UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

Mecanismos para interoperação de backbones MPLS e redes que utilizem outras arquiteturas de QoS

por

FERNANDO MANCHINI SERENATO

Dissertação submetida à avaliação, como
requisito parcial para a obtenção do grau de
Mestre em Ciência da Computação

Prof. Dr. Juergen Rochol
Orientador

Porto Alegre, novembro de 2002

CIP – CATALOGAÇÃO NA PUBLICAÇÃO

Serenato, Fernando Manchini

Mecanismos para interoperação de backbones MPLS e redes que utilizem outras tecnologias para fornecimento de QoS / por Fernando Manchini Serenato. – Porto Alegre: PPGC da UFRGS, 2002.

117p.: il.

Dissertação (mestrado) – Universidade Federal do Rio Grande do Sul. Programa de Pós-Graduação em Computação, Porto Alegre, RS – BR, 2002. Orientador: Rochol, Juergen.

1. Qualidade de Serviço (QoS). 2. Serviços Diferenciados. 3. Serviços Integrados. 4. MPLS. 5. Engenharia de Tráfego. I. Rochol, Juergen. II. Título.

"I do not fear computers. I
fear lack of them."
(Isaac Asimov)

Agradecimentos

Agradeço a toda a minha família: meus pais João e Suely, meus irmãos Eduardo e Silvia, que sempre apostaram na minha capacidade, pela compreensão, apoio, incentivo, e acima de tudo por terem me dado todas as oportunidades para chegar aqui. Seu investimento em meus hobbies permitiu que eu seguisse uma carreira onde sou pago para fazer o que gosto.

À minha namorada, Tatiana, pelo apoio, e principalmente pela paciência. Este título de mestre é tão dela quanto meu.

À minha "família" em Porto Alegre: Eidy Leandro Tanaka Guandeline, Cristiane Regina Yamaguti Mashuda e César Ida. Sem sua preciosa ajuda e dedicação tudo isto teria levado muito mais tempo.

Ao meu orientador, Prof. Juergen Rochol, por acreditar em minha capacidade orientando-me durante o mestrado. Sua assertividade em nossos encontros foi decisiva.

Aos colegas de turma: Carlos Gomiero Maluf, Daniela Satomi Saito, Dionísio Pinheiro de Oliveira, Leonardo Mota Pinheiro, Marcel Watanabe e Roberto Vedoato pelo companheirismo e pelos diversos momentos de diversão, embora jurássemos estar fazendo algum trabalho...

E a todos aqueles que direta ou indiretamente colaboraram para a conquista de mais um degrau em minha vida.

Sumário

Lista de Abreviaturas

AF	Assured Forwarding
AQ	Assured Queue
AS	Autonomous System
ATM	Asynchronous Transfer Mode
BA	Behavior Aggregate
BB	Bandwidth Broker
BE	Best Effort
CBQ	Class based Queuing
CBR	Constant Bit Rate
CBR	Constraint Based Routing
CBS	Committed Burst Size
CDR	Committed Data Rate
CIR	Committed Information Rate
CLP	Cell Loss Priority
CLS	Controlled Load Service
COPS	Common Open Policy Service
CR-LDP	Constraint Based Routing – Label Distribution Protocol
CR-LSP	Constraint Based Routing – Label Switched Path
CSPF	Constraint Shortest Path First
DRR	Deficit Round Robin
DSCP	Differentiated Services Codepoint
DWDM	Dense Wavelength Division Multiplexing
E-LSP	EXP-Inferred-PSC LSP
EBS	Excess Burst Size
EF	Expedited Forwarding
ERO	Explicit Route Object
FEC	Forwarding Equivalent Class
FTN	FEC to NHLFE Map
GS	Guaranteed Service
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
ILM	Incoming Label Map
IP	Internet Protocol
IPSec	IP Security
ISP	Internet Service Provider
LDAP	Lightweight Directory Access Protocol
LDP	Label Distribution Protocol
LIB	Label Information Base
L-LSP	Label-Only-Inferred-PSC LSP
LSP	Label Switched Path
LSR	Label Switched Router
MF	Multi-field
MIB	Management Information Base
MPLS	Multiprotocol Label Switching
NHLFE	Next Hop Label Forwarding Entry
OA	Ordered Aggregate

OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PBS	Peak Burst Size
PDP	Policy Decision Points
PDR	Peak Data Rate
PDU	Protocol Data Unit
PEP	Policy Enforcement Point
PHB	Per-hop Behavior
PM	Policy Management
PPP	Point to point protocol
PASTE	Provider Architecture for Differentiated Services and Traffic Engineering
PSC	PHB Scheduling Class
PQ	Priority Queue
PQ	Premium Queue
QoS	Quality of Service
RED	Random Early Detection
RIO	RED with in and out of profile
RSVP	Resource Reservation Protocol
RSVP-TE	Resource Reservation Protocol – Traffic Engineering
SLA	Service Level Agreement
SLS	Service Level Specification
SLSM	SLS Management
SPF	Shortest Path First
TCA	Traffic Control Agreement
TCP	Transmission Control Protocol
TE	Traffic Engineering
TLV	Type-Length-Value
ToS	Type of Service
TT	Traffic Trunk
TTL	Time to live
UDP	User Datagram Protocol
VBR	Variable Bit Rate
VC	Virtual Channel
VCI	Virtual Channel Identifier
VoIP	Voice Over IP
VP	Virtual Path
VPI	Virtual Path Identifier
VPN	Virtual Private Network
WFQ	Weighted Fair Queuing
WRR	Weighted Round Robin

Lista de Figuras

Lista de Tabelas

Resumo

Acredita-se que no futuro as redes de telecomunicação e dados serão integradas em uma só rede, baseada na comutação de pacotes IP. Esta rede deverá oferecer serviços com qualidade (QoS) para as aplicações atuais e futuras. Uma das tecnologias que deverá ser adotada no núcleo desta nova rede é MPLS. MPLS introduz o conceito de switching (comutação) no ambiente IP e também permite que seja implementada a Engenharia de Tráfego, otimizando sua utilização através do roteamento baseado em restrições. Junto com MPLS outras arquiteturas para fornecimento de QoS, como Serviços Integrados e Serviços Diferenciados, serão utilizadas. Entretanto, como nenhuma delas atende a todos os requisitos para garantia de QoS fim a fim e levando-se em consideração o fato de a Internet ser uma rede heterogênea, surge a necessidade de um framework que permita a interoperabilidade das diferentes arquiteturas existentes. Neste trabalho é proposto um modelo de integração que fornece garantias de QoS fim a fim para redes que utilizam tanto Serviços Integrados como Serviços Diferenciados através do emprego de uma infra-estrutura baseada em MPLS e Serviços Diferenciados. A aplicabilidade do modelo foi testada no simulador ns2 e os resultados são apresentados neste trabalho.

Palavras-chave: Qualidade de Serviço (QoS), Serviços Diferenciados, Serviços Integrados, MPLS, Engenharia de Tráfego.

TITLE: "A FRAMEWORK FOR MPLS BACKBONES AND ANOTHER QOS ENABLED NETWORKS INTEROPERATION"

Abstract

It is believed that in the future the telecommunication and data networks will be integrated into one network alone, based on IP switching. This network will have to offer services with guaranteed QoS for the current and future applications. One of the technologies that certainly will be adopted in the core of this new network is MPLS. MPLS introduces the concept of packet switching in IP networks. MPLS also allows that Traffic Engineering be deployed, optimizing network utilization. Together with MPLS, other QoS architectures, such as Integrated Services and Differentiated Services will be used. However, as none of them takes care of all the requirements for end to end QoS, and taking in consideration the fact of the Internet being a heterogeneous network, a framework that allows the interoperability of the different existing architectures is needed. In this paper an integration model based on MPLS and Differentiated Services is presented. The applicability of this model is simulated in ns2 and the results are also presented.

Keywords: Quality of Service (QoS), Differentiated Services, Integrated Services, MPLS, Traffic Engineering.

1 Introdução

Atualmente, a maior parte da infra-estrutura da Internet suporta apenas o serviço *best effort*. Os pacotes são processados da maneira mais rápida possível, todavia, não existem garantias quanto ao atraso e nem mesmo quanto ao seu recebimento. Anteriormente isto não representava um problema, mas com a recente popularização da Internet e o conseqüente crescimento do tráfego, começaram a surgir demandas por serviços com qualidade garantida.

Somando-se a isto, existe o problema de muitos dos *links* da Internet já apresentarem sinais de congestionamento crônico. Assim, para resolver estes problemas, duas alternativas são propostas: o superdimensionamento da rede, usando tecnologias como DWDM (*Dense Wave-lenght Division Multiplex*) e *Gigabit Ethernet*, ou então a utilização de tecnologias de comutação (*switching*) e Engenharia de Tráfego para minimizar o congestionamento e também o atraso da rede.

A primeira solução, além de cara, não aproveitará satisfatoriamente os recursos oferecidos pela rede. Também se acredita que, sempre que houver sobra na largura de banda disponível, serão criadas novas aplicações para ocupá-la. Já a segunda alternativa, baseada em um *framework* para a plataforma IP, pretende transformar a Internet em uma rede com integração de serviços e flexibilidade para suportar as novas aplicações que estão surgindo. Tudo isto com condições de prover qualidade de serviço (QoS) para todos.

Os serviços oferecidos poderão variar desde serviços com baixo atraso e pouca variação do atraso (*jitter*), para empresas que utilizam a Internet como meio de transmissão para aplicações de tempo real, até um serviço equivalente ao *Best effort* para pessoas que simplesmente necessitem de conectividade. Além de apresentarem níveis de qualidade diferentes, estes serviços também apresentarão preços diferentes: quanto maior for a qualidade desejada, maior será o preço a ser pago.

O IETF (*Internet Engineering Task Force*) propôs diversas arquiteturas para fornecimento de QoS, dentre elas: a arquitetura de Serviços Integrados [BRA 94], utilizando RSVP [BRA 97] como protocolo de sinalização, a arquitetura de Serviços Diferenciados [BLA 98], [NIC 98], o conceito de Roteamento Baseado em Restrições [CRA 98], [JAM 2002], e mais recentemente a arquitetura MPLS (*Multi-Protocol Label Switching*) [ROS 2001], [MAG 2001].

A arquitetura de Serviços Integrados [BRA 94] baseia-se na reserva de recursos da rede. Antes de se iniciar uma transmissão, são configurados caminhos, e reservados os recursos necessários. Para isto pode-se utilizar o protocolo RSVP [BRA 97], um protocolo de sinalização para configuração de caminhos e reserva de recursos.

Na arquitetura de Serviços Diferenciados [BLA 98], [NIC 98], os pacotes são marcados com diferentes valores para criar diversas classes de pacotes. Pacotes que se encontrem em classes diferentes recebem níveis de serviço diferentes.

O Roteamento Baseado em Restrições (CBR - *Constraint Based Routing*) [CRA 98], [JAM 2002] é uma forma mais sofisticada de roteamento, que consiste em encontrar rotas na rede que atendam a determinadas restrições, como largura de banda disponível e atraso, e que não leve em consideração somente o conceito de caminho mais curto (SPF – *Shortest Path First*), como nos protocolos de roteamento IGP atuais.

A arquitetura MPLS [ROS 2001], [MAG 2001] fornece um mecanismo de encaminhamento baseado em um rótulo, que os pacotes recebem quando entram em um domínio MPLS. Os procedimentos subseqüentes de classificação e encaminhamento são baseados somente nesse rótulo, agilizando o processo. MPLS também permite esquemas

sofisticados de roteamento baseados na capacidade de estabelecimento de LSPs (*Label Switched Paths*) explicitamente roteados. Esta característica é a base da Engenharia de Tráfego com MPLS [SWA 99]. Os caminhos podem ser definidos de acordo com o tipo de tráfego, ou com a situação atual de ocupação da rede via CBR. Isto permite que se divida a carga igualmente por todos os *links*, otimizando sua utilização e diminuindo as chances de congestionamento.

Levando-se em consideração as vantagens apresentadas pela arquitetura MPLS, podemos afirmar que essa será a tecnologia adotada pelos grandes provedores de serviço (ISPs) em um futuro próximo. Entretanto, a migração de uma rede para a arquitetura MPLS não é trivial [XIA 2000]. Por isto, acredita-se que esta migração, em um primeiro momento, será feita somente pelas empresas que se beneficiarão mais dela: os ISPs. Para as outras empresas, bastarão soluções que apresentem níveis de QoS satisfatórios, sem que seja necessário um grande gasto ou reestruturação da rede. Surge assim a necessidade de um framework que permita a interoperabilidade das diferentes arquiteturas utilizadas nas empresas, como Serviços Integrados ou Serviços Diferenciados, e nos ISPs, como MPLS, que é o objetivo principal deste trabalho.

O restante deste trabalho está organizado da seguinte forma: no capítulo 2 são mostradas as arquiteturas propostas pelo IETF para fornecimento de QoS e as razões para a sua integração. No capítulo 3 são mostrados diversos modelos de integração, incluindo os modelos em que este trabalho se baseia. No capítulo 4, é apresentado o modelo proposto. No capítulo 5 são apresentados os resultados de simulações do modelo proposto no simulador ns2 [NS2 2002]. Por fim, no capítulo 6 são apresentadas as conclusões e sugestões de trabalhos futuros.

2 Arquiteturas para fornecimento de QoS

2.1 A arquitetura de Serviços Integrados

Os princípios da arquitetura de Serviços Integrados estão em [BRA 94]. Seu objetivo era expandir os serviços da Internet, passando do simples *Best effort* para uma gama de serviços fim a fim adaptados para novas aplicações interativas e *streamings* de tempo real. A arquitetura de Serviços Integrados suporta duas grandes classes de aplicações:

- Aplicações de tempo real, com requisitos estritos de largura de banda e atraso, que não eram atendidas satisfatoriamente pelo serviço *Best effort*. O serviço que atende estas aplicações é conhecido como Serviço Garantido (*Guaranteed Service*) [SCH 97];
- Aplicações tradicionais, cujos usuários esperavam uma performance equivalente a de uma rede *Best effort* pouco utilizada, independentemente da carga real a que a rede estava sendo submetida. O serviço que atende estas aplicações é conhecido como Serviço de Carga Controlada (*Controlled Load*) [WRO 97a].

Destinada a suportar aplicações individualmente, a arquitetura de Serviços Integrados exige que os nós de um caminho tratem individualmente cada fluxo, além de necessitar de uma sinalização explícita *a priori* dos requisitos de cada um dos fluxos [ARM 2000].

A arquitetura de Serviços Integrados baseia-se em 4 componentes: o protocolo de sinalização, como RSVP, a rotina de controle de admissão, o classificador e o escalonador (ver FIGURA 2.1). As aplicações que desejarem utilizar o serviço Garantido ou de Carga Controlada devem configurar caminhos e reservar recursos através do protocolo de sinalização antes de iniciar a transmissão de seus dados. A rotina de controle de admissão verificará se uma requisição de recursos pode ser efetuada e retornará uma resposta positiva ou negativa. Quando um roteador receber um pacote, o classificador selecionará uma fila para o pacote baseado em múltiplos critérios de classificação. Depois disso, o escalonador atenderá cada uma das filas, de forma que todas cumpram seus requisitos de qualidade de serviço [XIA 99].

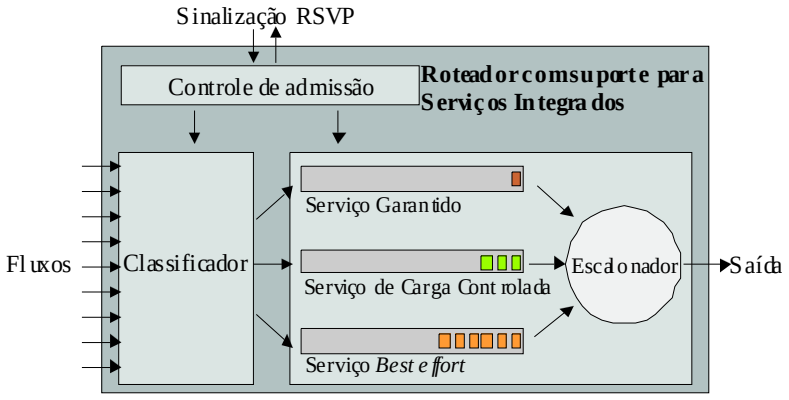

FIGURA 2.1 - Elementos da arquitetura de Serviços Integrados

2.1.1 Resource Reservation Protocol (RSVP)

RSVP [BRA 97], [WRO 97b] foi criado como um protocolo de sinalização para que aplicações fossem capazes de reservar recursos. A abordagem do protocolo é baseada no destino, de modo que são os computadores destino que escolhem o nível de recursos a serem reservados. A rede responde explicitamente, admitindo ou rejeitado as requisições. As aplicações que possuem necessidades quantificadas de recursos podem expressar tais necessidades através de parâmetros. As reservas efetuadas por RSVP são unidirecionais [BRA 97]. Assim para conexões bidirecionais é necessário configurar dois caminhos RSVP. O processo de sinalização é mostrado na FIGURA 2.2.

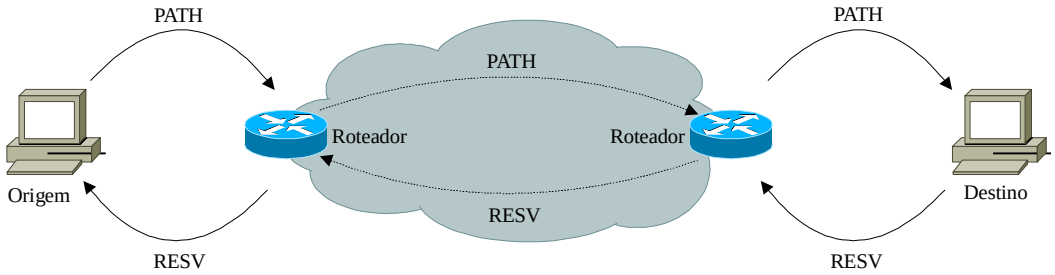

FIGURA 2.2 - Sinalização do protocolo RSVP

O computador origem envia uma mensagem PATH para o computador destino, especificando as características do tráfego que ele deseja enviar. A mensagem PATH descobre o caminho até o destino e prepara os roteadores intermediários para o caminho reverso, porém, não faz reserva de recursos. Cada roteador no caminho entre origem e destino envia a mensagem para o próximo *hop* determinado pelo protocolo de roteamento. Quando o computador destino recebe a mensagem PATH, ele responde utilizando uma mensagem RESV, que percorre a mesma rota no sentido reverso, para requisitar os recursos para o fluxo. Cada roteador no caminho pode aceitar ou rejeitar a requisição especificada na mensagem RESV. Se a requisição for rejeitada, o roteador enviará uma mensagem de erro RESVERR para o computador destino, e o processo de sinalização será encerrado. Se a requisição for aceita, a largura de banda e o espaço em *buffer* são alocados para o fluxo, e as informações relativas ao estado do fluxo são inseridas no roteador.

As reservas de recursos feitas por RSVP são *soft-state*, isto é, a reserva será cancelada se RSVP não enviar uma mensagem de confirmação através do caminho de uma reserva periodicamente [BRA 97].

Informações sobre caminhos e reservas nos roteadores também podem ser canceladas através de mensagens *teardown*. Mensagens *teardown* podem ser enviadas por computadores origem, destino ou roteadores que detectem um *timeout* de alguma reserva. Como as reservas RSVP são *soft-state* não é necessário cancelar explicitamente uma reserva. Entretanto, é recomendado que as mensagens *teardown* sejam enviadas sempre que uma reserva não for mais necessária [BRA 97].

Uma extensão ao protocolo RSVP foi proposta em [GUE 97] onde diversas reservas seriam agregadas em uma única reserva, fornecendo um desempenho melhor, apesar da diminuição do isolamento entre os fluxos.

2.1.2 Serviços Disponíveis

A arquitetura de serviços integrados define somente dois tipos de serviço. O Serviço Garantido fornece limites estritos do atraso fim a fim [SCH 97], enquanto o serviço de Carga Controlada, fornece limites nominais, com possibilidade de existência de *jitter* desde moderado até extremo [WRO 97a].

2.1.2.1 Serviço de Carga Controlada

A definição do serviço de Carga Controlada está em [WRO 97a]: "O comportamento fim a fim fornecido a uma aplicação por uma série de elementos de rede (roteadores, *links*, etc.) que provêem o serviço de Carga Controlada se aproxima muito do comportamento de aplicações utilizando o serviço *Best effort* em uma rede com os mesmos elementos de rede, mas com baixa carga de utilização".

Neste contexto, baixa carga de utilização significa "sem congestionamentos" e não "sem tráfego algum". Assim o serviço de Carga Controlada fornece um serviço *Best effort* melhorado, que mantém suas características mesmo quando a rede estiver sob forte carga ou congestionada. Em [WRO 97a] são apresentadas mais algumas características do serviço de Carga Controlada:

- Uma grande porcentagem dos pacotes transmitidos vai ser entregue com sucesso pela rede para os nós destino. A porcentagem de pacotes perdidos deve ser próxima à taxa de perdas do meio de transmissão;
- O atraso na transmissão experimentado pela grande maioria dos pacotes entregues não excederá em muito o atraso mínimo de transmissão de qualquer um dos outros pacotes entregues com sucesso. O atraso mínimo inclui a velocidade de propagação dos sinais mais o tempo de processamento nos roteadores e outros elementos de rede;

Assim, quando um fluxo requisita o serviço de Carga Controlada, este espera um serviço *Best effort* emulado, que se comportará como se a rede sempre estivesse com pouco tráfego, independentemente da situação real de ocupação da rede. Desta maneira, o serviço de Carga Controlada é extremamente útil por permitir que diversos fluxos compartilhem a mesma rede enquanto limita a interferência entre eles [ARM 2000].

2.1.2.2 Serviço Garantido

A definição do Serviço Garantido se encontra em [SCH 97]: "O Serviço Garantido fornece limites rígidos, matematicamente prováveis, para o atraso fim a fim de pacotes. Este serviço torna possível prover um serviço que garanta tanto o atraso como a largura de banda requisitada por um fluxo. O Serviço Garantido garante que os pacotes serão entregues dentro do tempo de entrega estabelecido e que não serão descartados por causa de estouros de fila, desde que a taxa de envio do fluxo esteja dentro dos limites estabelecidos".

Uma aplicação fornece uma caracterização de seu perfil de tráfego esperado e a rede calcula e retorna uma indicação do atraso fim a fim que ela pode garantir. Se este atraso está dentro dos limites desejados pela aplicação, esta pode transmitir os pacotes com a certeza de que estes serão entregues dentro do limite garantido. Caso contrário, a

aplicação pode modificar sua caracterização de tráfego e requerer uma nova indicação do atraso que a rede pode garantir.

O Serviço Garantido exige que a caracterização de tráfego de uma aplicação seja dada em termos de uma taxa de envio e de um tamanho de rajada, ou seja, os parâmetros de um *token bucket*. A rede calcula o atraso no pior caso somando os atrasos de enfileiramento, de propagação e etc. de todos os elementos de rede do caminho, tendo os parâmetros da caracterização de tráfego e a carga atual da rede devido às reservas já existentes.

O Serviço Garantido não limita ou quantifica o atraso mínimo, o atraso médio ou o *jitter* nominal, mas apenas o atraso no pior caso é garantido, sendo muito útil para aplicações de tempo real [ARM 2000].

2.2 A arquitetura de Serviços Diferenciados

A arquitetura de Serviços Diferenciados surgiu como uma alternativa para a arquitetura de Serviços Integrados. Nela as decisões complexas, como classificação, foram trazidas para as bordas do domínio, e serviços fim a fim são construídos a partir de um conjunto restrito de tratamentos nos roteadores de núcleo [BLA 98]. Assim, espera-se roteadores de núcleo mais rápidos e menos informações de estado para sinalizar. [ARM 2000] A arquitetura básica de serviços diferenciados pode ser vista na FIGURA 2.3.

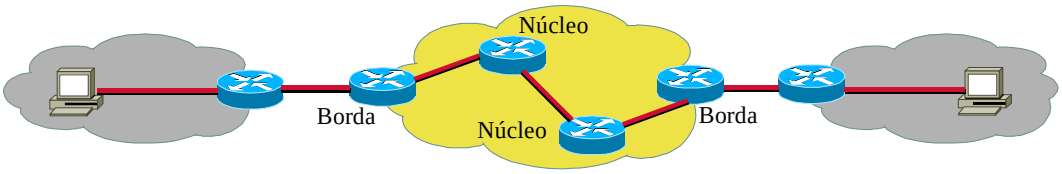

FIGURA 2.3 - Arquitetura de Serviços Diferenciados

São funções dos roteadores de borda:

- Examinar os pacotes que chegam e classificá-los de acordo com a política em vigor;
- Marcar os pacotes com um codepoint que reflita o nível de serviço desejado;
- Garantir que o tráfego dos clientes siga às especificações definidas, através do policiamento e da conformação.

São funções dos roteadores de núcleo:

- Examinar os pacotes que chegam e verificar o codepoint marcado em seus cabeçalhos pelos roteadores de borda;
- Classificar e encaminhar os pacotes que chegam de acordo com seus codepoints.

O cabeçalho do pacote IPv4 contém um byte de tipo de serviço (TOS), cuja interpretação foi especificada em [POS 81]. As aplicações podem configurar 3 bits do byte de TOS para especificar a necessidade de baixo atraso, alta largura de banda ou poucas perdas (descartes). No entanto, estas opções são limitadas. A arquitetura de

Serviços Diferenciados define uma nova interpretação [NIC 98] para o campo TOS (ver FIGURA 2.4), renomeado para Campo DS (*DS Field*), e um conjunto básico de regras para tratamento e encaminhamento de pacotes, os PHBs (*Per-hop behaviors*).

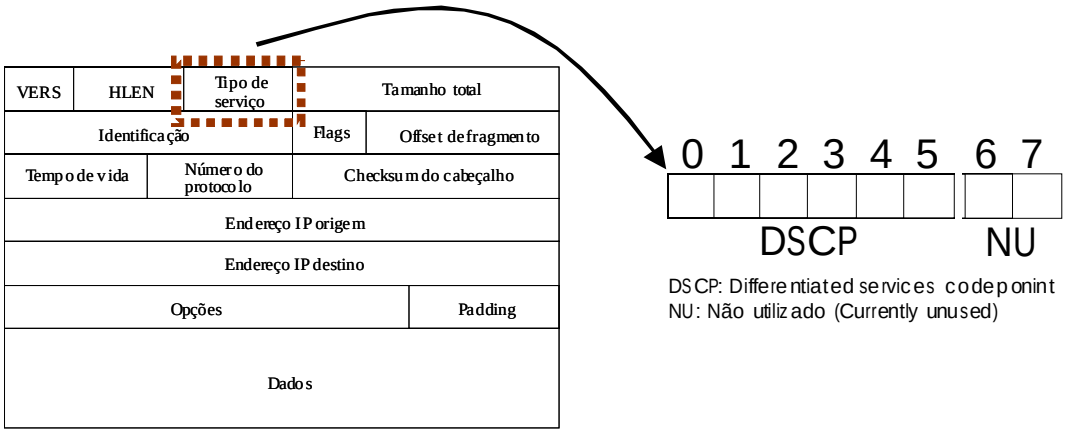

FIGURA 2.4 - Campo DS

Ao se utilizar a marcação diferenciada do campo DS e, posteriormente selecionar o tratamento de cada pacote de acordo com o conteúdo de seu campo DS, através da classificação dos agregados de tráfego (BA – *Behavior Aggregate*), diferentes classes de serviço podem ser criadas.

Para que um cliente possa utilizar os serviços diferenciados de um ISP, é necessário que ele estabeleça um Contrato de Nível de Serviço, ou SLA, com o ISP. Um SLA especifica as classes de serviço suportadas e a quantidade de tráfego permitida em cada classe. Um SLA pode ser estático ou dinâmico. SLAs estáticos são negociados regularmente (mensal, anual, etc.), enquanto SLAs dinâmicos devem utilizar algum protocolo de sinalização, como RSVP, para requisitar serviços sob-demanda [XIA 99].

Os clientes podem marcar os pacotes individualmente para indicar a classe de serviço desejada, ou então a classificação pode ser feita pelo roteador de borda do domínio de Serviços Diferenciados, após os pacotes passarem por um classificador multi-campo (MF – *Multi-field*) que indicará qual a classe de serviço a ser utilizada.

Ao ingressar no domínio de Serviços Diferenciados os pacotes podem ser classificados, policiados e possivelmente conformados. As regras de classificação, policiamento e conformação são derivadas do SLA. Quando um pacote passa de um domínio a outro, seu campo DS pode ser remarcado ou não, de acordo com o SLA estabelecido entre os dois domínios.

Através da utilização de mecanismos de classificação, policiamento, conformação e escalonamento muitos serviços podem ser fornecidos, como serviços com baixo atraso e baixo *jitter* ou serviços com maior confiabilidade do que o serviço *Best effort* padrão.

Dois PHBs foram publicados pelo IETF: o PHB EF (*Expedited Forwarding*) [JAC 99] e o PHB AF (*Assured Forwarding*) [HEI 99].

A arquitetura de serviços diferenciados define apenas valores para o campo DS e PHBs. É de responsabilidade dos ISP decidir quais serviços vão suportar [ARM 2000].

2.2.1 PHBs e Codepoints

Os PHBs especificam as características de enfileiramento e escalonamento de cada serviço. Esta metodologia permite que os ISPs tenham liberdade de escolha com relação aos algoritmos, como Weighted Fair Queueing (WFQ) [DEM 89] ou Class Based Queueing (CBQ) [FLO 95] para escalonamento, ou Random Early Detection (RED) [FLO 93] para gerenciamento de fila, que serão utilizados. Alguns PHBs são definidos com comportamentos bastante semelhantes e são tratados como grupos PHB. Por exemplo, PHBs que especificam comportamentos semelhantes de enfileiramento e escalonamento mas indicam diferentes prioridades de descarte.

Os PHBs são indicados por diferentes valores do DSCP. Apesar de cada definição de PHB indicar um DSCP recomendado, a arquitetura de serviços diferenciados permite que diversos valores do DSCP sejam mapeados em um mesmo PHB. Grupos PHB especificam diversos DSCP recomendados, tipicamente um para cada PHB específico dentro do grupo. Em [NIC 98] são definidas algumas diretrizes para a alocação dos valores dos DSCP, como visto na TABELA 2.1.

TABELA 2.1 - Alocação dos DSCP

DSCP	Utilização
xxxxx0	Atribuído pela IANA
xxxx11	Uso local/experimental
xxxx01	Uso local/experimental (Pode ser utilizado como padrão futuramente, se for o caso)

Fonte: [NIC 98]

O serviço *Best effort* tradicional é tratado como PHB Default, e tem 000000 como valor recomendado.

2.2.1.1 Class Selector Codepoints

Para fornecer compatibilidade com a antiga definição de precedência do campo TOS [BAK 95] são utilizados Class Selector Codepoints. Os Class Selector Codepoints são definidos de maneira que seus PHBs se aproximem dos tratamentos de pacotes definidos pelos níveis de precedência de IPv4. Os níveis de precedência e os Class Selector Codepoints equivalentes podem ser vistos na TABELA 2.2.

TABELA 2.2 - Class Selector Codepoints

Class Selector Codepoint	Precedência IPv4	
000000	000	Routine
001000	001	Priority
010000	010	Immediate
011000	011	Flash
100000	100	Flash override
101000	101	Critical
110000	110	Internet control
111000	111	Network control

Fonte: [NIC 98], [BAK 95]

2.2.1.2 O PHB EF (Expedited Forwarding)

O PHB EF é definido em [JAC 99]. Ele determina que todos os roteadores de um caminho sempre atendam os pacotes EF (pacotes cujo DSCP seja mapeado no PHB EF) com, pelo menos, a mesma velocidade com que estes pacotes chegam. Esta situação leva a três outras determinações:

- Todo o tráfego EF que entra no domínio deve ser policiado e conformado para limitar sua taxa de entrada;
- Os roteadores do núcleo da rede devem ser configurados para atender uma quantidade de tráfego EF superior à taxa máxima esperada;
- O tratamento do tráfego EF no núcleo da rede não deve ser afetado pela quantidade de tráfego não-EF esperando para ser atendido.

Apesar de, na prática, os pacotes EF serem enviados para uma fila específica para posterior escalonamento, a definição do PHB EF é tal que normalmente esta fila estará praticamente vazia ou mesmo vazia. Como conseqüência, o PHB EF é adequado para serviços com baixas perdas, baixo atraso e baixo *jitter*.

Para indicar o PHB EF é utilizado apenas um DSCP: 101110. É importante notar que apesar deste PHB ser fácil de definir, um serviço baseado no PHB EF necessita de uma cuidadosa coordenação entre policiamento, conformação e escalonamento nos caminhos que os pacotes EF poderão seguir [ARM 2000].

2.2.1.3 O PHB AF (Assured Forwarding)

O PHB AF é definido em [HEI 99]. Na verdade consiste de um grupo PHB com serviços especificados em termos da largura de banda relativa disponível e políticas de descarte de pacotes. Enquanto o PHB EF suporta um serviço com características estritas de largura de banda e *jitter*, o grupo PHB AF permite um compartilhamento mais flexível dos recursos da rede.

Em [HEI 99] são definidos 4 classes de serviço, cada uma suportando independentemente as características AF. Dois contextos distintos de classificação são codificados no DSCP: a classe de serviço e a precedência de descarte do pacote. A classe de serviço define em qual fila o pacote será armazenado, e assim, quanto da largura de banda esta classe de serviço receberá do escalonador. Já a precedência de descarte indica a possibilidade de o algoritmo de gerência de fila descartar o pacote, mais ou menos agressivamente caso a precedência de descarte seja, respectivamente, alta ou baixa.

Apesar de a definição do PHB AF não exigir um algoritmo específico de gerenciamento da fila, ele se adapta muito bem aos algoritmos RED [FLO 93], o qual mantém baixo o tamanho médio da fila, enquanto permite rajadas ocasionais de pacotes e RIO [CLA 98], uma versão aprimorada de RED.

Pode-se considerar que o DSCP seja codificado no formato cccpp0. Onde ccc indica a classe de serviço e pp a precedência de descarte. A TABELA 2.3 indica os valores DSCP associados com cada classe de serviço e nível de precedência.

TABELA 2.3 - Classes AF e DSCP

Precedência de descarte / Classe	AF1	AF2	AF3	AF4
1 – Baixa	001010	010010	011010	100010
2 – Média	001100	010100	011100	100100
3 – Alta	001110	010110	011110	100110

Fonte: [HEI 99]

Apesar do DSCP indicar uma das filas, ele não especifica nem o tamanho máximo desta fila nem o intervalo de serviço destinado a ela pelo escalonador. Estes parâmetros são configurados pela gerência da rede, dependendo da qualidade de serviço desejada de cada uma das classes de serviço. Cada classe de serviço é distinguida das demais pela quantidade de recursos recebidos, em cada nó da rede, independentemente das outras classes, o que implica na utilização de um escalonador como *Weighted Fair Queueing* (WFQ) [DEM 89], *Deficit Round Robin* (DRR) [SHR 95] ou similar.

A probabilidade de descarte de cada nível de precedência também é configurada pela gerência da rede, de forma a refletir as características desejadas de descarte de pacotes de cada classe. O único requisito é que a probabilidade de descarte da precedência alta (3) deve ser maior do que a da precedência média (2), e que esta seja maior do que a da precedência baixa (1). Apesar de [HEI 99] definir 3 níveis de precedência de descarte, uma implementação mínima do PHB AF pode contar com apenas 2 níveis de precedência, bastando mapear os níveis 2 e 3 para a mesma função de cálculo da probabilidade de descarte.

Como no PHB EF, a configuração de serviços AF exige coordenação entre os roteadores de borda, para limitar o tipo de tráfego mapeado para cada classe AF, e os roteadores de núcleo, para garantir que os recursos apropriados sejam fornecidos para cada classe [ARM 2000].

2.3 A arquitetura MPLS

MPLS é uma evolução de diversas tecnologias proprietárias como *IP Switch*, da Nokia e *Tag Switching* da Cisco. Resumidamente, MPLS é um esquema avançado de envio, baseado no princípio da comutação de pacotes. Considerando o modelo OSI de 7 camadas, MPLS se encontra entre a segunda camada, ou camada de enlace, e a terceira camada, ou camada de rede [XIA 99].

A idéia de se utilizar a comutação de pacotes IP teve como motivação a necessidade de diminuir a latência de propagação de pacotes para comportar o crescimento contínuo da Internet, e suportar as novas aplicações que iam surgindo. Entretanto, hoje sua maior motivação é viabilizar uma engenharia de tráfego que propicie uma operação mais eficaz das redes.

MPLS segue o modelo par, onde o plano de controle é unificado através da manutenção das funções referentes ao protocolo de rede, como IP, e eliminando as funções específicas da malha de comutação. Desta maneira, elimina-se a sobreposição de funções de controle e as excessivas conexões mantidas pelos roteadores [MAG 2001].

2.3.1 Componentes da arquitetura MPLS

Uma rede MPLS consiste de equipamentos de comutação habilitados para MPLS. Estes equipamentos são denominados Roteadores de comutação por rótulos, ou LSR. Um LSR localizado na fronteira de uma rede MPLS é denominado LSR de borda, enquanto um LSR no núcleo da rede é denominado LSR de núcleo [ROS 2001a].

Em MPLS os caminhos comutados são denominados caminhos comutados por rótulos, ou LSPs. LSPs são estabelecidos por ação de protocolos do plano de controle, ou por ação da gerência de rede.

Um LSP é uma seqüência ordenada de LSRs, sendo que o primeiro LSR é o LSR de ingresso e o último é o LSR de egresso (vide a FIGURA 2.5). Um LSP é similar a um circuito virtual ATM, sendo unidirecional no sentido da origem para o destino.

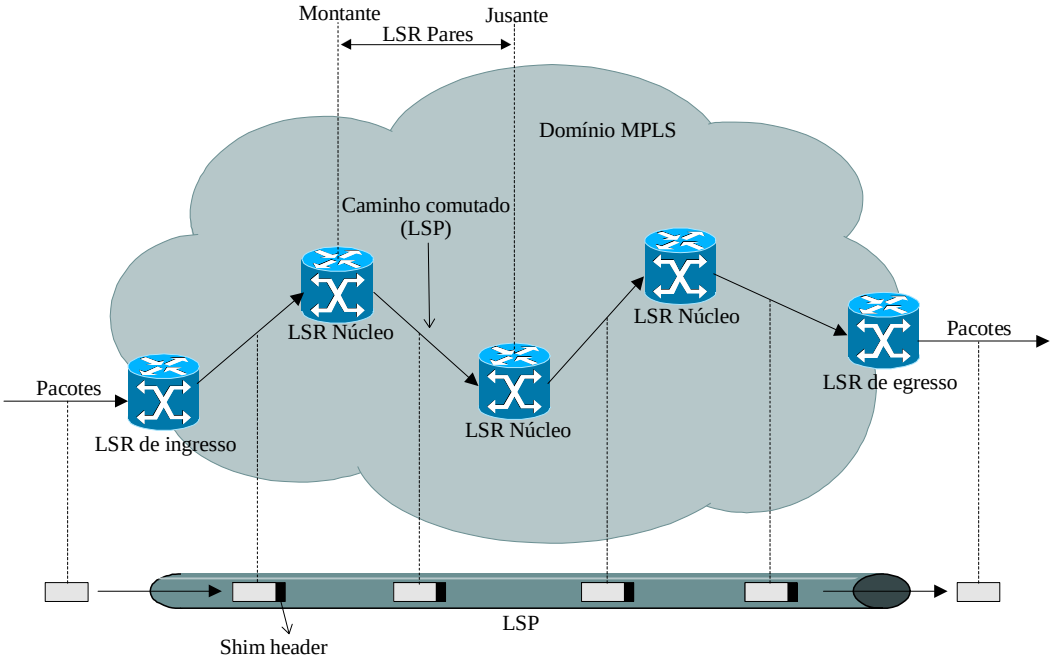

FIGURA 2.5 - Elementos da arquitetura MPLS [MAG01]

A configuração de um LSP pode ser feita com o auxílio de um protocolo de roteamento (orientado por topologia), como OSPF, ou então a partir da requisição de um LSP por um fluxo ou agregado (TT – *Traffic Trunk*) de fluxos (orientado por fluxo).

No caso de se utilizar OSPF no estabelecimento dos LSPs os pacotes enviados através do LSP seguem a mesma rota dos pacotes enviados pelo roteamento convencional. Um LSP pode ser estabelecido também segundo roteamento baseado em restrições, por exemplo, roteamento na origem ou roteamento com QoS.

Para poder controlar efetivamente o caminho de um LSP, pode-se conferir a ele um ou mais atributos, como largura de banda ou prioridades de estabelecimento e manutenção. Estes atributos vão ser considerados no momento em que o caminho do LSP for calculado [XIA 2000].

O roteamento de LSPs corresponde ao método selecionado para a escolha da rota durante o estabelecimento de um LSP. Em MPLS existem duas opções de estabelecimento de rotas [ROS 2001a]:

- Roteamento *hop-by-hop*: cada LSR escolhe de forma independente o próximo *hop*. É correspondente à forma tradicional de roteamento IP;
- Roteamento explícito: os LSRs não são autônomos na escolha do próximo *hop*. Normalmente o LSR de ingresso, ou egresso, especifica todos (estrito) ou parte (fraco) dos LSR que compõe o LSP.

Geralmente o roteamento explícito pode ser efetuado através de configuração ou dinamicamente. Neste último caso, com base em protocolos de roteamento que tenham o conceito de estado do enlace. O maior interesse no roteamento explícito está na possibilidade de realização de engenharia de tráfego.

Para configurar um LSP, MPLS necessita de um protocolo capaz de distribuir rótulos. Existem duas propostas de protocolos para suprir esta demanda. A primeira é o *Label Distribution Protocol* (LDP) [AND 2001], e sua extensão CR-LDP (*Constraint Routing - Label Distribution Protocol*) [JAM 2002], [ASH 2002a], um novo protocolo criado especialmente para esta função, baseado em TCP e com sessões *hard-state*. A segunda é o protocolo RSVP-TE (*Resource Reservation Protocol – Traffic Engineering*) [AWD 98], [AWD 2001a], [AWD 2001b], uma extensão de RSVP, que utiliza UDP e sessões *soft-state*. Devido às suas características *hard-state*, acredita-se que LDP/CR-LDP será mais escalável do que RSVP-TE, e graças à confiabilidade fornecida por TCP, a resposta à falhas de CR-LDP será mais rápida e confiável. Análises comparativas de ambos protocolos podem ser encontradas em [SER 2001A] e [GHA 99].

2.3.2 Shim Header

Os LSPs são caminhos comutados, os quais são equivalentes a conexões, portanto, existe a necessidade de rótulos para identificá-los. Os rótulos são locais ao enlace, sendo alocados pelo LSR a jusante (*downstream*) do fluxo e distribuídos pelo LSR a montante (*upstream*) do fluxo por ocasião do estabelecimento da conexão. Idealmente, os rótulos devem coincidir com identificadores de conexões de enlace. Entretanto, muitas tecnologias de enlace não empregam identificadores de conexão, como, por exemplo, enlaces PPP e *Ethernet*. Para estas situações MPLS define uma estrutura chamada *Shim header* [ROS 2001a] (ver FIGURA 2.6), que é posicionada entre o cabeçalho do enlace e sua carga.

Esta estrutura contém um rótulo de 20 bits, um campo Experimental de 3 bits, um indicador de pilha de rótulos de 1 bit (campo B) e um campo de tempo de vida, ou TTL, de 8 bits. O objetivo do campo B é indicar se o rótulo corresponde, ou não, ao último de uma pilha de rótulos, o que permite o encapsulamento de múltiplos rótulos [ROS 2001b].

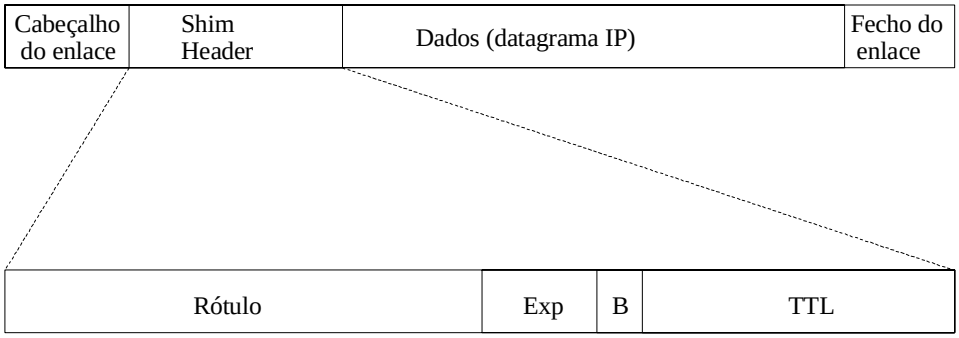

FIGURA 2.6 - *Shim header*

2.3.3 Funcionamento

Os pacotes que chegam a um domínio MPLS são classificados e roteados no LSR de ingresso do domínio, com base nas informações presentes no cabeçalho do pacote e nas informações de roteamento locais mantidas pelos LSRs. O *shim header* é inserido neste ponto.

Cada LSP está associado a uma classe equivalente de envio, ou FEC. Uma FEC determina quais pacotes serão enviados pelo LSP. FECs que tenham como LSR de egresso o mesmo LSR podem ser agregadas em uma só FEC, ou em um conjunto de menor cardinalidade de FECs. O LSR de ingresso, ao receber um pacote verifica se o mesmo pertence a uma FEC. Em caso afirmativo, o pacote é enviado através do LSP associado àquela FEC, caso contrário o pacote é enviado conforme as definições do protocolo IP padrão (*hop-by-hop*).

Quando um LSR recebe um pacote rotulado, ele utiliza o rótulo como índice na LIB. Isto é mais rápido do que o processo de busca na tabela roteamento feita pelo processo de roteamento IP. O pacote é então processado de acordo com as informações da LIB: o rótulo de entrada é substituído pelo rótulo de saída e o pacote é comutado para o próximo LSR. O processo de troca de rótulos é similar ao processamento de VPI/VCI presente em *switches* ATM.

Dentro de um domínio MPLS, o envio de pacotes, a classificação e o QoS são determinados pelos rótulos. Isto torna os LSRs do núcleo da rede mais simples.

Antes de um determinado pacote sair do domínio MPLS, o LSR de egresso remove o *shim header*. Todo o processo pode ser visto na **FIGURA 2.7**.

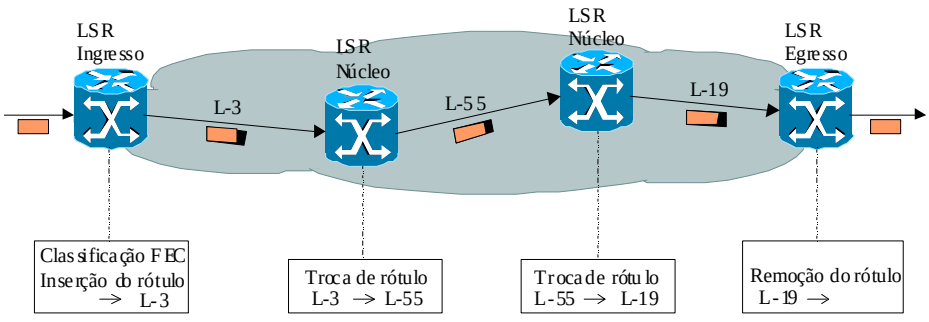

FIGURA 2.7 - Funcionamento básico do MPLS

Os LSPs podem ser utilizados como túneis. Depois de os LSPs serem configurados, o caminho que um pacote vai percorrer dentro do domínio MPLS pode ser determinado pelo rótulo atribuído pelo LSR de ingresso. Não existe a necessidade de enumerar cada LSR pelo qual o pacote deve passar. Em comparação com outros mecanismos de tunelamento, MPLS é único no sentido de que pode controlar todo o caminho de um pacote sem precisar especificar explicitamente os LSR intermediários [XIA 99].

O conceito de MPLS, apesar de ser simples em sua concepção, altera consideravelmente a característica mais marcante das redes IP, qual seja, a inexistência de conexões no nível de rede. Pois ao se impor um caminho comutado ao pacote, estabelece-se uma conexão implícita no nível de rede [MAG 2001].

2.3.4 Engenharia de Tráfego

A Engenharia de Tráfego pode ser definida como a tarefa de realizar o mapeamento dos fluxos de tráfego em uma infra-estrutura física de transporte de modo a atender critérios estabelecidos pela gerência de rede. Como resultado direto da ação da Engenharia de Tráfego é possível mover o tráfego para caminhos diferentes do caminho mais curto determinado pelo IGP. Conseqüentemente é viável balancear o tráfego de modo a ocupar os vários *links* e elementos de rede de modo que nenhum destes componentes fique super ou subutilizados [MAG 2001].

Os componentes de Engenharia de Tráfego associados a MPLS podem ser organizados nos seguintes elementos [MAG 2001]:

- Encaminhamento dos pacotes: é a função primordial de MPLS como visto nas seções anteriores. O aspecto mais importante é que o caminho a ser seguido por um LSP não é limitado àquele que o IGP escolheria como caminho mais curto;
- Distribuição das informações: a implementação deste elemento se dá através de extensões aos IGPs existentes, como OSPF, de modo que os atributos dos *links* sejam incluídos nas mensagens de anúncio de estado;
- Seleção do caminho: baseia-se em um algoritmo CSPF (*Constraint Shortest Path First*) utilizado pelo roteamento baseado em restrições. Este algoritmo procura determinar um caminho para o LSP que leve em consideração as restrições impostas aos elementos de rede (políticas administrativas, etc.) e que atenda aos atributos do LSP (largura de banda, prioridade, etc.);
- Sinalização: é o responsável pelo estabelecimento do estado do LSP e pela distribuição dos rótulos. Duas opções possíveis são extensões aos protocolos LDP e RSVP (Mais detalhes em [SER 2001A]).

A utilização de MPLS para Engenharia de Tráfego traz diversas vantagens [MAG 2001], [SWA 99], [FAU 2002b]:

- MPLS permite esquemas avançados de roteamento baseados na capacidade de estabelecimento de LSPs explicitamente roteados;
- Agregados de tráfego (TT) podem ser mapeados em LSPs;
- MPLS permite tanto agregação, como desagregação de tráfego;
- É relativamente simples integrar o roteamento baseado em restrições;
- Aumento da escalabilidade da rede;

- Simplificação do processo de integração de serviços;
- Recuperação automática de falhas (re-roteamento);
- Gerenciamento simplificado.

2.4 Por que integrar diferentes arquiteturas de QoS?

A arquitetura de Serviços Integrados, apesar de fornecer um alto nível de garantia de reserva de recursos por fluxo, tem sérios problemas de escalabilidade e complexidade. Já a arquitetura de Serviços Diferenciados, por sua vez, é simples e escalável, mas apresenta deficiências no gerenciamento de recursos. Outro problema é que a arquitetura de Serviços Diferenciados foi planejada para IP, mas seria interessante aplicá-la diretamente em tecnologias de enlace como ATM e *Frame Relay*.

Tanto a arquitetura de Serviços Integrados, como a de Serviços Diferenciados, utiliza o processo de roteamento IP da camada de rede. No entanto, o processo de roteamento na camada de rede é mais lento do que a comutação na camada de enlace. Além disso, o processo de roteamento é baseado no conceito SPF (*Shortest Path First*) que não utiliza eficientemente a infra-estrutura de rede causando o surgimento de gargalos. Estes problemas podem ser resolvidos com a utilização de Engenharia de Tráfego, em conjunto com MPLS.

A observação de que nenhuma das arquiteturas atende todos os requisitos para se fornecer uma garantia de QoS fim a fim, além do fato de a Internet ser uma rede heterogênea, onde sempre haverá a necessidade de interoperação de diversas tecnologias diferentes, tem propiciado o surgimento de modelos que combinam estas arquiteturas. Todas elas são vistas como complementares no provisionamento de QoS fim a fim. Desta maneira, procura-se unir suas vantagens em uma única implementação, como em [FAU 2002a], [BER 2000], [XIA 99], [RAJ 99] e [LI 98].

3 Modelos de Integração existentes

Nas seções a seguir serão apresentados diversos modelos de integração existentes, incluindo os dois modelos [BER 2000a], [FAU 2002a] utilizados neste trabalho. O modelo de Bernet et al. [BER 2000] propõe mecanismos para a interoperação das arquiteturas de Serviços Integrados e Serviços Diferenciados. A proposta de Rajan et al. examina as questões que surgem durante a definição, implantação e gerenciamento de políticas relacionadas à Qualidade de Serviço em uma rede IP. O modelo de Xiao et al. apresenta duas propostas de integração utilizando Serviços Integrados nos clientes e Serviços Diferenciados ou MPLS nos ISPs. O modelo de Li et al. apresenta uma proposta que integra Serviços Diferenciados e MPLS com RSVP para sinalização. Por último, o modelo de Le Faucheur et al. [FAU 2002a], [FAU 2001a] propõe um modelo de integração de MPLS e Serviços Diferenciados.

3.1 O modelo de Bernet et al.

Esta proposta está detalhada em [BER 2000a]. Trata-se de um modelo que combina a arquitetura de Serviços Integrados e a arquitetura de Serviços Diferenciados. Baseia-se em uma ou mais regiões que oferecem Serviços Diferenciados no meio de uma grande rede que suporta Serviços Integrados fim a fim. De modo simplificado, procura-se utilizar a arquitetura de Serviços Diferenciados nas redes centrais, chamadas redes de trânsito (ISPs), enquanto emprega-se a arquitetura de Serviços Integrados nas redes das extremidades (clientes), como visto na FIGURA 3.1.

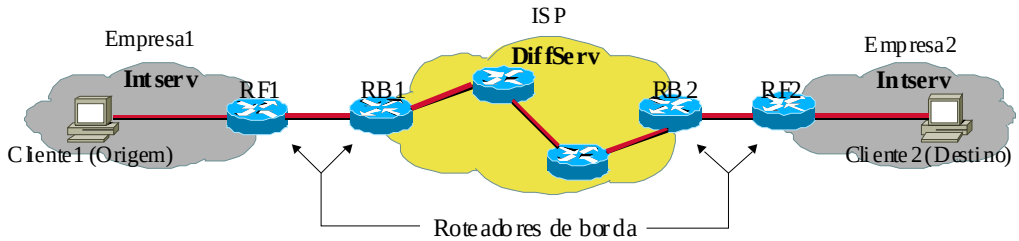

FIGURA 3.1 - O modelo de Bernet et al.

Neste modelo, os roteadores de borda entre uma região e outra desempenham papel fundamental, pois são eles os responsáveis pelo mapeamento das capacidades entre as diferentes regiões. Dentre os vários aspectos deste mapeamento, pode-se destacar: a escolha de um PHB para os fluxos, e a realização do controle de admissão, de acordo com os recursos disponíveis nas regiões de Serviços Diferenciados [BER 2000a].

Exatamente como essas funções serão realizadas depende da forma como os recursos são gerenciados dentro das redes de Serviços Diferenciados. [BER 2000] sugere três formas de se fazer este gerenciamento: estaticamente; dinamicamente, utilizando RSVP, ou dinamicamente utilizando outros meios, como um negociador (*broker*) de banda.

O conceito principal é de que as aplicações usem o protocolo RSVP para requisitar a admissão de seus fluxos na rede. Se a requisição for aceita, significa que existem recursos disponíveis nas redes de Serviços Integrados, bem como que os serviços requisitados foram mapeados em uma classe de serviços compatível dentro da

rede de Serviços Diferenciados. Os elementos da rede de Serviços Diferenciados devem ser capazes de transportar as mensagens RSVP até a rede de Serviços Integrados na outra extremidade, de modo que a reserva de recursos possa ser feita dentro desta última também. As redes de Serviços Diferenciados podem, mas não são obrigadas, a participar do processo de sinalização fim a fim, baseado em RSVP [BER 2000a]. Do ponto de vista de Serviços Integrados, as redes de Serviços Diferenciados são tratadas como *links* virtuais conectando elementos da rede de Serviços Integrados. Dentro das redes de Serviços Diferenciados, os elementos de rede implementam controle de tráfego agregado por classe. A quantidade de tráfego que será admitida nas redes de Serviços Diferenciados poderá ser controlada através de policiamento nos elementos de entrada da rede.

O modelo proposto em [BER 2000a] considera dois casos específicos: no primeiro, os recursos dentro da região de Serviços Diferenciados são distribuídos estaticamente e estas regiões não possuem dispositivos aptos a processar RSVP. No segundo, os recursos dentro das regiões de Serviços Diferenciados são alocados dinamicamente e os dispositivos dentro dessas regiões participam da sinalização RSVP.

Os roteadores de fronteira das redes de Serviços Integrados, denominados RF1 e RF2 (ver FIGURA 3.1), têm funcionalidades que variam dependendo do tipo de modelo adotado [BER 2000a]. No modelo onde as regiões de Serviços Diferenciados não processam RSVP, os roteadores RF funcionam como agentes de controle de admissão das redes de Serviços Diferenciados. Eles processam as mensagens de sinalização tanto dos emissores quanto dos receptores e aplicam o controle de admissão baseado na disponibilidade de recursos dentro da rede de Serviços Diferenciados e nas políticas de alocação definidas com os clientes (SLA).

No modelo em que as regiões de Serviços Diferenciados processam RSVP, os roteadores RF aplicam o controle de admissão baseado na disponibilidade de recursos locais (Serviços Integrados) e na política de alocação definida com os clientes (SLA). Neste último caso, são os roteadores de borda das redes de Serviços Diferenciados, chamados RB, que executam o controle de admissão (ver FIGURA 3.1) [BER 2000a].

Os roteadores RB, situados nas fronteiras das regiões de Serviços Diferenciados, também possuem funcionalidades que variam de acordo com o modelo adotado para a rede. Se as regiões de Serviços Diferenciados não são capazes de processar RSVP, então os roteadores RB agem como roteadores de Serviços Diferenciados puros, ou seja, eles apenas policiam o tráfego baseado no nível de serviço especificado no campo DS e no SLA negociado com o cliente. No entanto, se as regiões de Serviços Diferenciados são capazes de processar RSVP, os roteadores RB participam da sinalização RSVP e atuam como agentes de controle de admissão para as regiões de Serviços Diferenciados [BER 2000a].

3.1.1 Gerenciamento estático dos recursos das redes de Serviços Diferenciados

Neste caso, nenhum dispositivo das redes de Serviço Diferenciado está apto a processar RSVP. Os recursos das redes de Serviços Diferenciados são alocados estaticamente. Para tanto, o cliente e o administrador da rede de Serviço Diferenciado negociam um SLA estático, que determina quais os recursos a serem disponibilizados para o cliente em cada nível de serviço [BER 2000a].

Esses recursos podem ser simplesmente uma determinada quantidade de banda, ou mesmo um conjunto mais complexo envolvendo outros fatores como taxa de pico, tamanho da rajada, hora do dia, etc.

Cada roteador de fronteira, RF, na rede de Serviços Integrados do cliente deve ser composto de duas partes: uma parte Serviços Integrados, que interage com a rede do cliente, e uma parte Serviços Diferenciados, que, por sua vez, interage com a rede de Serviços Diferenciados. A parte Serviços Integrados está apta a identificar e processar o tráfego de acordo com forma padrão de Serviços Integrados, ou seja, por fluxo.

Já a parte Serviços Diferenciados do roteador de fronteira pode ser considerada como consistindo de um determinado número de *links* virtuais, um para cada classe de serviço negociada no SLA [BER 2000a]. O roteador deve manter uma tabela que indica os recursos a serem disponibilizados para cada classe de serviço, de acordo com o SLA firmado. Esta tabela em conjunto com o campo DS é utilizada para realizar o controle de admissão no fluxo que irá atravessar a rede de Serviços Diferenciados.

Existem várias possibilidades de se agregar (mapear) fluxos de Serviços Integrados para classes de Serviços Diferenciados. Um exemplo é sugerido em [WRO 2001], e pode ser visto na TABELA 3.1.

TABELA 3.1 - Mapeamento de Serviços Integrados em Serviços Diferenciados

Serviços Integrados	Serviços Diferenciados
Best effort	*Best effort*
Carga controlada	*Assured Forwarding* (AF)
Garantido	*Expedited Forwarding* (EF)

Fonte: [WRO 2001]

Na FIGURA 3.1 a máquina Cliente1 deseja enviar dados para a máquina Cliente2. A seguinte seqüência ilustra o processo através do qual uma aplicação obtém qualidade de serviço [BER 2000a]:

1. A máquina Cliente1 envia uma mensagem RSVP PATH descrevendo o fluxo que ela deseja transmitir;
2. A mensagem RSVP PATH é transmitida na direção da máquina destino, Cliente2. No domínio onde Cliente1 está conectado efetua-se o processamento RSVP/Serviços Integrados padrão nos nós aptos para tal;
3. Na fronteira da rede o roteador RF1 processa a mensagem RSVP PATH de acordo com o processamento RSVP padrão, e as informações de estado são instaladas no roteador. A mensagem RSVP PATH é enviada para a região de Serviços Diferenciados;
4. A mensagem RSVP PATH é ignorada pelos roteadores na região de Serviços Diferenciados. Ao chegar em RF2 ela é processada de acordo com as regras de processamento RSVP;
5. Quando a mensagem RSVP PATH chega a máquina Cliente2, esta, em resposta, envia uma mensagem RSVP RESV;
6. A mensagem RSVP RESV é transmitida de volta pela região de Serviços Diferenciados até a máquina Cliente1. Consistentemente com o processamento RSVP/Serviços Integrados padrão, ela pode ser rejeitada em qualquer um dos nós aptos a processar mensagens RSVP, caso os recursos sejam insuficientes para suportar o tráfego;
7. No roteador RF1 a mensagem RSVP RESV dispara o controle de admissão. RF1 compara os recursos requisitados com os recursos disponíveis na região de Serviços Diferenciados para a classe de serviço correspondente,

determinado através do processo de mapeamento mostrado anteriormente, além de poder levar em consideração critérios administrativos;

8. Se RF1 aprova a requisição a mensagem RSVP RESV é admitida e transmitida para a máquina Cliente1. RF1 também atualiza suas tabelas para indicar a nova capacidade disponível para a classe de serviço cuja requisiçao foi aprovada. Caso não seja aprovada a requisição, a mensagem RSVP RESV não é transmitida e as mensagem RSVP de erro apropriadas são enviadas;
9. A mensagem RSVP RESV chega à maquina Cliente1 indicando que o fluxo requisitado foi admitido.

3.1.2 Gerenciamento dinâmico utilizando RSVP

Neste caso os roteadores RB são capazes de processar mensagens RSVP e, além disso, outros roteadores da rede de Serviços Diferenciados podem ser capazes de processar mensagens RSVP. Assim, o controle de admissão faz parte da rede de Serviços Diferenciados e mudanças na rede de Serviços Diferenciados podem ser indicadas para os roteadores das redes periféricas de Serviços Integradas através de RSVP [BER 2000a].

Ao incluir roteadores da rede de Serviços Diferenciados no processo de sinalização RSVP é possível aumentar a eficiência na utilização de recursos dentro da rede de Serviços Diferenciados e simultaneamente melhorar o nível de confiança de que os recursos requisitados ao controle de admissão estarão disponíveis. Isto porque o controle de admissão vai estar ciente da disponibilidade de recursos através do caminho que será utilizado. Outro benefício de se utilizar a sinalização RSVP dentro da rede de Serviços Diferenciados é a possibilidade de efetuar alterações nas reservas de recursos em resposta a uma nova requisição de recursos efetuada do lado de fora das regiões de Serviços Diferenciados [BER 2000a].

3.2 O modelo de Rajan et al.

Esta proposta está detalhada em [RAJ 99] e especifica a regulamentação do acesso aos recursos e serviços da rede baseando-se em critérios administrativos. No caso de Serviços Integrados existe a necessidade de fornecer um controle baseado em políticas para cada fluxo, além de uma regulamentação de como eles devem efetuar a reserva de recursos da rede. Já o caso de Serviços Diferenciados depende de um controle administrativo da largura de banda disponível, do atraso e das precedências de descarte, ao invés de uma sinalização por fluxo, para comunicar informações sobre o nível de serviço desejado para os elementos da rede.

Assim, os operadores da rede obtêm maneiras de regular quais usuários, aplicações, ou servidores podem ter acesso a quais recursos ou serviços disponibilizados, e ainda, em que condições o acesso pode ser feito. A implantação em larga escala destes serviços depende da presença de uma infra-estrutura de políticas que abranja toda a rede, permitindo que os ISPs regulamentem sua rede ao invés de configurar individualmente cada elemento de rede.

Uma infra-estrutura de políticas é o conjunto de protocolos, modelos de informação e serviços que permitem que os objetivos administrativos sejam traduzidos em tratamentos diferenciados de pacotes dos diversos fluxos da rede [RAJ 99].

3.2.1 Políticas

Uma política pode ser definida como a regulamentação unificada do acesso aos recursos e serviços de uma rede, baseando-se em critérios administrativos. Como pode ser visto na FIGURA 3.2 existem diferentes níveis onde estas regulamentações podem ser expressas e utilizadas.

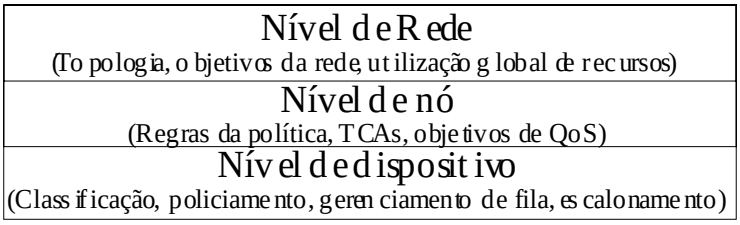

FIGURA 3.2 - Níveis de política

O nível de rede é uma perspectiva intuitiva de alto nível da topologia, da conectividade, dos objetivos de performance fim a fim e do estado dinâmico da rede. Este nível é composto por diferentes níveis de nó, que correspondem aos objetivos e requisitos das políticas em diversos nós da rede. Por fim, os níveis de nó são compostos por diversas regras de política que podem ser vistas como a maneira de se controlar diversos elementos da rede. Por exemplo, o nível de rede correspondente a seguinte situação: um administrador deseja que todo o tráfego HTTP de um determinado servidor utilize uma reserva de 2Mb/s, enquanto todo o tráfego UDP seja transmitido como tráfego *Best effort*, é composto por diversos níveis de nó, cada um correspondente a um dispositivo diferente (servidor, roteadores, etc.) que pode participar no cumprimento da política da rede [RAJ 99].

Dentro deste *framework* abstrato é necessária uma maneira padronizada de descrever, armazenar e informar as políticas, de forma que qualquer solução de gerenciamento de rede baseada em políticas possa funcionar em ambientes heterogêneos.

3.2.2 Requisitos para políticas de QoS

Para suprir as necessidades dos operadores de rede com relação ao acesso à recursos que forneçam QoS, diversas maneiras para discriminar os fluxos são propostas:

- As máquinas origem e destino dos fluxos;
- A rota utilizada;
- Os usuários ou grupos de usuários;
- Tipo de aplicação;
- Características dinâmicas da rede;
- Horário.

Enquanto algumas destas informações são facilmente inferidas dos pacotes trafegando pela rede, muitas das políticas úteis necessitarão de informações como identificação do usuário, ou então de coordenação entre diversos elementos de rede. Assim, a implantação de políticas é melhorada consideravelmente através de

mecanismos de transmissão de informações necessárias para cumprimento das políticas [RAJ 99].

Os critérios acima são úteis para discriminar fluxos ou grupos de fluxos e não são estranhos às políticas de QoS. Entretanto, existem situações específicas que são resolvidas, no caso de Serviços Integrados ou Diferenciados, com o controle sobre a alocação de recursos [RAJ 99].

3.2.2.1 Serviços Integrados resguardados através de sinalização RSVP

Em sua maneira mais simples as políticas podem ser utilizadas para controlar o número, o tamanho e a natureza das reservas feitas por RSVP, permitindo o controle das requisições do QoS em nível de fluxo, usuário ou aplicação. No entanto, diversas políticas mais interessantes necessitam de informações codificadas nos objetos das mensagens RSVP.

3.2.2.2 Proxy RSVP

Diz respeito ao estabelecimento de túneis RSVP entre roteadores ou outros elementos da rede e aos fluxos trafegando por dentro deles. Existem 3 instâncias comuns: túneis para tráfego *Best effort*, agregação de fluxos RSVP e mapeamentos de outras arquiteturas de QoS (Serviços Diferenciados, por exemplo) utilizando RSVP para a sinalização.

3.2.2.3 Serviços Diferenciados resguardados através de provisionamento

Refere-se à utilização de políticas para especificar e controlar a utilização de Serviços Diferenciados em um domínio e entre domínios. No último caso as políticas são utilizadas para mapear acordos bilaterais (SLAs) e para cumprimento das restrições de acesso.

3.2.2.4 Tunelamento de diversas tecnologias de QoS através de Serviços Diferenciados

RSVP ou outros protocolos de sinalização podem ser utilizados em um domínio e mapeados em Serviços Diferenciados em outros domínios. Neste caso as políticas são necessárias para mapear entre Serviços Integrados e Serviços Diferenciados, além do cumprimento de restrições de acesso.

3.2.3 Arquitetura das políticas

Um modelo generalizado do *framework* de políticas pode ser visto na FIGURA 3.3. A arquitetura mostra os diferentes componentes relacionados às políticas que podem existir em um domínio.

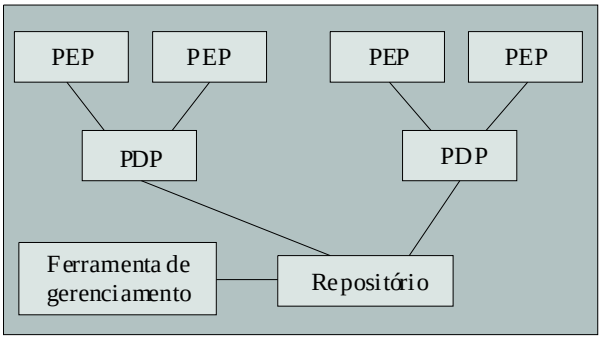

FIGURA 3.3 - Modelo generalizado de política

O modelo é composto de 3 camadas: pontos de cumprimento das políticas (PEP – *Policy Enforcement Point*), pontos de decisão de políticas (PDP – *Policy Decision Points*) e um repositório de políticas [RAJ 99].

Os PEPs são os componentes que encontram os pacotes e forçam o cumprimento das políticas estabelecidas. Eles podem tomar ações como filtragem, marcação, conformação e etc.

Os PDPs são responsáveis por determinar quais ações são aplicáveis a quais pacotes. O PDP interpreta as regras das políticas para um ou mais PEPs baseando-se nos dados presentes nos pacotes, nas condições atuais da rede ou ainda em outras informações, como endereços alocados dinamicamente.

O repositório de políticas é o local onde todas as políticas definidas para o domínio são armazenadas. As políticas são armazenadas no repositório por meio de uma ferramenta de gerenciamento de políticas.

Existe também um modelo arquitetural com apenas 2 níveis que advém do fato de que existem elementos de rede poderosos e flexíveis o suficiente para tomar decisões com relação às políticas juntamente com as ações de cumprimento. Neste caso os PEPs e PDPs são combinados em apenas um elemento o Cliente de Políticas. Em uma rede é possível existir uma combinação dos modelos de 2 e 3 níveis de acordo com o tipo de equipamento sendo utilizado.

Para a comunicação entre domínios são utilizados negociadores de banda (BB – *Bandwidth Broker*) que negociam a natureza e a carga do tráfego que atravessará suas fronteiras em comum.

Para a comunicação entre PEPs e PDPs utiliza-se o protocolo COPS (*Common Open Policy Service*) [DUR 2000] e para a comunicação entre os PDPs e o repositório pode-se utilizar diversos protocolos, como por exemplo LDAP (*Lightweight Directory Access Protocol*) [WAH 97].

3.3 O modelo de Xiao et al.

Em [XIA 99] são propostos dois modelos de integração de diferentes tecnologias de QoS, como Serviços Diferenciados, RSVP e MPLS. Ambos são baseados em 2 tipos de serviços além do *Best effort*: o serviço Assegurado e o serviço Premium.

O serviço Assegurado fornece um serviço confiável, independentemente do nível de carga da rede. Normalmente é configurado através de SLAs estáticos e o usuário é responsável pela divisão da largura de banda, configurada no SLA, entre as aplicações. Os pacotes do serviço Assegurado são colocados em uma fila própria chamada AQ (*Assured Queue*) que é gerenciada por um algoritmo RIO [CLA 98]. Como os pacotes que se encontram dentro do perfil (*in-profile*) sofrem poucas perdas mesmo em

momentos de congestionamento, os clientes receberão um serviço previsível da rede desde que não excedam a largura de banda especificada no SLA. Quando a rede não estiver congestionada, os pacotes que se encontram fora do perfil (*out-profile*) também são entregues, otimizando a utilização da rede.

O serviço Premium fornece um serviço com baixo atraso e baixo *jitter*, para tráfego cuja taxa máxima de envio é fixa. O SLA especifica a taxa máxima de envio e é responsabilidade do cliente evitar que ela seja excedida, pois o tráfego em excesso será descartado. O ISP garante que a largura de banda estará disponível quando a transmissão for iniciada. O serviço Premium é adequado para aplicações de tempo real, como telefonia e videoconferência ou para o estabelecimento de VPNs (*Virtual Private Network*). Como o serviço Premium é mais caro do que o serviço Assegurado, é interessante para os ISPs suportar tanto SLAs estáticos como SLAs dinâmicos.

O serviço *Best effort* é tratado de maneira semelhante ao tráfego do serviço Assegurado que se encontra fora do perfil.

Para a alocação dos serviços dentro dos domínios dos clientes [XIA 99] propõe a utilização de negociadores de banda (BB – *Bandwidth Broker*). Em um estágio inicial de implantação, as máquinas não necessitam de nenhum mecanismo de Serviços Diferenciados, basta enviar os pacotes e deixar que os roteadores de saída os marquem adequadamente. Em estágios mais avançados, pode ser que as máquinas contem com algum mecanismo de sinalização ou marcação. Assim, antes de uma máquina iniciar a transmissão ela pode decidir sozinha qual serviço utilizar ou então pode consultar o BB. A própria máquina pode marcar os pacotes, ou então enviar os pacotes sem nenhuma marcação e deixar este serviço para os roteadores. Neste caso o BB vai precisar de protocolos como RSVP ou LDAP para configurar as regras de classificação, marcação e conformação nos roteadores para que estes saibam como tratar e marcar os pacotes.

Se existir a negociação de SLAs dinâmicos entre os clientes e os ISPs, o BB do domínio cliente deve utilizar algum protocolo para a requisição sob demanda de recursos do ISP. Assume-se que será utilizado para este fim o protocolo RSVP [XIA 99].

Para a alocação de recursos dentro dos domínios dos ISPs, deve-se examinar os SLAs e a partir deles decidir como serão configurados os roteadores de borda, de maneira que estes saibam como tratar o tráfego que entra no domínio do ISP [XIA 99]. Para os SLAs estáticos os roteadores podem ser configurados manualmente, desta maneira os recursos são alocados estaticamente para cada cliente. Para SLAs dinâmicos a alocação de recursos depende do método de sinalização. No caso do BB do domínio cliente utilizar RSVP para requisição de recursos do ISP, o controle de admissão pode ser feito de maneira distribuída pelos roteadores de borda, ou então de maneira centralizada pelo BB do ISP. Se os roteadores de borda estiverem envolvidos na sinalização eles são configurados com as regras correspondentes de classificação, policiamento e conformação no momento em que aceitam um pedido. Se o BB do ISP estiver envolvido na sinalização, este deve configurar os roteadores de borda quando aceita um pedido.

Em ambos os casos, os roteadores do núcleo do ISP não participam da sinalização para evitar problemas de escalabilidade.

O primeiro modelo de [XIA 99] integra Serviços Diferenciados e o protocolo RSVP para que seja possível negociar dinamicamente os SLAs. São mostrados dois exemplos deste modelo. O primeiro (ver FIGURA 3.4) mostra o fornecimento de um serviço Assegurado, com SLA estático. Já o segundo (ver FIGURA 3.5) mostra o fornecimento de um serviço Premium, com negociação dinâmica de SLA.

3.3.1 Fornecimento de serviço Assegurado com SLA estático

Na FIGURA 3.4, a máquina Cliente1 da rede corporativa da Empresa1 deseja enviar dados utilizando o serviço Assegurado para a máquina Cliente2 da rede corporativa da Empresa2. A Empresa1 possui um SLA estático com o ISP. O processo de fornecimento segue as etapas indicadas pelos números na FIGURA 3.4 e descritos a seguir [XIA 99]:

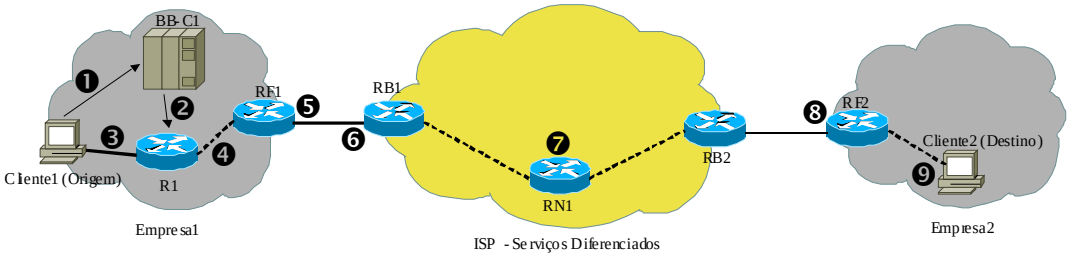

FIGURA 3.4 - Serviço Assegurado com SLA estático

1. A máquina Cliente1 envia uma mensagem RSVP para o BB local (BB-C1) requisitando o serviço Assegurado;
2. Se o BB aceita o pedido, então o roteador R1 será configurado para marcar os pacotes do fluxo como pacotes Assegurados e confirma o serviço para a máquina Cliente1, caso contrário Cliente1 receberá uma mensagem de erro;
3. Cliente1 começa a enviar pacotes para R1;
4. O roteador R1 marca os pacotes do fluxo como pacotes Assegurados;
5. Todos os outros roteadores no caminho até RF1 (inclusive) fazem uma classificação BA (*behavior aggregate*). Pacotes Assegurados serão considerados dentro do perfil (*in-profile*) enquanto os outros pacotes serão considerados fora do perfil (*out-profile*). Todos os pacotes entram em uma fila AQ na qual é utilizado o algoritmo RIO;
6. O roteador RB1 na entrada da rede do ISP policia o tráfego. Os pacotes fora do perfil continuam fora do perfil, e os pacotes dentro do perfil que excedam a taxa de envio configurada no SLA deixam de ser pacotes Assegurados. Todos os pacotes entram em uma fila AQ na qual é utilizado o algoritmo RIO;
7. Todos os roteadores entre RB1 e RB2 (inclusive) executam classificação BA e utilizam RIO em suas filas AQ;
8. O roteador RF2 executa as mesmas operações do roteador BR1 do ISP;
9. Os pacotes são entregues à máquina Cliente2.

3.3.2 Fornecimento de serviço Premium com SLA dinâmico

Na FIGURA 3.5, a máquina Cliente1 da rede corporativa da Empresa1, ou domínio Empresa1, deseja enviar dados utilizando o serviço Premium para a máquina Cliente2 da rede corporativa da Empresa2. A Empresa1 tem um SLA dinâmico com o ISP. O processo de fornecimento, neste caso, pode ser mostrado segundo duas fases distintas [XIA 99]:

- Sinalização, conforme etapas de 1 a 8;
- Transferência de dados, conforme etapas de 9 a 16.

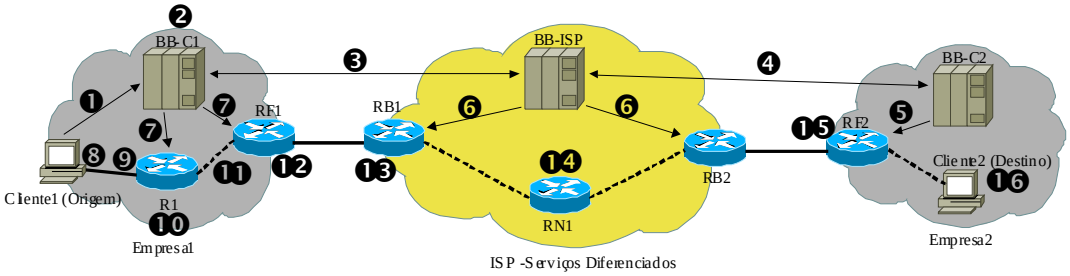

FIGURA 3.5 - Serviço Premium com SLA dinâmico

1. A máquina Cliente1 envia uma mensagem RSVP PATH ao BB local (BB-C1) do domínio corporativo da Empresa1;
2. BB-C1 efetua o controle de admissão. Se o resultado for negativo, envia uma mensagem de erro à máquina Cliente1 e o processo é encerrado;
3. Se a solicitação for aceita por BB-C1, este envia uma mensagem RSVP PATH ao BB do ISP (BB-ISP);
4. BB-ISP efetua o controle de admissão, se for negado, envia uma mensagem de erro à BB-C1, caso contrário, BB-ISP envia a mensagem RSVP PATH para o BB do domínio da Empresa2 (BB-C2);
5. BB-C2 efetua o controle de admissão. Se a solicitação for negada, retorna uma mensagem de erro à BB-ISP. Se aceito, BB-C2 utiliza o protocolo LDAP ou RSVP para configurar as regras de classificação e policiamento no roteador RF2, e envia uma mensagem RSVP RESV à BB-ISP;
6. BB-ISP ao receber a mensagem RSVP RESV configura as regras de classificação e policiamento de BR1 e as regras de policiamento e reconformação de BR2. Em seguida, envia a mensagem RSVP RESV à BB-C1;
7. BB-C1 ao receber a mensagem RSVP RESV configura as regras de classificação e conformação no roteador R1 e também define as regras de policiamento e reconformação no roteador RF1. Depois, manda a mensagem RSVP RESV para a máquina Cliente1;
8. A máquina Cliente1, ao receber a mensagem, fica liberada para enviar dados.
9. Cliente1 manda pacotes ao roteador R1;
10. R1 aplica classificação MF. Se o tráfego for não conformante, R1 faz a sua conformação. R1 também marca os pacotes do fluxo como pacotes Premium. Todos os pacotes entram na fila PQ;
11. Todos roteadores entre R1 e RF1 fazem classificação BA e encaminham os pacotes através da fila PQ;
12. RF1 faz classificação BA e reconforma o tráfego para assegurar que a taxa máxima de envio não é ultrapassada. A reconformação é feita em relação ao agregado de todos os fluxos que chegam a RF1, e não em relação aos fluxos individuais;
13. O roteador RB1 classifica e polícia o tráfego Premium. Pacotes Premium em excesso são descartados;
14. Os roteadores entre RB1 e RB2 (inclusive) fazem classificação BA. RB2 também realiza reconformação do tráfego Premium;
15. O roteador RF2 classifica e polícia o tráfego Premium. Pacotes em excesso são descartados;

16. Os pacotes do tráfego premium são entregues à máquina Cliente2.

O processo de sinalização RSVP neste caso é diferente do processo de sinalização da arquitetura de Serviços Integrados: quem requisita os recursos é a origem e não o destino da mensagem, uma rejeição pode ser efetuada no momento em que a mensagem PATH é recebida e não somente quando a mensagem RESV é recebida, um BB pode agregar pedidos e fazer uma única requisição de reserva e, por último, os domínios comportam-se como se fossem um único nó representados pelos BBs. Os roteadores do núcleo não participam do processo de sinalização.

3.3.3 Fornecimento de serviço Premium com SLA dinâmico em ISPs baseados em MPLS

O segundo modelo proposto em [XIA 99] (ver FIGURA 3.6) integra Serviços Diferenciados, MPLS e RSVP, novamente com o intuito de negociar dinamicamente os SLAs. MPLS e Serviços Diferenciados podem ser utilizados em conjunto para fornecer QoS. Neste modelo LSPs são configurados entre cada par LSR de Ingresso – LSR de Egresso. Para evitar que um número muito grande de LSPs seja configurado, os LSPs cujo LSR de egresso seja o mesmo podem ser agregados.

A operação dos roteadores neste modelo é praticamente idêntica à do modelo anterior, com algumas exceções:

- No ingresso do domínio do ISP, além de todo processo descrito anteriormente, um *shim-header* MPLS é inserido nos pacotes;
- Os LSR de núcleo processam o pacote baseando-se em seu rótulo e no campo EXP do *shim-header* ao invés de utilizar o campo DS;
- No LSR de egresso, a não ser que exista um LSP entre domínios configurado, o *shim header* é removido.

Os domínios dos clientes ainda precisam de um BB para requisitar serviços e recursos quando se empregam SLAs dinâmicos. No entanto, como LSPs são configurados dentro do domínio do ISP, as requisições podem passar desapercebidas pelos LSRs de núcleo através de túneis entre o LSR de ingresso e o LSR de egresso. Assim um BB não precisa necessariamente ser utilizado em ISPs baseados em MPLS. O controle de admissão é realizado de maneira distribuída pelos LSRs de ingresso e egresso.

Sem os BBs no domínio dos ISPs o processo de sinalização de SLAs dinâmicos é um pouco diferente do processo descrito anteriormente. Ele pode ser visto na FIGURA 3.6 e é descrito a seguir [XIA 99]:

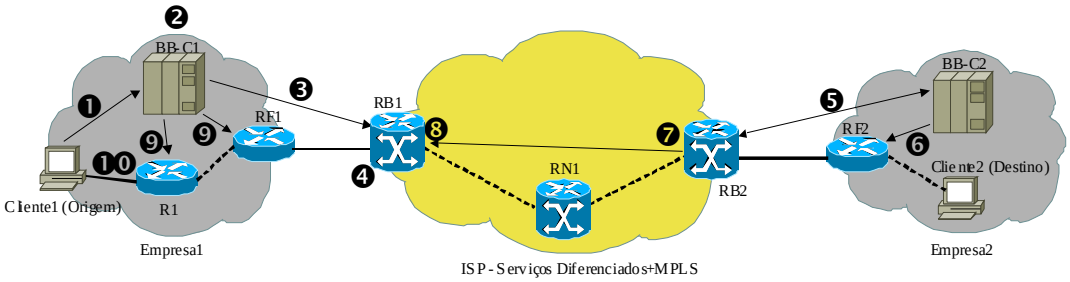

FIGURA 3.6 - Serviço Premium com SLA dinâmico em ISPs baseados em MPLS

1. A máquina Cliente1 envia uma mensagem RSVP PATH ao BB local (BB-C1) do domínio corporativo da Empresa1;
2. BB-C1 efetua o controle de admissão. Se o resultado for negativo, envia uma mensagem de erro à máquina Cliente1 e o processo é encerrado;
3. Se a solicitação for aceita por BB-C1, este envia uma mensagem RSVP PATH ao LSR de ingresso RB1;
4. RB1 verifica se existem os recursos necessários para enviar o tráfego para o LSR de egresso RB2. Se não existirem, RB1 envia uma mensagem de erro à BB-C1, caso contrário, RB1 envia a mensagem RSVP PATH para RB2 através de um LSP;
5. BR2 envia a mensagem RSVP PATH para o BB do domínio da Empresa2 (BB-C2);
6. BB-C2 decide se seu domínio pode suportar o tráfego. Se não suportar, BB-C2 retorna uma mensagem de erro à RB2. Se aceito, BB-C2 utiliza o protocolo LDAP ou RSVP para configurar as regras de classificação e policiamento no roteador RF2, e envia uma mensagem RSVP RESV à RB2;
7. RB2 configura suas regras de policiamento e reconformação para o tráfego e envia a mensagem RSVP RESV para RB1 através de um LSP;
8. RB1 configura suas regras de classificação e policiamento. Em seguida, envia a mensagem RSVP RESV à BB-C1;
9. BB-C1 ao receber a mensagem RSVP RESV configura as regras de classificação e conformação no roteador R1 e também define as regras de policiamento e reconformação no roteador RF1. Depois, manda a mensagem RSVP RESV para a máquina Cliente1;
10. A máquina Cliente1, ao receber a mensagem, fica liberada para enviar dados.

3.4 O modelo de Li et al.

Esta proposta, conhecida também pelo nome PASTE (*Provider Architecture for Differentiated Services and Traffic Engineering*) está detalhada em [LI 98]. Ela procura através da utilização conjunta de MPLS, Serviços Diferenciados e RSVP, criar uma arquitetura de tráfego escalável.

Para suportar serviços diferenciados, os pacotes são divididos em classes de tráfego separadas. A diferenciação das classes de tráfego de um pacote pode ser feita através do campo EXP do *shim-header* MPLS. Foram propostas três classes: *Best effort*, Prioridade (*Priority*) e Controle de Rede (*Network Control*) [LI 98].

A classe Controle de Rede consiste basicamente dos protocolos de roteamento e aplicações de gerenciamento da rede. A perda destes pacotes pode acarretar

instabilidades na rede. Assim, esta classe deve ter uma precedência de descarte muito baixa. Como o tráfego desta classe não é prejudicado por atrasos moderados e requer uma quantidade relativamente baixa da largura de banda, basta uma pequena garantia de largura de banda para que o tráfego de Controle de Rede opere corretamente.

O tráfego de Prioridade pode vir em diversas versões, dependendo da aplicação. Alguns fluxos podem necessitar de garantias de largura de banda, garantias de *jitter*, ou limites máximos de atraso. Assume-se que todo o tráfego de Prioridade tem uma reserva de recursos explícita.

Atualmente a grande maioria do tráfego nos ISPs é do tipo *Best effort*. Este tráfego é em grande parte insensível ao atraso e razoavelmente adaptável a congestionamentos.

Quando os fluxos são agregados de acordo com sua classe de tráfego e o fluxo agregado resultante é colocado em um LSP o resultado é um tronco de tráfego (*Traffic Trunk*). A classe de tráfego de um pacote é ortogonal ao LSP em que se encontra, assim diversos troncos de tráfego diferentes, cada um com sua classe de tráfego podem compartilhar um LSP desde que tenham classes de tráfego diferentes. Os troncos de tráfego podem ser agregados em outros troncos de forma a aumentar a escalabilidade da rede. Para aumentar a confiabilidade da rede um ou mais troncos *backup* podem ser configurados, de maneira que na eventualidade de falha no tronco primário, este possa ser substituído por um tronco *backup* [LI 98].

A utilização de RSVP no modelo PASTE é bastante diferente de sua utilização original. A primeira diferença é que RSVP agora é utilizado para configurar informações de estado referentes a uma coleção de fluxos que compartilharão recursos reservados e um caminho. A segunda diferença é que RSVP configura informações relacionadas ao encaminhamento de pacotes, incluindo informações de comutação, além das reservas de recursos. A terceira diferença é que o caminho em que são feitas as reservas não é mais restrito ao caminho selecionado pelo protocolo de roteamento.

Assim, RSVP desempenha diversas funções [LI 98]:

- Funções para configuração de encaminhamento através de uma rota explícita;
- Funções para estabelecimento de um LSP;
- Funções de reserva de recursos.

A Engenharia de Tráfego em PASTE é realizada através do direcionamento de troncos através de rotas explícitas dentro da rede. A especificação da rota é feita através de uma lista de roteadores que a comporão. Novamente, pode-se utilizar RSVP com o objeto de rota explícita (ERO – *Explicit Route Object*) [AWD 98]. O cálculo da rota pode levar em consideração políticas administrativas, alocação de largura de banda, congestionamento da topologia e outros aspectos.

Para o estabelecimento de troncos que atravessem diversos ISPs é necessária a negociação de SLAs entre os ISPs. Para colaborar neste aspecto [LI 98] propõe a utilização de mecanismos de policiamento e conformação.

3.4.1 Funcionamento do modelo PASTE

Na FIGURA 3.7 o usuário na máquina Cliente1 deseja fazer uma ligação telefônica para a máquina Cliente2 utilizando o serviço de voz sobre IP (VoIP – *Voice Over IP*). Apesar desta ligação ser *full-duplex* pode-se considerar o fluxo em cada direção como *half-duplex* pois a arquitetura opera simetricamente. Devido à natureza deste serviço, os pacotes são codificados como pertencentes à classe Prioridade.

Inicialmente esta codificação é feita nos bits de precedência do campo ToS do cabeçalho IP. Assim como no modelo apresentado anteriormente, são necessárias duas fases para o fornecimento do serviço: uma para o estabelecimento da conexão fim a fim (etapas de 1 a 6) e outra para a transmissão propriamente dita dos dados (etapas de 7 a 9) [LI 98].

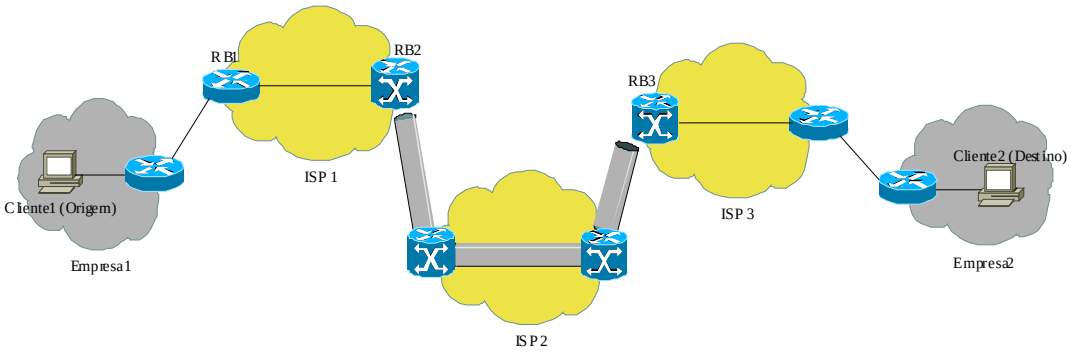

FIGURA 3.7 - Funcionamento do modelo PASTE

1. A máquina Cliente1, para estabelecer a conexão até a máquina Cliente2, envia uma mensagem RSVP PATH, a qual descreve o fluxo a ser transmitido detalhadamente;
2. Esta mensagem chega então ao ISP de Cliente1, o ISP1. ISP1 deve alocar o fluxo em um dos troncos existentes. Antes disso ele pode efetuar um controle de admissão no roteador RB1, determinando se tem capacidade suficiente para transportar o fluxo através de sua infra-estrutura até o roteador RB2;
3. Se a resposta for negativa RB1 pode informar a máquina Cliente1 através de RSVP. Caso contrário, a mensagem RSVP PATH é comutada até RB2.
4. Partindo de RB2 existe um tronco que vai até o ISP3, passando por ISP2. ISP3 é o ISP onde a máquina Cliente2 está conectada. RB2 então verifica os requisitos do fluxo presentes na mensagem RSVP e compara-os com os recursos restantes no tronco que vai para o ISP3. Assumindo que estes sejam compatíveis, o fluxo pode ser agregado ao tronco.
5. Para garantir a reserva de uma ponta à outra da conexão, a mensagem RSVP PATH é transmitida através do tronco até o ISP3 onde é recebida pelo roteador RB3.
6. A mensagem RSVP PATH é então encaminhada até a máquina Cliente2. As mensagens RSVP RESV fim a fim devem ser tratadas atenciosamente por RB3, sendo que as destinadas a RB2 devem ser encaminhadas diretamente a este através de um túnel.

RSVP também é utilizado por RB2 para estabelecer e manter o tronco para o ISP3. As mensagens RSVP de estabelecimento e manutenção não são enviadas pelo tronco, mas as mensagens RSVP fim a fim o são.

7. Os pacotes de dados enviados por Cliente1 são encaminhados através da infra-estrutura de ISP1 de acordo com a reserva de recursos feita anteriormente até chegar em RB2.
8. Neste ponto, eles recebem o *Shim header* MPLS e são transmitidos pelo tronco. A comutação MPLS vai levá-los através de ISP2. Para que a

codificação da classe de tráfego seja válida ela é copiada do cabeçalho IP para o campo EXP do *Shim header*.

9. Finalmente os pacotes chegam ao ISP3, mais exatamente à RB3 onde são removidos do tronco e encaminhados através do caminho computado por RSVP até a máquina Cliente2.

3.5 O modelo de Le Faucheur et al.

Esta proposta, detalhada em [FAU 2002a], [FAU 2001a], define uma solução flexível para suportar Serviços Diferenciados em redes que utilizam MPLS. Ela permite que o administrador da rede MPLS selecione como os fluxos agregados de Serviços Diferenciados (BA – *Behavior Aggregates*) sejam mapeados em LSPs de maneira que seja possível atingir os objetivos de diferenciação de serviços, Engenharia de Tráfego e proteção da rede.

Uma das principais características deste modelo é que ele permite que o administrador da rede decida se conjuntos diferentes de BAs serão mapeados no mesmo LSP ou em LSPs separados. Para que isso seja possível [FAU 2002a] propõe a utilização de dois tipos de LSP: E-LSPs (*EXP-Inferred-PSC LSPs*) e L-LSPs (*Label-Only-Inferred-PSC LSPs*).

Os E-LSPs são LSPs que podem ser utilizados para transportar um ou mais Agregados Ordenados (OA – *Ordered Aggregate*, conjunto de BAs que compartilham uma restrição de ordenação [GRO 2002]). Estes LSPs podem transportar até 8 BAs de uma determinada FEC. Nestes LSPs o campo EXP do *Shim Header* MPLS (por isso o nome E-LSP) é utilizado para indicar aos LSRs qual o PHB a ser aplicado a um pacote. Isto inclui tanto o PSC (*PHB Scheduling Class*, o conjunto de um ou mais PHBs que são aplicados aos BAs [GRO 2002]) como a precedência de descarte. O mapeamento do valor do campo EXP para o PHB a ser aplicado em um LSP é explicitamente sinalizado durante a distribuição dos rótulos ou então é pré-configurado. Para dois ou mais E-LSPs serem agregados eles devem obrigatoriamente suportar o mesmo conjunto de BAs.

Já os L-LSPs são LSPs que transportam somente um OA. Nestes LSPs o PSC é sinalizado explicitamente durante a distribuição dos rótulos de maneira que os LSRs podem inferir exclusivamente a partir do rótulo (por isso o nome L-LSP) qual o PSC a ser aplicado a um pacote. Quando o *Shim Header* MPLS é utilizado a precedência de descarte é codificada no campo EXP. Caso contrário, ela é codificada utilizando os mecanismos de descarte da tecnologia de enlace presente como, por exemplo, o campo CLP de ATM. Dois ou mais L-LSPs podem ser agregados somente se eles suportarem o mesmo PSC.

A TABELA 3.2 mostra as diferenças entre estes dois tipos de LSP.

TABELA 3.2 - Comparativo entre E-LSPs e L-LSPs

	E-LSP	L-LSP
Número de BAs por FEC	8	1
Significado do campo EXP	PSC e precedência de descarte	Precedência de descarte
Significado do rótulo	FEC e BAs (codificado no campo EXP)	FEC e OA (codificado no rótulo)

Para uma determinada FEC este modelo permite uma das seguintes combinações dentro de um domínio MPLS:

- 0 ou mais E-LSPs
- 0 ou mais L-LSPs

O administrador da rede seleciona a combinação de LSPs a partir do conjunto de combinações permitidas e também seleciona como os BAs serão transportados dentro desta combinação de LSPs de maneira a alcançar os objetivos de sua rede. Para uma determinada FEC pode existir mais de um LSP transportando o mesmo OA, por exemplo, para fins de balanceamento de carga do OA. Entretanto de maneira a respeitar as restrições de ordenação, todos os pacotes de um mesmo fluxo, possivelmente compreendendo múltiplos BAs de um OA devem obrigatoriamente ser transportados pelo mesmo LSP. Da mesma maneira, cada LSP deve ser capaz de suportar todos os BAs ativos de um determinado OA.

Um LSP, independentemente de ser E-LSP ou L-LSP, pode ser estabelecido com ou sem reserva de largura de banda. Quando se sinaliza os requisitos de largura de banda de um L-LSP, estes estão associados com o seu PSC. Assim, LSRs que efetuem o controle de admissão podem efetuá-lo sobre os recursos que foram provisionados para o PSC, como por exemplo, sobre a largura de banda garantida ao PSC através de seu peso configurado no escalonador. Já quando a sinalização for para o estabelecimento de um E-LSP, a largura de banda é associada coletivamente a todos os PSCs. Assim, os LSRs podem efetuar o controle de admissão sobre o conjunto global de recursos que são compartilhados por este conjunto de PSCs, como por exemplo, a largura de banda total do *link.*

3.5.1 Comutação de pacotes em LSRs que suportam Serviços Diferenciados

Como os Agregados Ordenados (OAs) de uma dada FEC podem ser transportados em diferentes LSPs a decisão com relação à comutação de um pacote nos LSRs que suportem Serviços Diferenciados depende do BA do pacote [FAU 2002a]. Além disso, como o campo DS do pacote IP pode não estar acessível ao LSR, por exemplo devido à utilização de IPSec, a maneira de determinar o PHB a ser aplicado em um pacote e a maneira de codificar o PHB em um pacote transmitido são diferentes das de um roteador que suporte somente Serviços Diferenciados.

Assim, para descrever o processo de comutação dos LSRs que suportam Serviços Diferenciados [FAU 2002a] divide-o em 4 estágios (ver a FIGURA 3.8):

- Determinação do PHB de entrada;
- Determinação do PHB de saída, opcionalmente com Conformação do Tráfego;
- Inserção/troca do rótulo;
- Codificação das informações de Serviço Diferenciados no protocolo de enlace (Campo EXP, CLP e etc.).

Para cumprir a diferenciação dos serviços o LSR também deve aplicar o PHB correspondente ao PHB de saída selecionado.

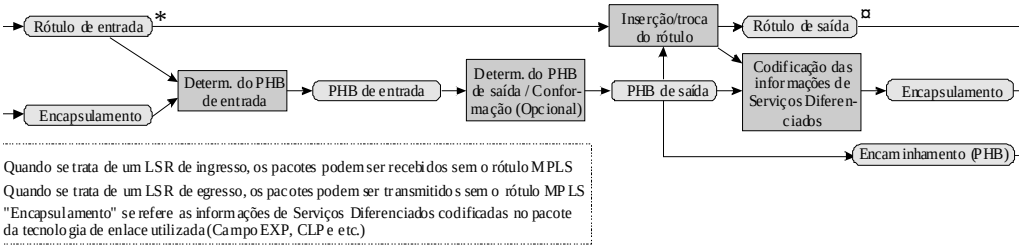

FIGURA 3.8 - Modelo de comutação

A primeira fase, Determinação do PHB de entrada, procura determinar a qual BA o pacote recebido pertence. Este processo pode tanto considerar uma pilha de rótulos, para o caso de estar sendo utilizado um túnel, somente o rótulo, as informações encapsuladas no protocolo de enlace, o tipo de LSP, ou ainda o cabeçalho IP do pacote.

A segunda fase, Determinação do PHB de saída, é opcional e pode ser utilizada em um LSR para executar a conformação do tráfego. É importante notar que o PHB escolhido nesta fase, que será aplicado ao pacote e transmitido para o LSR à jusante, pode ser diferente do PHB que foi associado a este pacote pelo LSR à montante (o PHB de entrada). Quando o estágio de conformação não está presente o PHB de saída é igual ao PHB de entrada.

A terceira fase, Inserção/troca do rótulo, é definida em [ROS 2001a]. A troca dos rótulos é efetuada pelos LSRs nos pacotes que são recebidos utilizando-se um Mapeamento de rótulo de entrada (ILM – *Incoming Label Map*), onde cada rótulo é mapeado em uma ou mais Entrada de próximo nó via comutação de rótulo (NHLFE - *Next Hop Label Forwarding Entry*). [ROS 2001a] também define como um rótulo é escolhido por um LSR para um pacote recebido sem o rótulo utilizando-se um Mapeamento de FEC em NHLFE (FTN – *FEC to NHLFE Map*) onde cada FEC é mapeada em um ou mais NHLFEs.

O contexto de Serviços Diferenciados em um rótulo é composto por:

- Tipo do LSP (E-LSP ou L-LSP);
- PHBs suportados;
- Mapeamento do “Encapsulamento” em PHB para um rótulo de entrada;
- Conjunto de mapeamentos de PHB em “Encapsulamento” para um rótulo de saída.

[FAU 2002a] define que o contexto de Serviços Diferenciados é armazenado no ILM para cada rótulo de entrada e na NHLFE para cada rótulo de saída (troca ou remoção). Estas informações são inseridas no ILM e no FTN durante o processo de sinalização de rótulos. Se durante o mapeamento através do ILM, ou do FTN, mais de uma NHLFE for válida, deve-se escolher somente uma delas.

Por fim, a quarta fase efetua a codificação das informações de Serviços Diferenciados no pacote do nível de enlace utilizando campos como EXP de MPLS e CLP de ATM.

3.5.2 Extensões para os protocolos de sinalização

Para que seja possível estabelecer LSPs com suporte a Serviços Diferenciados nas redes MPLS são necessárias modificações em diversos protocolos existentes. [FAU

2001a] propõe as mudanças necessárias em CR-LDP e RSVP-TE para que estes suportem Engenharia de Tráfego levando em consideração Serviços Diferenciados.

No caso de RSVP-TE, um novo objeto é definido em [FAU 2001a]: o objeto DIFFSERV para o estabelecimento de E-LSPs e L-LSPs. Este objeto pode ser utilizado em mensagens PATH e é opcional com relação ao protocolo RSVP, de maneira que implementações deste que não suportem o estabelecimento de LSPs não precisem tratar este objeto. As restrições definidas em [AWD 2001a] para o estabelecimento de LSPs túnel através de RSVP também se aplicam ao estabelecimento de LSPs túnel com suporte a Serviços Diferenciados. Tanto E-LSPs como L-LSPs podem ser estabelecidos com um sem reserva de largura de banda. No primeiro caso, é utilizado o Serviço de Carga Controlada, ou o Serviço Garantido, e a largura de banda é sinalizada no SENDER_TSPEC da mensagem PATH ou no FLOWSPEC da mensagem RESV. Se não for haver reserva durante o estabelecimento, especifica-se o serviço Nulo [BER 2000b]. É importante notar que apesar da sinalização conter um serviço pertencente à arquitetura de Serviços Integrados, como Carga Controlada, Garantido ou Nulo, e apesar de haver ou não reservas para o estabelecimento de um LSP, toda esta especificação é definida para criar LSPs com capacidade de suportar Serviços Diferenciados.

Para que o protocolo LDP possa estabelecer LSPs com suporte a Serviços Diferenciados [FAU 2001a] propõe o TLV DIFFSERV a ser utilizado nas mensagens LABEL REQUEST e LABEL MAPPING. Este TLV é opcional com relação ao protocolo LDP. Assim como quando se utiliza RSVP-TE também é possível sinalizar informações de largura de banda durante o estabelecimento de um E-LSP ou L-LSP. Para este fim utiliza-se o TRAFFIC PARAMETERS TLV de CR-LDP como definido em [JAM 2002].

Além das extensões a RSVP-TE e LDP também são propostas alterações [FAU 2001b] e [FAU 2001c] para, respectivamente, os protocolos OSPF [MOY 98] e ISIS [ORA 90] para que estes suportem Engenharia de Tráfego levando em consideração Serviços Diferenciados.

3.5.3 Exemplos de implantação de Serviços Diferenciados sobre MPLS

Para exemplificar a utilização do modelo proposto por [FAU 2002a] serão apresentados dois cenários de implantação do mesmo.

Cenário 1: um provedor de serviços cuja rede transporta mais de 8 BAs e que não implementa nem Engenharia de Tráfego e nem proteção, decide implantar Serviços Diferenciados sobre MPLS utilizando para cada FEC um E-LSP estabelecido através de LDP e contando com mapeamentos pré-configurados para suportar 8 ou menos BAs, e um L-LSP para cada par FEC-OA estabelecido através de LDP para transportar os BAs restantes da FEC. O processo de implantação pode ser resumido a seguir [FAU 2002a]:

- O ISP configura em cada LSR o mapeamento bi-direcional entre cada PHB e o valor do campo EXP para os BAs transportados através do E-LSP;
- O ISP configura em cada LSR, e para cada interface deste, o comportamento do escalonador para cada PSC suportado no E-LSP e também o comportamento de descarte para cada PHB correspondente;
- O ISP configura em cada LSR, e para cada interface deste, o comportamento do escalonador para cada PSC suportado nos L-LSPs e também o comportamento de descarte para cada PHB correspondente;

- Os LSRs sinalizam o estabelecimento de um E-LSP por FEC, para os BAs que serão transportados neste, através de LDP;
- Os LSRs sinalizam o estabelecimento de um L-LSP para cada par FEC-OA para os BAs restantes da FEC através de LDP;

Cenário 2: um provedor de serviços cuja rede transporta uma quantidade qualquer de BAs através de MPLS, efetuando Engenharia de Tráfego para cada OA, ou seja, para cada um deles é executado um processo independente de seleção de rota, e também efetuando proteção por OA, isto é, para diferentes OAs podem haver níveis diferentes de proteção, pode decidir implantar Serviços Diferenciados sobre MPLS utilizando um L-LSP para cada par FEC-OA estabelecido através de RSVP-TE ou CR-LDP. O processo de implantação pode ser resumido a seguir [FAU 2002a]:

- O ISP configura em cada LSR, e para cada interface deste, o comportamento do escalonador para cada PSC, isto é, a largura de banda para AF1, por exemplo, e o comportamento de descarte para cada PHB, ou seja, os perfis de descarte para AF11, AF12 e AF13;
- Os LSRs sinalizam o estabelecimento de um L-LSP para cada par FEC-OA, através de RSVP-TE ou CR-LDP;
- O nível de proteção adequado é ativado nos diferentes L-LSPs.

3.6 Comparação dos modelos de integração apresentados

Os diversos modelos de integração apresentados têm características bastante distintas uns dos outros. Cada um suporta um conjunto diferente de arquiteturas para fornecimento de QoS e conta com diferentes protocolos de sinalização. Uma síntese dessas características pode ser encontrada na TABELA 3.3.

TABELA 3.3 - Comparação dos modelos de integração

	Bernet et al.	Rajan et al.	Xiao et al.	Li et al.	Le Faucheur et al.
Suporte a Serviços Integrados	Sim	Sim	Não	Não	Não
Suporte a Serviços Diferenciados	Sim	Sim	Sim	Sim	Sim
Suporte a MPLS	Não	Não	Sim	Sim	Sim
Suporte a Engenharia de Tráfego	Não	Não	Sim	Não	Sim
Suporte a Roteamento Baseado em Restrições	Não	Não	Sim	Não	Sim
Suporte a SLAs dinâmicos	Sim	Sim	Sim	Sim	Sim
Protocolo de sinalização	RSVP	RSVP	RSVP	RSVP	RSVP/LDP

O modelo proposto neste trabalho procura suportar todos estes critérios, de forma flexível e escalável, sem sacrificar a performance geral da rede. Este modelo será apresentado no próximo capítulo.

4 Modelo Proposto

O modelo proposto neste trabalho indica mecanismos simples para que um domínio MPLS forneça garantias de serviço fim a fim para as redes clientes vizinhas, que podem estar utilizando as arquiteturas de Serviços Integrados, Serviços Diferenciados, MPLS, ou mesmo nenhuma arquitetura para fornecimento de QoS. O modelo proposto é, na verdade, uma extensão ao modelo de Le Faucheur [FAU 2002a], adicionando a este a possibilidade de suportar Serviços Integrados sobre uma rede que conta com MPLS e Serviços Diferenciados.

Este modelo está sendo proposto pois se acredita que os ISPs adotarão, em um futuro próximo, a arquitetura MPLS em razão das vantagens relacionadas à Engenharia de Tráfego. E que, ligados aos ISPs, estarão redes de clientes com arquiteturas diferentes para fornecimento de QoS.

Como MPLS é uma tecnologia destinada ao núcleo das redes existentes, uma das suas principais características é a escalabilidade, que é atingida com a agregação de fluxos com garantias de serviço fim a fim, sem a necessidade de controle individual dos fluxos em cada segmento de seu caminho. Assim, os mecanismos de Serviços Diferenciados tornam-se muito interessantes para fornecer QoS dentro de domínios MPLS pois seus serviços são baseados em um modelo *per-hop* e em recursos, como espaço em *buffer* e largura de banda, que são pré-alocados nos LSRs para cada serviço. Funções como classificação, marcação e policiamento são utilizadas somente nas bordas da rede enquanto os LSRs do núcleo precisam somente de classificadores, mantendo sua simplicidade e escalabilidade.

A FIGURA 4.1 mostra um exemplo de rede que utiliza o modelo proposto: no núcleo da rede existem somente LSRs MPLS, que também farão o papel de roteadores de núcleo de Serviços Diferenciados como em [FAU 2002a]. Nas bordas da rede estão os LSRs que também se comportarão como roteadores de borda de Serviços Diferenciados, e que, além disto, efetuarão o mapeamento dos serviços das redes clientes em serviços do modelo proposto. Ligadas aos LSRs de borda se encontram diversas redes clientes.

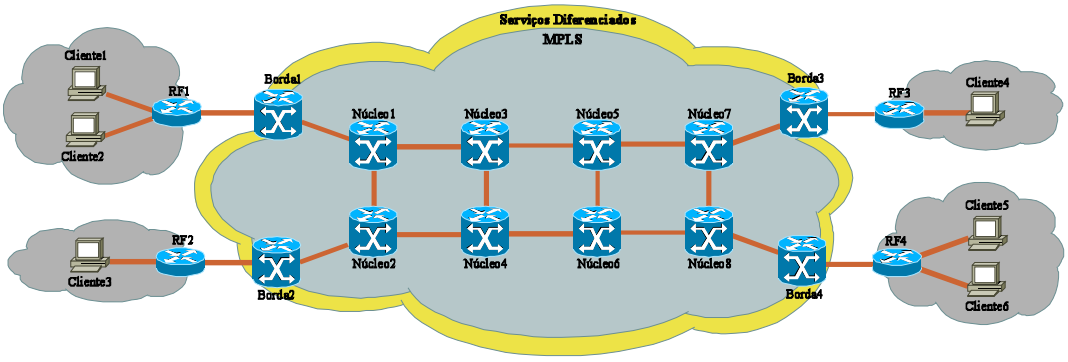

FIGURA 4.1 - Exemplo do modelo proposto

As seguintes razões, além das vantagens inerentes da utilização de MPLS e Serviços Diferenciados, levaram à escolha do modelo de Le Faucheur para o núcleo da rede [FAU 2002a]:

- Flexibilidade no mapeamento de BAs para LSPs;
- Suporte aos PHBs atuais e futuros;
- Flexibilidade para os ISPs selecionarem como as classes de serviço são roteadas dentro de seu domínio;
- A utilização de MPLS oferece maior capacidade de proteção e restauração quando ocorrem alterações na topologia;
- Flexibilidade na escolha dos níveis de proteção e restauração;
- Conservação da quantidade disponível de rótulos;
- Quando possível, otimiza a quantidade de mensagens de estabelecimento e encerramento de LSPs;
- Suporte a IPv4 e IPv6.

O modelo de Le Faucheur não oferece suporte a Serviços Integrados [FAU 2002a]. Como o objetivo principal do modelo proposto é a interoperação das principais arquiteturas para fornecimento de QoS existentes, é necessário um mecanismo de mapeamento de Serviços Integrados para o modelo proposto por Le Faucheur. Para efetuar este mapeamento, serão utilizados mecanismos como os propostos por Bernet [BER 2000a] para a operação com gerenciamento dinâmico, utilizando RSVP para sinalização. As principais vantagens deste modo de operação são:

- Permite a negociação de SLAs dinâmicos;
- Alterações da capacidade disponível no núcleo da rede podem ser sinalizadas para as redes clientes através de RSVP;
- É possível alterar o provisionamento do núcleo da rede para um determinado serviço através de RSVP e dos mecanismos apresentados em [ASH 2002b].

A utilização de todos estes mecanismos em conjunto leva a um modelo extremamente flexível, e ainda assim escalável, que pode ser utilizada pelos provedores de serviço para atender uma diversa gama de clientes.

4.1 Serviços suportados

Para suportar a diferenciação de serviços o modelo proposto indica as seguintes classes de tráfego, baseadas em [HEI 99]:

- Classe ouro: serviço com baixo atraso, baixo *jitter* e poucas perdas, para fluxos sensíveis ao atraso. Nesta classe, pacotes que excedam a taxa máxima de envio configurada no SLA são descartados;
- Classes prata e bronze: serviços destinados para fluxos sensíveis ao *throughput*. Pacotes pertencentes à classe prata têm maior prioridade do que os pacotes da classe bronze. Dentro de cada classe existem ainda dois níveis de precedência de descarte. Nestas classes, pacotes que excedam a taxa máxima de envio configurada no SLA podem ser descartados ou marcados com uma precedência de descarte mais alta;
- Classe *best effort*: serviço sem garantia nenhuma da rede.

TABELA 4.1 - Mapeamento de serviços

Serviços Integrados	Serviços Diferenciados	Modelo proposto	Campo EXP
Garantido (GS)	*Expedited Forwarding* (EF)	Classe ouro	111
Carga controlada (CL)	*Assured Forwarding* (AF)		
	AFx1	Classe prata	110/011*
	AFx2	Classe bronze	101/010*
	AFx3		100/001*
Best effort	*Best effort*	*Best effort*	000

* Dois valores, um para cada nível de precedência

O mapeamento proposto na TABELA 4.1 é feito pelos LSRs de ingresso, baseando-se no SLA em vigor com o domínio cliente. Podemos ainda considerar dois casos distintos: no primeiro os pacotes do domínio cliente já vêm com um tipo de serviço (tanto Serviços Integrados como Serviços Diferenciados) definido, e basta ao LSR de ingresso fazer o mapeamento. No segundo, os pacotes vêm sem nenhuma indicação de tipo de serviço. Neste caso, o LSR de ingresso deverá fazer uma classificação multi-campo (MF) para então atribuir o pacote a uma das classes.

Os pacotes que trafegam pelo núcleo da rede contendo mensagens de controle, como mensagens de roteamento ou mensagens LDP/CR-LDP, são tratados como pertencentes à classe Ouro, pois deles depende o funcionamento correto da rede do ISP. Como a quantidade de pacotes deste tipo não é muito grande, não há prejuízo para os fluxos que utilizam a classe Ouro.

4.1.1 Escalonamento e conformação

Os ISPs podem adotar diversos tipos de políticas de escalonamento e descarte de pacotes. Um exemplo é mostrado na FIGURA 4.2, e consiste em 4 filas, uma para cada classe, com um escalonador baseado em prioridade (PQ) servindo as filas. A fila Ouro é a de maior prioridade e a fila *Best effort* é a de menor prioridade.

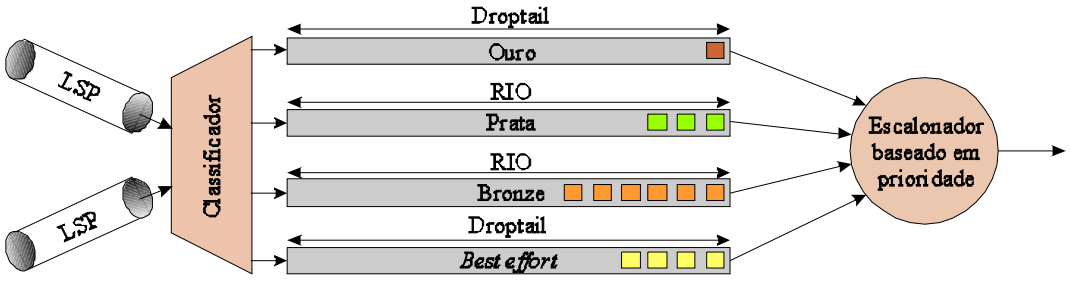

FIGURA 4.2 - Escalonamento no núcleo da rede MPLS

Nos LSRs de ingresso a conformação é efetuada por conformadores do tipo *Token Bucket*. Os conformadores são configurados através de uma CIR (*Commited Information Rate*) e uma CBS (*Commited Burst Size*). Para as classes Ouro e *Best effort* a CBS é igual a 0, pois não é permitido excesso algum de tráfego.

As simulações apresentadas no próximo capítulo utilizam este modelo de escalonamento e conformação.

4.2 Sinalização e mapeamento de serviços

Um cliente que deseje utilizar os serviços do domínio MPLS precisa, antes de tudo, estabelecer um SLA com este. O SLA pode ser estático ou dinâmico. No caso do estabelecimento de SLAs dinâmicos é necessária a utilização de algum protocolo de sinalização como RSVP. Para minimizar o tempo de estabelecimento dos LSPs a gerência da rede do ISP pode alocar estaticamente os recursos e configurar os LSPs baseando-se nas necessidades do cliente.

Para a sinalização entre as redes periféricas e o domínio MPLS pode ser utilizado RSVP, permitindo que sejam estabelecidos relacionamentos PHB→FEC, e talvez o estabelecimento de um novo LSP, dinamicamente (SLAs dinâmicos). Dentro do núcleo MPLS o protocolo de sinalização é o LDP [AND 2001], e sua extensão para roteamento baseado em restrições, o CR-LDP [JAM 2002]. Por ser baseado em TCP/IP e ser um protocolo *hard-state* acredita-se que LDP/CR-LDP será mais escalável e confiável do que RSVP-TE [SER 2001A]. O controle de admissão será efetuado pelos LSRs de ingresso, baseando-se nas informações providas pelo próprio núcleo MPLS.

O mapeamento dos serviços das redes cliente, visto na TABELA 4.1, será efetuado nos LSRs de ingresso, em conjunto com as suas funções normais, como classificação, conformação e etc.

Os valores do campo EXP presentes na TABELA 4.1 indicam além da classe de serviço a precedência de descarte: baixa, para pacotes dentro do perfil configurado (primeiro valor) e alta, para pacotes fora do perfil configurado (segundo valor)

No caso de a rede ligada ao ISP não contar com nenhum mecanismo de QoS, a classificação, marcação, policiamento e conformação, além do mapeamento, serão efetuados pelos LSRs de ingresso do ISP de acordo com o SLA estabelecido com o cliente.

4.3 Funcionamento

Assim como na arquitetura de Serviços Diferenciados, os LSRs do núcleo e da borda apresentam funções e responsabilidades diferentes. Tanto os LSRs de borda como os LSR de núcleo incluem as seguintes funções:

- Roteamento baseado em restrições;
- Estabelecimento de CR-LSPs;
- Controle de admissão;
- Mecanismos de escalonamento.

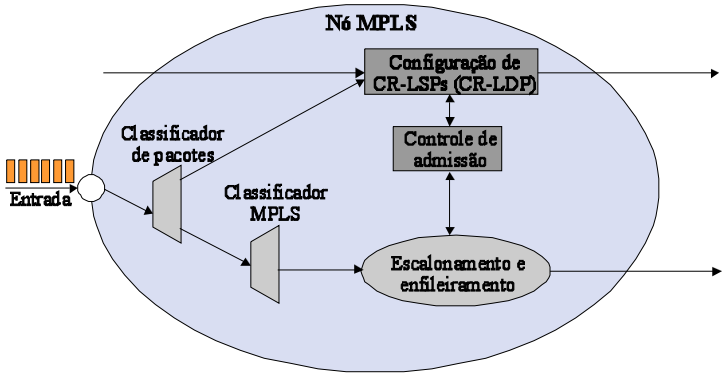

FIGURA 4.3 - Estrutura interna de um nó MPLS de núcleo

Além disso, os LSRs de ingresso são responsáveis por:

- Classificação;
- Policiamento;
- Conformação;
- Controle de admissão;
- Mapeamento de serviços das redes vizinhas em serviços do modelo proposto.

A estrutura interna dos LSRs de núcleo e dos LSRs de borda pode ser vista, respectivamente, na FIGURA 4.3 e na FIGURA 4.4.

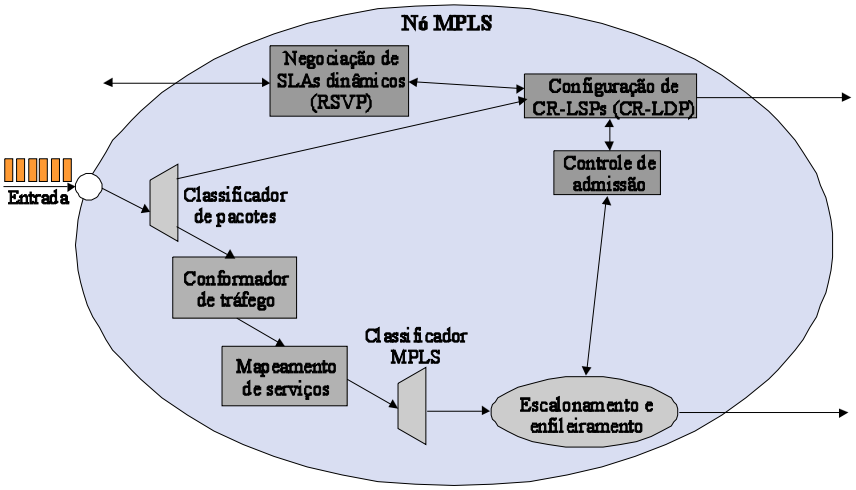

FIGURA 4.4 - Estrutura interna de um nó MPLS de borda

No núcleo MPLS existirão dois tipos de LSP: no primeiro, o E-LSP, será possível que a banda configurada seja compartilhada por diversos agregados (BA - *Behavior Aggregates*) cujas necessidades de QoS sejam parecidas. Para diferenciar cada um dos agregados, será utilizado o campo EXP, do *Shim Header*, que conterá o DSCP e a precedência de descarte. Quando o núcleo da rede for baseado em uma tecnologia de enlace que dispense a utilização do *Shim Header*, outros mapeamentos, utilizando características da tecnologia de enlace, são utilizados. Este tipo de LSP permitirá uma

maior agregação de fluxos, resultando em um número menor de LSPs configurados, e conseqüentemente, facilitando a Engenharia de Tráfego.

O segundo tipo de LSP, o L-LSP, transporta apenas um agregado, cujas necessidades de QoS sejam rígidas, neste caso infere-se seu DSCP através do rótulo dos pacotes. Separando-o em um LSP exclusivo, aumentamos seu isolamento, e podemos garantir um QoS bastante estrito. A divisão dos LSPs em dois tipos também facilita a Engenharia de Tráfego, pois permite ao administrador da rede saber exatamente que tipo de agregado está passando por que trecho da rede em um determinado momento.

O roteamento dos pacotes dentro do domínio MPLS será feito baseando-se no rótulo MPLS do pacote e o tratamento, ou PSC (*PHB Scheduling Class*), aplicado por cada LSR aos pacotes será baseado no DSCP e na precedência de descarte, ambos codificados no campo EXP (E-LSPs) ou no rótulo (L-LSPs) de cada pacote.

Assim, chegamos a uma arquitetura de QoS fim-a-fim completa, pois estão previstos:

- Mecanismos de tratamento de tráfego: baseado no DSCP, na precedência de descarte e no rótulo MPLS;
- Mecanismos de configuração: RSVP externamente (SLAs dinâmicos) e LDP/CR-LDP internamente;
- Provisionamento: controle de admissão nos roteadores de borda e PSCs nos LSRs.

Para ilustrar o funcionamento do modelo proposto serão apresentados os processos completos para obtenção de QoS de duas situações comuns: a obtenção de serviço da classe prata utilizando SLA estático e a obtenção de serviço da classe ouro utilizando SLA dinâmico.

4.3.1 Alocação de serviços nas redes clientes

Para a alocação dos serviços dentro das redes dos clientes existem duas alternativas, baseadas em [XIA 99]:

- Cada máquina decide sozinha quais serviços irá utilizar;
- Um negociador de banda (BB – *Bandwidth Broker*) decide quais serviços cada máquina poderá utilizar.

Assim, antes de uma máquina iniciar a transmissão ela pode decidir sozinha qual serviço utilizar ou então pode consultar o BB. As máquinas também podem, ou não, contar com algum mecanismo de marcação dos pacotes. Desta maneira, a própria máquina pode marcar os pacotes, ou então enviar os pacotes sem nenhuma marcação e deixar este serviço para os roteadores de fronteira. Neste último caso os roteadores terão que ser configurados, de forma manual ou automática. Se existir a negociação de SLAs dinâmicos entre os clientes e os ISPs, as máquinas, ou o BB, da rede cliente deverão utilizar um protocolo para a requisição sob demanda de recursos do ISP. Assume-se que será utilizado para este fim o protocolo RSVP.

4.3.2 Alocação de serviços na rede do ISP

Para a alocação de recursos dentro das redes dos ISPs, deve-se examinar os SLAs e a partir deles decidir como serão configurados os roteadores de borda, de maneira que estes saibam como tratar o tráfego entrante [XIA 99]. Para os SLAs estáticos os roteadores podem ser configurados manualmente, desta maneira os recursos são alocados estaticamente para cada cliente. Para SLAs dinâmicos a alocação de recursos depende do método de sinalização. No caso das máquinas, ou do BB, da rede cliente utilizar RSVP para requisição de recursos do ISP, o controle de admissão pode ser feito de maneira distribuída pelos LSRs de borda. Se a requisição for aceita os LSRs de borda são configurados com as regras correspondentes de classificação, policiamento e conformação. Os roteadores do núcleo do ISP não participam da sinalização para evitar problemas de escalabilidade.

4.3.3 Fornecimento de serviço da classe prata utilizando SLA estático

Na FIGURA 4.5, a máquina Cliente1 da rede corporativa da Empresa1 deseja enviar dados utilizando o serviço Prata para a máquina Cliente6 da rede corporativa da Empresa2. A Empresa1 possui um SLA estático com o ISP. A marcação dos pacotes da rede da Empresa1 será efetuada pelo seu roteador de saída, RF1, que foi previamente configurado. O processo de fornecimento segue as etapas indicadas pelos números na FIGURA 4.5 e descritos a seguir:

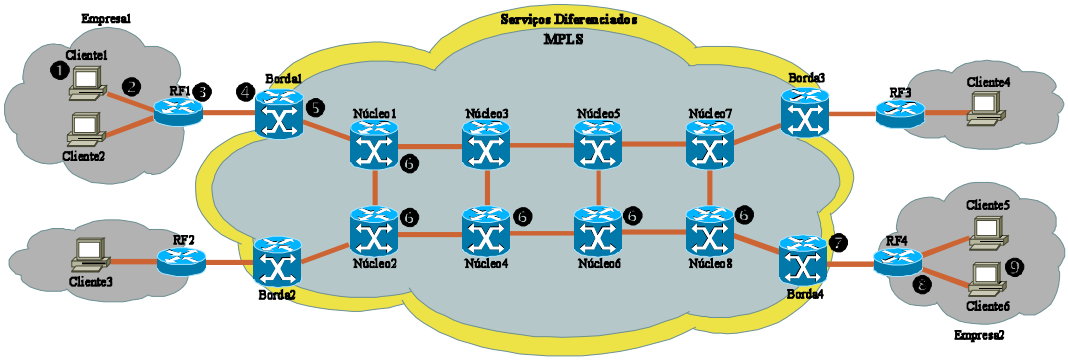

FIGURA 4.5 - Seqüência para obtenção de serviço da classe prata utilizando SLA estático sem a utilização de um BB

1. A máquina Cliente1 inicia a transmissão dos pacotes;
2. Todos os outros possíveis roteadores no caminho até RF1 (inclusive) fazem uma classificação BA (*behavior aggregate*). Pacotes da classe Prata serão considerados dentro do perfil (*in-profile*) enquanto os outros pacotes serão considerados fora do perfil (*out-profile*). Todos os pacotes entram em uma fila da classe Prata na qual é utilizado o algoritmo RIO;
3. O roteador RF1 marca os pacotes do fluxo como pacotes da classe Prata;
4. O LSR Borda1 na entrada da rede do ISP policia o tráfego. Os pacotes fora do perfil continuam fora do perfil, e os pacotes dentro do perfil que excedam a

taxa de envio configurada no SLA são classificados com o nível de precedência de descarte mais alto possível para pacotes Prata. Todos os pacotes entram em uma fila da classe Prata na qual é utilizado o algoritmo RIO;

5. O LSR Borda1 efetua o mapeamento dos pacotes da classe Prata em uma FEC, insere o *Shim header*, e os repassa para o núcleo da rede;
6. Todos os LSRs entre Borda1 e Borda4 (inclusive) executam classificação baseando-se no PSC do pacote e utilizam RIO em suas filas da classe Prata;
7. O LSR de borda Borda4 retira o *Shim header* do pacote e o repassa a RF4;
8. O roteador RF4 executa as mesmas operações de policiamento e conformação do LSR Borda1 do ISP;
9. Os pacotes são entregues à máquina Cliente2.

Nota: o passo 8 é opcional e depende de a gerência de rede da Empresa2 desejar efetuar o controle do tráfego entrante na sua rede.

Para o caso de se utilizar um BB na rede da Empresa1 o processo de fornecimento segue as etapas indicadas pelos números na FIGURA 4.6 e descritos a seguir:

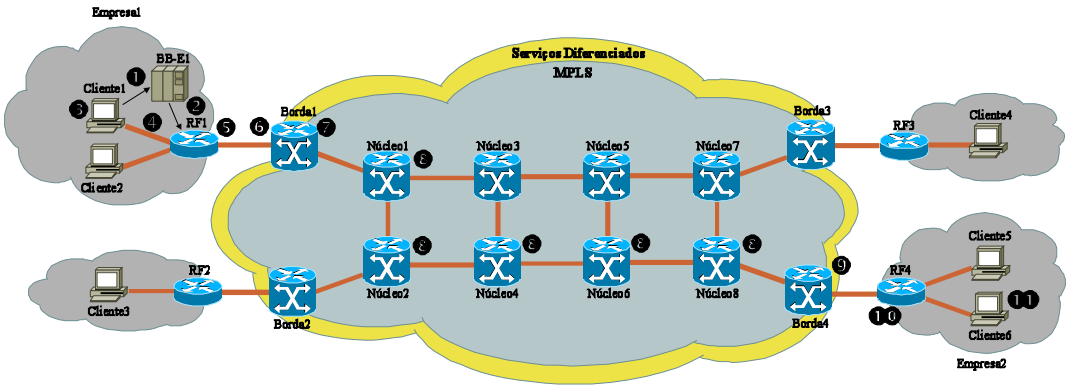

FIGURA 4.6 - Seqüência para obtenção de serviço da classe prata utilizando SLA estático com a utilização de um BB

1. A máquina Cliente1 envia uma mensagem RSVP para o BB local (BB-E1) requisitando o serviço Prata;
2. Se o BB aceita o pedido, então o roteador RF1 será configurado para marcar os pacotes do fluxo como pacotes Prata e confirma o serviço para a máquina Cliente1, caso contrário Cliente1 receberá uma mensagem de erro;
3. A máquina Cliente1 inicia a transmissão dos pacotes;
4. Todos os outros possíveis roteadores no caminho até RF1 (inclusive) fazem uma classificação BA (*behavior aggregate*). Pacotes da classe Prata serão considerados dentro do perfil (*in-profile*) enquanto os outros pacotes serão considerados fora do perfil (*out-profile*). Todos os pacotes entram em uma fila da classe Prata na qual é utilizado o algoritmo RIO;
5. O roteador RF1 marca os pacotes do fluxo como pacotes da classe Prata;
6. O LSR Borda1 na entrada da rede do ISP policia o tráfego. Os pacotes fora do perfil continuam fora do perfil, e os pacotes dentro do perfil que excedam a taxa de envio configurada no SLA são classificados com o nível de precedência de descarte mais alto possível para pacotes Prata. Todos os

pacotes entram em uma fila da classe Prata na qual é utilizado o algoritmo RIO;
7. O LSR Borda1 efetua o mapeamento dos pacotes da classe Prata em uma FEC, insere o *Shim header*, e os repassa para o núcleo da rede;
8. Todos os LSRs entre Borda1 e Borda4 (inclusive) executam classificação baseando-se no PSC do pacote e utilizam RIO em suas filas da classe Prata;
9. O LSR de borda Borda4 retira o *Shim header* do pacote e o repassa a RF4;
10. O roteador RF4 executa as mesmas operações de policiamento e conformação do LSR Borda1 do ISP;
11. Os pacotes são entregues à máquina Cliente2.

Nota: o passo 10 é opcional e depende de a gerência de rede da Empresa2 desejar efetuar o controle do tráfego entrante na sua rede.

4.3.4 Fornecimento de serviço da classe ouro utilizando SLA dinâmico

Na FIGURA 4.7, a máquina Cliente1 da rede corporativa da Empresa1 deseja enviar dados utilizando o serviço Ouro para a máquina Cliente6 da rede corporativa da Empresa2. A Empresa1 possui um SLA dinâmico com o ISP. O processo de fornecimento segue as etapas indicadas pelos números na FIGURA 4.7 e descritos a seguir:

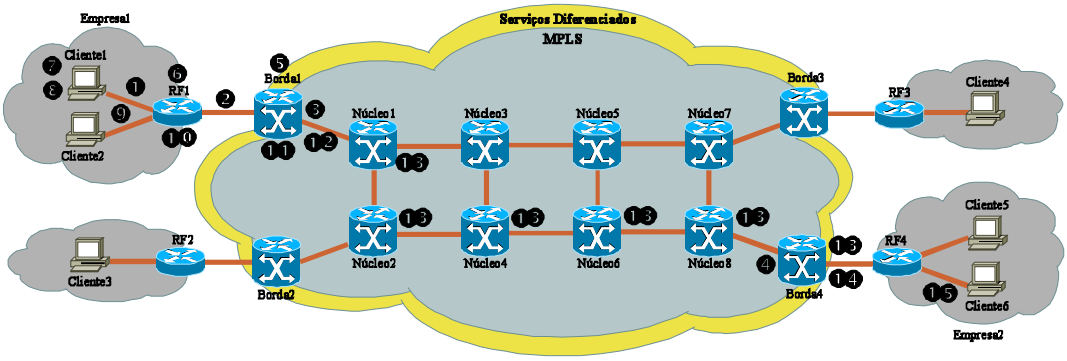

FIGURA 4.7 - Seqüência para obtenção de serviço da classe ouro utilizando SLA dinâmico sem a utilização de um BB

1. A máquina Cliente1 envia uma mensagem RSVP PATH ao roteador de fronteira da Empresa1, RF1;
2. RF1 repassa a mensagem RSVP PATH ao LSR de ingresso do ISP, Borda1;
3. Borda1 envia uma mensagem CR-LDP LABEL REQUEST para Borda4;
4. Se existem os recursos necessários para enviar o tráfego para o LSR de egresso Borda4, este retorna uma mensagem CR-LDP LABEL MAPPING para Borda1. Se não existirem, Borda4 envia uma mensagem de erro à Borda1;
5. Borda1 configura suas regras de classificação e policiamento. Em seguida, envia a mensagem RSVP RESV à RF1;

6. RF1 ao receber a mensagem RSVP RESV configura suas regras de classificação e conformação. Depois, manda a mensagem RSVP RESV para a máquina Cliente1;
7. A máquina Cliente1, ao receber a mensagem, fica liberada para enviar dados;
8. Cliente1 manda pacotes ao roteador RF1;
9. Todos roteadores entre Cliente1 e RF1 fazem classificação BA e encaminham os pacotes através da fila da classe Ouro;
10. RF1 faz classificação BA e conforma o tráfego para assegurar que a taxa máxima de envio não é ultrapassada. A conformação é feita em relação ao agregado de todos os fluxos que chegam a RF1, e não em relação aos fluxos individuais;
11. O LSR Borda1 classifica e polícia o tráfego Ouro. Pacotes Ouro em excesso são descartados;
12. RF1 efetua o mapeamento do tráfego classe Ouro em uma FEC, insere o *Shim-header* e o repassa para o núcleo da rede;
13. Os LSRs entre Borda1 e Borda4 (inclusive) fazem classificação BA e utilizam a fila da classe Ouro;
14. O LSR de egresso retira o *Shim-header* dos pacotes e os repassa ao roteador RF4;
15. Os pacotes do tráfego Ouro são entregues à máquina Cliente2.

Para o caso de se utilizar um BB na rede da Empresa1 o processo de fornecimento segue as etapas indicadas pelos números na FIGURA 4.8 e descritos a seguir:

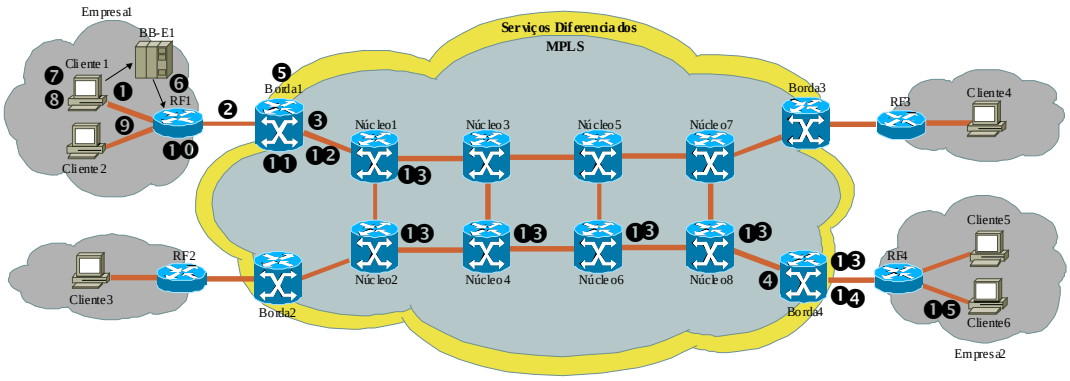

FIGURA 4.8 - Seqüência para obtenção de serviço da classe ouro utilizando SLA dinâmico com a utilização de um BB

1. A máquina Cliente1 envia uma mensagem RSVP PATH ao BB local (BB-E1) do domínio corporativo da Empresa1;
2. BB-E1 efetua o controle de admissão. Se o resultado for negativo, envia uma mensagem de erro à máquina Cliente1 e o processo é encerrado. Se a solicitação for aceita por BB-E1, este envia uma mensagem RSVP PATH ao LSR de ingresso Borda1;
3. Borda1 envia uma mensagem CR-LDP LABEL REQUEST para Borda4;
4. Se existem os recursos necessários para enviar o tráfego para o LSR de egresso Borda4, este retorna uma mensagem CR-LDP LABEL MAPPING para Borda1. Se não existirem, Borda4 envia uma mensagem de erro à Borda1;

5. Borda1 configura suas regras de classificação e policiamento. Em seguida, envia a mensagem RSVP RESV à BB-E1;
6. BB-E1 ao receber a mensagem RSVP RESV configura as regras de classificação e conformação de RF1. Depois, manda a mensagem RSVP RESV para a máquina Cliente1;
7. A máquina Cliente1, ao receber a mensagem, fica liberada para enviar dados;
8. Cliente1 manda pacotes ao roteador RF1;
9. Todos roteadores entre Cliente1 e RF1 fazem classificação BA e encaminham os pacotes através da fila da classe Ouro;
10. RF1 faz classificação BA e conforma o tráfego para assegurar que a taxa máxima de envio não é ultrapassada. A conformação é feita em relação ao agregado de todos os fluxos que chegam a RF1, e não em relação aos fluxos individuais;
11. O LSR Borda1 classifica e polícia o tráfego Ouro. Pacotes Ouro em excesso são descartados;
12. RF1 efetua o mapeamento do tráfego classe Ouro em uma FEC, insere o *Shim-header* e o repassa para o núcleo da rede;
13. Os LSRs entre Borda1 e Borda4 (inclusive) fazem classificação BA e utilizam a fila da classe Ouro;
14. O LSR de egresso retira o *Shim-header* dos pacotes e os repassa à ao roteador RF4;
15. Os pacotes do tráfego Ouro são entregues à máquina Cliente2.

5 Simulações e Resultados

Para efetuar a validação do modelo proposto com outros modelos já existentes foi utilizado o simulador de redes de computadores ns2 (*Network Simulator 2*) [NS2 2002]. ns2 é um simulador orientado a eventos, desenvolvido pela Universidade da Califórnia. Sua capacidade de extensão torna-o bastante dinâmico, com versões modificadas sendo disponibilizadas quase que diariamente. Seu *engine* de simulação é escrito em C++, e os usuários utilizam oTcl, uma versão orientada a objetos de Tcl, como interface de configuração e comando.

Para a simulação de redes MPLS e Serviços Diferenciados estão sendo utilizadas, respectivamente, as extensões [AHN 2001] e [PIE 2000] do ns2. [AHN 2001] implementa comutação MPLS de pacotes e manipulação de mensagens dos protocolos LDP/CR-LDP. A FIGURA 5.1 mostra a arquitetura de um nó MPLS. O classificador MPLS separa os pacotes recebidos em pacotes rotulados e não rotulados. Os pacotes não rotulados recebem tratamento convencional, sendo repassados ao classificador de endereços. Já os pacotes rotulados têm seu rótulo trocado e são enviados para o próximo nó diretamente, pelo próprio classificador MPLS. Para gerenciar as informações relacionadas aos LSPs, cada nó MPLS conta com 3 tabelas: a tabela parcial de encaminhamento (PFT), a base de informações de rótulo (LIB) e a base de informações de rotas explícitas (ERB).

A extensão de Serviços Diferenciados do ns2 [PIE 2000], implementa os serviços AF (*Assured Forwarding*) e EF (*Expedited Forwarding*). Para isto conta com uma estrutura de filas consistindo de 4 filas reais, cada uma contendo 3 filas RED [FLO 93] virtuais, que são os níveis de precedência. Cada fila real corresponde a uma classe de tráfego, e cada combinação de fila e nível de precedência é associada a um codepoint ou precedência de descarte. Existe também uma tabela contendo os mapeamentos de codepoints em PHBs e tabelas com as configurações de policiamento e marcação. Os roteadores de borda fazem marcação, conformação e policiamento dos fluxos, enquanto os roteadores do núcleo efetuam priorização.

Para que fosse possível simular a rede apresentada na FIGURA 5.2 foram necessárias algumas modificações nos arquivos fonte do simulador ns2. As modificações visavam aumentar a capacidade de definição de políticas dos nós de borda e tratamento de *codepoints* das filas da extensão de Serviços Diferenciados.

A versão do ns2 utilizada para a execução das simulações é o *snapshot* da versão 2.1b8 do dia 15/03/2002 (2.1b8-snapshot-20020315). Esta versão foi atualizada com as modificações citadas anteriormente, recompilada e validada, sendo que durante todo o processo não ocorreu nenhum erro ou falha de validação. O sistema operacional utilizado foi o Linux Mandrake 8.0 com *kernel* versão 2.4.3.

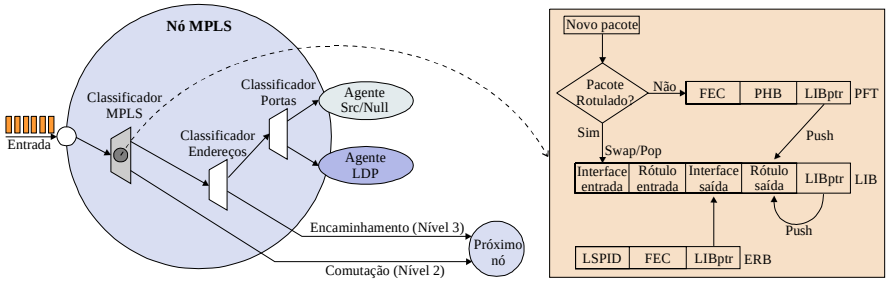

FIGURA 5.1 - Arquitetura de um nó MPLS

5.1 Descrição da simulação

A topologia utilizada nos testes é igual à mostrada na FIGURA 5.2, e consiste no seguinte: o núcleo da rede é composto por 8 LSRs MPLS (MPLS7 até MPLS14) ligados através de *links* de 1Mb/s. Estes *links* tem velocidade propositalmente baixa para facilitar a sua saturação. Nos pontos de acesso ao núcleo estão 6 LSRs (MPLS1 até MPLS6), que fazem o policiamento e a conformação do tráfego. Os LSRs de borda estão ligados aos LSRs do núcleo através de links de 1Mb/s, pelo mesmo motivo citado anteriormente. Assim sendo, um pacote, ao passar pelos LSRs da borda, é policiado e marcado com um DSCP, classificado em uma FEC e comutado, partindo então para o núcleo da rede. Nos testes atuais, estão sendo utilizados LSPs de mesma prioridade para cada agregado, escalonadores PQ, baseados em prioridade, para as filas dos serviços Ouro, Prata, Bronze e *Best effort*. A escolha de escalonadores PQ foi motivada pelo fato destes fornecerem o melhor comportamento com relação ao *jitter* [JAC 99]. A primeira e a última são filas *Droptail* enquanto a segunda e a terceira são gerenciadas por RIO [CLA 98], como pode ser visto na FIGURA 4.2. Esta configuração é derivada dos exemplos de [HEI 99] e [JAC 99]. A conformação é efetuada por conformadores *Token Bucket* nos LSRs de borda. A distribuição dos rótulos é efetuada através de LDP, operando no modo ordenado, sob demanda.

Ligados ao ISP estão 6 redes cliente, contendo diversos tipos de fonte de tráfego como CBR, FTP e HTTP. Os *links* que efetuam a ligação dos nós das redes cliente aos roteadores de fronteira RF e destes até os roteadores de borda da rede MPLS são de 2Mbps. Sua capacidade é maior do que a dos *links* da rede do ISP para que não ocorra a saturação de nenhum deles. Estão sendo considerados clientes que utilizam os serviços *Best effort*, *Assured Forwarding* (AF) e *Expedited Forwarding* (EF) de Serviços Diferenciados conectados ao ISP. Não estão sendo considerados clientes que utilizam Serviços Integrados.

A escolha desta topologia não visa simular uma rede já existente, mas deve-se ao fato de ela facilitar a análise dos resultados obtidos. A largura de banda dos links é propositadamente baixa para facilitar a sua saturação e a maneira como os nós estão interligados torna possível a análise dos dados em pontos pré-definidos da topologia. Além disto, esta topologia apresenta um tempo razoável para a execução das simulações e gera um arquivo de *trace* cujo tamanho não é exagerado (entre 12MBytes e 13MBytes). A análise de outra topologia e dos mecanismos integrados de MPLS e Serviços Diferenciados pode ser vista em [SER 2001b].

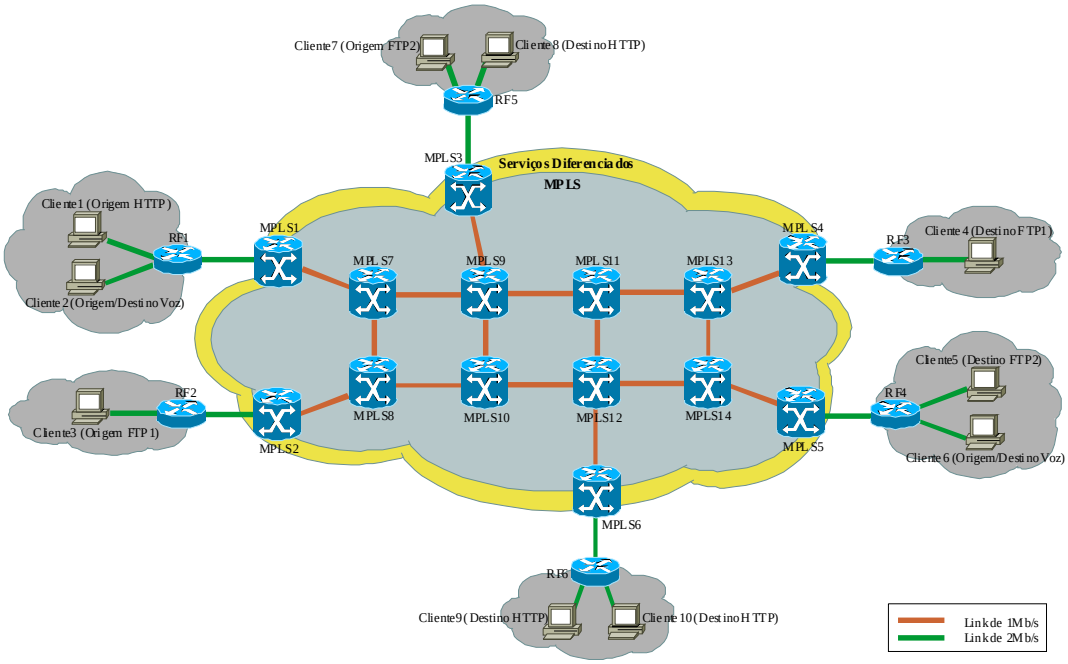

FIGURA 5.2 - Topologia utilizada nas simulações

5.1.1 Fluxos

Para a simulação foram criados diferentes fluxos. A modelagem das fontes de tráfego adotadas na simulação é detalhada a seguir:

- Tráfegos de voz
  - Protocolo: UDP
  - Tamanho do pacote: 66 bytes
  - Carga: 132Kbit/s
  - Intervalo entre as conexões: distribuição exponencial com valor médio de 20ms
  - Duração das conexões: distribuição exponencial com valor médio de 180ms
  - Quantidade de fluxos: 2
- Tráfegos FTP
  - Protocolo: TCP
  - Tamanho do pacote: 1500 bytes
  - Quantidade de fluxos: 2
- Tráfegos HTTP
  - Protocolo TCP
  - Tamanho máximo do pacote: 1500 bytes
  - Mensagem de requisição: 66 bytes
  - Resposta: 55.000 bytes
  - Intervalo entre as requisições: distribuição constante com valor médio de 0,2 segundo
  - Quantidade de fluxos: 3

Os fluxos de voz foram modelados de forma que simulassem a taxa de transmissão de fluxos VoIP (*Voice Over IP*) utilizando para compressão o CODEC G.729A [SAL 97]. Cada um dos fluxos é um agregado contendo 7 conversações simultâneas, e cada um dos pacotes transporta o equivalente a 30ms da conversação (3 *samples*). Para os fluxos FTP e HTTP foram utilizados pacotes com tamanho de 1500 bytes, pois é conhecida a preferência de TCP por pacotes de tamanho grande [KAM 2000]. O tamanho das páginas dos fluxos HTTP foi baseado na média de tamanho de algumas páginas escolhidas na Internet.

Os fluxos que trafegam pela rede, em conjunto com suas classes de serviço podem ser vistos na TABELA 5.1. Deseja-se que os fluxos de voz tenha maior prioridade do que os outros fluxos, por isto ele está sendo mapeado para a classe de tráfego Ouro. Ambos os fluxos FTP são mapeados para a classe prata, pois deseja-se que eles tenham um QoS superior e ao mesmo tempo possam efetuar eventuais rajadas. Os fluxos HTTP são os de menor prioridade, sendo por isto mapeados para as classes Bronze e *Best effort*. Cada classe tem um limite máximo de largura de banda, que pode ser visto na TABELA 5.2.

Para garantir filas pequenas ou inexistentes nos LSRs, as filas que servem os fluxos EF foram configuradas com sua taxa mínima de saída maior que a taxa máxima de chegada (taxa de chegada/serviço) [JAC 99]. Sabe-se que 6% a mais de reserva de largura de banda para os fluxos EF nos roteadores é um valor adequado para evitar instabilidade nos valores de atraso e *jitter* [ZIV 99]. Assim, como os fluxos de voz têm taxa de envio de aproximadamente 132Kbits/s utilizou-se a taxa de 150Kbits/s na configuração das filas EF do escalonador PQ. Para as outras classes, a largura de banda foi atribuída proporcionalmente à sua prioridade e levando em consideração os mecanismos de controle de fluxo do protocolo TCP.

TABELA 5.1 - Fluxos da simulação (Taxas de transmissão em Kbits/s)

Fluxo	Tipo	Origem	Destino	Taxa envio	CIR	CBS	Classe
VOZ1	Exponencial/UDP	Cliente2	Cliente6	~132Kb/s	150Kb/s	0Kb	Ouro
VOZ2	Exponencial/UDP	Cliente6	Cliente2	~132Kb/s	150Kb/s	0Kb	Ouro
FTP1	FTP/TCP	Cliente3	Cliente4	--	400Kb/s	1Kb	Prata
FTP2	FTP/TCP	Cliente7	Cliente5	--	400Kb/s	1Kb	Prata
HTTP1	HTTP/TCP	Cliente1	Cliente8	--	100Kb/s	0Kb	BE
HTTP2	HTTP/TCP	Cliente1	Cliente9	--	350Kb/s	1Kb	Bronze
HTTP3	HTTP/TCP	Cliente1	Cliente10	--	350Kb/s	1Kb	Bronze

Para os fluxos da classe prata e bronze os LSRs de borda remarcam todos os pacotes em excesso, marcando-os com uma precedência de descarte maior do que a de sua classe original. Desta forma, em caso de congestionamento, serão descartados primeiro os pacotes em excesso que entraram na rede.

O objetivo principal da simulação é mostrar que a infra-estrutura MPLS melhora em termos de provisionamento (largura de banda) e separação (*jitter*) dos fluxos quando se utiliza conjuntamente a ela mecanismos de Serviços Diferenciados.

TABELA 5.2 - Largura de banda configurada para os classes nos LSRs (Largura de banda em Kbits/s)

Classe	Largura de banda
Ouro	150Kb/s
Prata	400Kb/s
Bronze	350Kb/s
Best effort	100Kb/s

A sequência de eventos da simulação está na TABELA 5.3. A partir do instante 6.1s a rede ficará saturada, e o modelo proposto será colocado à prova. Foram executadas algumas variações da simulação com tempos de início da transmissão diferentes para os vários fluxos. Em todos os casos, verificou-se que os resultados não se alteravam substancialmente. Como a topologia tem largura de banda suficiente para suportar qualquer combinação com dois tipos de tráfego diferentes, entre Voz, FTP e HTTP, os resultados mais relevantes só podiam ser aferidos a partir do momento em que os três tipos de tráfego compartilhavam a rede, causando a sua saturação.

TABELA 5.3 - Eventos da simulação

Instante*	Evento
0.1s	Inicio da transmissão dos fluxos de voz
3.1s	Início da transmissão dos fluxos FTP
6.1s	Início da transmissão dos fluxos HTTP
22s	Encerramento da transmissão dos fluxos HTTP
25s	Encerramento da transmissão dos fluxos FTP
28s	Encerramento da transmissão dos fluxos de voz

* Valores aproximados

5.2 Requisitos e Resultados

Para efeito de comparação, duas simulações foram executadas, uma somente com MPLS e outra com o modelo proposto (MPLS e Serviços Diferenciados). Cada uma das simulações foi executada 10 vezes e os resultados foram tabulados e consolidados em planilhas. Os valores apresentados a seguir são os resultados médios da execução das 10 repetições. Em alguns casos é apresentado também o desvio padrão. Deve-se ressaltar que o simulador ns2 foi executado em modo não determinístico, por isso surgiram as variações nos resultados.

Para efetuar a análise dos dados foi utilizado o aplicativo TraceGraph [MAL 2002]. TraceGraph é um analisador de arquivos de *trace* gerados pelo simulador ns2 baseado nas bibliotecas de *run-time* do MatLab.

A definição de atraso adotada é de atraso fim a fim, ou seja, o valor absoluto da diferença entre o tempo de recepção do pacote no destino (t_r) e o tempo de transmissão na origem (t_t).

$$Atraso = t_r - t_t$$

EQUAÇÃO 5.1 - Cálculo do Atraso

A definição de *jitter* adotada é o valor absoluto da diferença entre os tempos de recepção (r_i e r_j) de dois pacotes consecutivos menos a diferença entre seus tempos de transmissão (t_i e t_j).

$$Jitter = \left|\left(r_j - r_i\right) - \left(t_j - t_i\right)\right|$$

EQUAÇÃO 5.2: Cálculo do jitter

5.2.1 Requisitos de QoS

Cada um dos tipos de fluxo presentes na simulação tem diferentes requisitos de qualidade de serviço. Os aspectos mais importantes a serem analisados são o atraso, o número de pacotes perdidos, o *jitter,* e a largura de banda recebida.

Atraso

O atraso faz com que uma conversação utilizando VoIP fique inadequada para os participantes e aumenta o tempo de resposta para aplicações de usuário iterativas. Para os fluxos de voz a recomendação G.114 do ITU-T [ITU 96] especifica que o atraso máximo de transmissão para conexões de voz deve ficar entre 0 e 150ms para ser aceitável na maioria das aplicações de usuário. No caso dos fluxos FTP, o atraso não é uma métrica relevante de QoS pois eles apresentam alta tolerância ao atraso [ARM 2000]. Já os fluxos HTTP têm uma tolerância um pouco menor, entre média e alta [ARM 2000].

Perda de pacotes

A perda de pacotes pode causar distorções em conversações VoIP, além da inevitável perda de informações, e conseqüente retransmissão, para os fluxos FTP e HTTP. Para os fluxos de voz é tolerável perder entre 1% e 3% dos pacotes [CHU 99], sendo que, acima de 3% a qualidade da conversação é muito baixa. Já os fluxos FTP e HTTP apresentam uma tolerância baixa a descartes, de forma que eles devem ser, a todo custo, evitados [ARM 2000].

Jitter

A ocorrência de *jitter* excessivo em um fluxo VoIP torna a conversação instável e difícil de entender. Para uma conversação de boa qualidade a média do intervalo de tempo entre a chegada de dois pacotes consecutivos no destino deve ser praticamente igual ao intervalo de tempo entre as suas transmissões na origem, e seu desvio padrão

deve ser baixo. No caso dos fluxos FTP e HTTP, ambos apresentam uma alta tolerância ao *jitter* [ARM 2000].

Largura de banda

A largura de banda é uma das medidas mais importantes de QoS para aplicações elásticas como FTP e HTTP. Elas são projetadas para transferir os dados no menor tempo possível, utilizando toda a largura de banda disponível. Assim, se a rede estiver congestionada, sua velocidade decresce. Já para os fluxos de voz, os requisitos de largura de banda não são muito altos, no entanto, esta largura de banda tem que estar disponível durante todo o tempo.

5.2.2 Resultados

A TABELA 5.4 mostra um resumo dos resultados obtidos. A parte superior da tabela mostra os resultados gerais sem fazer nenhuma distinção dos fluxos. Nela é possível perceber que em termos médios de pacotes enviados e descartados os dois modelos são praticamente equivalentes. Entretanto a previsibilidade do modelo MPLS é menor, como demonstrado pelo seu desvio padrão muito mais alto do que o do modelo MPLS+Serviços Diferenciados.

A parte inferior da tabela mostra diversos parâmetros de Qualidade de Serviço de cada fluxo tanto no modelo MPLS como no modelo MPLS+Serviços Diferenciados.

Atraso

O atraso é uma métrica de QoS extremamente importante para os fluxos VoIP. Analisando a TABELA 5.4 é possível perceber que o fluxo VOZ1 no modelo MPLS sofreu um atraso médio de 206ms, ou seja, 44ms maior que o máximo especificado na recomendação G.114 do ITU-T [ITU 96]. Já o fluxo VOZ2 sofreu um atraso aceitável de 34ms. Por conta destes resultados o modelo MPLS não atendeu satisfatoriamente os requisitos de atraso dos fluxos de voz. Quando se considera o modelo MPLS+Serviços Diferenciados, ambos os fluxos, VOZ1 e VOZ2, encontram-se dentro do limite tolerável, com atrasos médios de 55ms e 28ms respectivamente.

Perda de pacotes

A perda de pacotes deve ser evitada a todo o custo, independentemente do tipo de fluxo sendo transmitido. No entanto, os dois fluxos de voz, sofreram descartes no modelo MPLS. Além disto, os fluxos FTP2, HTTP2 e HTTP3 também sofreram perdas de pacotes, embora em menor escala. Deve-se lembrar que os fluxos que utilizam TCP como protocolo de transporte contam com mecanismos de controle de fluxo que reagem aos descartes diminuindo a taxa de envio. Como desejamos priorizar os fluxos VoIP e FTP, o modelo MPLS não tem correspondido às expectativas. No modelo MPLS + Serviços Diferenciados este problema não ocorre. Além disto, a quantidade total de pacotes enviados, tanto de voz como FTP é maior. O único fluxo que tem pacotes descartados é o fluxo HTTP1 que é o fluxo com menor prioridade (*Best Effort*).

Jitter

Os valores de *jitter*, assim como os de atraso, são muito importantes para os fluxos de voz. Valores muito altos de *jitter* podem tornar a conversação incompreensível. Analisando a TABELA 5.4 podemos comparar os valores médios de *jitter* de ambos os fluxos de voz, e também o intervalo entre os pacotes quando estes foram enviados. Ambos os modelos atendem satisfatoriamente os requisitos de *jitter* dos fluxos de voz, com uma pequena vantagem, também em termos de desvio padrão, para o modelo MPLS + Serviços Diferenciados. Esta vantagem deve-se à utilização de um escalonador baseado em prioridade [JAC 99].

Largura de banda

A largura de banda disponibilizada para cada fluxo é a métrica de QoS mais importante para aplicações elásticas como FTP e HTTP. Observando os resultados na TABELA 5.4 é possível verificar que para todos os fluxos, com exceção de HTTP3, a largura de banda aumenta quando passamos do modelo MPLS para o modelo MPLS + Serviços Diferenciados. A largura de banda de HTTP3 diminui porque ele é o fluxo de menor prioridade. O melhor exemplo é o fluxo FTP1 que tem um aumento de aproximadamente 13% do seu *throughput*. Como a taxa de envio dos fluxos VoIP varia pouco, o *throughput* dos fluxos FTP é uma das observações mais importantes. Ela representa o ganho em desempenho obtido pelo tráfego de prioridade média quando parte do tráfego HTTP é conformado através dos mecanismos de Serviços Diferenciados. Tendo isto em mente, verifica-se que o modelo MPLS+Serviços Diferenciados também atende melhor os fluxos dependentes de largura de banda.

TABELA 5.4 - Resultados da simulação

	MPLS (Média)	Desvio padrão	MPLS + Serviços Diferenciados (Média)	Desvio padrão
Total de pacotes enviados	9.146,4	50	9.244,4	11,5
Pacotes descartados	19	3,2	6,2	1,3
Quantidade de bytes enviados	5.593.070	39.795,8	5.675.368	1.551,7
Quantidade de bytes descartados	9.948,8	5.310,7	9.300	1.955,7
Pacotes enviados				
VOZ1	781,2	9	794	6,7
VOZ2	780,2	12,8	782	8,2
FTP1	1.498,2	1,6	1.629,8	3
FTP2	1.260,6	51,5	1.286,8	1,6
HTTP1	277,8	1,6	145	2,8
HTTP2	236,4	14,5	241,6	1,3
HTTP3	223,8	32,9	240,2	0,4

TABELA 5.5 - Resultados da simulação (Continuação)

	MPLS (Média)	Desvio padrão	MPLS + Serviços Diferenciados (Média)	Desvio padrão
Pacotes perdidos				
VOZ1	8,6	6,6	0	0
VOZ2	4,2	9,4	0	0
FTP1	0	0	0	0
FTP2	2,4	1,1	0	0
HTTP1	0	0	6,2	1,3
HTTP2	0,4	0,9	0	0
HTTP3	0,2	0,4	0	0
Atraso médio				
VOZ1	0,206s	0,009s	0,055s	0,0003s
VOZ2	0,034s	0,0004s	0,028s	0,000005s
FTP1	0,263s	0,0003s	0,240s	0,0005s
FTP2	0,253s	0,007s	0,296s	0,0004s
HTTP1	0,352s	0,005s	0,599s	0,0314s
HTTP2	0,385s	0,016s	0,359s	0,0158s
HTTP3	0,426s	0,057s	0,569s	0,0155s
Largura de banda				
VOZ1	133,52Kbit/s	--	139,21Kbit/s	--
VOZ2	131,39Kbit/s	--	141,31Kbit/s	--
FTP1	256,98Kbit/s	--	290,51Kbit/s	--
FTP2	215,81Kbit/s	--	229,37Kbit/s	--
HTTP1	47,65Kbit/s	--	24,74Kbit/s	--
HTTP2	40,48Kbit/s	--	43,06Kbit/s	--
HTTP3	38,53Kbit/s	--	42,81Kbit/s	--
Intervalo entre as transmissões				
VOZ1	0,03544s	0,010s	0,03561s	0,012s
VOZ2	0,03598s	0,013s	0,03564s	0,012s
Jitter				
VOZ1	0,03571s	0,006s	0,03567s	0,005s
VOZ2	0,03615s	0,015s	0,03572s	0,007s

Os gráficos a seguir permitem uma análise mais detalhada. Os gráficos de largura de banda mostram a largura de banda recebida pelos fluxos durante o tempo de execução da simulação. Os gráficos de *jitter* mostram o *jitter* entre os pacotes de cada fluxo, sendo estes ordenados através de seu número de seqüência. Os gráficos de atraso são apresentados utilizando a quantidade de pacotes de cada fluxo que sofreu determinado valor de atraso em segundos.

Ao se comparar os gráficos da FIGURA 5.3 e da FIGURA 5.4 é possível perceber que a largura de banda recebida pelo fluxo VOZ1 é muito mais constante quando se utiliza o modelo MPLS+Serviços Diferenciados. Considerando que as variações de largura de banda podem resultar em enfileiramentos desnecessários nos roteadores intermediários a variação do *jitter* também acaba sendo maior no modelo MPLS, como pode ser visto na FIGURA 5.5 e na FIGURA 5.6. O atraso dos pacotes, mostrado na FIGURA 5.7 e na FIGURA 5.8, mostra que a maior parte dos pacotes do

fluxo VOZ1 tem atraso superior a 0,1s no modelo MPLS, enquanto no modelo MPLS+Serviços Diferenciados a maior parte dos pacotes tem o atraso inferior a 0,055s. Considerando que o fluxo VOZ1 é sensível ao atraso e ao *jitter*, o modelo MPLS+Serviços Diferenciados mostra-se mais adequado para o transporte de fluxos deste tipo.

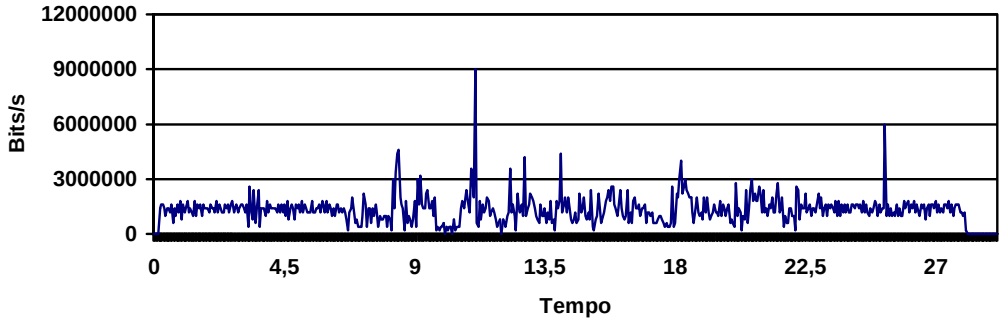

FIGURA 5.3 - Largura de banda recebida pelo fluxo Voz1 no modelo MPLS

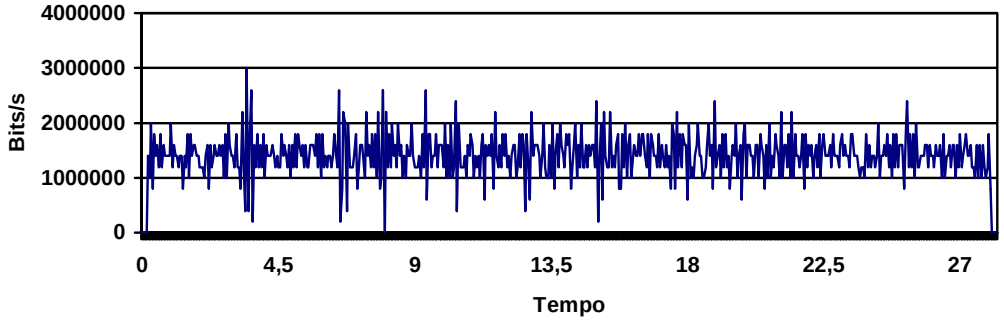

FIGURA 5.4 - Largura de banda recebida pelo fluxo Voz1 no modelo MPLS+Serviços Diferenciados

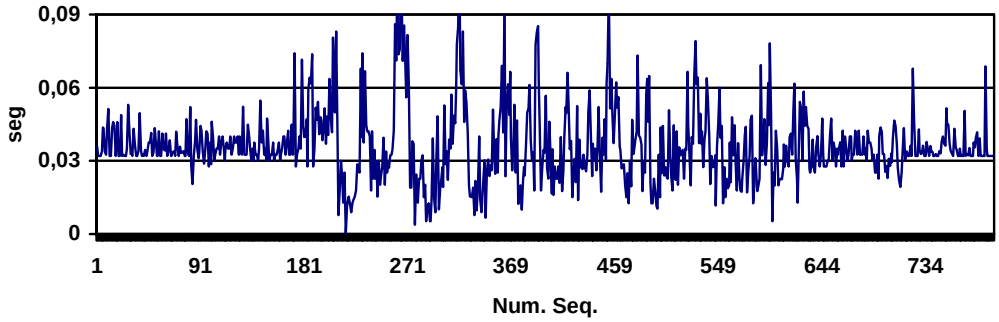

FIGURA 5.5 - Jitter apresentado pelo fluxo Voz1 no modelo MPLS

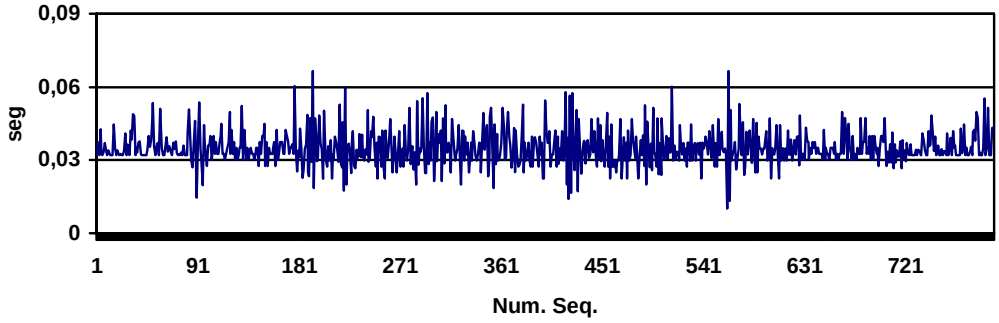

FIGURA 5.6 - Jitter apresentado pelo fluxo Voz1 no modelo MPLS+Serviços Diferenciados

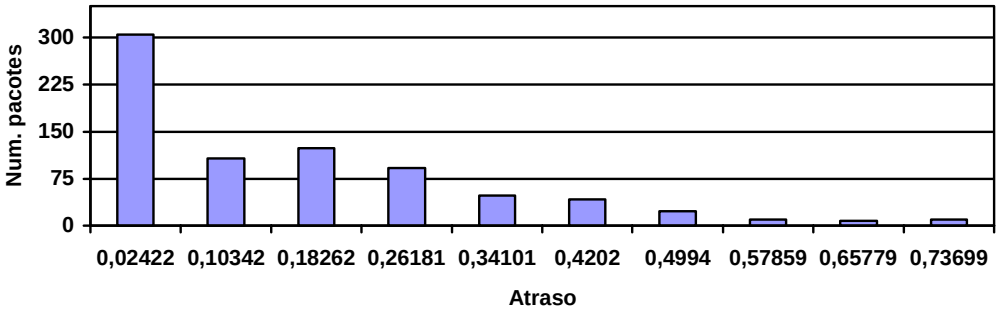

FIGURA 5.7 - Atraso entre a origem e o destino no fluxo Voz1 no modelo MPLS

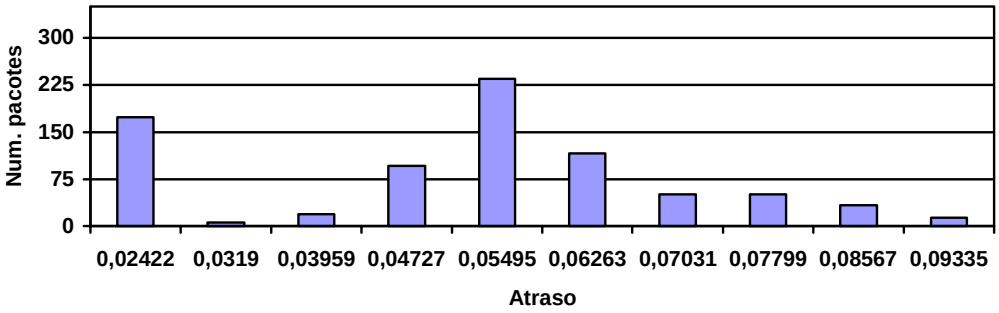

FIGURA 5.8 - Atraso entre a origem e o destino no fluxo Voz1 no modelo MPLS+Serviços Diferenciados

Analisando os gráficos de largura de banda recebida e jitter apresentado pelo fluxo VOZ2, tanto no modelo MPLS, na FIGURA 5.9 e FIGURA 5.11, como MPLS+Serviços Diferenciados, na FIGURA 5.10 e FIGURA 5.12, percebe-se que eles não apresentam grandes diferenças. Isto se deve ao fato de o fluxo VOZ2 disputar os *links* com um número menor de fluxos quando comparado com o fluxo VOZ1. Isso mostra que mesmo com a inserção do processamento de Serviços Diferenciados nos LSRs não há uma perda sensível de performance. Para fluxos de alta prioridade, como

VOZ2 ocorre exatamente o contrário: o atraso ainda diminui, como pode ser visto na FIGURA 5.13 e na FIGURA 5.14.

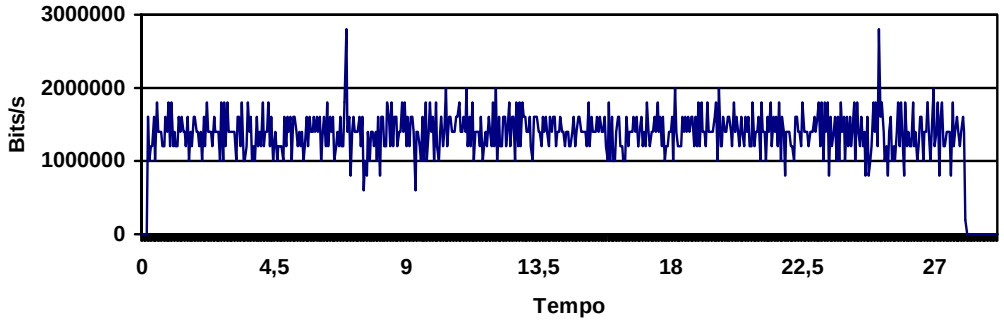

FIGURA 5.9 - Largura de banda recebida pelo fluxo Voz2 no modelo MPLS

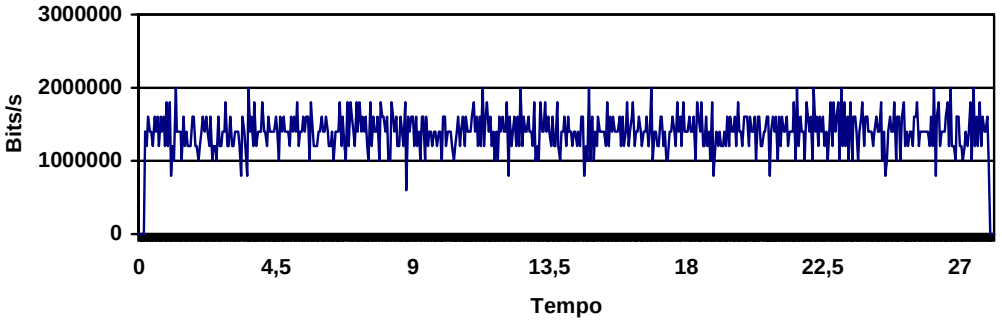

FIGURA 5.10 - Largura de banda recebida pelo fluxo Voz2 no modelo MPLS+Serviços Diferenciados

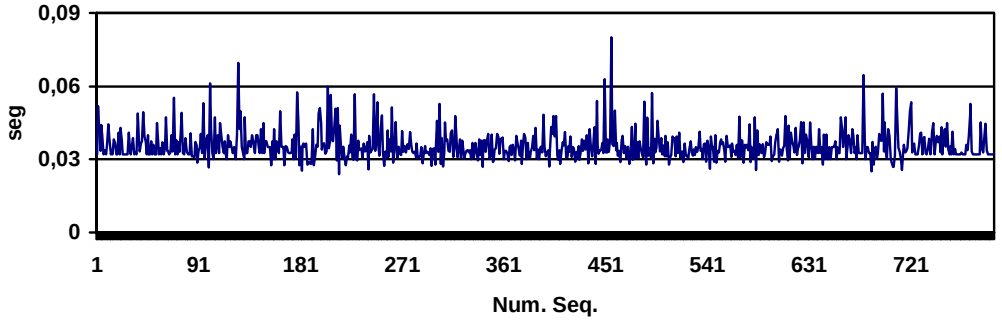

FIGURA 5.11 - Jitter apresentado pelo fluxo Voz2 no modelo MPLS

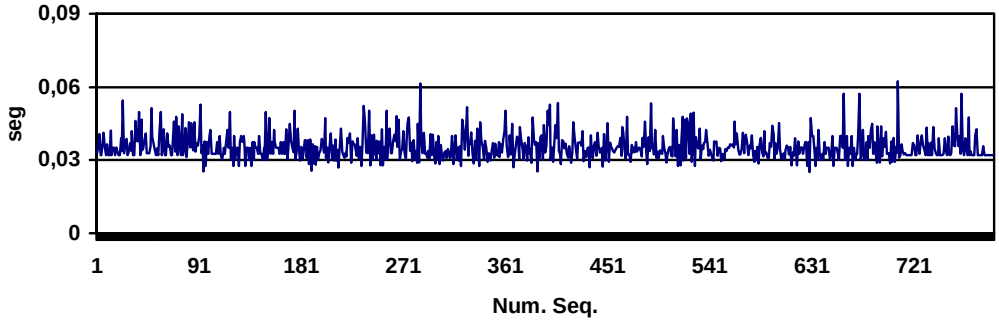

FIGURA 5.12 - Jitter apresentado pelo fluxo Voz2 no modelo MPLS+Serviços Diferenciados

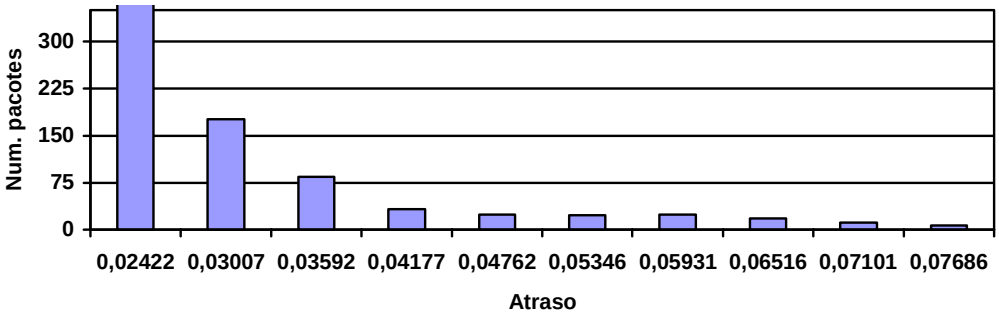

FIGURA 5.13 - Atraso entre a origem e o destino no fluxo Voz2 no modelo MPLS

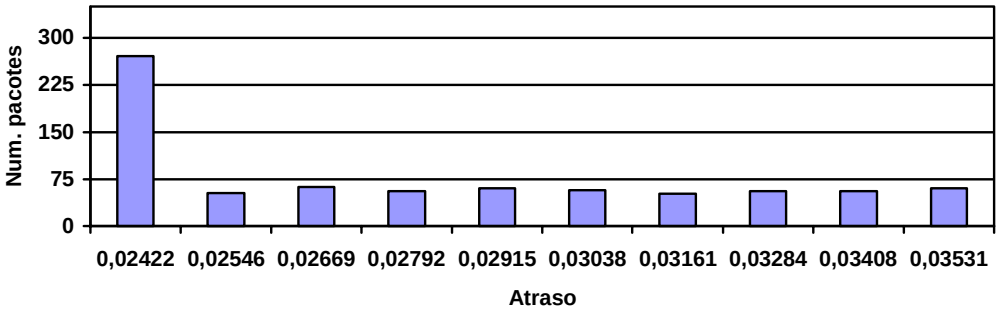

FIGURA 5.14 - Atraso entre a origem e o destino no fluxo Voz2 no modelo MPLS+Serviços Diferenciados

O fluxo FTP1 é mapeado para a classe Prata. Assim espera-se que ele obtenha um QoS superior ao das classes bronze e *Best effort*. Isto será alcançado através de sua priorização frente aos outros fluxos. A FIGURA 5.15 e a FIGURA 5.16 mostram que este objetivo é alcançado no modelo MPLS+Serviços Diferenciados. A largura de banda recebida pelo fluxo FTP1 é praticamente constante, em torno de 400Kb/s, o máximo configurado para a classe prata. A FIGURA 5.17 e a FIGURA 5.18 mostram que o jitter é um pouco mais previsível no modelo MPLS+Serviços Diferenciados, entretanto isto

não importa muito para fluxos FTP. O atraso dos pacotes, mostrado na FIGURA 5.19 e na FIGURA 5.20, é menor no modelo MPLS. No entanto, para fluxos FTP a largura de banda recebida é mais importante do que o atraso e o *jitter*, tanto que no mesmo espaço de tempo o modelo MPLS+Serviços Diferenciados permite a transmissão de 100 pacotes a mais do que o modelo MPLS, como pode ser visto na TABELA 5.4.

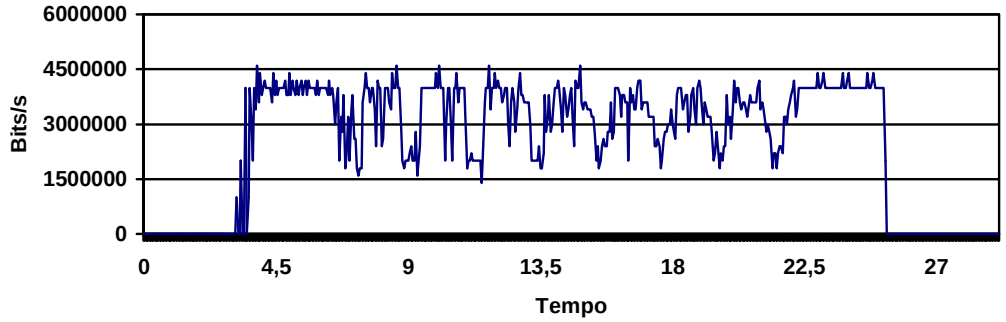

FIGURA 5.15 - Largura de banda recebida pelo fluxo FTP1 no modelo MPLS

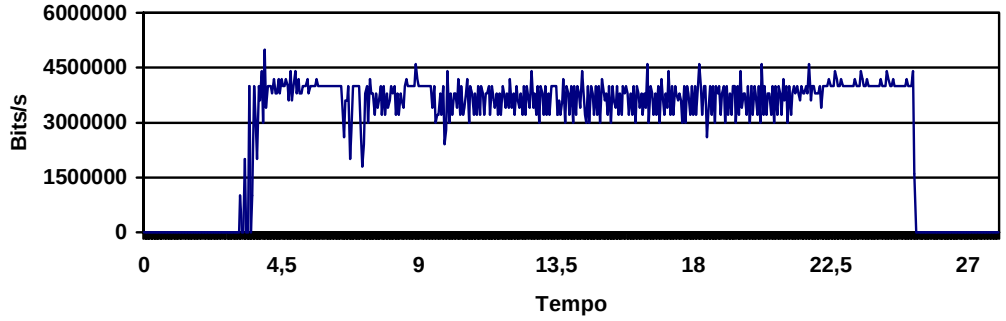

FIGURA 5.16 - Largura de banda recebida pelo fluxo FTP1 no modelo MPLS+Serviços Diferenciados

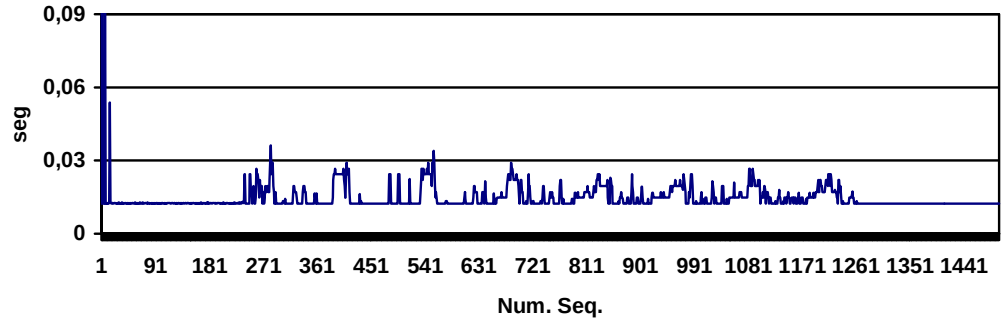

FIGURA 5.17 - Jitter apresentado pelo fluxo FTP1 no modelo MPLS

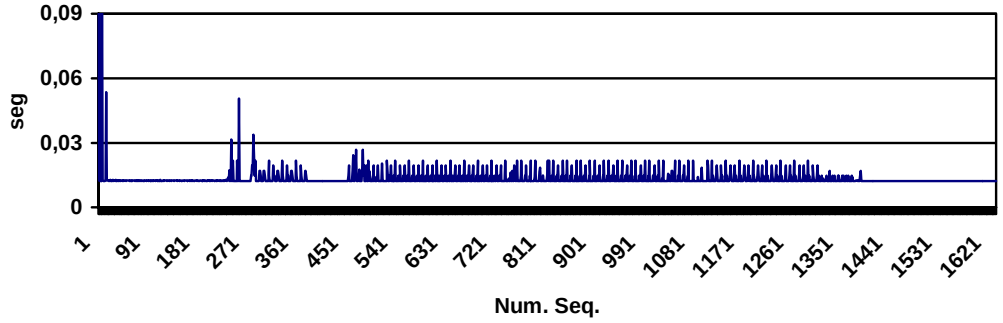

FIGURA 5.18 - Jitter apresentado pelo fluxo FTP1 no modelo MPLS+Serviços Diferenciados

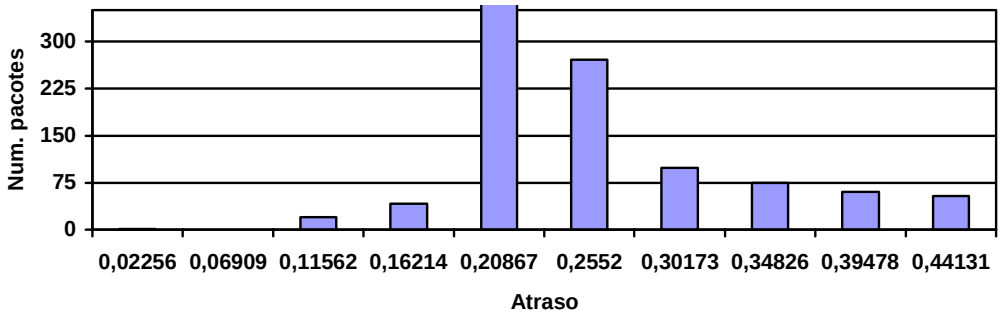

FIGURA 5.19 - Atraso entre a origem e o destino no fluxo FTP1 no modelo MPLS

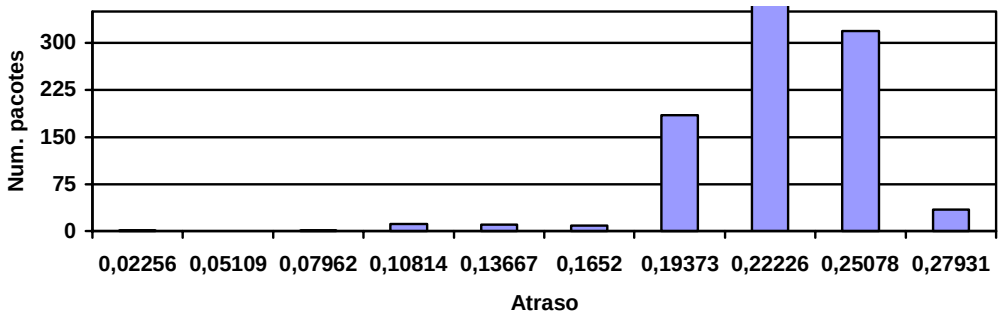

FIGURA 5.20 - Atraso entre a origem e o destino no fluxo FTP1 no modelo MPLS+Serviços Diferenciados

O fluxo FTP2 também é mapeado para a classe Prata. No entanto, ele disputa os *links* com uma quantidade maior de fluxos do que FTP1. A largura de banda recebida, mostrada na FIGURA 5.21 e na FIGURA 5.22, demonstra que no modelo MPLS a entrada dos fluxos HTTP depois do instante 6s prejudica muito a transmissão do fluxo FTP2. No modelo MPLS+Serviços Diferenciados isto também ocorre, mas em escala menor, graças aos mecanismos de conformação de tráfego. O fluxo FTP2 consegue manter um patamar constante de aproximadamente 250Kb/s. O jitter, mostrado na

FIGURA 5.23 e na FIGURA 5.24 não se altera muito. O atraso, representado na FIGURA 5.25 e na FIGURA 5.26 é menor no modelo MPLS, no entanto, como no fluxo FTP1 o que importa é a largura de banda, a quantidade de pacotes enviados é maior no modelo MPLS+Serviços Diferenciados.

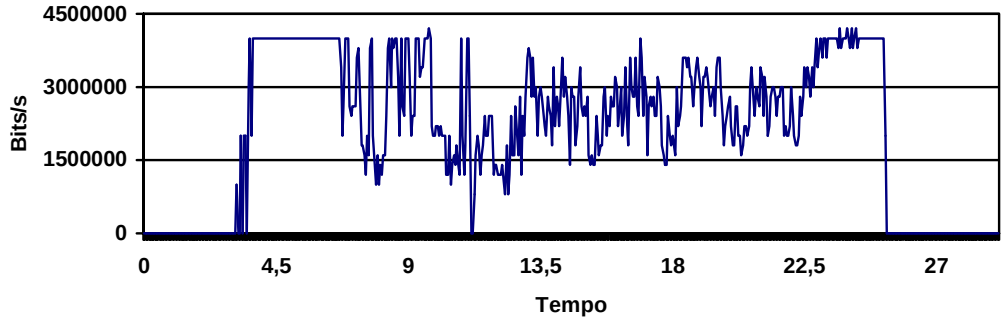

FIGURA 5.21 - Largura de banda recebida pelo fluxo FTP2 no modelo MPLS

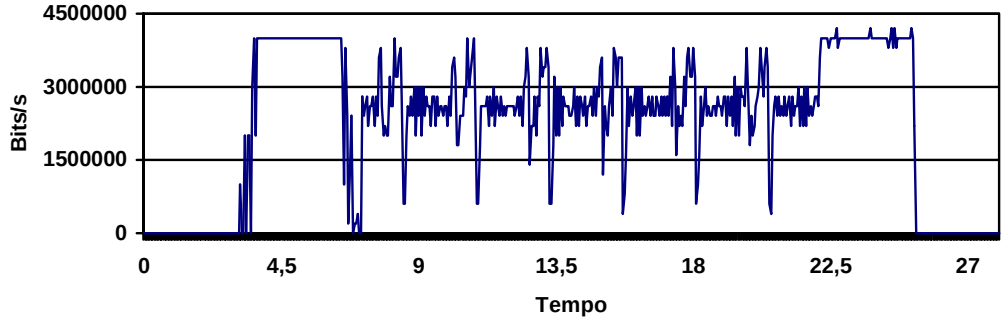

FIGURA 5.22 - Largura de banda recebida pelo fluxo FTP2 no modelo MPLS+Serviços Diferenciados

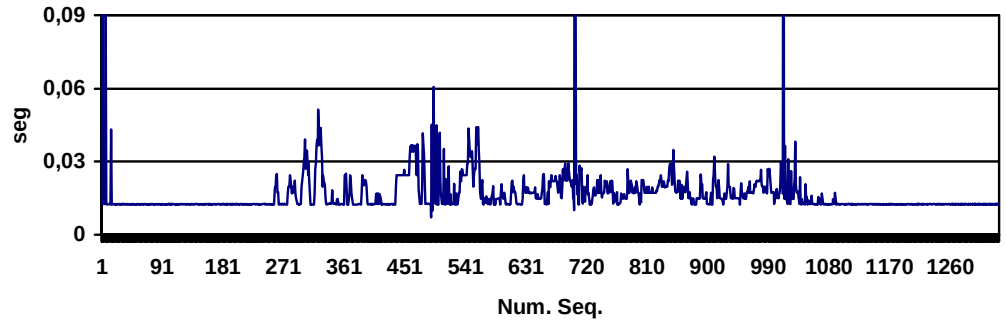

FIGURA 5.23 - Jitter apresentado pelo fluxo FTP2 no modelo MPLS

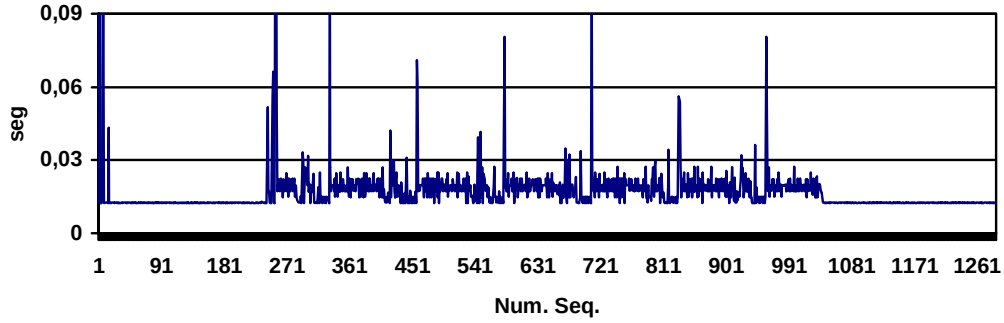

FIGURA 5.24 - Jitter apresentado pelo fluxo FTP2 no modelo MPLS+Serviços Diferenciados

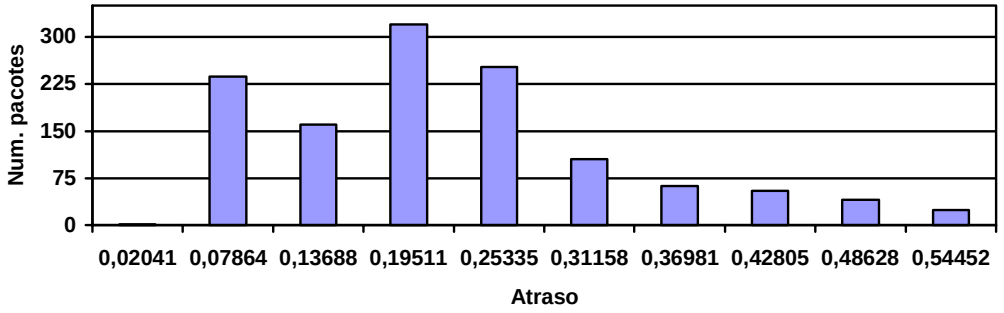

FIGURA 5.25 - Atraso entre a origem e o destino no fluxo FTP2 no modelo MPLS

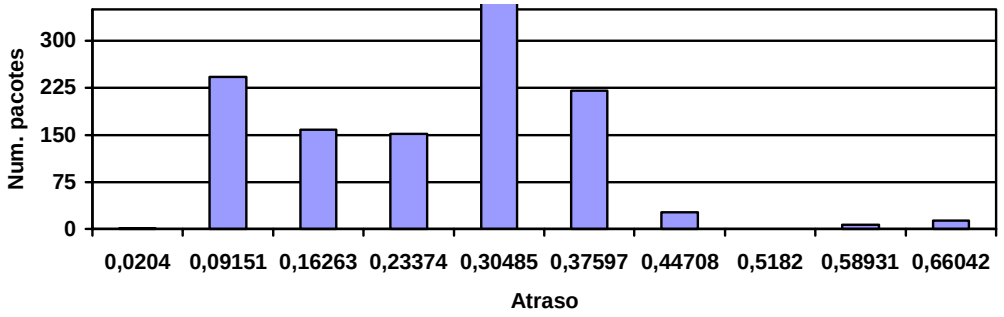

FIGURA 5.26 - Atraso entre a origem e o destino no fluxo FTP2 no modelo MPLS+Serviços Diferenciados

O fluxo HTTP1 é o fluxo com menor prioridade, pois pertence à classe *Best effort*. A largura de banda recebida é mostrada na FIGURA 5.27 e na FIGURA 5.28. No modelo MPLS, por não haver nenhum mecanismo de priorização e conformação, ele acaba prejudicando a transmissão dos outros fluxos. Já no modelo MPLS+Serviços Diferenciados sua largura de banda é limitada a 100Kb/s. O número de descartes é pequeno porque os mecanismos de controle de fluxo de TCP/IP adaptam a taxa de transmissão à largura de banda disponível.

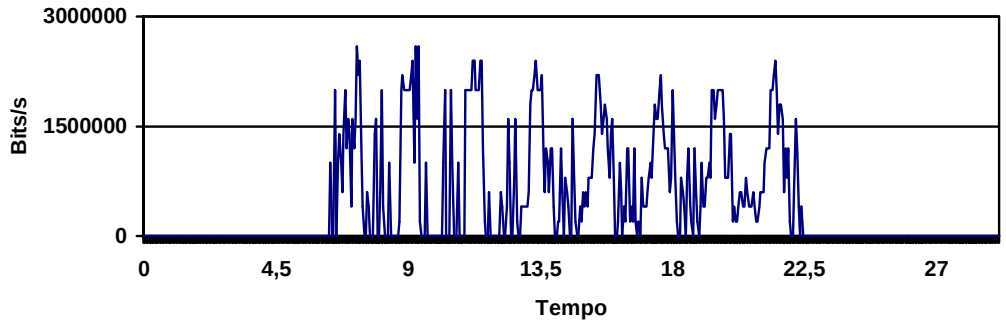

FIGURA 5.27 - Largura de banda recebida pelo fluxo HTTP1 no modelo MPLS

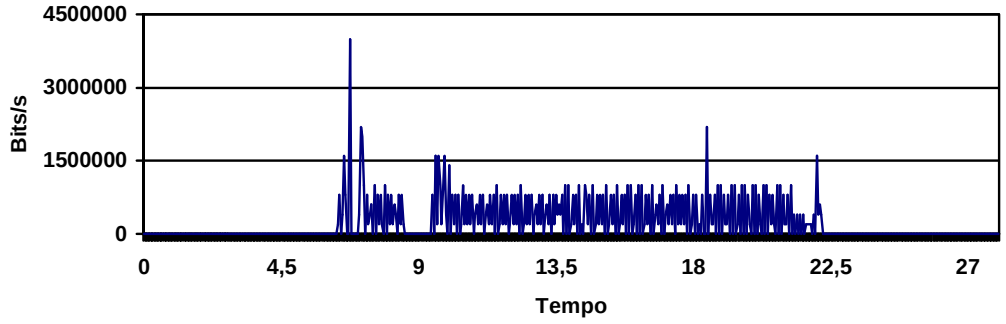

FIGURA 5.28 - Largura de banda recebida pelo fluxo HTTP1 no modelo MPLS+Serviços Diferenciados

O fluxo HTTP2 pertence à classe bronze, assim, tem prioridade maior do que os fluxos *Best effort*. A FIGURA 5.29 e a FIGURA 5.30 mostram a largura de banda recebida. No modelo MPLS+Serviços Diferenciados a largura de banda disponível após as requisições é maior, fazendo com que as páginas sejam transferidas mais rapidamente.

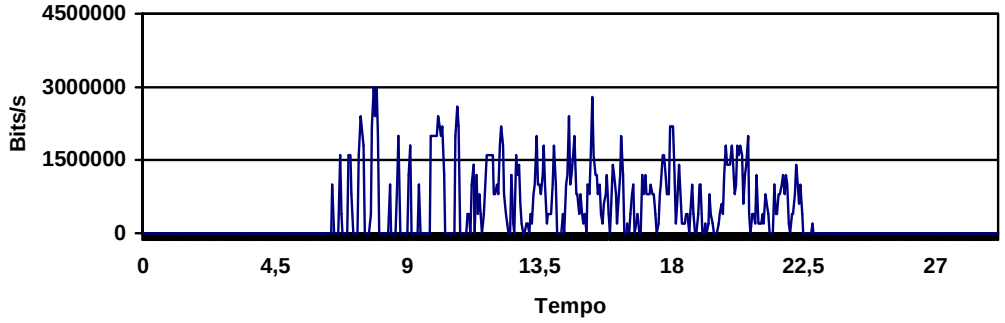

FIGURA 5.29 - Largura de banda recebida pelo fluxo HTTP2 no modelo MPLS

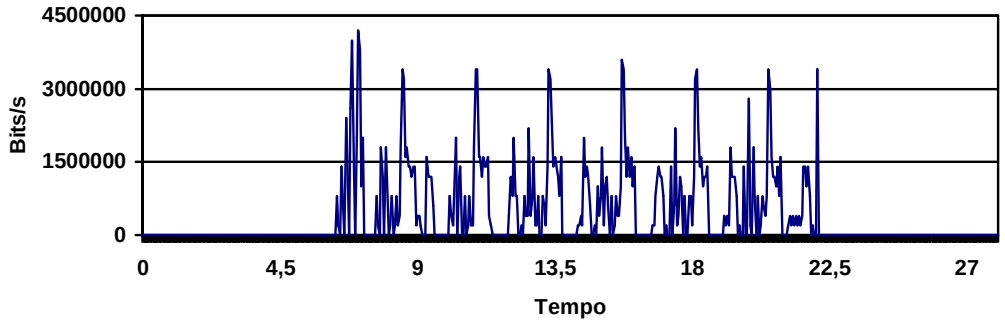

FIGURA 5.30 - Largura de banda recebida pelo fluxo HTTP2 no modelo MPLS+Serviços Diferenciados

O fluxo HTTP3, assim como o fluxo HTTP2 pertence à classe Bronze. A largura de banda recebida, mostrada na **FIGURA 5.31** e na FIGURA 5.32, não se altera muito entre os modelos MPLS e MPLS+Serviços Diferenciados, sendo um pouco maior neste último. Isto permite que um número um pouco maior de pacotes seja transferido.

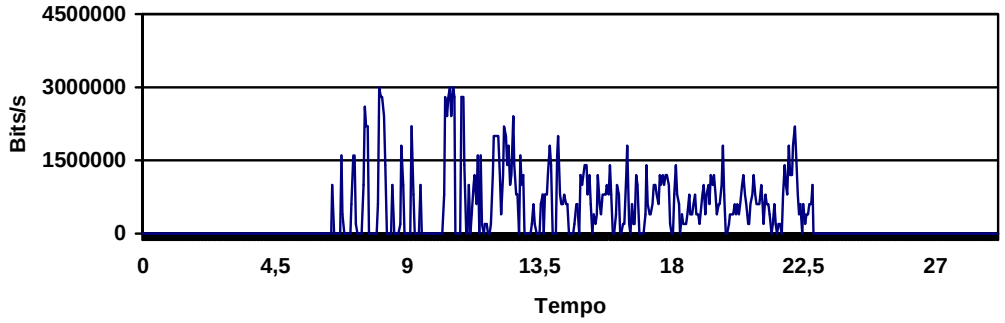

FIGURA 5.31 - Largura de banda recebida pelo fluxo HTTP3 no modelo MPLS

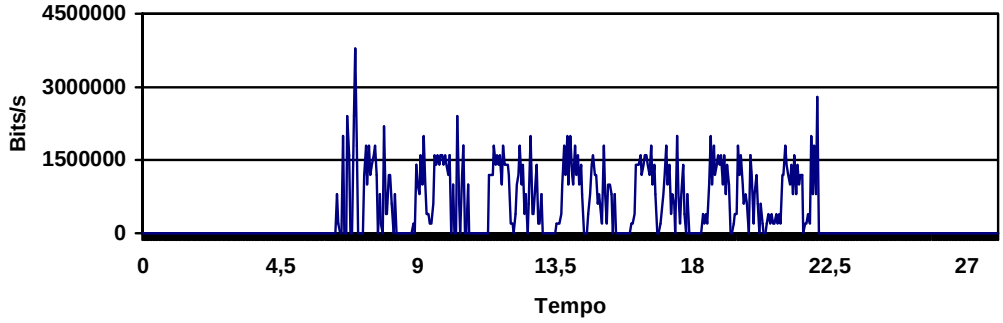

FIGURA 5.32 - Largura de banda recebida pelo fluxo HTTP3 no modelo MPLS+Serviços Diferenciados

Os gráficos mostrados anteriormente provam que os objetivos visados pelo modelo MPLS+Serviços Diferenciados, quais sejam, melhorar em termos de provisionamento (largura de banda) e separação (*jitter*) a transmissão dos fluxos na infra-estrutura MPLS através da introdução de mecanismos de Serviços Diferenciados, foram plenamente alcançados. Além disto, o modelo MPLS+Serviços Diferenciados mostrou-se mais adequado que o modelo MPLS para o transporte de fluxos com requisitos estritos de atraso, *jitter* e largura de banda, como VoIP, e de fluxos de aplicações elásticas, como FTP e HTTP, cujo requisito maior é a largura de banda.

6 Conclusão

As redes IP, e notadamente a Internet, estão se transformando rapidamente em uma infra-estrutura voltada ao foco comercial, vital para diversas empresas e usuários. Graças a esta transformação, surgiram também demandas clamando por uma melhora na qualidade do serviço oferecido. Ao invés de apenas um tipo de serviço, o *Best effort*, os serviços serão oferecidos através de classes com diferentes parâmetros de qualidade de serviço associadas a cada classe. Quanto maior a qualidade de serviço desejada, maior o preço a ser pago. As empresas, na ânsia de que seus clientes obtenham acesso rápido a seus produtos, estarão dispostas a pagar este preço para tornar seus serviços mais rápidos, eficientes e confiáveis, podendo tanto contratar somente uma classe, como diversas classes, utilizando-as para diversos fins além da troca de dados com os clientes.

No IETF, diversas arquiteturas têm sido propostas no intuito de oferecer mecanismos de fornecimento de Qualidade de Serviço (QoS) para a Internet, como por exemplo:

- A arquitetura de Serviços Integrados, baseada no RSVP como protocolo de sinalização;
- A arquitetura de Serviços Diferenciados;
- A arquitetura MPLS (*Multiprotocol Label Switching*);
- A Engenharia de Tráfego;
- O Roteamento baseado em restrições (CBR);

Cada uma destas arquiteturas apresenta vantagens e desvantagens. A arquitetura de Serviços Integrados, apesar de fornecer um alto nível de garantia de reserva de recursos por fluxo, possui sérios problemas de escalabilidade e complexidade. Já a arquitetura de Serviços Diferenciados, por sua vez, é simples e escalável, todavia apresenta deficiências no gerenciamento de recursos. Ambas utilizam o roteamento da camada de rede, que pode ocasionar o surgimento de gargalos. Estes problemas podem ser resolvidos com a utilização conjunta de Engenharia de Tráfego e MPLS.

Tendo em vista o fato da Internet ser uma rede heterogênea, a observação de que nenhuma das arquiteturas atende a todos os requisitos para se fornecer uma garantia de QoS fim a fim, tem propiciado o surgimento de modelos que combinam estas arquiteturas. Todas elas são vistas como complementares no provisionamento de QoS fim a fim. Desta maneira, tem-se como objetivo principal a união de suas vantagens em uma única implementação.

Este trabalho apresentou um modelo de integração de tecnologias de QoS que permite que redes periféricas baseadas em Serviços Diferenciados, Serviços Integrados, MPLS ou nenhuma arquitetura de fornecimento de QoS, utilizem os serviços de um backbone baseado em MPLS para comutação e Serviços Diferenciados para priorização dos pacotes. Assim, no *backbone*, combina-se a escalabilidade e a simplicidade de Serviços Diferenciados, com a velocidade de MPLS.

Não é necessário manter informações de estado em cada nó do núcleo aumentando a escalabilidade. O modelo propõe a utilização de 4 classes de serviços: ouro, prata, bronze e *best effort*. A agregação/separação dos fluxos em LSPs facilita a Engenharia de Tráfego, pois permite que o administrador saiba exatamente o que está passando e por onde em sua rede. Adicionalmente, tendo em vista as restrições de QoS e Engenharia de Tráfego, é possível o emprego do CBR de modo a encontrar as melhores rotas no núcleo da rede. Também foram apresentadas as maneiras como o modelo proposto pode interoperar com as redes vizinhas.

Para avaliar a funcionalidade do modelo proposto, foi utilizado o simulador de redes ns2. Para validar a simulação optou-se pela intuição de especialistas, uma vez que não existe nenhum laboratório para testes razoavelmente completo, em que fosse possível avaliar o comportamento do modelo de integração. Desta forma, diversas situações foram simuladas para testar o comportamento do modelo em diferentes circunstâncias consideradas críticas. As configurações utilizadas refletem, em grande parte, configurações possíveis nos roteadores existentes, bem como não foram empregados recursos inexistentes nas implementações de *firmware* atuais.

Os resultados obtidos atestam a aplicabilidade da proposta. O modelo MPLS+Serviços Diferenciados demonstrou melhor desempenho em todos os parâmetros de QoS analisados: atraso, *jitter*, perda de pacotes e largura de banda.

O atraso e o *jitter* são determinantes para fluxos de tempo real como VoIP. Já a largura de banda e a perda de pacotes são importantes para os fluxos de aplicações elásticas, como FTP e HTTP. Nas simulações, com fluxos de tempo real e fluxos elásticos, os parâmetros de QoS melhoraram para ambos os tipos na transposição do modelo MPLS para o modelo MPLS+Serviços Diferenciados o que comprova a validade do modelo. Além disto, a performance da rede, no aspecto global, também melhorou.

6.1 Trabalhos futuros

Futuramente serão testados outros tipos de escalonadores e políticas de filas, outros tipos de LSPs, tanto com relação à configuração, como ao tipo de fluxo, além de outros tipos de fontes de tráfego.

Outras possibilidades para desenvolvimento de um estudo posterior incluem um agente para ns2 que efetue o mapeamento de Serviços Integrados para os serviços do modelo proposto nos roteadores de borda, modificações no modelo proposto para suportar operações *multicast* e diretrizes voltadas a como dividir de modo eficaz o tráfego entre E-LSPs e L-LSPs através de Engenharia de Tráfego em um contexto complexo, como o de um ISP.

Anexo 1 Artigo submetido para publicação no SBRC 2002

Mecanismos para interoperação de backbones MPLS e redes que utilizem outras arquiteturas de QoS

Fernando M. Serenato **Juergen Rochol**

Universidade Federal do Rio Grande do Sul (UFRGS) / Instituto de Informática
Caixa Postal 15064 - CEP 91501-970 - Porto Alegre - RS
E-mail: {serenato, juergen}@inf.ufrgs.br

Resumo

Acredita-se que no futuro as redes de telecomunicação e dados serão integradas em uma só rede, baseada na comutação de pacotes IP. Esta rede deverá oferecer serviços com qualidade (QoS) para as aplicações atuais e futuras. Uma das tecnologias que deverá ser adotada no núcleo desta nova rede é MPLS. MPLS introduz o conceito de switching (comutação) no ambiente IP e também permite que seja implementada a Engenharia de Tráfego, otimizando sua utilização através do roteamento baseado em restrições. Junto com MPLS outras arquiteturas para fornecimento de QoS, como Serviços Integrados e Serviços Diferenciados, serão utilizadas. Entretanto, como nenhuma delas atende a todos os requisitos para garantia de QoS fim a fim e levando-se em consideração o fato de a Internet ser uma rede heterogênea, surge a necessidade de um framework que permita a interoperabilidade das diferentes arquiteturas existentes. Neste trabalho é proposto um modelo de integração que fornece garantias de QoS fim a fim para redes que utilizam tanto Serviços Integrados como Serviços Diferenciados através do emprego de uma infra-estrutura baseada em MPLS e Serviços Diferenciados. A aplicabilidade do modelo foi testada no simulador ns2 e os resultados também são apresentados neste trabalho.
Palavras-chave: qualidade de serviço (QoS), Serviços Diferenciados, Serviços Integrados, MPLS, Engenharia de Tráfego.

Abstract

It is given credit that in the future the telecommunication and data networks will be integrated into one network alone, based on IP switching. This network will have to offer services with guaranteed QoS for the current and future applications. One of the technologies that certainly will be adopted in the core of this new network is MPLS. MPLS introduces the concept of packet switching in IP networks. MPLS also allows that Traffic Engineering be deployed, optimizing network utilization. Together with MPLS, other QoS architectures, such as Integrated Services and Differentiated Services will be used. However, as none of them takes care of all the requirements for end to end QoS, and taking in consideration the fact of the Internet being a heterogeneous network, a framework that allows the interoperability of the different existing architectures is needed. In this paper an integration model based on MPLS and Differentiated Services is presented. The applicability of this model is simulated in ns2 and the results are also presented.
Keywords: quality of service (QoS), Diff-services, Int-services, MPLS, Traffic Engineering.

1 Introdução

Atualmente, a maior parte da infra-estrutura da Internet suporta apenas o serviço *best effort*. Os pacotes são processados o mais rápido possível, todavia não existem garantias quanto ao atraso e nem mesmo quanto ao seu recebimento. Anteriormente isto não representava um problema, mas com a recente popularização da Internet e o conseqüente crescimento do tráfego, começaram a surgir demandas por serviços com qualidade garantida.

Somando-se a isto, existe o problema de muitos dos *links* da Internet já apresentarem sinais de congestionamento crônico. Assim, para resolver estes problemas, duas alternativas são propostas: o superdimensionamento da rede, usando tecnologias como DWDM (*Dense Wave-lenght Division Multiplex*) e *Gigabit Ethernet*, ou então a utilização de tecnologias de comutação (*switching*) e Engenharia de Tráfego para minimizar o congestionamento e também o atraso da rede.

A primeira solução, além de cara, não aproveitará satisfatoriamente os recursos oferecidos pela rede. Também se acredita que, sempre que houver sobra na largura de banda disponível, serão criadas novas aplicações para ocupá-la. Já a segunda alternativa, baseada em um *framework* para a plataforma IP, pretende transformar a Internet em uma rede com integração de serviços e flexibilidade para suportar as novas aplicações que estão surgindo. Tudo isto com condições de prover qualidade de serviço (QoS) para todos.

Os serviços oferecidos poderão variar desde serviços com baixo atraso e pouca variação do atraso (*jitter*), para empresas que utilizam a Internet como meio de transmissão para aplicações de tempo real, até um serviço equivalente ao *Best effort* para pessoas que simplesmente necessitem de conectividade. Além de apresentarem níveis de qualidade diferentes, estes serviços também apresentarão preços diferentes: quanto maior for a qualidade desejada, maior será o preço a ser pago.

O IETF (*Internet Engineering Task Force*) propôs diversas arquiteturas para fornecimento de QoS, dentre elas: a arquitetura de Serviços Integrados [BRA 94], utilizando RSVP [BRA 97] como protocolo de sinalização, a arquitetura de Serviços Diferenciados [BLA 98], [NIC 98], o conceito de Roteamento Baseado em Restrições [CRA 98], [JAM 2001], e mais recentemente a arquitetura MPLS [ROS 2001], [MAG 2001].

A arquitetura de Serviços Integrados [BRA 94] baseia-se na reserva de recursos da rede. Antes de se iniciar uma transmissão, são configurados caminhos, e reservados os recursos necessários. Para isto pode-se utilizar o protocolo RSVP [BRA 97], um protocolo de sinalização para configuração de caminhos e reserva de recursos.

Na arquitetura de Serviços Diferenciados [BLA 98], [NIC 98], os pacotes são marcados com diferentes valores para criar diversas classes de pacotes. Pacotes que se encontrem em classes diferentes recebem níveis de serviço diferentes.

O Roteamento Baseado em Restrições (CBR - *Constraint Based Routing*) [CRA 98], [JAM 2001] é uma forma mais sofisticada de roteamento, que consiste em encontrar rotas na rede que atendam a determinadas restrições, como largura de banda disponível e atraso, e que não levem em consideração somente o conceito de caminho mais curto (SPF – *Shortest Path First*), como nos protocolos de roteamento IGP atuais.

A arquitetura MPLS [ROS 2001], [MAG 2001] fornece um mecanismo de encaminhamento baseado em um rótulo, que os pacotes recebem quando entram em um domínio MPLS. Os procedimentos subseqüentes de classificação e encaminhamento são baseados somente nesse rótulo, agilizando o processo. MPLS também permite esquemas sofisticados de roteamento baseados na capacidade de estabelecimento de LSPs (*Label*

Switched Paths) explicitamente roteados. Esta característica é a base da Engenharia de Tráfego com MPLS [SWA 99]. Os caminhos podem ser definidos de acordo com o tipo de tráfego, ou com a situação atual de carga da rede via CBR. Isto permite que se divida a carga igualmente por todos os *links*, otimizando sua utilização e diminuindo as chances de congestionamento.

Levando-se em consideração as vantagens apresentadas pela arquitetura MPLS, podemos afirmar que essa será a tecnologia adotada pelos grandes provedores de serviço (ISPs) em um futuro próximo. Entretanto, a migração de uma rede para a arquitetura MPLS não é trivial [XIA 2000]. Por isto, acredita-se que esta migração, em um primeiro momento, será feita somente pelas empresas que se beneficiarão mais dela: os ISPs. Para as outras empresas, bastarão soluções que apresentem níveis de QoS satisfatórios, sem que seja necessário um grande gasto ou reestruturação da rede. Surge assim a necessidade de um framework que permita a interoperabilidade das diferentes arquiteturas utilizadas nas empresas, como Serviços Integrados ou Serviços Diferenciados, e nos ISPs, como MPLS, que é o objetivo principal deste trabalho.

O restante deste artigo está organizado da seguinte forma: na seção 2 são discutidas as razões para a integração de diferentes arquiteturas de QoS e são mostrados os modelos de integração em que este trabalho se baseia. Na seção 3, é apresentado o modelo proposto. Na seção 4 são apresentados os resultados iniciais de simulações do modelo proposto. Por fim, na seção 5 são apresentadas as conclusões e sugestões de trabalhos futuros.

2 Modelos de Integração existentes

A arquitetura de Serviços Integrados, apesar de fornecer um alto nível de garantia de reserva de recursos por fluxo, tem sérios problemas de escalabilidade e complexidade. Já a arquitetura de Serviços Diferenciados, por sua vez, é simples e escalável, mas apresenta deficiências no gerenciamento de recursos. Outro problema é que a arquitetura de Serviços Diferenciados foi planejada para IP, mas seria interessante aplicá-la diretamente em tecnologias de enlace como ATM e *Frame Relay*.

Tanto a arquitetura de Serviços Integrados, como a de Serviços Diferenciados, utiliza o processo de roteamento IP da camada de rede. No entanto, o processo de roteamento na camada de rede é mais lento do que a comutação na camada de enlace. Além disso, o processo de roteamento é baseado no conceito SPF (*Shortest Path First*) que não utiliza eficientemente a infra-estrutura de rede causando o surgimento de gargalos. Estes problemas podem ser resolvidos com a utilização de Engenharia de Tráfego, em conjunto com MPLS.

A observação de que nenhuma das arquiteturas atende todos os requisitos para se fornecer uma garantia de QoS fim a fim, além do fato de a Internet ser uma rede heterogênea, onde sempre haverá a necessidade de interoperação de diversas tecnologias diferentes, tem propiciado o surgimento de modelos que combinam estas arquiteturas. Todas elas agora são vistas como complementares no provisionamento de QoS fim a fim. Desta maneira, procura-se unir suas vantagens em uma única implementação, como em [FAU 2002a], [BER 2000], [XIA 99], [RAJ 99] e [LI 98].

Nas subseções a seguir serão apresentados os modelos de integração utilizados neste trabalho. O modelo de Bernet et al. [BER 2000] propõe mecanismos para a interoperação das arquiteturas de Serviços Integrados e Serviços Diferenciados. Já o modelo de Le Faucheur et al. [FAU 2001a], [FAU 2001b] propõe um modelo de integração de MPLS e Serviços Diferenciados.

2.1 O modelo de Bernet et al.

Esta proposta está detalhada em [BER 2000]. Trata-se de um modelo que combina a arquitetura de Serviços Integrados e a arquitetura de Serviços Diferenciados. Baseia-se em uma ou mais regiões que oferecem Serviços Diferenciados no meio de uma grande rede que suporta Serviços Integrados fim a fim. De modo simplificado, procura-se utilizar a arquitetura de Serviços Diferenciados nas redes centrais, chamadas redes de trânsito (ISPs), enquanto emprega-se a arquitetura de Serviços Integrados nas redes das extremidades (clientes), como pode ser observado na Figura 1.

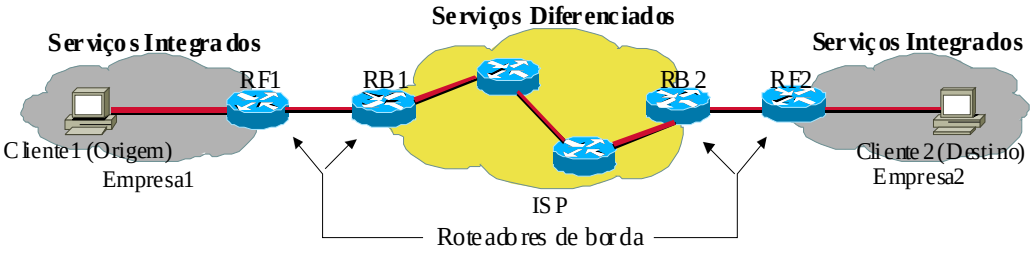

Figura 1 - O modelo de Bernet et al.

Neste modelo, os roteadores de borda entre uma região e outra desempenham papel fundamental, pois são eles os responsáveis pelo mapeamento das capacidades entre as diferentes regiões. Dentre os vários aspectos deste mapeamento, pode-se destacar: a escolha de um PHB para os fluxos, e a realização do controle de admissão, de acordo com os recursos disponíveis nas regiões de Serviços Diferenciados [BER 2000].

Exatamente como essas funções serão realizadas depende da forma como os recursos são gerenciados dentro das redes de Serviços Diferenciados. [BER 2000] sugere três formas de se fazer este gerenciamento: estaticamente; dinamicamente, utilizando RSVP, ou dinamicamente utilizando outros meios, como um negociador (*broker*) de banda.

O conceito principal é de que as aplicações usem o protocolo RSVP para requisitar a admissão de seus fluxos na rede. Se a requisição for aceita, significa que existem recursos disponíveis nas redes de Serviços Integrados, bem como que os serviços requisitados foram mapeados em uma classe de serviços compatível dentro da rede de Serviços Diferenciados. Os elementos da rede de Serviços Diferenciados devem ser capazes de transportar as mensagens RSVP até a rede de Serviços Integrados na outra extremidade, de modo que a reserva de recursos possa ser feita dentro desta última também. As redes de Serviços Diferenciados podem, mas não são obrigadas, a participar do processo de sinalização fim a fim, baseado em RSVP [BER 2000]. Do ponto de vista de Serviços Integrados, as redes de Serviços Diferenciados são tratadas como *links* virtuais conectando elementos da rede de Serviços Integrados. Dentro das redes de Serviços Diferenciados, os elementos de rede implementam controle de tráfego agregado por classe. A quantidade de tráfego que será admitida nas redes de Serviços Diferenciados poderá ser controlada através de policiamento nos elementos de entrada da rede.

O modelo proposto em [BER 2000] considera dois casos específicos: no primeiro, os recursos dentro da região de Serviços Diferenciados são distribuídos estaticamente e estas regiões não possuem dispositivos aptos a processar RSVP. No segundo, os

recursos dentro das regiões de Serviços Diferenciados são alocados dinamicamente e os dispositivos dentro dessas regiões participam da sinalização RSVP.

Os roteadores de fronteira das redes de Serviços Integrados, denominados RF1 e RF2 (ver Figura 1), têm funcionalidades que variam dependendo do tipo de modelo adotado [BER 2000]. No modelo onde as regiões de Serviços Diferenciados não processam RSVP, os roteadores RF funcionam como agentes de controle de admissão das redes de Serviços Diferenciados. Eles processam as mensagens de sinalização tanto dos emissores quanto dos receptores e aplicam o controle de admissão baseado na disponibilidade de recursos dentro da rede de Serviços Diferenciados e nas políticas de alocação definidas com os clientes (SLA).

No modelo em que as regiões de Serviços Diferenciados processam RSVP, os roteadores RF aplicam o controle de admissão baseado na disponibilidade de recursos locais (Serviços Integrados) e na política de alocação definida com os clientes (SLA). Neste último caso, são os roteadores de borda das redes de Serviços Diferenciados, chamados RB, que executam o controle de admissão (ver Figura 1) [BER 2000].

Os roteadores RB, situados nas fronteiras das regiões de Serviços Diferenciados, também possuem funcionalidades que variam de acordo com o modelo adotado para a rede. Se as regiões de Serviços Diferenciados não são capazes de processar RSVP, então os roteadores RB agem como roteadores de Serviços Diferenciados puros, ou seja, eles apenas policiam o tráfego baseado no nível de serviço especificado no campo DS e no SLA negociado com o cliente. No entanto, se as regiões de Serviços Diferenciados são capazes de processar RSVP, os roteadores RB participam da sinalização RSVP e atuam como agentes de controle de admissão para as regiões de Serviços Diferenciados [BER 2000].

Cada roteador de fronteira, RF, na rede de Serviços Integrados do cliente deve ser composto de duas partes: uma parte Serviços Integrados, que interage com a rede do cliente, e uma parte Serviços Diferenciados, que, por sua vez, interage com a rede de Serviços Diferenciados. A parte Serviços Integrados está apta a identificar e processar o tráfego de acordo com forma padrão de Serviços Integrados, ou seja, por fluxo.

Já a parte Serviços Diferenciados do roteador de fronteira pode ser considerada como um determinado número de *links* virtuais, um para cada classe de serviço negociada no SLA [BER 2000]. O roteador deve manter uma tabela que indica os recursos a serem disponibilizados para cada classe de serviço, de acordo com o SLA firmado. Esta tabela em conjunto com o campo DS é utilizada para realizar o controle de admissão no fluxo que irá atravessar a rede de Serviços Diferenciados.

Existem várias possibilidades de se agregar (mapear) fluxos de Serviços Integrados para classes de Serviços Diferenciados. Um exemplo é sugerido em [WRO 2001], e pode ser visto na Tabela 1.

Tabela 1 - Mapeamento de Serviços Integrados em Serviços Diferenciados

Serviços Integrados	Serviços Diferenciados
Best effort	*Best effort*
Carga controlada	*Assured Forwarding* (AF)
Garantido	*Expedited Forwarding* (EF)

2.2 O modelo de Le Faucheur et al.

Esta proposta, detalhada em [FAU 2001a], [FAU 2001b], define uma solução flexível para suportar Serviços Diferenciados em redes que utilizam MPLS. Ela permite que o administrador da rede MPLS selecione como os fluxos agregados de Serviços Diferenciados (BA – *Behavior Aggregates*) sejam mapeados em LSPs de maneira que seja possível atingir os objetivos de diferenciação de serviços, Engenharia de Tráfego e proteção da rede.

Uma das principais características deste modelo é que ele permite que o administrador da rede decida se conjuntos diferentes de BAs serão mapeados no mesmo LSP ou em LSPs separados. Para que isso seja possível [FAU 2001a] propõe a utilização de dois tipos de LSP: E-LSPs (*EXP-Inferred-PSC LSPs*) e L-LSPs (*Label-Only-Inferred-PSC LSPs*).

Os E-LSPs são LSPs que podem ser utilizados para transportar um ou mais Agregados Ordenados (OA – *Ordered Aggregate*, conjunto de BAs que compartilham uma restrição de ordenação [GRO 2001]). Estes LSPs podem transportar até 8 BAs de uma determinada FEC. Nestes LSPs o campo EXP do *Shim Header* MPLS (por isso o nome E-LSP) é utilizado para indicar aos LSR qual o PHB a ser aplicado a um pacote. Isto inclui tanto o PSC (*PHB Scheduling Class*, o conjunto de um ou mais PHBs que são aplicados aos BAs [GRO 2001]), como a precedência de descarte. O mapeamento do valor do campo EXP para o PHB a ser aplicado em um LSP é explicitamente sinalizado durante a distribuição dos rótulos ou então é pré-configurado. Para dois ou mais E-LSPs serem agregados eles devem obrigatoriamente suportar o mesmo conjunto de BAs.

Já os L-LSPs são LSPs que transportam somente um OA. Nestes LSPs o PSC é sinalizado explicitamente durante a distribuição dos rótulos de maneira que os LSRs podem inferir exclusivamente a partir do rótulo (por isso o nome L-LSP) qual o PSC a ser aplicado a um pacote. Quando o *Shim Header* MPLS é utilizado, a precedência de descarte é codificada no campo EXP. Caso contrário, ela é codificada utilizando os mecanismos de descarte da tecnologia de enlace presente como, por exemplo, o campo CLP de ATM. Dois ou mais L-LSPs podem ser agregados somente se eles suportarem o mesmo PSC.

A Tabela 2 mostra as diferenças entre estes dois tipos de LSP.

Tabela 2 - Comparativo entre E-LSPs e L-LSPs

	E-LSP	L-LSP
Número de BAs por FEC	8	1
Significado do campo EXP	PSC e precedência de descarte	Precedência de descarte
Significado do rótulo	FEC e BAs (codificado no campo EXP)	FEC e OA (codificado no rótulo)

Para uma determinada FEC, desde que não existam restrições no nível de enlace, como a inexistência do *Shim Header*, este modelo permite qualquer combinação de E-LSPs e L-LSPs dentro de um domínio MPLS. O administrador da rede seleciona a combinação de LSPs a partir do conjunto de combinações permitidas e também seleciona como os BAs serão transportados dentro desta combinação de LSPs de maneira a alcançar os objetivos de sua rede. Para uma determinada FEC pode existir

mais de um LSP transportando o mesmo OA, por exemplo, para fins de balanceamento de carga do OA. Entretanto, de maneira a respeitar as restrições de ordenação, todos os pacotes de um mesmo fluxo, possivelmente compreendendo múltiplos BAs de um OA devem obrigatoriamente ser transportados pelo mesmo LSP. Da mesma maneira, cada LSP deve ser capaz de suportar todos os BAs ativos de um determinado OA.

Como os OAs de uma dada FEC podem ser transportados em diferentes LSPs a decisão com relação à comutação de um pacote nos LSRs que suportem Serviços Diferenciados depende do BA do pacote [FAU 2001]. Além disso, como o campo DS do pacote IP pode não estar acessível ao LSR, devido à utilização de IPSec, por exemplo, a maneira de determinar o PHB a ser aplicado em um pacote e a maneira de codificar o PHB em um pacote transmitido são diferentes das de um roteador que suporte somente Serviços Diferenciados.

Assim, para descrever o processo de comutação dos LSRs que suportam Serviços Diferenciados [FAU 2001] divide-o em 4 estágios (ver Figura 2):

- Determinação do PHB de entrada;
- Determinação do PHB de saída, opcionalmente com Conformação de Tráfego;
- Inserção/troca do rótulo;
- Codificação das informações de Serviço Diferenciados no protocolo de enlace (Campo EXP, CLP e etc.).

Para cumprir a diferenciação dos serviços o LSR também deve aplicar o PHB correspondente ao PHB de saída selecionado.

A primeira fase, Determinação do PHB de entrada, procura determinar a qual BA o pacote recebido pertence. Este processo pode tanto considerar uma pilha de rótulos, para o caso de estar sendo utilizado um túnel, somente o rótulo, as informações encapsuladas no protocolo de enlace, o tipo de LSP, ou ainda o cabeçalho IP do pacote.

A segunda fase, Determinação do PHB de saída, é opcional e pode ser utilizada em um LSR para executar a conformação do tráfego. É importante notar que o PHB escolhido nesta fase, que será aplicado ao pacote e transmitido para o LSR à jusante, pode ser diferente do PHB que foi associado a este pacote pelo LSR à montante (o PHB de entrada). Quando o estágio de conformação não está presente o PHB de saída é igual ao PHB de entrada.

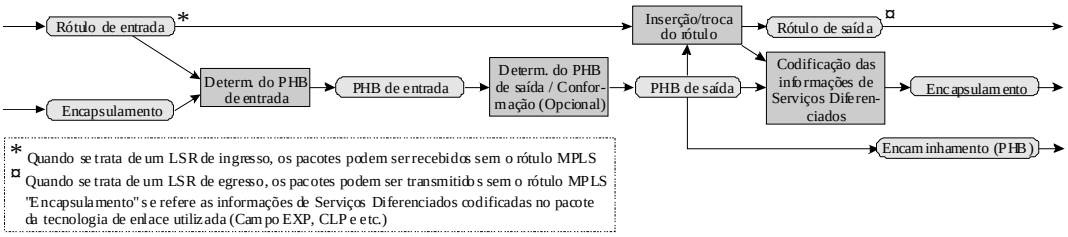

Figura 2 - Modelo de comutação

A terceira fase, Inserção/troca do rótulo, é definida em [ROS 2001]. A troca dos rótulos é efetuada pelos LSRs nos pacotes que são recebidos utilizando-se um Mapeamento de rótulo de entrada (ILM – *Incoming Label Map*), onde cada rótulo é mapeado em uma ou mais Entrada de próximo nó via comutação de rótulo (NHLFE - *Next Hop Label Forwarding Entry*). [ROS 2001] também define como um rótulo é escolhido por um LSR para um pacote recebido sem o rótulo utilizando-se um

Mapeamento de FEC em NHLFE (FTN – *FEC to NHLFE Map*) onde cada FEC é mapeada em um ou mais NHLFEs.

O contexto de Serviços Diferenciados em um rótulo é composto por:

- Tipo do LSP (E-LSP ou L-LSP);
- PHBs suportados;
- Mapeamento do "Encapsulamento" em PHB para um rótulo de entrada;
- Conjunto de mapeamentos de PHB em "Encapsulamento" para um rótulo de saída.

[FAU 2001] define que o contexto de Serviços Diferenciados é armazenado no ILM para cada rótulo de entrada e na NHLFE para cada rótulo de saída (troca ou remoção). Estas informações são inseridas no ILM e no FTN durante o processo de sinalização de rótulos. Se durante o mapeamento através do ILM, ou do FTN, mais de uma NHLFE for válida, deve-se escolher somente uma delas.

Por fim, a quarta fase efetua a codificação das informações de Serviços Diferenciados no pacote do nível de enlace utilizando campos como EXP de MPLS e CLP de ATM.

Para que seja possível estabelecer LSPs com suporte a Serviços Diferenciados nas redes MPLS são necessárias modificações em diversos protocolos existentes. [FAU 2001b] propõe as mudanças necessárias em CR-LDP e RSVP-TE para que estes suportem Engenharia de Tráfego levando em consideração Serviços Diferenciados. Além destas também são propostas alterações [FAU 2001d] e [FAU 2001e] para, respectivamente, os protocolos OSPF [MOY 98] e ISIS [ORA 90] com os mesmos objetivos.

3 Modelo Proposto

O modelo proposto neste trabalho indica mecanismos simples para que um domínio MPLS forneça garantias de serviço fim a fim para as redes (clientes) vizinhas, que podem estar utilizando as arquiteturas de Serviços Integrados, Serviços Diferenciados, ou mesmo nenhuma arquitetura para fornecimento de QoS. Este modelo é baseado principalmente em [FAU 2001a], com relação ao núcleo da rede, e [BER 2000], com relação ao mapeamento de dos serviços das redes clientes nas classes de tráfego que serão comutadas na infra-estrutura MPLS. Este modelo está sendo proposto pois se acredita que os ISPs adotarão, em um futuro próximo, a arquitetura MPLS em razão das vantagens relacionadas à Engenharia de Tráfego. E que, ligados aos ISPs, estarão redes de clientes com arquiteturas diferentes para fornecimento de QoS. Assim, é preciso um modelo capaz de integrar todas estas tecnologias.

Como MPLS é uma tecnologia destinada ao núcleo das redes existentes, uma das suas principais características é a escalabilidade, que é atingida com a agregação de fluxos com garantias de serviço fim a fim, sem a necessidade de controle individual dos fluxos em cada segmento de seu caminho. Assim, os mecanismos de Serviços Diferenciados tornam-se muito interessantes para fornecer QoS dentro de domínios MPLS pois seus serviços são baseados em um modelo *per-hop* e em recursos, como espaço em *buffer* e largura de banda, que são pré-alocados nos LSRs para cada serviço. Funções como classificação, marcação e policiamento são utilizadas somente nas bordas da rede enquanto os LSRs do núcleo precisam somente de classificadores, mantendo sua simplicidade e escalabilidade.

A Figura 3 mostra um exemplo de rede que utiliza o modelo proposto: no núcleo da rede existem somente LSRs MPLS, que também farão o papel de roteadores de núcleo de Serviços Diferenciados como em [FAU 2001a]. Nas bordas da rede estão os LSRs que também se comportarão como roteadores de borda de Serviços Diferenciados, e que, além disto, efetuarão o mapeamento dos serviços das redes clientes em serviços do modelo proposto. Ligadas aos LSRs de borda se encontram diversas redes clientes.

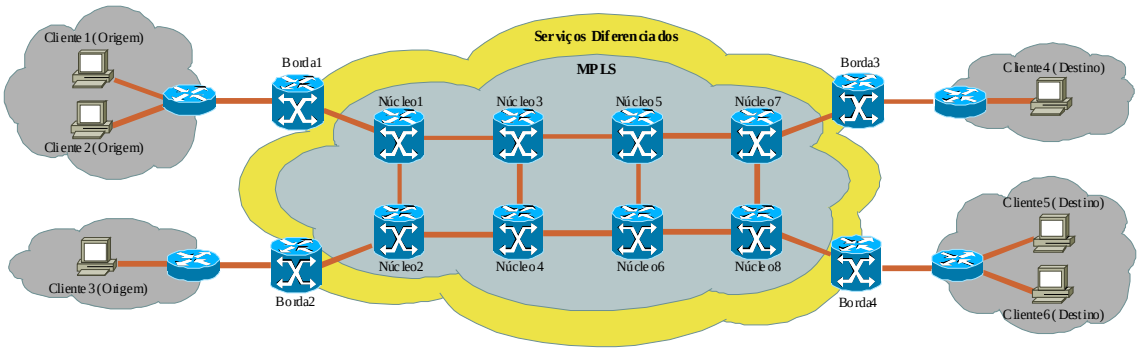

Figura 3 - Exemplo do modelo proposto

3.1 Funcionamento

Tanto os LSRs de borda como os LSR de núcleo incluem funções de roteamento baseado em restrições e estabelecimento de CR-LSPs, controle de admissão e mecanismos de escalonamento. Além disso, os LSRs de ingresso são responsáveis pela classificação, policiamento, conformação, controle de admissão e mapeamento de serviços das redes vizinhas em serviços do modelo proposto.

No núcleo MPLS existirão dois tipos de LSP: no primeiro, o E-LSP, será possível que a banda configurada seja compartilhada por diversos agregados (BA - *Behavior Aggregates*) cujas necessidades de QoS sejam parecidas. Para diferenciar cada um dos agregados, será utilizado o campo EXP, do *Shim Header*, que conterá o DSCP e a precedência de descarte. Quando o núcleo da rede for baseado em uma tecnologia de enlace que dispense a utilização do *Shim Header*, outros mapeamentos são utilizados. Este tipo de LSP permitirá uma maior agregação de fluxos, resultando em um número menor de LSPs configurados, e conseqüentemente, facilitando a Engenharia de Tráfego. O segundo tipo de LSP, o L-LSP, transportará apenas um agregado, cujas necessidades de QoS sejam rígidas, neste caso infere-se seu DSCP através do rótulo dos pacotes. Separando-o em um LSP exclusivo, aumentamos seu isolamento, e podemos garantir um QoS bastante estrito. A divisão dos LSPs em dois tipos também facilita a Engenharia de Tráfego, pois permite ao administrador da rede saber exatamente que tipo de agregado está passando por que trecho da rede em um determinado momento.

O roteamento dos pacotes dentro do domínio MPLS será feito baseando-se no rótulo MPLS do pacote e o tratamento, ou PSC (*PHB Scheduling Class*), aplicado por cada LSR aos pacotes será baseado no DSCP e na precedência de descarte, ambos codificados no campo EXP (E-LSPs) ou no rótulo (L-LSPs).

3.2 Sinalização e mapeamento de serviços

Um cliente que deseje utilizar os serviços do domínio MPLS precisa, antes de tudo, estabelecer um SLA com este. O SLA pode ser estático ou dinâmico. Para minimizar o tempo de estabelecimento dos LSPs a gerência da rede do ISP pode alocar estaticamente os recursos e configurar os LSPs baseando-se nas necessidades do cliente.

Para a sinalização entre as redes periféricas e o domínio MPLS pode ser utilizado RSVP, permitindo que sejam estabelecidos relacionamentos PHB→FEC, e talvez o estabelecimento de um novo LSP, dinamicamente (SLAs dinâmicos). Dentro do núcleo MPLS o protocolo de sinalização é o LDP [AND 2001], e sua extensão para roteamento baseado em restrições, o CR-LDP [JAM 2001]. O controle de admissão será efetuado pelos LSRs de borda, baseando-se nas informações providas pelo próprio núcleo MPLS.

Para suportar a diferenciação de serviços o modelo proposto indica as seguintes classes de tráfego, baseadas em [HEI 99]:

- Classe ouro: serviço com baixo atraso, baixo *jitter* e poucas perdas, para fluxos sensíveis ao atraso. Nesta classe, pacotes que excedam a taxa máxima de envio configurada no SLA são descartados;
- Classes prata e bronze: serviços destinados para fluxos sensíveis ao *throughput*. Pacotes pertencentes à classe prata têm maior prioridade do que os pacotes da classe bronze. Dentro de cada classe existem ainda dois níveis de precedência de descarte. Nestas classes, pacotes que excedam a taxa máxima de envio configurada no SLA podem ser descartados ou marcados com uma precedência de descarte mais alta;
- Classe *best effort*: serviço sem garantia nenhuma da rede.

Tabela 3 - Mapeamento de serviços

Serviços Integrados	Serviços Diferenciados	Modelo proposto	Campo EXP
Garantido (GS)	*Expedited Forwarding* (EF)	Classe ouro	111
Carga controlada (CL)	*Assured Forwarding* (AF)		
	AFx1	Classe prata	110/011*
	AFx2	Classe bronze	101/010*
	AFx3		100/001*
Best effort	*Best effort*	*Best effort*	000

O mapeamento dos serviços das redes cliente, visto na Tabela 3, será efetuado nos LSRs de borda, em conjunto com as suas funções normais, como classificação, conformação e etc.

Os valores do campo EXP presentes na Tabela 3 indicam além da classe de serviço a precedência de descarte: baixa, para pacotes dentro do perfil configurado (primeiro valor) e alta, para pacotes fora do perfil configurado (segundo valor)

No caso de a rede ligada ao ISP não contar com nenhum mecanismo de QoS, a classificação, marcação, policiamento e conformação, além do mapeamento, serão efetuados pelos LSRs de borda do ISP de acordo com o SLA estabelecido com o cliente.

Assim, chegamos a uma arquitetura de QoS fim-a-fim completa, pois estão previstos:

- Mecanismos de tratamento de tráfego: baseado no DSCP, na precedência de descarte e no rótulo MPLS;
- Mecanismos de configuração: RSVP externamente (SLAs dinâmicos) e LDP/CR-LDP internamente;

- Provisionamento: controle de admissão nos roteadores de borda e PSCs nos LSRs.

4 Simulações e Resultados

Para efetuar a validação do modelo proposto com outros modelos já existentes está sendo utilizado o simulador de redes de computadores ns2 (*Network Simulator 2*) [NS2 2002]. ns2 é um simulador orientado a eventos, desenvolvido pela Universidade da Califórnia. Sua capacidade de extensão torna-o bastante dinâmico, com versões modificadas sendo disponibilizadas quase que diariamente. Seu *engine* de simulação é escrito em C++, e os usuários utilizam oTcl, uma versão orientada a objetos de Tcl, como interface de configuração e comando.

Para a simulação de redes MPLS e Serviços Diferenciados estão sendo utilizadas, respectivamente, as extensões [AHN 2000] e [PIE 2000] do ns2. [AHN 2000] implementa comutação de pacotes e manipulação de mensagens dos protocolos LDP/CR-LDP. A Figura 4 mostra a arquitetura de um nó MPLS. O classificador MPLS separa os pacotes recebidos em pacotes rotulados e não rotulados. Os pacotes não rotulados recebem tratamento convencional, sendo repassados ao classificador de endereços. Já os pacotes rotulados têm seu rótulo trocado e são enviados para o próximo nó diretamente, pelo próprio classificador MPLS. Para gerenciar as informações relacionadas aos LSPs, cada nó MPLS conta com 3 tabelas: a tabela parcial de encaminhamento (PFT), a base de informações de rótulo (LIB) e a base de informações de rotas explícitas (ERB).

A extensão de Serviços Diferenciados do ns2 [PIE 2000], implementa os serviços AF (*Assured Forwarding*) somente. Para isto conta com uma estrutura de filas consistindo de 4 filas reais, cada uma contendo 3 filas RED [FLO 93] virtuais, que são os níveis de precedência. Cada fila real corresponde a uma classe de tráfego, e cada combinação de fila e nível de precedência é associada a um codepoint ou precedência de descarte. Existe também uma tabela contendo os mapeamentos de codepoints em PHBs e tabelas com as configurações de policiamento e marcação. Os roteadores de borda fazem marcação, conformação e policiamento dos fluxos, enquanto os roteadores do núcleo efetuam priorização.

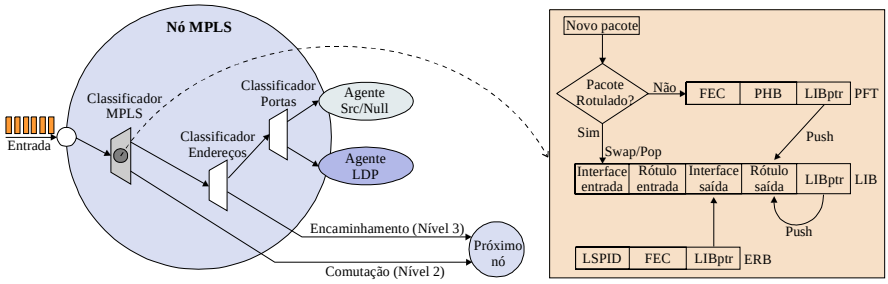

Figura 4 - Arquitetura de um nó MPLS

4.1 Descrição da simulação

Para que as extensões funcionassem corretamente em conjunto alguns ajustes nos *scripts* de simulação foram necessários. A topologia utilizada nos testes é igual à mostrada na Figura 3, e consiste no seguinte: o núcleo da rede é composto por 8 LSRs MPLS ligados através de *links* de 1Mb/s. Estes *links* tem velocidade propositalmente baixa para facilitar a sua saturação. Nos pontos de acesso ao núcleo estão LSRs, que fazem o policiamento e a conformação do tráfego. Desta maneira, um pacote, ao passar pelos LSRs da borda, é policiado e marcado com um DSCP, classificado em uma FEC e comutado, partindo então para o núcleo MPLS da rede. Nos testes atuais, estão sendo utilizados LSPs explicítamente roteados para cada agregado, escalonadores WRR para as filas dos serviços Prata e Bronze, que são gerenciadas por RIO [CLA 98], e conformadores *Token Bucket* nos nós de borda. Estão sendo considerados apenas clientes que utilizam os serviços *Best effort* e *Assured Forwarding* (AF) de Serviços Diferenciados conectados ao ISP.

Os fluxos que trafegam pela rede podem ser vistos na Tabela 4. Deseja-se que o fluxo FTP1 tenha maior prioridade do que os fluxos CBR1 e CBR2, por isto ele está sendo mapeado para a classe de tráfego Prata, enquanto os outros fluxos são mapeados para a classe Bronze.

Tabela 4 - Fluxos

Fluxo	Tipo	Origem	Destino	Taxa de envio	CIR	CBS	Classe
FTP1	FTP/TCP	Cliente1	Cliente5	--	800Kb/s	10Kb	Prata
CBR1	CBR/UDP	Cliente2	Cliente6	200Kb/s	200Kb/s	10Kb	Bronze
CBR2	CBR/UDP	Cliente3	Cliente4	700Kb/s	300Kb/s	10Kb	Bronze

Os LSRs de borda remarcam todos os pacotes em excesso, marcando-os com uma precedência de descarte maior do que a de sua classe original. Desta forma, em caso de congestionamento, serão descartados primeiro os pacotes em excesso que entraram na rede.

O objetivo principal da simulação é mostrar que a infra-estrutura MPLS melhora em termos de provisionamento (largura de banda) e separação (*jitter*) dos fluxos quando se utiliza conjuntamente a ela mecanismos de Serviços Diferenciados. A sequência de eventos da simulação está na Tabela 5. No instante 5.0s o modelo proposto é colocado à prova. Os LSPs que transportam os fluxos FTP1 e CBR2 são encerrados e em seus lugares são configurados dois LSPs explicitamente roteados, que passam pelo mesmo *link*. Desta maneira, o link irá saturar e os dois fluxos passam a disputar a largura de banda disponível, sendo que deve ser dada maior prioridade ao fluxo FTP1.

Tabela 5 - Eventos

Instante	Evento
0.1s até 0.5s	Inicio da transmissão de FTP1/CBR1/CBR2
5.0s	Encerra LSP – FTP1
5.0s	Encerra LSP – CBR2
5.1s	Cria LSP explícito para FTP1
5.1s	Cria LSP explícito para CBR2
9.9s	Fim da transmissão de FTP1/CBR1/CBR2

4.2 Resultados

Para efeito de comparação, duas simulações foram executadas, uma com o modelo proposto (MPLS e Serviços Diferenciados) e outra somente com MPLS. A Tabela 6 mostra um resumo dos resultados obtidos. É possível perceber que com a utilização do modelo proposto o *throughput* do fluxo FTP1 foi muito maior, uma vez que os LSRs do núcleo foram configurados para priorizá-lo. Como conseqüência, o número de descartes do fluxo CBR2, de menor prioridade e com diversos pacotes fora do perfil configurado (400Kb/s em excesso, que conseguiram entrar na rede porque o *link* só estava sendo utilizado por este fluxo), também cresceu pois ambos estavam disputando o mesmo *link*. Outro dado pertinente é nenhum pacote do fluxo CBR1 ter sido descartado. Isto se deve ao fato de que todos os seus pacotes estavam dentro do perfil configurado de 200Kb/s, assim sua precedência de descarte era mais baixa do que a de CBR2. Os gráficos a seguir permitem uma análise mais detalhada.

Tabela 6 - Resultados

	MPLS	MPLS + Serviços Diferenciados
Total de pacotes enviados	1844	2274
Descartes	3	94
Pacotes enviados		
FTP1	393	608
CBR1	157	157
CBR2	572	572
Pacotes recebidos		
FTP1	390	608
CBR1	157	157
CBR2	572	478

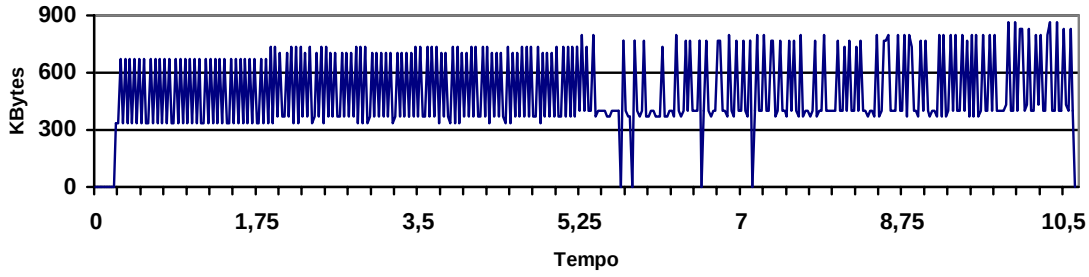

Figura 5 - Largura de banda recebida pelo fluxo CBR2 somente com a utilização de MPLS

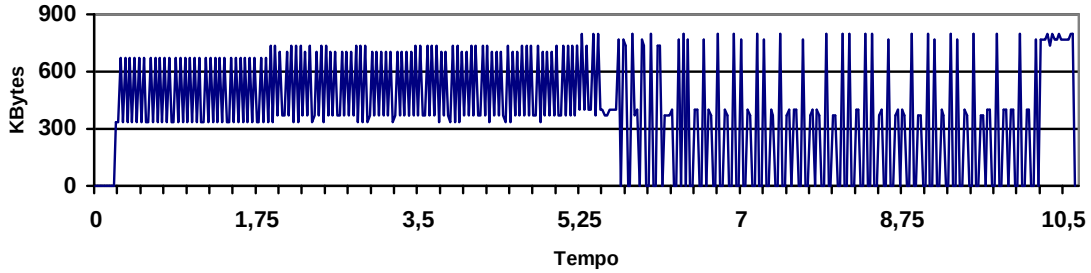

Figura 6 - Largura de banda recebida pelo fluxo CBR2 com a utilização do modelo proposto

Através da Figura 5 e da Figura 6 é possível perceber a atuação dos mecanismos de Serviços Diferenciados do modelo proposto. Quando somente a arquitetura MPLS é utilizada todos os fluxos recebem o mesmo tratamento do escalonador, além de não haver policiamento nas bordas da rede, assim CBR2 consegue manter sua taxa de ocupação da largura de banda praticamente constante, prejudicando o fluxo FTP1. Já quando são introduzidos os mecanismos de Serviços Diferenciados, os fluxos não são mais tratados igualmente. Até o instante 5,2s CBR2 tinha disponível somente para si um *link* de 1Mb/s, por isso pôde manter sua taxa de ocupação de banda. No entanto, a partir do momento em que foi forçado a dividir um *link* com o fluxo FTP1, de maior prioridade, seus pacotes passaram a ser descartados, visto que além de terem menor prioridade, sua precedência de descarte era alta, uma vez que sua taxa de envio, de 700Kb/s, era bem mais alta que o perfil configurado, de 300Kb/s.

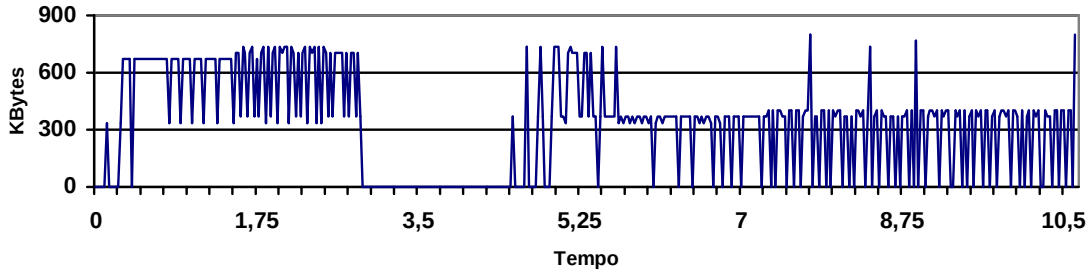

Figura 7 - Largura de banda recebida pelo fluxo FTP1 somente com a utilização de MPLS

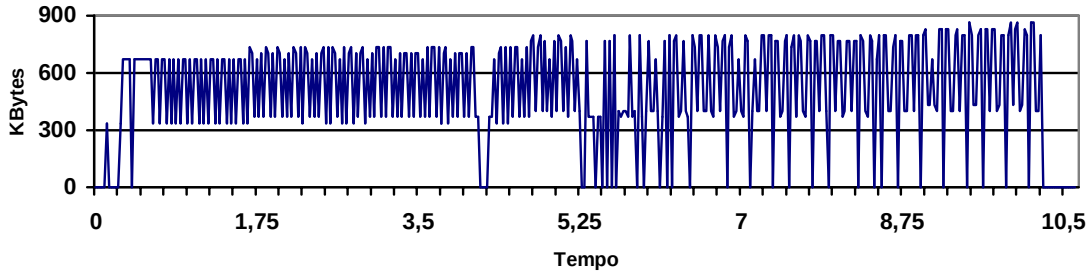

Figura 8 – Largura de banda recebida pelo fluxo FTP1 com a utilização do modelo proposto

Diferentemente do que ocorre com o fluxo CBR2, a taxa de ocupação de banda do fluxo FTP1 aumenta significativamente quando são introduzidos os mecanismos de Serviços Diferenciados do modelo proposto, como pode ser verificado nas Figuras 7 e 8. Isto ocorre porque quando se utiliza somente MPLS, o fluxo FTP1, por ser baseado em TCP, adapta sua taxa de envio à largura de banda disponível. Como o fluxo CBR2 não diminui sua taxa de envio no momento em que ambos passam a dividir o mesmo *link*, FTP1 o faz para evitar a perda de pacotes, e acaba sendo prejudicado. Em compensação, quando se utilizam os mecanismos de Serviços Diferenciados, e os pacotes de CBR2 são descartados, o fluxo FTP1 é priorizado e assim mantém constante sua taxa de ocupação de banda.

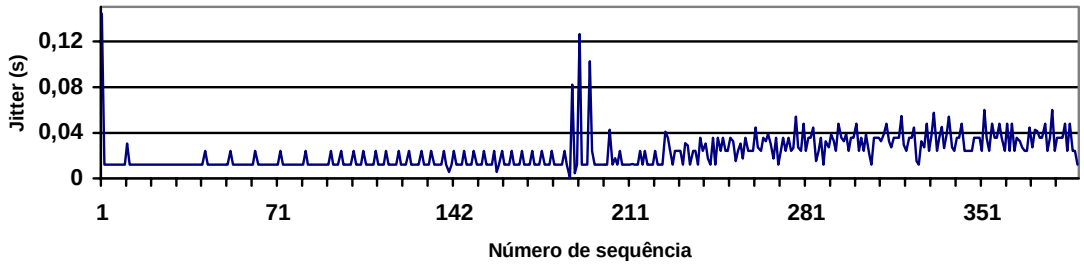

Figura 9 - Jitter medido no fluxo FTP1 com a utilização de MPLS somente

Outra melhora sensível, quando da utilização do modelo proposto, diz respeito à diminuição da interferência entre os fluxos que trafegam pela rede. Quando os fluxos FTP1 e CBR2 passam a dividir o mesmo *link* na rede que conta com MPLS somente, CBR2 interfere consideravelmente na transmissão de FTP1, como pode ser visto na Figura 9. O *jitter* medido aumenta a partir do momento em que FTP1 e CBR2 passam a dividir o mesmo *link*. Já quando se utiliza o modelo proposto, o isolamento entre os fluxos é maior, como indicado pelo gráfico da Figura 10. Apesar de ainda ocorrer um pequeno aumento do *jitter*, este continua constante e previsível, ao contrário do que ocorre no gráfico da Figura 9.

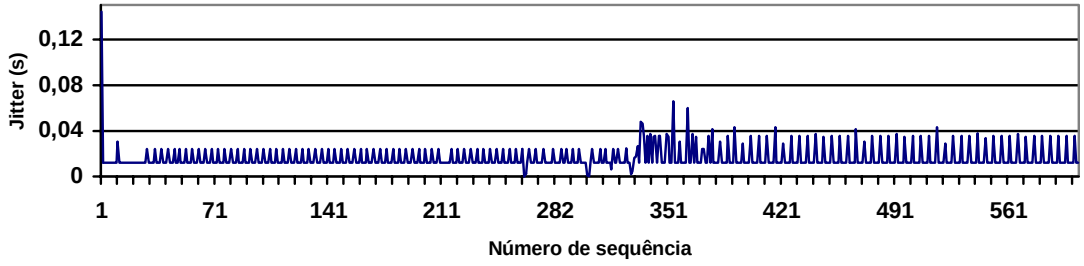

Figura 10 - Jitter medido no fluxo FTP1 com a utilização do modelo proposto

5 Conclusão

Este trabalho apresentou um modelo de integração de tecnologias de QoS que permite que redes periféricas baseadas em Serviços Diferenciados e Serviços Integrados, utilizem os serviços de um backbone baseado em MPLS para comutação e Serviços Diferenciados para priorização dos pacotes. Assim, no backbone combina-se a escalabilidade e a simplicidade de Serviços Diferenciados, com a velocidade de MPLS e a agregação/separação dos fluxos em LSPs facilita a Engenharia de Tráfego, pois permite que o administrador saiba exatamente o que está passando por onde em sua rede. Adicionalmente, pode-se utilizar CBR de forma a encontrar as melhores rotas no núcleo da rede levando em consideração as restrições de QoS e Engenharia de Tráfego.

Para avaliar a funcionalidade do modelo proposto, foi utilizado o simulador de redes ns2 e os resultados obtidos atestam a aplicabilidade do modelo. Ocorreram melhoras com relação à priorização e ao isolamento dos fluxos. Futuramente serão testados outros tipos de escalonadores e políticas de filas, outros tipos de LSPs, tanto com relação à configuração, como ao tipo de fluxo, além de outros tipos de fontes de tráfego.

Outras possibilidades para estudo futuro incluem um agente para ns2 que efetue o mapeamento de Serviços Integrados para os serviços do modelo proposto nos roteadores de borda, modificações no modelo proposto para suportar operações *multicast* e diretrizes de como dividir eficientemente o tráfego entre E-LSPs e L-LSPs através de Engenharia de Tráfego em um contexto complexo, como o de um ISP.

6 Bibliografia

[AHN 2000] AHN, G.; CHUN W. **Design and Implementation of MPLS Network Simulator supporting LDP and CR-LDP**. IEEE International Conference on Networks (ICON2000), IEEE, 2000.

[AND 2001] ANDERSSON, L. et al. **LDP Specification**. IETF RFC 3036, IETF, 2001.

[ARM 2000] ARMITAGE, G. **Quality of Service in IP Networks**. Macmillan Technical Publishing MTP, Indianapolis, 2000.

[BER 2000] BERNET, Y. et al. **A Framework for Integrated Services Operation over Diffserv Networks**. IETF RFC 2998. IETF, 2000.

[BLA 98] BLAKE, S.; BLACK, D.; CARLSON, M.; DAVIES, E.; WANG, Z.; WEISS, W. **An Architecture for Differentiated Services**, IETF RFC 2475, IETF, 1998.

[BRA 94] BRADEN, R.; et. al. **Integrated Services in the Internet Architecture: an Overview**. IETF RFC 1633, IETF, 1994.

[BRA 97] BRADEN, R.; et. al. **Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification**. IETF RFC 2205, IETF, 1997.

[CLA 98] CLARK, D.; FANG, W. **Explicit Allocation of Best Effort Packet Delivery Service**. IEEE/ACM Transactions on Networking, IEEE, 1998.

[CRA 98] CRAWLEY, E. et al. **A Framework for QoS-based Routing in the Internet**. IETF RFC2386, IETF, 1998.

[FAU 2001a] LE FAUCHEUR, F.; WU, L.; DAVIE, B.; DAVARI, S.; VAANANEN P.; KRISHNAN, R.; CHEVAL, P. **MPLS Support of Differentiated Services**. IETF Internet Draft, IETF, 2001.

[FAU 2001b] LE FAUCHEUR, F.; CHIU, A.; TOWNSEND, W.; SKALECKI D. **Extensions to RSVP-TE and CR-LDP for support of Diff-Serv-aware MPLS Traffic Engineering**. IETF Internet Draft, IETF, 2001.

[FLO 93] FLOYD, S.; JACOBSEN V. **Random Early Detection Gateways for Congestion Avoidance**. IEEE/ACM Transactions on Networking, IEEE, 1993.

[GRO 2001] GROSSMAN, D. **New Terminology and Clarifications for Diffserv**. IETF Internet Draft, IETF, 2001.

[JAM 2001] JAMOUSSI B. (Editor). **Constraint-Based LSP Setup using LDP**. IETF Internet Draft, IETF, 2001.

[LI 98] LI, T. e REKHTER, Y. **Provider Architecture for Differentiated Services and Traffic Enginnering (PASTE)**. IETF RFC 2430, IETF, 1998.

[MAG 2001] MAGALHÃES, M.; CARDOZO, E. **Introdução à Comutação IP por Rótulos Através de MPLS**. Minicurso - Anais do Simpósio Brasileiro de Redes de Computadores, SBC, 2001.

[MOY 98] MOY, J. **OSPF Version 2**. IETF RFC 2328, IETF, 1998.

[NIC 98] NICHOLS, K.; BLAKE, S.; BAKER, F.; BLACK, D. **Definition of the Differentiated Services Field (DS field) in the IPv4 and IPv6 Headers**. IETF RFC 2474, IETF, 1998.

[NS2 2002] **The Network Simulator ns-2**, http://www.isi.edu/nsnam/ns/index.html, 2002.

[ORA 90] ORAN, D., Editor, **OSI IS-IS Intra-domain Routing Protocol**, IETF RFC 1142, IETF, 1990.

[PIE 2000] PIEDA, P. et al. **A Network Simulator Differentiated Services Implementation**. *Technical Report*, Open IP – Nortel Networks, 2000.

[RAJ 99] RAJAN, R. et al. **A Policy Framework for Integrated and Differentiated Services in the Internet**. IEEE Network, IEEE, 1999.

[ROS 2001] ROSEN E.; VISWANATHAN A.; CALLON R. **Multiprotocol Label Switching Architecture**. IETF RFC 3031, IETF, 2001.

[SWA 99] SWALLOW, G. **MPLS Advantages for Traffic Engineering**. IEEE Communications Magazine, IEEE, 1999.

[WRO 2001] WROCLAWSKI, J.; CHARNY, A. **Integrated Service Mappings for Differentiated Services Networks**. IETF Internet Draft, IETF, 2001.

[XIA 99] XIAO, X.; NI, L. **Internet Qos: A Big Picture**. IEEE Network, IEEE, 1999.

[XIA 2000] XIAO, X.; HANNAN, A.; et. al. **Traffic Engineering with MPLS in the Internet**. IEEE Network, IEEE, 2000.

Anexo 2 Script de simulação da rede MPLS

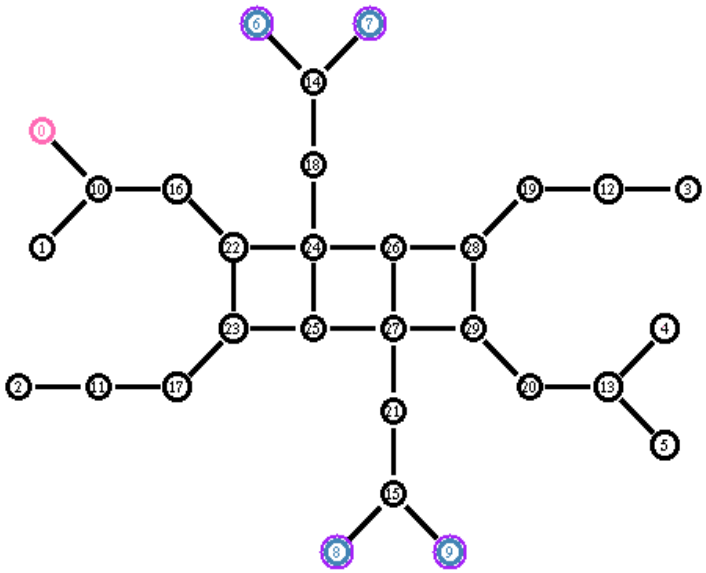

FIGURA 1 - Topologia resultante da execução do script de simulação de uma rede MPLS

```
#Cria uma instancia do simulador
set ns [new Simulator]

#Seed aleatoria para cada execucao
global defaultRNG
$defaultRNG seed 0

#Constantes

#Largura de banda e atraso dos links
set largbandaisp 1Mb
set largbandacli 2Mb
set atraso 2ms

#Tamanho dos pacotes e taxa de envio
set tampacotevoz 66
set taxavoz 16500
set duracvoz 180ms
set inatvoz 20ms
set tampacoteftp 1500
set tampacotehttp 1500
set tampaginahttp 40000
set intervaloreq 0.2

#Cores dos fluxos
$ns color 1 Red
$ns color 2 Green
$ns color 3 Blue

#Abre os arquivos de trace
set nf [open final-mpls.nam w]
set tr [open final-mpls.tr w]
$ns namtrace-all $nf
$ns trace-all $tr

#Funcoes
```

```
proc finaliza {} {

        global ns nf tr

        $ns flush-trace
        #Fecha o arquivo de trace
        close $nf
        close $tr
        #Executa o nam utilizando o arquivo de trace
        exec nam final-mpls.nam &
        exit 0
}

proc trafego-cbr-exponencial { origem destino tampac rajada inativo taxa } {

        global ns

        #Fluxos vermelhos
        set udp [new Agent/UDP]
        $udp set class_ 1
        $udp set packetSize_ $tampac
        $ns attach-agent $origem $udp

        set trafego [new Application/Traffic/Exponential]
        $trafego set packetSize_ $tampac
        $trafego set burst_time_ $rajada
        $trafego set idle_time_ $inativo
        $trafego set rate_ $taxa
        $trafego attach-agent $udp

        set destvoz [new Agent/Null]
        $ns attach-agent $destino $destvoz

        $ns connect $udp $destvoz
        return $trafego
}

proc trafego-ftp { origem destino tampac } {

        global ns

        #Fluxos verdes
        set tcp [new Agent/TCP/Reno]
        $tcp set class_ 2
        $tcp set packetSize_ $tampac
        $ns attach-agent $origem $tcp

        set trafego [new Application/FTP]
        $trafego attach-agent $tcp
        $trafego set packetSize_ $tampac

        set destftp [new Agent/TCPSink]
        $ns attach-agent $destino $destftp

        $ns connect $tcp $destftp

        return $trafego
}

proc servidor-http { no } {

        global ns pgp

        #Criacao do servidor e ligacao com o gerador de paginas
        set http [new Http/Server/Compound $ns $no]
        $http set-page-generator $pgp

        return $http
```

```
}

proc cliente-http { no intervalo } {

        global ns pgp

        set cliente [new Http/Client/Compound $ns $no]
        set tmp [new RandomVariable/Constant]
        $tmp set val_ $intervalo
        $cliente set-interval-generator $tmp
        $cliente set-page-generator $pgp

        return $cliente

}

proc iniciahttp { servidor cliente } {

        global ns

        $cliente connect $servidor
        $cliente start-session $servidor $servidor
}


proc encerrahttp { servidor cliente } {

        global ns

        $cliente stop-session $servidor
        $cliente disconnect $servidor

}

#Configuracoes de MPLS
Classifier/Addr/MPLS set control_driven_ 1
Classifier/Addr/MPLS enable-on-demand
Classifier/Addr/MPLS enable-ordered-control

#Configuracoes de TCP e HTTP
Agent/TCP/FullTcp set segsize_ 1460
Http set TRANSPORT_ FullTcp

#Imprime os traces de MPLS e LDP na saida padrao
Agent/LDP set trace_ldp_ 0
Classifier/Addr/MPLS set trace_mpls_ 0

#Gerador de paginas para os servidores HTTP
set pgp [new PagePool/CompMath]
#Tamanho da pagina
$pgp set main_size_ $tampaginahttp
#Tamanho dos objetos (gifs, p.ex.) presentes na pagina
$pgp set comp_size_ 5000
#Quantidade de objetos
$pgp set num_pages_ 3

#Tempo de validade dos objetos
set tmp [new RandomVariable/Constant]
$tmp set val_ 5
$pgp ranvar-obj-age $tmp

#Tempo de validade da pagina
set tmp [new RandomVariable/Constant]
$tmp set val_ 3
$pgp ranvar-main-age $tmp


#Cria os nos da rede da acordo com a topologia mostrada no cabecalho
```

```
#Nos dos clientes
set c1 [$ns node]
set c2 [$ns node]
set c3 [$ns node]
set c4 [$ns node]
set c5 [$ns node]
set c6 [$ns node]
set c7 [$ns node]
set c8 [$ns node]
set c9 [$ns node]
set c10 [$ns node]

#Nos de fronteira
set rf1 [$ns node]
set rf2 [$ns node]
set rf3 [$ns node]
set rf4 [$ns node]
set rf5 [$ns node]
set rf6 [$ns node]

$ns node-config -MPLS ON

#Nos MPLS de borda
set mpls1 [$ns node]
set mpls2 [$ns node]
set mpls3 [$ns node]
set mpls12 [$ns node]
set mpls13 [$ns node]
set mpls14 [$ns node]

#Nos MPLS do nucleo
set mpls4 [$ns node]
set mpls5 [$ns node]
set mpls6 [$ns node]
set mpls7 [$ns node]
set mpls8 [$ns node]
set mpls9 [$ns node]
set mpls10 [$ns node]
set mpls11 [$ns node]

$ns node-config -MPLS OFF

#Configura os links entre os nos
$ns duplex-link $c1 $rf1 $largbandacli $atraso DropTail
$ns duplex-link $c2 $rf1 $largbandacli $atraso DropTail
$ns duplex-link $rf1 $mpls1 $largbandacli $atraso DropTail
$ns duplex-link $c3 $rf2 $largbandacli $atraso DropTail
$ns duplex-link $rf2 $mpls2 $largbandacli $atraso DropTail

$ns duplex-link $mpls1 $mpls4 $largbandaisp $atraso DropTail
$ns duplex-link $mpls2 $mpls5 $largbandaisp $atraso DropTail
$ns duplex-link $mpls4 $mpls5 $largbandaisp $atraso DropTail
$ns duplex-link $mpls4 $mpls6 $largbandaisp $atraso DropTail
$ns duplex-link $mpls5 $mpls7 $largbandaisp $atraso DropTail
$ns duplex-link $mpls6 $mpls7 $largbandaisp $atraso DropTail
$ns duplex-link $mpls6 $mpls8 $largbandaisp $atraso DropTail
$ns duplex-link $mpls7 $mpls9 $largbandaisp $atraso DropTail
$ns duplex-link $mpls8 $mpls9 $largbandaisp $atraso DropTail
$ns duplex-link $mpls8 $mpls10 $largbandaisp $atraso DropTail
$ns duplex-link $mpls9 $mpls11 $largbandaisp $atraso DropTail
$ns duplex-link $mpls10 $mpls11 $largbandaisp $atraso DropTail
$ns duplex-link $mpls10 $mpls12 $largbandaisp $atraso DropTail
$ns duplex-link $mpls11 $mpls13 $largbandaisp $atraso DropTail

$ns duplex-link $mpls12 $rf3 $largbandacli $atraso DropTail
$ns duplex-link $rf3 $c4 $largbandacli $atraso DropTail
$ns duplex-link $mpls13 $rf4 $largbandacli $atraso DropTail
$ns duplex-link $rf4 $c5 $largbandacli $atraso DropTail
```

```
$ns duplex-link $rf4 $c6 $largbandacli $atraso DropTail

#Novos links
$ns duplex-link $mpls6 $mpls3 $largbandaisp $atraso DropTail
$ns duplex-link $mpls3 $rf5 $largbandacli $atraso DropTail
$ns duplex-link $rf5 $c7 $largbandaisp $atraso DropTail
$ns duplex-link $rf5 $c8 $largbandaisp $atraso DropTail

$ns duplex-link $mpls9 $mpls14 $largbandaisp $atraso DropTail
$ns duplex-link $mpls14 $rf6 $largbandacli $atraso DropTail
$ns duplex-link $rf6 $c9 $largbandaisp $atraso DropTail
$ns duplex-link $rf6 $c10 $largbandaisp $atraso DropTail

#Orienta os links para que eles fiquem organizados no NAM
$ns duplex-link-op $c1 $rf1 orient down-right
$ns duplex-link-op $c2 $rf1 orient up-right
$ns duplex-link-op $rf1 $mpls1 orient right
$ns duplex-link-op $c3 $rf2 orient right
$ns duplex-link-op $rf2 $mpls2 orient right

$ns duplex-link-op $mpls1 $mpls4 orient down-right
$ns duplex-link-op $mpls2 $mpls5 orient up-right

$ns duplex-link-op $mpls4 $mpls5 orient down
$ns duplex-link-op $mpls4 $mpls6 orient right
$ns duplex-link-op $mpls5 $mpls7 orient right

$ns duplex-link-op $mpls6 $mpls7 orient down
$ns duplex-link-op $mpls6 $mpls8 orient right
$ns duplex-link-op $mpls7 $mpls9 orient right

$ns duplex-link-op $mpls8 $mpls9 orient down
$ns duplex-link-op $mpls8 $mpls10 orient right
$ns duplex-link-op $mpls9 $mpls11 orient right

$ns duplex-link-op $mpls10 $mpls11 orient down
$ns duplex-link-op $mpls10 $mpls12 orient up-right
$ns duplex-link-op $mpls11 $mpls13 orient down-right

$ns duplex-link-op $mpls12 $rf3 orient right
$ns duplex-link-op $rf3 $c4 orient right
$ns duplex-link-op $mpls13 $rf4 orient right
$ns duplex-link-op $rf4 $c5 orient up-right
$ns duplex-link-op $rf4 $c6 orient down-right

#Novos links
$ns duplex-link-op $mpls6 $mpls3 orient up
$ns duplex-link-op $mpls3 $rf5 orient up
$ns duplex-link-op $rf5 $c7 orient up-left
$ns duplex-link-op $rf5 $c8 orient up-right

$ns duplex-link-op $mpls9 $mpls14 orient down
$ns duplex-link-op $mpls14 $rf6 orient down
$ns duplex-link-op $rf6 $c9 orient down-left
$ns duplex-link-op $rf6 $c10 orient down-right


#Configura os agentes LDP em todos os nos MPLS
for {set i 1} {$i < 15} {incr i} {
        for {set j [expr $i+1]} {$j < 15} {incr j} {
                set a mpls$i
                set b mpls$j
                eval $ns LDP-peer $$a $$b
        }
}

#Configura as cores das mensagens LDP
$ns ldp-request-color blue
```

```
$ns ldp-mapping-color orange
$ns ldp-withdraw-color magenta
$ns ldp-release-color yellow
$ns ldp-notification-color red

#Cria agentes geradores de trafego

#Fluxos de voz
set voz0 [trafego-cbr-exponencial $c2   $c6 $tampacotevoz $duracvoz $inatvoz
$taxavoz]
set voz1 [trafego-cbr-exponencial $c6   $c2 $tampacotevoz $duracvoz $inatvoz
$taxavoz]

#Fluxos FTP
set ftp0 [trafego-ftp $c3 $c4 $tampacoteftp]
set ftp1 [trafego-ftp $c7 $c5 $tampacoteftp]

#Servidores HTTP
set shttp0 [servidor-http $c1]

#Clientes HTTP
set chttp0 [cliente-http $c8 $intervaloreq]
set chttp1 [cliente-http $c9 $intervaloreq]
set chttp2 [cliente-http $c10 $intervaloreq]

#Eventos

for {set i 1} {$i < 15} {incr i} {
        set a mpls$i
        set m [eval $$a get-module "MPLS"]
        eval set mpls$i $m
}

$ns at 0.1  "$voz0 start"
$ns at 0.1  "$voz1 start"
$ns at 3.1  "$ftp0 start"
$ns at 3.1  "$ftp1 start"
$ns at 6.1  "iniciahttp $shttp0 $chttp0"
$ns at 6.1  "iniciahttp $shttp0 $chttp1"
$ns at 6.1  "iniciahttp $shttp0 $chttp2"
$ns at 22.0  "encerrahttp $shttp0 $chttp2"
$ns at 22.0  "encerrahttp $shttp0 $chttp1"
$ns at 22.0  "encerrahttp $shttp0 $chttp0"
$ns at 25.0  "$ftp1 stop"
$ns at 25.0  "$ftp0 stop"
$ns at 28.0  "$voz0 stop"
$ns at 28.0  "$voz1 stop"

$ns at 30.0 "finaliza"

#Executa a simulacao
$ns run
```

Anexo 3 Script de simulação da rede MPLS + Serviços Diferenciados

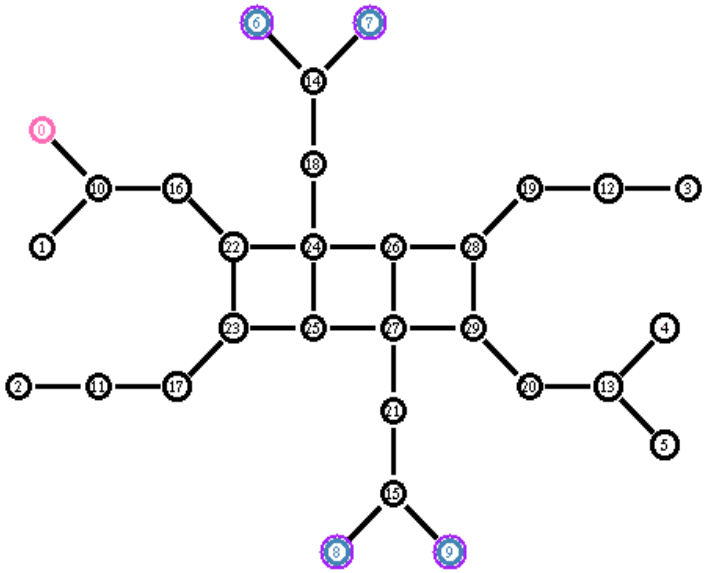

FIGURA 2 - Topologia resultante da execução do script de simulação de uma rede MPLS com Serviços Diferenciados

```
#Cria uma instancia do simulador
set ns [new Simulator]

#Seed aleatoria para cada execucao
global defaultRNG
$defaultRNG seed 0

#Constantes

#Largura de banda e atraso dos links
set largbandaisp 1Mb
set largbandacli 2Mb
set atraso 2ms

#Tamanho dos pacotes e taxa de envio
set tampacotevoz 66
set taxavoz 16500
set duracvoz 180ms
set inatvoz 20ms
set tampacoteftp 1500
set tampacotehttp 1500
set tampaginahttp 40000
set intervaloreq 0.2

#Parametros de Diffserv
set cirouro     150000
set cbsouro     0
set cirprata    400000
set cbsprata    1000
set cirbronze   350000
set cbsbronze   1000
set cirbe       100000
set cbsbe       0
```

```
#Cores dos fluxos
$ns color 1 Red
$ns color 2 Green
$ns color 3 Blue

#Abre os arquivos de trace
set nf [open final-mpls-ds.nam w]
set tr [open final-mpls-ds.tr w]
$ns namtrace-all $nf
$ns trace-all $tr

#Funcoes
proc finaliza {} {

        global ns nf tr

        $ns flush-trace
        #Fecha o arquivo de trace
        close $nf
        close $tr
        #Executa o nam utilizando o arquivo de trace
        exec nam final-mpls-ds.nam &
        exit 0
}

proc trafego-cbr-exponencial { origem destino tampac rajada inativo taxa } {

        global ns

        #Fluxos vermelhos
        set udp [new Agent/UDP]
        $udp set class_ 1
        $udp set packetSize_ $tampac
        $ns attach-agent $origem $udp

        set trafego [new Application/Traffic/Exponential]
        $trafego set packetSize_ $tampac
        $trafego set burst_time_ $rajada
        $trafego set idle_time_ $inativo
        $trafego set rate_ $taxa
        $trafego attach-agent $udp

        set destvoz [new Agent/Null]
        $ns attach-agent $destino $destvoz

        $ns connect $udp $destvoz
        return $trafego
}

proc trafego-ftp { origem destino tampac } {

        global ns

        #Fluxos verdes
        set tcp [new Agent/TCP/Reno]
        $tcp set class_ 2
        $tcp set packetSize_ $tampac
        $ns attach-agent $origem $tcp

        set trafego [new Application/FTP]
        $trafego attach-agent $tcp
        $trafego set packetSize_ $tampac

        set destftp [new Agent/TCPSink]
        $ns attach-agent $destino $destftp

        $ns connect $tcp $destftp
```

```
        return $trafego
}

proc servidor-http { no } {

        global ns pgp

        #Criacao do servidor e ligacao com o gerador de paginas
        set http [new Http/Server/Compound $ns $no]
        $http set-page-generator $pgp

        return $http
}

proc cliente-http { no intervalo } {

        global ns pgp

        set cliente [new Http/Client/Compound $ns $no]
        set tmp [new RandomVariable/Constant]
        $tmp set val_ $intervalo
        $cliente set-interval-generator $tmp
        $cliente set-page-generator $pgp

        return $cliente

}

proc iniciahttp { servidor cliente } {

        global ns

        $cliente connect $servidor
        $cliente start-session $servidor $servidor
}


proc encerrahttp { servidor cliente } {

        global ns

        $cliente stop-session $servidor
        $cliente disconnect $servidor

}

#Configura os parametros diffserv de um no de borda
proc configura-borda-edge { fila } {

        global c1 c2 c3 c4 c5 c6 c7 c8 c9 c10 cirouro cirprata cirbronze cirbe
cbsouro cbsprata cbsbronze cbsbe

        $fila setSchedularMode PRI
        $fila setMREDMode DROP 0
        $fila setMREDMode RIO-C 1
        $fila setMREDMode RIO-C 2
        $fila setMREDMode DROP 3
        $fila meanPktSize 395 #Varia entre 40 e 1500
        $fila set numQueues_ 4
        $fila setNumPrec 2
        $fila addQueueRate 0 150000
        $fila addQueueRate 1 400000
        $fila addQueueRate 2 350000
        $fila addQueueRate 3 100000

        #Pacotes LDP serao tratados como pertencentes a classe ouro
        for {set i 16} {$i < 30} {incr i} {
```

```
                for {set j [expr $i+1]} {$j < 30} {incr j} {
                        $fila addPolicyEntry $i $j TokenBucket 10 $cirouro
                        $cbsouro
                        $fila addPolicyEntry $j $i TokenBucket 10 $cirouro
                        $cbsouro
                }
        }

        $fila addPolicyEntry [$c2 id] [$c6 id] TokenBucket 10 $cirouro
        $cbsouro
        $fila addPolicyEntry [$c6 id] [$c2 id] TokenBucket 10 $cirouro
        $cbsouro
        $fila addPolicyEntry [$c3 id] [$c4 id] TokenBucket 20 $cirprata
        $cbsprata
        $fila addPolicyEntry [$c4 id] [$c3 id] TokenBucket 20 $cirprata
        $cbsprata
        $fila addPolicyEntry [$c5 id] [$c7 id] TokenBucket 20 $cirprata
        $cbsprata
        $fila addPolicyEntry [$c7 id] [$c5 id] TokenBucket 20 $cirprata
        $cbsprata
        $fila addPolicyEntry [$c1 id] [$c9 id] TokenBucket 30 $cirbronze
        $cbsbronze
        $fila addPolicyEntry [$c9 id] [$c1 id] TokenBucket 30 $cirbronze
        $cbsbronze
        $fila addPolicyEntry [$c1 id] [$c10 id] TokenBucket 30 $cirbronze
        $cbsbronze
        $fila addPolicyEntry [$c10 id] [$c1 id] TokenBucket 30 $cirbronze
        $cbsbronze
        $fila addPolicyEntry [$c1 id] [$c8 id] TokenBucket 40 $cirbe $cbsbe
        $fila addPolicyEntry [$c8 id] [$c1 id] TokenBucket 40 $cirbe $cbsbe

        $fila addPolicerEntry TokenBucket 10 11
        $fila addPolicerEntry TokenBucket 20 21
        $fila addPolicerEntry TokenBucket 30 31
        $fila addPolicerEntry TokenBucket 40 41
        #$fila addPHBEntry 0 0 0
        $fila addPHBEntry 10 0 0
        $fila addPHBEntry 11 0 1
        $fila addPHBEntry 20 1 0
        $fila addPHBEntry 21 1 1
        $fila addPHBEntry 30 2 0
        $fila addPHBEntry 31 2 1
        $fila addPHBEntry 40 3 0
        $fila addPHBEntry 41 3 1
        $fila configQ 0 0 20 40 0.02
        $fila configQ 0 1 10 20 0.10
        $fila configQ 1 0 20 40 0.02
        $fila configQ 1 1 10 20 0.10
        $fila configQ 2 0 20 40 0.02
        $fila configQ 2 1 10 20 0.10
        $fila configQ 3 0 20 40 0.02
        $fila configQ 3 1 10 20 0.10

        return $fila

}

#Configura os parametros diffserv de um no de borda
proc configura-borda-core { fila } {

        $fila setSchedularMode PRI
        $fila setMREDMode DROP 0
        $fila setMREDMode RIO-C 1
        $fila setMREDMode RIO-C 2
        $fila setMREDMode DROP 3
        $fila meanPktSize 395 #Varia entre 40 e 1500
        $fila set numQueues_ 4
        $fila setNumPrec 2
```

```
        $fila addQueueRate 0 150000
        $fila addQueueRate 1 400000
        $fila addQueueRate 2 350000
        $fila addQueueRate 3 100000
        $fila addPHBEntry 0 0 0
        $fila addPHBEntry 10 0 0
        $fila addPHBEntry 11 0 1
        $fila addPHBEntry 20 1 0
        $fila addPHBEntry 21 1 1
        $fila addPHBEntry 30 2 0
        $fila addPHBEntry 31 2 1
        $fila addPHBEntry 40 3 0
        $fila addPHBEntry 41 3 1
        $fila configQ 0 0 20 40 0.02
        $fila configQ 0 1 10 20 0.10
        $fila configQ 1 0 20 40 0.02
        $fila configQ 1 1 10 20 0.10
        $fila configQ 2 0 20 40 0.02
        $fila configQ 2 1 10 20 0.10
        $fila configQ 3 0 20 40 0.02
        $fila configQ 3 1 10 20 0.10

        return $fila

}

#Configura os parametros diffserv de um noh do nucleo
proc configura-nucleo { fila } {

        global cirouro cirprata cirbronze cirbe

        $fila setSchedularMode PRI
        $fila setMREDMode DROP 0
        $fila setMREDMode RIO-C 1
        $fila setMREDMode RIO-C 2
        $fila setMREDMode DROP 3
        $fila meanPktSize 395 #Varia entre 40 e 1500
        $fila set numQueues_ 4
        $fila setNumPrec 2
        $fila addQueueRate 0 150000
        $fila addQueueRate 1 400000
        $fila addQueueRate 2 350000
        $fila addQueueRate 3 100000
        $fila addPHBEntry 0 0 0
        $fila addPHBEntry 10 0 0
        $fila addPHBEntry 11 0 1
        $fila addPHBEntry 20 1 0
        $fila addPHBEntry 21 1 1
        $fila addPHBEntry 30 2 0
        $fila addPHBEntry 31 2 1
        $fila addPHBEntry 40 3 0
        $fila addPHBEntry 41 3 1
        $fila configQ 0 0 20 40 0.02
        $fila configQ 0 1 10 20 0.10
        $fila configQ 1 0 20 40 0.02
        $fila configQ 1 1 10 20 0.10
        $fila configQ 2 0 20 40 0.02
        $fila configQ 2 1 10 20 0.10
        $fila configQ 3 0 20 40 0.02
        $fila configQ 3 1 10 20 0.10

        return $fila

}

#Configuracoes de MPLS
Classifier/Addr/MPLS set control_driven_ 1
Classifier/Addr/MPLS enable-on-demand
```

```
Classifier/Addr/MPLS enable-ordered-control

#Configuracoes de TCP e HTTP
Agent/TCP/FullTcp set segsize_ 1460
Http set TRANSPORT_ FullTcp

#Imprime os traces de MPLS e LDP na saida padrao
Agent/LDP set trace_ldp_ 0
Classifier/Addr/MPLS set trace_mpls_ 0

#Gerador de paginas para os servidores HTTP
set pgp [new PagePool/CompMath]
#Tamanho da pagina
$pgp set main_size_ $tampaginahttp
#Tamanho dos objetos (gifs, p.ex.) presentes na pagina
$pgp set comp_size_ 5000
#Quantidade de objetos
$pgp set num_pages_ 3

#Tempo de validade dos objetos
set tmp [new RandomVariable/Constant]
$tmp set val_ 5
$pgp ranvar-obj-age $tmp

#Tempo de validade da pagina
set tmp [new RandomVariable/Constant]
$tmp set val_ 3
$pgp ranvar-main-age $tmp


#Cria os nos da rede da acordo com a topologia mostrada no cabecalho
#Nos dos clientes
set c1 [$ns node]
set c2 [$ns node]
set c3 [$ns node]
set c4 [$ns node]
set c5 [$ns node]
set c6 [$ns node]
set c7 [$ns node]
set c8 [$ns node]
set c9 [$ns node]
set c10 [$ns node]

#Nos de fronteira
set rf1 [$ns node]
set rf2 [$ns node]
set rf3 [$ns node]
set rf4 [$ns node]
set rf5 [$ns node]
set rf6 [$ns node]

$ns node-config -MPLS ON

#Nos Diffserv+MPLS de borda
set mpls1 [$ns node]
set mpls2 [$ns node]
set mpls3 [$ns node]
set mpls12 [$ns node]
set mpls13 [$ns node]
set mpls14 [$ns node]

#Nos MPLS do nucleo
set mpls4 [$ns node]
set mpls5 [$ns node]
set mpls6 [$ns node]
set mpls7 [$ns node]
set mpls8 [$ns node]
set mpls9 [$ns node]
```

```
set mpls10 [$ns node]
set mpls11 [$ns node]

$ns node-config -MPLS OFF

#Configura os links entre os nos
$ns duplex-link $c1 $rf1 $largbandacli $atraso DropTail
$ns duplex-link $c2 $rf1 $largbandacli $atraso DropTail
$ns duplex-link $rf1 $mpls1 $largbandacli $atraso DropTail
$ns duplex-link $c3 $rf2 $largbandacli $atraso DropTail
$ns duplex-link $rf2 $mpls2 $largbandacli $atraso DropTail

$ns simplex-link $mpls1 $mpls4 $largbandaisp $atraso dsRED/edge
$ns simplex-link $mpls4 $mpls1 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls2 $mpls5 $largbandaisp $atraso dsRED/edge
$ns simplex-link $mpls5 $mpls2 $largbandaisp $atraso dsRED/core

$ns simplex-link $mpls4 $mpls5 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls5 $mpls4 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls4 $mpls6 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls6 $mpls4 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls5 $mpls7 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls7 $mpls5 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls6 $mpls7 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls7 $mpls6 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls6 $mpls8 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls8 $mpls6 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls7 $mpls9 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls9 $mpls7 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls8 $mpls9 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls9 $mpls8 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls8 $mpls10 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls10 $mpls8 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls9 $mpls11 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls11 $mpls9 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls10 $mpls11 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls11 $mpls10 $largbandaisp $atraso dsRED/core

$ns simplex-link $mpls12 $mpls10 $largbandaisp $atraso dsRED/edge
$ns simplex-link $mpls10 $mpls12 $largbandaisp $atraso dsRED/core
$ns simplex-link $mpls13 $mpls11 $largbandaisp $atraso dsRED/edge
$ns simplex-link $mpls11 $mpls13 $largbandaisp $atraso dsRED/core

$ns duplex-link $mpls12 $rf3 $largbandacli $atraso DropTail
$ns duplex-link $rf3 $c4 $largbandacli $atraso DropTail
$ns duplex-link $mpls13 $rf4 $largbandacli $atraso DropTail
$ns duplex-link $rf4 $c5 $largbandacli $atraso DropTail
$ns duplex-link $rf4 $c6 $largbandacli $atraso DropTail

#Novos links
$ns simplex-link $mpls3 $mpls6 $largbandaisp $atraso dsRED/edge
$ns simplex-link $mpls6 $mpls3 $largbandaisp $atraso dsRED/core
$ns duplex-link $mpls3 $rf5 $largbandacli $atraso DropTail
$ns duplex-link $rf5 $c7 $largbandaisp $atraso DropTail
$ns duplex-link $rf5 $c8 $largbandaisp $atraso DropTail

$ns simplex-link $mpls14 $mpls9 $largbandaisp $atraso dsRED/edge
$ns simplex-link $mpls9 $mpls14 $largbandaisp $atraso dsRED/core
$ns duplex-link $mpls14 $rf6 $largbandacli $atraso DropTail
$ns duplex-link $rf6 $c9 $largbandaisp $atraso DropTail
$ns duplex-link $rf6 $c10 $largbandaisp $atraso DropTail

#Orienta os links para que eles fiquem organizados no NAM
$ns duplex-link-op $c1 $rf1 orient down-right
$ns duplex-link-op $c2 $rf1 orient up-right
$ns duplex-link-op $rf1 $mpls1 orient right
$ns duplex-link-op $c3 $rf2 orient right
$ns duplex-link-op $rf2 $mpls2 orient right
```

```
$ns duplex-link-op $mpls1 $mpls4 orient down-right
$ns duplex-link-op $mpls2 $mpls5 orient up-right

$ns duplex-link-op $mpls4 $mpls5 orient down
$ns duplex-link-op $mpls4 $mpls6 orient right
$ns duplex-link-op $mpls5 $mpls7 orient right

$ns duplex-link-op $mpls6 $mpls7 orient down
$ns duplex-link-op $mpls6 $mpls8 orient right
$ns duplex-link-op $mpls7 $mpls9 orient right

$ns duplex-link-op $mpls8 $mpls9 orient down
$ns duplex-link-op $mpls8 $mpls10 orient right
$ns duplex-link-op $mpls9 $mpls11 orient right

$ns duplex-link-op $mpls10 $mpls11 orient down
$ns duplex-link-op $mpls10 $mpls12 orient up-right
$ns duplex-link-op $mpls11 $mpls13 orient down-right

$ns duplex-link-op $mpls12 $rf3 orient right
$ns duplex-link-op $rf3 $c4 orient right
$ns duplex-link-op $mpls13 $rf4 orient right
$ns duplex-link-op $rf4 $c5 orient up-right
$ns duplex-link-op $rf4 $c6 orient down-right

#Novos links
$ns duplex-link-op $mpls6 $mpls3 orient up
$ns duplex-link-op $mpls3 $rf5 orient up
$ns duplex-link-op $rf5 $c7 orient up-left
$ns duplex-link-op $rf5 $c8 orient up-right

$ns duplex-link-op $mpls9 $mpls14 orient down
$ns duplex-link-op $mpls14 $rf6 orient down
$ns duplex-link-op $rf6 $c9 orient down-left
$ns duplex-link-op $rf6 $c10 orient down-right

#Associa as filas aos links (qXY, com link indo de mplsX ateh mplsY)
set q14 [[$ns link $mpls1 $mpls4] queue]
set q41 [[$ns link $mpls4 $mpls1] queue]
set q25 [[$ns link $mpls2 $mpls5] queue]
set q52 [[$ns link $mpls5 $mpls2] queue]
set q45 [[$ns link $mpls4 $mpls5] queue]
set q54 [[$ns link $mpls5 $mpls4] queue]
set q46 [[$ns link $mpls4 $mpls6] queue]
set q64 [[$ns link $mpls6 $mpls4] queue]
set q57 [[$ns link $mpls5 $mpls7] queue]
set q75 [[$ns link $mpls7 $mpls5] queue]
set q67 [[$ns link $mpls6 $mpls7] queue]
set q76 [[$ns link $mpls7 $mpls6] queue]
set q68 [[$ns link $mpls6 $mpls8] queue]
set q86 [[$ns link $mpls8 $mpls6] queue]
set q79 [[$ns link $mpls7 $mpls9] queue]
set q97 [[$ns link $mpls9 $mpls7] queue]
set q89 [[$ns link $mpls8 $mpls9] queue]
set q98 [[$ns link $mpls9 $mpls8] queue]
set q810 [[$ns link $mpls8 $mpls10] queue]
set q108 [[$ns link $mpls10 $mpls8] queue]
set q911 [[$ns link $mpls9 $mpls11] queue]
set q119 [[$ns link $mpls11 $mpls9] queue]
set q1011 [[$ns link $mpls10 $mpls11] queue]
set q1110 [[$ns link $mpls11 $mpls10] queue]
set q1210 [[$ns link $mpls12 $mpls10] queue]
set q1012 [[$ns link $mpls10 $mpls12] queue]
set q1311 [[$ns link $mpls13 $mpls11] queue]
set q1113 [[$ns link $mpls11 $mpls13] queue]
set q36 [[$ns link $mpls3 $mpls6] queue]
set q63 [[$ns link $mpls6 $mpls3] queue]
```

```
set q149 [[$ns link $mpls14 $mpls9] queue]
set q914 [[$ns link $mpls9 $mpls14] queue]

#Configura os parametros Diffserv de cada fila
set q14 [configura-borda-edge $q14]
set q41 [configura-borda-core $q41]
set q25 [configura-borda-edge $q25]
set q52 [configura-borda-core $q52]

set q45 [configura-nucleo $q45]
set q54 [configura-nucleo $q54]
set q46 [configura-nucleo $q46]
set q64 [configura-nucleo $q64]
set q57 [configura-nucleo $q57]
set q75 [configura-nucleo $q75]
set q67 [configura-nucleo $q67]
set q76 [configura-nucleo $q76]
set q68 [configura-nucleo $q68]
set q86 [configura-nucleo $q86]
set q79 [configura-nucleo $q79]
set q97 [configura-nucleo $q97]
set q89 [configura-nucleo $q89]
set q98 [configura-nucleo $q98]
set q810 [configura-nucleo $q810]
set q108 [configura-nucleo $q108]
set q911 [configura-nucleo $q911]
set q119 [configura-nucleo $q119]
set q1011 [configura-nucleo $q1011]
set q1110 [configura-nucleo $q1110]
set q1210 [configura-borda-edge $q1210]
set q1012 [configura-borda-core $q1012]
set q1311 [configura-borda-edge $q1311]
set q1113 [configura-borda-core $q1113]
set q36 [configura-borda-edge $q36]
set q63 [configura-borda-core $q63]
set q149 [configura-borda-edge $q149]
set q914 [configura-borda-core $q914]


#Configura os agentes LDP em todos os nos MPLS
for {set i 1} {$i < 15} {incr i} {
        for {set j [expr $i+1]} {$j < 15} {incr j} {
                set a mpls$i
                set b mpls$j
                eval $ns LDP-peer $$a $$b
        }
}

#Configura as cores das mensagens LDP
$ns ldp-request-color blue
$ns ldp-mapping-color orange
$ns ldp-withdraw-color magenta
$ns ldp-release-color yellow
$ns ldp-notification-color red

#Cria agentes geradores de trafego

#Fluxos de voz
set voz0 [trafego-cbr-exponencial $c2   $c6 $tampacotevoz $duracvoz $inatvoz
$taxavoz]
set voz1 [trafego-cbr-exponencial $c6   $c2 $tampacotevoz $duracvoz $inatvoz
$taxavoz]

#Fluxos FTP
set ftp0 [trafego-ftp $c3 $c4 $tampacoteftp]
set ftp1 [trafego-ftp $c7 $c5 $tampacoteftp]

#Servidores HTTP
```

```
set shttp0 [servidor-http $c1]

#Clientes HTTP
set chttp0 [cliente-http $c8 $intervaloreq]
set chttp1 [cliente-http $c9 $intervaloreq]
set chttp2 [cliente-http $c10 $intervaloreq]

#Eventos

for {set i 1} {$i < 15} {incr i} {
        set a mpls$i
        set m [eval $$a get-module "MPLS"]
        eval set mpls$i $m
}

$ns at 0.1  "$voz0 start"
$ns at 0.1  "$voz1 start"
$ns at 3.1  "$ftp0 start"
$ns at 3.1  "$ftp1 start"
$ns at 6.1  "iniciahttp $shttp0 $chttp0"
$ns at 6.1  "iniciahttp $shttp0 $chttp1"
$ns at 6.1  "iniciahttp $shttp0 $chttp2"
$ns at 22.0  "encerrahttp $shttp0 $chttp2"
$ns at 22.0  "encerrahttp $shttp0 $chttp1"
$ns at 22.0  "encerrahttp $shttp0 $chttp0"
$ns at 25.0  "$ftp1 stop"
$ns at 25.0  "$ftp0 stop"
$ns at 28.0  "$voz0 stop"
$ns at 28.0  "$voz1 stop"

$ns at 30.0 "finaliza"

#Executa a simulacao
$ns run
```

Bibliografia

[AHN 2001] AHN, G.; CHUN W. Design and Implementation of MPLS Network Simulator supporting LDP and CR-LDP. In: IEEE INTERNATIONAL CONFERENCE ON INFORMATION NETWORKING, ICOIN, 15., 2001, Oita-Japan. **Proceedings…** New York: IEEE Press, 2001.

[AND 2001] ANDERSSON, L. et al. **LDP Specification**. [S.l.]: IETF, Jan. 2001. (Request for Comments 3036). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[ARM 2000] ARMITAGE, G. **Quality of Service in IP Networks**. Indianapolis: Macmillan Technical Publishing MTP, 2000. 336p.

[ASH 2002a] ASH, J. et al. **Applicability Statement for CR-LDP**. [S.l.]: IETF, Jan. 2002. (Request for Comments 3213). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[ASH 2002b] ASH, J. et al. **LSP Modification using CR-LDP**. [S.l.]: IETF, Jan. 2002. (Request for Comments 3214). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[AWD 98] AWDUCHE, D. et al. **Extension to RSVP for Traffic Engineering**. [S.l.]: IETF, Aug. 1998. (Internet draft <draft-swallow-mpls-RSVP-trafeng-00.txt> work in progress). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[AWD 2001a] AWDUCHE, D. et al. **RSVP-TE: Extensions to RSVP for LSP Tunnels**. [S.l.]: IETF, Dec. 2001. (Request for Comments 3209). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[AWD 2001b] AWDUCHE, D. et al. **Applicability Statement for Extensions to RSVP for LSP-Tunnels**. [S.l.]: IETF, Dec. 2001. (Request for Comments 3210). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[BAK 95] BAKER, F. (Ed.). **Requirements for IP Version 4 routers**. [S.l.]: IETF, June 1995. (Request for Comments 1812). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[BER 2000a] BERNET, Y. et al. **A Framework for Integrated Services Operation over Diffserv Networks**. [S.l.]: IETF, Nov. 2000. (Request for Comments 2998). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[BER 2000b] BERNET, Y. et al. **Specification of the Null Service Type**. [S.l.]: IETF, Nov. 2000. (Request for Comments 2997). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[BLA 98] BLAKE, S. et al. **An Architecture for Differentiated Services.** [S.l.]: IETF, Dec. 1998. (Request for Comments 2475). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[BRA 94] BRADEN, R. et al. **Integrated Services in the Internet Architecture: an Overview**. [S.l.]: IETF, June 1994. (Request for Comments 1633). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[BRA 97] BRADEN, R. et al. **Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification**. [S.l.]: IETF, Sept. 1997. (Request for Comments 2205). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[CHU 99] CHUAH, N.; KATZ, R. **Network Provisioning and Resource Management for IP Telephony**. Berkeley: University of California, 1999. (Relatório técnico UCB/CSD-99-1061).

[CLA 98] CLARK, D.; FANG, W. Explicit Allocation of Best Effort Packet Delivery Service. **IEEE/ACM Transactions on Networking**, New York, v. 6, n. 4, p. 362-373, 1998.

[CRA 98] CRAWLEY, E. et al. **A Framework for QoS-based Routing in the Internet**. [S.l.]: IETF, Aug. 1998. (Request for Comments 2386). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[DEM 89] DEMERS, A.; KESHAV, S.; SHENKER, S. Analysis and Simulation of a Fair-queueing Algorithm. In: SYMPOSIUM ON COMMUNICATIONS ARCHITECTURES AND PROTOCOLS, SIGCOMM, 1989, Austin – United States. **Proceedings…**[S.l.:s.n.], 1989.

[DUR 2000] DURHAM, D. et al. **The COPS (Common Open Policy Service) Protocol**. [S.l.]: IETF, Jan. 2000. (Request for Comments 2748). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[FAU 2002a] LE FAUCHEUR, F. et al. **MPLS Support of Differentiated Services**. [S.l.]: IETF, May. 2002. (Request for Comments 3270). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[FAU 2001a] LE FAUCHEUR, F. et al. **Extensions to RSVP-TE and CR-LDP for support of Diff-Serv-aware MPLS Traffic Engineering**. [S.l.]: IETF, Feb. 2001. (Internet draft <draft-ietf-mpls-diff-te-ext-01.txt> work in progress). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[FAU 2002b] LE FAUCHEUR F. et al. **Requirements for support of Diff-Serv-aware MPLS Traffic Engineering**. [S.l.]: IETF, Feb. 2002. (Internet draft <draft-ietf-tewg-diff-te-reqts-03.txt> work in progress). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[FAU 2001b] LE FAUCHEUR F. et al. **Extension to OSPF for support of Diff-Serv-aware MPLS Traffic Engineering**. [S.l.]: IETF, Feb. 2001. (Internet draft <draft-ietf-ospf-diff-te-00.txt> work in progress). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[FAU 2001c] LE FAUCHEUR F. et al. **Extension to ISIS for support of Diff-Serv-aware MPLS Traffic Engineering.** [S.l.]: IETF, Feb. 2001. (Internet draft <draft-ietf-isis-diff-te00.txt> work in progress). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[FLO 93] FLOYD, S.; JACOBSEN V. Random Early Detection Gateways for Congestion Avoidance. **IEEE/ACM Transactions on Networking**, Piscataway, v. 1, n. 4, p. 397-413, 1993.

[FLO 95] FLOYD, S.; JACOBSON V. Link-sharing and Resource Management Models for Packet Networks. **IEEE/ACM Transactions on Networking**, Piscataway, v. 3, n. 4, p. 365-386, 1995.

[GHA 99] GHANWANI, A. et al. Traffic Engineering Standards in IP Networks using MPLS. **IEEE Communications Magazine**, New York, v. 37, n. 12, p. 49-53, 1999.

[GUE 97] GUERIN, R. et al. **Aggregating RSVP based QoS Requests**. [S.l.]: IETF, Nov. 1997. (Internet draft <draft-guerin-aggreg-rsvp-00.txt> work in progress). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[GRO 2002] GROSSMAN, D. **New Terminology and Clarifications for Diffserv**. [S.l.]: IETF, Apr. 2002. (Request for Comments 3260). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[HEI 99] HEINANEN, J. et al. **Assured Forwarding PHB Group**. [S.l.]: IETF, June 1999. (Request for Comments 2597). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[ITU 96] ITU-T. **General Characteristics of International Telephone Connections and International Telephone Circuits:** One-Way Transmission Time, Recommendation G.114. Geneva, 1996.

[JAC 99] JACOBSEN, V.; NICHOLS, K.; PODURI, K. **An expedited forwarding PHB**. [S.l.]: IETF, June 1999. (Request for Comments 2598). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[JAM 2002] JAMOUSSI B. (Ed.). **Constraint-Based LSP Setup using LDP**. [S.l.]: IETF, Jan. 2002. (Request for Comments 3212). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[KAM 2000] KAMIENSKI, C.A.; SADOK, D. Engenharia de Tráfego em uma Rede de Serviços Diferenciados, In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, 18., 2000, Belo Horizonte. **Anais…** Belo Horizonte: UFMG, 2000.

[LI 98] LI, T.; REKHTER, Y. **Provider Architecture for Differentiated Services and Traffic Enginnering (PASTE)**. [S.l.]: IETF, Oct. 1998. (Request for Comments 2430). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[MAG 2001] MAGALHÃES, M.; CARDOZO, E. Introdução à Comutação IP por Rótulos Através de MPLS. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, 19., 2001, Florianópolis. **Anais…** Florianópolis: UFSC, 2001.

[MAL 2002] MALEK, J. **TraceGraph - Trace File Analyser**. Disponível em: <http://www.geocities.com/tracegraph/>. Acesso em 22 maio 2002.

[MOY 98] MOY, J. **OSPF Version 2**. [S.l.]: IETF, Apr. 1998. (Request for Comments 2328). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[NIC 98] NICHOLS, K. et al. **Definition of the Differentiated Services Field (DS field) in the IPv4 and IPv6 Headers**. [S.l.]: IETF, Dec. 1998. (Request for Comments 2474). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[NS2 2002] THE NETWORK Simulator ns-2. Disponível em: <http://www.isi.edu/nsnam/ns/index.html. Acesso em: 22 maio 2002.

[ORA 90] ORAN, D. (Ed.). **OSI IS-IS Intra-domain Routing Protocol**. [S.l.]: IETF, Feb. 1990. (Request for Comments 1142). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[PIE 2000] PIEDA, P. et al. **A Network Simulator Differentiated Services Implementation**. Toronto: Nortel Networks, 2000.

[POS 81] POSTEL, J (Ed.). **Internet Protocol**. [S.l.]: IETF, Sept. 1981. (Request for Comments 791). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[RAJ 99] RAJAN, R. et al. A Policy Framework for Integrated and Differentiated Services in the Internet. **IEEE Network Magazine**, New York, v. 13, n. 5, p. 36-41, 1999.

[ROS 2001a] ROSEN E.; VISWANATHAN A.; CALLON R. **Multiprotocol Label Switching Architecture.** [S.l.]: IETF, Jan. 2001. (Request for Comments 3031). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[ROS 2001b] ROSEN E. et al. **MPLS Label Stack Encoding**. [S.l.]: IETF, Jan. 2001. (Request for Comments 3032). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[SCH 97] SCHENKER, S. et al. **Specification of Guaranteed Quality of Service**. [S.l.]: IETF, Sept. 1997. (Request for Comments 2212). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[SAL 97] SALAM, R. et al. ITU-T G.729 Annex A: Reduced complexity 8 kb/s CS-ACELP codec for digital simultaneous voice and data. **IEEE Communications Magazine**, New York, v. 35, n. 9, p. 56-63, 1997.

[SER 2001a] SERENATO, Fernando M.; ROCHOL, Juergen. **Análise comparativa dos protocolos CR-LDP e RSVP-TE**. 2001. Trabalho Individual (Mestrado em Ciência da Computação) – Instituto de Informática, Universidade Federal do Rio Grande do Sul, Porto Alegre.

[SER 2001b] SERENATO, Fernando M.; ROCHOL, Juergen. **Mecanismos para interoperação de backbones MPLS e redes que utilizem outras arquiteturas de QoS**. Seminário de andamento (Mestrado em Ciência da Computação) – Instituto de Informática, Universidade Federal do Rio Grande do Sul, Porto Alegre.

[SHR 95] SHREEDHAR, M.; VARGHESE, G. Efficient Fair Queuing Using Deficit Round Robin. In: SYMPOSIUM ON COMMUNICATIONS ARCHITECTURES AND PROTOCOLS, SIGCOMM, 1995, Cambridge – United States. **Proceedings…** [S.l.:s.n.], 1995.

[SWA 99] SWALLOW, G. MPLS Advantages for Traffic Engineering. **IEEE Communications Magazine**, New York, v. 37, n. 12, p. 54-57, 1999.

[WAH 97] WAHL, T. et al. **Lightweight Directory Access Protocol V3**. [S.l.]: IETF, Dec. 1997. (Request for Comments 2251). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[WRO 97a] WROCLAWSKI, J. **Specification of the Controlled-Load Network Element Service**. [S.l.]: IETF, Sept. 1997. (Request for Comments 2211). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[WRO 97b] WROCLAWSKI, J. **The use of RSVP with IETF Integrated Services**. [S.l.]: IETF, Sept. 1997. (Request for Comments 2210). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[WRO 2001] WROCLAWSKI, J.; CHARNY, A. **Integrated Service Mappings for Differentiated Services Networks**. [S.l.]: IETF, Mar. 2001. (Internet draft <draft-ietf-issll-ds-map-01.txt> work in progress). Disponível em: <http://www.ietf.org>. Acesso em: 5 maio 2002.

[XIA 99] XIAO, X.; NI, L. Internet Qos: A Big Picture. **IEEE Network Magazine**, New York, v. 13, n. 2, p. 8-18, 1999.

[XIA 2000] XIAO, X.; HANNAN, A.; et. al. Traffic Engineering with MPLS in the Internet. **IEEE Network Magazine**, New York, v. 13, n. 2, p. 28-33, 2000.

[ZIV 99] ZIVIANI, A. ; REZENDE, J. F.; DUARTE, O. C. M. B.; Tráfego de Voz em um Ambiente de Diferenciação de Serviços na Internet, In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, 17., 2000, Salvador. **Anais…** Salvador: UFBA, 1999.