assured Forwarding*
PHB EF	*Per Hop Behavior Expedited Forwarding*
PPP	*Point to Point Protocol*
QoS	*Quality of Service*
RIP	*Routing Information Protocol*
RSVP	*Resource Reservation Protocol*
RSVP-TE	*Resource Reservation Protocol – Traffic Engineering*
RT1	*Real Time Traffic 1*
RT2	*Real Time Traffic 2*
SBT	*Simple Best Effort Traffic*
SLA	*Service Level Agreement*
SPF	*Shortest Path First*
ST	*Signalling Traffic*
TCP	*Transport Control Protocol*
TLV	*Time-Length-Value*
TOS	*Type of Service*
TTL	*Time To Live*
UDP	*User Datagram Protocol*

VCI/VPI	*Virtual Channel Identifier/Virtual Path Identifier*
VPN	*Virtual Path Network*
WAN	*Wide Area Network*
WFQ	*Weight Fair Queue*

UM ESTUDO SOBRE A APLICABILIDADE DO MODELO MPLS/CBR NO PROVIMENTO DE QoS NUMA REDE IP

Capítulo 1

INTRODUÇÃO

Até início da década de 90, nos sistemas finais da Internet executavam basicamente aplicações baseadas em texto (correio eletrônico, transferência de arquivos) que se comportavam de maneira satisfatória no modelo de serviço oferecido pela Internet, o serviço do melhor esforço. Isto acontecia porque as aplicações eram tolerantes a temporização, ou seja, o desempenho dessas aplicações não sofria tanta influencia dos níveis de retardo fim-a-fim e variação de retardo percebido pelos pacotes. Contudo, com o surgimento e popularização das aplicações multimídia (videoconferência, telefone por IP), o serviço do melhor esforço tornou-se limitado, pois não oferecia garantias quanto a níveis de retardo fim-a-fim e variação de retardo exigido por essas aplicações, uma vez que elas são sensíveis a temporização.

A partir daí, certos recursos de QoS foram introduzidos numa rede IP para oferecer outros modelos de serviço que satisfaçam às necessidades das aplicações multimídias, ou seja, que ofereçam garantias quanto à temporização para estas aplicações.

No âmbito do IETF, atualmente, estão sendo discutidas cinco abordagens para provimento de QoS em redes IP [56] : A arquitetura de serviços integrados [17], a arquitetura de serviços diferenciados [16], MPLS [48], roteamento baseado em restrição [21] e engenharia de tráfego [14]. Cada solução possui seus aspectos positivos e negativos, por isso o uso mais comum destas arquiteturas é através de uma solução integrada onde as funcionalidades mais importantes de cada abordagem podem ser combinadas.

Esta dissertação tem como objetivo mostrar a aplicabilidade de um modelo de serviço MPLS/CBR em oferecer QoS em redes IP, através do uso de caminhos LSP's com largura de banda garantida (CR-LSP's). Estes caminhos serão utilizados naquelas aplicações sensíveis a temporização, tal como as aplicações multimídias, para que desta forma possa haver um controle nos níveis de retardo fim-a-fim e variação de retardo, através da reserva de largura de banda. Um outro objetivo é apresentar de forma detalhada o mecanismo de construção dos caminhos CR-LSP's utilizando os dois protocolos de sinalização MPLS (CR-LDP e RSVP-TE). Como último objetivo, descrever o mecanismo de funcionamento do protocolo CR-LDP, no módulo MNS 2.0, para oferecer QoS e gerenciar a reserva de recursos.

A utilização da tecnologia MPLS dentro desta solução integrada se deve ao fato dela oferecer o serviço de roteamento explícito, um mecanismo essencial para implementar roteamento baseado em restrição.

O serviço de roteamento explícito do MPLS atende aos requisitos do roteamento baseado em restrição, ao processar o cálculo da rota no nó origem e encaminhar os pacotes ao longo da rota calculada sem violar o caminho predeterminado. Além disso, o MPLS utiliza os protocolos de sinalização do roteamento explícito (RSVP-TE [13] e CR-LDP [34]) para reservar os recursos requeridos pelo tráfego durante o estabelecimento da rota calculada.

Para que uma rede possa oferecer roteamento baseado em restrição é necessário que o cálculo da rota leve em conta não somente métricas escalares, mas também restrições referentes aos recursos disponíveis. Depois, a rede deve possuir um mecanismo de estabelecimento e encaminhamento, ao longo da rota calculada, que suporte roteamento explícito. Finalmente, deverá também possuir protocolos de roteamento intradomínio capazes de distribuir outras informações sobre os enlaces, além de identificar o seu estado [24].

A implementação deste modelo MPLS/CBR para o provimento de QoS em redes IP trabalha com a construção de caminhos LSP's com largura de banda garantida para aquelas aplicações de missão crítica ou tempo real. Uma vez que este tipo de aplicação exige garantia de QoS na transmissão dos dados.

As técnicas de QoS implementadas pelos simuladores NS 2 [41] e MNS 2 [40] na dissertação para construir um modelo de arquitetura MPLS/CBR se baseiam em quatro componentes [3]. O primeiro componente, o classificador de serviços, verifica a classe de serviço a qual pertence o pacote e enfileira-o no *buffer* correspondente da fila baseada em classes (CBQ). A seguir, o componente escalonador de pacotes seleciona uma das filas CBQ para encaminhar pacotes para o enlace. O componente controle de admissão é ativado pela mensagem CR-LDP *request* para verificar se o roteador tem o recurso solicitado pelo tráfego.

O último componente conhecido como gerenciador de recursos é ativado pela mensagem CR-LDP *mapping* para criar ou excluir filas CBQ a serem administradas pelo componente escalonador de pacotes, além do gerenciamento da informação dos recursos.

A abordagem de filas baseada em classes é importante dentro do modelo MPLS/CBR para o oferecimento de QoS. Pois, neste tipo de fila se aplicam as seguintes filosofias:

1) Cada classe de serviço possui sua própria fila de encaminhamento;
2) O esvaziamento das filas segue uma política de escalonamento definida pelo componente escalonador de pacotes, onde as filas com maior prioridade são as primeiras a serem esvaziadas.

Sendo assim, as filas CBQ desempenham a função de controlar os recursos locais de cada roteador ao longo da LSP [24].

Para avaliar o desempenho do modelo MPLS/CBR no oferecimento de QoS foram simulados três cenários. O primeiro cenário considera uma rede *backbone* com roteamento IP convencional. A seguir, a rede *backbone* implementa o mecanismo MPLS. No último cenário trabalha-se com o modelo proposto MPLS/CBR. Em todos os cenários monitora-se os valores obtidos na vazão, retardo fim-a-fim e variação de retardo experimentada pelos tráfegos. Principalmente, numa situação de congestionamento é avaliado o comportamento destes cenários na manutenção do oferecimento de QoS pela rede *backbone*.

Dentro dos cenários simulados foram injetadas três classes de tráfego. A primeira classe especificada pelo tráfego de tempo real, solicita que o encaminhamento dos pacotes nos enlaces seja realizado com baixos níveis de retardo fim-a-fim, variação de retardo e perda de pacotes, e a largura de banda dedicada ao tráfego. A classe de tráfego de melhor esforço

aceita a regra de transmissão tradicional da arquitetura Internet. Por fim, têm-se uma classe de tráfego que constitui-se um nível intermediário entre os tráfegos de tempo real e melhor esforço, denominada tráfego de melhor esforço de alta prioridade.

Apresenta-se a seguir, a organização de cada um dos capítulos que formam o restante do trabalho.

O Capítulo 2 começa definindo o conceito de QoS nas redes IP. A seguir, descreve as principais tecnologias de QoS, apresentando o princípio de funcionamento de cada uma e a interoperação entre as mesmas, ressaltando a adequação de uso de cada uma destas.

A arquitetura MPLS é estudada de forma detalhada no Capítulo 3. Neste capítulo são apresentados a origem da tecnologia MPLS, o conceito *label switching* e suas implementações. Depois, retrata-se o mecanismo de funcionamento de cada um dos componentes associados a esta arquitetura e as principais aplicações ligadas a ela.

No Capítulo 4 faz-se uma revisão sobre o conceito de Roteamento baseado em Restrição, o princípio de funcionamento dos componentes pertencente a ele e apresentam-se as aplicações implementadas pelo Roteamento baseado em Restrição, ressaltando o oferecimento de QoS em redes MPLS.

O Capítulo 5 detalha todos os procedimentos que foram seguidos na realização das simulações, mostrando os cenários de simulação configurados, os resultados obtidos quanto à vazão experimentada e os níveis de retardo fim-a-fim e variação de retardo sofrido na transmissão dos dados. Em seguida, faz-se uma análise destes parâmetros em cada um dos cenários simulados, avaliando o desempenho de cada modelo (Roteamento IP convencional, MPLS e MPLS/CBR) no provimento de QoS em uma rede *backbone*.

Finalmente, o Capítulo 6 descreve as conclusões gerais relativas a este trabalho, incluindo algumas sugestões para futuras pesquisas relacionadas ao tema aqui estudado.

Capítulo 2

Qualidade de Serviço em Redes IP

2.1 Introdução

Nos últimos anos, observou-se um intenso crescimento do número de usuários na Internet. Observou-se também o crescimento do interesse dos usuários pelas aplicações multimídia, tais como, ensino à distância, jogos interativos, vídeo sob demanda, teleconferência, dentre outras. Como conseqüência, o perfil do tráfego existente na Internet também vem sendo modificado. Contudo, a arquitetura Internet foi criada para oferecer basicamente o serviço melhor esforço, ou seja, a transmissão dos dados até o nó destino sem garantir padrões de confiabilidade e rapidez na entrega dos pacotes. Este tipo de serviço se torna eficaz em aplicações elásticas (correio eletrônico e transferência de arquivos), que suportam este modelo de serviço. Mas, quando se trata de aplicações multimídia, a arquitetura Internet não pode oferecer garantias aos parâmetros de QoS (vazão, retardo fim-a-fim, variação de retardo e perda de pacotes) solicitados por este tipo de tráfego. Já que, o serviço melhor esforço não pode garantir a entrega rápida e confiável dos dados ao nó destino, surge à necessidade de oferecer novos modelos de serviço baseados em um conceito emergente, a QoS nas redes IP.

Por essa razão, neste capítulo será abordada, primeiramente, a definição de QoS nas redes IP. Logo após, os modelos de serviço para provimento de QoS nas redes IP são estudados para definir a filosofia de cada um, suas principais características e como se inter-relacionam.

2.2 Definição de Qualidade de Serviço em Redes IP

A qualidade de serviço nas redes IP especifica um conjunto de requisitos de processamento e comunicação suportadas por um serviço e que permite a provisão da funcionalidade desejada por usuários do ambiente. Estes requisitos são chamados normalmente, de parâmetros de especificação de QoS. Em geral, os serviços de transporte de dados, fornecidos por provedores de serviço Internet (ISPs), possuem associados os seguintes parâmetros de QoS: vazão obtida no nó destino, retardo fim-a-fim e variação de retardo na entrega dos pacotes e, taxa de perda de pacotes [08, 36, 56].

A vazão é um parâmetro de QoS que mede a quantidade de pacotes transmitidos e reconhecidos que chegam no hospedeiro destino. Altos níveis de vazão indicam que grande parte do tráfego gerado pelas aplicações no hospedeiro origem está chegando no seu destino.

Outros dois parâmetros bastante empregados na especificação de QoS são o retardo fim-a-fim e a variação de retardo (*jitter*). O primeiro identifica o tempo total gasto pelos pacotes para percorrer entre o hospedeiro transmissor e receptor, levando em conta retardo de transmissão, retardo de propagação, retardo de processamento e retardo nas filas de saída dos roteadores. A variação de retardo representa a variação máxima em retardo fim-a-fim experimentada pelos pacotes em uma única sessão. Por exemplo, se o retardo fim-a-fim

mínimo atingido por qualquer pacote é 1ms e o máximo é 6 ms, então a variação de retardo experimentada é 5ms. Aplicações multimídia são sensíveis a estes dois parâmetros, quando os valores ultrapassam limites pré-definidos, seu desempenho atenua; ao contrário, o desempenho dessas aplicações na rede aumenta. Para aplicações elásticas, há maior tolerância ao aumento ou a diminuição do retardo fim-a-fim e da variação de retardo.

A última métrica a ser avaliada na especificação de QoS é a perda de pacotes sofrida durante a transmissão de uma mensagem. Neste parâmetro procura-se controlar a quantidade de pacotes descartados, principalmente numa situação de congestionamento, pois a perda de pacotes excessiva prejudica a qualidade da aplicação executada no hospedeiro receptor.

Como pôde ser observado nos parágrafos anteriores, diz-se que um modelo de serviço oferece QoS para seus fluxos, quando há um controle dos níveis de vazão, retardo fim-a-fim, variação de retardo e perda de pacotes na transmissão de uma mensagem entre um hospedeiro origem e destino. Na próxima seção serão vistos os principais modelos de serviço implementados, atualmente, para fornecimento de QoS em redes IP.

2.3 Modelos de Serviço para Fornecimento de QoS em Redes IP

Essa seção apresenta os cinco principais modelos de serviço para fornecimento de QoS nas redes IP definido pelo IETF : Serviços Integrados e RSVP, Serviços Diferenciados, MPLS, Roteamento Baseado em Restrição e Engenharia de Tráfego; e os relacionamentos que podem existir entre eles.

2.3.1 Serviços Integrados (IntServ) e RSVP

O modelo de serviços integrados, conforme descrito na Figura 2.1, tem seu funcionamento baseado em quatro rotinas fundamentais: a reserva de recursos, o controle de admissão, o classificador e o escalonador de pacotes [17].

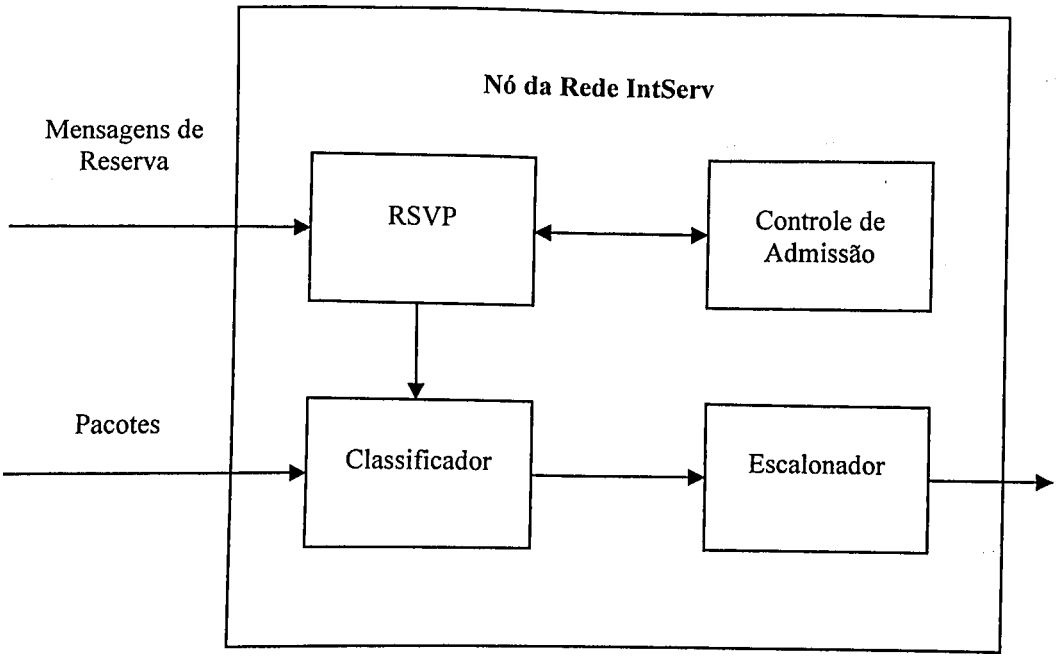


Figura 2.1 - Componentes da Arquitetura IntServ/RSVP

A reserva de recursos utiliza um protocolo de sinalização chamado RSVP [18] para solicitar aos roteadores pertencente ao caminho utilizado pelo fluxo, os serviços necessários para atender as características do tráfego.

A Figura 2.2 mostra como ocorre o processo de sinalização RSVP. O host origem envia uma mensagem PATH ao host destino, contendo as informações sobre o fluxo a ser transmitido. Essa mensagem percorre cada um dos roteadores, ao longo do caminho calculado, até alcançar o host destino. Quando o receptor é avisado dessa solicitação, ele

responde com uma mensagem RESV que será enviada de volta para o host origem, solicitando aos roteadores do domínio Intserv/RSVP, os recursos requeridos pelo fluxo. Se a resposta de algum roteador for negativa, será enviada uma mensagem de erro ao transmissor, encerrando o processo de sinalização. Caso contrário, o roteador aloca banda passante e espaço de armazenagem para o fluxo e a sua informação de estado será instalada nos roteadores [18].

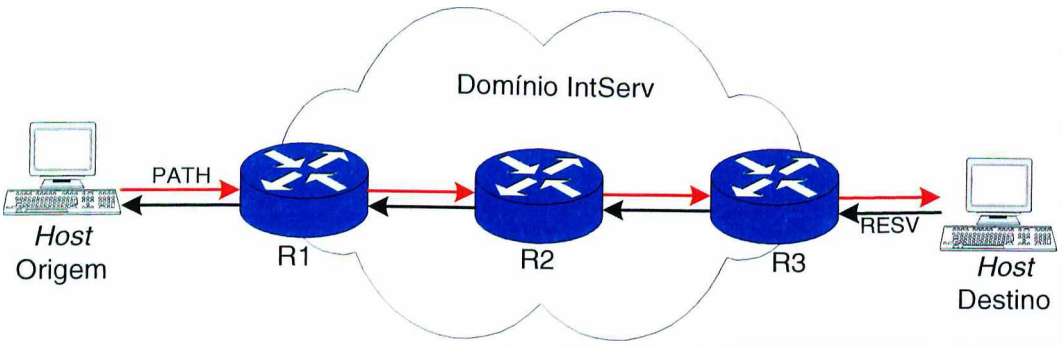


Figura 2.2 - Sinalização do protocolo RSVP na rede IntServ.

O controle de admissão é responsável em verificar se a reserva de recursos solicitada por um determinado fluxo pode ser atendida.

O classificador mapeia cada um dos pacotes de entrada dentro de alguma classe de serviço. Os pacotes classificados com uma mesma classe receberão o mesmo tratamento pelo escalonador de pacotes. A escolha de uma classe pode ser definida pelas características do fluxo.

O escalonador de pacotes utiliza uma política de filas e possivelmente também outro tipo de mecanismo, para gerenciar a transmissão dos pacotes mapeados pelo classificador.

O modelo Intserv/RSVP oferece duas classes de serviço além do serviço do melhor esforço. Elas são: serviço garantido [49] para aplicações que necessitam de um limite de

retardo constante; e serviço de carga controlada [58] para aplicações que requerem confiabilidade e um serviço de melhor esforço mais aprimorado.

A baixa escalabilidade em redes de grande dimensão acaba limitando o uso do modelo Intserv/RSVP para as redes de acesso (LAN, Frame-relay, X.25). Isso se deve aos seguintes problemas [36, 56]:

1) A quantidade de informação de estado cresce proporcionalmente com o número de fluxos. Por consequência, os roteadores do domínio, principalmente os localizados no núcleo, sofrem uma grande sobrecarga, ocasionada pelo aumento exagerado de *overhead* e espaço de armazenagem gerado pelas informações de estado;

2) As exigências sobre os roteadores são altas. Já que, todos devem implementar as quatro rotinas (classificador, escalonador de pacotes, reserva de recursos e controle de admissão) para o funcionamento do modelo Intserv/RSVP;

3) O protocolo RSVP para construir e manter um caminho a ser utilizado pelos fluxos, gera um grande tráfego de sinalização. Pois, mesmo depois que os recursos tenham sido mapeados pelo RSVP, existe a necessidade de manter esse processo de sinalização. Já que, o protocolo trabalha em modo de estado leve, ou seja, se qualquer roteador dentro do conjunto deixa de receber uma solicitação de reserva de recursos, a conexão é interrompida. Esse crescimento do tráfego de sinalização ocasiona problemas de escalabilidade.

2.3.2 Serviços Diferenciados (DiffServ)

Como pode ser observado na Figura 2.3, o objetivo principal de uma arquitetura de serviços diferenciados é agregar o tráfego que entra no domínio, através dos roteadores de borda, vindo de diferentes redes de acesso e associá-lo a um comportamento agregado. Esse comportamento será utilizado para definir a classe de encaminhamento (PHB) do tráfego, ou seja, como ele será transmitido dentro da rede [16, 36].

A definição dessas classes de encaminhamento ocorre por meio de um contrato de serviço (SLA) feito entre o usuário e o provedor de serviço Internet (ISP). Esse contrato pode especificar as regras de condicionamento de tráfego [16] ou também determinar se o fluxo agregado está ou não em conformidade com o perfil de tráfego requerido. O SLA pode ser negociado com o usuário, de forma estática, onde as negociações ocorrem em um determinado período de tempo (mensamelmente, semestralmente); ou dinâmica, as negociações aos serviços são feitas sob demanda, utilizando um protocolo de sinalização.

Os pacotes agregados são identificados por um código (*codepoint*) que determina sua classe de encaminhamento dentro da arquitetura de serviços diferenciados. Esse código fica localizado no caso do IPv4, no campo TOS, ou no caso do IPv6, no campo *traffic class*. Geralmente, esse campo é renomeado para DS, em ambos padrões de formato IP (IPv4 ou IPv6). A estrutura do campo DS é mostrada na Figura 2.4 [42]. Os seis bits mais à esquerda do campo DS formam o subcampo *Differentiated Service CodePoint*, que é responsável em definir as regras de encaminhamento a ser utilizada pelo PHB para a transmissão do pacote agregado. Os outros dois bits não são atualmente utilizados. Por isso, são conhecidos como *Currently Unused* [42].

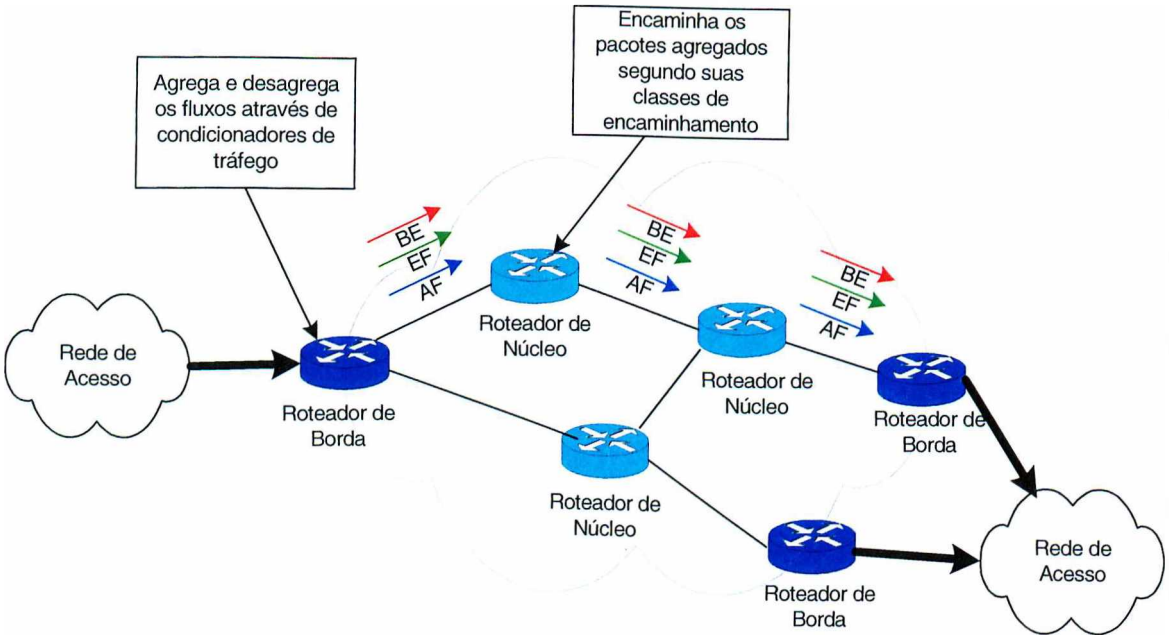


Figura 2.3 - Arquitetura Serviços Diferenciados

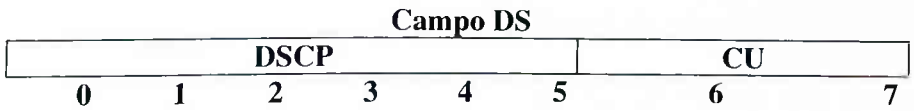


Figura 2.4 - Formato de um campo DS.

O modelo DiffServ é composto por quatro componentes: o classificador, o medidor, o marcador e o moldador/descartador [16]. Como pode ser visto na Figura 2.5.

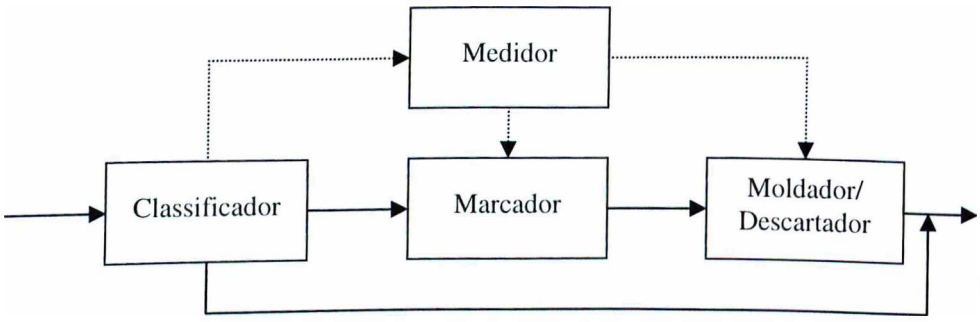


Figura 2.5 - Condicionador de Tráfego

O classificador de pacotes associa o fluxo de entrada a um determinado comportamento agregado, especificado pelo contrato de serviço, através de um perfil de tráfego. Existem dois métodos de classificação: multi-campo (MF), que seleciona os pacotes baseados na combinação de um ou mais campos do cabeçalho IP (endereço origem e destino, campo DS, protocolo ID, número das portas origem e destino); e comportamento agregado (BA), que classifica os pacotes baseando-se somente no campo DSCP.

Depois de classificados, os pacotes são enviados para as rotinas de medição e marcação. Na fase de medição é verificado se o pacote está dentro ou fora do perfil de tráfego requerido. A análise do perfil de tráfego pode ser feita utilizando o mecanismo de "balde de permissão" (*Token Bucket*), onde o pacote avaliado deve ter permissões suficientes no balde para ser considerado em conformidade. Esse mecanismo pode ser implementado de duas maneiras: com um "balde de permissão", avaliando se o pacote está ou não em conformidade; ou com dois "baldes de permissão", que permitem classificar um pacote em três níveis de descarte (alto, médio e baixo), de acordo com a quantidade de permissões existente nos baldes [36].

Com base no resultado da medição, o marcador configura o campo DS do pacote com a classe de encaminhamento apropriada.

O moldador retarda o tráfego para que haja permissões suficientes para encaminhá-lo pela rede e torná-lo em conformidade com algum PHB. Quando isso não acontece, entra em ação o descartador, para liberar espaço de armazenagem do moldador. Além disso, os pacotes marcados com alta prioridade de descarte e não em conformidade com o perfil de tráfego são descartados. Por isso, o descartador também é conhecido como policiamento de tráfego.

Os quatro componentes discutidos anteriormente formam uma função muito importante dentro do modelo de serviços diferenciados, o condicionamento de tráfego. Essa função, geralmente, é implementada nos roteadores de borda, pois eles são responsáveis em adequar o tráfego, tanto para entrar quanto para sair do domínio Diffserv. Por conseguinte, os roteadores de núcleo dedicam a maior parte dos seus recursos no encaminhamento de pacotes, de acordo com seu PHB.

Uma classe de encaminhamento, geralmente, pode ser definida como: *default* ou melhor esforço (BE) [16], expresso (EF) [33] ou *premium* e assegurado (AF) [32]. As regras de cada classe determinam como os pacotes agregados devem ser transmitidos dentro do domínio DiffServ.

A classe de encaminhamento do melhor esforço (PHB BE) segue a regra de transmissão tradicional de uma arquitetura Internet. O valor assumido pelo DSCP é "000000" [42].

Para aplicações que exigem o tamanho da fila de espera para transmissão muito pequeno ou nulo, utiliza-se à classe de encaminhamento expresso (PHB EF). Ela se dedica a oferecer encaminhamento com baixos níveis de retardo fim-a-fim, variação de retardo e perda de pacotes, e uma largura de banda dedicada ao tráfego. As aplicações multimídia são as mais indicadas para esse tipo de serviço. O valor assumido por um DSCP para um PHB EF é "101110" [42].

A alternativa da classe de encaminhamento assegurado (PHB AF) constitui-se um nível intermediário entre as classes expresso e melhor esforço. Ela pode oferecer vários níveis de garantia no encaminhamento dos pacotes dentro do domínio Diffserv. Sendo que, cada nível de garantia especifica uma classe AF, que determina os recursos alocados (largura de banda e

espaço de armazenagem) em cada roteador para a transmissão do fluxo agregado. Além disso, todas as classes AF possuem nível de garantia de entrega menor do que as obtidas pelo encaminhamento expresso, permitindo assim, a existência de congestionamento dentro da rede. Como consequência, os pacotes de cada classe de encaminhamento assegurado podem ser marcados com um dos três níveis possíveis de descarte (alto, médio e baixo). Em caso de congestionamento, o nível de descarte determina qual a importância do pacote para a classe AF e descarta, prioritariamente, os pacotes com alta probabilidade de descarte. Dessa forma, procuram proteger os dados considerados importantes para a classe. Atualmente, existem quatro classes AF padronizadas.

A implementação de uma classe de encaminhamento assegurado tenta "minimizar o congestionamento de longa duração dentro de cada classe, enquanto permite o congestionamento de curta duração resultante do tráfego de rajadas" [32, pg. 12]. Por isso, torna-se necessário um mecanismo moldador/descartador que atue sobre os dois tipos de congestionamento e utilize um nível de congestionamento suavizado [32] para determinar quando os pacotes devem ser descartados. A Tabela 2.1 [42] define os valores DSCP assumidos na classe de encaminhamento assegurado:

Tabela 2.1 - Classes de Encaminhamento AF e seus níveis de descarte

		Classes			
		Classe 1	Classe 2	Classe 3	Classe 4
Prioridade de Descarte	Baixa	001010	010010	011010	100010
	Média	001100	010100	011100	100100
	Alta	001110	010110	011110	100110

A arquitetura de serviços diferenciados possui algumas diferenças estruturais com relação ao modelo IntServ/RSVP. A primeira diferença está na forma do oferecimento de QoS. No modelo DiffServ, esse oferecimento ocorre para os agrupamentos de fluxo. Enquanto, na outra arquitetura, a QoS é oferecida para cada fluxo do domínio. Isso gera um ganho na questão da escalabilidade da rede. Pois, a quantidade de informações de estado é proporcional ao número de agrupamento de fluxos (no modelo DiffServ). Como a quantidade de classes é um número limitado, a rede pode aumentar o número de nodos e continuar oferecendo uma garantia confiável na entrega dos pacotes.

A outra diferença é que as operações funcionais para prover diferenciação de serviços se concentram nas fronteiras (roteadores de borda) do domínio DiffServ, deixando o núcleo (roteadores intermediários) dedicado ao encaminhamento dos pacotes agregados, segundo sua classe de encaminhamento. Dessa forma, a alternativa de arquitetura de serviços diferenciados torna-se mais indicada para redes de grande dimensão (WAN).

2.3.3 *Multiprotocol Label Switching*

A Figura 2.6 ilustra o modo de encaminhamento IP tradicional: quando um pacote chega no roteador de entrada da rede, ele tem seu cabeçalho analisado e busca na tabela de roteamento o próximo salto (roteador) correspondente ao pacote. Esta tabela armazena, todas as rotas existentes que o ligam a outros roteadores. Esse mecanismo de envio é repetido em todos os roteadores até alcançar o nó destino.

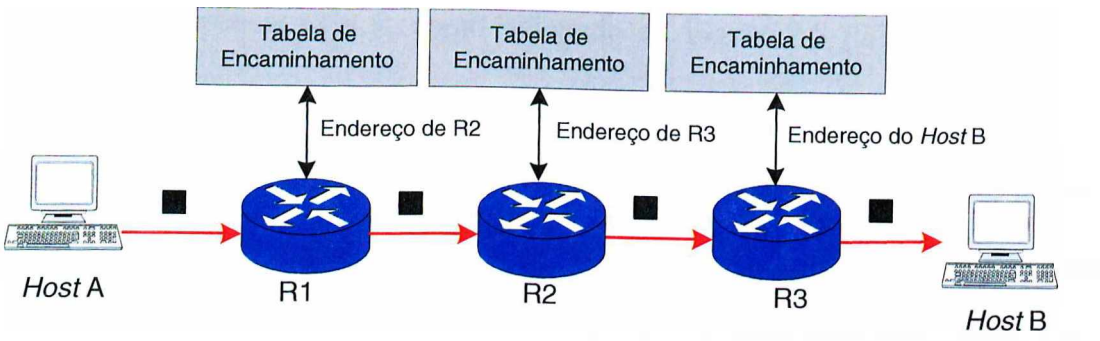


Figura 2.6 – Encaminhamento IP tradicional

O MPLS [48] surge como uma alternativa para melhorar a transmissão IP tradicional, propondo uma arquitetura baseada na tecnologia de comutação de rótulos (*label switching*), onde é atribuída aos pacotes que possuem uma mesma política de encaminhamento, uma classe de equivalência de encaminhamento (FEC). Essa FEC é codificada em uma variável de tamanho fixo e curto, chamado de rótulo. Depois, busca-se na tabela de roteamento do roteador de entrada, o seu próximo salto e envia-se o pacote rotulado para esse salto. A partir daí, não existe mais a necessidade de analisar o cabeçalho do pacote para poder fazer a busca pelo próximo salto na tabela de roteamento. O rótulo é utilizado como um índice para acessar as informações de próximo salto e valor de rótulo contida numa tabela de informações de rótulo (LIB). O valor do rótulo deve ser trocado a cada passagem por um roteador intermediário, pois os rótulos têm escopo de funcionamento local. Depois de conhecido os novos valores de rótulo e o próximo salto, o pacote rotulado pode ser encaminhado ao próximo roteador do caminho e se ele ainda estiver localizado no núcleo da rede MPLS, as rotinas descritas anteriormente se repetem. Quando, o pacote rotulado alcança o roteador de saída, o rótulo é removido do pacote e o mecanismo de envio IP tradicional pode ser retomado. A Figura 2.7 descreve o mecanismo de funcionamento do MPLS apresentado anteriormente.

O formato de um pacote MPLS, como mostrado na Figura 2.8 [22], é dividido da seguinte forma: 20 bits de rótulo, um campo experimental – formalmente conhecido como classe de serviço (CoS) – com 3 bits, 1 bit de um indicador de pilha de rótulos e, por último, um campo TTL com 8 bits. Num quadro PPP/LAN, o cabeçalho MPLS fica encapsulado entre os cabeçalhos da camada de enlace e da camada de rede. Ao contrário do quadro *frame relay* que fica localizado no DLCI, ou das células ATM que fica localizado no VCI/VPI [22, 48].

Pelo MPLS ser um protocolo orientado a conexão, os pacotes somente são enviados após a configuração do caminho. Segundo [48], um caminho baseado em comutação de rótulos ou LSP é gerado sempre que grupos de pacotes pertencentes a uma mesma FEC precisam ser transmitidos do roteador de entrada para o roteador de saída de um domínio MPLS. Um roteador que reconhece a tecnologia de comutação de rótulos é formalmente denominado de roteador baseado em comutação de rótulos (LSR). Existem dois tipos de LSR: aqueles localizados na fronteira de uma rede MPLS, os LERs ou roteadores de borda, e aqueles situados na região central, os LSRs ou roteadores de núcleo. Os roteadores de borda são responsáveis: na entrada, por analisar o cabeçalho IP do pacote, determinar sua FEC e especificá-la através de um rótulo e gravar essas informações numa tabela conhecida como Base de Informações do Rótulo (LIB); e na saída, por readequar o tráfego ao encaminhamento IP tradicional e remover o rótulo do pacote. As funções de troca de rótulos e acesso a tabela LIB são desempenhadas pelos roteadores de núcleo. Todos os roteadores tem a função de encaminhamento inerente a eles.

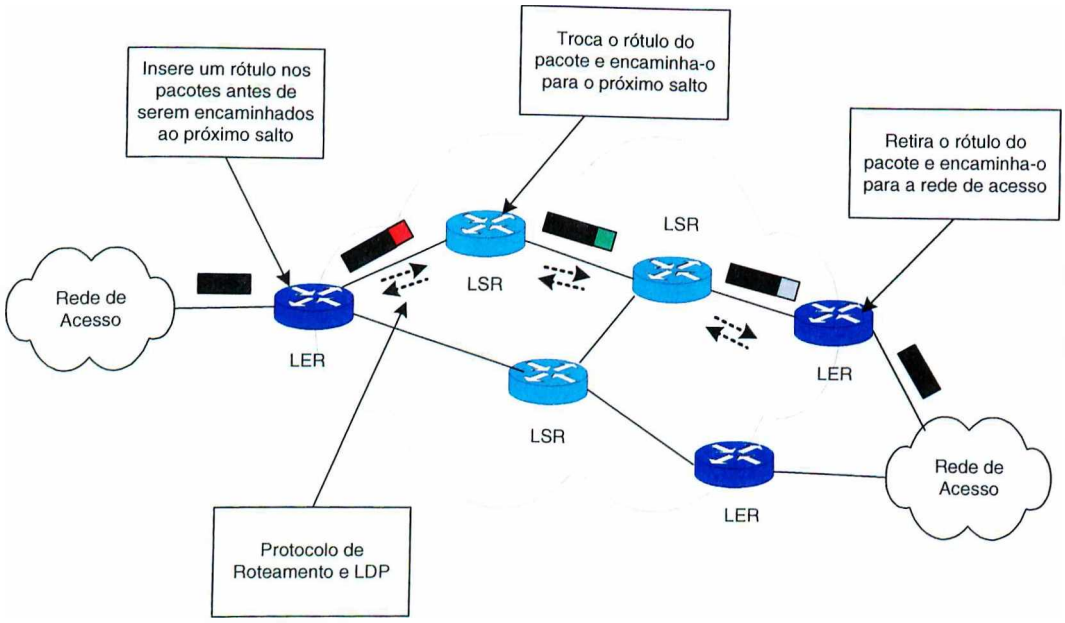


Figura 2.7 – Encaminhamento MPLS.

Para estabelecer um LSP, a arquitetura MPLS pode utilizar alguns protocolos de sinalização como RSVP [18] ou LDP [05]. Esses protocolos também podem distribuir rótulos para os roteadores. Uma outra alternativa de distribuição de rótulos pode ocorrer por meio dos protocolos de roteamento da rede (BGP, OSPF).

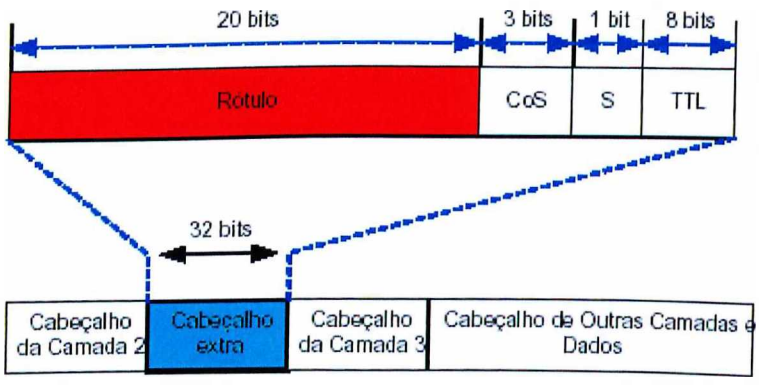


Figura 2.8 – Formato de um pacote MPLS.

As principais vantagens no modelo MPLS são: implementar Engenharia de Tráfego em redes IP com o uso dos LSPs com rota explícita; suportar qualidade de serviço e classe de serviço para diferenciação de serviços; melhorar a interoperabilidade entre redes IP e ATM, fornecendo uma ponte entre os dois tipos de rede; e melhorar a performance do encaminhamento de pacotes numa rede, ocasionado pela simplificação do mecanismo de transmissão.

2.3.4 Roteamento baseado em Restrição

O cálculo do caminho para qualquer protocolo de roteamento intradomínio tradicional baseia-se em um algoritmo que otimiza uma determinada métrica escalar. Por exemplo, se um dado protocolo de roteamento têm como métrica o número de saltos, quando na seleção do caminho a ser utilizado para transmitir os pacotes, poderá ser escolhido o caminho com o menor número de saltos. Como também, pode ser considerada a métrica do primeiro caminho mais curto, onde a rota escolhida pode ser aquela com o menor retardo de propagação ao nó destino.

No roteamento baseado em restrição, a seleção de uma rota não é baseada somente em parâmetros escalares (menor caminho, número de saltos), mas também é levado em conta um conjunto de restrições especificadas pelo usuário. Por exemplo, se uma determinada aplicação distribuída por um hospedeiro origem solicita certos níveis de QoS, o CBR selecionará um caminho que satisfaça os parâmetros escalares e os requisitos de QoS exigidos pela aplicação.

Os principais objetivos do Roteamento baseado em Restrição [56] são:

a) selecionar rotas que possam satisfazer certos requisitos de QoS e;

b) aumentar a utilização da rede.

Contudo, o CBR tem algumas dificuldades para ser implementado junto com o roteamento IP tradicional. A primeira dificuldade é a exigência de que o cálculo do caminho seja feito no nó origem. Isto porque diferentes nós origem podem ter diferentes restrições para o caminho, mesmo tendo um nó destino semelhante. Além disso, as restrições associadas ao caminho ficam localizadas somente no roteador origem, nenhum outro roteador da rota calculada conhece essas restrições. Ao contrário, no roteamento tradicional, a rota é calculada de forma distribuída por todos os roteadores da rede e este cálculo não considera as restrições de diferentes roteadores origem. A segunda dificuldade é que a transmissão orientada ao destino não pode ser utilizada pelo roteamento baseado em restrição. Já que, diferentes roteadores origem podem ter diferentes caminhos a um mesmo destino. O nó destino não pode ser aplicado como único componente para determinar o modo de encaminhamento dos pacotes. Por isso, alguns serviços do roteamento explícito são exigidos para encaminhar os dados. Finalmente, o roteamento tradicional não consegue distribuir informações sobre as restrições impostas aos enlaces para o roteamento baseado em restrição fazer o cálculo da rota no roteador origem. Isso se deve ao fato dos protocolos de roteamento tradicional distribuirem somente informações sobre a métrica escalar (número de saltos, primeiro caminho mais curto) implementada por eles.

Para [24] deve-se construir um sistema de roteamento numa rede IP que suporte ambos tipos de roteamento (restrição e tradicional). Dessa forma, pode-se oferecer um determinado tipo de roteamento de acordo com as necessidades dos pacotes a serem encaminhados.

O MPLS e o Roteamento baseado em Restrição, quando utilizados em conjunto podem oferecer uma alternativa na construção de caminhos LSPs com uma carga de tráfego estável e assim tenta minimizar o problema da má distribuição de tráfego pelos enlaces.

2.3.5 Engenharia de Tráfego

A Engenharia de Tráfego procura otimizar a utilização dos recursos disponíveis e a performance da rede, de modo que o tráfego seja distribuído de maneira uniforme pelos enlaces [11, 12, 14, 51].

Os principais objetivos observados pela Engenharia de Tráfego, segundo a performance da rede, podem ser divididos em duas categorias: orientado a tráfego, dedicam-se em melhorar as garantias de qualidade de serviço ao tráfego da rede, e orientado a recursos, procura fornecer uma alocação eficiente dos recursos oferecidos [12].

Um problema comum enfrentado por ambos objetivos de performance (tráfego e recursos) é o congestionamento. Ele pode surgir, principalmente, devido a duas situações [12]:

1) Os recursos utilizados para suprir a demanda de tráfego são insuficientes ou inadequados; ou
2) O tráfego foi mal distribuído pela topologia da rede, fazendo com que alguns enlaces se tornem sobrecarregados de fluxo de dados enquanto outros estão subutilizados. A Engenharia de Tráfego dedica-se em solucionar, principalmente, a segunda situação de congestionamento.

A Engenharia de Tráfego possui um modelo de processos onde se procura implementar os objetivos de performance (tráfego e recursos). Este modelo possui uma característica iterativa de processamento. Por isso, as rotinas pertencentes a ele são repetidas continuamente até que seja alcançado os objetivos de performance definido pelo administrador da rede.

A Figura 2.9 apresenta através de um fluxograma como ocorre o processo de Engenharia de Tráfego. Este modelo de processos pode ser descrito em 4 módulos principais: formulador, observador, analisador/caracterizador e otimizador.

O módulo formulador é invocado para criar a política de controle que obedeça os objetivos de performance pretendido pelo administrador da rede. A formulação dessa política leva em conta requisitos operacionais da rede, tais como: o modelo de negócios predominante, a estrutura de custo da rede, as restrições operacionais e o critério de otimização.

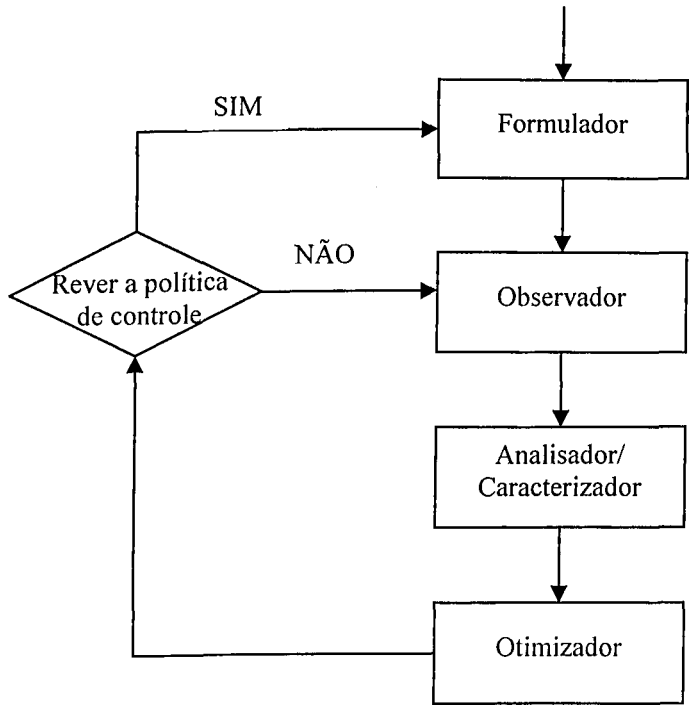


Figura 2.9 – Modelo de Processos da Engenharia de Tráfego

Depois de formulada a política de controle, o próximo módulo a ser executado é o Observador. Nele, um conjunto de funções de monitoramento podem ser utilizadas para fornecer as informações que descrevem o estado da rede. As informações geradas pelo monitoramento, posteriormente, terão um papel importante para determinar a qualidade dos serviços da rede e avaliar a eficiência das políticas de controle. Como também, otimizar o desempenho da rede em resposta aos estímulos e eventos originados dentro e fora dela.

Quando as informações obtidas pelo módulo observador entram no módulo Analisador/Caracterizador. Ele analisa esses dados para verificar possíveis problemas que possam existir atualmente ou futuramente no desempenho da rede. A partir daí, define-se um conjunto de alternativas para saná-los. Além disso, este módulo também investiga o comportamento do tráfego dentro da rede, identificando os pontos relevantes da rede, as características do tráfego oferecido, as regiões de risco (gargalos, pontos de falha, enlaces subutilizados ou congestionados) que podem comprometer os objetivos de performance. Os resultados deste módulo são utilizados na otimização da performance da rede, no planejamento da capacidade dos recursos disponíveis, no projeto e controle das operações da rede.

O último módulo, o Otimizador, dedica-se a otimização da performance da rede. Este módulo utiliza um processo de decisão para selecionar um conjunto de ações que identificam e implementam uma solução para as questões levantadas pelo módulo Analisador/Caracterizador.

A implementação de Engenharia de Tráfego em uma rede IP torna-se uma tarefa complexa devido, principalmente, às limitações dos protocolos de roteamento intradomínio

(OSPF, IS-IS e RIP), que focalizam a decisão de roteamento somente nos aspectos topológicos, não levando em conta outros fatores como disponibilidade de recursos e características do tráfego. Conseqüentemente, acaba gerando uma má distribuição do tráfego dentro da rede.

Uma alternativa oferecida para minimizar a limitação dos protocolos de roteamento intradomínio em suportar Engenharia de Tráfego consiste no acréscimo de requisitos não-topológicos às informações que são distribuídas por eles. Além disso, pode ser aplicado um novo tipo de roteamento, conhecido como Roteamento baseado em Restrição (CBR) [21], que considera esses novos requisitos no cálculo do caminho.

2.4 Conclusões

Os modelos de serviço apresentados neste capítulo devem ser aplicados de forma integrada, pois nenhum deles consegue satisfazer, de forma efetiva, os requisitos para QoS fim-a-fim. Por exemplo, o modelo IntServ tem como característica fundamental prover QoS em nível de fluxo. Por isso, ele acaba sendo mais indicado para redes de pequeno porte (LANs). Quando implementado em redes de grande porte pode haver uma sobrecarga de processamento ocasionado pelo mecanismo de reserva de recursos que necessita constantemente de mensagens de *refresh* (PATH e RESV) para manter o caminho onde os pacotes são encaminhados.

A visão agregada de fluxos proporciona uma alta escalabilidade para as redes DiffServ, o que acaba tornando-a mais interessante para redes de grande porte (WANs). O principal problema do modelo DiffServ é a sua interoperação com outros tipos de domínio. Como, ele

trabalha com agregação de fluxo, deve existir nos roteadores de fronteira condicionadores de tráfego que façam o processo de agrupamento e desagrupamento dos fluxos. Conseqüentemente, a complexidade do funcionamento desses roteadores torna-se elevada exigindo mais capacidade de processamento, podendo causar uma queda de desempenho na rede.

As principais habilidades do MPLS são oferecer encaminhamento de pacotes em alta velocidade e prover roteamento explícito. Consequentemente, ele acaba se tornando uma ferramenta poderosa para a implementação de outro modelo de serviço, a Engenharia de Tráfego. Como, o MPLS atua entre as camadas de enlace e rede, sua utilização se concentra no transporte dos dados. Por isso, ele atua em conjunto com outros modelos de serviço (Diffserv , Roteamento Baseado em Restrição e Engenharia de Tráfego) para prover QoS em redes de grande porte e backbones.

Dessa forma, a interoperação entre os modelos de serviço para oferecimento de QoS é o principal obstáculo a ser vencido para conseguir prover QoS fim-a-fim para o usuário final. Por isso, os pesquisadores concentram seus esforços em oferecer num futuro próximo modelos de QoS interoperável que não afetem profundamente o desempenho da rede.

Capítulo 3

Visão Geral da Tecnologia MPLS

3.1 Introdução

Tradicionalmente, a arquitetura Internet se baseia numa forma de encaminhamento onde os pacotes a serem enviados a um determinado receptor, têm seu cabeçalho IP analisado pelo roteador, para obter o prefixo do endereço destino. Com esta informação, a tabela de encaminhamento é acessada e o próximo salto em direção ao receptor é definido. A partir daí, o roteador encaminha os pacotes para o próximo salto e repete-se todo o processo descrito anteriormente, nó após nó, até atingir o nó destino.

No entanto, com o crescimento das aplicações de tempo real dentro dos serviços oferecidos pela Internet, a arquitetura atual tem certas deficiências com relação à velocidade de transmissão, controle de tráfego e garantia de entrega dos pacotes, o que acaba impossibilitando um desempenho satisfatório dos serviços de tempo real. Já que, a Internet foi construída, inicialmente, apenas para transmitir pacotes de um ponto ao outro, sem levar em conta nenhuma política de controle e entrega de pacotes. Assim, surge a necessidade por novos modelos de serviço na camada de rede que ofereçam confiabilidade no encaminhamento dos pacotes.

A tecnologia MPLS foi criada para suprir algumas das limitações do modelo IP tradicional, principalmente, questões de velocidade e controle do tráfego dentro da rede. O sucesso desta tecnologia deve-se pela simplicidade do mecanismo de encaminhamento que permite aos pacotes serem transmitidos numa velocidade mais rápida. Uma vez que o cabeçalho IP dos pacotes somente precisa ser analisado no primeiro nó (roteador de entrada). A partir daí, um índice (rótulo) é associado aos pacotes e distribuído aos outros pontos da rede através de um protocolo de distribuição de rótulos. Dessa forma, quando o tráfego chega em qualquer ponto da rede, o rótulo é utilizado para acessar a tabela de encaminhamento e determinar o próximo salto. Este processo se repete até alcançar o último nó (roteador de saída) que retira o rótulo do pacote e o encaminha no modo tradicional ao destino escolhido. Uma outra característica importante do MPLS é a dissociação entre os planos de controle e encaminhamento. Isto propicia a aplicação de políticas diferentes de roteamento e envio sem que um módulo interfira no outro. Finalmente, a característica multiprotocolo permite a interoperabilidade com vários tipos de tecnologia de camada 2 (LAN, ATM, *Frame Relay*), permitindo um aumento na popularização do MPLS.

A necessidade deste capítulo deve-se ao objeto de pesquisa, o modelo MPLS/CBR, ser baseado nesta tecnologia. Assim, o Capítulo 3 é dividido da seguinte forma: a primeira seção trata da origem da tecnologia MPLS, o conceito *Label Switching* e suas implementações. Depois, os principais componentes associados a arquitetura MPLS são levantados, enfocando basicamente o mecanismo de funcionamento de cada um deles e a função dos mesmos dentro do domínio MPLS. Logo após, uma seção descreverá os procedimentos para encaminhar pacotes dentro de uma rede MPLS. A próxima seção apresentará as principais aplicações MPLS (VPN, Engenharia de tráfego). A última seção é dedicada à apresentação de algumas

conclusões surgidas após o embasamento teórico apresentado nas seções anteriores deste capítulo.

3.2 Tecnologia *Label Switching* e o MPLS

A tecnologia *label switching* é um novo paradigma de sistema de roteamento onde existem duas funções bem distintas desempenhadas pelo roteador. A primeira função é chamada de plano de encaminhamento, a qual é responsável pelo envio dos pacotes de acordo com as informações contidas na tabela de encaminhamento (LIB) e no cabeçalho do pacote a ser transportado. A outra função trata dos parâmetros de construção e manutenção da tabela de encaminhamento. Por isso, ela é conhecida como plano de controle [08, 15, 22, 24, 48].

A arquitetura *label switching* é composta por dois dispositivos fundamentais: o roteador de borda (ER) e o roteador *label switching* (LSR). O roteador de borda pode ser visto como entrada, quando recebe pacotes convencionais, analisa seus cabeçalhos para definir os respectivos rótulos como índice na LIB, ou saída, quando o pacote rotulado vai sair do domínio *label switching* e seu rótulo deve ser removido. O roteador *label switching* se preocupa em trocar o rótulo de entrada do pacote pelo seu correspondente rótulo de saída contido na LIB, para que ele seja enviado corretamente para o seu próximo salto na rede [22, 24].

Diferentes abordagens foram dadas a tecnologia *label switching* até chegar na arquitetura MPLS. A primeira abordagem *label switching* popularizada foi a CSR da *Toshiba*. Ela introduzia a idéia que uma malha de comutação ATM podia ser controlada por protocolos IP, em vez dos protocolos de sinalização ATM. Logo após, a *Ipsilon* lançou o modelo IP

Switching, a segunda geração desta tecnologia, onde um switch ATM pode ser controlado por um dispositivo externo baseado em roteamento IP, por meio de um protocolo de controle de comutação (GSMP). O objetivo principal desta abordagem é integrar os switches ATM e roteamento IP em um simples e eficiente mecanismo. A configuração das tabelas de encaminhamento dos switches depende da percepção do fluxo de dados chegando neles, por isso, o IP *Switching* é definido como um modelo orientado a dados. Alguns meses após o lançamento do IP *Switching*, a *Cisco Systems* apresentou uma outra implementação, denominada *Tag Switching*. Esta arquitetura teve um papel importante na criação do MPLS, pois a maioria de seus serviços, tais como: suporte a uma grande gama de granularidade do tráfego, agrupamento dos fluxos em classes (FEC), criação de *tags* que identificam unicamente a FEC específica, roteamento explícito e política de distribuição de rótulos, foram aplicados na padronização do MPLS. A pilha de rótulos é considerada uma das principais inovações oferecida pelo *Tag Switching*. Pois, com a aplicação deste mecanismo, o sistema de roteamento pode ser hierarquizado, sendo cada nível desta hierarquia associado a um rótulo. O *Tag Switching* é uma abordagem orientada a controle, ou seja, a manipulação dos dados na tabela de encaminhamento ocorre sempre que os switches recebem informações sobre fluxo de controle. A seguir, surgiu a abordagem *label switching* implementada pela IBM conhecida como ARIS. Sua estrutura se assemelha mais ao modelo *Tag Switching*. As tabelas de encaminhamento também são configuradas através de um mapeamento orientado a controle. A principal diferença em relação as outras abordagens é o estabelecimento do caminho *label switched* (LSP) a partir do roteador de saída em direção ao roteador de entrada. A identificação dos pontos de saída onde serão criados os LSPs é implementado por um dispositivo especificado como identificador de saída. Além disso, este identificador também

pode oferecer alguns serviços como *multicast*, rotas explícitas e reserva de recursos [22, 24, 36].

Estes diferentes tipos de abordagens levaram a formação de um grupo de trabalho pelo IETF para a construção de uma arquitetura *label switching* chamada MPLS, que padronizou as principais características dos modelos anteriores sobre uma mesma base tecnológica.

O tratamento dos pacotes IP dentro de uma rede MPLS, mostrado na Figura 3.1, procede da seguinte forma: quando um pacote chega na entrada de um domínio MPLS, o roteador de entrada (*Label Switching Edge Router Ingress*) analisa seu cabeçalho e insere um rótulo que está associado ao próximo salto no qual deve ser encaminhado. A ligação FEC-rótulo é gravada na tabela LIB e distribuída via LDP aos seus roteadores vizinhos para que possam indexar o rótulo de entrada com o endereço do próximo salto, através de um novo rótulo. Quando o pacote rotulado é encaminhado para os elementos centrais do domínio MPLS. Ele é recebido pelo LSR que emprega o mecanismo de troca de rótulos (*label swapping*) para atualizar o valor do rótulo do pacote para que seja transportado ao próximo LSR apropriado. A operação de troca de rótulos é repetida enquanto o pacote trafegar no núcleo da rede. Quando o pacote atinge o roteador de saída (*Label Switching Edge Router Egress*), remove-se o rótulo e encaminha o pacote no modo IP convencional ao seu próximo destino [22, 24, 48].

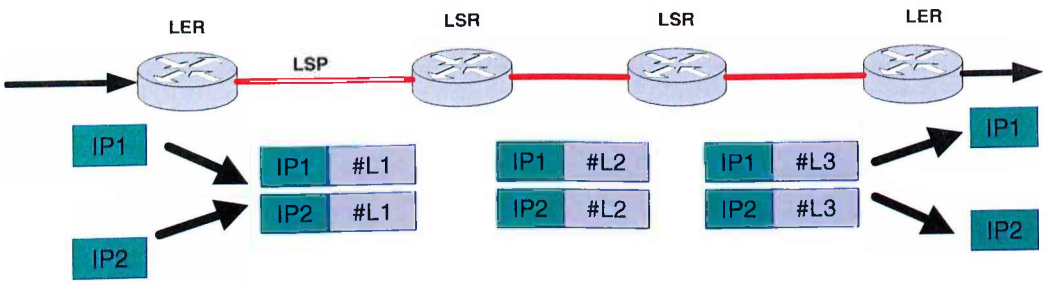


Figura 3.1 – Funcionamento simplificado do MPLS

3.3 Componentes de uma arquitetura MPLS

A arquitetura MPLS é constituída dos seguintes componentes fundamentais: rótulo e FEC, roteadores *Label Switching* (LSR), caminhos *Label Switched* (LSP) e protocolo de distribuição de rótulos. A seguir será apresentado cada um desses componentes, seus mecanismos de funcionamento e suas principais características.

3.3.1 Classe de Equivalência de Encaminhamento e Rótulo

Uma função do plano de encaminhamento de um LSR é particionar o conjunto de todos os pacotes que um roteador possa encaminhar dentro de um número finito de subconjuntos diferentes. A partir daí, os pacotes pertencentes a cada subconjunto são tratados pelo roteador da mesma forma, mesmo que a informação contida no cabeçalho de cada um deles diferir. Estes subconjuntos são denominados Classe de Equivalência de Encaminhamento (FEC) [24].

A razão pela qual um roteador encaminha os pacotes pertencentes a uma determinada FEC, de maneira semelhante, é a questão do mapeamento entre a informação carregada no

cabeçalho desses pacotes e as entradas na tabela de encaminhamento empregar a relação muitos-para-um , como pode ser visto na Figura 3.2 [24].

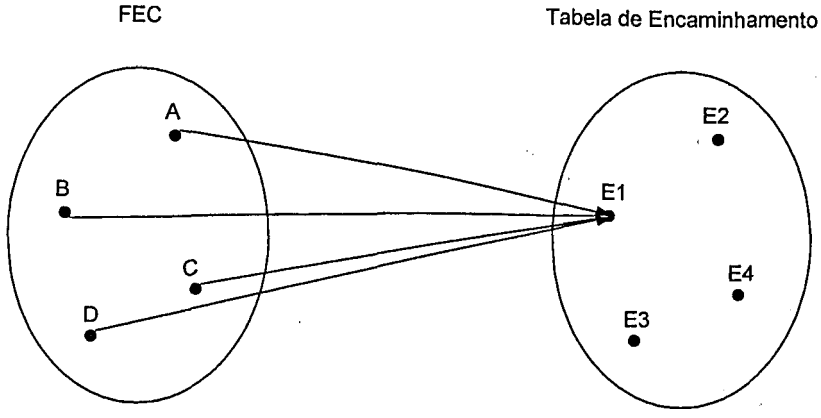


Figura 3.2 – Mapeamento entre os elementos da FEC e as entradas na tabela LIB

Uma propriedade importante da FEC é fornecer granularidade ao processo de encaminhamento. Uma vez que a FEC pode englobar tantos pacotes com um nível de granularidade mais abrangente, por exemplo, agrupar pacotes com um determinado prefixo de endereço destino, quanto em situações onde a granularidade é bastante específica, por exemplo, pacotes que representam uma dada aplicação entre dois computadores. Isto termina possibilitando uma grande faixa de granularidade no encaminhamento dos pacotes e uma melhoria considerável na escalabilidade da rede [08, 24].

A representação física de uma FEC é definida através de uma variável de tamanho fixo, curto e sem estrutura interna conhecida como rótulo [15, 22, 24, 48].

A criação do rótulo torna-se necessária, pois é utilizado como índice na tabela LIB do roteador para indicar o encaminhamento dos pacotes associados a ele. Um rótulo é formado pelos seguintes componentes: rótulo, pilha de rótulo, classe de serviço e TTL.

A forma em que o rótulo será transportado no pacote depende da tecnologia de camada 2 (ATM, *Frame Relay*, PPP, *Ethernet*) empregada. Nas Figuras 3.3 e 3.4 são ilustrados a inserção de rótulos em redes ATM e *Frame Relay* nos campos VPI/VCI e DLCI, respectivamente. No entanto, existem tecnologias (*Ethernet*, PPP, FDDI) que não permitem o uso dos seus cabeçalhos para o transporte do rótulo. Neste caso é criado um cabeçalho de rótulo *Shim* inserido entre os cabeçalhos da camada 2 e 3, como pode ser visto na Figura 3.5 [15, 22, 24, 48].

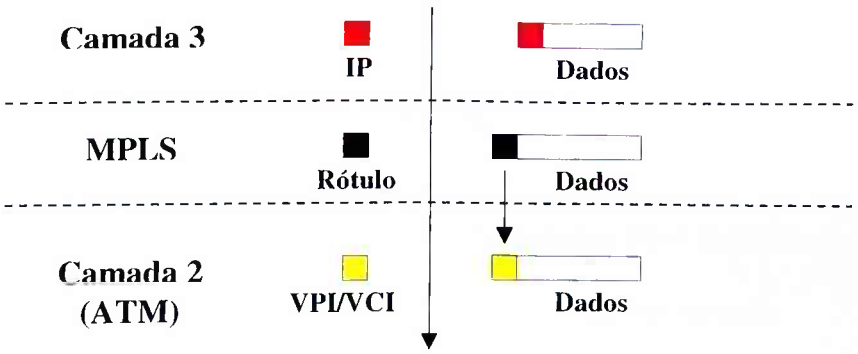


Figura 3.3 - Encapsulamento de um rótulo MPLS em uma célula ATM

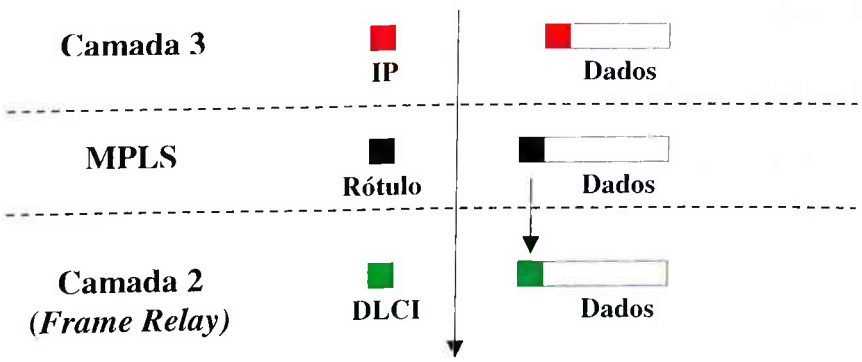


Figura 3.4 - Encapsulamento de um rótulo MPLS em um quadro *Frame Relay*

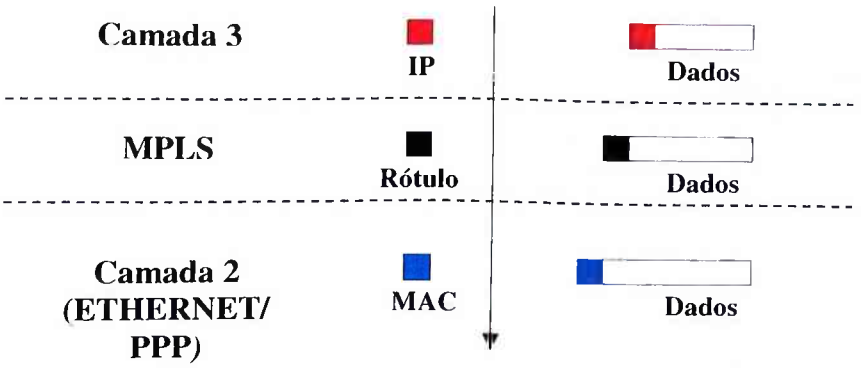


Figura 3.5 - Encapsulamento de um rótulo MPLS em um quadro ETHERNET/PPP

3.3.2 Roteadores *Label Switching*

Como em todo roteador que implementa tecnologia *label switching*, o LSR também é separado em duas partes: plano de encaminhamento e plano de controle.

A principal função do plano de encaminhamento é transmitir os pacotes para o seu próximo destino. A Figura 3.6 simplifica o mecanismo de encaminhamento do LSR. A operação de envio de cada pacote é inteiramente determinada pelo índice pesquisado na tabela LIB, usando o rótulo do pacote (e ás vezes, a identificação da porta de entrada) como chave. O rótulo de entrada é substituído por um novo rótulo (rótulo de saída) que indica o próximo salto do pacote. A seguir, o pacote é enfileirado na porta de saída apropriada para sua transmissão [15, 24, 48].

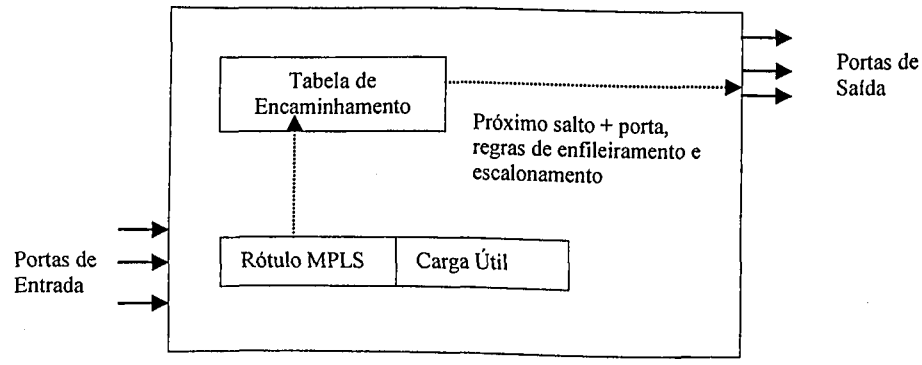


Figura 3.6 – Mecanismo simplificado de encaminhamento de um LSR

A tabela de encaminhamento (LIB) representa um dos elementos fundamentais na estrutura de um LSR. Ela consiste de numa seqüência de entradas, denominada NHLFE, mantidas pelo plano de controle do roteador, onde cada entrada contém um rótulo de entrada e uma ou mais subentradas, como pode ser visto na Figura 3.7. Estas subentradas são compostas por um rótulo de saída, uma porta de saída e o endereço do próximo salto. A tabela de encaminhamento é indexada pelo valor existente no rótulo de entrada. Além disso, ela também pode definir quais recursos podem ser oferecidos aos pacotes [15, 24, 48].

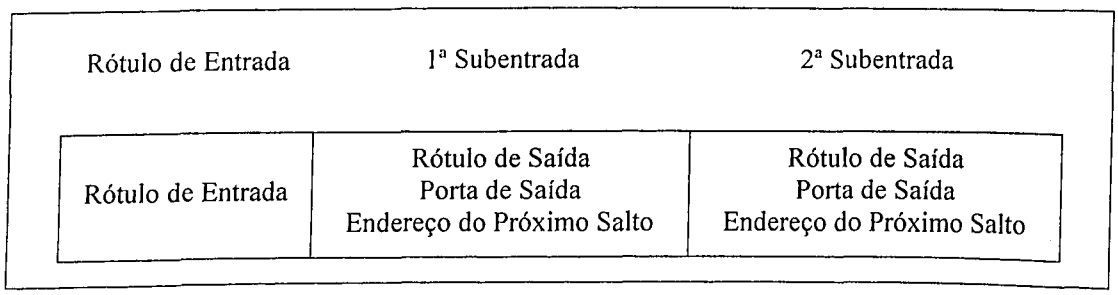


Figura 3.7 – Entrada na tabela LIB

A operação de troca de rótulos executada pelo algoritmo de envio é um dos pontos fundamentais para o sucesso do MPLS. Isto se deve a propriedade que num único acesso à

memória pode ser obtido todas as informações necessárias para encaminhar o pacote, assim como definir quais recursos podem ser oferecidos. Também é importante salientar que o uso deste algoritmo combinado com a capacidade de transportar rótulos em um grande conjunto de tecnologias de camada 2 proporciona que diferentes dispositivos implementem um roteador LSR [22, 24, 48].

O outro mecanismo executado pelo LSR, o plano de controle, limita-se em distribuir as informações de roteamento aos outros roteadores e convertê-las em entradas dentro da tabela de encaminhamento. Para realizar a construção da tabela de encaminhamento, como é mostrado na Figura 3.8, são necessários os seguintes mapeamentos [15, 24, 48]:

1) O mapeamento entre a FEC e o próximo salto é realizado pelos protocolos de roteamento convencionais (OSPF, BGP, RIP) para distribuir as informações de roteamento entre os LSRs;

2) O mapeamento entre a FEC e o rótulo feito através de procedimentos de ligação FEC-rótulo e a distribuição dela para outros roteadores através de um protocolo de distribuição de rótulos;

3) O mapeamento entre o rótulo e o próximo salto que ocorre dentro da tabela de encaminhamento, gerado das ligações FEC-rótulo recebidas e dos endereços próximo salto transportado pelos protocolos de roteamento convencionais.

Além disso, o LSR mantém o mapeamento FTN que associará um pacote rotulado com uma entrada da tabela LIB. O mapeamento torna-se necessário porque podem existir múltiplas entradas para uma FEC na tabela de encaminhamento. Para um determinado pacote, o mapeamento FTN selecionará uma única entrada, mas o mapeamento pode ser alterado por

várias razões, tais como balanceamento de carga sobre múltiplos caminhos ou reroteamento de um caminho obstruído para um caminho alternativo [24].

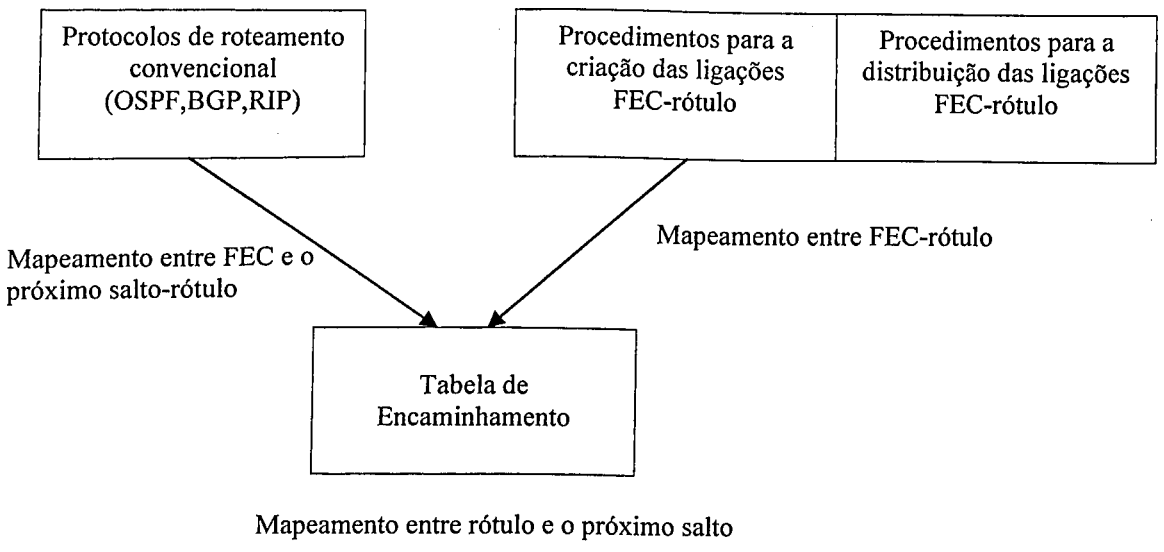


Figura 3.8 – Construção de uma tabela de encaminhamento (LIB).

Em um domínio MPLS, como é ilustrado na Figura 3.9, podem existir três tipos de LSR [48]:

1) LSR de entrada – responsável em receber os pacotes vindos de redes de acesso, dividi-los em FECs, associar cada FEC a sua entrada na tabela LIB (Mapeamento FTN), criar o rótulo que representará a FEC e encapsulá-lo nos pacotes pertencente a ela, distribuir as ligações FEC-rótulo aos outros roteadores e encaminhar o pacote para o núcleo da rede;

2) LSR ou LSR de núcleo – utiliza o algoritmo de envio *label swapping* para substituir o rótulo do pacote que chegou no roteador por um novo rótulo que indicará para onde o pacote deve ser encaminhado;

3) LSR de saída – a principal ação executada por este roteador é remover o rótulo dos pacotes e encaminhá-los para fora do domínio MPLS.

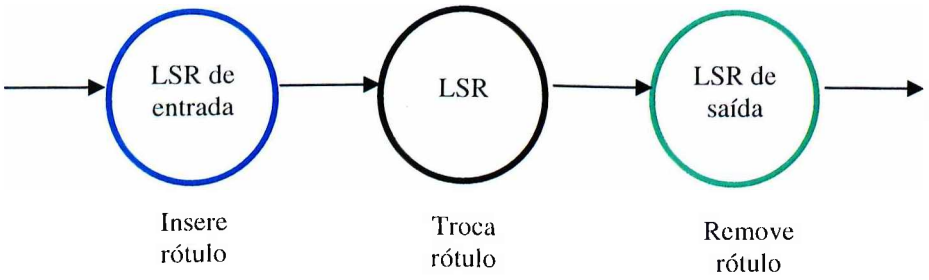


Figura 3.9 – Tipos de LSR em um domínio MPLS

3.3.3 Protocolos de Distribuição de Rótulos

Um outro componente importante da tecnologia *label switching* é o protocolo de distribuição de rótulos. Ele deve distribuir para todos os roteadores do domínio as informações sobre os rótulos.

No MPLS, este componente pode vir encapsulado num protocolo já existente (RSVP [18] e BGP) ou num projeto de protocolo de distribuição de rótulos separado (LDP [05] ou CR-LDP [34]). Esta seção enfocará o protocolo LDP por ser o método padrão para distribuição de rótulos na abordagem MPLS.

Inicialmente, torna-se indispensável introduzir alguns conceitos básicos de um protocolo LDP [05, 48]:

1) Pontos LDP – Roteadores (LSR) que usam LDP para trocar informações sobre rótulo entre eles;

2) Sessão LDP – Representa o momento em que os pontos LDP informam e trocam ligações FEC-rótulos entre eles;

3) LSR *upstream* e LSR *downstream* – Supondo que Ru e Rd estejam trocando informações para criar uma ligação FEC-rótulo para os pacotes enviados de Ru para Rd , como pode ser observado na Figura 3.10. De acordo com esta ligação, Ru é o LSR *upstream*, e Rd é o LSR *downstream*.

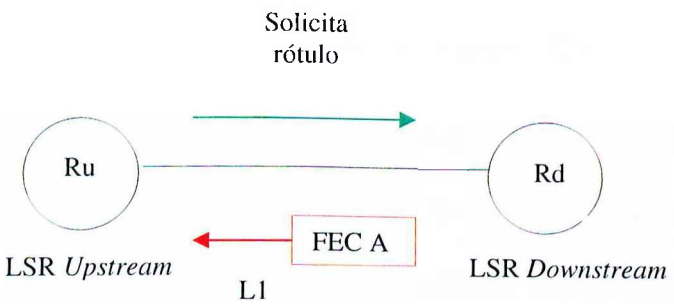


Figura 3.10 - LSR *upstream* e LSR *downstream.*

Como mostra a Figura 3.11, o protocolo LDP é composto de mensagens divididas nas seguintes categorias:

1) Mensagens de Descoberta – informam a presença de LSRs;

2) Mensagens Sessão – estabelecem e mantém sessões LDP;

3) Mensagens Anúncio – criam, alteram e removem as ligações FEC-rótulo;

4) Mensagens Notificação – fornecem informações de erro, diagnóstico e status.

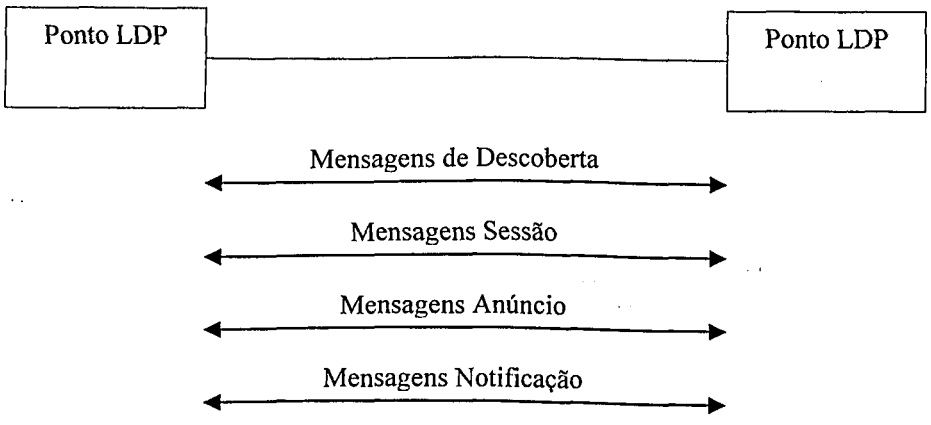


Figura 3.11 – Categorias de mensagens LDP

A Figura 3.12 descreve o seguinte formato para mensagens LDP [05, 15]: o primeiro campo verifica se o roteador reconhece a mensagem recebida, caso contrário, notifica ao transmissor da mensagem o problema ocorrido; o próximo campo identifica o tipo de mensagem enviada pelo LDP; o campo tamanho da mensagem define o tamanho total da mensagem em bytes; o campo identificação fornece um número que representa unicamente uma determinada mensagem; os últimos dois campos representam respectivamente os parâmetros obrigatórios e opcionais da mensagem, sendo suas configurações de acordo com o tipo da mensagem carregada. Geralmente, o LDP utiliza a codificação TLV para implementar os parâmetros obrigatórios e opcionais de uma mensagem LDP.

Bits:	1	15	16	32	Variável	Variável
	U (Mensagem Desconhecida)	Tipo de Mensagem	Tamanho da Mensagem	Identificação da Mensagem	Parâmetros Obrigatórios	Parâmetros Opcionais

Figura 3.12 – Formato das mensagens LDP.

Como pode ser visto anteriormente, o campo tipo de mensagem é o componente fundamental de uma mensagem LDP, pois define em qual categoria a mensagem está

classificada e como configurar os parâmetros obrigatórios e opcionais. A Tabela 3.1 [15] detalha os principais tipos de mensagem que um LDP pode assumir.

Tabela 3.1 – Tipos de Mensagens LDP.

Tipo de Mensagem	**Função**
Hello	Trocar informações entre dois pontos LDP durante a operação de descoberta LDP.
Inicialização	Avisar ao outro ponto LDP que deseja estabelecer uma sessão LDP.
Keep Alive	Manter a continuidade de uma sessão LDP na falta de outras mensagens.
Address	Informar os endereços das interfaces para o outro ponto LDP.
Address Withdraw	Retirar previamente os endereços das interfaces informados pela mensagem *Address*.
Mapping Label	Avisar a um ponto LDP as ligações FEC-rótulo pertencente a ele.
Request Label	Solicitar uma ligação FEC-rótulo a outro ponto LDP.
Label Withdraw	Destruir uma ligação FEC-rótulo anteriormente estabelecida.
Label Release	Liberar uma ligação FEC-rótulo.
Notification	Informar ao outro ponto LDP que ocorreu situações de erro ou anômalas.

Como é apresentada na Figura 3.13, a codificação TLV é definida como um campo de dois octetos que usam 14 bits para especificar o tipo de TLV e 2 bits para o comportamento quando um LSR não reconhece o tipo, seguido por um campo de 2 octetos que define o tamanho do campo valor em bytes e finalmente, um campo de tamanho variável chamado valor que define o tipo de TLV [05, 15].

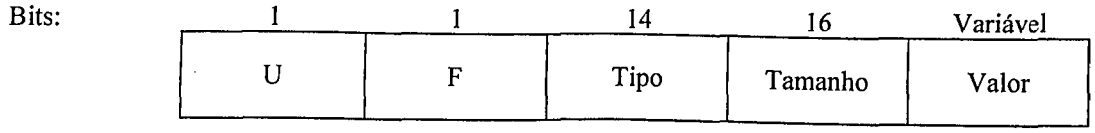


Figura 3.13 – Codificação TLV.

3.3.3.1. Procedimentos para o estabelecimento, manutenção e encerramento de uma sessão LDP

A Figura 3.14 descreve o primeiro passo dado pelos LSRs para estabelecer uma sessão LDP, que é descobrir a presença dos roteadores vizinhos a eles, através de um procedimento de descoberta utilizando mensagens *Hello*. Ao término desta operação cada par de LSRs adjacentes podem iniciar o estabelecimento de uma sessão LDP. Para que isso aconteça, os pontos LDP abrirão uma conexão TCP, como pode ser observado na Figura 3.15, sendo que todas as mensagens LDP exceto mensagens de descoberta usam o TCP como protocolo de transporte por causa das suas características de confiabilidade e segurança, e trocarão mensagens de inicialização para negociar os parâmetros da sessão (versão do protocolo LDP, métodos de distribuição). Como mostra a Figura 3.16, uma sessão LDP está finalmente estabelecida quando existe troca de mensagens *Keep Alive* entre os pontos LDP. Mensagens *Hello* devem continuar sendo trocadas periodicamente para manter o espaço de rótulo e o relacionamento entre os pontos LDP. A ausência de um *Hello* indica que um ponto LDP deseja terminar a sessão ou o ponto "caiu". A partir daí, como é mostrado na Figura 3.17, a sessão LDP é encerrada. Também, na falta de outras mensagens, o *Keep Alive* deve ser enviado regularmente para manter a sessão [05, 15].

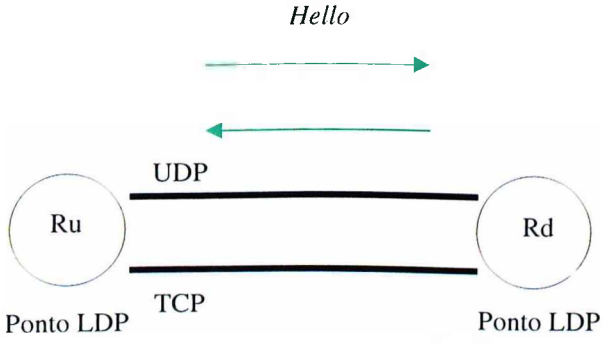


Figura 3.14 - Procedimento de descoberta dos pontos LDP

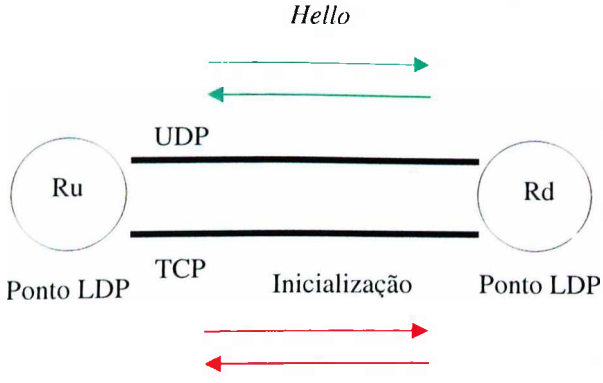


Figura 3.15 - Procedimento para inicialização de uma sessão LDP

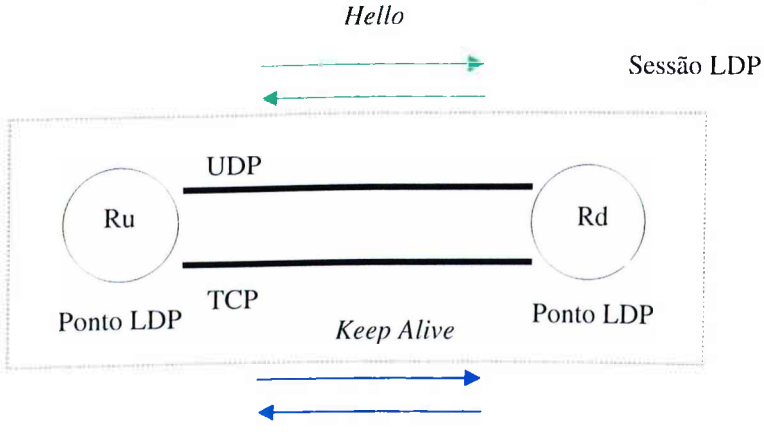


Figura 3.16 - Sessão LDP estabelecida

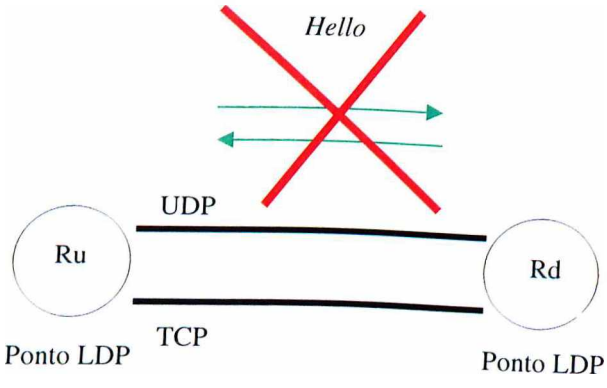


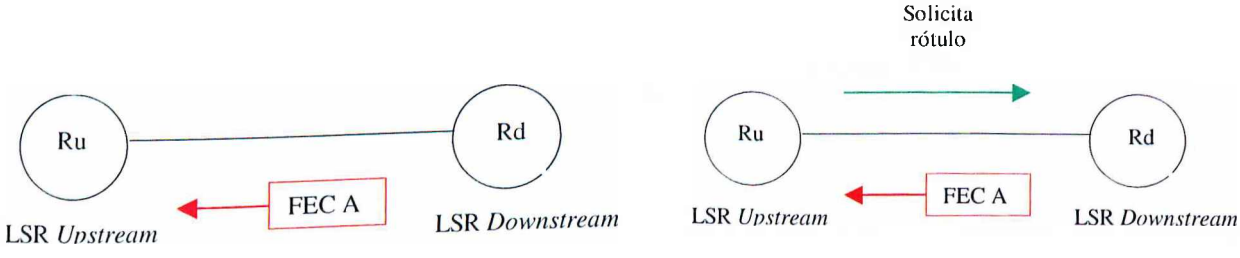
Figura 3.17 - Sessão LDP encerrada

3.3.3.2. Métodos de Distribuição, Controle e Retenção de Rótulo

Durante uma sessão LDP [15, 22, 24, 48], as ligações FEC-rótulo são criadas pelo LSR *downstream* e elas são distribuídas em sentido contrário ao dos pacotes, ou seja, partem do LSR *downstream* em direção ao LSR *upstream*. Esta distribuição pode ser realizada, automaticamente, pelo LSR *downstream* informando seus vizinhos via mensagem *Label Mapping* sem uma solicitação de rótulo, chama-se distribuição de rótulo *downstream* não solicitada; ou sob demanda quando um ponto LDP requisita associação de rótulo de um LSR *downstream* via mensagem *Label Request*, chama-se distribuição de rótulo *downstream* sob demanda. As Figuras 3.18.a e 3.18.b representam os dois métodos de distribuição de rótulo: *downstream* não solicitada e *downstream* sob demanda, respectivamente.

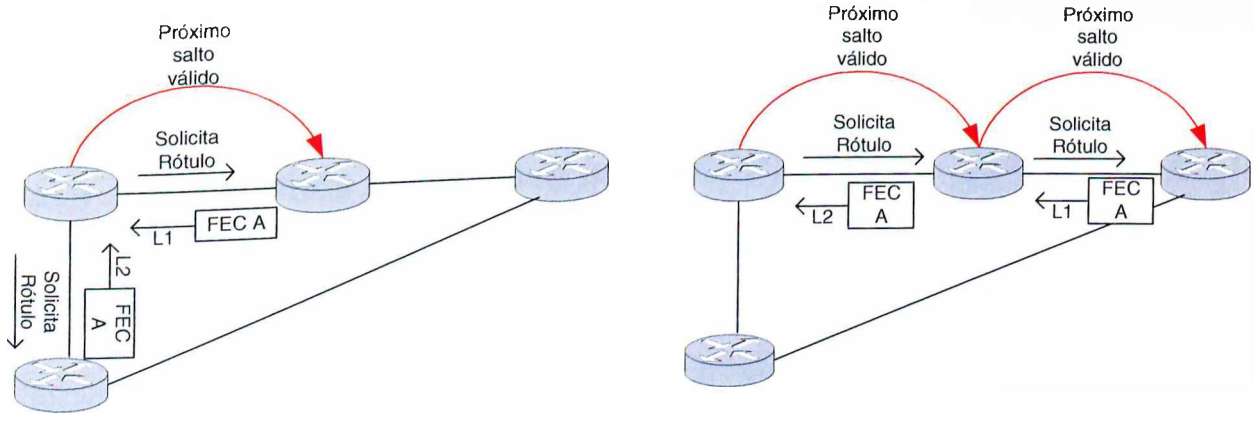
Com relação à forma de controle da distribuição de rótulos, mostrado nas Figuras 3.19.a e 3.19.b, o protocolo LDP pode assumir um modo independente ou um modo ordenado. No controle independente, o roteador toma uma decisão própria para mapear uma ligação FEC-rótulo e distribuí-la aos seus pontos LDP. Enquanto, no modo de controle ordenado, o

mapeamento do rótulo e sua distribuição pelo LSR só acontece se o ponto LDP vizinho seja o próximo salto dele ou roteador de saída do domínio MPLS [15, 22, 24, 48].



(a) *Downstream* não solicitada (b) *Downstream* sobre demanda

Figura 3.18 – Métodos de distribuição de rótulo.



(a) Controle Independente (b) Controle Ordenado

Figura 3.19 – Métodos de controle de distribuição de rótulos.

Conforme ilustrado nas Figuras 3.20.a e 3.20.b, o protocolo LDP pode suportar dois modos de retenção de ligações FEC-rótulo num LSR : modo liberal e modo conservativo. Se um roteador mantêm as ligações FEC-rótulo recebidas de pontos LDP que não são próximo salto da FEC armazenada então se diz que o LSR suporta modo de retenção de rótulo liberal.

Se o roteador está configurado no modo de retenção de rótulo conservativo, ele descarta todas as ligações FEC-rótulo recebidas daqueles roteadores que não são seu próximo salto [15, 22, 24, 48].

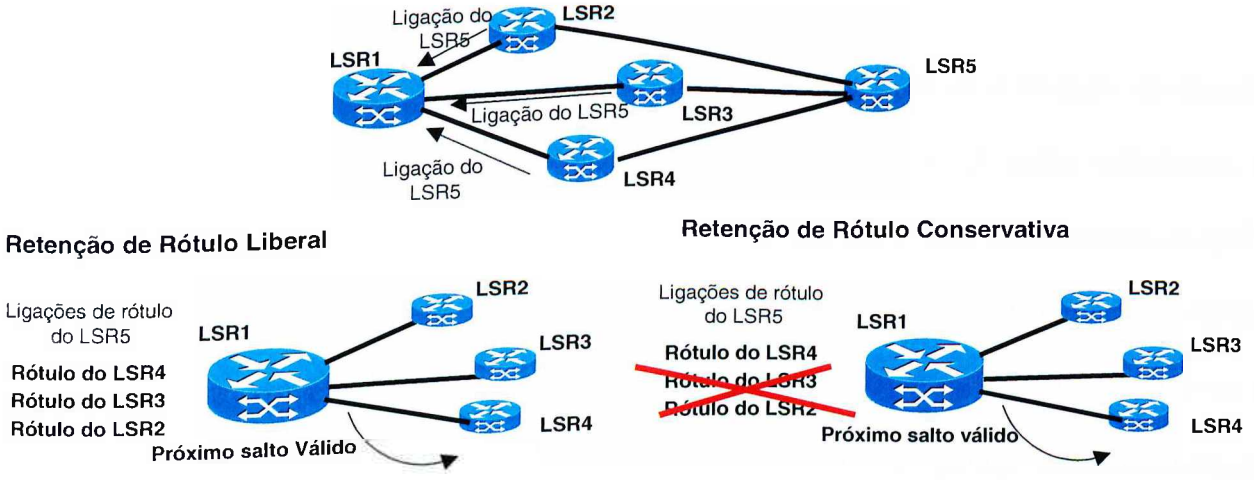


Figura 3.20 – Modos de retenção de rótulo

3.3.4 Caminhos *Label Switching* (LSP)

LSP é uma rota predeterminada que um conjunto de pacotes ligados a uma FEC utilizam para percorrer uma rede MPLS e alcançar seu destino. Cada LSP é unidirecional, assim, o tráfego de volta deve usar um LSP separado [48].

Para o estabelecimento de um LSP, primeiramente, o roteador de entrada envia protocolos de sinalização para configurar a rota a ser utilizada. Esta configuração pode ser feita através de roteamento salto-a-salto, quando cada LSR independentemente seleciona o próximo salto para uma FEC específica, ou roteamento explícito, somente um LSR (o nó de entrada do LSP) designa os roteadores que fazem parte do caminho. Um caminho LSP roteado explicitamente (ER-LSP) permite dois modos de configuração: *strict*, se o LSP foi

especificado completamente por roteamento explícito, e *loose*, quando apenas parte do caminho empregou esta técnica de roteamento. O ER-LSP pode ser uma ferramenta valiosa para suportar tráfego que exige requisitos de QoS e para o provimento de Engenharia de Tráfego [24, 48].

O processo de configuração do LSP transcorre da seguinte forma: o roteador de entrada encaminha uma mensagem *Label Request* em direção ao roteador de saída, solicitando o mapeamento de rótulo para uma determinada FEC para todos os LSRs pertencentes ao LSP. Quando a solicitação chega no roteador de saída, ela é atendida (caso exista recursos disponíveis para supri-la, senão o estabelecimento é cancelado) e enviada de volta para o transmissor desta requisição através de uma mensagem *Label Mapping* para distribuir as ligações FEC-rótulo aos outros LSRs do caminho. Se um LSR intermediário não mapear a ligação FEC-rótulo, o estabelecimento também pode ser encerrado. Ao atingir o roteador de entrada, o processo de configuração está completo. A seguir, os pacotes são encaminhados pelo caminho construído [24, 48].

A construção e encerramento de um LSP podem pertencer a dois estados. Se o caminho só permanece estabelecido enquanto está sendo utilizado, ele é considerado um LSP *soft-state*. Caso contrário, o caminho continua estabelecido, mesmo estando em estado ocioso e somente é liberado quando houver mudanças de roteamento ou mudanças na topologia da rede, o LSP está num estado *hard-state* [22, 24].

Ainda, com relação ao estabelecimento de um LSP. Ele pode ser ativado de duas formas: abordagem orientada a dados, se um tráfego de dados seja detectado na entrada de uma rede MPLS, inicia-se o processo de criação do caminho; e abordagem orientada a

controle, o LSP é ativado quando alguma informação de controle (atualizações de roteamento OSPF, mensagens PATH/RESV do RSVP) seja detectada [22, 24].

3.3.5 Procedimentos para Encaminhamento de pacotes em uma rede MPLS

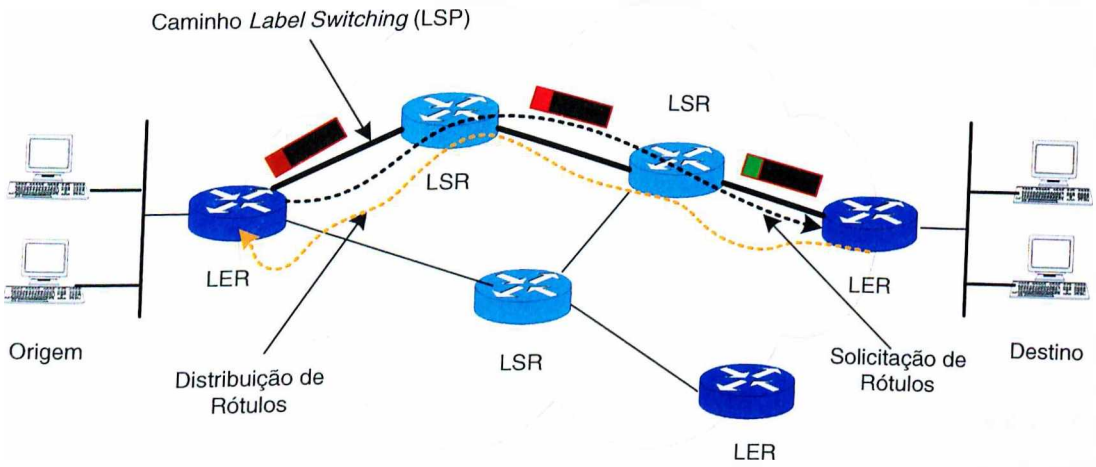


Figura 3.21 – Procedimentos para Encaminhamento de pacotes em uma rede MPLS

Como mostra a Figura 3.21, os seguintes passos devem ser tomados por um tráfego de dados para viajar através de um domínio MPLS [31]:

1) Criação e distribuição do rótulo – Antes de qualquer tráfego ser encaminhado, o roteador de entrada divide-o em FECs e solicita o mapeamento de rótulo para cada uma das FECs nos LSRs pertencentes a rota solicitada. Quando a ligação FEC-rótulo é construída pelos LSRs *downstream*, partindo do roteador de saída. Eles respondem a solicitação dos LSRs *upstream* com a distribuição das ligações para eles. Assim, o processo de distribuição de rótulos transcorre em sentido contrário ao processo de solicitação de ligações nos roteadores do LSP.

2) Criação da tabela de encaminhamento em cada LSR – Com as ligações de rótulo sendo recebidas, cada LSR cria entradas na tabela de encaminhamento (LIB) que especificam o mapeamento entre um rótulo e uma FEC. As entradas são atualizadas sempre que ocorrer renegociação das ligações.

3) Criação da LSP – O LSP é configurado para o encaminhamento de um pacote específico baseando-se na FEC. Por isso, a relação binária entre uma FEC e um LSP, geralmente, é um-para-um. O cálculo da rota pode ser feito independentemente por cada roteador quando o pacote chega nele (roteamento salto-a-salto) ou roteador de entrada determina os roteadores pertencentes ao caminho até a saída do domínio MPLS (roteamento explícito). Depois que o modo de roteamento foi escolhido, o ponto inicial (LER) do LSP implementa algum protocolo de sinalização (RSVP, LDP) para estabelecer o caminho.

4) Encaminhamento dos pacotes – Logo que, o LSP está construído, o roteador de entrada pode iniciar o encaminhamento dos pacotes pela rede MPLS. Primeiro, ele analisa o cabeçalho do pacote IP convencional e de acordo com as informações contidas nele é especificado um rótulo. A seguir, o pacote rotulado é enviado ao próximo salto no interior do domínio MPLS. Cada roteador intermediário (LSR) examinará o rótulo do pacote recebido e o substitui pelo rótulo de saída, acessado na tabela de encaminhamento a partir do rótulo de entrada e encaminha-o para o seu próximo salto. Quando o pacote rotulado alcança o roteador de saída, o rótulo dele é removido e o pacote é encaminhado ao destino desejado.

3.4 Aplicações MPLS

A tecnologia MPLS é uma poderosa ferramenta para o provimento de Engenharia de Tráfego, pois o uso do ER-LSP contribui para a diminuição do problema de caminhos sobrecarregados/subtilizados. Uma vez que o tráfego pode ser mais bem distribuído pelos ER-LSPs através da rede, fugindo daqueles caminhos críticos com relação ao consumo de banda passante.

Um importante aspecto do MPLS é sua capacidade de operar sobre redes ATM, um conceito chamado *overlay*. Esta aplicação propicia a integração de operações IP e ATM em único switch, em vez de executar IP no roteador e ATM num switch *backbone*. Esta integração não é uma tarefa fácil, mas a tecnologia MPLS procura oferecer alguns serviços (circuitos virtuais, rótulos ATM, circuitos virtuais permanentes) semelhantes ao ATM para auxiliar na interoperabilidade de uma rede IP sobre ATM [15].

MPLS também permite a configuração de redes privadas virtuais (VPN – *Virtual Private Network*). VPNs são canais de transmissão de dados com alto nível de segurança empregado por empresas para conectar as matrizes com as filiais ou com outros parceiros comerciais. Devido à fragilidade de segurança existente na Internet, o recurso mais utilizado pelas empresas para implementar VPN são linhas de comunicação privadas. Com o MPLS, uma VPN pode ser implementada na arquitetura Internet empregando o serviço de emulação de uma rede orientada a conexão, uma característica presente no MPLS, ou então configurando os LSRs nas redes dos usuários para serem o início e o final das LSPs. Como o LSP é construído sobre regras semelhantes de um circuito virtual ATM, o nível de segurança oferecido é alto [31].

3.5 Conclusões

O MPLS é considerado uma tecnologia promissora devido à simplicidade de seu mecanismo de encaminhamento, que permite aos pacotes serem enviados em uma velocidade muito maior do que a arquitetura IP tradicional pode oferecer. Isto se deve ao procedimento de troca de rótulos presente nos roteadores LSR que possibilita ao cabeçalho IP tradicional ser analisado somente uma vez para a criação do rótulo, depois substitui o rótulo recebido pelo LSR por um rótulo de saída na tabela de encaminhamento que indique o próximo salto do pacote.

Uma outra vantagem desta tecnologia é auxiliar na integração do IP e da comutação ótica num único dispositivo que comute e roteie oticamente, trabalhando no surgimento da nova geração de sistema de roteamento baseada puramente em encaminhamento ótico.

Além disso, o MPLS é considerado um modelo de serviço escalável, pois como o modelo DiffServ, a complexidade desta arquitetura se concentra nas bordas. Visto que, os roteadores de borda são responsáveis pela criação, inserção e remoção dos rótulos dentro dos pacotes IP encaminhados no domínio. Sendo assim, pode-se aumentar a quantidade de roteadores de núcleo (LSR's), que não afeta no desempenho da rede, pois os LSR's somente atualizam o valor do rótulo encapsulado em cada pacote.

O MPLS será uma importante ferramenta no oferecimento de QoS em redes IP. Contudo, é importante salientar que a estrutura do MPLS não oferece QoS. Para que isso aconteça, torna-se necessário utilizar o modelo de serviço CBR, pois com a funcionalidade do CBR em também selecionar caminhos baseados em parâmetros de QoS. Os LSP's construídos

pelo MPLS poderão oferecer especificações de QoS determinadas pelo usuário. Este assunto será tratado com mais abrangência no Capítulo 4.

Capítulo 4

Roteamento Baseado em Restrição

4.1 Introdução

A arquitetura Internet se baseia num paradigma de roteamento cujas principais características são: calcular a rota, otimizando algumas métricas escalares da rede (número de saltos, caminho mais curto) e encaminhar os pacotes segundo um modelo de encaminhamento orientado ao nó destino. Contudo, na atualidade, a exigência por partes dos usuários por redes que ofereçam QoS, fez surgir um novo tipo de roteamento, muito utilizado em aplicações de Engenharia de Tráfego, chamado Roteamento Baseado em Restrição ou Roteamento QoS. O diferencial existente neste roteamento, quando comparado com o roteamento IP tradicional, é o cálculo da rota não levar em conta, apenas as métricas escalares, mas também um conjunto de restrições impostas pelo tráfego. Uma outra novidade é a utilização do roteamento explícito para determinar como os pacotes devem ser encaminhados. Essas novas funcionalidades permitem que alguns parâmetros de QoS sejam atendidos pelas redes onde são aplicados.

O objetivo deste Capítulo é procurar descrever como o roteamento baseado em restrição pode ser uma ferramenta valiosa no provimento de QoS em uma rede MPLS. Assim, ele

começa definindo o conceito de roteamento baseado em restrição. A seguir, os componentes de um CBR são mostrados. Encerrando o Capítulo 4, são apresentadas as principais aplicações do CBR.

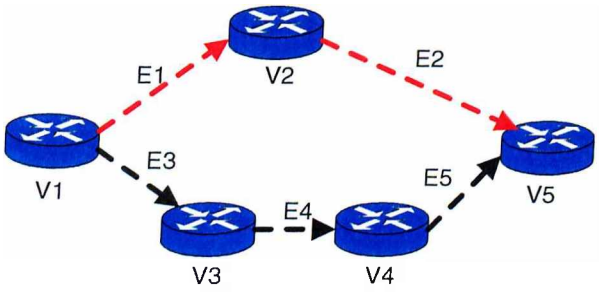
4.2 Definição de Roteamento Baseado em Restrição

Para entender o conceito de CBR, primeiramente, será apresentado como é o funcionamento de um sistema de roteamento tradicional implementado nas redes IP, como pode ser observado na Figura 4.1. A Internet é composta por um conjunto de sistemas autônomos (AS) interligados, onde as rotas dentro de um sistema autônomo são especificadas pelo roteamento intra-AS e rotas que interligamos vários sistemas autônomos são especificadas pelo roteamento inter-AS [24]. Para o restante deste capítulo, quando o termo roteamento IP for citado, será considerado o roteamento intra-AS, pois o CBR age nele.

O cálculo de uma rota para qualquer protocolo de roteamento intra-AS (RIP, OSPF, IS-IS) baseia-se num algoritmo que busca otimizar uma determinada métrica escalar.

Formalmente, o CBR pode ser definido da seguinte maneira: Considere uma rede sendo representada pelo grafo (V, E), onde V é um conjunto de nós e E é um conjunto de enlaces que ligam estes nós. Associado com cada enlace está um conjunto de atributos. Para cada par de nós no grafo, ocorre um conjunto de restrições que devem ser satisfeitas pelos nós do início ao fim do enlace. As restrições deste conjunto estão expressas em termo de atributos dos enlaces e geralmente só é conhecida pelo nó origem do caminho [24]. O objetivo do roteamento baseado em restrição é calcular uma rota que ligue o nó origem ao nó destino, de

modo a otimizar a métrica escalar definida pelo protocolo de roteamento e ao mesmo tempo, não violar as restrições definidas para atingir certos requisitos de QoS. Uma vez calculado o caminho, o CBR é responsável por estabelecer e conservar o estado de encaminhamento ao longo do caminho.



		Atributo
		Banda Passante
Enlaces	E1	1Mb/s
	E2	1Mb/s
	E3	2Mb/s
	E4	2Mb/s
	E5	2Mb/s

Rota calculada pelo roteamento IP

Rota calculada pelo roteamento CBR

Cálculo da rota

m – métrica escalar do protocolo intradomínio
r – restrição
s – nó origem
d – nó destino
IPR(s, d, m) – a rota calculada pelo roteamento IP
CBR(s, d, m, r) – a rota calculada pelo roteamento baseado em restrição

IPR(V1, V5, nº de saltos) = V1→ V2 → V5
CBR(V1, V5, nº de saltos, banda passante = 2Mb/s) = V1 → V3 → V4 → V5

Figura 4.1 – Representação e cálculo de uma rota utilizando Roteamento IP e Roteamento Baseado em Restrição.

Como uma das principais razões para a implementação do CBR foi a necessidade de um roteamento que suportasse qualidade de serviço. Apareceu uma outra questão, podia um sistema de roteamento IP suportar o CBR? Mostrou-se que não. Já que, existem algumas características técnicas que impedem esse funcionamento. A principal delas é a exigência do

cálculo da rota ser executado no nó origem, uma vez que diferentes nós origens podem ter diferentes restrições para o caminho, mesmo tendo um nó destino semelhante e além disso, as restrições associadas ao nó origem são conhecidas somente por ele. Ao contrário, no roteamento IP, a rota é calculada de forma distribuída por todos os nós da rede, como também, não é levado em conta no cálculo as restrições dos diferentes nós origem. Uma outra dificuldade é como encaminhar os pacotes através do caminho calculado, considerando que no roteamento IP, cada nó da rede verifica qual é o próximo salto para onde os pacotes devem ser enviados, de acordo com o endereço IP de destino, encaminha-os e continua repetindo estas operações até alcançar o nó destino. Este mecanismo de encaminhamento repete o mesmo problema do cálculo da rota ao permitir a cada nó da rede encaminhar os pacotes segundo o seu critério, podendo assim, violar a rota calculada no nó origem. Por isso, torna-se necessário utilizar roteamento explícito para solucionar esta deficiência. Finalmente, para que o nó origem possa executar o cálculo da rota, ele deve tomar conhecimento sobre os atributos relacionados a cada enlace da rede. Desta forma, deve existir um protocolo de roteamento que leve essas informações para ele. Entretanto, o roteamento IP não oferece protocolos que carreguem esses dados [15, 24].

As restrições apresentadas anteriormente não indicam que o roteamento IP não possa ser melhorado e passe a oferecer novas funcionalidades características do CBR. Como também, nada impede que possamos implementar um sistema de roteamento combinando os dois métodos e assim, possa satisfazer uma diversidade de aplicações.

4.3 Componentes do Roteamento Baseado em Restrição

Para entender quais serviços adicionais devem ser introduzidos no sistema de roteamento IP para que suporte o CBR, vamos relembrar os principais mecanismos [15, 24] necessários para suportar CBR.

1) O cálculo da rota deve ser feito na origem. Além disso, deve considerar não somente as métricas escalares, que são utilizadas como um critério de otimização, mas também um conjunto de restrições que não devem ser violadas.

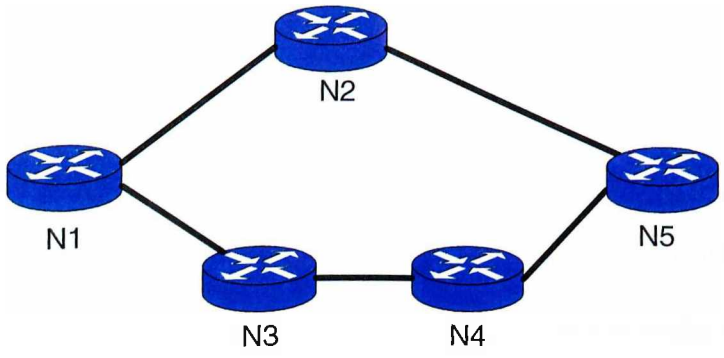
2) Distribuir a informação sobre a topologia da rede e os atributos relacionados aos enlaces através da rede. Para que, o cálculo da rota possa representar fielmente o estado da rede.

3) Uma vez a rota calculada torna-se necessário um mecanismo de encaminhamento que suporte roteamento explícito.

4) O estabelecimento da rota calculada deve reservar recursos ao longo da rota, de modo, a satisfazer as exigências do tráfego que vai utilizá-la . Como também, alterar os valores dos atributos do enlaces pertencentes a rota, modificados pela reserva de recursos

4.3.1 *Constrained Shortest Path First*

Como foi mostrado anteriormente, o cálculo da rota feito pelo roteamento baseado em restrição busca otimizar alguma métrica escalar e satisfazer um conjunto de restrições imposta pelo tráfego.



Iteração	Lista de Nós Candidatos	Árvore de Caminho mais Curto
1	N2 N3	N1
2	N3 N5	N1 N2
3	N3	N1 N2 N5

Figura 4.2 – Primeiro caminho mais curto entre os nós 1 e 5.

Uma forma de atingir estes objetivos é utilizar o algoritmo de caminho mais curto (SPF), modificado para atender o conjunto de restrições. Por isso, o novo algoritmo é chamado *Constrained Shortest Path First*.

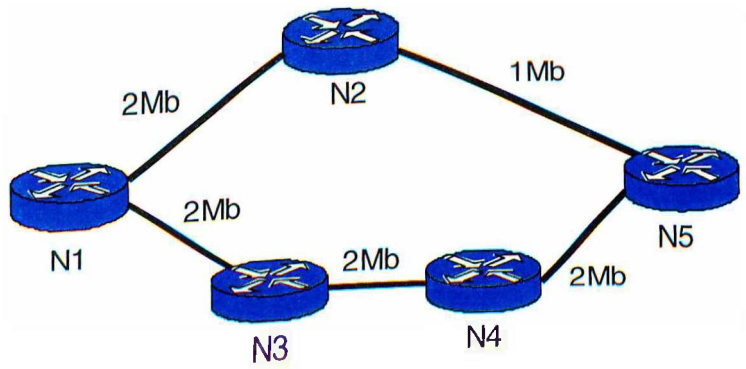
Para entender como o SPF deve ser modificado para levar em conta as restrições, torna-se necessário descrever o funcionamento do algoritmo SPF, mostrado na Figura 4.2. Inicialmente, o algoritmo SPF considera o nó origem como sendo a raiz da árvore de caminho mais curto e os nós adjacentes à raiz são inseridos numa lista de nós candidatos. Depois entre os nós existentes na lista de nós candidatos, procurem aquele mais próximo da raiz (segundo a

métrica utilizada pelo SPF). O nó escolhido será inserido na árvore do caminho mais curto e removido da lista de nós candidatos. A partir daí, a cada iteração examine os nós vizinhos ao último nó inserido na árvore do caminho mais curto, insira-os na lista de nós candidatos, selecione o nó da lista que está mais próximo a partir da raiz, insira-o na árvore e remova-o da lista. Estas operações se repetem até a lista de nós candidatos esteja vazia, quando deseja-se encontrar o caminho mais curto da raiz a todos os outros nodos, ou quando o nó destino é inserido na árvore SPF, neste caso, procura-se encontrar o caminho mais curto até um determinado nó destino [15, 24].

Apresentado o mecanismo de SPF, será abordada a partir deste parágrafo, a modificação realizada no algoritmo original para transformá-lo em CSPF. Como ilustra a Figura 4.3, a principal mudança a ser realizada, foi à introdução do conjunto de restrições como parâmetros para a escolha do nó mais próximo da raiz na lista de nós candidatos. Sendo assim, quando se escolhe o nó candidato a ser inserido na árvore do caminho mais curto não basta selecionar o nó mais próximo da raiz, mas também que satisfaça as restrições especificadas [15, 24].

Note que a utilização do algoritmo CSPF para o cálculo da rota, obriga o roteador de origem ter informações sobre todos os enlaces na rede. Isto, por sua vez, impõe uma restrição no tipo de protocolo de roteamento a ser usado. Os protocolos de roteamento de vetor de distância não podem ser utilizados por causa das seguintes limitações [15, 24] :

- Cada roteador envia informação de roteamento somente para os seus vizinho;
- A informação enviada é uma estimativa do seu custo do caminho para todas as redes.
- A informação é enviada a cada período regular;



Iteração	Lista de Nós Candidatos	Restrições	Árvore de Caminho mais Curto
1	N2 N3	Banda passante = 2Mb	N1
2	N3 N5	Banda passante = 2Mb	N1 N2
3	N4 N5	Banda passante = 2Mb	N1 N3 N2
4	N5	Banda passante = 2Mb	N1 N3 N2 N4
5	Vazia	Banda passante = 2Mb	N1 N3 N2 N4 N5

Figura 4.3 – Primeiro caminho mais curto com restrição (CSPF) entre os nós 1 e 5.

O mecanismo de "inundação" existente nos protocolos de roteamento de estado de enlace, juntamente com o conteúdo da informação distribuída que representa o custo do enlace, possibilita a utilização do mesmo para o CBR.

4.3.2 Serviço de Roteamento Explícito do MPLS

Como foi mencionado anteriormente, um dos mecanismos-chave para suportar o CBR é o roteamento explícito. Segundo [15], o roteamento explícito é "uma rota configurada na borda da rede, segundo um critério de QoS e informação de roteamento". Para oferecer este serviço será utilizado o serviço de roteamento explícito do MPLS.

As razões para escolher o MPLS são as seguintes [15, 24, 48]:

1) O MPLS permite separar a informação utilizada para o encaminhamento (um rótulo) de uma informação carregada no cabeçalho IP;

5) O mapeamento entre uma FEC e um LSP está completamente confinado no roteador do inicio da LSP. Em outras palavras, a decisão por qual rota explícita encaminhar os pacotes IP, se restringe ao roteador que calcula a rota.

Como qualquer outro serviço MPLS, o roteamento explícito pode ser dividido em dois componentes : controle e encaminhamento. O componente de controle fica responsável em estabelecer o estado de encaminhamento ao longo da rota explícita. Para estabelecer o estado de encaminhamento podem ser executados dois protocolos de sinalização: RSVP melhorado e CR-LDP, ambos serão estudados no decorrer deste capítulo. O componente de encaminhamento aplica o caminho estabelecido pelo componente de controle para encaminhar os pacotes através da rota explícita [48].

4.3.3 Protocolos de Sinalização MPLS

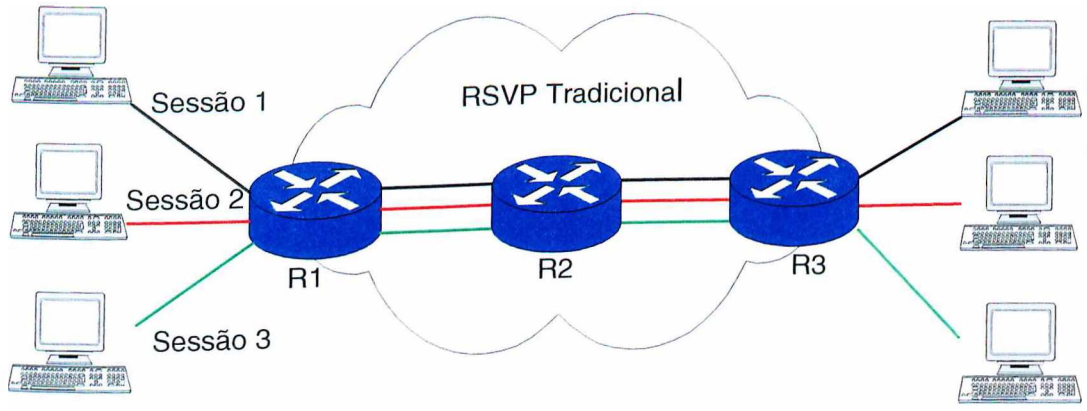
Uma vez calculado o caminho com CSPF, o próximo passo a ser executado é estabelecer o estado de encaminhamento através do caminho, como também reservar os recursos solicitados. Existem dois protocolos de sinalização MPLS responsáveis por esta função: RSVP melhorado [13] e CR-LDP [34]. A seguir, o mecanismo de funcionamento de cada um dos protocolos será apresentado.

4.3.3.1 RSVP Melhorado (RSVP-TE)

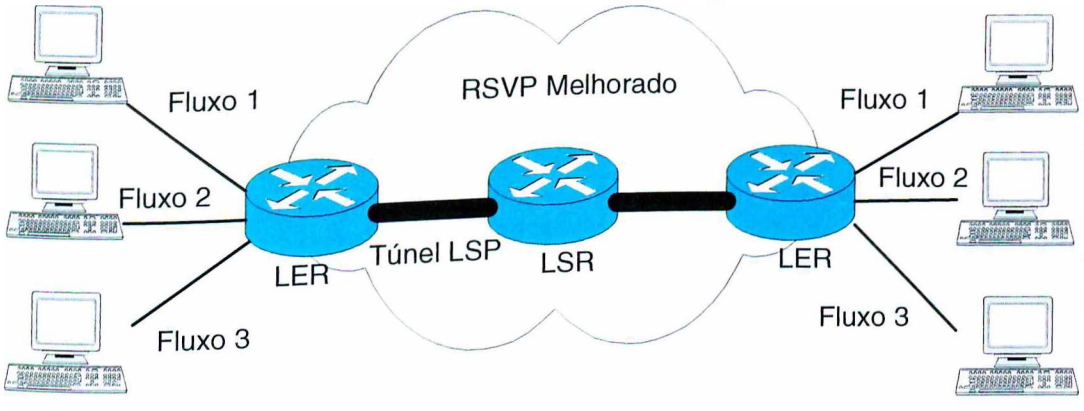
Para começar a especificação do protocolo RSVP-TE, inicialmente, será interessante distinguir os aspectos fundamentais entre a especificação RSVP-TE e o protocolo original RSVP [18], como pode ser observado na Figura 4.4.

A primeira diferença é o fato que o protocolo RSVP-TE é utilizado pelos LSR´s para estabelecer e conservar o caminho LSP. Além de reservar recursos da rede para o tráfego a ser transmitido. A especificação RSVP original, por outro lado, é utilizada pelos *hosts* para solicitar e reservar recursos da rede para microfluxos [13, 23, 35].

A segunda diferença diz respeito à especificação RSVP-TE generalizar o conceito de "fluxo RSVP" [13, 23, 35]. A especificação RSVP-TE, essencialmente, permite uma sessão RSVP ser composta por uma agregação arbitrária de tráfego entre o nó origem e o nó destino do LSP. Enquanto, no protocolo RSVP original, uma sessão RSVP é composta por um fluxo de dados com um determinado destino e protocolo de transporte.



(a) Protocolo RSVP tradicional



(b) Protocolo RSVP melhorado

Figura 4.4 – RSVP tradicional x RSVP melhorado

Para o CBR, as principais funções exercidas pelo RSVP-TE são estabelecer o caminho de acordo com a rota explícita definida e reservar os recursos da rede ao longo do LSP [24]. Por isso, entre os novos objetos introduzidos no protocolo RSVP melhorado, aqueles com maior destaque para o CBR são: o objeto rota explícita (ERO) que define o caminho a ser percorrido, e os objetos *label* e *request-label*, ambos são essenciais para o estabelecimento do LSP. A seguir será feita uma breve descrição do protocolo RSVP melhorado.

A construção de um LSP através do protocolo RSVP melhorado aciona basicamente dois tipos de mensagens. A mensagem RSVP PATH é transmitida pelo LSR de entrada, no sentido origem-destino, até o LSR de saída. O nó destino responde a mensagem RSVP PATH recebida transmitindo uma mensagem RSVP RESV, no sentido destino-origem até o LSR de entrada. Quando o nó da origem recebe a mensagem RESV, o LSP está construído e o tráfego já pode ser encaminhado ao seu nó destino [13, 23, 35].

Para estabelecer uma LSP com CBR, torna-se necessário inserir o objeto ERO na mensagem PATH. O objeto ERO pode ser inserido para especificar um caminho predefinido para o LSP através da rede. Quando ERO está presente, a mensagem PATH é transmitida, no sentido do roteador de saída, ao longo da rota especificada pelo ERO, independentemente do roteamento IP tradicional. No ponto de vista da codificação, objeto ERO é uma seqüência de triplas (tipo, tamanho, valor), onde cada tripla descreve um nó abstrato. A cada nó abstrato está associado um bit que identifica o tipo de roteamento explicito, livre ou restrito. A Figura 4.5 ilustra como cada nó abstrato é codificado no objeto ERO [13, 23, 35].

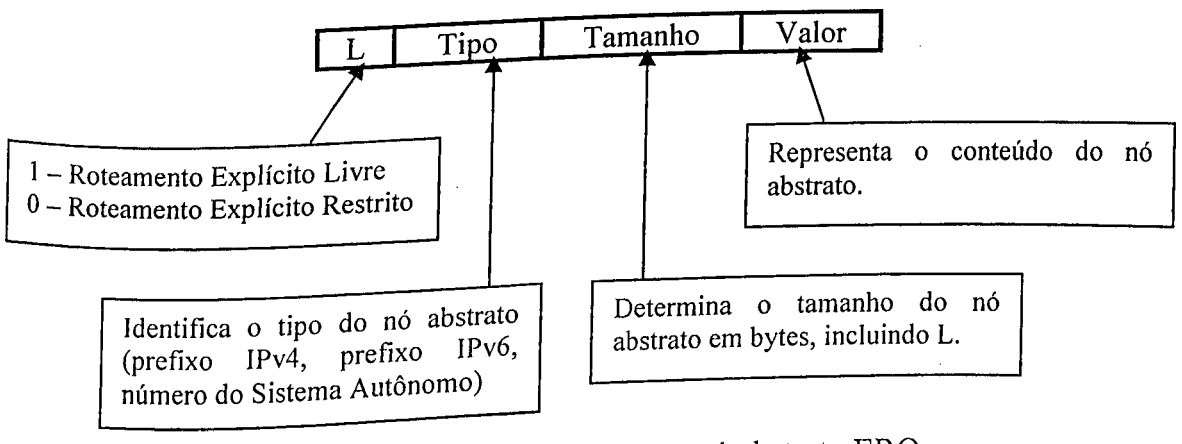


Figura 4.5 – Codificação de um nó abstrato ERO.

Como mostra a Figura 4.6, o estabelecimento de um caminho LSP com CBR utilizando RSVP melhorado segue os seguintes passos [13, 23, 35, 48]:

1) O roteador de entrada, LSR1, determina que é preciso configurar um novo LSP até o LSR3. O LSR1 constrói uma mensagem PATH com uma rota explícita de (2,3) e as especificações dos parâmetros de tráfego solicitado pela nova rota. Depois, LSR1 encaminha PATH ao LSR2 como um datagrama IP;

2) LSR2 recebe a mensagem PATH, determina que não é a saída para este LSP, e a envia ao longo da rota especificada na solicitação. Ele modifica a rota explícita na mensagem PATH e passa para LSR3.

3) LSR3 descobre que é a saída para este novo LSP. A seguir, determina a partir dos parâmetros de tráfego solicitado quanto de banda passante é necessário reservar e aloca os recursos requeridos. Em seguida, seleciona um rótulo para o novo LSP e o distribui para LSR2 na mensagem RESV, que também contém os detalhes de reserva requeridos para o LSP.

4) LSR2 recebe a mensagem RESV e liga-o a solicitação original através do LSPID contido em ambas as mensagens (PATH e RESV) do protocolo RSVP melhorado. Depois, determina quais recursos reservar a partir dos detalhes na mensagem RESV, aloca um rótulo para o LSP, configura a tabela de encaminhamento e passa o novo rótulo para LSR1.

5) O processamento no LSR1 é similar, mas não tem que alocar um novo rótulo e nem encaminhar isto para um LSR anterior já que é o roteador de entrada para o novo LSP.

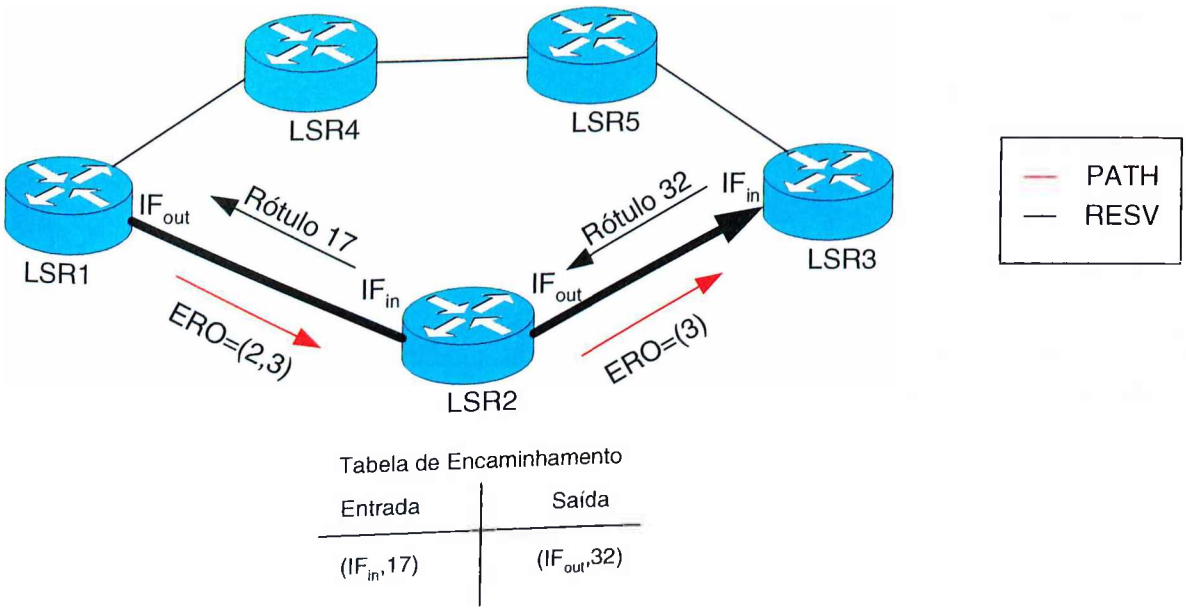


Figura 4.6 – Estabelecimento de um LSP com o protocolo RSVP melhorado

4.3.3.2 CR-LDP (*Constraint Routed Label Distribution Protocol*)

Um outro protocolo utilizado para o estabelecimento de LSP é o LDP [05]. Apesar de ser o protocolo nativo na arquitetura MPLS [48], quando se deseja implementar caminhos LSP´s com roteamento baseado em restrição, surgem duas limitações que o impossibilita de suportar CBR [24]. A primeira limitação é a ausência de um mecanismo de roteamento explícito nas mensagens LDP. A outra limitação diz respeito à reserva de recursos ao longo da rota, não existe esta operação no protocolo LDP. A partir dessas limitações levantadas, foram feitas modificações no LDP para atender esses novos requisitos, surgindo assim, o protocolo CR-LDP [34].

Para atender o requisito de rota explícita foi introduzido na mensagem LABEL REQUEST do CR-LDP, o objeto *Explicit Route*. A composição deste objeto é uma seqüência de triplas (tipo, tamanho, valor) que indicam os saltos da rota explícita ao longo do caminho.

Como pode ser percebido, a estrutura deste objeto é semelhante ao objeto ERO do protocolo RSVP melhorado [34, 15]. A codificação deste objeto é descrita na Figura 4.7 [34, 15] mostrada abaixo.

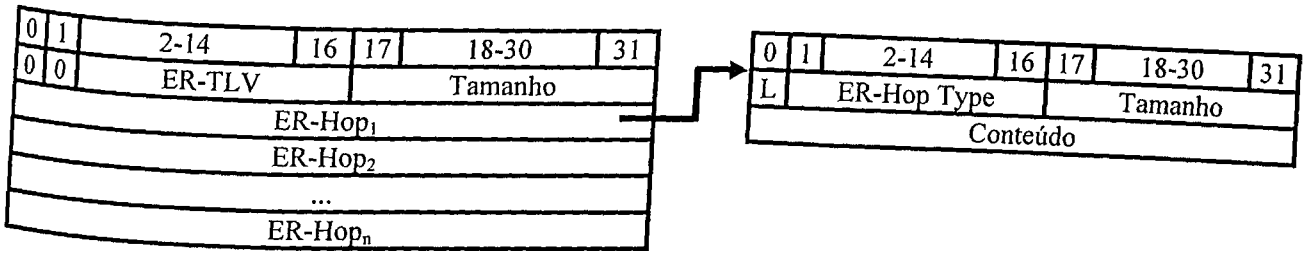


Figura 4.7 – Codificação do Objeto *Explicit Route*.

0	1	2-14	16	17	18-30	31
0	0	*Traffic Parameter* TLV		Tamanho		
Flags		Frequência		Reservado	Peso	
Peak Data Rate (PDR)						
Peak Burst Size (PBS)						
Committed Data Rate (CDR)						
Committed Burst Size (CBS)						
Excess Burst Size (EBS)						

Figura 4.8 – Codificação do Objeto *Traffic Parameter*.

Com relação ao requisito de reserva de recursos para o tráfego a ser transmitido no LSP, um novo objeto chamado *Traffic Parameter* é introduzido tanto na mensagem LABEL REQUEST quanto na mensagem LABEL MAPPING. Este objeto também é uma tripla (tipo, tamanho, valor), onde os valores dele são parâmetros ligados ao tráfego. A codificação do objeto *Traffic Parameter* é mostrada na Figura 4.8 [34, 15]. As especificações CR-LDP [34, 15] definem os seguintes parâmetros de tráfego:

- *Peak Data Rate*

- *Peak Burst Size*
- *Committed Data Rate*
- *Committed Burst Size*
- Freqüência
- Peso

A taxa máxima de tráfego, configurada pelo CR-LDP num caminho, é definida em função de uma estrutura conhecida como balde de permissões de taxa máxima (BPTM), onde o parâmetro CDR define a taxa máxima de entrada de permissões no balde e a quantidade máxima de permissões contida pelo balde é especificada pelo parâmetro PBS [34, 15].

O mecanismo de funcionamento do BPTM segue os seguintes procedimentos [34, 15]:

1) Inicialmente, o balde está cheio (isto é, o contador de permissões *Cp* no instante 0 é igual PBS). Depois disso, se o contador *Cp* estiver menor que PBS então o balde permite a entrada de PDR permissões por segundo.

2) Quando um pacote de *B* bytes chega em um tempo *t*, o balde faz as seguintes operações [34, 15]:

   - Se $Cp(t)-B >= 0$, o pacote não está sendo excedendo a taxa máxima do balde e decrementa *B* permissões do contador *Cp* até o valor mínimo 0, senão;
   - O pacote violou a taxa máxima do balde e o contador *Cp* não é decrementado.

A taxa comprometida de tráfego utiliza dois baldes de permissão para configurar esse parâmetro no estabelecimento do LSP. O primeiro balde é ajustado pelos parâmetros CDR, que indica a taxa comprometida de entrada de permissões no balde e CBS, que especifica a quantidade comprometida de permissões contida pelo balde. No outro balde continua-se utilizando o parâmetro CDR e para configurar a quantidade máxima de permissões do balde utiliza-se o parâmetro EBS [34, 15].

Para entender, como os baldes ajustam a taxa comprometida de tráfego, a seguir será apresentado o funcionamento deles [34, 15]:

1) Os baldes C e E estão cheios (isto é, o contador de permissões do balde C, *Pc* é igual a CBS e o contador de permissões do balde E, *Pe*, é igual a EBS, ambos no instante 0);

2) Se o contador *Pc* é menor que CBS, então o balde C permite a entrada de CDR permissões por segundo, senão se o contador *Pe* é menor que EBS então o balde E permite a entrada de CDR permissões por segundos.

3) Quando um pacote de *B* bytes chega em um tempo *t*, o balde C verifica se $Pc(t)$-$B >= 0$, caso seja verdadeiro, o pacote não violou a taxa comprometida do balde C e decrementa B permissões do contador *Pc* até o valor mínimo de 0. Caso contrário o balde E é ativado e testa a condição $Pe(t)$-$B >= 0$. Caso a condição seja satisfeita, o pacote violou a taxa comprometida, mas não excedeu a quantidade máxima de permissões do balde, EBS. O contador *Pe* é decrementado B permissões. Entretanto, se nenhuma das condições forem satisfeitas ($Pc(t)$-$B >= 0$ ou $Pe(t)$-$B >= 0$), o pacote excedeu tanto a taxa

comprometida quanto o EBS. Sendo assim, nenhum dos contadores de permissão são decrementados.

O parâmetro de freqüência indica, aproximadamente, um intervalo de tempo sobre o qual um LSP leva a fornecer uma banda passante disponível maior ou igual ao CDR. O parâmetro peso é usado para especificar o quanto de banda passante extra acima do total de CDR de todos os LSP´s deve ser dividido entre LSP´s que compartilham um mesmo enlace congestionado [34, 15].

Um outro componente do objeto *Traffic Parameter* é o campo flag que indica se um determinado parâmetro de tráfego é negociável [34, 15].

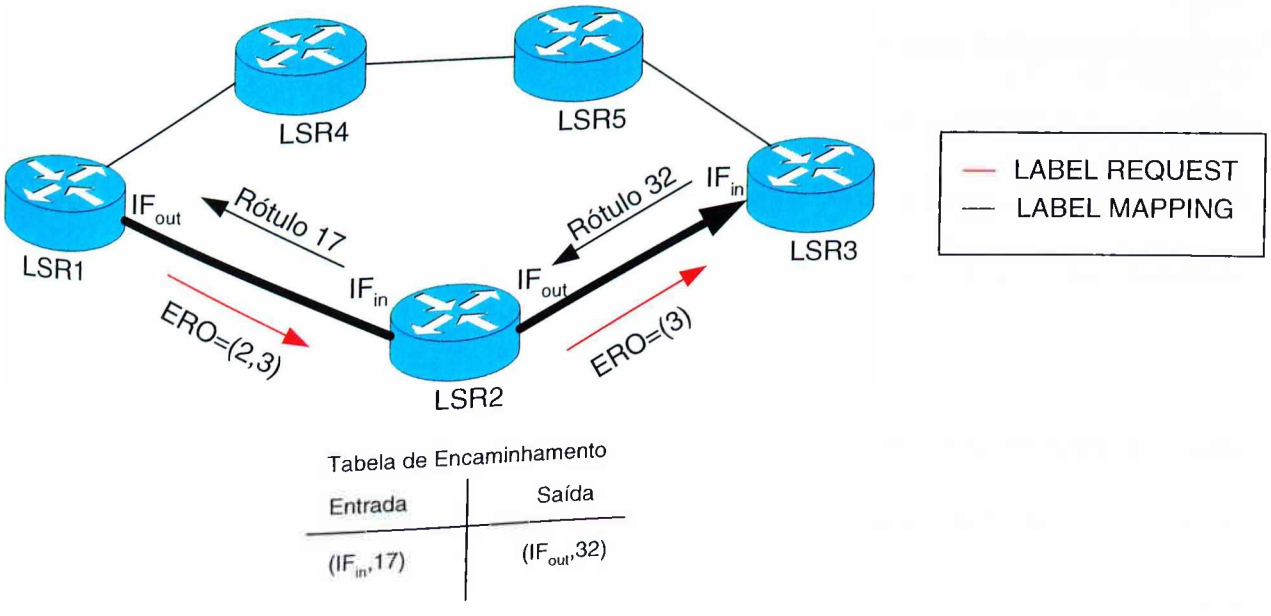


Figura 4.9 – Estabelecimento de um LSP com o protocolo CR-LDP

Como ilustra a Figura 4.9, o protocolo CR-LDP estabelece um LSP com CBR da seguinte forma [34, 15, 24, 48]:

1) O roteador de entrada, LSR1, indica que precisa configurar um novo LSP até LSR3. Os parâmetros de tráfego requerido pela sessão ou políticas administrativas da rede habilitam o roteador de entrada a determinar que a rota para o novo LSP deve ser através do LSR2. O LSR1 constrói uma mensagem LABEL-REQUEST com uma rota explícita (LSR2, LSR3) e os detalhes dos parâmetros de tráfego requerido pela nova rota. LSR1 reserva os recursos que precisa para o novo LSP e, depois, encaminha a mensagem LABEL-REQUEST até LSR2 sobre um sessão TCP.

2) LSR2 recebe a mensagem LABEL-REQUEST, determina que não é a entrada para este LSP, e encaminha a solicitação ao longo da rota especificada na mensagem. Ele reserva os recursos solicitados para o novo LSP, modifica a rota explícita na mensagem LABEL-REQUEST e transmite a mensagem para LSR3. Se necessário, LSR2 pode reduzir a reserva feita para o novo LSP, se os parâmetros apropriados estiverem marcados "negociável" no LABEL-REQUEST.

3) LSR3 determina que é a saída para este novo LSP. Ele executa qualquer negociação final sobre os recursos e faz a reserva para o LSP. Depois, aloca um rótulo para o novo LSP e distribui o rótulo para LSR2 utilizando a mensagem LABEL-MAPPING, que contém os detalhes dos parâmetros finais de tráfego reservado para o LSP.

4) LSR2 recebe a mensagem LABEL-MAPPING e liga-o a solicitação original através do LSPID contido em ambas as mensagens LABEL-REQUEST e LABEL-MAPPING.

5) O processamento em LSR1 é similar, mas não tem que alocar um rótulo e transmiti-lo para um LSR *upstream* por que ele é o roteador de entrada para o novo LSP.

4.3.4 Protocolos de Roteamento Intradomínio de Estado de Enlace (OSPF e IS-IS) Melhorado

O algoritmo CSPF assume que o nó, onde é processado, tem informação não só sobre o estado (ativado/desativado) de todos os enlaces na rede mas também a respeito de outros atributos dos enlaces, como a banda passante disponível, permitindo ao nó verificar se um determinado enlace violou as restrições associadas ao caminho calculado [24].

Para satisfazer este requisito, os protocolos de estado de enlace sofreram algumas modificações para carregar outras informações sobre os enlaces. Como já foi comentada na Seção 4.3.1, a principal razão em utilizar os protocolos de estado de enlace para distribuir informações pela rede é o mecanismo de "inundação" presente neles. Este mecanismo possibilita distribuir os atributos relacionados aos enlaces para todos os nós da rede, fazendo com que o nó origem calcule a rota respeitando tanto as métricas escalares quando as restrições.

Detalhes de como a informação sobre os atributos do enlace está codificada são especificações de protocolo e podem ser encontradas em [15] e [30]. Com o OSPF, esta

informação é carregada no objeto *Opaque Link-State Advertisement*. Com o IS-IS esta informação é carregada pelos pacotes *Link-State*. Em ambos os casos, a informação é codificada como um conjunto de objetos TLV, onde cada objeto transporta informação ligada a um determinado atributo.

Uma outra função do mecanismo de inundação é informar à todos os nós da rede sobre qualquer mudança que ocorra em um determinado enlace. Contudo, se qualquer mudança que houver nos atributos de um enlace resultar em "inundação" desta informação através da rede, isso pode ocasionar um aumento excessivo na quantidade de atualizações de roteamento, que por sua vez, pode sobrecarregar o componente de controle dos roteadores envolvidos na "inundação". Uma forma de amenizar este problema é definir limites suportados pelos enlaces, onde o mecanismo de inundação só é ativado quando atinge estes limites [24].

4.3.5 Aplicações

As principais aplicações do CBR são engenharia de tráfego, reroteamento rápido e qualidade de serviço. Como o objetivo principal desta pesquisa é especificar como o modelo MPLS/CBR pode prover QoS em uma rede IP, o enfoque desta seção será em cima das aplicações para QoS.

A engenharia de tráfego busca otimizar a utilização dos recursos disponíveis e o desempenho da rede, de modo que o tráfego seja distribuído de maneira uniforme pelos enlaces [15].

Qualquer solução para o provimento da engenharia de tráfego em uma rede deve satisfazer duas condições [15]:

1) Estabelecer rotas que sejam otimizadas de acordo com uma determinada métrica escalar e;
2) Levar em conta a banda passante disponível sobre os enlaces a serem percorridos;

Estes são, exatamente, os serviços que podem ser fornecidos pelo CBR, onde a restrição utilizada é a banda passante disponível. Mais informações podem ser encontradas em [15] .

Outra aplicação do CBR é oferecer o serviço de reroteamento rápido. Quando em um caminho estabelecido, algum enlace e/ou roteador "cai", o roteamento sobre esses pontos desativados entram em *loop* até que ocorra o reroteamento do tráfego que atravessava esses pontos para outros nós em funcionamento. Este evento é chamado como reroteamento rápido. Com o roteamento IP convencional, o tempo necessário para rerotear o tráfego dos nós desativados e conseqüentemente, recalcular as tabelas de encaminhamento dos roteadores sobre o novo caminho produz uma perda de pacotes significativa. Isto se deve diretamente ao roteamento IP ser baseado em um roteamento salto a salto e ao encaminhamento orientado ao destino [06, 24].

Por sua vez, o CBR tem como componente o roteamento explícito que soluciona as limitações do roteamento em IP em oferecer um reroteamento rápido com baixa perda de pacotes. O CBR faz isso construindo ao redor dos enlaces um caminho de "proteção". Quando algum enlace falha, o roteador *upstream* ligado ao enlace desativado utiliza o serviço de pilha de rótulos [48] do MPLS para "aninhar" todas as rotas que costumam percorrer o enlace desativado dentro do caminho de proteção.

Normalmente, o mecanismo de roteamento é implementado de forma separada das técnicas de QoS. Por exemplo, os modelos IntServ [17] e DiffServ [16] tomam decisões de alocação de recursos independentemente da rota calculada. Isto por sua vez, pode acarretar que um caminho calculado pelo SPF (roteamento) não satisfaça as solicitações de QoS, em algum ponto de rota. O CBR é aplicado na construção de caminhos com garantias de QoS pela sua característica de calcular o novo caminho levando em conta métricas de roteamento (SPF) e QoS (banda passante disponível, tamanho de buffer) [24].

Para o CBR construir caminhos com garantia de QoS, um mecanismo de controle de admissão é implementado através de filas que controlam os recursos locais de cada nó ao longo do LSP. Por esta razão, o parâmetro tamanho do buffer juntamente com a banda passante disponível são as principais restrições utilizadas no cálculo de um caminho.

4.4 Conclusões

O roteamento baseado em restrições é um passo além do roteamento IP convencional porque, além de minimizar algumas métricas administrativas, o CBR também seleciona caminhos que satisfaçam uma ou mais restrições. As restrições mais comuns incluem a banda passante disponível ao longo do caminho e restrições administrativas.

Um sistema de roteamento baseado em restrição é construído a partir de um conjunto de componentes. O primeiro é a seleção do caminho, que é referida como CSPF. O segundo é o mecanismo de encaminhamento o qual utiliza-se o MPLS. A seguir, um mecanismo de estabelecimento de LSP que forneça suporte ao roteamento explícito; RSVP e CR-LDP são duas opções para este componente. Finalmente, os protocolos de estado de enlace (OSPF e IS-

IS) sofreram algumas modificações para distribuir outras informações sobre os enlaces, além de identificar seu estado (ativado/desativado).

CBR tem inúmeras aplicações. Provavelmente, a mais conhecida é a Engenharia de tráfego - capacidade de controlar como o tráfego é roteado em uma rede de forma a otimizar a utilização dos recursos. Uma outra aplicação é o reroteamento rápido, que é a capacidade de responder rapidamente aos enlaces e nós desativados, roteando ao redor deles. Finalmente, o CBR pode ser combinado com técnicas de QoS para fornecer LSP com banda passante garantida.

Capítulo 5

Avaliação de Desempenho de uma rede MPLS-CBR para provimento de QoS

5.1 Introdução

Para validar a solução MPLS/CBR como um modelo de serviço que oferece QoS, torna-se necessário implementar uma rede real com essa estrutura e monitorar os parâmetros de QoS no encaminhamento de pacotes gerados por aplicações de tempo real e elástica. Contudo, o custo financeiro desta implementação pode ser muito alto, visto que se precisa adquirir equipamentos com essas características ou implementá-los e a resposta a esses investimentos pode ser muito baixa, então surge uma alternativa de avaliação de desempenho de uma rede através de estudos baseados em simulação.

A técnica de simulação baseia-se em uma abstração do sistema real, chamado modelo de um sistema, onde é capturado para o modelo o comportamento "essencial" do sistema real, descartando as características julgadas irrelevantes do sistema. Com a construção desse modelo, são injetados valores de testes nas suas entradas e com as saídas obtidas é avaliado o comportamento do modelo do sistema para uma determinada situação. É importante salientar que a correspondência direta entre as saídas do modelo e do sistema pode não ser possível

devido às simplificações feitas quando da modelagem. É principalmente por esta razão que um estudo baseado em simulação é freqüentemente aplicado para determinar tendências no comportamento do sistema modelado ao invés de obter valores reais para suas saídas. Exatamente por isso, os resultados obtidos em estudos baseados em simulações devem ser associados a intervalos de confianças, para determinar o nível de confiabilidade das saídas.

Os estudos baseados em simulações apresentadas neste capítulo procurarão mostrar a viabilidade de se utilizar um mecanismo de roteamento baseado em restrição juntamente com a tecnologia MPLS no estabelecimento de caminhos com requisitos de QoS garantida. Este objetivo é atingido comparando-se o desempenho de uma rede IP convencional, de uma rede MPLS, do CBR implementado em conjunto com o MPLS em uma rede com o mesmo ambiente e condições de tráfego semelhantes. As simulações foram feitas utilizando os mesmos fatores para todos os experimentos.

A implementação do CBR juntamente com o MPLS proporciona a seleção de rotas calculadas através de métricas escalares (primeiro caminho mais curto) e restrições ou requisitos de QoS (largura de banda disponível, tamanho de *buffer* disponível). Como também, protocolos de sinalização (RSVP-TE [13] e CR-LDP [34]) que estabelecem caminhos e reservam recursos em cada nó percorrido pelo caminho estabelecido, permitindo a construção de LSP's com Qualidade de Serviço garantida. Isto permite um passo importante para fazer com que uma rede *backbone* tenha certas garantias de qualidade de serviço, através de uma arquitetura simplificada e confiável.

5.2 Simulação de um Modelo de uma Arquitetura MPLS/CBR para Provimento de QoS

5.2.1 Descrição do Modelo

Como mostra a Figura 5.1, o modelo de rede a ser simulado é constituído por:

- Um domínio MPLS/CBR, onde existem: dois roteadores de borda *label switching* (LER), que inserem (LER de entrada) e removem (LER de saída) rótulos aos pacotes que entram e saem da rede MPLS, e um roteador intermediário *label switching* que só encaminha os pacotes rotulados;
- Dois domínios IP que representam redes de acesso que injetam e recebem pacotes no domínio MPLS/CBR;
- Quatro fontes de tráfegos UDP que querem: serviço de melhor esforço (fonte SBT), serviço de melhor esforço com alta prioridade (fonte HBT) e serviço de tempo real (fontes RT1 e RT2). SBT e HBT geram um tráfego com uma taxa de envio igual à 250 kbps. RT1 e RT2 geram tráfegos com as seguintes taxas de envio, respectivamente, 350 kbps e 450 kbps. A escolha desses serviços para o ambiente de simulação é para criar um cenário que envolva os principais tipos de serviço existente na Internet.
- Todos os enlaces do modelo simulado possuem 1 Mbits/s de largura de banda, exceto o enlace que liga o nó pertencente à rede de acesso 1 ao LER de Entrada da

rede *backbone*, cuja largura de banda é igual a 2 Mbits/s. A existência de um enlace com capacidade mais alta do que o restante da rede é utilizada para criar um cenário de "gargalo" e verificar como a rede gerencia os diferentes tipos de serviço sob esta situação. Além disso, cada enlace apresenta um atraso no encaminhamento dos pacotes de 10 ms.

A topologia "halteres" foi utilizada para construção do modelo pela sua característica de representar sistemas finais que estão conectados a roteadores, os quais se conectam a roteadores de um nível maior que agrega tráfego de vários outros. Isso ocorre sucessivamente até atingir o "gargalo" da rede, representado geralmente por um enlace de capacidade muito inferior aos demais [37].

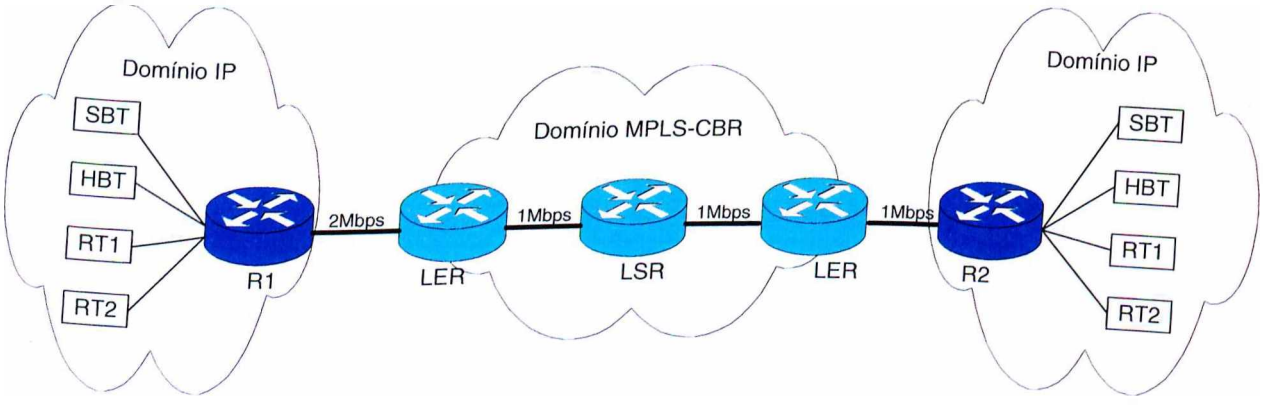


Figura 5.1 – Modelo de uma arquitetura MPLS/CBR para provimento de QoS.

Apresentam-se nas Tabelas 5.1 e 5.2, alguns parâmetros e considerações relacionadas às simulações:

Tabela 5.1 – Parâmetros utilizados nas simulações

	Domínio IP1	Domínio MPLS	Domínio IP2
Quantidade de roteadores IP	1	-	1
Quantidade de LERs	-	2	-
Quantidade de LSRs	-	1	-
Banda passante dos enlaces	2 Mbps	1 Mbps	1 Mbps
Tipos de Filas implementadas pelos roteadores	FIFO ou *Droptail*	CBQ	FIFO ou *Droptail*
Atraso apresentado por cada enlace	10 ms	10 ms	10 ms
Tempo de simulação	45s, sendo que os tráfegos HBT, SBT e RT1 começam e encerram o envio de pacotes, respectivamente, nos instantes 1 e 40 segundos. Já, o tráfego RT2 inicia no instante 11 s e cessa aos 30 s o envio dos pacotes.		
Intervalo dos pacotes UDP	0,005 s		

Tabela 5.2 – Fatores ligados ao Roteamento Baseado em Restrição/MPLS

Quesito	Fator Utilizado
Limite das Filas CBQ para todos os tipos de serviço (HBT, SBT, RT e ST)	10
Tipo de Fila do Escalonador de Pacotes	WFQ
Peso definido pelo Escalonador de Pacotes para cada fila CBQ	▪ Fila CBQ para o Tráfego SBT – 0.1 ▪ Fila CBQ para o Tráfego HBT – 0.05 ▪ Fila CBQ para o Tráfego RT – 0.8 ▪ Fila CBQ para o Tráfego ST – 0.05
Protocolo de Sinalização para o Estabelecimento do LSP	CR-LDP
Tipo de LSP	▪ ER-LSP para os tráfegos SBT e HBT ▪ CR-LSP para os tráfegos RT1 e RT2

O interesse está em avaliar o desempenho de uma arquitetura MPLS/CBR, de acordo com os principais parâmetros de QoS na Internet (retardo fim-a-fim, variação de retardo ou *jitter* e vazão) [37].

5.2.2 Descrição dos Simuladores

A implementação do modelo de rede proposto, conforme é visto na Figura 5.1, foi desenvolvida sobre uma plataforma LINUX utilizando os softwares de simulação: *Network Simulator* versão NS-2.1b6 [41], e MPLS *Network Simulator* versão 2.0 [40], um *patch* criado na Universidade de Chungnam – Coréia com o objetivo de simular redes MPLS no NS2.

O NS2 é um programa simulador bastante utilizado para estudo de protocolos sobre redes com ou sem fio, roteamento *unicast* e *multicast* [41]. Utiliza-se ainda da linguagem OTCL para a implementação de topologia de redes e demais necessidades em uma simulação e as diversas classes de objetos pré-definidas, ou construídas na linguagem de programação C++. Além disso, o NS2 gera saídas na forma de arquivos *trace*, bem como saídas no terminal e oferece suporte a uma ferramenta de animação denominada *Network Animator*. O NAM utiliza os arquivos *traces* gerados pelo NS2 para apresentar a visualização da simulação [41]. Uma outra forma de visualização da simulação gerada pelos arquivos *trace* é utilizando softwares geradores de gráficos, como o GNUPLOT [28].

Para implementar caminhos LSP's com garantias de qualidade de serviço, o MNS 2 utiliza o protocolo CR-LDP para o estabelecimento de LSP's com roteamento baseado em restrição (CR-LSP) e para a reserva de recursos no caminho estabelecido para o tráfego a ser encaminhado.

Para que a rede MPLS suporte tráfego com qualidade de serviço, o MNS 2 implementa dois componentes, o classificador de serviços, que fica residente no roteador LSR, e o escalonador de pacotes, que fica na entrada de cada enlace. A Figura 5.2 [3] mostra o

processamento de um tráfego com qualidade de serviço no roteador LSR e no enlace. Quando um pacote MPLS chega no roteador LSR, busca na tabela LIB o rótulo e a interface de saída correspondente ao rótulo de entrada que carrega. A seguir, inicia uma busca na tabela ERB para conseguir o *Service ID*, que indica a classe de serviço a qual pertence o pacote. De acordo com a classe que o pacote pertence e a interface de saída, o componente classificador de pacotes enfileira no *buffer* correspondente da fila baseada em classes (CBQ). Depois, os pacotes ficam enfileirados nas filas do CBQ, na entrada de cada enlace conectado ao LSR, esperando o componente escalonador de pacotes selecionar qual fila dentro do CBQ encaminha pacotes para o enlace [3].

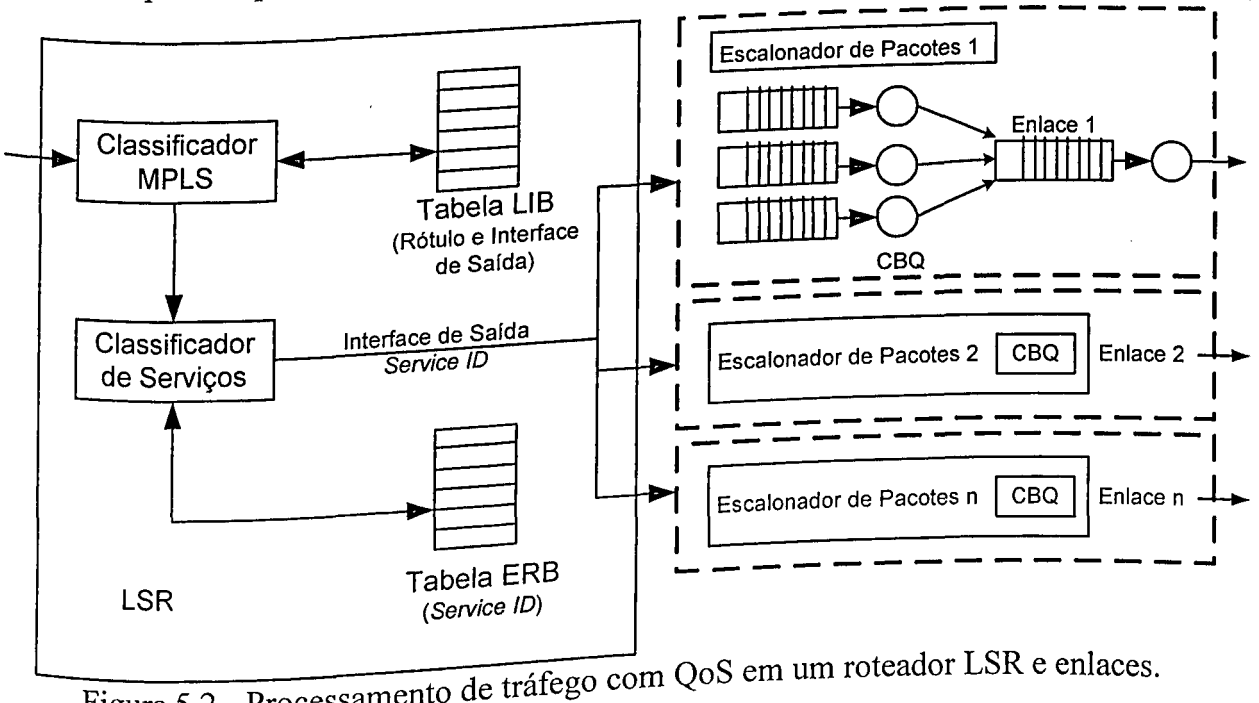


Figura 5.2 - Processamento de tráfego com QoS em um roteador LSR e enlaces.

Os componentes Controle de Admissão e Gerenciador de Recursos foram projetados e implementados no MNS 2 para o gerenciamento dos recursos. O componente Gerenciador de Recursos é responsável pela criação e exclusão de filas CBQ e o gerenciamento da informação de recursos (isto é, tabela de recursos) [3].

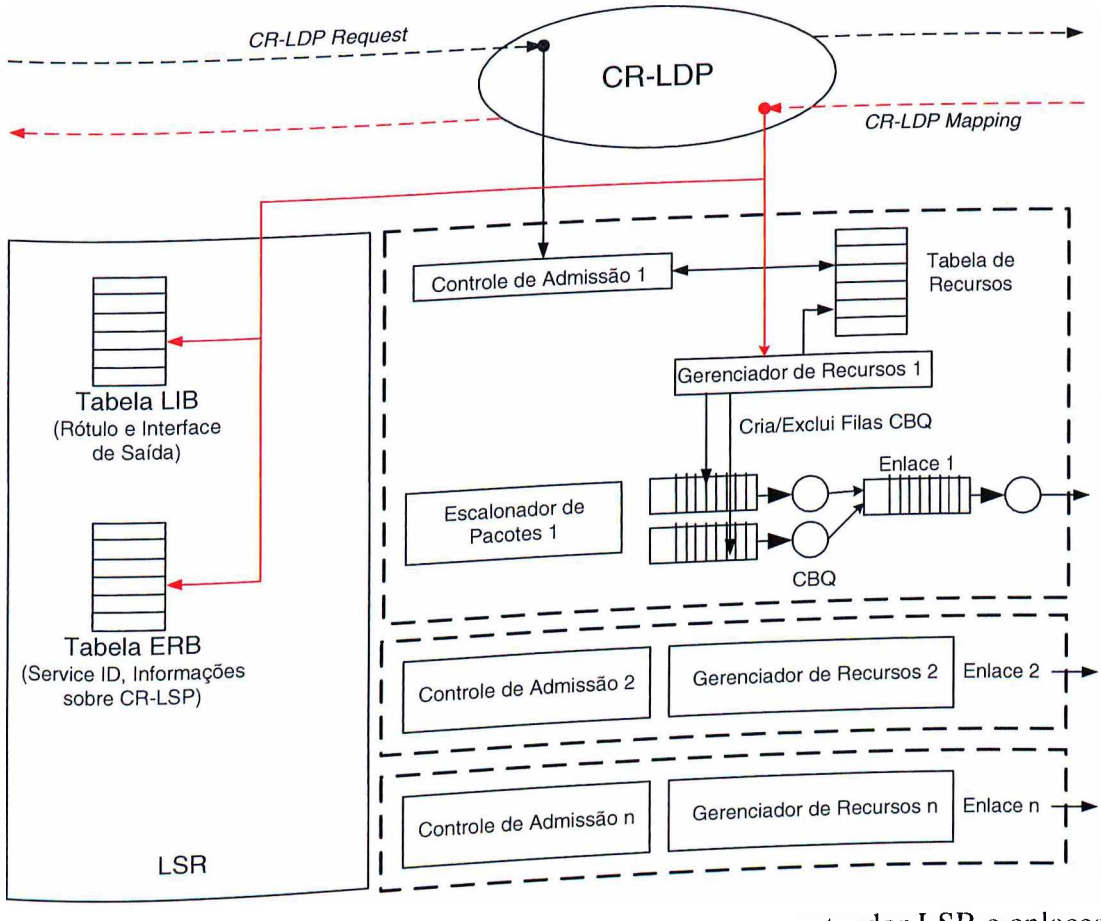


Figura 5.3 – Processamento de reserva de recursos em um roteador LSR e enlaces.

A Figura 5.3 [3] descreve como ocorre o processo de reserva de recursos nos LSRs e seus respectivos enlaces. Quando o componente CR-LDP recebe uma mensagem CR-LDP *Request*, o Controle de Admissão é ativado para verificar se o LSR tem o recurso solicitado. Se houver recurso disponível suficiente, o componente Controle de Admissão reserva o recurso e atualiza a tabela de recursos, com as novas informações sobre o recurso alocado. A seguir, a mensagem LDP *Request* é enviada para o LSR *downstream* (próximo salto) [3].

Quando o componente CR-LDP recebe uma mensagem LDP *Mapping*, ele salva as informações sobre interface e rótulo na tabela LIB e a informação sobre o CR-LSP solicitado (a identificação do caminho LSP) na tabela ERB. Depois, o componente Gerenciador de

Recursos é ativado e cria uma fila para servir ao CR-LSP solicitado, e salva seu ID *service* na tabela ERB. Finalmente, a mensagem LDP *Mapping* é enviada para o LSR *upstream* (salto anterior) [3].

5.3 Avaliação de Desempenho, Apresentação e Análise dos Resultados Obtidos

5.3.1 Envio de Tráfegos com a Utilização do Roteamento IP Convencional

A Figura 5.4 apresenta a vazão obtida no destino pelos tipos de tráfego analisados versus tempo de simulação sem a utilização dos mecanismos MPLS e CBR.

Como pode ser visto na Figura 5.4, enquanto o tráfego RT2 não injeta pacotes na rede, os tráfegos SBT, HBT e RT1 tem como vazão média, a taxa máxima de envio pretendida por cada um. No entanto, quando RT2 é ativado (a partir do instante 11 s), os tráfegos RT1 e RT2 sofrem uma atenuação na vazão dos pacotes enviados acima de 30% e os tráfegos SBT e HBT mantém o nível de vazão obtido antes da entrada do tráfego RT2. Aos 30 segundos, o tráfego RT2 é desativado e os outros tráfegos voltam a se comportar como no início da simulação (0 a 10 s), ou seja, atingem a capacidade de vazão desejada.

Os resultados de simulação para o retardo fim-a-fim de transferência dos pacotes gerados pelos tráfegos HBT, SBT, RT1 e RT2 sobre uma rede IP são mostrado na Figura 5.5.

Observa-se que com o tráfego RT2 desativado, o tráfego HBT sofre níveis mais altos de retardo fim-a-fim em seus pacotes, bem como o fato de que os três tipos de tráfegos possuem uma variação entre o valor máximo e mínimo do tempo de retardo fim-a-fim em torno de 5%. Quando RT2 começa trafegar na rede, o tráfego SBT é beneficiado, pois seu tempo de retardo fim-a-fim é em média 5% menor que os outros tráfegos. Além disso, os tráfegos baseados no serviço do melhor esforço (HBT e SBT) possuem um taxa de variação entre o valor máximo e mínimo do tempo de retardo fim-a-fim nula. Enquanto, os tráfegos de tempo real continuam com o mesmo nível de variação entre o valor máximo e mínimo do tempo de retardo fim-a-fim apresentado antes de RT2 ser ativado. Quando RT2 é desativado novamente, o restante dos tráfegos retornam ao seu comportamento anterior.

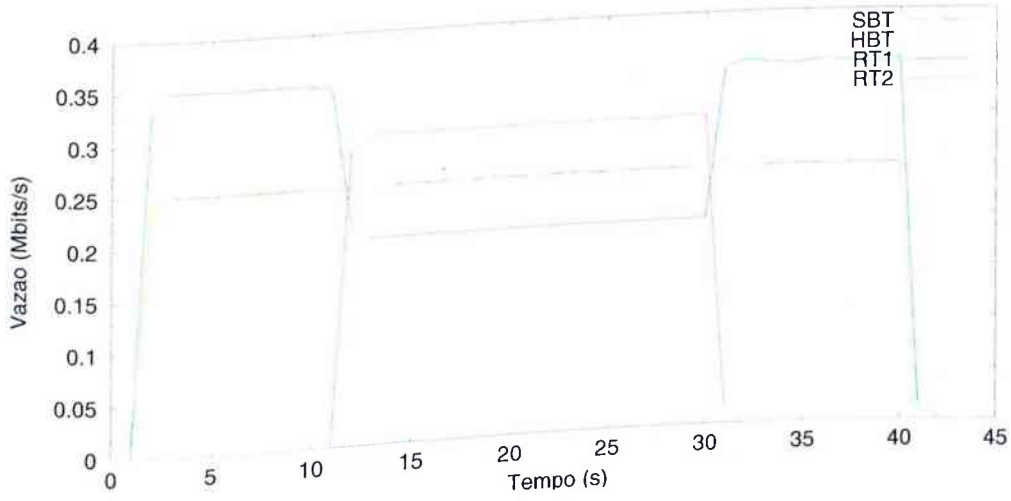


Figura 5.4 – Vazão obtida pelos tráfegos HBT, SBT, RT1 e RT2, sem a utilização dos mecanismos MPLS ou CBR.

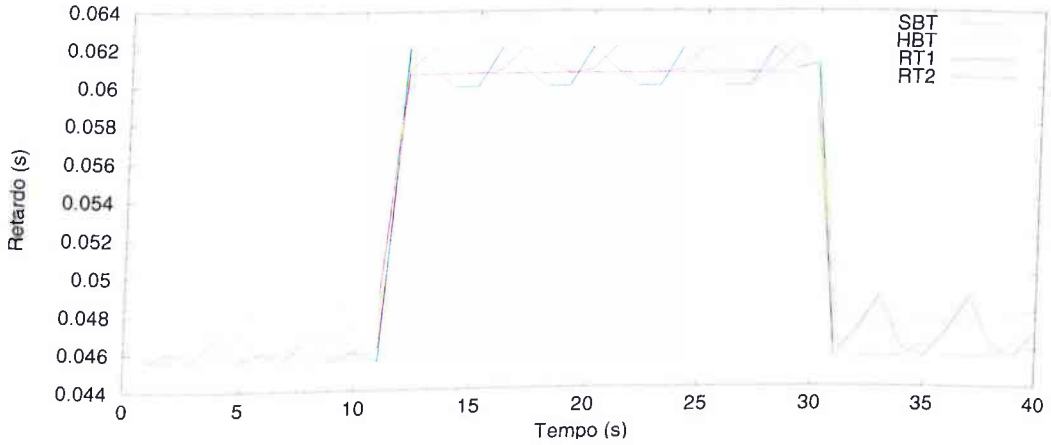


Figura 5.5 – Retardo fim-a-fim de transferência a que os tráfegos HBT, SBT, RT1 e RT2 ficaram sujeitos, sem a utilização dos mecanismos MPLS ou CBR.

A Figura 5.6 apresenta os tempos de variação de retardo (*jitter*) sentidos pelos tráfegos HBT, SBT, RT1 e RT2 em uma rede IP. Primeiramente, pode-se perceber que os tráfegos de melhor esforço (HBT e SBT) atingem os maiores valores de *jitter* entre os tráfegos observados. No entanto, quando o tráfego RT2 é ativado, os valores máximos de *jitter* dos tráfegos HBT e SBT sofrem uma atenuação de aproximadamente 30%, enquanto RT1 continua com a mesma taxa assumida antes de RT2 ser acionado ou tem seu valor máximo de *jitter* acrescido em 10%. Além disso, durante todo o tempo em que RT2 trafega pela rede, os níveis de *jitter* de HBT e SBT são constantes, ao contrário do que ocorre com os tráfegos de tempo real (RT1 e RT2) que possuem uma variação entre o valor máximo e mínimo de *jitter* em torno de 60 %. Quando RT2 deixa de injetar tráfego na rede, SBT continua a apresentar altas taxas de *jitter*, SBT tem seus valores de *jitter* atenuados e RT1 continua a repetir seu comportamento da primeira fase desta simulação.

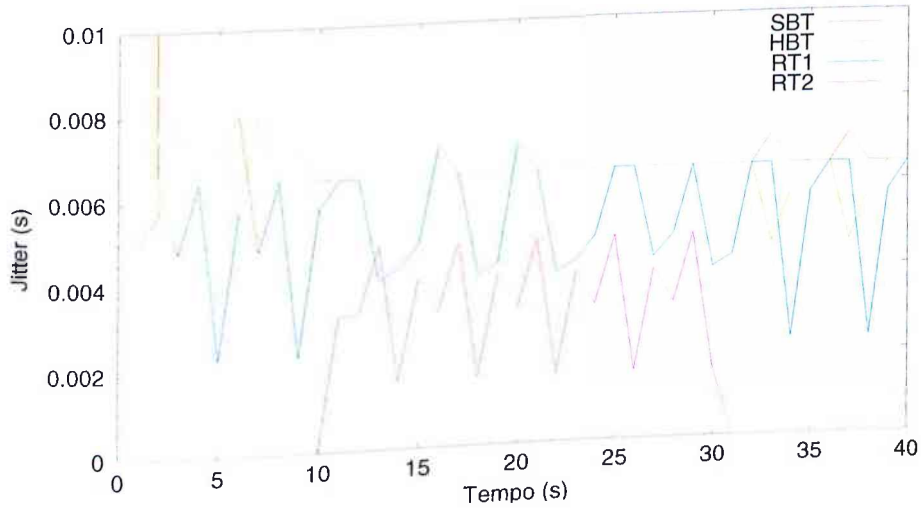


Figura 5.6 - *Jitter* experimentada pelos tráfegos HBT, SBT, RT1 e RT2, sem a utilização dos mecanismos MPLS ou CBR.

Fazendo uma análise dos resultados apresentados nas Figuras 5.4 a 5.6, quando uma rede *backbone* é implementada somente com roteamento IP convencional, não existe garantia de qualidade de serviço. Isso pode ser observado quando a soma dos tráfegos injetados na rede ultrapassa a largura de banda disponível (ou seja, quando RT2 é ativado). O roteamento IP convencional mantêm os níveis médios de vazão das fontes de tráfego de melhor esforço (HBT e SBT) no nível máximo pretendido por cada um (250 kbits/s). Enquanto, as fontes de tráfego de tempo real (RT1 e RT2) diminuem suas vazões em aproximadamente 30 %. Esta ausência de um mecanismo de qualidade de serviço no roteamento IP convencional também pode ser confirmada nos gráficos apresentados sobre retardo fim-a-fim e variação de retardo dos pacotes, onde todos os tráfegos apresentam valores bem reduzidos. Isto acontece porque o mecanismo de escalonamento aplicado nas filas de saída dos roteadores não prioriza determinados tipos de tráfego, fazendo com que os pacotes sejam injetados nos enlaces de forma FIFO, primeiro que chega é o primeiro que sai.

5.3.2 Envio de Tráfegos com a Utilização do Mecanismo MPLS

Neste cenário considera-se uma rede *backbone* que utiliza o mecanismo MPLS para o seu funcionamento. Como pode ser observado nas Figuras 5.7 a 5.9, os resultados obtidos quanto à vazão, retardo fim-a-fim dos pacotes e jitter com relação aos tráfegos HBT, SBT, RT1 e RT2 são exatamente iguais quando o cenário simulado implementava roteamento IP convencional, ou seja, os tráfegos percorrem a rede *backbone* sem nenhuma política de qualidade de serviço. Os tráfegos de melhor esforço (HBT e SBT) continuam com os seus níveis de vazão atingindo o valor máximo durante todo o cenário simulado (conforme é mostrado na Figura 5.7), o retardo fim-a-fim sofrido durante a propagação do tráfego pela rede mantendo-se em níveis bem reduzidos (conforme é mostrado na Figura 5.8), como também a variação do retardo segue este mesmo comportamento, assumindo valores muito baixos (conforme é mostrado na Figura 5.9). Estes resultados voltam a reiterar o papel da tecnologia MPLS como uma técnica de roteamento rápido, mas sem nenhum provimento de qualidade de serviço. Uma vez que os tráfegos são tratados da mesma maneira pelos mecanismos de encaminhamento e controle.

5.3.3 Envio de Tráfegos com a Utilização dos Mecanismos MPLS e Roteamento Baseado em Restrição

Neste último cenário considera-se uma rede *backbone* que implementa MPLS e roteamento baseado em restrição. Para que o modelo simulado ofereça qualidade de serviço são utilizados dois tipos de caminhos LSP: ER-LSP e CR-LSP. O ER-LSP configura

caminhos com rota explícita para os tráfegos SBT e HBT, dando prioridade mais alta para o caminho do HBT quando ocorre uma situação de congestionamento. Para assegurar reserva de recursos aos tráfegos RT1 e RT2 utilizam-se caminhos LSP com roteamento baseado em restrição (CR-LSP) que através de um mecanismo de escalonamento de pacotes baseado em WFQ prioriza na entrada dos enlaces aquelas filas pertencentes aos tráfegos de tempo real (RT1 e RT2).

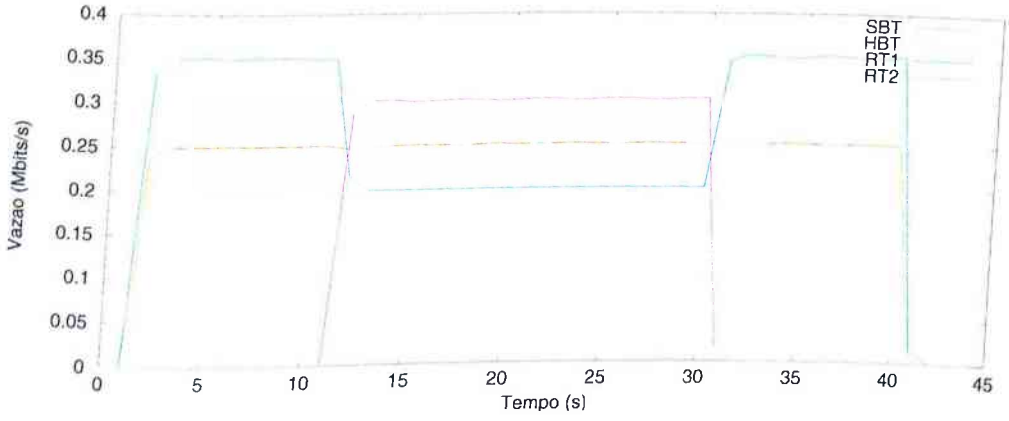


Figura 5.7 – Vazão obtida pelos tráfegos HBT, SBT, RT1 e RT2, com a utilização do mecanismo MPLS.

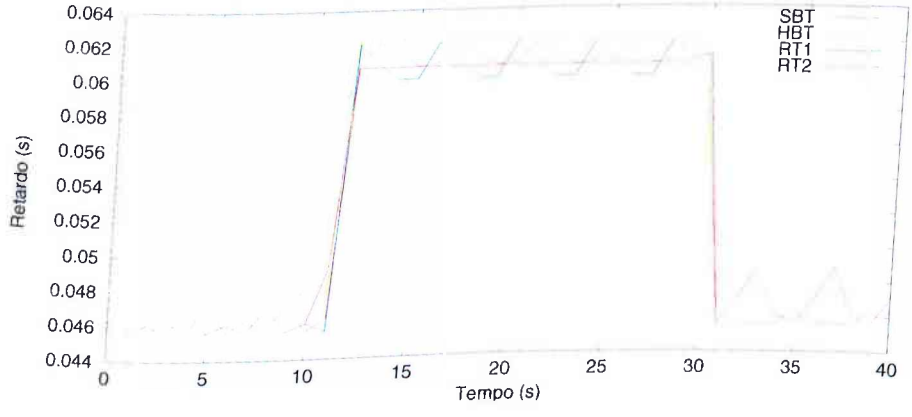


Figura 5.8 – Retardo fim-a-fim de transferência a que os tráfegos HBT, SBT, RT1 e RT2 ficaram sujeitos, com a utilização do mecanismo MPLS.

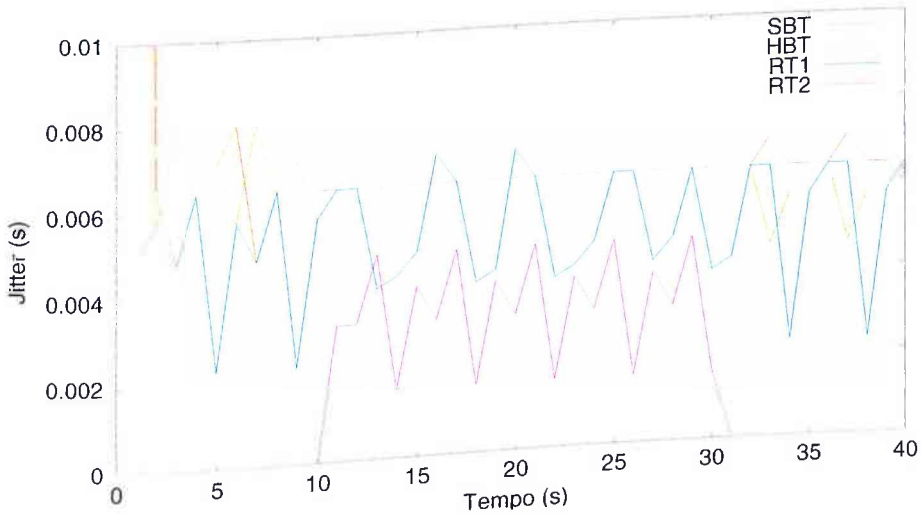


Figura 5.9 - *Jitter* experimentada pelos tráfegos HBT, SBT, RT1 e RT2, com a utilização do mecanismo MPLS.

A Figura 5.10 descreve a vazão obtida no destino pelos tipos de tráfego analisados versus tempo de simulação com a utilização dos mecanismos MPLS e CBR. Antes do tráfego RT2 ser injetado na rede, os tráfegos HBT, SBT e RT1 ocupam todo o espaço da largura de banda destinado a eles. Visto que a soma das vazões obtidas pelos tráfegos não ultrapassa a capacidade de vazão dos enlaces em que trafegam. A partir do momento no qual o tráfego RT2 começa a trafegar pelos enlaces, a vazão dos tráfegos de tempo real é mantida no seu limiar, ou seja, ocupam o espaço destinado a eles na largura de banda. Ao contrário, os tráfegos de melhor esforço sofrem uma atenuação na sua vazão, sendo o tráfego SBT mais atenuado que o HBT, apesar de ambos os tráfegos percorrerem ER-LSPs, o caminho configurado para o tráfego HBT possui uma prioridade maior na divisão da largura de banda, por isso ocorre essa diferenciação na vazão destes tráfegos. Quando o tráfego RT2 encerra sua transmissão, volta-se ao cenário simulado anteriormente, pois a soma de todos as vazões não supera a capacidade total de vazão do enlace.

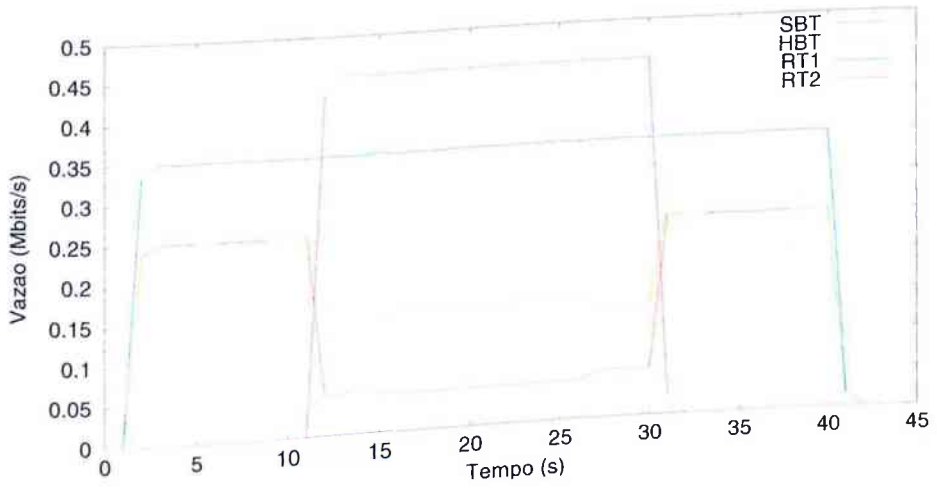


Figura 5.10 – Vazão obtida pelos tráfegos HBT, SBT, RT1 e RT2, com a utilização dos mecanismos MPLS e CBR.

O retardo fim-a-fim sofrido pelos tráfegos HBT, SBT, RT1 e RT2 durante suas propagações pelos enlaces é mostrada na Figura 5.11. Inicialmente, sem a presença de RT2, os tráfegos analisados sofrem um retardo fim-a-fim bem reduzido. A ausência de sobrecarga nos enlaces pode ser considerada uma razão para este valor reduzido no retardo fim-a-fim dos tráfegos, pois cada tráfego atinge a capacidade total de vazão requerida por ele. Logo depois, quando os quatro tráfegos estão em operação, os tráfegos de melhor esforço sofrem um forte acréscimo no retardo fim-a-fim dos pacotes. Principalmente, o tráfego SBT, pela mesma razão ocorrida na medição da vazão, ou seja o caminho ER-LSP do tráfego HBT é configurado com uma prioridade mais alta quando comparado com o ER-LSP do SBT. Por outro lado, os tráfegos de tempo real mantêm os níveis de retardo fim-a-fim na transferência dos pacotes em valores bem reduzidos. Já que, os caminhos CR-LSP reservam os recursos necessários para que estes tráfegos continuem utilizando o espaço de largura de banda nos enlaces reservado

para eles. Quando, o tráfego RT2 é desativado, volta-se ao cenário anterior a ativação do tráfego RT2.

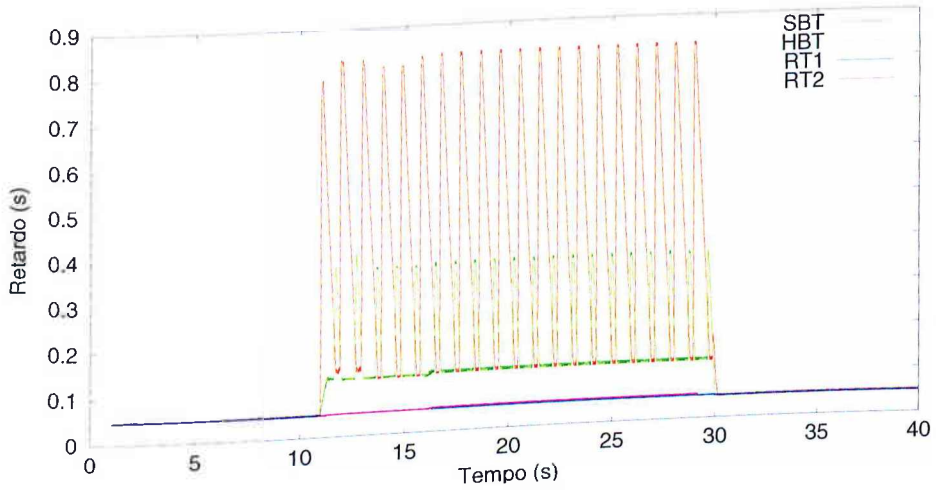


Figura 5.11 – Retardo fim-a-fim de transferência a que os tráfegos HBT, SBT, RT1 e RT2 ficaram sujeitos, com a utilização dos mecanismos MPLS e CBR.

Como mostra a Figura 5.12, quando a variação de retardo sofrida pelos tráfegos é medida, percebe-se um cenário muito parecido com o desempenho dos tráfegos quanto ao retardo fim-a-fim de transferência sofrido. Isto é, antes e depois de RT2 ser ativado, os tráfegos HBT, SBT e RT1 sofrem uma variação de retardo bem reduzida. Da mesma forma, quando RT2 é transmitido pelos enlaces, os tráfegos de melhor esforço sofrem uma variação de retardo acentuada. Já que, o escalonador de pacotes utiliza o mecanismo de escalonamento WFQ e a fila CBQ do tráfego de tempo real possui maior peso dentre as outras filas servidas pelo escalonador, sendo assim dificilmente pode ocorrer sobrecarga na fila e o descarte de alguns pacotes, atingindo assim um valor de retardo fim-a-fim e variação de retardo muito pequeno.

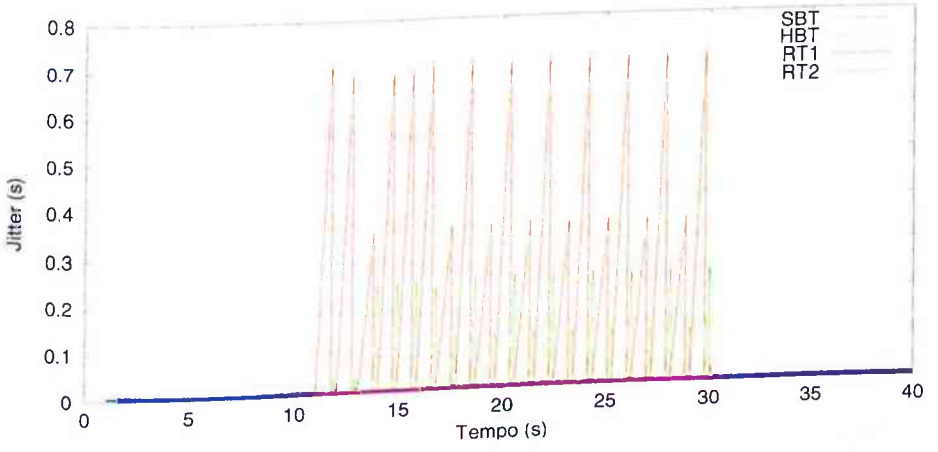


Figura 5.12 - *Jitter* experimentada pelos tráfegos HBT, SBT, RT1 e RT2, com a utilização dos mecanismos MPLS e CBR.

A partir dos resultados apresentados nas Figuras 5.10 a 5.12 pode ser observada a aplicabilidade do roteamento baseado em restrição juntamente com a tecnologia MPLS para o provimento de qualidade de serviço na rede *backbone*. Isto pode ser confirmado, através dos dados apresentados quanto à vazão obtida pelos tráfegos, o retardo fim-a-fim e o *jitter* sofrido por eles. Em todos os três parâmetros de medição de qualidade de serviço percebeu-se uma definição de prioridades quanto às classes de serviços, enquanto os tráfegos de tempo real, considerados mais importantes por trafegar pacotes que exigem alta vazão nos enlaces e baixo retardo e *jitter* na entrega dos pacotes, são privilegiados na divisão da largura de banda. Os tráfegos de melhor esforço perdem espaço na largura de banda pela sua característica de entregar os pacotes ao seu destino sem levar em conta parâmetros como vazão, retardo fim-a-fim e *jitter* atingido pelos tráfegos.

Sendo assim, a construção de caminhos LSPs com roteamento baseado em restrição possibilita aos tráfegos a facilidade do roteamento rápido, característica básica do MPLS e

provimento de QoS permitido pelo roteamento baseado em restrição através do mecanismo de filas CBQ na saída de cada roteador LSR.

5.4 Conclusões

Como foi afirmado no início deste capítulo, um estudo baseado em simulações apresenta somente uma tendência no comportamento do sistema modelado ao invés de obter valores reais para suas saídas. Sendo assim, os resultados apresentados nestas simulações mostram uma tendência de aplicabilidade do modelo de serviço MPLS/CBR em oferecer QoS em redes IP através de caminhos LSP's com largura de banda garantida.

Isto pode ser observado através dos níveis de vazão obtidos pelas fontes de tráfego analisadas numa rede MPLS/CBR quando ocorre um "estrangulamento" na capacidade de largura de banda nos enlaces. As fontes de tráfego de tempo real mantêm seus níveis máximos de vazão durante todo período simulado. Isto ocorre porque os tráfegos de tempo real são encaminhados através de caminhos LSP com largura de banda garantida, ou seja, há uma reserva de recursos (largura de banda disponível) na construção do caminho por onde os pacotes serão transmitidos. Por outro lado, as fontes de tráfego de melhor esforço terão que competir pelo resto de largura de banda dos enlaces. Por isso, os níveis de vazão das fontes SBT e HBT sofrem uma forte atenuação, pois o tamanho do *buffer* nos roteadores fica bem restringido e por conseqüência, a largura de banda disponível nos enlaces também.

Esta mesma tendência também pode ser observada nos valores de retardo fim-a-fim e *jitter*. Visto que, o tamanho do buffer utilizado pelos tráfegos de melhor esforço fica reduzido, o tempo nas filas de saída dos roteadores aumenta e por conseqüência, os níveis de retardo

fim-a-fim e jitter sofrem um forte crescimento. No caso dos tráfegos de tempo real, como utilizam caminhos LSP´s com reserva de largura de banda, os níveis de retardo fim-a-fim e *jitter* são bem reduzidos. Uma vez que a reserva de largura de banda nos enlaces é feita através de um mecanismo de escalonamento nas filas de saída dos roteadores que prioriza o escalonamento naqueles filas que contém pacotes gerados por fontes de tráfego de tempo real.

Capítulo 6

Conclusões Gerais

Com o crescimento do número de aplicações de missão crítica na Internet, o modelo de serviço tradicional da rede tem se tornado ineficiente para atendê-las, uma vez que, este modelo não procura atender aos requisitos de QoS exigidos pelas mesmas.

Em vista disso, surgiram várias propostas de modelos de provimento de QoS. Entre os modelos propostos pelo IETF, destacam-se os seguintes: Intserv [18], Diffserv [17], MPLS [47], Roteamento Baseado em Restrição [22] e Engenharia de Tráfego [15]. Contudo, observou-se que quando as soluções são aplicadas de forma isolada não obtém-se um desempenho satisfatório da rede.

Por exemplo, a solução Intserv empregada isoladamente, tem seu uso limitado a redes de pequeno porte. Já que, este tipo de abordagem gera muito tráfego de controle para estabelecer e manter os caminhos com reserva de recursos.

No caso do modelo Diffserv , o principal problema é a sua interoperação com outros tipos de domínio. Uma vez que aplica-se agregação de fluxos na entrada desta rede, então deve existir nos roteadores de fronteira, condicionadores de tráfego que façam o processo de agrupamento e desagrupamento. Conseqüentemente, a complexidade do funcionamento

desses roteadores torna-se elevada, exigindo mais capacidade de processamento, podendo causar uma queda de desempenho na rede.

Com relação à tecnologia MPLS, apesar de oferecer velocidades elevadas de transmissão dos dados e o serviço de roteamento explícito, este modelo não foi desenvolvido especificamente para oferecer QoS às aplicações em tempo real. Isto se deve ao fato de que o roteamento IP convencional é utilizado para calcular o próximo salto do roteador.

Contudo, o roteamento baseado em restrição foi criado com o intuito de oferecer uma técnica de roteamento capaz de convergir o tradicional cálculo do próximo salto e mecanismos de QoS. Contudo, quando é implementado de forma isolada numa rede IP, a mesma não o suporta, pois não possui um serviço de roteamento explícito nativo, uma ferramenta essencial para aplicar CBR em uma rede.

Como a engenharia de tráfego é um processo iterativo de planejamento e otimização da rede [15], para empregá-la na Internet torna-se imprescindível algumas funcionalidades, tais como: roteamento explícito, roteamento baseado em restrição, presentes nos modelos de QoS apresentados anteriormente.

Sendo assim, o uso de soluções integradas para o oferecimento de QoS na Internet é fundamental na aplicação de uma abordagem que procura atender de forma mais simplificada e eficiente as garantias de QoS sem causar queda no desempenho da rede.

A partir desse ponto de vista, o nosso trabalho é um estudo sobre a aplicabilidade de um modelo de provimento de QoS em redes IP que integra os benefícios existentes num cálculo de rota que não leva em conta somente às métricas provenientes dos protocolos de roteamento intradomínio, mas também restrições quanto ao tipo de tráfego a ser transportado, realizado

através do roteamento baseado em restrição. Em conjunto com o mecanismo MPLS, para que construa e mantenha caminhos que satisfaçam a rota calculada pelo CBR.

Essa aplicabilidade é avaliada a partir dos resultados obtidos na simulação de três cenários. O primeiro cenário mostra a inexistência de um mecanismo de QoS no roteamento IP convencional quando ocorre congestionamento. Já que, os pacotes são descartados aleatoriamente quando o limite da largura de banda disponível é ultrapassado, fazendo com que os tráfegos de tempo real (RT1 e RT2) sofram uma queda na vazão acima de 30%, pois são os tráfegos com maior carga, logo tem maior chance de serem descartados, uma vez que os tráfegos de melhor esforço (SBT) e melhor esforço de alta prioridade (HBT) consomem toda a largura de banda disponível. A razão para os tráfegos SBT e HBT serem privilegiados neste cenário é a mesma que descarta uma grande quantidade de pacotes dos tráfegos RT1 e RT2, ou seja, o descarte aleatório de pacotes. Os níveis de retardo fim-a-fim e *jitter* também confirmam a inexistência de um mecanismo de QoS ao assumirem valores bem reduzidos, mesmo quando ocorre congestionamento. Isto indica que os pacotes saem das filas de saídas dos roteadores segundo uma política de escalonamento que procura atender a todas as filas de maneira igual, ou seja, todos os pacotes têm a mesma prioridade na competição pelos enlaces.

A abordagem MPLS é empregada isoladamente no segundo cenário simulado. O comportamento observado pelos parâmetros analisados foi semelhante ao cenário anterior, ou seja, a vazão dos tráfegos de tempo real sendo comprometida no enlace congestionado, o retardo fim-a-fim e a variação de retardo são tão pequenos que não influem no comportamento dos tráfegos. Conseqüentemente, pode-se concluir, como já tinha sido

comentado no decorrer deste trabalho, que a tecnologia MPLS não provê QoS como uma funcionalidade nativa de seu modelo.

No entanto, quando aplica-se a tecnologia MPLS conjuntamente com o roteamento baseado em restrição, observam-se mudanças no cenário simulado. Os tráfegos de tempo real atingem sua vazão máxima durante todo o período analisado, mesmo quando ocorre congestionamento. O mesmo não acontece com os tráfegos HBT e SBT, que sofrem uma atenuação na vazão oferecida. Os parâmetros retardo fim-a-fim e variação de retardo confirmam a presença de QoS no modelo MPLS/CBR, pois os valores obtidos no enlace congestionado mostram o aumento acentuado desses dois parâmetros para os tráfegos HBT e SBT, enquanto os tráfegos de tempo real quase não sentem a presença deles. Isto acontece devido a maior parte da largura de banda está reservada para os tráfegos de tempo real.

A garantia de QoS aos tráfegos de tempo real é conseguida através do uso de caminhos LSP's com largura de banda garantida, uma aplicação do CBR. Estes caminhos conhecidos como CR-LSP (*Constraint Routed Label Switching Path*) empregam o protocolo CR-LDP para estabelecer e fazer as reservas de recurso em cada roteador pertence a eles.

Contudo, é interessante em trabalhos futuros avaliar o desempenho do roteamento baseado em restrição interoperando com outros modelos de serviço, tais como: DiffServ com CBR, IntServ com CBR. Pois, a partir destes estudos será possível especificar quais modelos possuem melhor desempenho quanto ao oferecimento de QoS em redes IP e qual o custo computacional e financeiro despendido por eles, possibilitando aos provedores de serviço Internet escolher aquele que melhor se adequa a sua rede.

Um outro assunto também a ser abordado em outros trabalhos, seria o desempenho do protocolo RSVP-TE como ferramenta para a construção dos LSP´s com largura de banda reservada. Já que, neste trabalho foi enfocado apenas o protocolo de sinalização CR-LDP. Assim, pode-se verificar a viabilidade do RSVP-TE e comparar seu desempenho com o CR-LDP.

REFERÊNCIAS BIBLIOGRÁFICAS

[01] ABOUL-MAGD, O. e JAMOUSSI, B., QoS and Service Interworking using Constraint-Route Label Distribution Protocol (CR-LDP), IEEE Communications Magazine, páginas 134-139, Maio 2001.

[02] AHN, G. e CHUN, W., Design and Implementation of MPLS Network Simulator supporting LDP and CR-LDP, ICON'2000, páginas 441-446, Setembro 2000.

[03] AHN, G. e CHUN, W., Design and Implementation of MPLS Network Simulator Supporting QoS, ICIN'2001, páginas 694-699, Jan/Fev. 2001.

[04] AHN, G. e CHUN, W., Simulator for MPLS Path Restoration and Performance Evaluation, ICATM'2001, páginas 32-36, Abril 2001.

[05] ANDERSON, L. et. al, LDP specification, RFC 3036, Janeiro 2001.

[06] APOSTOLOPOULOS, G. et. al, Quality of Service Based Routing: A performance Perspective, ACM SIGCOMM'98, Agosto 1998.

[07] ARMITAGE, Grenville, MPLS: The Magic Behind the Myths, IEEE Communications Magazine, páginas 124-131, Janeiro 2000.

[08] ARMITAGE, Grenville, Quality of Service in IP Networks, Macmillan Technical Publishing, 2000.

[09] ASH, J. et. al, LSP Modification using CR-LDP, Internet Draft, <draft-ietf-mpls-crlsp-modify-03.txt>, Março 2001.

[10] AYYANGAR, A. e SIDHU, D., Analysis of MPLS based Traffic Engineering Solution, ICATM'2001 , páginas 21-27, 2001.

[11] AWDUCHE, Daniel O., MPLS and Traffic Engineering in IP Networks, IEEE Communication Magazine, páginas 42-47, Dezembro 1999.

[12] AWDUCHE, Daniel O. et. al, Overview and Principles of Internet Traffic Engineering, Internet Draft, <draft-ietf-tewg-principles-02.txt>, Maio 2000.

[13] AWDUCHE, Daniel O. et. al, RSVP-TE: Extensions to RSVP for LSP Tunnels, Internet Draft, <draft-ietf-mpls-rsvp-lsp-tunnel-09.txt>, Agosto 2001.

[14] AWDUCHE, Daniel O. et al, Requirements for Traffic Engineering over MPLS, RFC 2702, Setembro 1999.

[15] BLACK, U., MPLS and Label Switching Networks, Prentice Hall, 2001.

[16] BLAKE, S. et. al, An Architecture for Differentiated Services, RFC 2475, Dezembro 1998.

[17] BRANDEN, R. , CLARK, D. e SHENKER, S., Integrated Services in the Internet Architecture: an Overview, RFC 1633, Junho 1994.

[18] BRANDEN, R. et. al, Resource Reservation Protocol (RSVP) – Version 1 Functional Specification, RFC 2205, Setembro 1997.

[19] CHEN, T. M. e OH, T. H., Reliable Services in MPLS, IEEE Communications Magazine, páginas 58-62, Dezembro 1999.

[20] CHUNG, J., Analysis of MPLS Traffic Engineering, Proc. 43rd IEEE Midwest Simp. On Circuits and Systems, páginas 550-553, Agosto 2000.

[21] CRAWLEY, E. et. al, A Framework for QoS-based Routing in the Internet, RFC 2702, Setembro 1999.

[22] CUNHA, D. V., Proposta e Avaliação de Desempenho de uma Política de Mapeamento de Rótulos orientado a Controle com Característica *Soft-State* em uma Rede *Label Switching*, Tese de Mestrado, Universidade Federal de Uberlândia, Maio 2001.

[23] DATA CONNECTION. A Comparison of MPLS Traffic Engineering: A choice of Signaling Protocols, White Paper, 2000.

[24] DAVIE, B. e REKHTER, Y., MPLS: Technology and Applications, Morgan Kaufmann, 2000.

[25] FALL, K. e VARADHAN, K., The *ns* Manual, The VINT Project, Fevereiro 2002.

[26] FERGUSON, P. e HUSTON, G., Quality of Service in the Internet: Fact, Fiction or Compromise?, INET'98, Julho 1998.

[27] GHANWANI, A. et al, Traffic Engineering Standards in IP Networks using MPLS, IEEE Communications Magazine, p. 49-53, Dezembro 1999.

[28] GNUPLOT, http://www.ucc.ie/gnuplot/gnuplot.html, Abril 2001.

[29] GONZALES, F. et al, Using MPLS to improve IP network Traffic Engineering. http://198.11.21.25/capstoneTest/Students/Papers/docs/UsingMultiprotocolLabelSwitching37148.pdf, 2000.

[30] GUERIN, R., et. al, QoS Routing Mechanisms and OSPF Extensions. RFC 2676, Agosto1999.

[31] GUO, Y., Multiple Protocol Label Switching Technique, http://trident.mcs.kent.edu/~yguo/mpls.pdf, 2000.

[32] HEINANIN, J. et. al, Assured Forwarding PHB Group, RFC 2597, Junho 1999.

[33] JACOBSON,V., NICHOLS, K. e PODURI, K., An Expedited Forwarding PHB, RFC 2598, Junho 1999.

[34] JAMOUSSI, B. et. al, Constraint-Based LSP Setup using LDP. RFC 3212, Janeiro 2002.

[35] JUNIPER NETWORKS, RSVP Signaling Extensions for MPLS Traffic Engineering, White Paper, 2000.

[36] KAMIENSKI, C. A. e SADOK, D., Qualidade de Serviço na Internet, Anais da XIX Jornada de Atualização em Informática – SBC'2000, Vol. 2, páginas 123-162, Julho 2000.

[37] KAMIENSKI, C. A. et al, Simulando a Internet: Aplicações na Pesquisa e no Ensino, Anais da XXI Jornada de Atualização em Informática – SBC'2002, Vol. 2, páginas 33-88, Julho 2002.

[38] LAWRENCE, J., Designing Multiprotocol Label Switching Networks, IEEE Communications Magazine, páginas 134-142, Julho 2001.

[39] LI, T., MPLS and The Evolving Internet Architecture. IEEE Communication Magazine, páginas 38-41, Dezembro 1999.

[40] MPLS Network Simulator (versão 2.0), http://flower.ce.cnu.ac.kr/~fog1/mns/, Fevereiro 2001.

[41] Network Simulator (versão 2.1b6a), http://www.isi.edu/nsnam/ns, Julho 2000.

[42] NICHOLS, K. et. al, Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers, RFC 2474, Dezembro 1998.

[43] NORTEL NETWORKS, MPLS - An Introduction to Multiprotocol Label Switching, White Paper, Abril 2001.

[44] NORTEL NETWORKS, Using CR-LDP for Service Interworking, Traffic Engineering and Quality of Service in Carrier Networks, White Paper, 1999.

[45] OHBA, Y., Issues on Loop Prevetion in MPLS Networks, IEEE Communications Magazine, páginas 64-68, Dezembro 1999.

[46] OLIVEIRA, R., Um Estudo Comparativo dos Algoritmos TCP Reno e TCP Vegas sobre uma Rede de Serviços Diferenciados, em termos de Distribuição de Banda Passante, Tese de Mestrado, Universidade Federal de Uberlândia, Fevereiro 2001.

[47] RESENDE, R. A. e YAMAKAMI, A., Roteamento de Tráfego baseado em Restrições em Redes MPLS, Anais do XIX Simpósio Brasileiro de Telecomunicações - XIX SBrT 2001, Vol. 1, pp.1-4, Fortaleza, CE, BRASIL, 2001 .

[48] ROSEN, E. et al, Multiprotocol Label Switching Architecture. RFC 3031, Janeiro 2001.

[49] SHENKER, S., Specification of Guaranteed Quality of Service, RFC 2212, Setembro 1997.

[50] STALLINGS, W., High-Speed Networks: TCP/IP and ATM Design Principles. In: Protocols and the TC/IP suite. 1 ed. New Jersey: Prentice Hall, 1998. 576p. páginas 23-41.

[51] SWALLOW, G., MPLS Advantages for Traffic Engineering, IEEE Communications Magazine, páginas 54-57, Dezembro 1999.

[52] SUN, W. , BHANIRAMKA, P. e JAIN, R., Quality Of Service Using Traffic Engineering Over MPLS: An Analysis, LCN'2000, páginas 238-241, Novembro 2000.

[53] THOMAS, B. e GRAY, E., LDP Applicability, RFC 3037, Janeiro 2001.

[54] VISWANATHAN, A. et al, Evolution of Multiprotocol Label Switching, IEEE Communications Magazine, páginas 1-12. Dez. 1999.

[55] XIAO, X., Providing QoS in the Internet, PhD Thesis, Michigan State University, 2000.

[56] XIAO, X. et al, Internet QoS: A big picture, IEEE Network Magazine, páginas 8-18, Março/Abril 1999.

[57] XIAO, X. et al, Traffic Engineering with MPLS in the Internet, IEEE Communications Magazine, Março 2000.

[58] WROCLAWSKI, J., Specification of the Controlled-load Network Element Service, RFC 2211, Setembro 1997.

TRABALHOS PUBLICADOS PELO AUTOR

[59] ARAUJO, N. V. S., GUARDIEIRO, P. R. e AGUIAR, E. L., Traffic Engineering in IP Networks: an MPLS-based Approach, aceito para publicação na WSEAS International Conference on Computer Networks 2002, Rio de Janeiro - Brasil, Outubro 2002

[60] ARAUJO, N. V. S., GUARDIEIRO, P. R. e AGUIAR, E. L., Estudo Comparativo dos Protocolos de Sinalização MPLS em uma Rede IP Utilizando Engenharia de Tráfego, 10º Congresso Mato-grossense de Informática e Telecomunicações – SUCESU-MT 2001, Cuiabá - Brasil, Outubro 2001