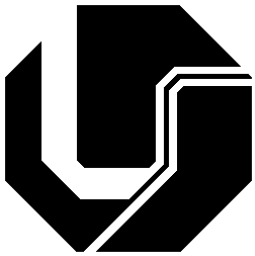
UNIVERSIDADE FEDERAL DE UBERLÂNDIA

FACULDADE DE ENGENHARIA ELÉTRICA

PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA



UM ESTUDO SOBRE A PREEMPÇÃO DE LSPs EM REDES MPLS COM DIFFSERV PARA O PROVIMENTO DE QoS

SANDRO RODRIGO GONÇALVES BASTOS

MARÇO

2005

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

FACULDADE DE ENGENHARIA ELÉTRICA

PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

UM ESTUDO SOBRE A PREEMPÇÃO DE LSPs EM REDES MPLS COM DIFFSERV PARA O PROVIMENTO DE QoS

SANDRO RODRIGO GONÇALVES BASTOS

Dissertação apresentada por Sandro Rodrigo Gonçalves Bastos à Universidade Federal de Uberlândia para obtenção do título de Mestre em Engenharia Elétrica aprovada em 30/03/2005 pela Banca Examinadora:

Paulo Roberto Guardieiro, Dr. (UFU) - Orientador

Walter Godoy Júnior, Dr. (CEFET-PR)

Jamil Salem Barbar, Dr. (UFU)

UM ESTUDO SOBRE A PREEMPÇÃO DE LSPs EM REDES MPLS COM DIFFSERV PARA O PROVIMENTO DE QoS

SANDRO RODRIGO GONÇALVES BASTOS

Dissertação apresentada por Sandro Rodrigo Gonçalves Bastos à Universidade Federal de Uberlândia como parte dos requisitos à obtenção do título de Mestre em Engenharia Elétrica.

_____	_____
Prof. Dr. Paulo Roberto Guardieiro	Prof. Dr. Gilberto Arantes Carrijo
Orientador	Coordenador do Curso de Pós Graduação

DEDICATÓRIA

Para minha família, em especial meus pais Mário e Adília, por todo o apoio e incentivo que sempre demonstraram em minha vida.

“ Embora ninguém possa voltar atrás e fazer um novo começo, qualquer um pode começar agora e fazer um novo fim. ”

Chico Xavier

AGRADECIMENTOS

À Deus, pela vida e oportunidades que têm me oferecido. Aos meus pais, minha avó, meus irmãos, cunhado e cunhada, que sempre me deram forças para crescer.

Agradeço a Universidade Santa Cecília (Unisanta), que acreditou em minha competência e capacidade de trabalho. A todos os colegas da Unisanta, pela ajuda e companheirismo durante a pós-graduação.

Ao Prof. Dr. Paulo Roberto Guardieiro, pelo seu apoio e dedicação na orientação deste trabalho.

Aos colegas do Laboratório de Redes de Computadores, pela ajuda e paciência durante toda a dissertação. Aos funcionários do setor de pós-graduação, pelo bom atendimento sempre que necessário.

Aos colegas da Embratel S/A, pela atenção e conselhos nos momentos em que precisei.

À minha namorada, amigos e todas as pessoas que indiretamente contribuíram neste trabalho, meu muito obrigado.

RESUMO

Bastos, S. R. G., Um Estudo sobre a Preempção de LSPs em Redes MPLS com DiffServ para o Provimento de QoS, UFU, Uberlândia, Brasil, 2005, 120p.

Qualidade de Serviço (QoS – *Quality of Service*) é um dos requisitos mais importantes para o bom desempenho das aplicações multimídia. A integração das tecnologias MPLS e DiffServ tornou-se uma das principais propostas para o provimento de QoS às aplicações multimídia nas redes *backbone*, associando a QoS oferecida pelo DiffServ com a engenharia de tráfego do MPLS. A preempção de LSPs (*Label Switching Paths*) tem se tornado um tópico de amplo estudo pelo IETF, devido a sua grande importância no suporte à engenharia de tráfego em redes MPLS/DiffServ (DS-TE). O objetivo desta dissertação é aplicar uma nova tecnologia (preempção) em um *backbone* com MPLS/DiffServ, avaliando seu desempenho através de simulação, devido a impossibilidade de se trabalhar com um ambiente real. Um modelo de simulação, baseado no *backbone* regional da Embratel dentro do Estado de São Paulo, foi utilizado em cinco experimentos diferentes, onde tráfegos multimídia são mapeados em classes DiffServ pelo roteador de borda e, em seguida, inseridos em LSPs até o roteador de destino. Os resultados dos experimentos permitem concluir que a preempção exerce um papel fundamental na garantia dos parâmetros de QoS exigidos pelas aplicações mais importantes, como vazão, atraso, *jitter* e perda de pacotes.

Palavras-chave: Preempção, Qualidade de Serviço, MPLS, Serviços Diferenciados, Engenharia de Tráfego.

ABSTRACT

Bastos, S. R. G., A Study of LSP Preemption for QoS Provisioning in DiffServ-aware MPLS Networks, UFU, Uberlândia, Brazil, 2005, 120p.

Quality of Service (QoS) is one of the most important requirements for the good performance of multimedia applications. The combination of MPLS and DiffServ technologies presents a very attractive strategy for QoS provisioning of multimedia applications, associating the QoS of the DiffServ with the traffic engineering of the MPLS. LSPs (Label Switching Paths) preemption becomes a topic of ample study for the IETF, which a great importance supporting traffic engineering in DiffServ-aware MPLS networks (DS-TE). The objective of this dissertation is to apply a new technology (preemption) in a MPLS/DiffServ network, analyzing its effectiveness by performing simulation, because it was not possible use a real network. A simulation model, based on the backbone of Embratel located in the State of São Paulo, was used in five different experiments, where multimedia traffics are mapped in DiffServ classes by the edge router and, after that, inserted in LSPs until the destination router. The results allow to conclude that preemption does a fundamental work in the guarantee of the QoS parameters demanded by the most important applications, as throughput, delay, jitter and packet loss.

Key words: Preemption, Quality of Service, MPLS, Differentiated Services, Traffic Engineering.

UM ESTUDO SOBRE A PREEMPÇÃO DE LSPs EM REDES MPLS COM DIFFSERV PARA O PROVIMENTO DE QoS

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

ABREVIATURAS E SÍMBOLOS

AF	*Assured Forwarding*
ATM	*Asynchronous Transfer Mode*
BA	*Behavior Aggregate*
BE	*Best Effort*
BC	*Bandwidth Constraint*
BGP	*Border Gateway Protocol*
BTT	*Bidirectional Traffic Trunk*
CBQ	*Class Based Queueing*
CBR	*Constant Bit Rate*
CLP	*Cell Loss Priority*
CLS	*Controlled Load Service*
CR-LDP	*Constraint-Based Routed LDP*
CR-LSP	*Constraint-Based Routed LSP*
CSPF	*Constrained Shortest Path First*
CT	*Class Type*
DiffServ	*Differentiated Services*
DLCI	*Data Link Connection Identifier*
DSCP	*DiffServ Code Point*
DSL	*Digital Subscriber Line*
DS-TE	*DiffServ-aware MPLS Traffic Engineering*
EF	*Expedited Forwarding*
E-LSP	*EXP Inferred LSP*
ER	*Explicit Route*

FEC	*Forward Equivalence Class*
FIFO	*First In, First Out*
FTN	*FEC-to-NHLFE*
FTP	*File Transfer Protocol*
GS	*Guaranteed Service*
HTTP	*Hypertext Transfer Protocol*
IETF	*Internet Engineering Task Force*
IGP	*Interior Gateway Protocol*
ILM	*Incoming Label Mapping*
IntServ	*Integrated Services*
IP	*Internet Protocol*
ISP	*Internet Service Provider*
IS-IS	*Intermediate Station to Intermediate Station*
ITU	*International Telecommunications Union*
LAN	*Local Area Network*
LDP	*Label Distribution Protocol*
LER	*Label Edge Router*
L-LSP	*Label-Only Inferred LSP*
LM	*Incoming Label Mapping*
LPCD	*Linha Privativa de Comunicação de Dados*
LSPs	*Label Switched Paths*
LSR	*Label Switching Router*
MAM	*Maximum Allocation Model*
MF	*Multi Field*
MNS	*MPLS Network Simulator*

MPLS	*MultiProtocol Label Switching*
NHLFE	*Next Hop Label Forwarding Entry*
NS	*Network Simulator*
OSI	*Open Systems Interconnection*
OSPF	*Open Shortest Path First*
OTCL	*Object Tool Command Language*
PHB	*Per Hop Behavior*
POP	*Ponto de Presença*
PQ	*Priority Queueing*
QoS	*Quality of Service*
RDM	*Russian Dolls Model*
RED	*Random Early Detection*
RFC	*Request for Comments*
RIP	*Routing Information Protocol*
RSVP	*Resource Reservation Protocol*
RTPC	*Rede de Telefonia Pública Comutada*
SLA	*Service Level Agreement*
SPF	*Shortest Path First*
TB	*Token Bucket*
TCP	*Transmission Control Protocol*
TE-Class	*Trafic Engineering Class Type*
TEWG	*Traffic Engineering Working Group*
TLV	*Type, Length and Value*
TOS	*Type of Service*
TTL	*Time to Live*

UB	*Unreserved Bandwidth*
UDP	*User Datagram Protocol*
VC	*Virtual Circuit*
VoIP	*Voice over IP*
VPI/VCI	*Virtual Path Identifier / Virtual Channel Identifier*
WAN	*Wide Area Network*
WFQ	*Weighted Fair Queueing*
WRED	*Weighted Random Early Detection*
WRR	*Weighted Round Robin*
WWW	*World Wide Web*

UM ESTUDO SOBRE A PREEMPÇÃO DE LSPs EM REDES MPLS COM DIFFSERV PARA O PROVIMENTO DE QoS

CAPÍTULO 1

INTRODUÇÃO

O tráfego nas redes IP (*Internet Protocol*) está passando atualmente por um forte crescimento, com o surgimento de novos serviços e modificação na forma de utilização de alguns já existentes. Os tráfegos de voz, multimídia, comércio eletrônico e educação a distância têm incentivado a criação de aplicações com características de tempo real que requerem novas funcionalidades, níveis diferenciados de transporte e qualidade de serviço (QoS - *Quality of Service*). Por esse motivo, é necessário que as redes de comunicação suportem contratos de nível de serviço (SLA - *Service Level Agreement*), com parâmetros que definam as garantias mínimas de QoS para as aplicações dos usuários.

A qualidade de serviço nas redes IP é fundamental principalmente para o bom desempenho de aplicações em tempo real. Entre os principais requisitos exigidos pelas

aplicações através dos contratos de serviço SLA, destacam-se parâmetros como o atraso, *jitter*, largura de banda, vazão e perda de pacotes [01].

Porém, uma das principais características que permitiu a disseminação do protocolo IP é a sua simplicidade de funcionamento, oferecendo apenas o serviço de melhor esforço *(best effort*), sem nenhuma garantia na entrega dos pacotes de dados transmitidos pelas aplicações. Em situações em que a rede está congestionada, os pacotes podem ser perdidos ou sofrer atrasos indeterminados. A inadequação deste serviço aos requisitos das novas aplicações motivou, nos últimos anos, o surgimento de muitas propostas com o objetivo de criar um novo modelo de serviços para a Internet. Dentre estas propostas, destacam-se os modelos de serviços integrados (IntServ), serviços diferenciados (DiffServ) e o MPLS *(Multiprotocol Label Switching*) [02].

A utilização da arquitetura IntServ em redes de grande porte se torna muito complexa, pois cada fluxo de dados é tratado individualmente. Essa característica implica em uma baixa escalabilidade, pois o gerenciamento do fluxo de informações se torna mais difícil na medida que aumenta o tráfego de pacotes no *backbone*.

A arquitetura DiffServ é a mais indicada para as redes de grande porte, devido a sua melhor escalabilidade. Seu objetivo é agregar os fluxos provenientes das aplicações interligadas a seus roteadores de borda em classes de tráfego pré-definidas. Dessa forma, minimiza-se o processamento nos roteadores da rede, uma vez que as informações deixam de ser manuseadas por fluxo simples e passam a ser tratadas por agregados de fluxos.

Originalmente, a tecnologia MPLS foi desenvolvida sem o objetivo de oferecer QoS às aplicações. Entretanto, suas características de rápida comutação de pacotes e facilidade na implementação de engenharia de tráfego têm levado sua implantação em diversos *backbones* ao redor do mundo. Uma maneira utilizada pelo MPLS para prover engenharia de tráfego é o roteamento explícito, onde o roteador de borda determina a seqüência completa dos

roteadores que compõem uma rota, denominada LSP (*Label Switching Path*). Isso é possível através da inclusão de um rótulo pequeno e de tamanho fixo, sendo lido pelos roteadores dentro do domínio MPLS, tornando-se desnecessária a leitura de todo o cabeçalho IP.

O uso combinado entre MPLS e DiffServ permite que a rede ofereça a garantia da qualidade de serviço do DiffServ aliado com o encaminhamento rápido de pacotes e engenharia de tráfego oferecidos pelo MPLS. Para isso é necessário o mapeamento do campo DSCP (*DiffServ Codepoint*) em rótulos MPLS, porque os roteadores MPLS não examinam o conteúdo do cabeçalho IP, ficando restritos apenas ao conteúdo dos rótulos. Porém, o DSCP está alocado dentro do cabeçalho IP, com as informações sobre o tipo de tratamento que os roteadores devem oferecer para cada classe de serviço. Há duas soluções para esse problema: E-LSP (*EXP Inferred LSP*) e L-LSP (*Label-Only Inferred LSP*). Na primeira abordagem, os 3 bits do campo EXP do rótulo MPLS são utilizados como suporte ao DiffServ, podendo estabelecer até 8 classes de serviço. A segunda solução geralmente é utilizada em redes em que é necessário mais que oito classes de serviço, ou em redes como o ATM (Asynchronous Transfer Mode) e *Frame-Relay*, onde não é utilizado o campo EXP [03].

Recentemente, o IETF (*Internet Engineering Task Force*) publicou a RFC (*Request for Comments*) 3564 [04], com os requisitos necessários para a implementação de engenharia de tráfego em redes MPLS/DiffServ (DS-TE). Este documento identifica a necessidade de priorização e preempção de LSPs, que já haviam sido definidos anteriormente pela RFC 2702 [05].

A preempção (*preemption*) determina se um LSP com um certo nível de prioridade pode apropriar os recursos de outro(s) LSP(s) de menor prioridade, quando há competição pelos recursos disponíveis. São definidos 8 níveis de prioridade, podendo variar de 0 a 7. Um LSP com nível de preempção 0 tem prioridade maior que os demais. O nível 7 é atribuído aos LSPs menos importantes. Na realidade, cada LSP possui duas prioridades: uma prioridade de

Setup e uma prioridade de *Holding*. A prioridade de *Setup* de um LSP a ser estabelecido na rede é comparada com a prioridade de *Holding* dos LSPs já existentes. Caso algum LSP tenha uma prioridade de *Holding* menor que a prioridade de *Setup* do novo LSP, será descartado e seus recursos serão transferidos ao novo LSP. Para se evitar disputas contínuas entre os LSPs, a prioridade de *Holding* sempre deve ser maior que a prioridade de *Setup*.

1.1. Definição do Problema

Devido a simplicidade original em seu desenvolvimento, o protocolo IP apresenta limitações para a implementação de QoS. Neste protocolo, a rede fornece apenas o serviço "melhor esforço", sem nenhum tipo de priorização, classificação e reserva de recursos. As aplicações multimídia e em tempo real, como voz, videoconferência e telemedicina, têm apresentado um forte crescimento, exigindo níveis mais rígidos de QoS que não podem ser oferecidos pelo modelo tradicional.

O simples aumento de largura de banda nas redes dos ISPs não é a solução mais adequada, principalmente devido ao custo envolvido na atualização da infra-estrutura a cada vez que se fizer necessário este aumento. Para atender as necessidades atuais, a rede *backbone* deve utilizar a largura de banda disponível com maior eficiência, evitando pontos de congestionamento para encaminhamento do tráfego, além de oferecer uma redução no atraso, *jitter* e perda de pacotes.

1.2. Solução Proposta

Apresenta-se como proposta à necessidade de se oferecer níveis adequados de QoS às aplicações multimídia o uso da preempção de LSPs combinado com as tecnologias DiffServ e MPLS nas redes *backbone*. Essa arquitetura permite associar a QoS resultante do DiffServ com a comutação rápida de pacotes IP e engenharia de tráfego oferecidos pelo MPLS. A RFC

3564 [04] destaca a necessidade do uso da preempção de LSPs com o objetivo de garantir que os LSPs mais importantes possam sempre manter a transmissão de pacotes mesmo em situações de insuficiência de recursos ou após falhas na rede.

O IETF criou um grupo de trabalho denominado *Internet Traffic Engineering* (TEWG) [06], onde diversas RFCs e *Internet Drafts* envolvem o tema da preempção. O assunto vem sendo muito discutido, com diversos tópicos de interesse ainda em fase de desenvolvimento. Baseado na literatura pesquisada, verificou-se a necessidade de um estudo sobre as principais características do uso da preempção de LSPs em uma rede MPLS com serviços diferenciados. Para atingir esse objetivo, descreve-se o estágio atual de desenvolvimento de algumas soluções, como o DiffServ, o MPLS, a Engenharia de Tráfego e a preempção de LSPs, além da integração dessas tecnologias e sua adequação no suporte de QoS às aplicações.

Neste estudo propõe-se avaliar o comportamento de um *backbone* MPLS/DiffServ com preempção de LSPs, verificando sua eficiência no provimento de QoS às aplicações de multimídia, por meio de modelagem e simulação, uma vez que não foi possível trabalhar com um *backbone* real. Um modelo de rede foi criado tendo como base informações coletadas no *backbone* regional da Embratel, localizado dentro do Estado de São Paulo. Aplicou-se a preempção neste modelo, permitindo a avaliação do comportamento do *backbone* no encaminhamento dos tráfegos de aplicações multimídia em termos de vazão, atraso, *jitter* e perda de pacotes.

1.3. Trabalhos Relacionados

Os artigos [07], [08], [09] e [10], e a tese de doutorado em [11] formaram a base de um *Internet Draft* [12] recentemente publicado no IETF, descrevendo uma proposta de política de preempção de LSPs para a engenharia de tráfego em redes MPLS/DiffServ. Neste documento, a política de preempção pode ser alterada para se alcançar diferentes objetivos, como reduzir

o número de LSPs que devem sofrer preempção, apropriar os LSPs de menor prioridade ou então escolher os LSPs que serão apropriados com o objetivo de reduzir o desperdício de largura de banda.

Atualmente, apenas o método *Hard Preemption* [13] está definido. Neste método, o algoritmo de preempção descarta imediatamente o LSP escolhido para liberar espaço ao novo LSP. O inconveniente deste método é a desconexão abrupta do LSP escolhido, causando interrupção no fluxo de pacotes. Um novo método que vem sendo discutido é o *Soft Preemption* [14], cujo objetivo é reduzir e/ou eliminar a interrupção do tráfego do LSP apropriado. O algoritmo *Soft Preemption* permite que o LSP que irá sofrer a preempção encontre um novo caminho antes da preempção ocorrer, garantindo assim a continuidade do fluxo de seus pacotes.

A preempção também é utilizada como solução em outras áreas, como nas redes de telefonia móvel [15]. Em [16] foi feito um estudo sobre o uso da preempção em redes de telefonia fixa, móvel e redes de acesso. Basicamente, a preempção é utilizada em casos de congestionamento, com o objetivo de priorizar as conexões dos usuários principais. O artigo [17] mostra um algoritmo onde a preempção é inserida no processo de criação de circuitos virtuais em redes ATM.

Em [18], é proposto um novo algoritmo ao protocolo CSPF (*Constrained Shortest Path First*) para minimizar a preempção de LSPs de menor prioridade, aprimorando a estabilidade das redes MPLS. Em [19] é proposto um algoritmo onde integra-se o conceito de preempção a um mecanismo de roteamento de LSPs, selecionando quais LSPs serão re-roteados em casos de congestionamento ou falhas nos enlaces. O artigo [20] descreve propostas de políticas de preempção de LSPs em redes MPLS com o objetivo de otimizar o uso de largura de banda pelas aplicações.

1.4. Estrutura da Dissertação

A organização da dissertação foi realizada da seguinte forma: No Capítulo 1 apresenta-se os objetivos da dissertação e um estudo sobre os trabalhos relacionados. Apresenta-se também a estrutura de organização do trabalho. No Capítulo 2 mostra-se os principais conceitos e definições sobre a qualidade de serviço em redes de computadores. Descreve-se o modo de funcionamento das principais tecnologias propostas pelo IETF, como o IntServ, o DiffServ e o MPLS.

No Capítulo 3 detalha-se a engenharia de tráfego em redes MPLS/DiffServ. Inicialmente apresenta-se a integração entre essas duas tecnologias, destacando seus benefícios e o modo de funcionamento conjunto. A seguir, desenvolve-se os principais conceitos relacionados à engenharia de tráfego, finalizando com os requisitos necessários para sua aplicação em redes MPLS/DiffServ, como a formação de *Class Types*, a implementação de modelos de restrições de largura de banda e a preempção de LSPs. No capítulo 4 descreve-se os principais conceitos envolvidos na preempção de LSPs, como os critérios de aplicação, modos de funcionamento e políticas de preempção existentes.

No Capítulo 5 avalia-se o desempenho de uma rede com MPLS e DiffServ na obtenção de qualidade de serviço para aplicações multimídia. Introduz-se a preempção de LSPs com o objetivo de ilustrar sua capacidade em garantir recursos de rede para as aplicações mais importantes, principalmente nos casos de congestionamento. Através de modelagem e simulação com o auxílio do programa *Network Simulator* (NS-2), obteve-se os gráficos que permitiram a apresentação e análise de resultados.

Finalmente, no Capítulo 6 apresenta-se as conclusões finais e as principais contribuições do trabalho, além de sugestões de trabalhos futuros que podem ser desenvolvidos dentro deste contexto. No Capítulo 7 encontra-se as referências bibliográficas utilizadas nesta dissertação.

CAPÍTULO 2

QUALIDADE DE SERVIÇO EM REDES IP

2.1. Introdução

As redes IP (*Internet Protocol*) continuam crescendo de forma exponencial em praticamente todo o mundo. Esta tecnologia, criada nos anos 70, teve como premissa básica a possibilidade de utilizar os diversos meios físicos e tecnologias existentes na época. As redes IP foram projetadas tendo como fundamento a criação da chamada “arquitetura aberta de rede”, com princípios como autonomia, controle descentralizado e uso do serviço de melhor esforço [21].

No cenário atual, é cada vez maior o tráfego de aplicações multimídia, com requisitos de tempo, sincronização e largura de banda para a sua operação com qualidade. As redes de comunicação convergem para uma estrutura única, suportando áudio, vídeo e tráfego de dados críticos para a operação de uma empresa. Diferente das redes de comutação de circuitos, como o sistema telefônico, as redes de comutação de pacotes, como a Internet, não foram desenvolvidas para prover garantias de serviço em uma conexão. Como resultado, pacotes de um mesmo fluxo de dados podem chegar ao destino percorrendo rotas diferentes, além de sofrer diferentes níveis de atraso, *jitter* e perda de pacotes. Isto tem se tornado um grave problema, principalmente porque diversas aplicações originalmente desenvolvidas para trafegar em redes de comutação de circuitos estão sendo migradas para a Internet.

A arquitetura atual da Internet baseada no modelo de serviços "melhor esforço" (*best-effort*), tem bom desempenho para as aplicações elásticas como e-mail, FTP (*File Transfer Protocol*) e HTTP (*Hypertext Transfer Protocol*). Por outro lado, as aplicações de multimídia requerem diferentes níveis de serviços para cada classe de tráfego, com garantias mínimas de atraso e *jitter*. Nesse sentido, é necessário estudar os aspectos mais importantes relacionados à Qualidade de Serviço (QoS - *Quality of Service*), permitindo oferecer o serviço adequado para cada tipo de tráfego, independente da tecnologia de rede utilizada. A necessidade de QoS se torna mais evidente nas redes de longa distância *WAN (Wide Area Network*), que geralmente apresentam enlaces de baixa velocidade devido ao custo mensal envolvido. Assim, pode ser fundamental priorizar alguns tipos de tráfego em detrimento de outros, otimizando o uso dos recursos de rede.

Este capítulo tem como objetivo apresentar os conceitos fundamentais de QoS, apresentando os métodos de medição e mecanismos atualmente disponíveis para sua implementação.

2.2. Definição de QoS

De acordo com o ITU (*International Telecommunications Union*), a QoS é definida como sendo o efeito coletivo do desempenho de um serviço que determina a satisfação do usuário deste serviço [22]. Entretanto, os diversos serviços existentes na Internet possuem características distintas, o que torna o conceito de QoS subjetivo e dependente destas características. Assim, sob o ponto de vista dos parâmetros de desempenho de uma rede, a QoS é um requisito das aplicações para a qual exige-se que determinados parâmetros (vazão, atraso, perdas, etc) estejam dentro de limites bem definidos [23].

Os mecanismos de QoS têm como princípio a otimização no uso dos recurso de rede. O incremento de largura de banda tem sido defendido pelos administradores de diversos ISPs

(*Internet Service Providers*) como a melhor solução para os problemas relacionados com o congestionamento, perda de pacotes e atraso, principalmente devido à queda dos valores praticados no mercado. Entretanto, aplicações em tempo real como voz sobre IP (VoIP), requerem garantias de atraso, *jitter* e perda de pacotes, não apenas de largura de banda. Além disso, com a crescente necessidade do uso de Internet diariamente associado com novas aplicações de multimídia, certamente a largura de banda oferecida será consumida em pouco tempo, retornando ao estágio anterior de limitação de recursos. Outra vantagem da implementação de mecanismos de QoS é a priorização e proteção de determinados fluxos de tráfego, geralmente necessário quando a rede experimenta picos de utilização [24].

2.3. Medidas de QoS

Os parâmetros de QoS definem os requisitos de cada aplicação e quantificam o desempenho da rede, dentre os quais destacam-se o atraso, *jitter*, largura de banda, vazão e perda de pacotes. A especificação dos parâmetros de QoS geralmente depende do tipo de aplicação envolvida, sendo que diferentes aplicações podem ter diferentes interpretações de requisitos de QoS, porém os parâmetros descritos nesta seção podem ser considerados uma base única que envolve as diversas formas de tráfego.

2.3.1. Atraso

Quando um pacote viaja de um nó ao nó subseqüente (sistema final ou roteador), ele sofre, ao longo desse caminho, diferentes tipos de atraso em cada nó existente no caminho. Os mais importantes desses atrasos são o atraso de processamento nodal, o atraso de fila, o atraso de transmissão e o atraso de propagação; juntos, esses atrasos se acumulam para formar o atraso nodal total [21].

O atraso de processamento inclui fatores como o tempo requerido para examinar o cabeçalho do pacote e determinar para onde direcioná-lo e o tempo necessário para verificar os erros em bits existentes no pacote. O atraso de processamento em roteadores de alta velocidade normalmente se situa na faixa dos microssegundos ou menos. Ao chegar à fila (*buffer*) de saída, o pacote sofre um atraso de fila enquanto espera para ser transmitido no enlace. Este atraso dependerá da quantidade de outros pacotes que chegaram antes. Se a fila estiver vazia e não houver nenhuma transmissão de pacote em curso, o tempo de atraso de fila será zero. Porém, se o tráfego estiver pesado e houver muitos pacotes esperando para serem transmitidos, o atraso de fila será longo [21].

O atraso de transmissão é a quantidade de tempo exigida para a transmissão de todos os bits do pacote no enlace, sendo obtido através da divisão do comprimento do pacote (bits) pela velocidade de transmissão do enlace (bits por segundo). O atraso de propagação é o tempo que leva para um bit se propagar de um roteador até o roteador seguinte. O bit se propaga à velocidade de propagação do enlace, sendo uma função da distância entre os dois roteadores [21].

O atraso fim a fim é o acúmulo de atrasos de processamento de transmissão e de formação de filas nos roteadores, atrasos de propagação e atrasos de processamento nos sistemas finais ao longo do trajeto da fonte ao destino [21]. Um valor elevado de atraso pode prejudicar o desempenho de aplicações em tempo real. Como exemplo, para as aplicações de áudio, atrasos fim a fim menores do que 150 milissegundos não são percebidos pelo ouvido humano; atrasos entre 150 e 400 milissegundos podem ser aceitáveis, mas não são o ideal, e atrasos que excedem 400 milissegundos podem atrapalhar seriamente a interatividade.

2.3.2. *Jitter*

Por causa de atrasos variáveis dentro da rede, o tempo decorrido entre o momento em que um pacote é gerado na fonte e o momento em que é recebido no destinatário pode variar de pacote para pacote. Isso é denominado variação de atraso ou *jitter* [21].

No roteador de destino, o *jitter* introduz distorções no processamento do fluxo de informações, podendo comprometer a inteligibilidade de um sinal de áudio, por exemplo. A variação de atraso pode ser atenuada ou até eliminada através do uso de mecanismos específicos, sendo uma das soluções mais comuns a utilização de *buffers* responsáveis pelo armazenamento de uma certa quantidade de pacotes, permitindo assim o seu posterior ordenamento.

2.3.3. Largura de Banda e Vazão

Largura de banda e vazão (*throughput*) são dois dos termos mais confusos usados em redes. Quando falamos sobre a largura de banda de um enlace de comunicação, normalmente nos referimos ao número de bits por segundo que podem ser transmitidos no enlace. Podemos dizer que a largura de banda de uma rede *Ethernet* é 10 Mbps. Porém, uma distinção importante poderia ser feita entre a largura de banda que está disponível no enlace e o número de bits por segundo que podemos realmente transmitir pelo enlace na prática. Costumamos usar a palavra *throughput* para nos referirmos ao desempenho medido de um sistema. Assim, devido às diversas ineficiências de implementação, um par de nós conectados por um enlace com uma largura de banda de 10 Mbps poderia atingir um *throughput* de apenas 2 Mbps [25].

2.3.4. Perda de Pacotes

A perda de pacotes mostra a quantidade de pacotes que foram transmitidos, porém não alcançaram o destino em um certo período de tempo. É uma grandeza geralmente

representada como probabilidade de perda de pacotes. Pode haver perda devido a erros provocados por problemas no enlace, ou então os pacotes podem ser simplesmente descartados pelos equipamentos de rede. Devem ser definidos limites específicos para cada tipo de aplicação, para que a perda de pacotes não afete seu desempenho.

2.4. Mecanismos para Obtenção de QoS

O suporte necessário para a obtenção de QoS nas redes de dados inclui certas funcionalidades como a classificação e admissão de tráfego, mecanismos de escalonamento, congestionamento e policiamento. Estas funcionalidades são geralmente implementadas em estágios, podendo utilizar diversas combinações de acordo com as capacidades de *hardware*, tipo de aplicações e nível solicitado de QoS.

2.4.1. Classificação e Admissão de Tráfego

Neste estágio é feita a classificação dos pacotes em determinadas classes de tráfego, permitindo assim que políticas de admissão sejam implementadas. Através da classificação, é possível controlar se determinado tráfego está de acordo com uma política preestabelecida entre o usuário e o provedor. Esta etapa é fundamental para a implementação de QoS, pois permite o controle de congestionamento de rede.

2.4.2. Escalonamento

Escalonamento é o modo como os pacotes enfileirados são selecionados para transmissão pelo enlace. Os algoritmos de enfileiramento têm como principal objetivo alocar largura de banda entre várias classes de tráfego de maneira justa, provendo garantias de limites de atraso, *jitter* e perda de pacotes aos fluxos ou agregados de fluxos [24]. Existem diversas técnicas propostas, e a escolha deve levar em conta o tamanho máximo da fila e o

comportamento do tráfego presente na rede. Algumas técnicas utilizadas são: FIFO (*First In, First Out*), PQ (*Priority Queueing*), CBQ (*Class Based Queueing*), WRR (*Weighted Round Robin*) e WFQ (*Weighted Fair Queueing*).

O mecanismo FIFO armazena os pacotes quando a rede está congestionada, e os envia na ordem de chegada quando a rede estiver livre. Esse algoritmo oferece o mesmo nível de prioridade a todos os fluxos, prejudicando a provisão de QoS. Devido a essa deficiência, surgiu a necessidade de se implementar filas distintas com diferentes níveis de prioridade. O algoritmo de enfileiramento por prioridade (PQ) funciona nessa filosofia, dividindo o tráfego em diversos níveis de prioridade. É uma solução superior à anterior, porém apresenta algumas desvantagens, principalmente se o volume de tráfego de alta prioridade for muito alto, pois o tráfego normal poderá ser descartado devido a insuficiência de espaço no armazenamento.

O algoritmo CBQ é uma variação do enfileiramento por prioridade, implementando várias filas de saída e definindo a quantidade de tráfego que deve ser encaminhado por cada fila. É um método razoável no gerenciamento dos recursos das filas, permitindo seu compartilhamento entre diversas classes de serviço. Para enlaces de alta capacidade, apresenta problemas de escalabilidade devido ao elevado custo computacional no re-ordenamento de pacotes e gerenciamento das filas. O mecanismo WFQ assegura que o tráfego receba um serviço previsível, priorizando os tráfegos com menor volume, de forma que seus pacotes sejam transmitidos em pouco tempo. Os tráfegos de maior volume compartilham o restante da capacidade de forma proporcional. Da mesma forma que os outros mecanismos, também apresenta problemas de escalabilidade [21].

2.4.3. Mecanismos de Descarte (*Dropper*)

Os algoritmos de controle de congestionamento mais utilizados são o RED (*Random Early Detection*) e WRED (*Weighted Random Early Detection*). Basicamente, esses

mecanismos reduzem o fluxo de pacotes durante períodos de congestionamento. Com um menor volume de pacotes sendo encaminhados, o nível de congestionamento na rede é reduzido.

O mecanismo RED detecta quando a quantidade média de *bytes* na fila ultrapassa determinado limiar, selecionando fluxos aleatórios para descarte de pacotes, forçando os emissores de tráfego a reduzir as taxas de transmissão. O mecanismo RED oferece o mesmo nível de prioridade a todos os fluxos de pacotes, não sendo possível implementar nenhuma forma de diferenciação de classes. Essa deficiência resultou no desenvolvimento do mecanismo WRED, onde o tráfego é marcado na borda da rede, permitindo a diferenciação no processamento dos nós intermediários [24].

2.4.4. Policiamento de Tráfego

Controla o volume de tráfego que é inserido na rede, determinando assim a taxa em que esse tráfego será transmitido. São utilizados dois métodos para policiamento de tráfego, *leaky bucket* e *token bucket*. O primeiro método é similar a um balde com água e um furo embaixo, resultando em um fluxo de saída constante, independente do volume de água inserido no balde. De forma análoga, o tráfego encaminhado pela fonte é armazenado em uma fila e, mesmo quando rajadas forem enviadas à rede, o tráfego inserido na rede será enviado com taxa constante.

Na segunda solução, são gerados *tokens* em determinados intervalos de tempo, sendo que um pacote pode ser encaminhado apenas se um *token* estiver disponível. Esta solução permite o encaminhamento de tráfego em rajadas de curta duração, enquanto que o primeiro mecanismo encaminha um tráfego mais regular.

2.5. Características das Aplicações

Um dos principais fatores para a obtenção de QoS está no comprometimento com o tempo de transferência dos pacotes. Levando-se em conta o atraso fim a fim, pode-se definir as aplicações em dois tipos: Aplicações em Tempo Real e Aplicações Elásticas [23].

As aplicações em tempo real precisam que a informação chegue ao destino em um tempo máximo determinado. São aplicações sensíveis ao atraso e, como principais exemplos têm-se as aplicações de voz e vídeo. As aplicações elásticas sempre toleram maiores atrasos. Porém, isso não significa que elas sejam insensíveis ao atraso, que é responsável pela redução da performance da aplicação. As aplicações elásticas podem ser divididas em três tipos, de acordo com a sensibilidade do atraso: Alta sensibilidade (ex. Telnet), média sensibilidade (ex. FTP) e baixa sensibilidade (ex. E-mail). A Tabela 2.1 apresenta os requisitos necessários de algumas aplicações [26].

Tabela 2.1 - Requisitos de QoS típicos de algumas aplicações

Aplicação	Vazão	Atraso	*Jitter*	Taxa de Erro
Voz	64 Kbps	100 a 250 ms	< 400 ms	10^{-2}
Vídeo MPEG	1 a 6 Mbps	100 a 500 ms	< 100 ms	10^{-5}
Videoconferência	112 Kbps	100 a 500 ms	< 400ms	10^{-4}
FTP, Telnet	-	-	-	10^{-4}

A caracterização dos tipos de aplicações é citada como guia para o desenvolvimento de um modelo de serviços, devendo ser capaz de incorporar diversos conceitos não relacionados. Assim, diferentes aplicações podem possuir exigências distintas, como por exemplo, um aumento da capacidade de largura de banda ou um valor específico na taxa de erro de pacotes.

2.6. Tecnologias para Obtenção de QoS

Atualmente a Internet oferece apenas o modelo de serviço de melhor esforço (BE - B*est Effort*). Este modelo não oferece garantias, sendo adequado para aplicações menos exigentes, como correio eletrônico e transferência de arquivos. Entretanto, a busca por QoS tem se acentuado nos últimos anos, principalmente devido as exigências das novas aplicações (Voz sobre IP, multimídia, etc), cujos requisitos não conseguem ser atendidos pelo mecanismo de melhor esforço. Na tentativa de permitir o funcionamento de tais aplicações, diversos estudos vêm sendo apresentados pelo IETF *(Internet Engineering Task Force*), dentre os quais destacam-se os Serviços Integrados (IntServ - *Integrated Services*), Serviços Diferenciados (DiffServ - *Differentiated Services*) e o MPLS (*Multiprotocol Label Switching*) [23].

2.6.1. Serviços Integrados (IntServ)

A arquitetura IntServ é baseada na reserva de recursos através do protocolo RSVP (*Resource Reservation Protocol*). Isto significa que, antes que os dados sejam efetivamente transmitidos, as aplicações devem primeiro efetuar a reserva de recursos na rota determinada. O modelo IntServ propõe duas classes de serviço além da classe BE: Serviço Garantido (GS - *Guaranteed Service*) e o Serviço de Carga Controlada (CLS - *Controlled Load Service*).

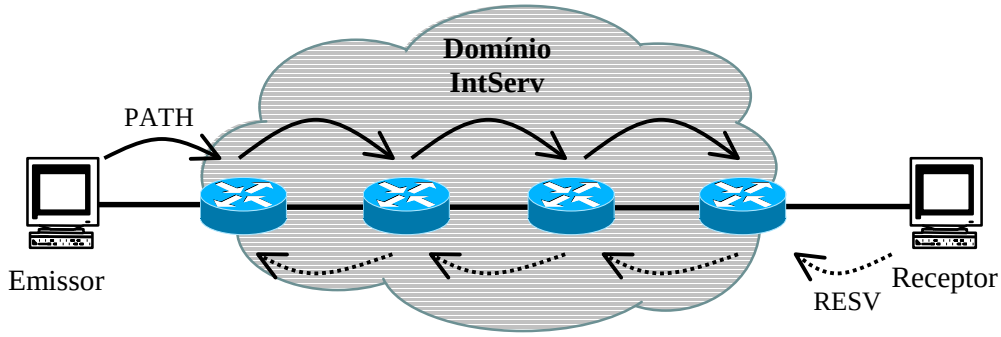


Figura 2.1 - Protocolo RSVP em uma rede IntServ

O Serviço Garantido é destinado a aplicações em tempo real, como áudio e vídeo. Oferece limites rígidos, garantindo o atraso e o *jitter*. Basicamente, uma sessão requisitando GS está solicitando que os pacotes tenham uma taxa de transmissão garantida. O Serviço de Carga Controlada oferece uma QoS muito próxima daquela que um fluxo de pacotes poderia receber em uma rede não sobrecarregada. Este serviço oferece um nível superior ao *best effort*, sendo utilizado para aplicações críticas como transações bancárias ou telemedicina.

A arquitetura IntServ pode ser classificada em quatro componentes [26]:

Protocolo de Sinalização: O protocolo de sinalização utilizado é o RSVP, e consiste em troca de mensagens entre o emissor e o receptor, através da rota estabelecida pelo protocolo de roteamento.

Controle de Admissão: Decide se um pedido de alocação de recursos pode ser atendido. Esse controle é feito pelo roteador para determinar se um novo fluxo pode ter sua QoS garantida sem afetar fluxos anteriormente garantidos.

Classificador: O roteador classifica e coloca os pacotes em uma fila específica em função do resultado da classificação. A classificação utilizada é Multicampo (MF - *Multifield*), baseado no conteúdo de alguns campos do cabeçalho IP como endereço de origem, endereço de destino, byte ToS (*Type of Service*), etc. Os pacotes de uma mesma classe recebem o mesmo tratamento no escalonador.

Escalonador: Seleciona os pacotes para transmissão de modo a satisfazer os requisitos de QoS. O gerenciamento da transmissão é feito através do uso de um conjunto de filas e temporizadores.

A arquitetura IntServ não oferece bom desempenho em redes de grande porte. O principal motivo é a baixa escalabilidade dessa tecnologia, pois a quantidade de informações de estado de tráfego nos roteadores cresce com o aumento do número de fluxos. Como os

grandes *backbones* trabalham com grandes taxas de fluxos, a quantidade de informações que devem receber tratamento torna impraticável o uso do IntServ.

2.6.2. Serviços Diferenciados (DiffServ)

As redes DiffServ têm como objetivo oferecer um tratamento diferenciado aos pacotes. Diferentes níveis de serviço são estabelecidos através de um contrato (SLA – *Service Level Agreement*) estabelecido entre o usuário e o provedor local. Este contrato é estabelecido estaticamente ou dinamicamente, e especifica as garantias mínimas de QoS para aplicações dos usuários. Caso o tráfego não esteja em conformidade com o contratado, poderá sofrer atrasos ou simplesmente ser descartado.

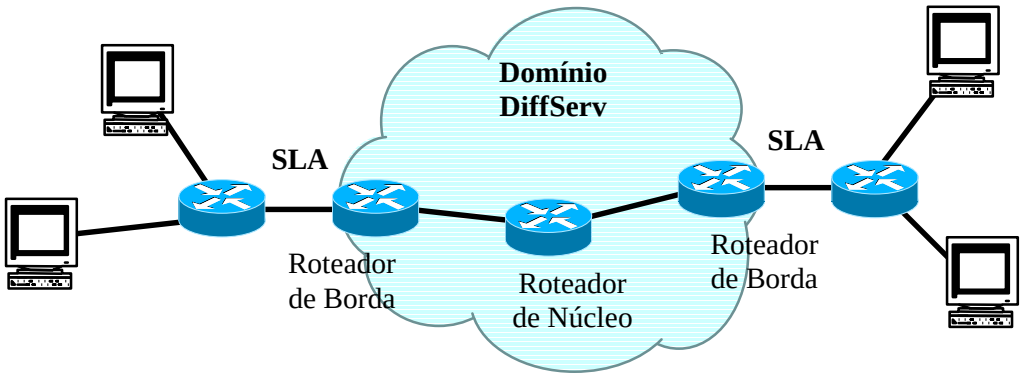


Figura 2.2 - Arquitetura DiffServ

Na arquitetura DiffServ não existe alocação de recursos e não é feita sinalização, permitindo assim uma maior escalabilidade e baixa sobrecarga de sinalização. Um domínio DiffServ é formado por roteadores de borda e roteadores de núcleo. Os roteadores de borda são responsáveis pela classificação e condicionamento do tráfego, enquanto que os roteadores de núcleo encaminham os pacotes de acordo com a classe de serviço definida.

A informação necessária para prover diferenciação nos pacotes é armazenada no campo ToS (*Type of Service*) do cabeçalho dos pacotes IPv4, ou no campo *Traffic Class* do cabeçalho dos pacotes IPv6. Estes campos são denominados DSCP (*DiffServ Code Point*), conforme mostrado na Figura 2.3.

Figura 2.3 - Campo DSCP

São definidas classes de serviço através do PHB (*Per Hop Behavior*), que define como os equipamentos se comportam com relação aos pacotes. Há várias propostas para tipos de PHBs, porém há basicamente dois tipos padronizados: Encaminhamento Expresso (*EF - Expedited Forwarding*) e Encaminhamento Assegurado (*AF - Assured Forwarding*), documentados nas RFCs (*Request for Comments*) 2598 [27] e 2597 [28] respectivamente. Além desses dois, há o PHB BE para o encaminhamento de tráfego *best effort*, pois o DiffServ deve ser compatível com as implementações já definidas e em funcionamento.

A classe de serviço EF provê o maior nível de qualidade de serviço. A idéia é emular uma linha dedicada convencional minimizando o atraso, a probabilidade de perda e o *jitter* para os pacotes. Em condições normais, a rede não oferece congestionamento para o tráfego EF, porém são utilizados mecanismos para descartar pacotes em excesso. Este serviço foi denominado inicialmente de *Premium Service*, sendo destinado para aplicações em tempo real que apresentam uma taxa máxima ou constante. Entre os aplicativos que se utilizam da classe EF, destacam-se a voz sobre IP e a transmissão de vídeo. O codepoint recomendado pelo IETF é 1 0 1 1 1 0.

Já a classe de serviço AF emula um comportamento semelhante a uma rede com pouca carga mesmo durante a ocorrência de congestionamento. São definidas quatro classes de serviços com três níveis de prioridade de descarte. O padrão recomendado para o PHB AF é mostrado na Tabela 2.2, onde os três primeiros bits definem a classe, enquanto que os bits restantes determinam o nível de descarte. Aplicações sensíveis ao tempo de resposta, como transações bancárias, são empregadas nesse tipo de serviço.

Tabela 2.2 - *Codepoints* do serviço AF

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

O serviço BE não oferece nenhuma garantia de encaminhamento de pacotes. Os datagramas que não são marcados com *codepoints* EF ou AF são enviados como tráfego BE, cujo padrão é 0 0 0 0 0 0. As aplicações que geralmente estão relacionadas a este serviço são o FTP (*File Transfer Protocol*) e WWW (*World Wide Web*).

A arquitetura DiffServ envolve um conjunto de mecanismos com o objetivo de garantir um tratamento diferenciado aos pacotes. As funções destes mecanismos consistem em: classificação, monitoração, marcação, descarte, enfileiramento, retirada das filas e moldagem dos pacotes. Os roteadores de borda possuem um conjunto completo de funcionalidades DiffServ, enquanto que os roteadores de núcleo possuem um conjunto menor de blocos. A Figura 2.4 mostra o diagrama geral do modelo DiffServ.

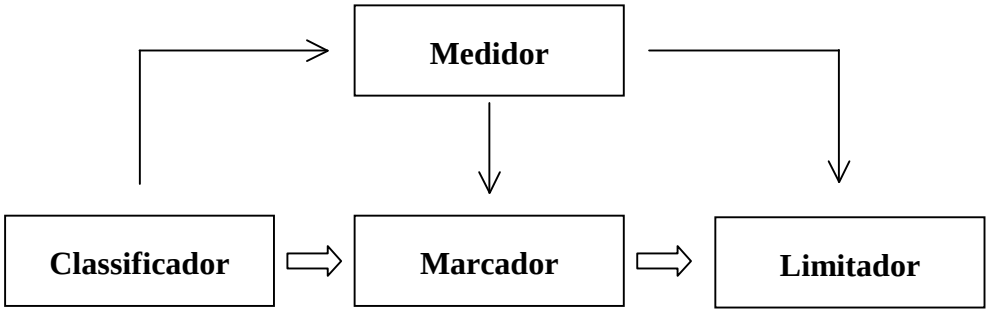


Figura 2.4 - Estrutura do Modelo DiffServ

Classificador: Classifica os pacotes em classes de tráfego. Este bloco utiliza o princípio do comportamento agregado (BA - *Behavior Aggregate*), onde são consideradas apenas classes de tráfego ao invés de fluxos isolados. A classe de tráfego de cada pacote é marcada na primeira seção do *codepoint*, não sendo mais alterada por nenhum outro roteador.

Medidor: O pacote classificado é enviado ao bloco medidor que o compara com um perfil de tráfego a fim de verificar a conformidade com os requisitos de SLA. Este bloco funciona com o auxílio de mecanismos denominados *Token Buckets* (TB). O sistema emite periodicamente "permissões" de maneira que o pacote recebido é comparado com a quantidade de permissões disponível em seu TB.

Marcador: Com o resultado dessa comparação, o pacote é marcado com uma prioridade de descarte igual ou maior à sua prioridade de descarte inicial. O marcador altera apenas a prioridade de descarte do pacote (segunda parte do *codepoint*), mantendo a classe intacta.

Limitador: Esta etapa é responsável em manter os pacotes em conformidade com o perfil de tráfego contratado. Para evitar congestionamentos, os pacotes com prioridade alta ou média de descarte são descartados primeiramente em relação aos de prioridade baixa. Os pacotes não descartados são armazenados em filas diferentes, de acordo com sua classe de

tráfego. Finalmente, mecanismos de esvaziamento de filas (*dequeueing*) realizam a moldagem do tráfego, através do atraso ou descarte de alguns pacotes.

2.6.3. *MultiProtocol Label Switching* (MPLS)

O MPLS não foi criado para o suporte à Qualidade de Serviço. Seu principal objetivo está em permitir uma rápida comutação dos pacotes, através do uso de rótulos ao invés do encaminhamento baseado no cabeçalho IP. Pela sua facilidade em prover Engenharia de Tráfego, além da possibilidade de configurar LSPs com requisitos de QoS através da integração das arquiteturas IntServ e DiffServ, seu uso tem se tornado muito difundido nas redes *backbone*.

O MPLS é uma padronização de diversas técnicas de comutação por rótulos em redes IP, implementadas nos últimos anos através de soluções de diversos fabricantes como a IP *switching* (Ipsilon), a ARIS (IBM) e a *tag switching* (Cisco), para citar-se algumas. Uma das principais características do MPLS é permitir que o roteamento seja implementado de forma independente do encaminhamento, que corresponde ao mecanismo de escolha da interface de saída por onde cada pacote deve ser transmitido. Desta forma, pode-se restringir o cálculo das rotas somente a alguns pontos, geralmente localizados na borda da rede. No núcleo, por sua vez, onde o processamento deve ser mais simples e eficiente, pode-se implementar o encaminhamento baseado apenas na leitura dos rótulos MPLS.

Pacotes que seguem a mesma rota pertencem à mesma classe de encaminhamento ou FEC (*Forward Equivalence Class*). Uma FEC pode ser representada por um endereço de rede destino ou por um prefixo do mesmo. O MPLS torna possível a associação de rótulos a FECs. A partir da identificação da FEC ao qual um pacote pertence, normalmente realizada pelo roteador de borda de entrada do domínio MPLS, um rótulo é acrescentado ao mesmo. Os roteadores do domínio, chamados de LSRs (*Label Switching Router*s) na nomenclatura

MPLS, encaminham os pacotes simplesmente a partir da leitura e análise do rótulo. Cabe aos LSRs de borda de saída do domínio MPLS a retirada do referido rótulo e a entrega dos pacotes originais ao destino.

Um rótulo MPLS tem tamanho fixo e significado local em cada LSR. Esta estrutura, mostrada na Figura 2.5, possui os seguintes campos: um rótulo de 20 bits, um campo EXP de 3 bits, um campo S de 1 bit para indicar se o rótulo é o último de uma pilha e um campo TTL de 8 bits.

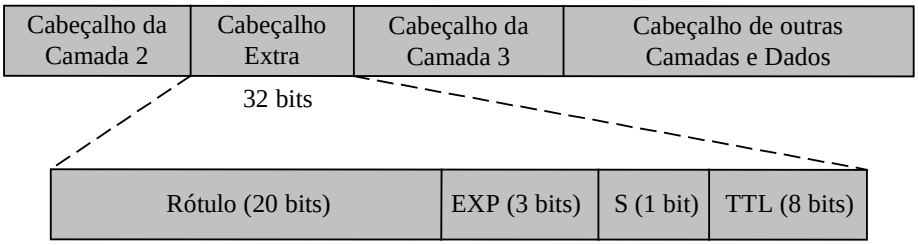


Figura 2.5 - Formato do Rótulo MPLS

O rótulo pode ser acrescentado ao pacote IP, ou embutido ao cabeçalho de um quadro. É possível ainda utilizar os campos VPI/VCI (*Virtual Path Identifier / Virtual Channel Identifier*) das células ATM e o campo DLCI (*Data Link Connection Identifier*) de um quadro Frame-Relay para a adaptação do rótulo MPLS.

A associação de rótulos a FECs deve ser acordada entre LSRs vizinhos, o que pode ser feito estaticamente ou dinamicamente. Na associação estática, os mapeamentos são configurados manualmente pelo administrador do domínio, em contraste com a associação dinâmica, onde as configurações são realizadas por intermédio de um protocolo de sinalização. Cabe ao LSR que recebe o tráfego, normalmente chamado de *downstream* LSR, criar e informar as associações de rótulos ao LSR que envia o tráfego, denominado de *upstream* LSR [29].

Um LSP (*Label Switched Path*) é um caminho virtual estabelecido através do núcleo da rede MPLS que define uma rota de encaminhamento para os pacotes, desde o ponto de entrada até o ponto de saída. Sendo assim, o LSP é formado por meio do uso de uma seqüência de rótulos em cada nó ao longo do caminho compreendido entre a origem e o destino.

LDP (*Label Distribution Protocol*) é o protocolo que determina como os nós MPLS se comunicam e ligam os rótulos. É um conjunto de procedimentos e mensagens onde os LSRs estabelecem os LSPs da rede. À medida que o LDP distribui rótulos para uma dada FEC, cria-se uma conexão fim a fim para o envio de pacotes. Dois LSRs que se comunicam para a troca de informações de rótulos são denominados LSRs pares (*LSR peers*), e diz-se haver uma sessão LDP entre eles. O LDP possui quatro categorias de mensagens:

Mensagens de Descoberta

Empregadas para anunciar a presença de um LSR em uma rede e ratificar que o LSR continua presente.

Mensagens de Sessão

Usadas para estabelecer, manter e terminar sessões LDP entre dois LSRs.

Mensagens de Anúncio

Utilizadas para criar, modificar e suprimir associações rótulo-FEC.

Mensagens de Notificação

Para prover informações de estado da rede e sinalizar erros.

O MPLS não define um único método de distribuição de rótulos, pois protocolos já existentes como BGP (*Border Gateway Protocol*) ou RSVP (*Resource Reservation Protocol*) estendido também podem ser usados.

Outro método disponível é o CR-LDP (*Constraint-Based Routed LDP*), que adiciona características ao LDP com o objetivo de implementar Engenharia de Tráfego. A engenharia de tráfego preocupa-se com a otimização da performance nas redes operacionais, com um processo que melhora a utilização da rede através de uma distribuição uniforme e diferenciada do tráfego. Utiliza-se a engenharia de tráfego para se alcançar os requisitos de qualidade de serviço, através da escolha de caminhos diferenciados para os fluxos de dados, visando minimizar atrasos e congestionamentos.

As restrições do CR-LDP são parâmetros passados para os LSRs nas requisições de atribuição de rótulos, a fim de determinar se eles podem fornecer a qualidade desejada. Esses parâmetros são: ER (*Explicit Route*), onde pode-se indicar um conjunto de nós a serem seguidos; Tráfego (*Traffic Parameters*); Preempção (*Preemption*); LSP-ID; Classes de Recursos (*Resource Class*) e *Route Pinning*.

Outros componentes da tecnologia MPLS são:

NHLFE (*Next Hop Label Forwarding Entry*)

Contém informações a serem aplicadas à pilha de rótulos de um pacote, como o endereço do próximo roteador, ou informações sobre a troca de rótulos do topo da pilha.

LM (*Incoming Label Mapping*)

Implementado nos roteadores de núcleo, pois é utilizado apenas para pacotes já rotulados. Cada rótulo que entra no domínio é mapeado em uma NHLFE.

FTN (*FEC-to-NHLFE*)

Implementado pelos roteadores de borda em pacotes não rotulados. Faz o mapeamento de cada FEC em uma entrada NHLFE.

2.7. Conclusões

O crescimento do tráfego de aplicações multimídia nas redes IP fez com que aumentasse a demanda por soluções de Qualidade de Serviço (QoS). A obtenção de QoS requer o controle do *jitter* e do atraso, e a disponibilização de vazão e minimização de perdas de pacotes dos fluxos de tráfego. Através de um gerenciamento eficiente dos recursos de rede, os objetivos de QoS podem ser alcançados ao invés da simples adição de largura de banda. Diversas propostas estão sendo desenvolvidas pelo IETF, dentre os quais destacam-se o IntServ, o DiffServ e o MPLS.

A utilização da arquitetura IntServ permite uma maior granularidade na gerência dos recursos, porém em redes de grande porte se torna muito complexa, visto que cada fluxo de dados é tratado individualmente. A arquitetura DiffServ coloca a complexidade de processamento nos roteadores de borda responsáveis pela classificação dos pacotes, permitindo a agregação de fluxos de dados em classes e aprimorando a escalabilidade no núcleo da rede. A proposta MPLS também tem como requisito alocar a complexidade de processamento nos roteadores de borda, permitindo uma maior escalabilidade, além de facilitar a implementação de engenharia de tráfego.

As arquiteturas propostas apresentam características adequadas para situações específicas. Porém, uma única solução para a obtenção de QoS não é capaz de alcançar seu objetivo, considerando a enorme quantidade de tecnologias e aplicações existentes em uma rede IP. Atualmente, diversas pesquisas estão sendo feitas para se buscar soluções que integrem essas tecnologias, tendo como objetivo agregar seus pontos positivos, resultando em uma solução mais abrangente.

CAPÍTULO 3

ENGENHARIA DE TRÁFEGO EM REDES MPLS COM DIFFSERV (DS-TE)

3.1. Introdução

Atualmente, a maioria das redes *backbone* utiliza algoritmos de roteamento IGP *(Interior Gateway Protocol*), como o OSPF (*Open Shortest Path First*) ou IS-IS *(Intermediate Station to Intermediate Station*), no mapeamento dos fluxos de tráfego para o encaminhamento de pacotes. Porém, essas soluções são caracterizadas pelo envio de tráfego pelo caminho mais curto, ocasionando o congestionamento de alguns enlaces, enquanto outros ficam ociosos. Uma solução utilizada em caso de congestionamento é o simples aumento da capacidade dos enlaces. Entretanto, o aumento do tráfego observado nos últimos anos e a necessidade de uma eficiência maior na utilização dos recursos de rede gerou a necessidade de se introduzir conceitos de engenharia de tráfego para otimizar a utilização dos *backbones*.

A arquitetura DiffServ vem sendo muito utilizada pelos ISPs (*Internet Service Providers*) que buscam oferecer um tratamento diferenciado aos diversos fluxos de pacotes, através do uso de classes de serviços de acordo com alguns parâmetros de QoS, como vazão, atraso, *jitter*, etc. O rótulo DiffServ (DSCP - *DiffServ Codepoint*) define algumas classes de

serviços através de PHBs (*Per-Hop Behavior*), que informam como os equipamentos se comportam em relação aos pacotes. Os tipos de PHBs padronizados são: Encaminhamento Expresso (EF - *Expedited Forwarding*), Encaminhamento Assegurado (AF - *Assured Forwarding*) e o PHB BE, para encaminhamento de tráfego *best effort*. A classe de serviço EF provê o maior nível de qualidade de serviço, minimizando os atrasos, a probabilidade de perda e o *jitter* dos pacotes. Já a classe de serviço AF emula o comportamento de uma rede com pouca carga mesmo durante a ocorrência de congestionamento. São definidas quatro classes de serviço AF com três níveis de prioridade de descarte [30].

A crescente necessidade de redes que suportem QoS exige a integração de novas arquiteturas, onde destacam-se o MPLS e o DiffServ. Um dos principais benefícios alcançados com a implementação do MPLS é o suporte para a engenharia de tráfego. Isto é possível através da criação de túneis LSPs na rede para encaminhamento de tráfego. O pacote IP, ao entrar em uma rede MPLS, recebe um rótulo que estabelece o caminho completo a ser seguido ao invés do encaminhamento baseado pelo prefixo utilizado no roteamento IP tradicional. Com isso, é possível criar rotas diferentes daquelas de menor custo determinado pelo IGP.

As redes MPLS/DiffServ são usadas por alguns ISPs para suportar de forma escalável múltiplas classes de serviços nas redes, otimizando os recursos de transmissão através da engenharia de tráfego em nível de classes (*per-class*). Para alcançar esse objetivo, a engenharia de tráfego agrega fluxos de tráfego pertencentes à mesma classe, ou seja, o tráfego entre um ponto de entrada na rede e outro de saída e mesma FEC (*Forwarding Equivalence Class*). Esse conjunto de fluxos é denominado *Traffic Trunk* [31].

Os benefícios alcançados com a implementação de engenharia de tráfego em redes MPLS/DiffServ focam ambientes onde os recursos são escassos, ou que possuem um volume significativo de tráfego sensível a atraso. O mapeamento do tráfego de uma classe de serviço

DiffServ em um LSP, permite que este tráfego utilize os recursos disponíveis em rotas que tenham as mesmas restrições específicas a esta classe. Isso é denominado "Engenharia de Tráfego em Redes MPLS com Serviços Diferenciados" (DS-TE, *DiffServ-aware MPLS Traffic Engineering*) [04].

3.2. Serviços Diferenciados em Redes MPLS

A RFC 3270 [32] descreve os mecanismos para o suporte de serviços diferenciados em redes MPLS. DiffServ e MPLS têm alguns pontos em comum. As duas tecnologias colocam a complexidade do processamento nos roteadores de borda da rede. Ambas rotulam os pacotes após classificá-los, onde os rótulos são chamados rótulos MPLS em uma rede MPLS e DSCP em uma rede DiffServ. Os roteadores internos encaminham os pacotes de acordo com as informações dos rótulos.

No DSCP é feito o mapeamento de alguns procedimentos para encaminhar os pacotes que os nós da rede devem adotar, definindo a classe e a prioridade de descarte desses pacotes. O rótulo MPLS determina o LSP em que o pacote deve ser encaminhado. A utilização conjunta dessas duas tecnologias permite garantir QoS em uma rede, através da determinação do caminho que os pacotes devem seguir e o tipo de tratamento dos mesmos em cada roteador.

Os roteadores MPLS não examinam o conteúdo do cabeçalho IP, ficando restritos apenas ao conteúdo dos rótulos. Porém, o DSCP está alocado dentro do cabeçalho IP. Assim, a informação contida no DSCP deve ser mapeada no rótulo MPLS para cada pacote que entre no domínio. Outra dificuldade reside no fato de que o DSCP tem 6 bits mas o campo EXP do rótulo MPLS possui apenas 3 bits. Existem dois modelos propostos que determinam como os pacotes marcados com um determinado PHB são encaminhados em uma rede MPLS. As

soluções diferem basicamente no posicionamento da informação PHB no rótulo MPLS, e denominam-se: E-LSP (*EXP Inferred LSP*) e L-LSP (*Label-Only Inferred LSP)* [32].

3.2.1. E-LSP (*EXP Inferred LSP*)

Na primeira abordagem, os 3 bits do campo EXP do rótulo MPLS são utilizados como suporte ao DiffServ, podendo estabelecer no máximo 8 classes de serviço. O campo DSCP permite implementar uma quantidade maior de classes, porém esta limitação não inviabiliza o suporte do DiffServ em redes MPLS, pois no contexto atual da Internet 8 classes de serviço possibilitam um bom nível de diferenciação. Os E-LSPs utilizam apenas um LSP para a diferenciação de tráfego [33].

Na Figura 3.1, o roteador de ingresso determina o rótulo e o LSP através do cabeçalho do pacote, mapeando o campo DSCP diretamente no campo EXP. Todos os LSRs do domínio MPLS encaminham o pacote baseado em seu campo EXP, através da utilização de filas específicas para cada classe de serviço, assegurando a diferenciação de tráfego dentro de um mesmo LSP.

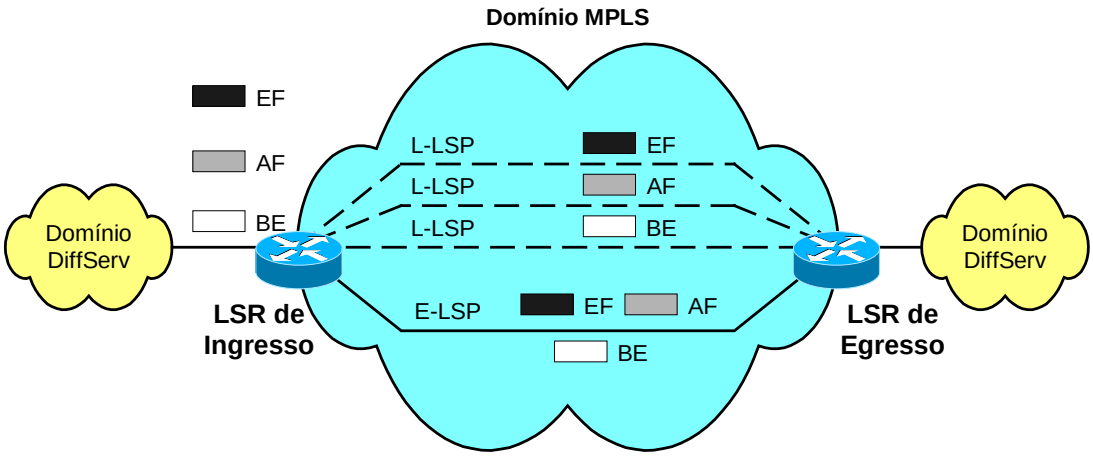


Figura 3.1 - LSPs em uma rede MPLS/DiffServ

O mapeamento do PHB DiffServ no campo EXP do rótulo MPLS pode ser feito de forma estática ou através da propagação de mensagens do protocolo de sinalização. A Tabela 3.1 descrita em [34], mostra uma possibilidade de mapeamento entre as classes DiffServ e o conteúdo do campo EXP do rótulo MPLS para obter classes de serviço equivalentes. Como as oito classes possíveis em uma rede MPLS oferecem uma granularidade menor que as classes DiffServ, deve-se agrupar fluxos de pacotes com características semelhantes em uma mesma classe de serviço MPLS.

Tabela 3.1 - Mapeamento DiffServ/MPLS

DiffServ		**MPLS**	
PHB	**DSCP**	**EXP**	**Classe**
EF	101110	111	Premium
AF11	001010	110	Ouro
AF12	001100	101	
AF13	001110		
AF21	010010	100	Prata
AF22	010100	011	
AF23	010110		
AF31	011010	010	Bronze
AF32	011100	001	
AF33	011110		
AF41	100010		
AF42	100100		
AF43	100110		
BE	000000	000	Best-Effort

Como é feito o mapeamento direto do campo DSCP nos 3 bits EXP do rótulo MPLS, essa solução não pode ser utilizada em redes ATM ou Frame-Relay, devido a inexistência do campo EXP quando da implementação do MPLS.

3.2.2. L-LSP (*Label-Only Inferred LSP*)

Neste modelo, utiliza-se bits localizados no próprio rótulo MPLS para se codificar o PHB. Assim, é possível implementar até 2^n $(1 \leq n \leq 6)$ classes de serviço, sendo n o número de bits utilizados. Cada classe de serviço é servida por um LSP. A Figura 3.1 ilustra uma rede com 3 L-LSPs, um para cada classe de serviço e com prioridades específicas [33].

Esta solução é utilizada em redes onde é necessário mais que oito classes de serviço, ou em redes como o ATM e Frame-Relay, onde não é utilizado o campo EXP. Quando o MPLS trabalha em conjunto com o ATM, o bit CLP (*Cell Loss Priority*) é usado como campo de diferenciação de serviços, enquanto que no Frame-Relay o campo DE é utilizado. O tamanho pequeno destes campos limitam sua utilização quando muitos fluxos devem ser mapeados. Por exemplo, como o campo CLP tem apenas 1 bit, no ATM são suportadas apenas duas classes de serviço.

Os LSPs são formados a partir do mapeamento direto dos rótulos às FECs, efetuadas pelos LSRs de borda, levando-se em conta os PHBs que devem ser associados aos mesmos. Para cada classe de serviço é formado um LSP, o que aumenta a complexidade de gerenciamento por parte dos LSRs.

Isto pode levar a um grave problema de escalabilidade. Em uma rede com três PHBs diferentes, o número de rótulos necessários é multiplicado por três. Serão necessários três rótulos diferentes indicando o mesmo LSP, mas com diferentes níveis de prioridade. Assim, a manutenção desse conjunto de rótulos irá se tornar um problema caso o número de PHBs aumente.

3.2.3. Distribuição de Rótulos em Redes MPLS/DiffServ

Há diversos protocolos responsáveis pela distribuição de rótulos em uma rede MPLS/DiffServ. Protocolos que já estão em uso em uma rede MPLS podem ser adaptados

para essa nova tarefa, através do acréscimo de informações trocadas entre os roteadores. Outra solução é implementar um protocolo com a tarefa específica de distribuir rótulos, como o LDP (*Label Distribution Protocol*) [35].

Algumas extensões foram definidas no protocolo RSVP (*Resource Reservation Protocol*), permitindo implementar engenharia de tráfego e o estabelecimento de LSPs. Se uma rede já utiliza o RSVP, esta solução pode evitar a implementação de um novo protocolo, economizando recursos de rede. Como as mensagens RSVP permitem o estabelecimento de LSPs e reserva de recursos ao mesmo tempo, há uma redução no tráfego de rede específico para esse fim.

LDP é um protocolo desenvolvido especificamente para a distribuição de rótulos MPLS entre LSRs. Com algumas extensões, o LDP pode ser usado para estabelecer LSPs com requisitos de QoS. O LDP implementado com essas extensões é conhecido como CR-LDP (*Constraint-based Routed LDP*), permitindo o uso de engenharia de tráfego em redes MPLS e definindo as características de tráfego de um LSP. O estabelecimento de um LSP é um processo bem simples: uma requisição e um mapeamento.

3.2.3.1. CR-LDP (Constraint-based Routed Label Distribution Protocol)

CR-LDP é um conjunto de extensões do protocolo LDP, com o objetivo de facilitar o roteamento baseado em restrições de LSPs. Da mesma forma que o LDP, utiliza sessões TCP (*Transmission Control Protocol*) entre LSRs pares e envia mensagens de distribuição de rótulos durante as sessões. Isso permite uma distribuição confiável das mensagens de controle [36].

O processo de criação de um novo LSP é mostrado na Figura 3.2. O roteador de ingresso LSR A determina a necessidade de um novo LSP em direção ao LSR C. LSR A constrói uma mensagem LABEL_REQUEST especificando a rota desejada (B-C) e os parâmetros de tráfego requisitados para a nova rota. O LSR A reserva os recursos necessários para o novo

LSP, e então encaminha a mensagem LABEL_REQUEST para o LSR B através de uma sessão TCP [36].

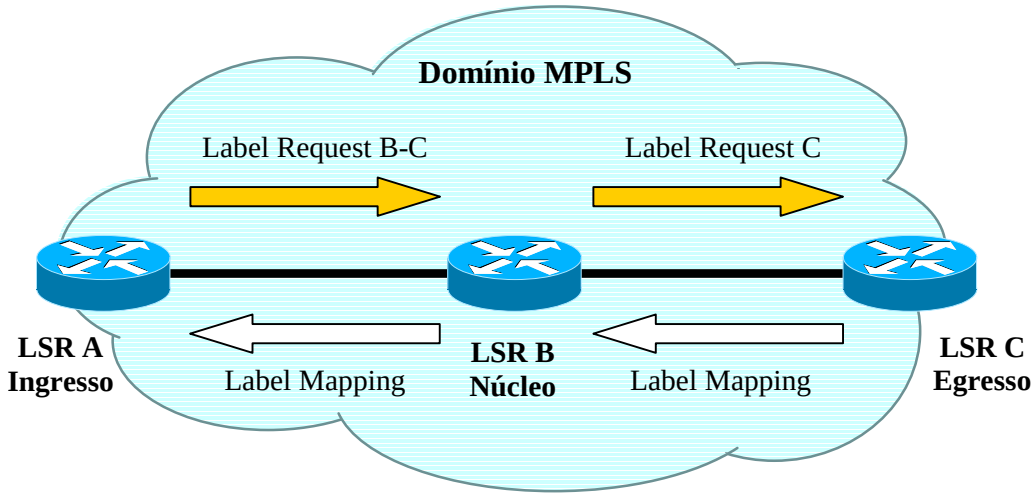


Figura 3.2 - Funcionamento do CR-LDP

O roteador B recebe a mensagem LABEL_REQUEST e verifica que não é o roteador de egresso deste LSP, encaminhando a mensagem ao próximo roteador especificado. Faz a reserva de recursos solicitados pelo novo LSP, modifica a mensagem com a nova rota e encaminha ao roteador C.

O LSR C determina que é o roteador de egresso, efetuando a reserva de recursos para o novo LSP. Aloca um rótulo para o novo LSP e encaminha o rótulo ao roteador B através de uma mensagem LABEL_MAPPING, que contém detalhes dos parâmetros de tráfego reservados ao novo LSP [36].

LSR B recebe a mensagem LABEL_MAPPING e compara com a solicitação original da mensagem LABEL_REQUEST. Finaliza a reserva e aloca um rótulo para o novo LSP. Além disso, atualiza a tabela NHLFE (*Next Hop Label Forwarding Entry*) e distribui o novo rótulo para o LSR A através de uma mensagem LABEL_MAPPING. O processo no roteador A é

semelhante, com a diferença que não é necessário alocar um novo rótulo, pois o LSR A é o roteador de ingresso do novo LSP [36].

3.2.3.2. RSVP-TE (Resource Reservation Protocol - Traffic Engineering)

O RSVP utiliza a troca de mensagens para reservar recursos para os fluxos de pacotes. RSVP-TE é uma extensão ao RSVP com o objetivo de distribuir rótulos MPLS, e assim implementar túneis LSP. Por utilizar UDP (*User Datagram Protocol*) na comunicação entre LSRs pares ao invés de sessões TCP, o protocolo deve ter a capacidade de gerenciar uma possível perda de mensagens de controle.

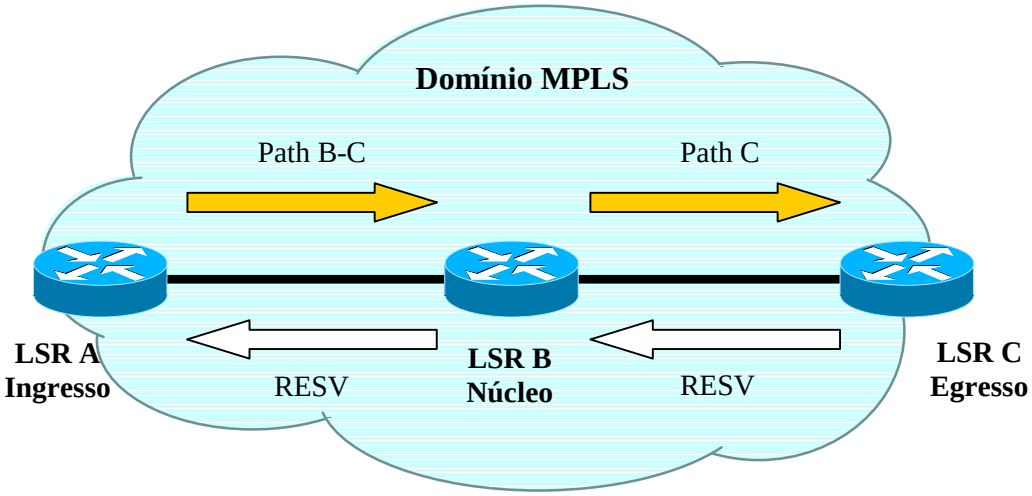


Figura 3.3 - Funcionamento do RSVP-TE

O processo de funcionamento do protocolo RSVP-TE é semelhante ao CR-LDP, e é ilustrado na Figura 3.3. O roteador de ingresso determina a necessidade de um novo LSP em direção ao LSR C. Através dos parâmetros de tráfego solicitados, o LSR A determina que a rota do novo LSP deve passar através do LSR B, e envia uma mensagem PATH com a rota determinada (B-C) e detalhes dos parâmetros de tráfego. A mensagem é enviada utilizando o protocolo UDP [13].

O LSR B verifica que não é o destino final da mensagem, e encaminha nova mensagem para o roteador C. LSR C determina que é o roteador de egresso para o novo LSP e reserva a largura de banda solicitada. Seleciona um rótulo e retorna uma mensagem RESV para o LSR B, contendo detalhes da largura de banda reservada e o rótulo vinculado ao novo LSP. Ao receber essa mensagem, o roteador B faz a reserva de recursos e encaminha nova mensagem RESV para o LSR A, contendo o valor do novo rótulo alocado. Finalmente, o roteador de ingresso A recebe a mensagem RESV e inicia a transmissão [13].

O protocolo RSVP-TE utiliza o mecanismo *soft-state* de retenção de LSPs. Já o protocolo CR-LDP mantém o caminho uma vez estabelecido até que uma requisição explícita seja feita, ou seja, é um mecanismo *hard-state*. Dentre outras diferenças, destacam-se a confiabilidade que o protocolo TCP oferece ao CR-LDP, e o sentido utilizado para a reserva de recursos, pois o CR-LDP reserva a largura de banda no encaminhamento das mensagens LABEL_REQUEST e o RSVP efetua a reserva no sentido reverso. A Tabela 3.2 apresenta uma análise comparativa entre os dois protocolos.

Tabela 3.2 - Análise comparativa entre CR-LDP e RSVP-TE

	CR-LDP	**RSVP-TE**
Transporte	TCP	UDP
Mecanismo de Retenção	*Hard State*	*Soft State*
Mecanismo de Refresh	Não necessário	Necessário
Confiabilidade em Falhas	Sim	Não
Aplicação	*Backbones*	*Backbones*
Escalabilidade	Sim	Sim

3.3. Engenharia de Tráfego em Redes MPLS

No roteamento IP tradicional, os roteadores tomam decisões independentes para encaminhar os pacotes. Quando um pacote chega, o roteador o encaminha de acordo com seu endereço de destino, devendo manter uma tabela de roteamento que especifique o próximo salto (*hop*) do pacote. As tabelas de roteamento podem ser estáticas ou dinâmicas, onde as tabelas estáticas são configuradas manualmente e as tabelas dinâmicas são modificadas de acordo com as mudanças na rede. Protocolos de roteamento mantêm as tabelas atualizadas e calculam a rota de encaminhamento. Os protocolos mais utilizados são: RIP (*Routing Information Protocol*), OSPF (*Open Shortest Path First*) e IS-IS (*Intermediate System to Intermediate System*) [37].

O congestionamento de enlaces é um dos principais problemas que podem afetar o desempenho das aplicações multimídia, podendo ocorrer devido a insuficiência ou má distribuição na utilização dos recursos. Caso o problema esteja na falta de recursos de rede, a única solução possível é a atualização da infra-estrutura para suportar os novos requisitos de tráfego. Porém, nas redes com má distribuição no uso dos recursos, a principal solução utilizada é a engenharia de tráfego.

Nas redes IP tradicionais, o tráfego é encaminhado pela rota mais curta até o destino, utilizando-se o número de saltos que os pacotes terão até o destino. Este tipo de algoritmo facilita o congestionamento de alguns enlaces da rede, enquanto que outros enlaces ficam ociosos. A engenharia de tráfego permite o balanceamento dos pacotes entre as diversas rotas possíveis.

Os protocolos de roteamento tradicionalmente utilizados, como o OSPF, possuem extensões que permitem implementar uma forma rudimentar de engenharia de tráfego. Porém, essa solução não é adequada porque o protocolo não considera o estado dos enlaces, permitindo ainda a ocorrência de congestionamentos.

Devido à inadequação dos protocolos IGP na engenharia de tráfego, soluções envolvendo IP sobre ATM ou IP sobre Frame-Relay vêm sendo implantadas. Essas soluções montam circuitos virtuais (VC - *Virtual Circuits*), permitindo o roteamento desses circuitos através de restrições de tráfego. Porém, essas técnicas possuem problemas de escalabilidade.

Os problemas enfrentados nas redes que utilizam as soluções descritas acima estão sendo solucionados com a introdução do MPLS. Os componentes e requisitos para a realização de engenharia de tráfego em redes MPLS são definidos pela RFC 2702 [05]. Dentre os principais tópicos abordados, o documento engloba soluções para o encaminhamento dos pacotes, a seleção de caminhos e os protocolos de distribuição de pacotes.

3.3.1. Traffic Trunks

Os pacotes inseridos em um domínio MPLS são mapeados em FECs (*Forwarding Equivalence Class*). FECs com características semelhantes são mapeados em troncos de tráfego (*Traffic Trunks*), que por sua vez são mapeados em LSPs.

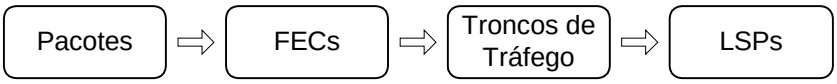


Figura 3.4 - Mapeamento de Pacotes em LSPs

Os troncos de tráfego são uma agregação de fluxos de tráfego que pertencem a uma mesma classe e são encaminhados por um mesmo caminho através da rede. Um tronco de tráfego é uma representação abstrata de tráfegos com características específicas, e pode ser comparado com os circuitos virtuais das redes *Frame-Relay* e ATM. Os troncos de tráfego encapsulam o tráfego entre o LSR de ingresso até o LSR de egresso. É importante observar

que um tronco de tráfego não é mapeado de forma definitiva em um LSP, podendo ser movimentado entre LSPs diferentes.

Troncos de tráfego são unidirecionais, porém é possível implementar um tronco bidirecional (BTT - *Bidirectional Traffic Trunk*) através do uso de dois troncos com direções diferentes. Ambos troncos são implementados e finalizados juntos, e não podem existir sozinhos. É possível que os troncos sejam mapeados em diferentes caminhos através do uso de dois LSPs, sendo denominados troncos bidirecionais assimétricos. Caso os troncos percorram o mesmo caminho, são denominados simétricos.

O entendimento do modo de operação de um tronco de tráfego é fundamental para a implementação de engenharia de tráfego. As principais operações envolvem o estabelecimento, ativação, desativação, modificação de atributos, re-roteamento e finalização. Um tronco de tráfego é inicialmente criado através da operação de estabelecimento, porém os pacotes não podem ser encaminhados pelo tronco de tráfego até que a operação de ativação seja finalizada. Caso a rota utilizada tenha que ser alterada, utiliza-se o processo de re-roteamento através do uso de protocolos específicos. Quando a fonte de tráfego termina a transmissão é implementada a operação de finalização liberando a largura de banda [38].

O comportamento de um tronco de tráfego é determinado por alguns parâmetros definidos na RFC 2702 [05]. Dentre os parâmetros mais importantes especificados, encontra-se o atributo de tráfego que determina as características (taxa de pico, taxa permitida, etc) dos fluxos de tráfego encaminhados pelo tronco. O atributo de prioridade determina a importância de um tronco em relação aos demais. O atributo de preempção (*preemption*) determina regras que permitem a apropriação de troncos menos importantes pelos mais importantes, com o objetivo de liberar largura de banda. Outro atributo é o gerenciamento e seleção de caminhos, podendo ser estabelecido estaticamente ou dinamicamente.

3.3.2. Roteamento Baseado em Restrições

O objetivo da engenharia de tráfego é encontrar um caminho dentro da rede que suporte as restrições solicitadas pelas aplicações. Assim, essas restrições devem ser consideradas quando do cálculo da rota, desde a origem até o destino. Algumas restrições utilizadas são: a largura de banda solicitada para um LSP, as características dos enlaces que permitam o encaminhamento correto do tráfego (por exemplo, o atraso), o número de saltos permitidos para o tráfego e a prioridade do LSP em relação aos demais.

Para se calcular o caminho que satisfaça essas restrições, é necessário que as informações sobre a disponibilidade ou não dos recursos solicitados sejam distribuídas para todos os roteadores. Isto significa que as propriedades dos enlaces devem ser distribuídas por toda a rede. Isto é possível através da adição de extensões aos protocolos IS-IS ou OSPF, permitindo o envio de informações sobre o estado do enlace, como largura de banda, atraso, etc [39].

Com esta informação disponível, uma versão modificada do algoritmo *SPF (Shortest Path First*), denominada CSPF (*Constrained SPF*), pode ser usada pelo roteador de ingresso para calcular uma rota que atenda às restrições solicitadas.

No exemplo da Figura 3.5, todos os enlaces tem 10 Mbps, e um LSP de 7 Mbps já está estabelecido na rota A-B-E. A única restrição utilizada é a largura de banda necessária para a transmissão dos pacotes. Dessa forma, caso um novo LSP necessite mais que 3 Mbps, não poderá ser estabelecido na rota de menor custo A-B-E. O algoritmo CSPF deve então alocar o novo LSP em uma rota alternativa, mesmo com um custo total maior que a anterior, desde que atenda à solicitação de largura de banda. Nesse caso, a rota escolhida será entre os roteadores A-C-D-E.

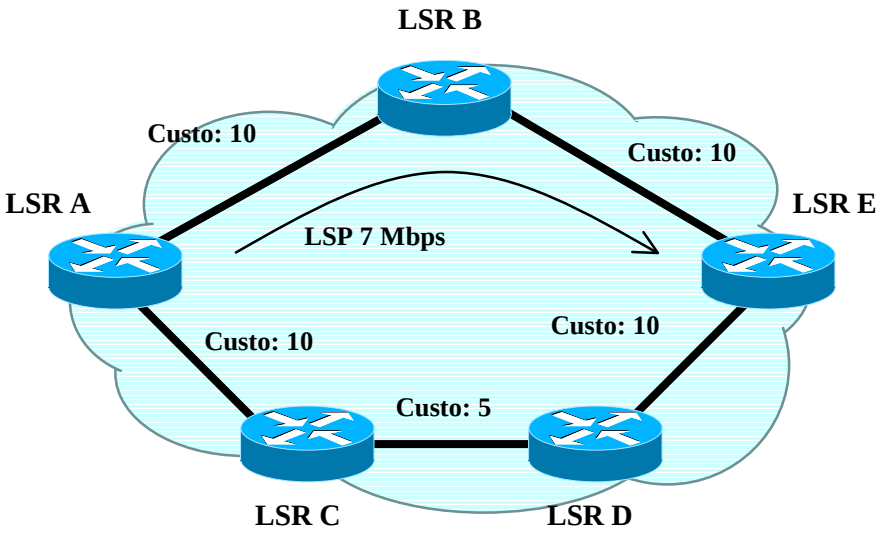


Figura 3.5 - Cálculo de rota utilizando CSPF

Finalmente, após o caminho ter sido calculado, um protocolo de distribuição de rótulos (CR-LDP ou RSVP-TE) é utilizado para o estabelecimento do novo LSP. Uma vez que esse novo LSP tenha sido implementado, os roteadores devem atualizar a informação sobre os recursos disponíveis.

3.4. Engenharia de Tráfego DS-TE

DiffServ é usado por alguns ISPs para suportar de forma escalável múltiplas classes de serviços nas redes. Em redes DiffServ onde deseja-se alcançar uma maior otimização dos recursos de transmissão e aprimorar a performance e eficiência, pode ser desejável realizar engenharia de tráfego em um nível de classes (*per-class*). Para alcançar esse objetivo, a engenharia de tráfego agrega fluxos de tráfego pertencentes à mesma classe, ou seja, o tráfego entre um ponto de entrada na rede e outro de saída e mesma FEC (*Forwarding Equivalence Class*). Esse conjunto de fluxos é denominado *Traffic Trunk*. O mapeamento do tráfego de uma das classes de serviço DiffServ em um LSP separado, permite a este tráfego utilizar os

recursos disponíveis em rotas que tenham as mesmas restrições específicas a esta classe. Isso é denominado como "Engenharia de Tráfego em Redes MPLS com Serviços Diferenciados" (DS-TE, *DiffServ-aware MPLS Traffic Engineering)* [04].

3.4.1. Cenários Aplicados

A RFC 3564 [04] apresenta alguns cenários que não podem ser solucionados com uma rede utilizando apenas DiffServ ou MPLS-TE. Estes cenários formam a base que estimulou o desenvolvimento da Engenharia de Tráfego em Redes MPLS / DiffServ (DS-TE).

O primeiro cenário envolve uma rede com dois tipos de tráfego: voz e dados. O objetivo é manter uma boa qualidade para o tráfego de voz, com um baixo índice de perda de pacotes, *jitter* e atraso, enquanto mantém o serviço do tráfego de dados. A solução da tecnologia DiffServ é o mapeamento do tráfego de voz em um PHB que garanta um nível baixo de atraso e *jitter*, como por exemplo o PHB EF. Porém, o atraso encontrado pelo tráfego de voz é a soma do atraso de propagação que o pacote sofre ao atravessar a rede e o atraso das filas encontradas em cada salto. O atraso de propagação é praticamente constante, resultando assim na necessidade de reduzir o atraso nas filas utilizadas. Um baixo atraso de enfileiramento precisa de uma fila pequena, que na prática significa que apenas uma proporção dos *buffers* implementados nas filas podem ser usados para tráfego de voz.

Assim, o requisito principal é a necessidade de limitar a proporção de tráfego de voz em cada enlace. No passado, os ISPs simplesmente aumentavam a largura de banda dos enlaces sempre que necessário. Esta solução, além de aumentar os custos devido a constante necessidade de incremento de capacidade, também é deficiente em casos de falhas em algum enlace. No exemplo da Figura 3.6, o tráfego de voz encaminhado pelo roteador A utiliza o enlace A-E, por ser a menor rota até o destino. Caso ocorra uma falha nesse enlace, o tráfego será roteado para a menor rota disponível, formada por A-B-E. Porém, o enlace B-E tem

menor capacidade que os outros, o que resultará em aumento da porcentagem de tráfego de voz encaminhado. A melhor solução para esse caso seria a escolha da rota A-C-D-E, que manteria a mesma relação entre tráfego de voz com os demais.

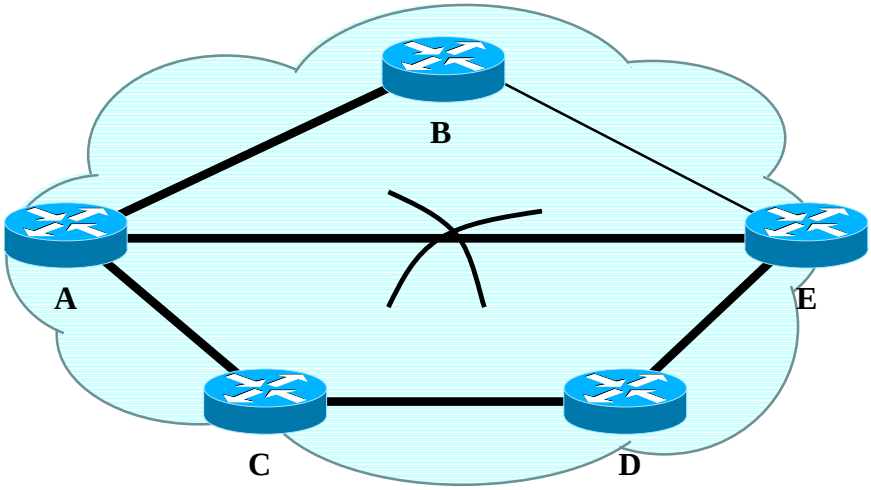


Figura 3.6 - Roteamento em caso de falha no enlace

Para se limitar a proporção de tráfego de voz em todos os enlaces, pode-se limitar a largura de banda disponível em um nível que satisfaça os parâmetros solicitados pelo tráfego de voz. A engenharia de tráfego é utilizada para garantir que todos os tráfegos sejam mapeados de forma a respeitar os limites impostos de largura de banda. Esta solução atinge o objetivo proposto mas desperdiça recursos, pois a largura de banda que poderia ser alocada para o tráfego com poucos requisitos de *jitter* e atraso fica indisponível. O problema reside no fato de que a engenharia de tráfego não consegue distinguir entre dois tipos de tráfego e não pode estabelecer restrições em um nível de granularidade por classe de tráfego.

O segundo cenário é uma extensão do primeiro, considerando uma rede que suporta três tipos de tráfego que são mapeados para três classes de serviço. O principal desafio é configurar o tamanho das filas e das políticas de escalonamento em cada enlace para assegurar que o PHB correto está sendo oferecido para cada classe. Torna-se impraticável

configurar esses parâmetros tendo como base o nível de carga do enlace em um certo tempo: mudanças na rota e falhas nos enlaces e roteadores são variáveis que podem ser alteradas de forma dinâmica. Uma solução possível é fixar a proporção de cada tráfego nos enlaces, alocando de forma proporcional o tamanho das filas e utilizando a engenharia de tráfego para forçar os tráfegos a obedecer o limite de recursos. Esta solução exige que sejam aplicadas diferentes restrições de largura de banda para diferentes classes de tráfego.

No terceiro cenário, há dois tipos de tráfego: *best effort* e serviço garantido. O tráfego de serviço garantido deve estar de acordo com um dado SLA (*Service Level Agreement*). O objetivo é prover o nível de serviço requisitado e também estar apto a implementar engenharia de tráfego no tráfego *best effort*. Como no primeiro exemplo, com o objetivo de obedecer o SLA determinado, o serviço garantido deve ter apenas uma porcentagem do enlace, através do uso de engenharia de tráfego. Além disso, o tráfego *best effort* também deve ser moldado pelas restrições da engenharia de tráfego.

3.4.2. *Class Type* (CT)

O requisito básico exigido é a possibilidade de se efetuar diferentes reservas de largura de banda para diferentes classes de tráfego. Isto implica a necessidade de se conhecer o total de largura de banda disponível para cada tipo de tráfego em todos os roteadores na rede. Com esse objetivo, a RFC 3564 [04] redefine o conceito de *Class Type* (CT) como sendo o conjunto de *traffic trunks* atravessando um enlace, gerenciados por um conjunto específico de restrições de largura de banda. CT é utilizado na alocação de largura de banda de um enlace, no roteamento baseado em restrições e no controle de admissão de tráfego. Um dado *traffic trunk* pertence ao mesmo CT em todos os enlaces.

A RFC 3564 não define como deve ser feito o mapeamento do tráfego para CT. O IETF exige o suporte de até oito CTs, denominadas CT0 a CT7. Os LSPs criados pela engenharia

de tráfego para garantir a largura de banda de um determinado CT são chamados DS-TE LSPs. No modelo atual, um DS-TE LSP pode transportar tráfego de apenas um CT. LSPs que transportam tráfego de um mesmo CT podem usar diferentes prioridades de preempção. Por convenção, o tráfego *best-effort* é mapeado como CT0.

No primeiro cenário discutido na seção anterior, os tráfegos de voz e dados são suportados por dois PHBs, EF e BE respectivamente. O objetivo é prover garantias de serviço para o tráfego EF. CT0 é mapeado para a fila BE e CT1 é mapeado para a fila EF. A largura de banda disponível para CT1 é limitada à porcentagem do enlace requisitado para assegurar o mínimo de atraso na fila de tráfego de voz. São estabelecidos LSPs separados com requisitos específicos de largura de banda para CT0 e CT1.

3.4.3. Modelos de Restrições de Largura de Banda

Um dos aspectos mais importantes no cálculo da disponibilidade de largura de banda é a sua alocação entre diferentes CTs. A porcentagem de largura de banda utilizada por um CT é determinada por uma restrição de largura de banda (BC - *Bandwidth Constraint*). Alguns modelos de restrições de largura de banda estão sendo discutidos no âmbito do IETF, dentre os quais destacam-se o MAM (*Maximum Allocation Model*) e RDM (*Russian Dolls Model*).

3.4.3.1. MAM (Maximum Allocation Model)

Neste modelo definido em [40], a largura de banda disponível no enlace é dividida entre diferentes CTs, como ilustra a Figura 3.7. O principal problema deste modelo é a impossibilidade de compartilhamento da largura de banda não utilizada entre os diversos CTs, desperdiçando largura de banda ao invés de utilizá-la para o tráfego de outros CTs.

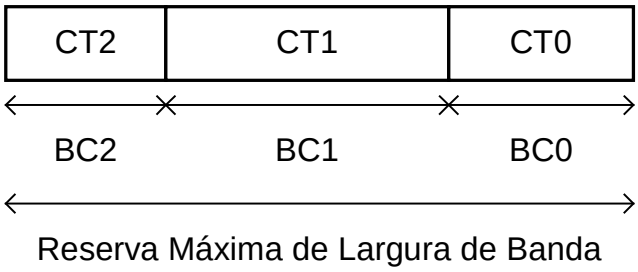


Figura 3.7 - *Maximum Allocation Model* (MAM)

No exemplo da Figura 3.8, o tráfego de voz é mapeado como CT1 e o tráfego de dados é mapeado como CT0. Todos os enlaces têm a largura de banda distribuída da seguinte forma: CT1 com 1 Mbps e CT0 com 9 Mbps. Há um LSP de dados já implementado na menor rota disponível. Dessa forma, caso um novo LSP de dados com 1 Mbps tenha que ser implementado, não poderá utilizar a rota de menor custo, pois a largura de banda disponível está reservada para CT1. Mesmo que nenhum tráfego de voz esteja utilizando o recurso reservado, o novo LSP será obrigado a utilizar a outra rota disponível. Por outro lado, depois que os dois LSPs de dados já estiverem estabelecidos, um novo LSP de voz encontrará largura de banda disponível na rota de menor custo [41].

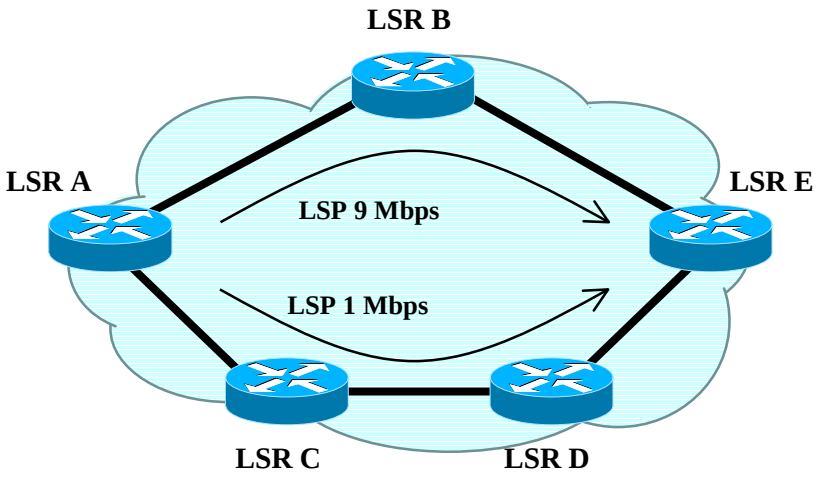


Figura 3.8 - Exemplo de rede com MAM

O benefício alcançado pelo MAM é o completo isolamento entre os diferentes CTs. Por este motivo, não é necessário configurar prioridades entre LSPs carregando tráfego de diferentes CTs. No exemplo citado, caso um LSP com tráfego de voz tenha que ser implementado, há a garantia de disponibilidade de recursos, não sendo necessário a preempção de LSPs de dados.

3.4.3.2. RDM (Russian Dolls Model)

O RDM é definido em [42], e tem como principal diferença com relação ao MAM a possibilidade de compartilhar largura de banda entre CTs. Neste modelo, CT7 é o tráfego com requisitos mais exigentes, enquanto que o CT0 é o tráfego *best-effort*. O grau de compartilhamento varia entre dois extremos. De um lado, a restrição BC7 é uma porcentagem fixa da largura de banda do enlace que é reservada somente para o tráfego CT7. Por outro lado, BC0 representa a largura de banda total do enlace, e é compartilhada entre todos os CTs. Dentro desses dois extremos há diversos graus de compartilhamento: BC6 acomoda os tráfegos de CT7 e CT6, BC5 com os tráfegos de CT7, CT6 e CT5, e assim por diante.

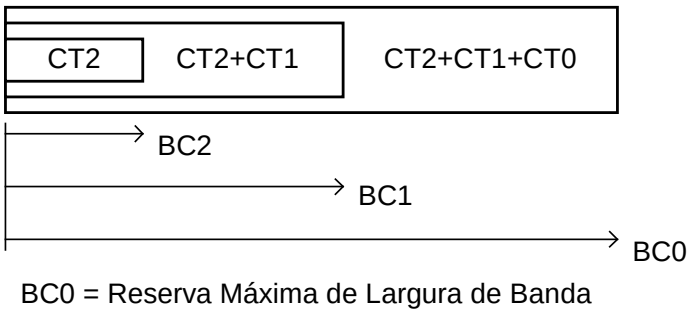


Figura 3.9 - *Russian Dolls Model* (RDM)

Este modelo é inspirado no famoso brinquedo das bonecas russas, onde a maior boneca (BC0) contém uma boneca menor (BC1), que por sua vez contém uma boneca menor ainda (BC2), até atingir a menor boneca de todas (BC7). A alocação de largura de banda pelo modelo RDM é ilustrada na Figura 3.9.

Na rede ilustrada na Figura 3.10, todos os enlaces têm 10 Mbps, onde 1 Mbps é alocado para BC1 e 10 Mbps é alocado para BC0. O tráfego de voz utiliza as restrições de BC1, e o tráfego de dados usa BC0. Isto permite que cada enlace possa transportar de 0 a 1 Mbps de tráfego de voz, utilizando a largura de banda restante para dados. Assumindo que um LSP de 9 Mbps de dados já esteja implementado na rota A-B-E, na ausência de tráfego de voz um segundo LSP de 1 Mbps pode ser inserido nessa mesma rota, aproveitando a largura de banda disponível. A desvantagem do RDM em relação ao MAM é que não há separação entre os diferentes CTs, sendo necessário o uso da preempção para assegurar que cada CT tenha garantido sua cota de largura de banda, não importando se outros LSPs estão compartilhando esses recursos.

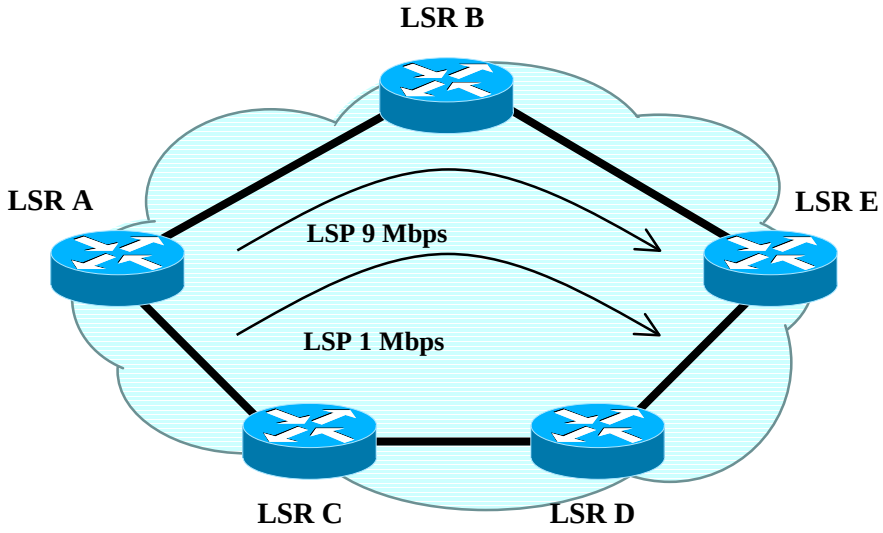


Figura 3.10 - Exemplo de rede com RDM

Se, após o estabelecimento do segundo LSP de dados for necessário a implantação de um LSP de voz, um dos LSPs de dados terá que ser retirado da rede, pois não há espaço para o novo LSP. Isto significa que os LSPs de voz e dados devem ter diferentes níveis de prioridade, porque eles podem competir pelos recursos disponíveis [41].

O cálculo da largura de banda disponível é mais complexo que no modelo anterior, porque deve considerar LSPs com diversas prioridades de todos os CTs que compartilham um determinado BC. A Tabela 3.3 compara as principais características dos dois modelos.

Tabela 3.3 - Comparação entre os modelos MAM e RDM

MAM	**RDM**
Mapeia um BC para um CT	Mapeia um BC para um ou mais CTs
Isolamento entre os CTs	Compartilhamento entre os CTs
Desperdício de Largura de Banda	Uso eficiente de Largura de Banda
Não é necessário preempção	Necessário preempção

3.4.4. Priorização e Preempção de LSPs

A RFC 3272 [43] define a noção de priorização e preempção (*preemption*) de LSPs. A solução DS-TE deve ter total suporte à preempção, deixando livre a escolha de sua utilização ao administrador da rede. A RFC 3564 [04] introduz o conceito de TE-*Class (Traffic Engineering Class Type*), como sendo um CT (*Class Type*) com um nível associado de prioridade de preempção.

O objetivo da priorização é marcar quais LSPs são mais importantes, permitindo assim que eles apropriem os recursos dos LSPs de menor importância. O uso da priorização de LSPs garante que, na ausência de LSPs prioritários, os recursos possam ser utilizados pelos LSPs de

menor prioridade. Além disso, os LSPs mais importantes têm maior probabilidade de serem estabelecidos na rota de menor caminho, e em caso de falhas nos enlaces, eles têm uma chance maior de encontrar uma rota alternativa.

O uso de políticas de priorização e preempção de LSPs torna-se fundamental principalmente quando do uso do modelo de restrição de largura de banda RDM. Como nesse modelo não existe uma divisão entre os diferentes *Class Types*, é necessário a preempção como forma de garantir que as aplicações mais importantes possam sempre utilizar os recursos de rede.

3.5. Conclusões

Para suportar o rápido crescimento do fluxo de dados e manter uma infra-estrutura "enxuta", as empresas precisam balancear a utilização do tráfego em seus enlaces, roteadores e demais equipamentos. O congestionamento nas redes IP atuais ocorre devido à seleção do caminho de menor custo calculado pelo IGP (*Interior Gateway Protocol*). A engenharia de tráfego resolve esse problema selecionando o caminho menos congestionado ao invés do menor caminho, permitindo uma utilização mais eficiente da estrutura da rede.

A crescente necessidade de redes que suportem QoS exige a integração de novas arquiteturas, onde destacam-se o MPLS e o DiffServ. Essas duas tecnologias são soluções complementares para o provimento de diferentes níveis de serviços em uma rede. Ambas colocam a complexidade de processamento na borda da rede, aprimorando a escalabilidade.

O MPLS proporciona uma excelente plataforma para a implementação de engenharia de tráfego. Através do mecanismo de roteamento explícito, é possível configurar rotas com base em restrições de largura de banda, atraso e outros atributos, importantes para o fornecimento de níveis de QoS às aplicações.

Porém, alguns cenários não podem ser solucionados apenas com o uso de engenharia de tráfego. Para esses casos, utiliza-se a engenharia de tráfego em rede MPLS/DiffServ (DS-TE), definida na RFC 3564 [04]. Essa solução é aplicada principalmente nos seguintes cenários: quando se deseja limitar a proporção de tráfego de uma classe em um determinado enlace, quando é necessário fixar a proporção relativa de cada tráfego no enlace ou quando simplesmente se deseja implementar um serviço de largura de banda garantida, além do serviço *best effort*. DS-TE pode ser utilizado em outros cenários, devendo ter suporte às soluções anteriores já padronizadas.

Modelos de restrições de largura de banda são utilizados para garantir que determinadas classes de serviço tenham recursos suficientes para a transmissão dos pacotes. Alguns modelos estão sendo discutidos no âmbito do IETF, onde destacam-se o MAM (*Maximum Allocation Model*) e RDM (*Russian Dolls Model*). Estes modelos encontram-se na forma de *Internet Drafts*. Alguns estudos ([11], [42] e [44]) demonstram que o modelo RDM é o mais adequado, principalmente devido à possibilidade de compartilhamento de largura de banda entre CTs (*Class Types*). Como o RDM não separa a largura de banda entre os diversos CTs, é necessário o uso de uma política adequada de priorização e preempção de LSPs, para assegurar que os tráfegos mais importantes tenham sua cota de largura de banda, não importando se outros LSPs estão compartilhando esses recursos.

CAPÍTULO 4

PRIORIZAÇÃO E PREEMPÇÃO DE LSPs

4.1. Introdução

A preempção de LSPs é considerada um meio para se prover serviços confiáveis e com disponibilidade para as conexões de alta prioridade, principalmente quando a rede está fortemente carregada ou em casos de falhas nos enlaces e/ou roteadores.

A rede pode sofrer condições de instabilidade devido a diversos fatores como falha nos enlaces, alta demanda de tráfego ou um comportamento desconhecido no padrão de transmissão dos fluxos. Sob essas condições, novos pedidos de criação de LSPs não podem ser atendidos e a única solução possível é a apropriação de recursos de algumas conexões ativas. A política de preempção utilizada deve minimizar o impacto sofrido pelas conexões de maior prioridade, provavelmente com o custo de um impacto maior nas conexões de menor prioridade. Os mecanismos de preempção também podem ser utilizados para o gerenciamento e reserva de largura de banda.

A importância de uma conexão é expressa por um nível de prioridade. Os níveis de prioridade podem ser definidos pelo administrador da rede, utilizando diversos fatores como confiabilidade, requisitos de largura de banda, restrições de entrega em tempo real, probabilidade de bloqueio desejado, e a natureza do tráfego como dados, voz, multimídia, etc.

Para minimizar o impacto sofrido pelas conexões de maior prioridade em uma rede sob condições de instabilidade, é necessário que os novos LSPs sejam capazes de apropriar os recursos dos LSPs existentes e de menor prioridade. A preempção disponibiliza largura de banda, permitindo o funcionamento normal das conexões prioritárias. As conexões que sofreram preempção podem ser re-roteadas, que por sua vez podem causar novas preempções de outros LSPs. Esta situação ocorre apenas se a rede permitir re-roteamento. Caso o LSP não possa ser novamente estabelecido, a conexão será descartada.

Quando a preempção é inevitável, um algoritmo deve selecionar um ou mais LSPs de menor prioridade, permitindo o estabelecimento da conexão que disparou o algoritmo de preempção. Este algoritmo deve causar um mínimo possível de interrupção na rede devido a apropriação dos LSPs. Também deve ser rápido para minimizar o tempo da interrupção e o tempo de criação do novo LSP. Sendo assim, o algoritmo deve funcionar em tempo real [45].

4.2. Conceito de Preempção

Em um ambiente multitarefa, a preempção é o ato de tirar o controle do sistema operacional de uma tarefa e entregar a outra tarefa [46]. Essa técnica vem sendo muito discutida na comunidade científica, e aplicada em diversas áreas do conhecimento. Vários estudos têm sido apresentados sobre o uso da preempção, inclusive fora do contexto de redes de computadores. Em [15], o conceito de preempção é aplicado no processo de *handoff* em uma rede de telefonia móvel. Em [47], os autores desenvolveram um trabalho envolvendo conceitos de preempção em redes Petri, que é uma ferramenta muito utilizada na modelagem e análise de sistemas estocásticos. Utiliza-se algoritmos de preempção em sistemas de *Call Center*, com o objetivo de manter o fluxo de ligações em situações de congestionamento [48]. Nas arquiteturas de redes óticas, políticas de preempção são utilizadas para reduzir o tempo de recuperação de rotas em caso de falhas.

A Rede de Telefonia Pública Comutada (RTPC) tem como objetivo suportar a maior quantidade possível de usuários e aplicações em situações de congestionamento. Em [16], elaborou-se um estudo onde aplica-se a preempção em diversos ambientes, como a RTPC, redes de telefonia celular, redes de acesso DSL (*Digital Subscriber Line*) e a cabo. Em todos esses casos, reservas são estabelecidas para usuários que desejam ter um nível determinado de QoS. Assim, na ocorrência de algum congestionamento, os usuários selecionados têm um tratamento preferencial no estabelecimento e manutenção de suas conexões.

Em [17], um algoritmo foi desenvolvido para adicionar funções de preempção no processo de estabelecimento de conexões em redes ATM (*Asynchronous Transfer Mode*). Ainda sobre redes ATM, em [49] desenvolveu-se um estudo focado principalmente no contexto de sinalização e nos métodos para definição de qual conexão deve sofrer preempção. Extensões foram implementadas nas mensagens de sinalização e definidos os procedimentos no processamento das mensagens para o controle da preempção.

4.3. Preempção em Redes MPLS/DiffServ

Alguns tipos de tráfego são mais importantes do que outros. Pode-se ter LSPs transportando tráfego VoIP (Voz sobre IP) e LSPs transportando tráfego de dados competindo pelos mesmos recursos. Ou então, pode-se ter simplesmente alguns LSPs de dados que são mais importantes do que outros. Caso a rede não ofereça recursos suficientes para todas as aplicações, é necessário um meio de permitir que alguns LSPs apropriem-se dos recursos utilizados por outros LSPs.

A engenharia de tráfego DS-TE oferece um mecanismo para fazer isso. Cada LSP tem uma prioridade, e LSPs mais importantes têm preferência em relação a LSPs menos importantes. Os LSPs com menor prioridade são afastados do caminho, e seus recursos são

dados ao LSP de maior prioridade. A isso chamamos apropriação, ou preempção (*preemption*) [37].

A RFC 3209 [13] define uma prioridade de *Setup* e uma prioridade de *Holding*. Elas são comparadas com as prioridades de *Preemption* e *Defending* da RFC 2751 [50]. A idéia é que, quando um LSP é configurado inicialmente, sua prioridade de *Setup* seja considerada quando se decide que o LSP será admitido. Quando outro LSP aparece e compete com o primeiro pela largura de banda do enlace, a prioridade de *Setup* do novo LSP é comparada com a prioridade de *Holding* do primeiro.

Na engenharia de tráfego DS-TE utiliza-se até oito *Class Types*. Com o objetivo de prover diferentes restrições de largura de banda, é configurado um valor máximo de largura de banda que pode ser reservado para cada *Class Type*. No exemplo da Figura 4.1, um enlace de 1.500 Mbps possui dois *Class Types*: CT1 para o tráfego de voz e CT0 para o tráfego de dados. Considera-se que o tráfego de voz tem maior prioridade que o tráfego de dados. A máxima largura de banda que pode ser reservada é de 50% para CT1 e 100% para CT0, ou seja, o tráfego de voz pode utilizar até 750 Mbps, enquanto que o tráfego de dados pode utilizar toda a capacidade do enlace [07].

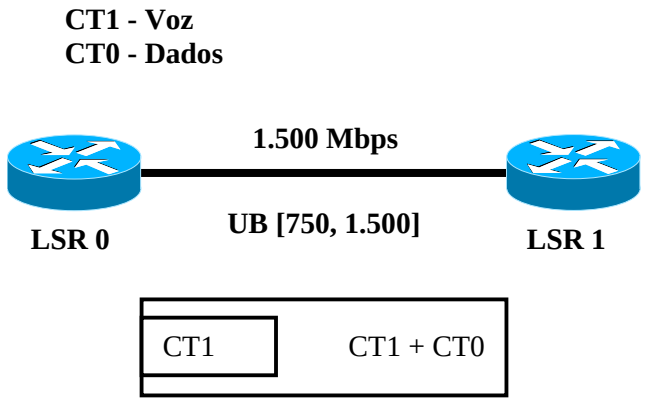


Figura 4.1 - Reservas de largura de banda por *Class Type*

Considere o vetor UB (*Unreserved Bandwidth*) como sendo a largura de banda que pode ser reservada por *Class Type*. No exemplo, o vetor UB será [750, 1.500], que determina as reservas que podem ser feitas por CT1 e CT0 respectivamente. Suponha que quatro novas solicitações de LSPs cheguem no enlace com a seguinte ordem: 500 Mbps para CT0, 500 Mbps para CT1, 250 Mbps para CT0 e 250 Mbps para CT1. O vetor UB será alterado a cada nova solicitação de largura de banda:

[750, 1.500] - Situação inicial;

[750, 1.000] - Vetor UB após a solicitação de 500 Mbps de CT0;

[250, 500] - Vetor UB após a solicitação de 500 Mbps de CT1;

[250, 250] - Vetor UB após a solicitação de 250 Mbps de CT0;

[0, 0] - Vetor UB após a solicitação de 250 Mbps de CT1.

A preempção neste caso não é necessária, pois o enlace dispõe de recursos suficientes para acomodar todas as solicitações. Considere agora a seguinte seqüência: 750 Mbps para CT0, novamente 750 Mbps para CT0 e 500 Mbps para CT1. A largura de banda disponível no enlace será:

[750, 1.500] - Situação inicial;

[750, 750] - Vetor UB após a solicitação de 750 Mbps de CT0;

[750, 0] - Vetor UB após nova solicitação de 750 Mbps de CT0;

[250, 0] - Vetor UB após a solicitação de 500 Mbps de CT1;

Na última etapa torna-se necessário adotar a preempção, disponibilizando largura de banda para CT1. Uma política de preempção deve ser acionada para escolher quais LSPs devem ser retirados da rede, causando o menor impacto possível [07].

4.3.1. Critérios de Preempção

Para cada classe de tráfego, existem 8 níveis de preempção (*preemption*) variando de 0 a 7. O número mais baixo representa o LSP de mais alta prioridade; assim, o LSP com valor 0 pode apropriar os recursos de todos os outros LSPs com valor diferente de 0. Um novo pedido de criação de LSP tem dois parâmetros importantes: largura de banda e prioridade. Com o objetivo de minimizar o desperdício de recursos de rede, não se deve levar em consideração apenas o valor de prioridade do conjunto de LSPs a se apropriar, mas sim combinar outros critérios [11]:

- Apropriar as conexões de menor prioridade. Assim a QoS de tráfegos de maior prioridade será melhor atendida.

- Apropriar o menor número de LSPs. Essa ação reduz o número de LSPs que precisam ser novamente roteados, minimizando o tráfego necessário para se encontrar uma nova rota.

- Apropriar a menor quantidade de largura de banda. A utilização de recursos ficará melhor, reduzindo desperdícios na rede.

O fluxograma da Figura 4.2 ilustra o processo de implantação de um novo LSP na rede. Ao chegar um novo pedido de criação de LSP, deve-se verificar se na rota solicitada há largura de banda suficiente. Caso tenha recursos suficientes, o novo LSP será implementado na rede.

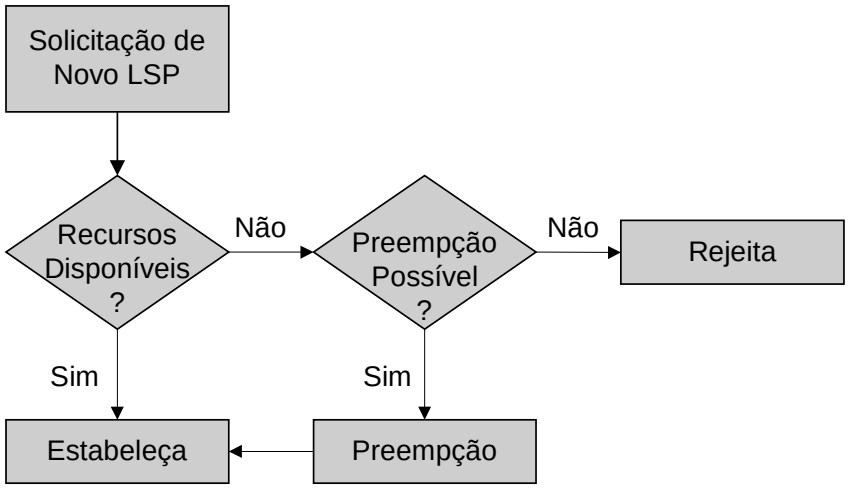


Figura 4.2 - Fluxograma do processo de criação de um novo LSP

Caso a largura de banda seja insuficiente e exista LSPs com menor prioridade naquela rota, uma política de preempção deve ser ativada para encontrar os LSPs com prioridade menor, e se possível encontrar uma solução que retire o menor número de LSPs e minimize o desperdício de largura de banda.

4.3.2. Exemplo de Funcionamento

A Figura 4.3 ilustra uma rede com alguns LSPs já implementados, enquanto que a Tabela 4.1 mostra as prioridades de *Holding* e a largura de banda utilizada pelos LSPs. Suponha que um novo LSP, com prioridade de *Setup* maior do que as prioridades de *Holding* dos demais LSPs, tenha que ser criado entre os nós 0, 1, 3 e 4. Caso a rede não possua recursos suficientes para acomodar esse novo LSP, é necessário que alguns LSPs sejam retirados para dar lugar a essa nova solicitação.

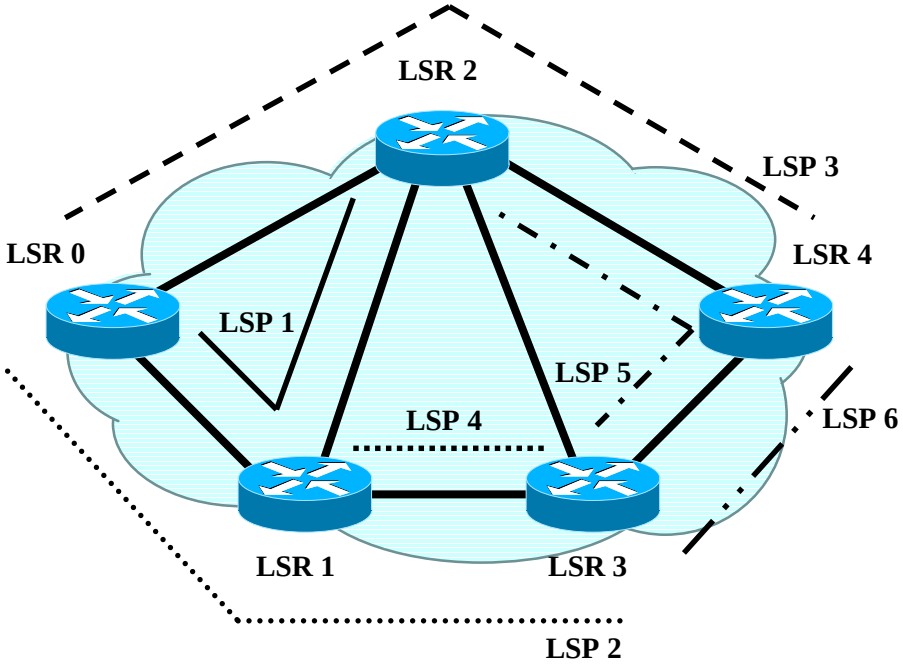


Figura 4.3 - Topologia de rede ilustrando LSPs

Tabela 4.1 - Prioridade e largura de banda dos LSPs

LSP	Prioridade	Largura de Banda
LSP1	7	800 Kbps
LSP2	4	500 Kbps
LSP3	2	200 Kbps
LSP4	5	500 Kbps
LSP5	6	700 Kbps
LSP6	5	600 Kbps

Utilizando uma política que considere apenas a prioridade, os LSPs 1, 4 e 5 seriam apropriados pelo novo LSP. Essa solução atingiu o objetivo inicial, porém pode não ser a ideal. Suponha que um ISP *(Internet Service Provider*) queira reduzir o número de LSPs apropriados, ou então, o administrador de rede tenha a necessidade de minimizar o desperdício de largura de banda caso um novo LSP seja introduzido na rede. Uma solução

melhor seria o novo LSP apropriar os recursos dos LSPs 2 e 6, reduzindo o número de LSPs apropriados e otimizando o uso de largura de banda.

4.4. Preempção com CR-LDP

O protocolo CR-LDP sinaliza para cada roteador de uma determinada rota quais os recursos solicitados pelo novo LSP. Se a rota solicitada não dispor de recursos suficientes, os LSPs existentes podem ser realocados para liberar recursos ao novo LSP. As prioridades de *Setup* e *Holding* dos LSPs são utilizadas para determinar se o novo LSP pode apropriar os recursos dos LSPs já implementados. A preempção irá ocorrer caso o novo LSP tenha uma prioridade de *Setup* maior que a prioridade de *Holding* do LSP atual.

Um mesmo LSP não pode ter uma prioridade de *Setup* maior que a prioridade de *Holding*. Como exemplo, considere dois LSPs com prioridade de *Setup* 1 e prioridade de *Holding* 7 competindo pelos mesmos recursos. Nessa situação, a preempção irá ocorrer alternadamente entre os dois LSPs, pois a prioridade de *Holding* não é suficiente para que eles possam se manter na rede [37].

CR-LDP utiliza mensagens TLV (*Type*, *Length* e *Value*) com os parâmetros de tráfego necessários para a implementação de um LSP. O campo *Type* define o tipo de mensagem, o campo *Length* o tamanho dessa mensagem e o campo *Value* mostra seus parâmetros. A Figura 4.4 ilustra uma mensagem TLV utilizada na preempção, onde é possível observar os campos de prioridades do LSP. O campo *Type* tem 14 bits, e para uma mensagem de preempção seu valor é 0x820. O campo *Length* especifica o tamanho em bytes do campo *Value*, cujo valor deverá ser 4.

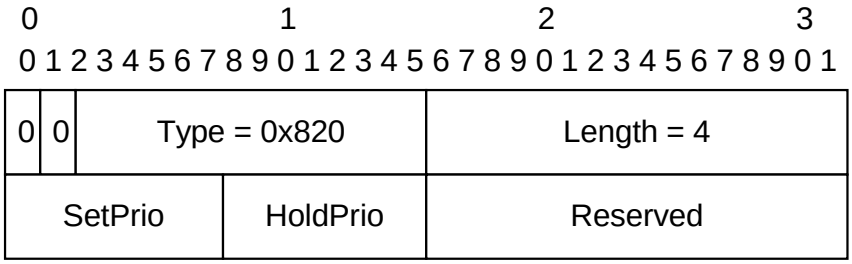


Figura 4.4 - Parâmetros de preempção TLV

O campo *SetPrio* define o valor de prioridade na implementação de um novo LSP. O valor 0 é a prioridade definida para o LSP mais importante. O valor 7 é a prioridade do LSP de menor importância. Quanto maior a prioridade de *Setup*, mais LSPs podem ser retirados para dar espaço ao novo LSP. O campo *HoldPrio* também utiliza o valor 0 para os LSPs mais importantes, e o valor 7 para os LSPs menos importantes. Quanto maior a prioridade de *Holding*, menor é a possibilidade do LSP ter sua largura de banda realocada para um novo LSP.

As prioridades de *Setup* e *Holding* devem ser inicialmente definidas com valor 4, possibilitando uma mudança gradual nos valores de acordo com o funcionamento da rede. Como o parâmetro de priorização é opcional, os LSPs que são implementados na rede sem uma prioridade definida devem ser considerados como tendo o valor padrão, ou seja, com prioridade 4.

Quando um LSP é apropriado, o LSR que iniciou a preempção manda uma mensagem WITHDRAW no sentido *upstream*, e uma mensagem RELEASE no sentido *downstream*. Quando um LSP sofre preempção no meio de seu processo de estabelecimento, o LSR que iniciou a preempção deve mandar uma mensagem NOTIFICATION no sentido *upstream*, e uma mensagem ABORT no sentido *downstream* [36].

4.5. Preempção com RSVP-TE

O suporte às prioridades de *Setup* e *Holding* é opcional. Os roteadores devem ser capazes de reconhecer essas informações caso a preempção seja necessária, e encaminhá-las no sentido *downstream* sem nenhuma mudança. Como ilustrado na Figura 4.5, a preempção é implementada através de duas prioridades: *Setup* e *Holding*. A prioridade de *Setup* é a responsável pela conquista de recursos, enquanto que a prioridade de *Holding* faz a manutenção da reserva dos recursos de uma sessão. A prioridade de *Setup* nunca deve ser maior que a prioridade de *Holding* em uma sessão. O valores podem variar de 0 a 7, sendo o valor 0 alocado para a sessão de maior prioridade.

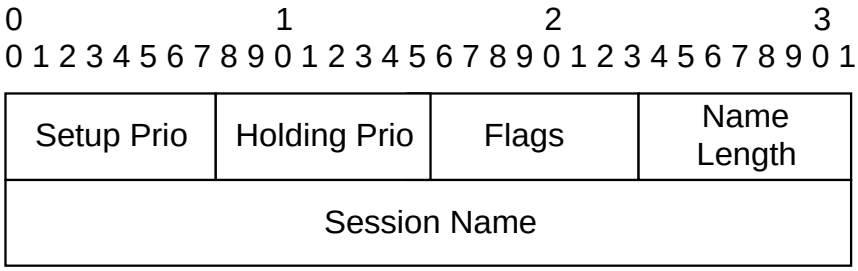


Figura 4.5 - *Session Atribute Message* - RSVP

Quando uma nova mensagem PATH é inserida na rede para admissão, a largura de banda solicitada é comparada com a largura de banda disponível com a prioridade especificada no campo *Setup Prio*. Se a largura de banda solicitada não estiver disponível, uma mensagem PATH_ERR é retornada indicando a indisponibilidade da largura de banda solicitada.

Se a largura de banda solicitada for menor que a largura de banda não utilizada, então o processo será completado. Se a largura de banda disponível estiver em uso por sessões de

menor prioridade, então as sessões de menor prioridade sofrerão preempção para liberar a largura de banda necessária.

Cada sessão que sofreu preempção deve disparar uma mensagem, enviando um código indicando o motivo da preempção. Uma mensagem RESV_ERR e/ou PATH_ERR deve ser enviada no sentido *downstream* para o destino do tráfego e no sentido *upstream* para os emissores do tráfego [13].

4.6. Hard Preemption

Inicialmente, a engenharia de tráfego em redes MPLS definiu apenas o método de preempção que descarta imediatamente os LSPs apropriados, indiferente à existência de algum outro LSP no meio de um processo de preempção. Esse método é denominado *Hard Preemption* [13].

Esse processo simples, porém abrupto, garante que o tráfego apropriado seja descartado, até que a mensagem do protocolo RSVP PATH_ERROR alcance o roteador de ingresso e seja processada, e uma nova conexão possa ser estabelecida. Este método pode ser de grande ajuda quando não há disponibilidade de recursos, porém a preempção pode ser disparada mesmo em casos de simples disputa de recursos em uma rota. O resultado é que algumas conexões serão desnecessariamente descartadas, podendo ser alocadas em uma nova rota apenas após o descarte.

O método *Hard Preemption* pode ser um requisito importante para proteger o tráfego em uma rede sem DiffServ, mas em uma arquitetura DiffServ não é necessário confiar exclusivamente na preempção para garantir a prioridade no tratamento dos tráfegos mais valiosos, uma vez que o próprio processo DiffServ já oferece um método de diferenciação de serviços.

Não há nenhum mecanismo que permita aos LSPs que sofreram a preempção trocarem a rota utilizada por um outro caminho alternativo. Ao invés disto, o esquema *Hard Preemption* pode causar interrupção no tráfego para um conjunto muito grande de LSPs [14].

4.7. Soft Preemption

O método *Soft Preemption* resulta de um conjunto de modificações no protocolo RSVP com o objetivo de reduzir e/ou eliminar a interrupção de tráfego dos LSPs que sofreram preempção. O uso de mensagens indicando uma preempção pendente ajuda a aliviar o processo de re-roteamento dos LSPs que serão apropriados.

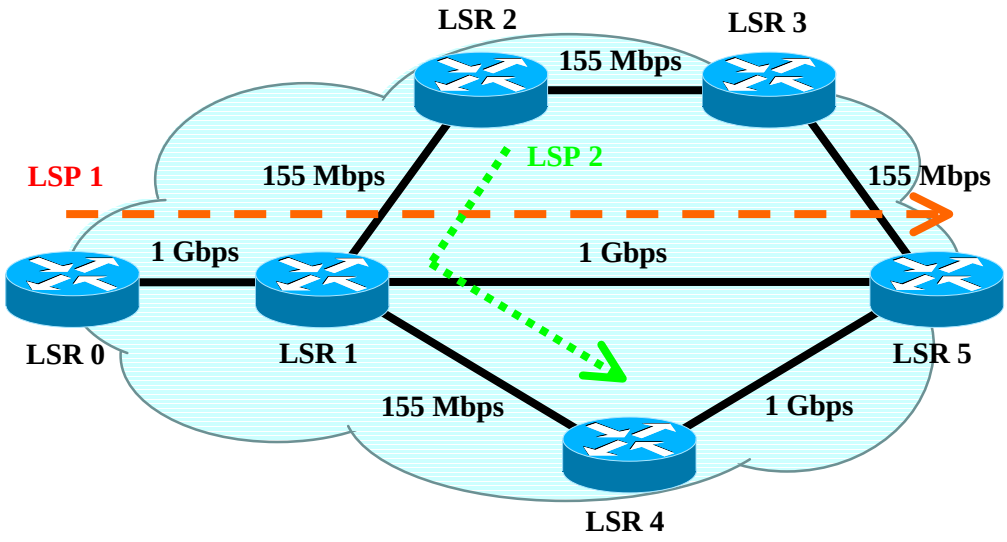


Figura 4.6 - Exemplo de funcionamento do método *Soft Preemption*

No exemplo da Figura 4.6, há dois LSPs estabelecidos ocupando uma largura de banda de 155 Mbps. O LSP1 tem prioridade de *Setup* e *Holding* com valor 0, enquanto que o LSP2 tem prioridade 7. Na ocorrência de uma falha no enlace entre os roteadores LSR1 e LSR5, o roteador LSR1 envia uma mensagem PATH_ERROR para todos os roteadores de ingresso que possuem algum LSP atravessando o enlace com problemas (no caso, o LER de ingresso

será o LSR0). Após receber a notificação de falha no enlace, o LSR0 dispara uma sinalização de re-roteamento do LSP1, indicando uma nova rota através dos roteadores LSR0 - LSR1 - LSR4 - LSR5, que poderá satisfazer as restrições impostas pelo LSP1.

Como o enlace entre os LSRs 1 e 4 não tem recursos suficientes para as reservas de largura de banda de ambos LSPs, o mecanismo *Soft Preemption* irá atuar no LSP2, pois tem menor prioridade. Ao invés de simplesmente excluir o LSP2, que irá resultar em uma interrupção imediata em seu tráfego, o roteador LSR1 envia uma mensagem indicando uma preempção pendente de LSP2 em direção ao roteador de ingresso LSR2. Ao receber essa mensagem, LSR2 estabelece o novo caminho do LSP2 utilizando, por exemplo, o protocolo CSPF. Após o LSP2 ter se estabelecido em uma nova rota, as antigas reservas são liberadas para o LSP1. Como resultado, o tráfego do LSP2 não será simplesmente cortado devido a uma simples disputa por recursos, uma vez que há outros caminhos na rede que podem ser utilizados. O LSP será excluído da rede apenas em cenários de real congestionamento, onde não é possível encaminhá-lo em outra rota [14].

4.8. Políticas de Preempção de LSPs

Uma política de preempção é um conjunto de regras que tem como objetivo escolher quais LSPs devem sofrer preempção para atender os requisitos dos LSPs mais importantes. Os algoritmos devem otimizar o uso dos recursos de rede, e podem levar em conta diversos fatores como: prioridade dos LSPs, número de LSPs apropriados, quantidade de largura de banda a ser apropriada, etc.

No contexto de redes de computadores, diversas propostas têm sido desenvolvidas no sentido de otimizar a escolha das conexões que devem ser excluídas da rede. No âmbito do IETF, algumas propostas encontram-se sob a forma de *Internet Drafts*.

4.8.1. Método Proposto por Garay e Gopal

Em [51], Garay e Gopal desenvolveram um estudo sobre o problema da preempção de conexões em redes centralizadas, através de um algoritmo de seleção de conexões a se apropriar. Esse algoritmo é adequado para um ambiente de rede centralizado, onde um ponto central de controle é responsável pela maioria das funções de controle de rede, pois o algoritmo exige como parâmetros de entrada informações sobre a rota completa da conexão apropriada, bem como as rotas completas das conexões que compartilham um ou mais enlaces com a conexão apropriada. Assim, um controlador central monitora as informações sobre toda a rede, e dispara o algoritmo de preempção para selecionar as conexões que devem ser descartadas. Devido a natureza inerente de um sistema distribuído, uma entidade central de controle não terá sempre as informações atualizadas sobre o comportamento de toda a rede. Além do mais, quando uma falha em um enlace ou nó dispara a preempção, não é desejável ter um ponto de controle central que considere o caminho completo (fim a fim) das conexões que possam sofrer preempção, pois isso irá ocasionar problemas de escalabilidade e eficiência. A complexidade computacional desse algoritmo é dado por $Q\ (n\ .\ m^2)$, onde n é o número de enlaces ao longo do caminho de preempção, e m é o tamanho do conjunto de todas as conexões existentes que possuem ao menos um enlace em comum com a rota selecionada para a preempção, e tendo uma prioridade menor que a conexão que disparou o processo de preempção.

4.8.2. Método Proposto por Peyravian e Kshemkalyani

Em [45], desenvolveu-se dois algoritmos de preempção de conexões em redes descentralizadas/distribuídas, minimizando interrupções nas conexões existentes e satisfazendo as restrições impostas pelas conexões de maior prioridade. Estes algoritmos consideram a preempção no nível de enlace, funcionando localmente em cada enlace, ou seja,

se uma nova conexão fim a fim tem que ser estabelecida, cada enlace ao longo da rota escolhida pela nova conexão irá utilizar o algoritmo de preempção caso o enlace não possa alocar largura de banda suficiente para essa nova conexão. Assim, cada nó de origem do enlace irá funcionar como um ponto de controle, resultando assim em um algoritmo útil para redes descentralizadas/distribuídas. Estes algoritmos têm como principais parâmetros a largura de banda a ser apropriada, o número de conexões a se apropriar e a apropriação de conexões de menor prioridade.

O primeiro algoritmo minimiza, em primeiro lugar, o número de conexões que devem sofrer preempção, para depois escolher uma combinação de conexões que minimizem a largura de banda apropriada. Caso o processo retorne mais que uma solução, o algoritmo deve selecionar aquela que possua conexões de menor prioridade. Este algoritmo tem uma complexidade computacional de Q (k^2), onde k é o número de conexões que compartilham o enlace sob consideração e com prioridade menor que a conexão a ser estabelecida. O segundo algoritmo inicialmente minimiza a largura de banda a ser apropriada no enlace, escolhendo depois uma combinação de conexões com menor prioridade. Caso exista mais que uma solução, é escolhida a solução com o menor número de conexões que devem sofrer preempção. Este algoritmo é exponencial e tem uma complexidade Q ($k \cdot 2^k$).

Estes algoritmos foram desenvolvidos com base em observações feitas em diversos estudos de simulação com várias possibilidades de preempção de conexões. Como comparação conclui-se que, em termos gerais de performance de rede, não há grande diferença de qualidade entre os dois algoritmos. Observa-se apenas que o segundo algoritmo tem melhor performance quando a rede está mais carregada ou em estado de congestionamento, porque essa solução tem como principal objetivo minimizar a preempção excessiva de largura de banda, resultando em maior eficiência no uso dos recursos de rede. Em termos de complexidade computacional, o primeiro algoritmo é polinomial, enquanto que

o segundo é exponencial. Sob esse foco, conclui-se que o primeiro algoritmo é o mais adequado, porque a preempção de conexões é um problema que deve ser solucionado no menor intervalo de tempo possível.

4.8.3. Método Proposto por Blanchy

Em [19], foi proposto um mecanismo de integração de uma política de preempção com um esquema de re-roteamento de LSPs dentro do contexto de redes MPLS. O mecanismo envolve um algoritmo de escolha dos LSPs mais interessantes para a preempção, sendo re-roteados em outros enlaces através de mecanismos de roteamento.

4.8.4. Proposta do IETF

Em [11], é demonstrado através de simulações com roteadores comerciais, que os LSPs apropriados são sempre aqueles de menor prioridade, mesmo que a largura de banda alocada seja muito maior do que aquela solicitada para o novo LSP. Esta política resulta em um alto desperdício de largura de banda para os casos em que um novo roteamento não é permitido. Como solução, em [12] propõe-se uma função matemática que agrega os principais critérios para a preempção de LSPs: número de LSPs, prioridade dos LSPs e largura de banda a ser apropriada. Através de um sistema de pesos, pode-se implementar esse algoritmo em um *backbone*, dando mais ênfase ao critério desejado de acordo com as características do ISP (*Internet Service Provider*). Além dessa solução, o trabalho desenvolveu um amplo estudo na otimização e desenvolvimento de novas técnicas para a provisão de QoS fim a fim em redes MPLS/DiffServ, envolvendo novas políticas de implementação, preempção, roteamento e dimensionamento de LSPs.

4.9. Conclusões

A Internet está evoluindo de forma muito rápida, tornando-se uma estrutura padronizada no transporte de serviços em tempo real e sensíveis a atrasos, como por exemplo voz e multimídia. O sucesso no oferecimento desses serviços depende da habilidade da rede em prover um transporte de pacotes de forma confiável e previsível. Porém, devido a fatores como alterações freqüentes nos padrões de tráfego, falhas nos enlaces e equipamentos ou insuficiência de recursos, o estabelecimento de novos LSPs na rede pode vir a fracassar, impossibilitando o tráfego de determinadas aplicações.

A preempção de LSPs pode ser usada como um mecanismo eficiente na reserva e gerenciamento de largura de banda. Sua implementação fornece confiabilidade e disponibilidade de serviços para as conexões prioritárias. A importância de um LSP pode ser relacionada com os parâmetros de QoS solicitados por uma aplicação, podendo ser expressa através de um nível de prioridade. Os tráfegos de voz e vídeo são exemplos de aplicações que podem se beneficiar com a preempção, pois são aplicações em tempo real.

Quando a preempção se torna necessária, um algoritmo deve escolher um ou mais LSPs que serão retirados com o objetivo de permitir a implementação da nova conexão. Esse algoritmo deve causar a menor interrupção possível dos LSPs que sofreram a preempção, além de ser suficientemente rápido para minimizar a duração desta interrupção e do estabelecimento do novo LSP [52].

Diversos algoritmos têm sido desenvolvidos para otimizar o processo de preempção. No âmbito do IETF, o estudo sobre a preempção de LSPs está sob comando do grupo de pesquisas sobre Engenharia de Tráfego. Algumas propostas estão sendo discutidas sobre qual a política mais adequada, porém ainda encontram-se sob a forma de *Internet Drafts*.

CAPÍTULO 5

AVALIAÇÃO DE DESEMPENHO DE UMA REDE *BACKBONE* COM MPLS/DIFFSERV E PREEMPÇÃO DE LSPS

5.1. Introdução

Um dos principais campos de estudo do IETF é o desenvolvimento de um modelo de rede IP capaz de suportar as necessidades atuais e futuras dos usuários e das aplicações multimídia. As arquiteturas IntServ, DiffServ e MPLS solucionam alguns problemas encontrados pelos ISPs, porém não conseguem prover uma solução completa. Assim, as tecnologias MPLS e DiffServ são integradas resultando em uma rede com soluções de QoS mais abrangentes. A preempção de LSPs é um recurso importante para se garantir o bom desempenho de algumas aplicações, tornando-se uma peça fundamental para o funcionamento adequado de uma rede MPLS/DiffServ.

Por meio de modelagem e simulação demonstra-se os benefícios alcançados com a introdução de uma política de preempção de LSPs em uma rede MPLS/DiffServ. O modelo de simulação utilizado foi baseado no ambiente de rede da Empresa Brasileira de Telecomunicações S/A (Embratel), considerando apenas os Centros de Roteamento do Estado de São Paulo. Um ISP local conectado a um ISP regional encaminha alguns tipos de tráfego,

permitindo uma avaliação do comportamento da rede *backbone* no encaminhamento desses pacotes.

Cinco experimentos foram realizados, sendo que no primeiro experimento utilizou-se o encaminhamento de melhor esforço oferecido atualmente pela Internet. No segundo e terceiro experimentos, as tecnologias DiffServ e MPLS foram inseridas isoladamente na rede com o objetivo de permitir a avaliação de desempenho destas soluções no suporte à QoS. No quarto experimento, as tecnologias MPLS e DiffServ foram utilizadas em conjunto, e no quinto experimento a preempção de LSPs foi implementada com o objetivo de priorizar algumas aplicações em uma situação de congestionamento.

5.2. Ambiente de Rede

A topologia da Internet, isto é, a estrutura de interconexão entre as suas várias partes, é levemente hierárquica. Em linhas gerais, a hierarquia consiste em sistemas finais conectados aos provedores de serviços de Internet (*Internet Service Providers* – ISPs) por meio de redes de acesso. Os ISPs locais estão conectados a ISPs regionais, que por sua vez estão ligados a ISPs nacionais e internacionais. Os ISPs nacionais e internacionais estão interligados no nível mais alto da hierarquia [21].

Este trabalho foi desenvolvido com base em informações da rede *backbone* da Empresa Brasileira de Telecomunicações S/A (Embratel), que é atualmente o maior ISP nacional, tanto em termos de abrangência como em capacidade de transmissão [53].

A Figura 5.1 mostra todos os Centros de Roteamento disponíveis no *backbone* nacional da Embratel. Além desses pontos, há mais de 310 cidades consideradas POPs (Pontos de Presença), cujo função é levar o tráfego ao Centro de Roteamento mais próximo [53].

Figura 5.1 - Ambiente de Rede

Os parâmetros de desempenho do *backbone* nacional da Embratel são baseados em um rígido SLA (*Service Level Agreement*), que contempla dois itens diferentes de desempenho: o circuito de acesso e o *backbone* nacional.

O circuito de acesso é empregado para se conectar um ISP ao *backbone* nacional da Embratel. Essa solução geralmente é implementada através de fibra ótica, rádio enlace ou LPCD (Linha Privativa de Comunicação de Dados). Para essas tecnologias, adotam-se alguns parâmetros e valores-objetivo conforme a Tabela 5.1.

O valor-objetivo para o tempo de resposta apresentado não se aplica para circuitos de acesso implementados eventualmente através de solução via satélite devido ao atraso inerente a essa tecnologia [54].

Tabela 5.1 - Parâmetros e valores-objetivo de um circuito de acesso

Parâmetro	Objetivo
Tempo de resposta (milisegundos)	75 ms (máximo)
Disponibilidade (%)	99,7 % (mínimo)

O *backbone* nacional envolve todos os equipamentos, excluindo o circuito de acesso. Entre a origem e o destino do tráfego, muitos ISPs podem utilizar diversas tecnologias de transporte (satélite, fibras óticas, etc.) e capacidades de enlace. Assim sendo, o *backbone* nacional da Embratel garante apenas a largura de banda disponível no circuito de acesso (levando-se em conta a tecnologia de transporte utilizada) e o desempenho da conexão entre o usuário e a sua porta de entrada no *backbone* [53].

Os níveis de desempenho garantidos pelo *backbone* nacional da Embratel são mostrados na Tabela 5.2.

Tabela 5.2 - Parâmetros e valores-objetivo no *backbone* nacional da Embratel

Parâmetro	Objetivo
Tempo de resposta (milisegundos)	75 ms (máximo)
Perda de Pacotes (%)	1 % (máximo)
Tempo de recuperação de falhas (horas)	4 horas (máximo)
Disponibilidade (%)	99,7 % (mínimo)

5.3. Modelo de Simulação

Em simulação, os experimentos são realizados com um modelo do sistema e não com o sistema. Um estudo por simulação de um sistema começa extraindo-se as características importantes deste sistema. Esse processo, que envolve uma certa medida de abstração, é conhecido como modelagem [55]. O modelo utilizado na simulação é apresentado na Figura 5.2. Este modelo simplificado considera apenas os Centros de Roteamento do Estado de São Paulo, tendo em vista a simulação do comportamento de todo o *backbone*, porém em uma escala menor. O modelo simulado é um ISP regional, onde um ISP local está conectado através do LER (*Label Edge Router*) presente em Santos (STS). Os roteadores de borda são responsáveis por efetuar o mapeamento do tráfego oriundo dos ISPs locais em classes DiffServ, permitindo seu encaminhamento com diferenciação de serviços.

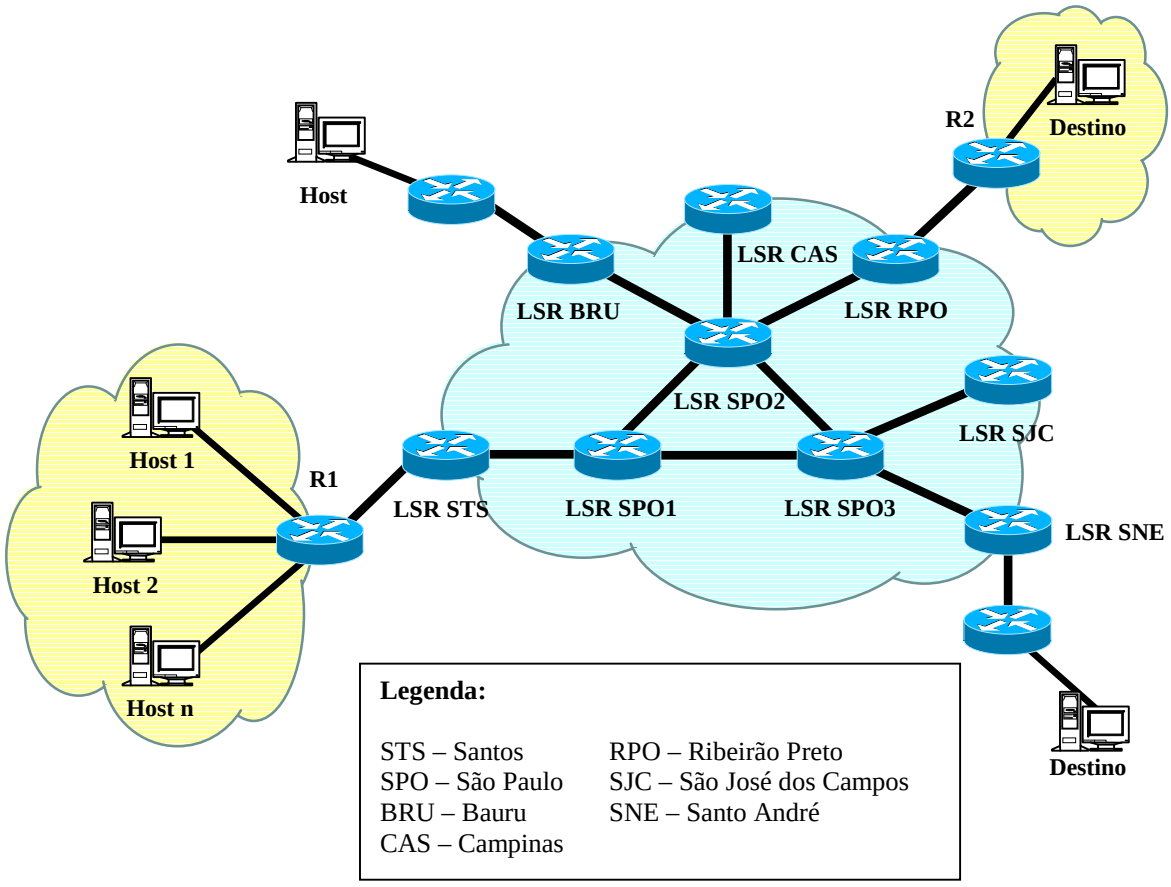


Figura 5.2 - Modelo de Simulação

A largura de banda dos enlaces entre o ISP regional e o ISP local tem 2 Mbps com atraso de 10 ms. Dentro do ISP regional, os enlaces dos roteadores de borda tem 1 Mbps, enquanto que as conexões entre os roteadores de núcleo operam a 2 Mbps, todos com atraso de 10 ms.

Nas simulações referentes aos experimentos de 1 a 4, o ISP local possui três tipos de fontes geradoras de tráfego ilustradas na Tabela 5.3: uma fonte para simular o tráfego de voz, uma fonte para tráfego de dados preferencial e uma terceira para o tráfego de dados com serviço de melhor esforço.

Tabela 5.3 - Classificação das aplicações

Tráfego	Aplicação	PHB
UDP	Voz	EF - Expedited Forwarding
TCP-1	FTP	AF1 - Assured Forwarding
TCP-2	FTP	BE - Best Effort

O tráfego de voz é simulado através de uma fonte de tráfego CBR (*Constant Bit Rate*), utilizando o UDP (*User Datagram Protocol*) como protocolo de transporte. O tráfego é modelado a uma taxa de 128 Kbps, sendo que os pacotes de 80 bytes são encaminhados a cada 5 ms. Ao entrar no ISP regional, os pacotes UDP são mapeados com o PHB EF, cuja característica é garantir um valor baixo no atraso, *jitter* e perda de pacotes.

Os tráfegos de dados preferencial e *best effort* são gerados por fontes FTP (*File Transfer Protocol*) transportados pelo TCP (*Transmission Control Protocol*). Na simulação do domínio DiffServ, o tráfego preferencial é mapeado com o PHB AF que permite uma priorização em relação ao tráfego *best effort*, mapeado com o PHB BE.

No experimento 5, o ISP local possui quatro fontes de tráfego CBR, permitindo simular a disputa de alguns tráfegos multimídia pelos recursos de rede. Todos são transportados através do protocolo UDP e mapeados em classes DiffServ ao entrar no ISP regional.

No LER em Bauru (BRU), considera-se a existência de fontes de tráfego FTP transportados pelo TCP, tendo como destino o Centro de Roteamento em Santo André (SNE). Este tráfego permanece ativo durante todo o período de simulação e não é analisado neste estudo, pois sua função é gerar um tráfego secundário de "retaguarda" (*background*), cujo objetivo é competir com o tráfego multimídia submetendo-o a interferências comuns em uma rede IP [61].

Todas as simulações foram feitas com duração de 60 segundos. Esse período de simulação foi considerado suficiente para se alcançar uma condição de regime permanente, pois foram realizados testes com tempos de simulação maiores com pouca variação nos resultados obtidos. Cada experimento foi simulado 5 vezes, pois números maiores de replicações não alteraram de forma significativa os resultados. O nível de confiança utilizado foi de 95 %.

5.3.1. Simulador de Redes NS

As simulações apresentadas neste trabalho foram realizadas com o auxílio do simulador de redes NS (*Network Simulator*) [56]. Implementado em duas linguagens, C++ e OTcl (*Object Tool Command Language*), o NS é bastante utilizado em pesquisas na área de redes de comunicações e provê suporte para a simulação de protocolos de roteamento, protocolos TCP e UDP, e protocolos *multicast*, tanto em redes convencionais como em redes sem fio [57].

Utilizou-se a versão all-in-one-2.1b6a, em uma ambiente Red Hat Linux 6.2, versão 2.2.14, em um computador Pentium 233 MHz com 64 MB de memória. Os módulos MNS

v2.0 [58] e DiffServ [59] foram adicionados para permitir a simulação de serviços diferenciados em redes MPLS.

O *Network Simulator* está sendo muito utilizado no meio acadêmico, tornando-se um padrão para a comunidade científica, principalmente por ser um programa de código aberto e gratuito. Além de prover uma grande quantidade de protocolos e tecnologias existentes, permite ainda o desenvolvimento de novos protocolos. Dentre as limitações desse simulador, destaca-se sua limitação para o estudo aplicado apenas de protocolos/tecnologias no padrão IP. Outra desvantagem é sua curva de aprendizado difícil para iniciantes e, à medida que se necessita desenvolver novos protocolos ou mecanismos não existentes, deve-se ter intimidade no desenvolvimento em C++ e desvendar seu esquema de hierarquias de classe para saber onde novas classes podem ser derivadas e encaixadas [61].

Suporte ao MPLS

O simulador de redes MPLS (MNS - *MPLS Network Simulator*) é uma extensão ao NS-2 para permitir a simulação de diversas aplicações MPLS reduzindo a necessidade de se construir uma rede real. Suporta diversas funcionalidades específicas à tecnologia MPLS como: operações de troca de rótulo, atualizações de tabelas NHLFE, encaminhamento de mensagens LDP e CR-LDP e estabelecimento de LSPs [60].

A versão utilizada nas simulações é a MNS v2.0, que é uma extensão da versão original. Entre as principais modificações, destaca-se a possibilidade de se estabelecer CR-LSPs (*Constraint-Based Routed Label Switching Path*) baseados em parâmetros como largura de banda, que permite sua utilização de acordo com os requisitos de QoS exigidos pelas aplicações. Essa versão também suporta a preempção de LSPs, sendo necessário informar a rota completa do CR-LSP com seus respectivos valores de prioridade de *Setup* e *Holding*.

Suporte aos Serviços Diferenciados

O módulo DiffServ é uma extensão ao simulador de redes NS com o objetivo de simular redes com serviços diferenciados. O módulo possui três componentes básicos que permitem seu funcionamento [59]:

- O cabeçalho IP foi modificado para incluir o DiffServ *codepoint* (DSCP).
- Introduziu-se uma etapa que analisa o comportamento de cada tipo de tráfego, verificando sua conformidade com o padrão previamente contratado. Este bloco denomina-se Condicionador ou Limitador. Se os pacotes EF não estiverem de acordo com o padrão contratado, o condicionador simplesmente os descarta. No caso do tráfego AF, o condicionador remarca os pacotes reduzindo sua prioridade, tendo o descarte como última ação a ser tomada.
- Um escalonador foi adicionado, consistindo em filas específicas a cada classe de serviço (EF, AF e BE). As filas utilizam o esquema de escalonamento WRR (*Weighted Round Robin*).

5.4. Apresentação e Análise de Resultados

Cinco cenários são avaliados, e os resultados obtidos são analisados tendo como foco a QoS oferecida aos diversos tipos de tráfego presentes na rede. No primeiro cenário utiliza-se o roteamento IP tradicional, sem nenhum mecanismo de QoS. No segundo cenário utiliza-se o mecanismo DiffServ para prover a diferenciação de serviços, enquanto que o terceiro cenário utiliza apenas o encaminhamento de pacotes provido pela tecnologia MPLS. No quarto cenário, as tecnologias MPLS e DiffServ são combinadas. Finalmente, no último cenário utiliza-se a preempção de LSPs como forma de garantir a QoS dos tráfegos de maior importância.

Para todos os cenários obteve-se gráficos de vazão, atraso, *jitter* e perda de pacotes, que são os principais parâmetros para a avaliação do nível de QoS. O tempo de simulação utilizado em todos os gráficos é de 60 segundos.

5.4.1. Cenário 1: Rede IP Tradicional

No primeiro cenário avaliado, utilizou-se apenas o serviço de melhor esforço oferecido atualmente pela Internet. Todos os tráfegos receberam o mesmo tratamento no encaminhamento de pacotes e utilizaram a rota de menor caminho disponível, formada pelos roteadores STS, SPO1, SPO2 e RPO dentro do ISP regional.

A Figura 5.3 ilustra a vazão alcançada pelos três tráfegos, onde é possível observar os dois tráfegos TCP tendo seu desempenho afetado quando em presença do tráfego UDP. Devido ao mecanismo de controle de congestionamento, as fontes TCP reduzem a taxa de envio de pacotes ao detectarem congestionamento na rede. Assim, o desempenho do tráfego TCP é prejudicado em redes que não oferecem um tratamento diferenciado às aplicações, resultando em uma distribuição irregular dos recursos disponíveis. A Tabela 5.4 mostra o valor médio da vazão e intervalo de confiança dos tráfegos analisados.

O gráfico da Figura 5.4 mostra o atraso dos tráfegos TCP e UDP. É possível observar que o atraso da aplicação UDP é muito elevado, prejudicando o seu desempenho. Apesar do gráfico de vazão mostrar que a rede encaminha os pacotes UDP no nível desejado, o gráfico de atraso deixa claro a necessidade de se implementar uma política de priorização de serviços para a obtenção de QoS. O atraso médio e respectivo intervalo de confiança é mostrado na Tabela 5.5.

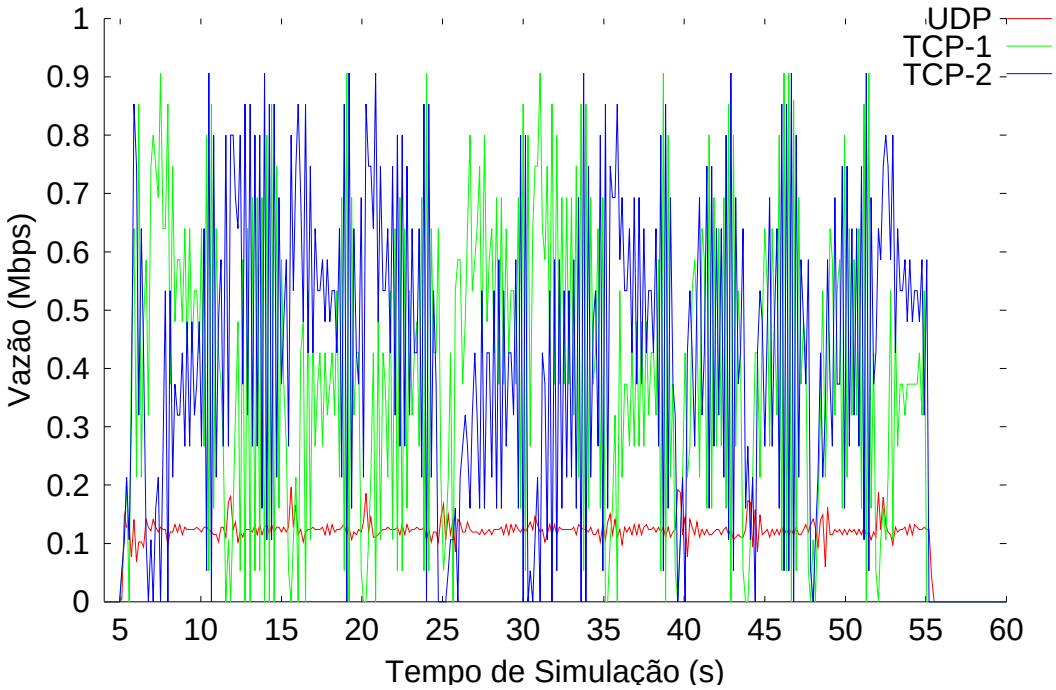


Figura 5.3 - Vazão em uma rede IP tradicional

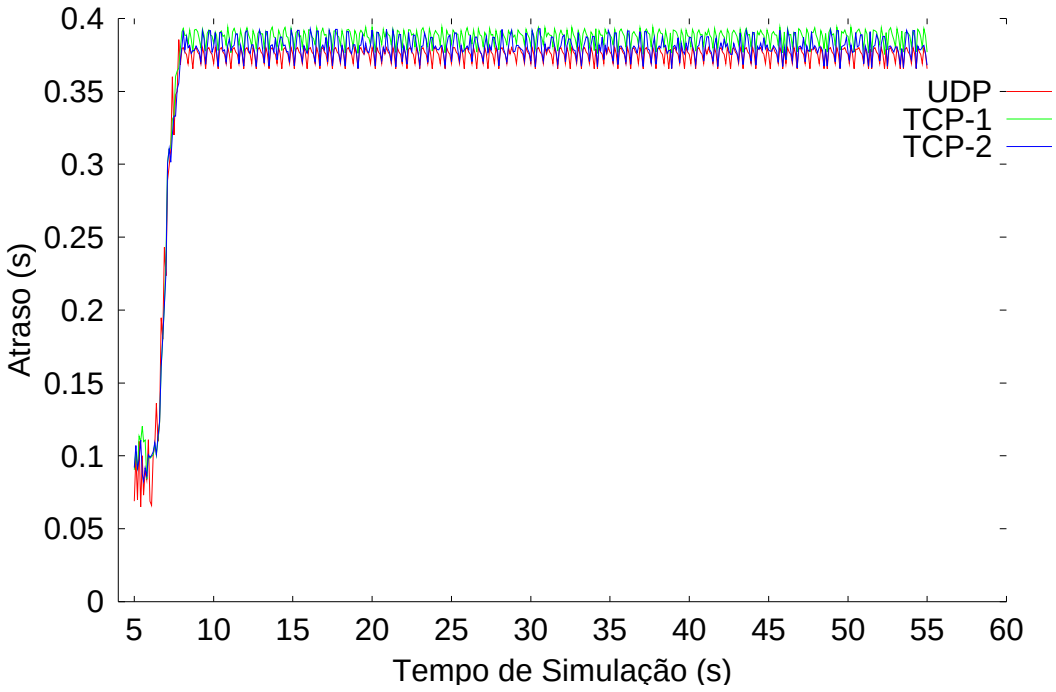


Figura 5.4 - Atraso em uma rede IP tradicional

Tabela 5.4 - Vazão média e intervalo de confiança em uma rede IP tradicional

Tráfego	Vazão Média (Kbps)	Intervalo de Confiança
UDP	123,3138	(121,4103 ; 125,2174)
TCP-1	401,7017	(373,9202 ; 429,4831)
TCP-2	435,9281	(407,9883 ; 463,8679)

Tabela 5.5 - Atraso médio e intervalo de confiança em uma rede IP tradicional

Tráfego	Atraso Médio (ms)	Intervalo de Confiança
UDP	363,5550	(358,8591 ; 368,2508)
TCP-1	375,2112	(370,4463 ; 379,9761)
TCP-2	368,3584	(363,6234 ; 373,0935)

Na Figura 5.5 observa-se o *jitter* sofrido pelos tráfegos. Da mesma forma que no gráfico anterior, é possível verificar que os valores são insuficientes aos requisitos de uma aplicação multimídia. Na Tabela 5.6 encontra-se o *jiiter* médio e o intervalo de confiança.

Algumas aplicações multimídia toleram um certo nível de perda de pacotes sem alterar de forma significativa a qualidade de reprodução. Porém, níveis elevados de descarte de pacotes podem prejudicar a qualidade e até mesmo impedir a transmissão. O gráfico da Figura 5.6 mostra o descarte de pacotes em cada instante de tempo simulado, enquanto que a Tabela 5.7 mostra o descarte médio de pacotes durante o período de simulação. O descarte de pacotes é medido na camada 3 (camada de rede) do modelo OSI (*Open Systems Interconnection*). Apesar dos valores serem baixos, é importante notar que o nível médio de perdas permitido no ambiente de rede considerado é de 1 %, o que permite concluir a ineficiência do método tradicional de encaminhamento de pacotes IP sem mecanismos de QoS.

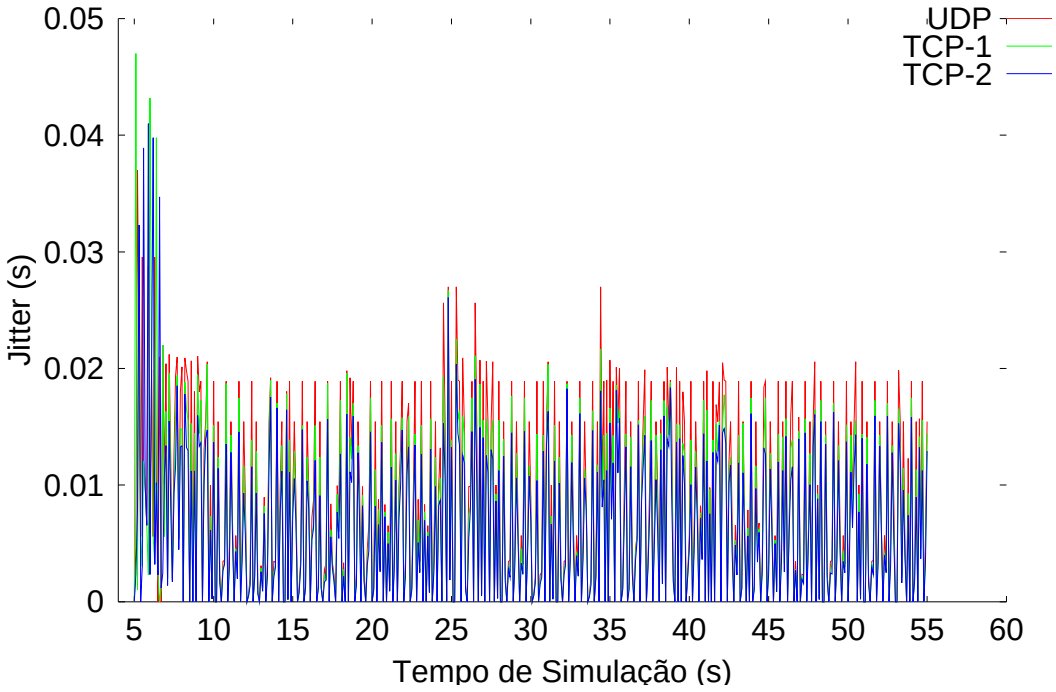


Figura 5.5 - *Jitter* em uma rede IP tradicional

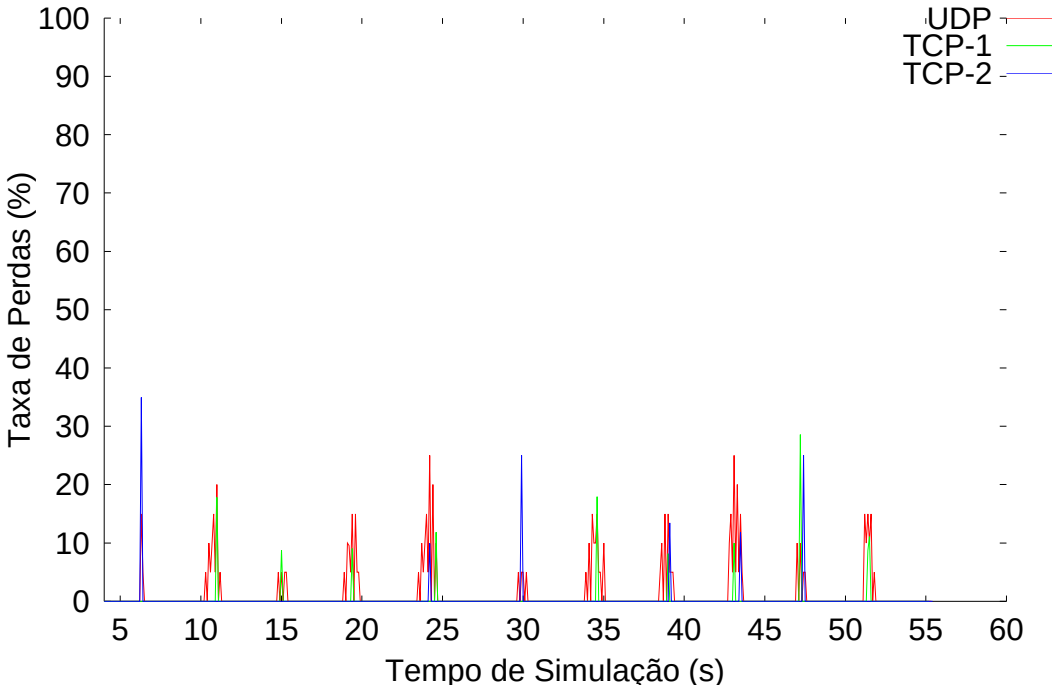


Figura 5.6 - Perda de pacotes em uma rede IP tradicional

Tabela 5.6 - *Jitter* médio e intervalo de confiança em uma rede IP tradicional

Tráfego	*Jitter* Médio (ms)	Intervalo de Confiança
UDP	8,3906	(7,6801 ; 9,1010)
TCP-1	7,1675	(6,5237 ; 7,8113)
TCP-2	6,2858	(5,7075 ; 6,8641)

Tabela 5.7 - Perda média e intervalo de confiança em uma rede IP tradicional

Tráfego	Perda Média (%)	Intervalo de Confiança
UDP	1,3190	(0,9844 ; 1,6536)
TCP-1	0,2627	(0,0839 ; 0,4415)
TCP-2	0,4377	(0,0169 ; 0,8585)

5.4.2. Cenário 2: Rede IP apenas com DiffServ

Os resultados obtidos no cenário anterior mostraram-se inadequados ao transporte conjunto de tráfegos UDP e TCP, devido à agressividade do tráfego de pacotes UDP e o controle de congestionamento do TCP. Neste segundo cenário, a rede foi configurada com a tecnologia DiffServ para prover diferenciação de serviços. Considera-se que os segmentos UDP são mapeados com o PHB EF e o tráfego TCP-1 é mapeado com PHB AF, podendo representar aplicações bancárias ou transferência de arquivos através de FTP. O tráfego TCP-2 foi mapeado com PHB BE, sendo encaminhado através do serviço de melhor esforço [03].

Na configuração do modelo DiffServ utilizou-se uma taxa de pico de 0,4 Mbps para o tráfego marcado com o PHB AF, enquanto que o tráfego com o PHB EF tem sua taxa de pico configurada em 128 Kbps. Os pacotes EF que não estiverem dentro do perfil configurado são descartados, e os pacotes AF têm sua prioridade remarcada para níveis mais baixos, podendo ser descartados caso não seja possível o encaminhamento. Utilizou-se como escalonador o

modelo CBQ (*Class Based Queueing*), onde o enlace de 1 Mbps foi divido em filas na proporção 4 : 4 : 2 para as classes de serviços EF, AF e BE.

O tamanho dos pacotes UDP é configurado em 80 bytes e encaminhados com um intervalo de 5 ms, gerando um tráfego constante de 128 Kbps. As fontes FTP utilizaram pacotes com o tamanho padrão disponível no simulador NS-2, que é de 1.500 bytes. Não é necessário configurar a taxa de transmissão, pois o protocolo TCP adapta a taxa de transmissão de acordo com as condições disponíveis na rede com o objetivo de utilizar a capacidade máxima do enlace disponível. A Figura 5.7 e a Tabela 5.8 mostram a vazão alcançada pelos tráfegos quando em presença do mecanismo DiffServ, sendo possível observar que o tráfego UDP manteve o seu nível estabelecido, enquanto que os tráfegos TCP utilizam a largura de banda disponível com menos oscilações que o modelo anterior.

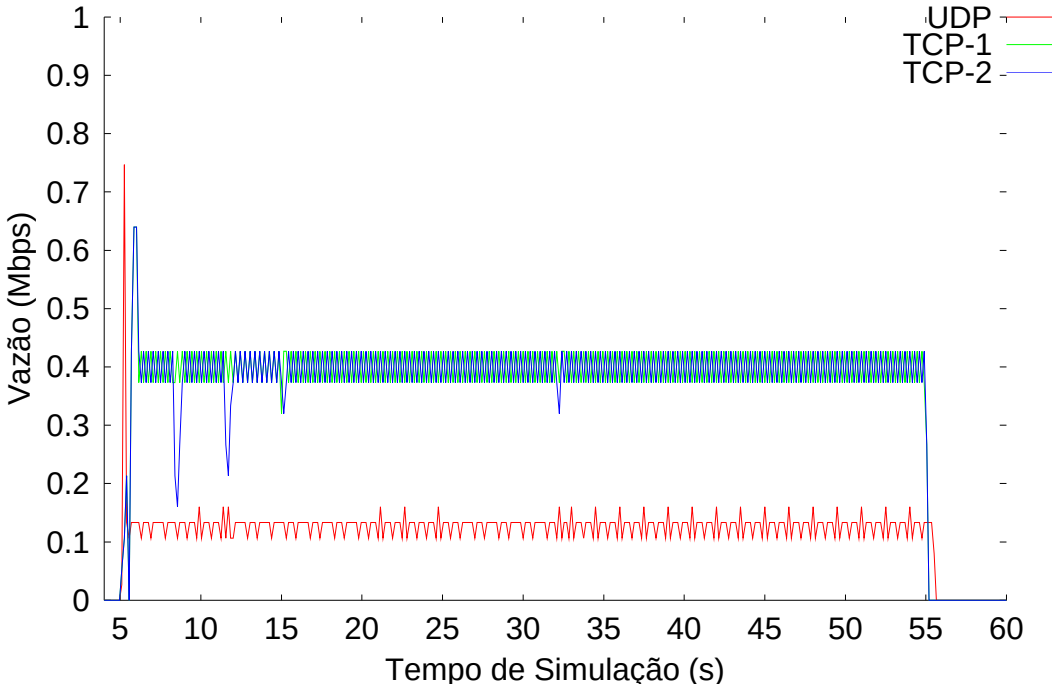


Figura 5.7 - Vazão em uma rede DiffServ

Tabela 5.8 - Vazão média e intervalo de confiança em uma rede DiffServ

Tráfego	Vazão Média (Kbps)	Intervalo de Confiança
UDP	127,3768	(123,4090 ; 131,3446)
TCP-1	397,2854	(392,1290 ; 402,4417)
TCP-2	394,1317	(388,4657 ; 399,7976)

A inclusão do modelo DiffServ também modificou intensamente o gráfico de atraso disponível na Figura 5.8. Observa-se a diferenciação de serviços nesta arquitetura, onde o tráfego UDP atingiu valores de atraso de 102 ms, satisfazendo os requisitos de QoS para um tráfego de voz ou de videoconferência. Para os tráfegos TCP observa-se uma redução do atraso comparado com o modelo anterior. A redução do tempo de atraso imposto pela rede pode ser um fator diferencial de um *backbone* em relação aos de outros ISPs.

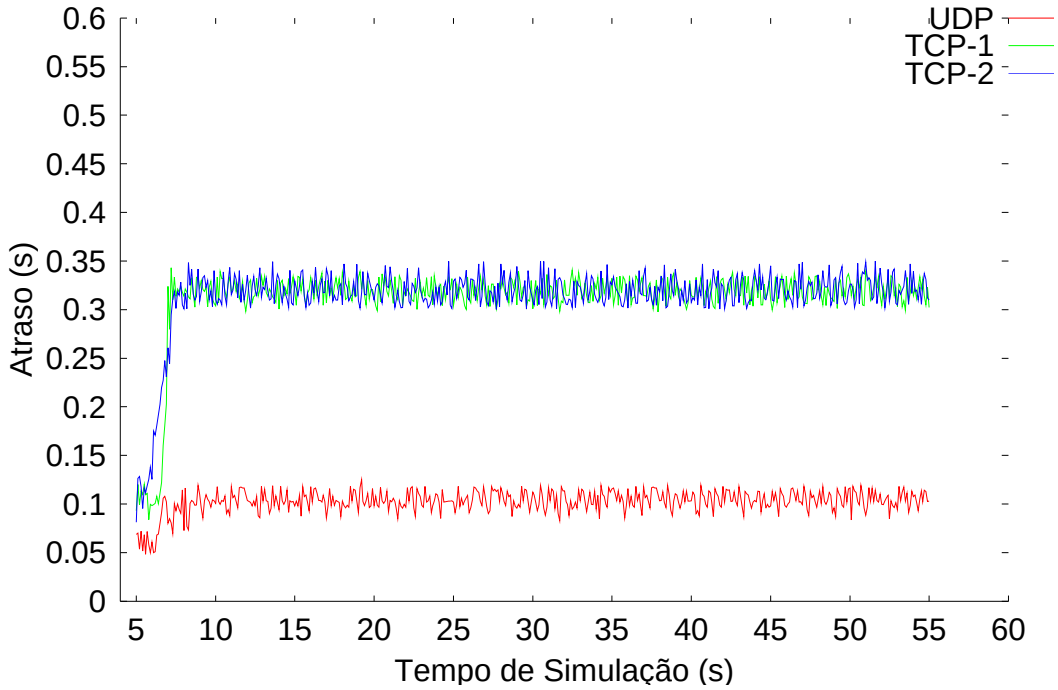


Figura 5.8 - Atraso em uma rede DiffServ

Tabela 5.9 - Atraso médio e intervalo de confiança em uma rede DiffServ

Tráfego	Atraso Médio (ms)	Intervalo de Confiança
UDP	102,6712	(101,6353 ; 103,7072)
TCP-1	311,6129	(307,9837 ; 315,2421)
TCP-2	313,6854	(310,5223 ; 316,8486)

A Figura 5.9 e a Tabela 5.10 ilustram o *jitter* sofrido pelas aplicações, com valores menores que os tipicamente obtidos no modelo atual da Internet.

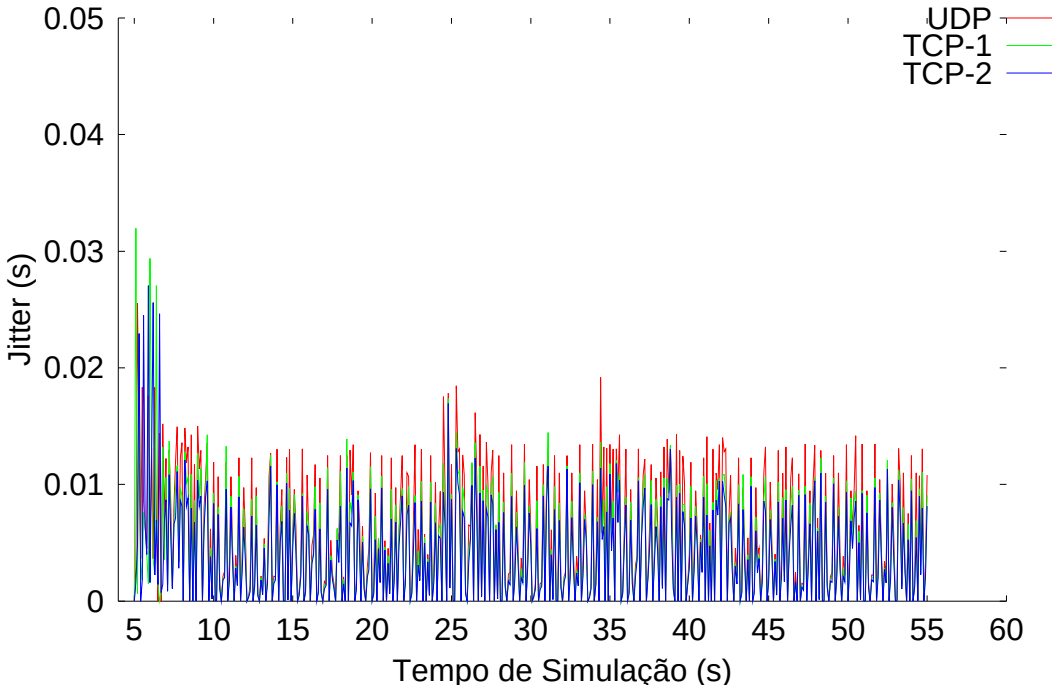


Figura 5.9 - *Jitter* em uma rede DiffServ

Tabela 5.10 - *Jitter* médio e intervalo de confiança em uma rede DiffServ

Tráfego	*Jitter* Médio (ms)	Intervalo de Confiança
UDP	5,5686	(5,0947 ; 6,0425)
TCP-1	4,6380	(4,2159 ; 5,0602)
TCP-2	4,0663	(3,6887 ; 4,4440)

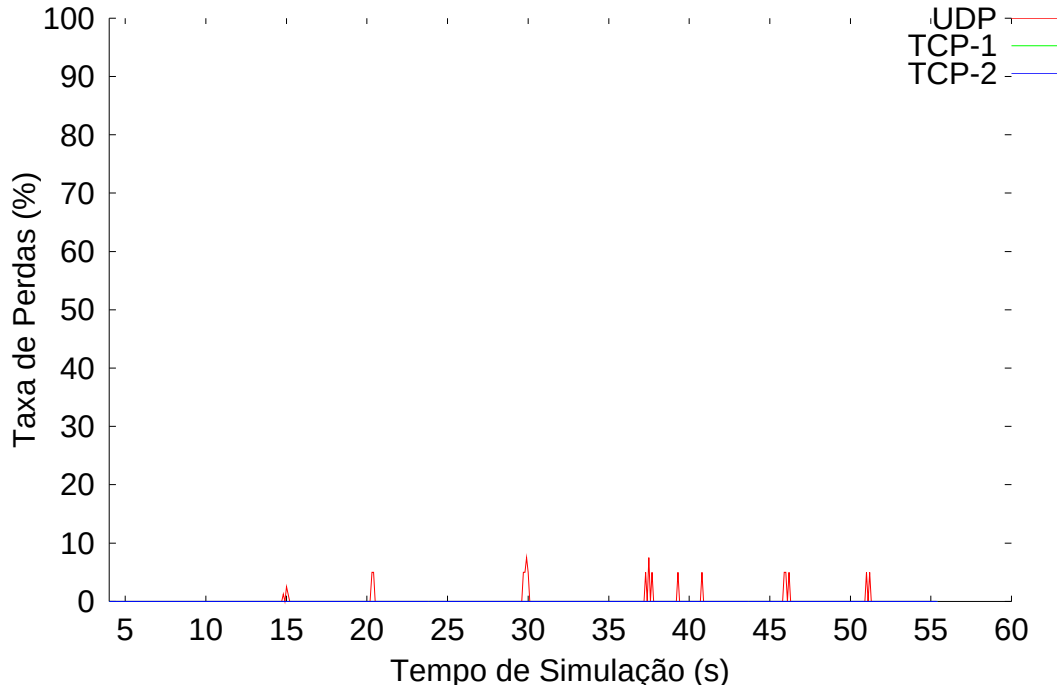


Figura 5.10 - Perda de pacotes em uma rede DiffServ

Tabela 5.11 - Perda média e intervalo de confiança em uma rede DiffServ

Tráfego	Perda Média (%)	Intervalo de Confiança
UDP	0,1800	(0,0962 ; 0,2637)
TCP-1	0	(0 ; 0)
TCP-2	0	(0 ; 0)

Na Figura 5.10 observa-se a redução no nível de perdas de pacotes das aplicações, com nenhum descarte para os tráfegos TCP. Há uma sensível redução na perda dos pacotes UDP durante todo o período de simulação, como pode ser observado na Tabela 5.11. Isto ocorre devido ao método imposto pelo mecanismo DiffServ, que imediatamente descarta os pacotes contendo UDP que não estiverem em conformidade com o padrão esperado, enquanto que para os pacotes contendo TCP o modelo reduz sua prioridade, postergando o descarte apenas como última ação a ser tomada.

5.4.3. Cenário 3: Rede IP apenas com MPLS

Como discutido anteriormente, o modelo MPLS não oferece QoS às aplicações. As principais habilidades desta arquitetura estão na facilidade de se implementar engenharia de tráfego e no seu processo rápido de encaminhamento de pacotes.

Neste cenário foi estabelecido um E-LSP através dos roteadores em STS, SPO1, SPO2 e RPO. Como pode ser observado nos gráficos das Figuras 5.11, 5.12, 5.13 e 5.14, e nos valores das Tabelas 5.12, 5.13, 5.14 e 5.15, não houve modificações significativas nos resultados alcançados em relação ao modelo IP tradicional simulado no cenário 1, devido à inexistência de mecanismos de QoS no modelo MPLS. A engenharia de tráfego poderia ser utilizada com o objetivo de dividir o tráfego em rotas diferentes, resultando em uma melhor utilização dos enlaces disponíveis. Porém, no modelo de rede utilizado não existem rotas alternativas para se distribuir o tráfego; além disso, o objetivo deste trabalho é mostrar o uso da preempção em uma rede MPLS/DiffServ, ficando essa solução, portanto, fora do contexto deste estudo.

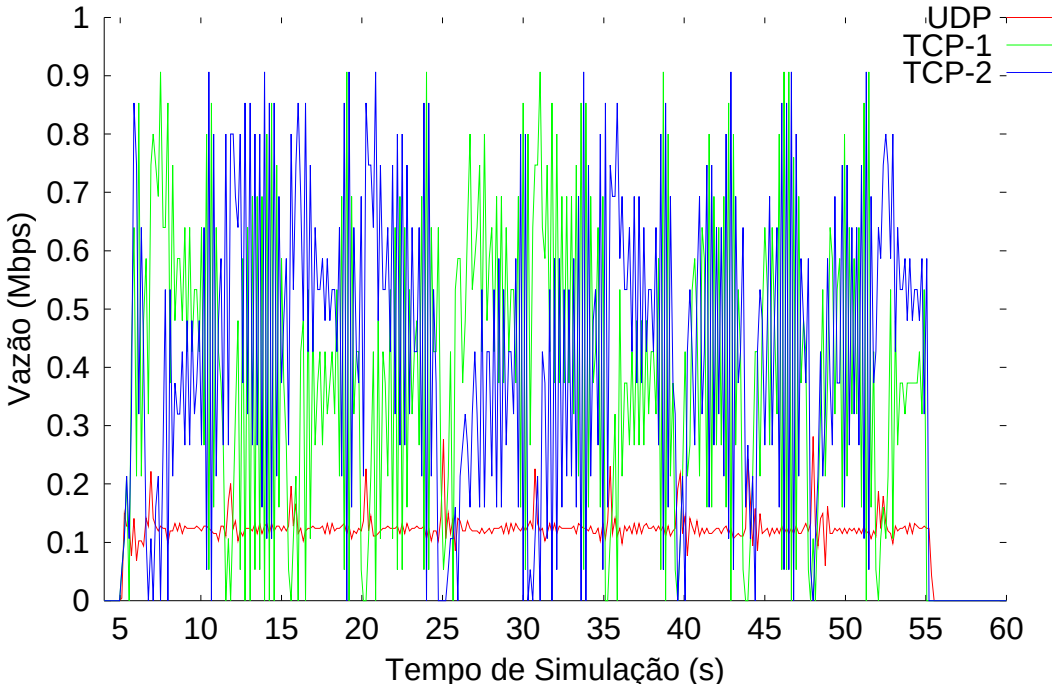


Figura 5.11 - Vazão em uma rede MPLS

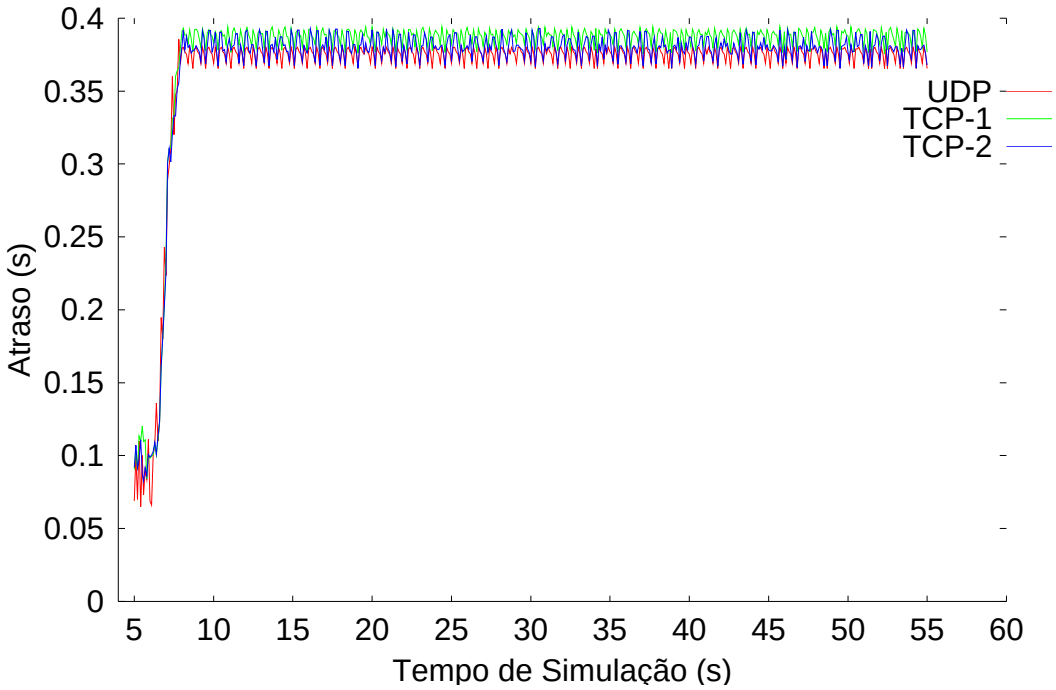


Figura 5.12 - Atraso em uma rede MPLS

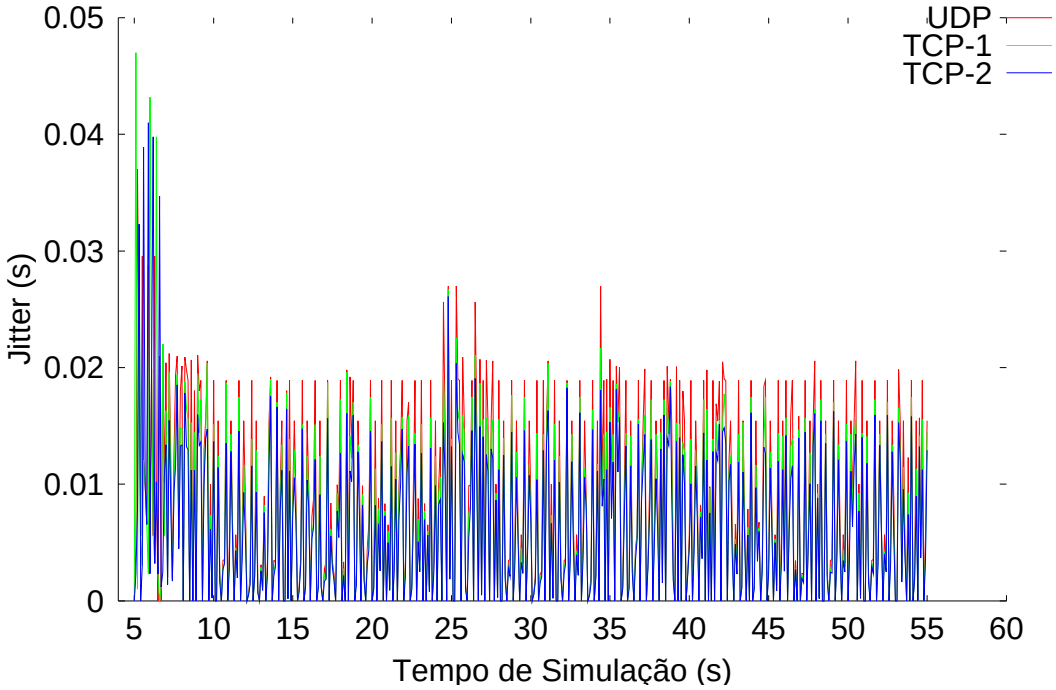


Figura 5.13 - *Jitter* em uma rede MPLS

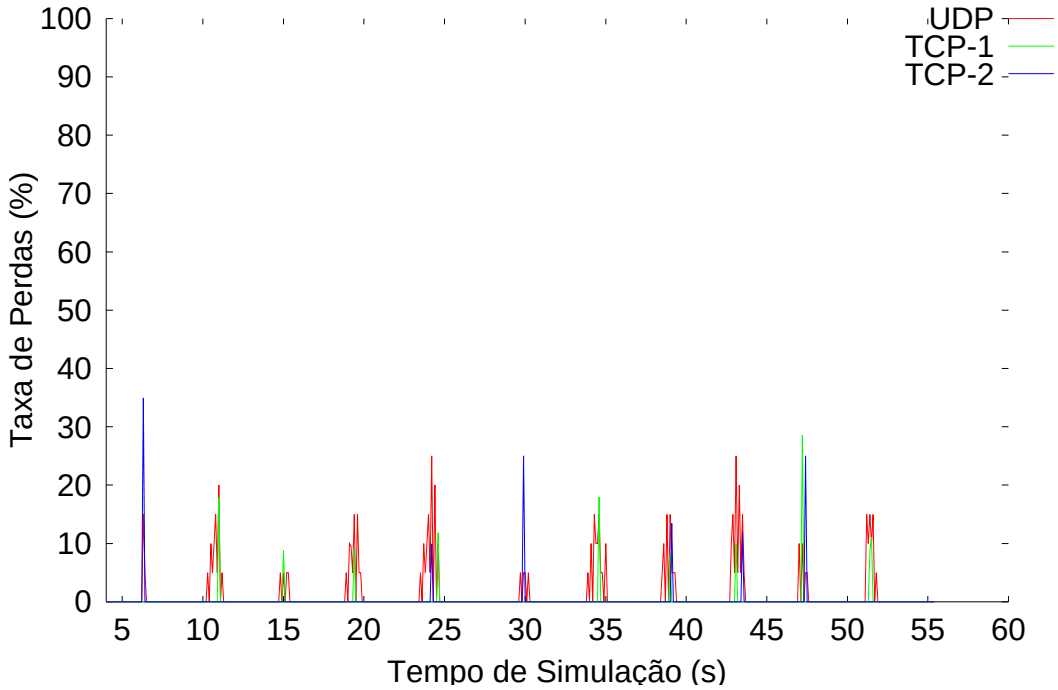


Figura 5.14 - Perda de pacotes em uma rede MPLS

Tabela 5.12 - Vazão média e intervalo de confiança em uma rede MPLS

Tráfego	Vazão Média (Kbps)	Intervalo de Confiança
UDP	125,3079	(122,6449 ; 127,9709)
TCP-1	401,4014	(373,6710 ; 429,1317)
TCP-2	435,9281	(407,9883 ; 463,8679)

Tabela 5.13 - Atraso médio e intervalo de confiança em uma rede MPLS

Tráfego	Atraso Médio (ms)	Intervalo de Confiança
UDP	365,5961	(362,1277 ; 369,0645)
TCP-1	377,7906	(373,4381 ; 382,1431)
TCP-2	367,9069	(362,9705 ; 372,8433)

Tabela 5.14 - *Jitter* médio e intervalo de confiança em uma rede MPLS

Tráfego	*Jitter* Médio (ms)	Intervalo de Confiança
UDP	8,3811	(7,6698 ; 9,0925)
TCP-1	7,1818	(6,5351 ; 7,8285)
TCP-2	6,2818	(5,7020 ; 6,8616)

Tabela 5.15 - Perda média e intervalo de confiança em uma rede MPLS

Tráfego	Perda Média (%)	Intervalo de Confiança
UDP	1,3164	(0,9818 ; 1,6509)
TCP-1	0,2632	(0,0841 ; 0,4424)
TCP-2	0,4403	(0,0171 ; 0,8635)

5.4.4. Cenário 4: Rede IP com MPLS/DiffServ

Neste cenário, considerou-se uma rede MPLS com suporte a serviços diferenciados. Utilizando os mesmos mecanismos dos cenários 2 e 3, o roteador de borda STS faz o mapeamento dos tráfegos em classes DiffServ. Além disso, criou-se um LSP entre os roteadores STS, SPO1, SPO2 e RPO, para o encaminhamento dos três tráfegos.

Como pode ser observado nas Figuras 5.15, 5.16, 5.17 e 5.18, e nas Tabelas 5.16, 5.17, 5.18 e 5.19, os resultados são praticamente iguais aos resultados obtidos com o *backbone* funcionando apenas com a arquitetura DiffServ. Isto se deve ao fato de não ter sido utilizado a principal vantagem do MPLS, que é a engenharia de tráfego. Como foi implementado apenas um LSP percorrendo o mesmo caminho utilizado pelo cenário anterior, os resultados ficaram muito semelhantes.

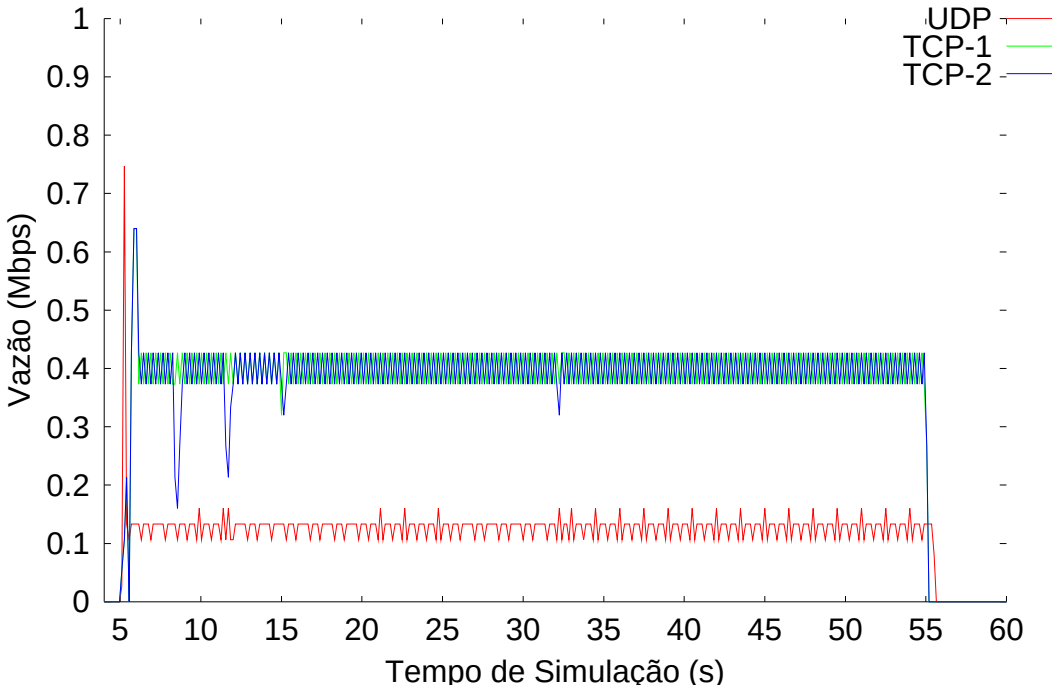


Figura 5.15 - Vazão em uma rede MPLS/DiffServ

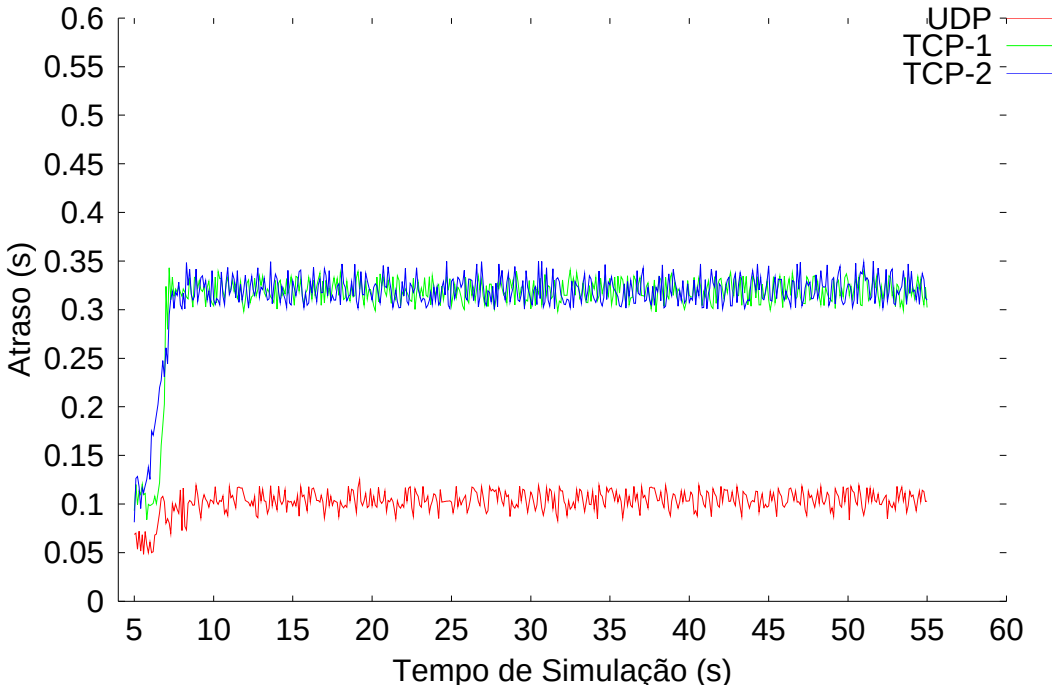


Figura 5.16 - Atraso em uma rede MPLS/DiffServ

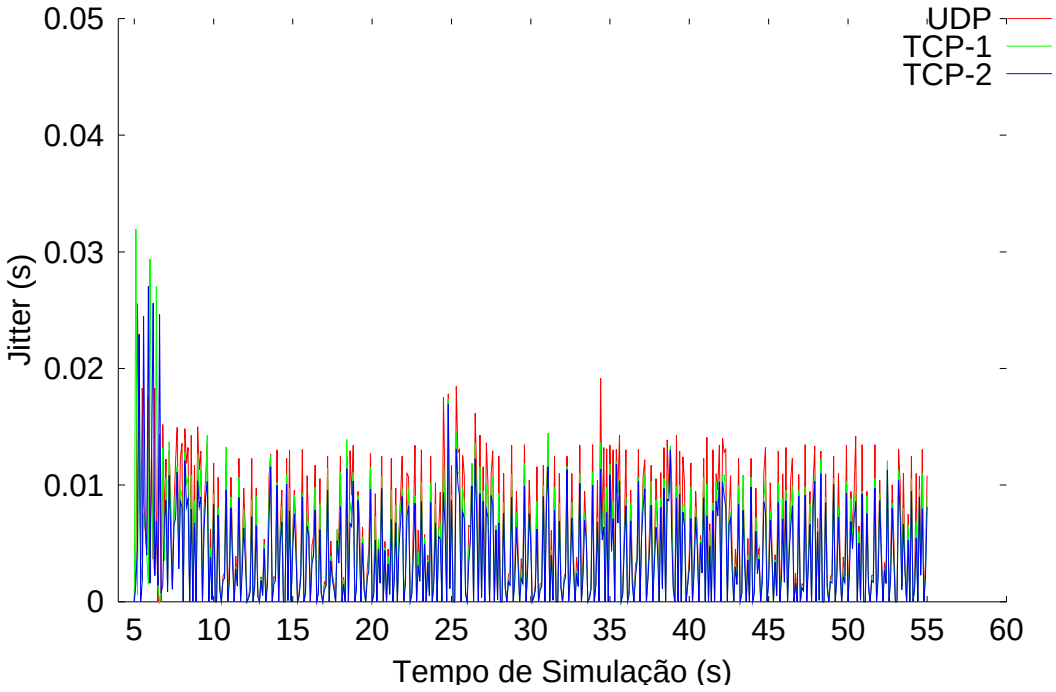


Figura 5.17 - *Jitter* em uma rede MPLS/DiffServ

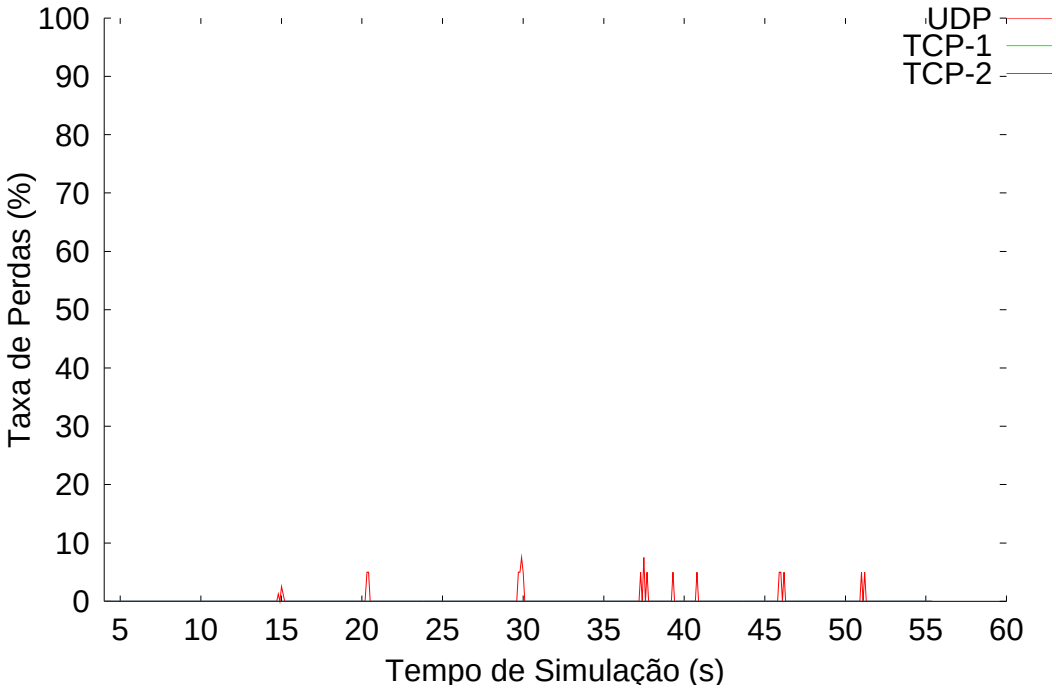


Figura 5.18 - Perda de pacotes em uma rede MPLS/DiffServ

Tabela 5.16 - Vazão média e intervalo de confiança em uma rede MPLS/DiffServ

Tráfego	Vazão Média (Kbps)	Intervalo de Confiança
UDP	127,4779	(123,5101 ; 131,4457)
TCP-1	397,0168	(391,8604 ; 402,1731)
TCP-2	394,7483	(389,0824 ; 400,4142)

Tabela 5.17 - Atraso médio e intervalo de confiança em uma rede MPLS/DiffServ

Tráfego	Atraso Médio (ms)	Intervalo de Confiança
UDP	102,2895	(101,2536 ; 103,3255)
TCP-1	312,1083	(308,4791 ; 315,7375)
TCP-2	313,9581	(310,7949 ; 317,1212)

Tabela 5.18 - *Jitter* médio e intervalo de confiança em uma rede MPLS/DiffServ

Tráfego	*Jitter* Médio (ms)	Intervalo de Confiança
UDP	5,6038	(5,1299 ; 6,0777)
TCP-1	4,6036	(4,1814 ; 5,0258)
TCP-2	3,8957	(3,5180 ; 4,2734)

Tabela 5.19 - Perda média e intervalo de confiança em uma rede MPLS/DiffServ

Tráfego	Perda Média (%)	Intervalo de Confiança
UDP	0,1799	(0,0952 ; 0,2645)
TCP-1	0	(0 ; 0)
TCP-2	0	(0 ; 0)

5.4.5. Cenário 5: Rede IP com MPLS/DiffServ e Preempção de LSPs

Baseado em [61], utilizou-se quatro fontes CBR com o protocolo UDP, permitindo simular o encaminhamento de alguns tráfegos pelo ISP modelado, conforme ilustra a Tabela

5.20. Quatro *hosts* conectados em R1 são responsáveis por gerar as fontes de tráfego, sendo o *host* conectado em R2 o mesmo destino para todos os fluxos. Ao entrar no ISP regional estruturado com as tecnologias MPLS/DiffServ, os tráfegos são mapeados em classes DiffServ e inseridos em LSPs com diferentes prioridades de *Setup* e *Holding*.

Neste caso foram realizados dois experimentos. No primeiro experimento nenhuma política de preempção foi considerada, enquanto que no segundo experimento utilizou-se a preempção para garantir o encaminhamento adequado de uma aplicação considerada mais importante. Com isso é possível avaliar através de comparação o impacto que a preempção exerce sobre as aplicações.

Tabela 5.20 - Mapeamento de tráfegos e prioridades de LSPs

Tráfego	Aplicação	Taxa de Geração (Kbps)	PHB	Prioridade de Setup	Prioridade de Holding
UDP-1	Áudio	250 Kbps	EF	2	1
UDP-2	Vídeo	700 Kbps	AF1	4	2
UDP-3	Vídeo Conferência	500 Kbps	AF2	6	5
UDP-4	Dados	120 Kbps	BE	7	3

Cenário 5a: Avaliação da rede MPLS/DiffServ sem preempção

Neste cenário, apenas os tráfegos EF, AF2 e BE iniciam a transmissão de pacotes, onde é possível observar na Figura 5.19 que eles atingem a vazão desejada. A fonte AF1 inicia a transmissão de pacotes no instante t = 30 s, resultando em uma disputa de recursos com as outras aplicações devido à escassez de largura de banda nos enlaces. Observa-se que o tráfego AF2 tem uma expressiva queda de desempenho. Além disso, a vazão observada do tráfego

AF1 é inferior à taxa de geração de 700 Kbps, o que pode resultar em uma perda na qualidade de um sinal de vídeo. O tráfego BE também tem seu desempenho afetado, devido à concorrência pelos recursos disponíveis, enquanto que o tráfego EF mantém inalterada sua vazão, devido a maior prioridade de encaminhamento. A Tabela 5.21 ilustra a vazão média e intervalo de confiança dos tráfegos analisados em dois períodos diferentes: antes e após o tráfego AF1 iniciar a transmissão de pacotes.

Como não foi implementada nenhuma política de preempção, todos os tráfegos permanecem ativos no *backbone* sem nenhuma alteração em sua prioridade, mesmo sem largura de banda suficiente para acomodar todas as aplicações. A Figura 5.20 ilustra o atraso dos tráfegos, onde é possível observar um aumento no atraso dos pacotes após a nova aplicação AF1 iniciar sua transmissão. Novamente, apenas o fluxo EF permanece com os mesmos níveis de atraso.

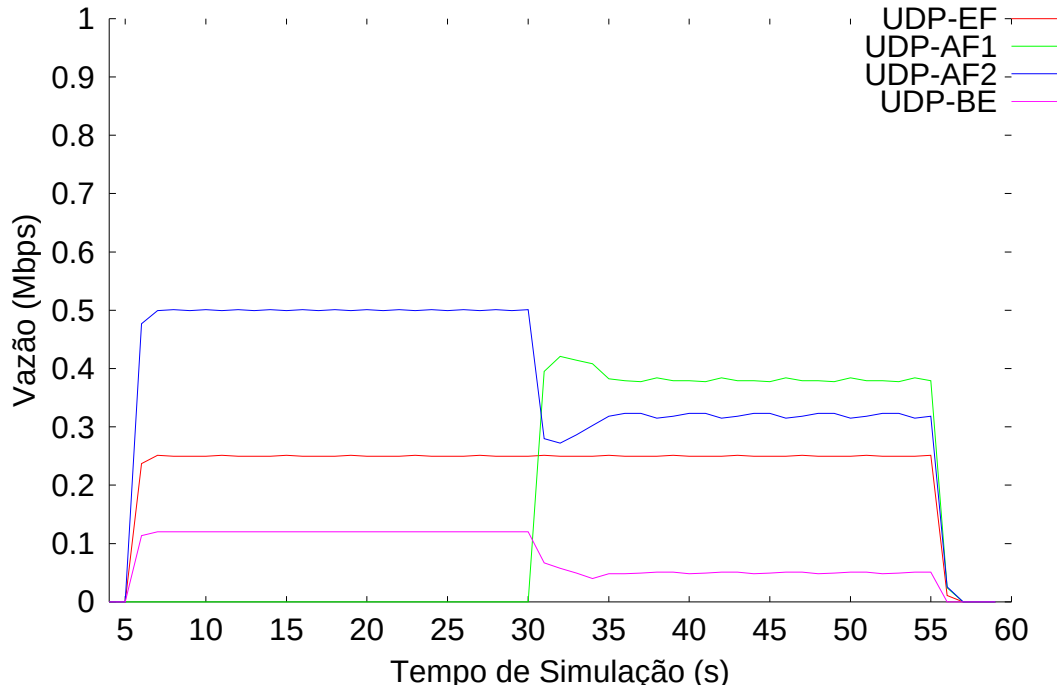


Figura 5.19 - Vazão em uma rede MPLS/DiffServ sem preempção

Tabela 5.21 - Vazão média e intervalo de confiança em uma rede MPLS/DiffServ sem preempção

	T < 30 s		T > 30 s	
Tráfego	Vazão Média (Kbps)	Intervalo de Confiança	Vazão Média (Kbps)	Intervalo de Confiança
UDP-EF	239,8769	(221,0428 ; 258,7110)	240,8615	(222,8542 ; 258,8687)
UDP-AF1	-x-	-x-	370,9538	(343,3862 ; 398,5214)
UDP-AF2	479,8769	(442, 2134 ; 517,5403)	303,2615	(280,8534 ; 325,6696)
UDP-BE	115,1384	(106,0989 ; 124,1780)	48,5538	(44,3864 ; 52,7212)

Na Figura 5.21 observa-se um aumento no *jitter* dos tráfegos AF2 e BE quando o tráfego AF1 está presente. O tráfego EF não sofreu variações devido a sua maior prioridade em relação aos demais. A Figura 5.22 mostra a taxa de perda de pacotes, permitindo visualizar um índice baixo de descarte, mesmo quando ocorre disputa por recursos. As Tabelas 5.22, 5.23 e 5.24 mostram os valores médios de vazão, *jitter* e perda de pacotes.

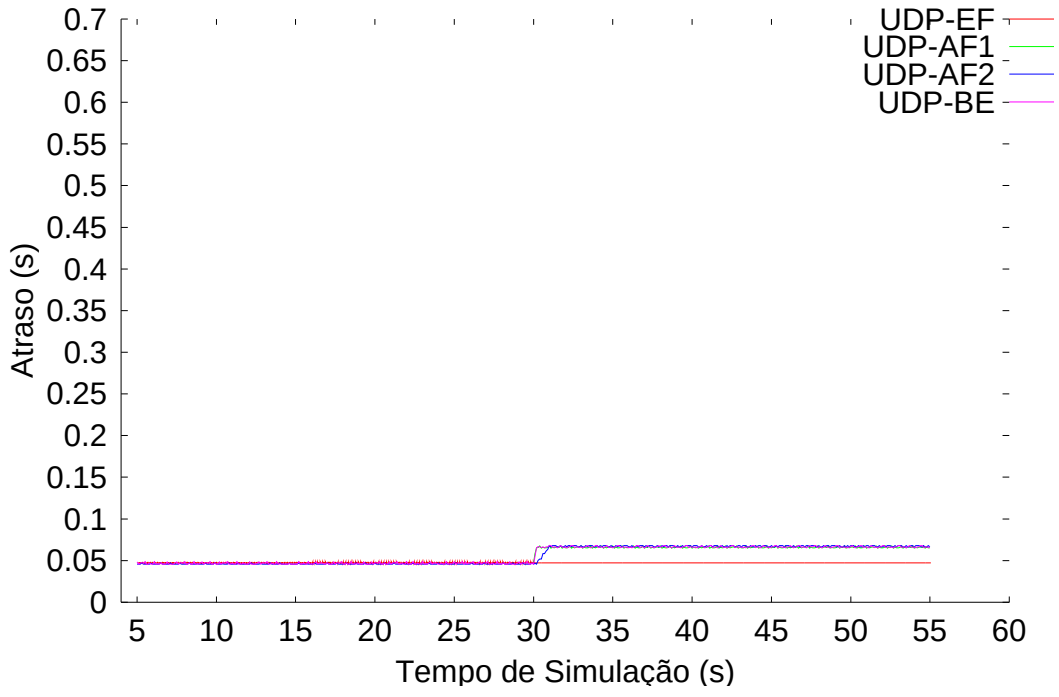


Figura 5.20 - Atraso em uma rede MPLS/DiffServ sem preempção

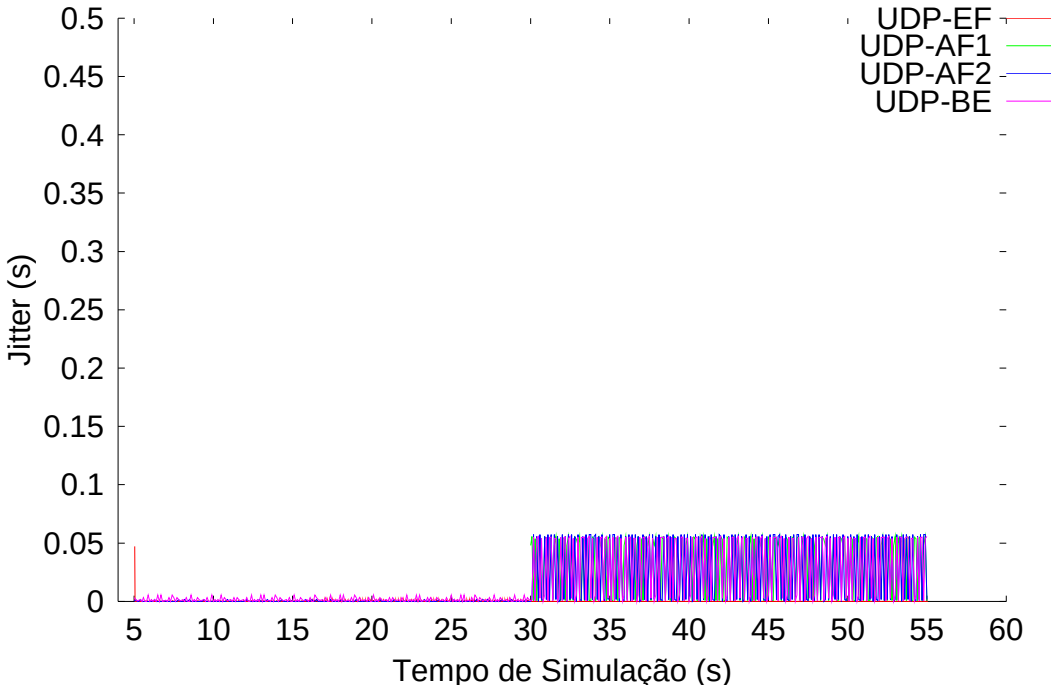


Figura 5.21 - *Jitter* em uma rede MPLS/DiffServ sem preempção

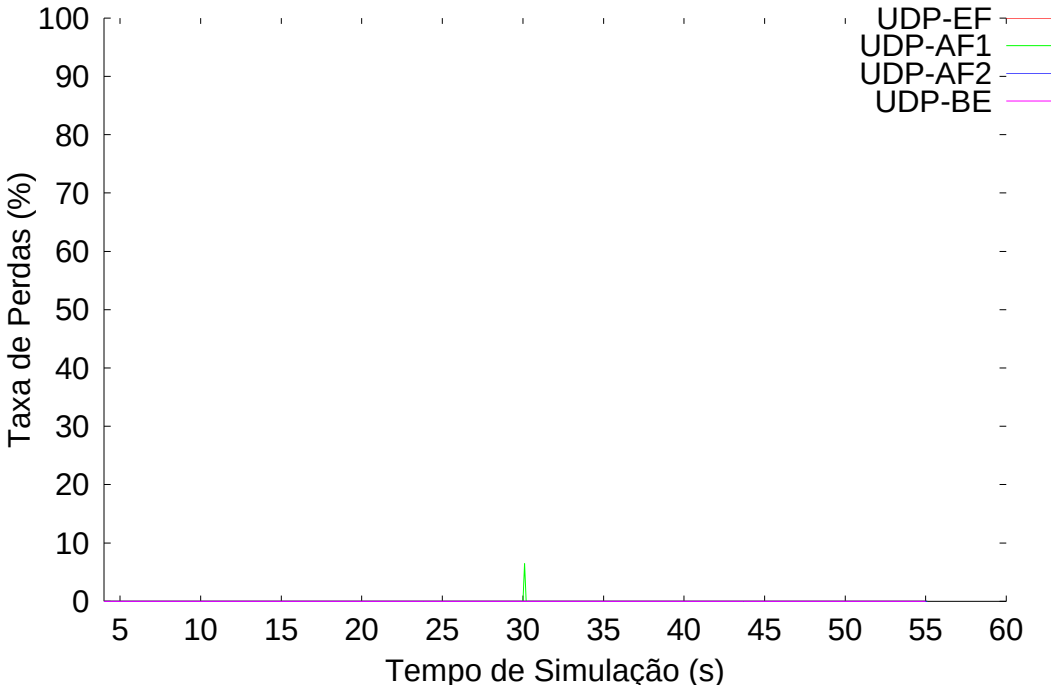


Figura 5.22 - Perda de pacotes em uma rede MPLS/DiffServ sem preempção

Tabela 5.22 - Atraso médio e intervalo de confiança em uma rede MPLS/DiffServ sem preempção

	T < 30 s		T > 30 s	
Tráfego	Atraso Médio (ms)	Intervalo de Confiança	Atraso Médio (ms)	Intervalo de Confiança
UDP-EF	47,2361	(47,1965 ; 47,2756)	47,2001	(47,1986 ; 47,2015)
UDP-AF1	-x-	-x-	65,8604	(65,6737 ; 66,0470)
UDP-AF2	45,8199	(45,3737 ; 46,2661)	66,7166	(63,7906 ; 69,6426)
UDP-BE	46,5322	(45,5465 ; 47,5179)	66,3546	(64,8292 ; 67,8801)

Tabela 5.23 - *Jitter* médio e intervalo de confiança em uma rede MPLS/DiffServ sem preempção

	T < 30 s		T > 30 s	
Tráfego	*Jitter* Médio (ms)	Intervalo de Confiança	*Jitter* Médio (ms)	Intervalo de Confiança
UDP-EF	0,1215	(0,0309 ; 0,2120)	0,1384	(0,0478 ; 0,2289)
UDP-AF1	-x-	-x-	33,9735	(30,8066 ; 37,1405)
UDP-AF2	0,2123	(0,1277 ; 0,2970)	27,3024	(22,8586 ; 31,7461)
UDP-BE	1,5264	(1,2468 ; 1,8059)	31,8321	(27,6210 ; 36,0432)

Tabela 5.24 - Perda média e intervalo de confiança em uma rede MPLS/DiffServ sem preempção

	T < 30 s		T > 30 s	
Tráfego	Perda Média (%)	Intervalo de Confiança	Perda Média (%)	Intervalo de Confiança
UDP-EF	0	(0 ; 0)	0	(0 ; 0)
UDP-AF1	-x-	-x-	0,0257	(0,0004 ; 0,0509)
UDP-AF2	0	(0 ; 0)	0	(0 ; 0)
UDP-BE	0	(0 ; 0)	0	(0 ; 0)

Cenário 5b: Avaliação da rede MPLS/DiffServ com preempção

No último cenário avaliado, introduziu-se uma política de preempção onde os LSPs com maior prioridade de *Setup* podem apropriar os recursos dos LSPs com menor prioridade de *Holding*. Os tráfegos EF, AF2 e BE iniciam a transmissão e conseguem atingir a vazão desejada. A partir do instante t = 30 s, o tráfego AF1 começa a transmitir, e para que isso seja possível o protocolo CR-LDP inicia o processo de preempção para liberar recursos à nova aplicação. A preempção é feita através do método *hard state*, excluindo o LSP do tráfego AF2 que tem menor prioridade e possui recursos suficientes para o novo LSP. O tráfego AF2 é encaminhado a partir desse instante da mesma forma que o tráfego BE.

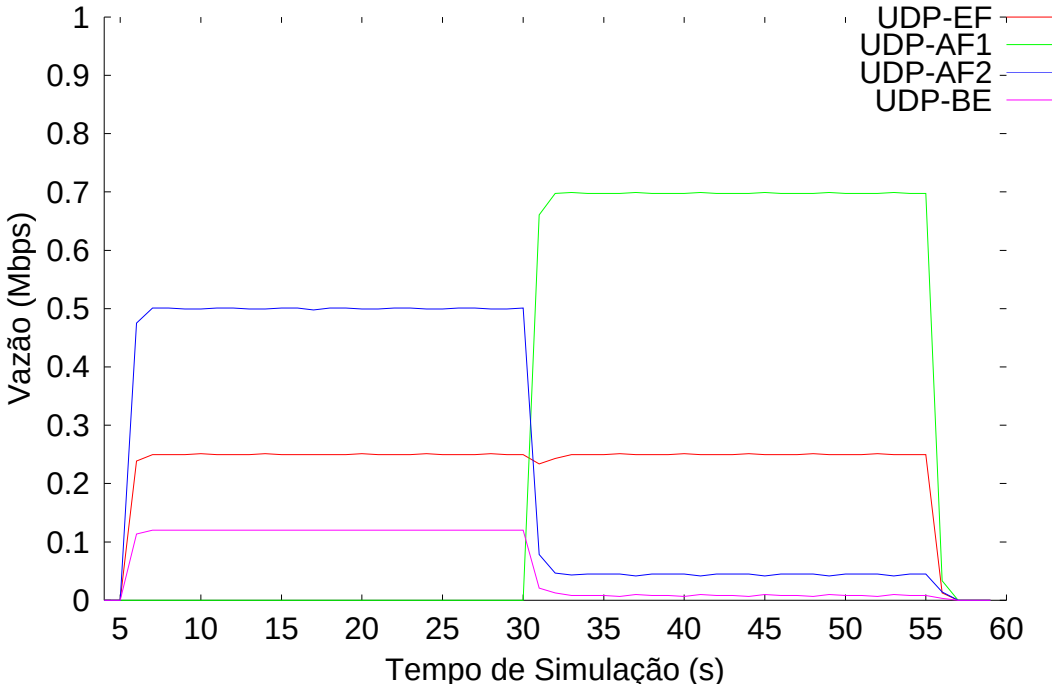


Figura 5.23 - Vazão em uma rede MPLS/DiffServ com preempção

Tabela 5.25 - Vazão média e intervalo de confiança em uma rede MPLS/DiffServ com preempção

	T < 30 s		T > 30 s	
Tráfego	Vazão Média (Kbps)	Intervalo de Confiança	Vazão Média (Kbps)	Intervalo de Confiança
UDP-EF	238,4605	(219,6264 ; 257,2945)	240,2962	(222,7712 ; 257,8213)
UDP-AF1	-x-	-x-	671,0153	(620,9637 ; 721,0670)
UDP-AF2	479,9634	(442,3001 ; 517,6269)	61,2148	(27,2697 ; 95,1599)
UDP-BE	114,9354	(105,8958 ; 123,9749)	8,4923	(7,3284 ; 9,6562)

O gráfico de vazão da Figura 5.23 mostra o instante em que a preempção ocorre, onde é possível observar que o novo tráfego AF1 conseguiu atingir a vazão desejada. O tráfego EF permanece sem alterações, enquanto que os tráfegos BE e AF2 têm suas vazões reduzidas, devido ao fato de estarem disputando os recursos alocados para o tráfego *best effort*. É possível observar que o tráfego AF2 atinge uma vazão superior à do tráfego EF, pois ainda tem prioridade maior no encaminhamento. A Tabela 5.25 mostra o valor médio da vazão e intervalo de confiança dos quatro tráfegos analisados.

O gráfico da Figura 5.24 mostra que os tráfegos EF e AF1 sofreram o menor atraso, enquanto que os outros tráfegos tiveram um aumento sensível no atraso após a preempção ocorrer. Da mesma forma, o *jitter* ilustrado na Figura 5.25 permite observar um aumento para os tráfegos BE e AF2, permanecendo inalterado para o tráfego EF. O novo tráfego AF1 tem um *jitter* semelhante ao tráfego preferencial EF.

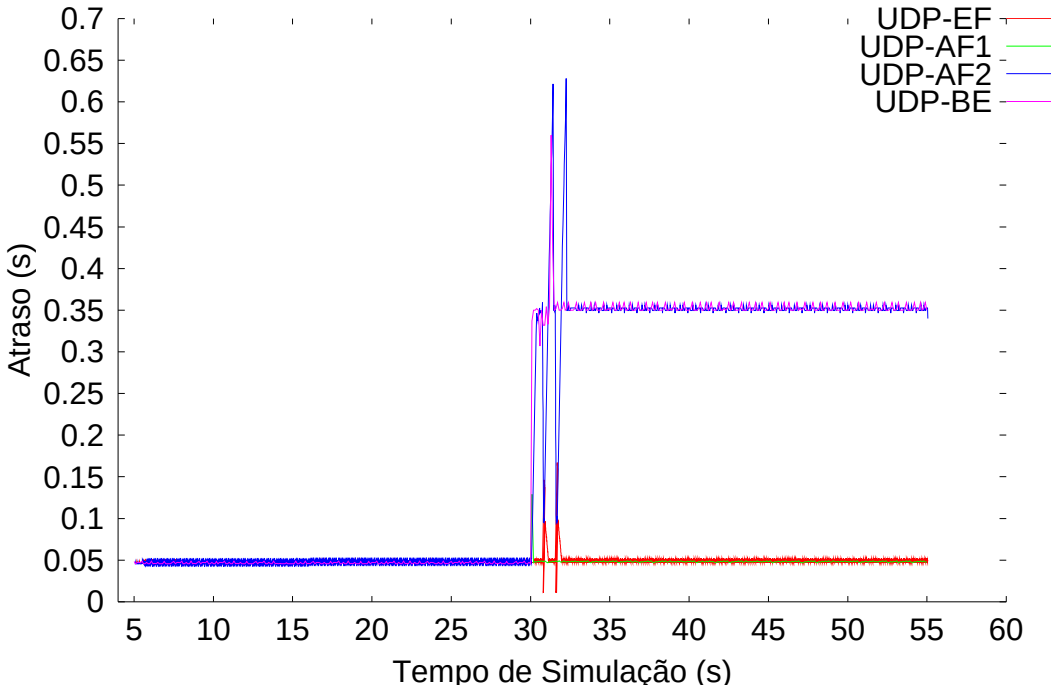


Figura 5.24 - Atraso em uma rede MPLS/DiffServ com preempção

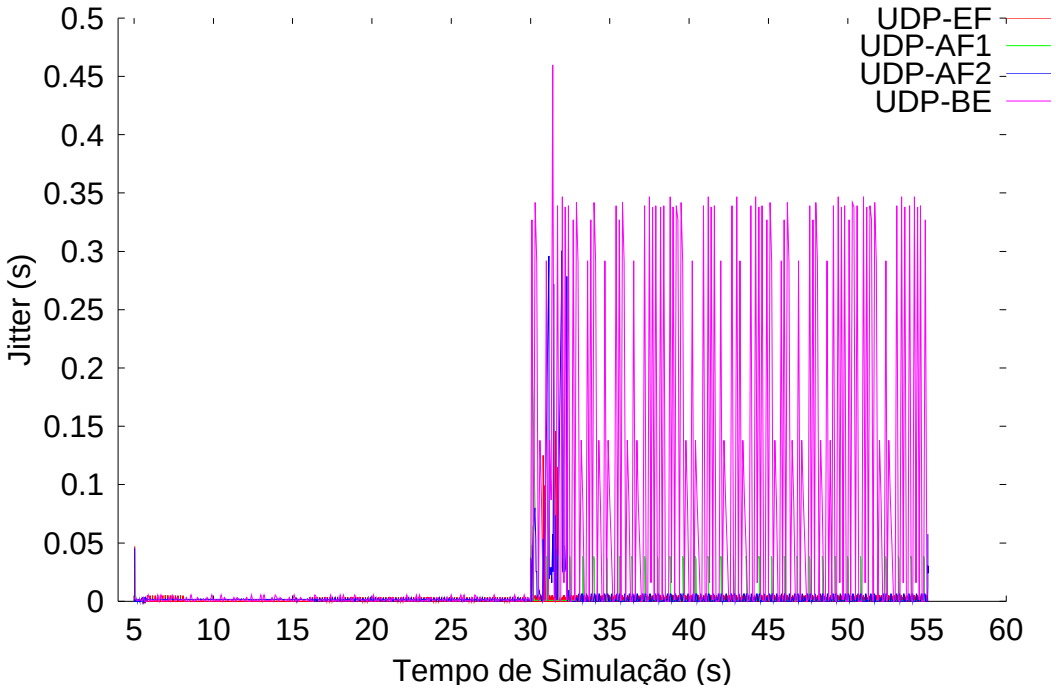


Figura 5.25 - *Jitter* em uma rede MPLS/DiffServ com preempção

A taxa de perda de pacotes é mostrada na Figura 5.26. O índice de descarte é praticamente igual ao observado no experimento anterior, com exceção ao tráfego AF2. Devido ao fato do LSP transportando esse tráfego ter sofrido preempção, e o *host* emissor continuar gerando pacotes, o *backbone* inicia o descarte de pacotes de forma intensa, pois agora ele está sendo tratado como se fosse um tráfego *best effort*.

As Tabelas 5.26, 5.27 e 5.28 ilustram o valor médio do atraso, *jitter* e perda de pacotes dos tráfegos, com seus respectivos intervalos de confiança.

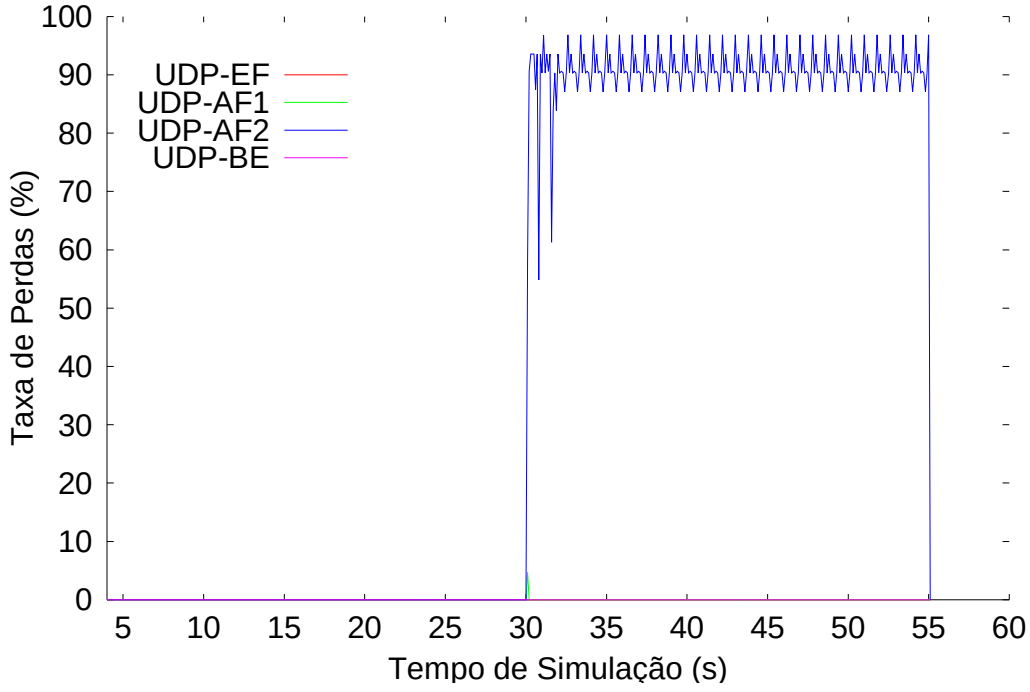


Figura 5.26 - Perda de pacotes em uma rede MPLS/DiffServ com preempção

Tabela 5.26 - Atraso médio e intervalo de confiança em uma rede MPLS/DiffServ com preempção

	T < 30 s		T > 30 s	
Tráfego	Atraso Médio (ms)	Intervalo de Confiança	Atraso Médio (ms)	Intervalo de Confiança
UDP-EF	47,6121	(47,5725 ; 47,6516)	50,0142	(48,2729 ; 51,7556)
UDP-AF1	-x-	-x-	48,5277	(47,8926 ; 49,1629)
UDP-AF2	45,2934	(44,8472 ; 45,7396)	338,8708	(325,4368 ; 352,3047)
UDP-BE	46,9123	(45,9266 ; 47,8981)	351,8071	(330,4517 ; 373,1626)

Tabela 5.27 - *Jitter* médio e intervalo de confiança em uma rede MPLS/DiffServ com preempção

	T < 30 s		T > 30 s	
Tráfego	*Jitter* Médio (ms)	Intervalo de Confiança	*Jitter* Médio (ms)	Intervalo de Confiança
UDP-EF	0,1193	(0,0287 ; 0,2099)	1,7696	(1,2074 ; 2,3319)
UDP-AF1	-x-	-x-	1,0363	(0,5808 ; 1,4917)
UDP-AF2	0,2284	(0,1437 ; 0,3131)	5,7041	(2,8635 ; 8,5446)
UDP-BE	1,5734	(1,2939 ; 1,8530)	126,5048	(108,1449 ; 144,8646)

Tabela 5.28 - Perda média e intervalo de confiança em uma rede MPLS/DiffServ com preempção

	T < 30 s		T > 30 s	
Tráfego	Perda Média (%)	Intervalo de Confiança	Perda Média (%)	Intervalo de Confiança
UDP-EF	0	(0 ; 0)	0	(0 ; 0)
UDP-AF1	-x-	-x-	0,0185	(0,0058 ; 0,0312)
UDP-AF2	0	(0 ; 0)	90,4245	(88,3986 ; 92,4504)
UDP-BE	0	(0 ; 0)	0	(0 ; 0)

5.5. Conclusões

Utilizando modelagem e simulação, este capítulo apresenta a avaliação de algumas tecnologias para se prover QoS. O *backbone* regional da Embratel foi utilizado como ambiente de rede, e um modelo de simulação simplificado foi criado com características próximas ao referido *backbone*.

Através de resultados obtidos para a vazão, o atraso, o *jitter* e a perda de pacotes das aplicações, foi possível analisar o impacto das tecnologias estudadas na diferenciação de serviços às aplicações que exigem parâmetros mais rígidos de QoS. O primeiro experimento envolveu um ambiente sem nenhum mecanismo de QoS, utilizando apenas o método de encaminhamento de pacotes existente atualmente na Internet. Como resultado, não foi possível atingir os requisitos de QoS impostos pelas aplicações. O segundo experimento contou com a presença do modelo DiffServ e, comparando-se com o ambiente anterior, observou-se uma melhora sensível nos parâmetros analisados. No terceiro experimento foi implementada apenas a arquitetura MPLS, onde os resultados alcançados foram próximos do primeiro modelo, pois o MPLS não possui suporte à QoS em sua forma original.

O quarto experimento levou em conta a presença das arquiteturas MPLS e DiffServ, mapeando-se os valores contidos no DSCP do cabeçalho IP dentro do rótulo MPLS. Devido ao fato de não se utilizar engenharia de tráfego com o objetivo de alocar os tráfegos em rotas diferentes, os resultados foram muito semelhantes ao modelo funcionando apenas com DiffServ.

Finalmente, no último experimento utilizou-se a preempção de LSPs para permitir que os tráfegos mais importantes atinjam os requisitos de QoS. Foi utilizado o método *hard state* de preempção, pois o método *soft state* ainda encontra-se em desenvolvimento no âmbito do IETF.

A integração das tecnologias MPLS e DiffServ em conjunto com a preempção de LSPs, resultou em uma arquitetura simples e eficientes, sendo recomendável seu uso principalmente em redes de grande porte. Observou-se que após a preempção, a rede conseguiu oferecer os recursos necessários para a nova aplicação, cumprindo com os parâmetros contratados por um SLA (*Service Level Agreement*), em detrimento das aplicações menos importantes [62].

CAPÍTULO 6

CONCLUSÕES GERAIS

O crescimento do número de usuários e o surgimento de novas aplicações na Internet vêm exigindo dos ISPs, além da disponibilização de mais largura de banda, o suporte adequado a alguns requisitos de qualidade de serviço. Diversas soluções vêm sendo desenvolvidas como alternativas ao serviço *best effort*, destacando-se os serviços integrados (IntServ), os serviços diferenciados (DiffServ) e o MPLS.

A proposta da arquitetura IntServ de gerenciar cada fluxo de pacotes individualmente permite um maior controle dos recursos disponíveis, mas resulta em problemas de escalabilidade. A arquitetura DiffServ utiliza classes de serviços, permitindo assim uma priorização no tratamento a determinados tipos de tráfego. Como os diversos fluxos são mapeados em algumas classes, esta solução tem melhor escalabilidade, sendo recomendada às redes *backbone* (ISPs nacionais e regionais).

Um dos principais benefícios do MPLS está na capacidade de se prover engenharia de tráfego, permitindo assim uma maior otimização dos recursos de rede. Devido à impossibilidade de se fornecer QoS utilizando o MPLS em sua forma nativa, o uso conjunto com o modelo DiffServ tem se destacado pois otimiza os recursos de rede e fornece QoS para cada classe de serviço.

Este trabalho apresenta os principais conceitos de qualidade de serviço em redes IP, descrevendo os parâmetros de medição utilizados e algumas arquiteturas propostas pelo IETF, como o IntServ, o DiffServ e a integração MPLS com DiffServ. A engenharia de tráfego em redes MPLS/DiffServ é detalhada, mostrando-se a necessidade do uso da preempção de LSPs como forma de garantir recursos de rede suficientes às aplicações mais importantes. O estudo da preempção de LSPs em redes MPLS/DiffServ encontra-se em desenvolvimento no âmbito do IETF, envolvendo diversos pesquisadores, fabricantes de equipamentos e administradores de redes *backbone* ao redor do mundo. Por esse motivo e através de uma ampla bibliografia pesquisada, verificou-se a necessidade de se avaliar a adequação de uma rede MPLS/DiffServ com preempção de LSPs no provimento de QoS, principalmente às aplicações de multimídia.

Para atingir esse objetivo, utilizou-se simulação devido à impossibilidade de se avaliar o comportamento de um *backbone* real. Desenvolveu-se um modelo de rede através de informações coletadas do *backbone* regional da Empresa Brasileira de Telecomunicações S/A (Embratel), considerando-se apenas os Centros de Roteamento existentes no Estado de São Paulo. Um ISP local conectado a este modelo encaminha alguns tipos de tráfego, permitindo a avaliação do comportamento da rede *backbone* no encaminhamento desses pacotes.

Os resultados das simulações descritas no capítulo 5 mostram os benefícios obtidos com a utilização das tecnologias MPLS e DiffServ funcionando em conjunto com uma política de preempção de LSPs. As avaliações dos experimentos foram baseadas nos resultados obtidos para os parâmetros de QoS.

No primeiro experimento considerou-se apenas o modelo de serviço *best-effort* disponível atualmente na Internet, sendo possível observar sua inadequação na garantia dos requisitos mínimos de QoS exigidos por uma aplicação multimídia, como por exemplo o atraso e o *jitter*. O segundo experimento foi implementado apenas com a arquitetura DiffServ, onde é possível verificar que a rede classificou os pacotes, priorizando a utilização dos

recursos da rede. Através de um contrato SLA negociado entre o roteador de borda do ISP regional e o roteador do ISP local, os tráfegos foram divididos em diferentes classes e receberam o tratamento diferenciado previamente acordado.

No terceiro experimento, o *backbone* operou apenas com o MPLS. Nesta situação foi possível observar que a tecnologia MPLS não oferece QoS às aplicações, restringindo-se apenas ao encaminhamento dos pacotes de acordo com os rótulos estabelecidos. O quarto experimento foi desenvolvido com as duas tecnologias atuando em conjunto: MPLS e DiffServ. Com as duas tecnologias foi possível oferecer níveis de QoS diferenciados aos pacotes. Porém, na medida em que novos tráfegos foram inseridos na rede resultando em disputa por recursos, as tecnologias implementadas não foram suficientes para manter os parâmetros de QoS fornecidos anteriormente. Finalmente, introduziu-se a preempção de LSPs no quinto experimento, garantindo que os tráfegos de maior importância pudessem receber os recursos de rede necessários para o desempenho requerido pelas aplicações.

Nesta dissertação desenvolveu-se uma pesquisa bibliográfica envolvendo diversos artigos, livros, documentação de empresas de telecomunicações e fabricantes de equipamentos, além dos padrões e propostas disponíveis no IETF.

O trabalho apresentou os conceitos de qualidade de serviço em redes IP, descrevendo os principais parâmetros solicitados pelas aplicações multimídia. Dentre as tecnologias propostas para se aprimorar o serviço *best-effort* disponível atualmente na Internet, descreveu-se o modo de funcionamento das arquiteturas de serviços integrados, serviços diferenciados e MPLS.

O trabalho mostrou a importância da integração de diferentes tecnologias, com o objetivo de se montar arquiteturas simples e eficientes. Em redes de grande porte, é recomendável o uso da solução DiffServ devido a sua boa escalabilidade. Ao se utilizar o MPLS, é possível obter uma plataforma adequada para o provimento de QoS com

diferenciação de serviços, além de facilitar a engenharia de tráfego e a conseqüente otimização dos enlaces do *backbone*.

Introduziu-se o conceito de preempção de LSPs, que é um assunto muito estudado atualmente pelos pesquisadores, recebendo especial atenção pelo IETF, onde discute-se a maneira mais adequada de sua implementação com o objetivo de auxiliar a engenharia de tráfego em redes MPLS/DiffServ.

Com os resultados obtidos nessa dissertação foi possível mostrar a aplicabilidade da arquitetura MPLS/DiffServ em oferecer QoS aos tráfegos mais importantes. A preempção tem um papel fundamental neste modelo, pois garante os recursos necessários para que o *backbone* possa cumprir com os parâmetros contratados através de um SLA (*Service Level Agreement*).

No desenvolvimento desta dissertação, algumas áreas se mostraram promissoras para futuros estudos, dentre os quais destacam-se:

- Desenvolver um estudo comparativo entre as diversas propostas de políticas de preempção existentes, definindo qual algoritmo é o mais eficiente em termos de simplicidade computacional, facilidade de implementação nos *backbones* e adequação na escolha dos LSPs que devem sofrer preempção.

- O método *Soft Preemption* encontra-se em fase inicial de estudos no IETF, permitindo assim que pesquisadores contribuam na implementação de novas políticas de preempção, avaliando sua performance em uma rede *backbone*.

- Utilizar um modelo de simulação de redes IP mais realista, com mais tráfegos multimídia e maior número de LSPs implementados.

- Embora os resultados obtidos através de modelagem e simulação tenham sido satisfatórios, sugere-se a implementação de políticas de preempção em um *backbone* real,

permitindo assim a visualização do desempenho dessas políticas em um ambiente MPLS/DiffServ existente.

CAPÍTULO 7

REFERÊNCIAS BIBLIOGRÁFICAS

[01] SEITZ, N., ITU-T QoS Standards for IP-Based Networks, IEEE Communications Magazine, Junho 2003.

[02] GOZDECKI, J., JAJSZCZYK, A., STANKIEWICZ, R., Quality of Service Terminology in IP Networks, IEEE Communications Magazine, Março 2003.

[03] RAGHAVAN, S., An MPLS-based Quality of Service Architecture for Heterogeneous Networks, Dissertação de Mestrado, Virginia Polytechnic Institute, E.U.A., Novembro 2001.

[04] FAUCHEUR, F., LAI, W., Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering, IETF, RFC 3564, Julho 2003.

[05] AWDUCHE, O., Requirements for Traffic Engineering over MPLS, IETF, RFC 2702, Setembro 1999.

[06] TEWG - Internet Traffic Engineering Work Group, IETF, disponível em: <http://www.ietf.org/html.charters/tewg-charter.html>. Acesso em: 04 nov. 2004.

[07] OLIVEIRA, J. C., SCOGLIO, C., AKYILDIZ, I. F., UHL, G., A New Preemption Policy for DiffServ-aware Traffic Engineering to Minimize Rerouting, Proceedings of IEEE INFOCOM, New York, E.U.A., Junho 2002.

[08] OLIVEIRA, J. C., et. al., Design and Management Tools for a DiffServ-aware MPLS Domain QoS Manager, Proceedings of SPIE ITCOM, Boston, E.U.A., Agosto 2002.

[09] OLIVEIRA, J. C., SCOGLIO, C., AKYILDIZ, I. F., UHL, G., SMITH, J., A New Topology-aware LSP Preemption Policy for DiffServ-based MPLS Networks, Proceedings of IEEE Networks, Atlanta, E.U.A., Agosto 2002.

[10] OLIVEIRA, J. C., SCOGLIO, C., AKYILDIZ, I. F., UHL, G., New Preemption Policies for DiffServ-aware Traffic Engineering to Minimize Rerouting in MPLS Networks, IEEE/ACM Transaction on Networking, 2003.

[11] OLIVEIRA, J. C., New Techniques for End-to-End Quality of Service Provisioning in DiffServ/MPLS Networks, Tese de Doutorado, Geórgia Institute of Technology, E.U.A., Março 2003.

[12] OLIVEIRA, J. C., VASSEUR, J. P., CHEN, L. C., SCOGLIO, C., LSP Preemption Policies for MPLS Traffic Engineering, IETF, Internet Draft, Maio 2004.

[13] AWDUCHE, D., et. al., RSVP-TE: Extensions to RSVP for LSP Tunnels, IETF, RFC 3209, Dezembro 2001.

[14] MEYER, M., MADDUX, D., VASSEUR, J., VILLAMIZAR, C., BIRJANDI, A., MPLS Traffic Engineering Soft Preemption, IETF, Internet Draft, Março 2004.

[15] WANG, J., ZENG, A., AGRAWAL, D. P., Performance Analysis of Preemptive Handoff Scheme for Integrated Wireless Mobile Networks, IEEE Globecom, San Antonio, E.U.A., 2001.

[16] BEARD, C., Preemptive and Delay-Based Mechanisms to Provide Preference to Emergence Traffic, Computer Networks Journal, E.U.A., Julho 2004.

[17] PORETSKY, S., GANNON, D., An Algorithm for Connection Precedence and Preemption in Asynchronous Transfer Mode Networks, IEEE International Conference on Communications, páginas 299 - 303, 1998.

[18] SZVIATOVSZKI, B., SZENTESI, A., JÜTTNER, A., Minimizing re-routing in MPLS networks with preemption-aware constraint-based routing, Computer Communications Journal on Advances in Performance Evaluation of Computer and Telecommunications Networking, Maio 2003.

[19] BLANCHY, F., MÉLON, L., LEDUC, G., Routing in a MPLS network featuring preemption mechanisms, IEEE International Conference on Telecommunications ICT'03, Fevereiro 2003.

[20] STANISIC, V., DEVETSIKIOTIS, M., Distributed On-Line Bandwidth Allocation and Preemption Algorithms in MPLS Networks, CACC Communicator, North Carolina State University, E.U.A., disponível em: <http://www.ece.ncsu.edu/cacc/index.php>. Acesso em: 18 dez. 2004.

[21] KUROSE, J. F., ROSS, K. W., Redes de Computadores e a Internet: uma nova abordagem, São Paulo, Editora Addison Wesley, 2003.

[22] ITU-T Recommendation E.800, Terms and Definitions Related to Quality of Service and Network Performance Includind Dependability, ITU-T Study Group, Agosto 1993.

[23] MARTINS, J., Qualidade de Serviço (QoS) em Redes IP: Princípios Básicos, Parâmetros e Mecanismos, disponível em: <http://www.jsmnet.com>. Acesso em: 20 set. 2003.

[24] EL-GENDY, M., BOSE, A., SHIN, K., Evolution of the Internet QoS and Support for Soft Real-Time Applications, Proceedings of the IEEE, volume 91, Julho 2003.

[25] PETERSON, L. L., DAVIE, B. S., Redes de Computadores: Uma abordagem de sistemas, 3º. edição, Editora Campus, 2004.

[26] XIAO, X., Providing Quality of Service in the Internet, Tese de Doutorado, Michigan State University, E.U.A., Março 2000.

[27] JACOBSON, V., NICHOLS, K., An Expedited Forwarding PHB, IETF, RFC 2598, Junho 1999.

[28] HEINANEN, J., BAKER, F., WEISS, W., Assured Forwarding PHB Group, IETF, RFC 2597, Junho 1999.

[29] ROSEN, E., VISWANATHAN, A., CALLON, R., Multiprotocol Label Switching Architecture, IETF, RFC 3031, Janeiro 2001.

[30] CARPENTER, B., E., NICHOLS, K., Differentiated Services in the Internet, Invited Paper in Proceedings of IEEE, vol. 90, Setembro 2002.

[31] ANDRIKOPOULOS, I., PAVLOU, G., Supporting Differentiated Services in MPLS Networks, IEEE Workshop on Quality of Service (IWQoS 99), Inglaterra, 1999.

[32] FAUCHEUR, F., WU, L., DAVIE, B., DAVARI, S., VAANANEN, P., KRISHNAN, R., CHEVAL, P., HEINANEN, J., MPLS Support for Differentiated Services, IETF, RFC 3270, Maio 2002.

[33] LAW, R., RAGHAVAN, S., DiffServ and MPLS - Concepts and Simulation, Virginia Polytechnic Institute and State University, E.U.A, disponível em: <http://citeseer.ist.psu.edu/700179.html>. Acesso em: 16 ago. 2003.

[34] HORLAIT, E., ROUHANA, N., Differentiated Services and Integrated Services use of MPLS, IEEE Symposium on Computers and Communications, França, Julho 2000.

[35] CAMARILLO, G., Routing Architecture in DiffServ MPLS Networks, Ericsson Research Laboratory, disponível em: <http://standards.ericsson.net/gonzalo/papers/>. Acesso em: 12 fev. 2003.

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

[37] OSBORNE, E., SIMHA, A., Engenharia de Tráfego com MPLS: Projeto, configuração e gerenciamento do MPLS-TE para otimização de desempenho de rede, CISCO Press, Editora Campus, 2002.

[38] SUSITAIVAL, R., Load Balancing by MPLS in Differentiated Services Networks, Dissertação de Mestrado, Helsinki University of Technology, Finlândia, Setembro 2002.

[39] WENPENG, Z., Provision and Route Optimization in Differentiated Services Networks, Dissertação de Mestrado, Helsink University of Technology, Finlândia, Setembro 2002.

[40] FAUCHEUR, F., Maximum Allocation Bandwidth Constraints Model for DiffServ-aware MPLS Traffic Engineering, IETF, Internet Draft, Março 2004.

[41] MINEI, I., MPLS DiffServ-aware Traffic Engineering, White Paper Juniper Networks, disponível em: <http://www.juniper.net>. Acesso em: 25 abr. 2004.

[42] FAUCHEUR, F., Russian Dolls Bandwidth Constraints Model for DiffServ-aware MPLS Traffic Engineering, IETF, Internet Draft, Março 2004.

[43] AWDUCHE, D., CHIU, A., ELWALID, A., WIDJAJA, I., XIAO, X., Overview and Principles of Internet Traffic Engineering, IETF, RFC 3272, Maio 2002.

[44] FAUCHEUR, F., Considerations on Bandwidth Constraint Models for DS-TE, IETF, Internet Draft, Junho 2002.

[45] PEYRAVIAN, M., KSHEMKALYANI, A. Connection Preemption: Issues, Algorithms and a Simulation Study, Proceedings of IEEE Infocom, páginas 143 - 151, Abril 1997.

[46] THING, L., Dicionário de Tecnologia, São Paulo, Editora Futura, 2003.

[47] BOBBIO, A., PULIAFITO, A., TEKEL, M., A Modeling Framework to Implement Preemption Policies in Non-Markovian SPNs, IEEE Transactions on Software Engineering, Janeiro 2000.

[48] RIDLEY, A., FU, M., MASSEY, W., Fluid Approximations for a Priority Call Center with Time-Varying Arrivals, Proceedings of Winter Simulation Conference, E.U.A., 2003.

[49] JIAO, D., Analysis of a New Connection Preemption Protocol for ATM, Dissertação de Mestrado, Universidade de Missouri - Kansas City, E.U.A., Julho 2001.

[50] HERZOG, S., Signaled Preemption Priority Policy Element, IETF, RFC 2751, Janeiro 2000.

[51] GARAY, J. A., GOPAL, I. S. Call Preemption in Communication Networks, Proceedings of IEEE Infocom, páginas 1043 - 1050, Maio 1992.

[52] CISCO Systems Inc., DiffServ-aware Traffic Engineering (DS-TE), disponível em: <http://www.cisco.com>. Acesso em: 26 out. 2004.

[53] EMBRATEL S/A, Topologia do Backbone Internet, disponível em: <http://www.embratel.com.br/Embratel02/cda/portal/0,2997,MG_P_951,00.html>. Acesso em: 06 dez. 2004.

[54] EMBRATEL S/A, Índices de SLA do Backbone Internet, disponível em: <http://sla11.rjo.embratel.net.br/cgi-bin/Natl_report_por_mes_media.pl>. Acesso em: 06 dez. 2004.

[55] MOURA, J. A. B., et. al., Redes Locais de Computadores: Protocolos de alto nível e avaliação de desemepenho, Editora McGraw-Hill, 1986.

[56] NS-2, The Network Simulator NS-2, disponível em: <http://www.isi.edu/nsnam/ns>. Acesso em: 02 set. 2004.

[57] TGUILLÉN, A. M., MPLS-DS: Uma plataforma para validação de políticas no contexto das redes MPLS/DiffServ, Dissertação de Mestrado, Universidade Estadual de Campinas, 2001.

[58] AHN, G. C., MPLS Network Simulator, disponível em: <http://flower.ce.cnu.ac.kr/~fog1/mns>. Acesso em: 10 jul. 2004.

[59] MURPHY, S., The NS MPLS/DiffServ Patch, disponível em: <http://www.eeng.dcu.ie/~murphys>. Acesso em: 23 mai. 2004.

[60] AHN, G., CHUN, W., Design and Implementation of MPLS Network Simulator (MNS) supporting QoS, IEEE International Conference on Networks (ICON 00), Cingapura, 2000.

[61] KAMIENSKI, C. A., SADOK, T., CAVALCANTI, D., DIAS, K., Simulando a Internet: Aplicações na Pesquisa e no Ensino, SBC - Sociedade Brasileira de Computação, Julho 2002.

TRABALHOS PUBLICADOS PELO AUTOR

[62] BASTOS, S. R. G., GUARDIEIRO, P. R., Um Estudo sobre a Preempção de LSPs em Redes MPLS com Diffserv para o Provimento de Qualidade de Serviço, WebMedia/LA-Web, SBC - Sociedade Brasileira de Computação, 12 a 15 de outubro de 2004, Ribeirão Preto, Brasil.

[63] BASTOS, S. R. G., GUARDIEIRO, P. R., Políticas de Priorização de LSPs em Redes MPLS com DiffServ para a obtenção de Qualidade de Serviço Fim a Fim, SUCESU 2004 - Congresso Nacional de Tecnologia da Informação e Comunicação, 26 a 28 de abril de 2004, Florianópolis, Brasil.

[64] BASTOS, S. R. G., GUARDIEIRO, P. R., Um Estudo sobre Serviços Diferenciados Suportados em uma Rede MPLS para o Provimento de Qualidade de Serviço, Conferência Ibero-americana en Sistemas, Cibernética e Informática CISCI 2003, 31 de julho a 2 de agosto de 2003, páginas 62 - 66, Flórida, EUA.

[65] BASTOS, S. R. G., Multiprotocol Label Switching - MPLS, Revista Ceciliana, páginas 37 - 49, Janeiro 2003.

[66] BASTOS, S. R. G., GUARDIEIRO, P. R., Um Estudo sobre a Preempção de LSPs em Redes MPLS/DiffServ para o Provimento de QoS, submetido para publicação no XXII Simpósio Brasileiro de Telecomunicações – SBrT 2005, Campinas, Brasil, 04 a 08 de Setembro de 2005.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo