UNIVERSIDADE FEDERAL FLUMINENSE
CENTRO TECNOLÓGICO
MESTRADO EM ENGENHARIA DE TELECOMUNICAÇÕES

DANIEL BARROSO MONTEIRO

PROPOSIÇÃO DE SUPORTE A SERVIÇOS ATENDIDOS POR DCN, COM BASE NA ANÁLISE DE TÉCNICAS DE TE COM QOS

NITERÓI-RJ
2011

DANIEL BARROSO MONTEIRO

PROPOSIÇÃO DE SUPORTE A SERVIÇOS ATENDIDOS POR DCN, COM BASE NA ANÁLISE DE TÉCNICAS DE TE COM QOS

Dissertação apresentada ao Curso de Mestrado em Engenharia de Telecomunicações da Universidade Federal Fluminense, como requisito parcial para a obtenção do Grau de Mestre. Área de Concentração: Sistemas de Telecomunicações

Orientador: Prof. Dr. CARLOS ALBERTO MALCHER BASTOS

NITERÓI-RJ
201

DANIEL BARROSO MONTEIRO

PROPOSIÇÃO DE SUPORTE A SERVIÇOS ATENDIDOS POR DCN, COM BASE NA ANÁLISE DE TÉCNICAS DE TE COM QOS

Dissertação apresentada ao Curso de Pós-Graduação "*Stricto Sensu*" em Engenharia de Telecomunicações da Universidade Federal Fluminense, como requisito parcial para obtenção do Grau de Mestre. Área de concentração: Sistemas de Telecomunicações.

Aprovada 14 de dezembro de 2011.

BANCA EXAMINADORA

Prof. Dr. Carlos Alberto Malcher Bastos – Orientador
Universidade Federal Fluminense – UFF

Prof. Drª. Débora Christina Muchaluat Saade
Universidade Federal Fluminense – UFF

Prof. Dr. Sidney Cunha de Lucena
Universidade Federal do Estado do Rio de Janeiro - UNIRIO

Niterói
2011

Aos meus pais, pelo amor e incentivo que sempre me deram em tudo na minha vida.

AGRADECIMENTOS

Primeiramente a Deus, fonte de todas as forças.

A meu orientador e professor Malcher, que confiou em mim e tornou possível a concretização de um sonho.

A Ana Carolina que sempre me apoiou e incentivou na conquista deste objetivo.

A todos os profissionais e colegas como Débora, Rogério Mariano, Ricardo, Eunice e Ana Elisa, que colaboraram com este trabalho, enriquecendo-o de maneira incomensurável.

RESUMO

É evidente a expansão, impulsionada pela popularização da Internet, do emprego das redes de dados para o transporte de aplicações que geram altas taxas de dados, através de meios multiprotocolo e abrangendo múltiplos domínios administrativos.

Face à esta necessidade crescente, têm sido desenvolvidas diversas técnicas que visam a garantir confiabilidade, eficiência e qualidade no envio dos dados.

Dentre elas pode ser citada a DCN (*Dynamic Circuit Network*), que consiste na alocação dinâmica de circuitos determinísticos e gerenciáveis fim a fim para o transporte de serviços que exigem redes de alta capacidade, com ou sem a direta intervenção do usuário final, sendo estabelecidos e mantidos por um tempo limitado.

Apesar das vantagens inerentes à DCN, seu emprego requer cuidado, pois a entrada em operação, em uma rede já existente, de um novo serviço baseado em DCN deve ser conduzida de tal forma a não causar impactos negativos em todos os demais serviços pré-existentes.

Tais benefícios e riscos serviram de inspiração para o presente trabalho, no qual são apresentadas algumas técnicas mais usuais de engenharia de tráfego, definidas a partir de necessidades de QoS (*Quality of Service*), para segregação dos fluxos de dados do serviço de DCN dos demais serviços existentes em uma rede.

Para atestar o bom funcionamento das técnicas sugeridas são apresentados os resultados das simulações realizadas em laboratório, nos quais se evidencia, inclusive, a garantia de algum nível de separação, mesmo utilizando-se, por exemplo, equipamentos que suportam poucas filas de QoS e impossibilitam uma segregação ideal entre serviços.

O trabalho é concluído com a apresentação de uma proposta de suporte ao serviço DCN que é composta por três modalidades com diferentes níveis de qualidade, priorização e disponibilidade. São apresentadas propostas aplicáveis a redes com equipamentos que possuem limitações quanto a quantidades de filas de QoS suportadas e também para redes que possuem maior flexibilidade e granularidade quanto ao número de filas. Para a implementação da DCN foram utilizados os *frameworks* DRAGON, como parte do plano de controle de alocação de circuitos dinâmicos.

Palavras-chaves: MPLS, Roteamento, DCN, RSVP-TE, QoS.

ABSTRACT

It is clear the expansion, driven by the popularization of Internet, of the use of data networks to carry applications that generate high data rates through multiprotocol networks and across multiple administrative domains.

Faced with this growing need, several techniques have been developed that aim to ensure reliability, efficiency and quality in data transmission.

The DCN (Dynamic Circuit Network) is the dynamic allocation of deterministic and manageable circuits to transport services that require high-capacity networks, with or without the direct intervention of the end user, being established and maintained for a limited time.

Despite the advantages inherent in the DCN, it requires care since the start of operations in an existing network, a new service based on DCN must be conducted so as not to negatively impact all other pre-existing services.

These benefits and risks were the inspiration for this work, in which are most common techniques of traffic engineering, from requirements defined QoS (Quality of Service) for segregation of the flow of service data from other DCN services on a network.

To demonstrate the proper functioning of the suggested techniques are presented the results of the simulations in the laboratory, which is evident in even the guarantee of some level of separation, even using, for example, a few devices that support QoS queues segregation and an impossible ideal of service.

The work concludes with the presentation of a proposed service support DCN which is composed of three types with different levels of quality, priority and availability. The proposals are made applicable to networks that have limitations on the amounts of supported QoS queues and for networks that have greater flexibility and granularity on the number of queues. For the implementation of the DCN was used frameworks DRAGON, as part of control plan of dynamic allocation circuits.

Keywords: MPLS, Routing, DCN, RSVP-TE, QoS.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE QUADROS

GLOSSÁRIO

API - *Application Programming Interface*

AF - *Assured Forwarding*

AUTOBAHN - *Automated Bandwidth Allocation across Heterogeneous Networks*

CBQ - *Class Based Queuing*

CBWFQ - *Class Based Weighted Fair Queuing*

DCN - *Dynamic Circuit Network*

DRAGON – *Dynamic Resource Allocation via GMPLS Optical Networks*

DSCP - *Differentiated Services Code Point*

EF - *Expedited Forwarding*

FEC - *Forwarding Equivalence Class*

FIFO - *First-in-first-out*

WDM – *Wavelength Division Multiplexing*

GMPLS – *Generalized Multi-Protocol Label Switching*

IP - *Internet Protocol*

LLQ - *Low Latency Queuing*

LER - *Label Edge Router*

LSP - *Label Switched Path*

LSR - *Label Switched Router*

MPLS – *Multi-Protocol Label Switching*

NARB – *Network Aware Resource Broker*

NHLFE - *Next Hop Label Forwarding Entry*

NOC - *Network Operation Center*

OSCARS – *On-demand Secure Circuits and Advance Reservation System*

OSPF - *Open Shortest Path First*

PCE - *Path Computation Element*

PE – *Provider Edge*

PERFSONAR - *Performance Focused Service Oriented Network Monitoring Architecture*

PHB - *Per Hop Behavior*

PQ - *Priority Queuing*

PQ-CBWFQ - *Priority Queuing - Class Based Weighted Fair Queuing*

QoS – *Quality of Service*

RCE – *Resource Computation Element*

RNP – Rede Nacional de Ensino e Pesquisa

RSVP-TE - *Resource Reservation Protocol Traffic Engineering*

SDH – *Synchronous Digital Hierarchy*

SNMP - *Simple Network Management Protocol*

SLA – *Service Level Agreement*

TE - *Traffic Engineering*

UFF - Universidade Federal Fluminense

VLAN - *Virtual Local Area Network*

VLBI - *Very Long Baseline Interferometry*

VLSR - *Virtual Label Switch Router*

VPN - *Virtual Private Network*

WAN - *Wide Area Network*

WEB – *World Wide Web*

WFQ - *Weighted-Fair Queuing*

WRR - *Weighted Round Robin*

1. INTRODUÇÃO

A expansão do uso das redes de dados, impulsionada pela popularização da Internet, tem contribuído para o desenvolvimento de técnicas que permitem garantir sua confiabilidade, eficiência e qualidade; e possibilitam o seu emprego por modernas aplicações científicas, que se caracterizam por serem grandes consumidoras de recursos de rede.

Tais aplicações geram fluxos da ordem de Gigabits por segundo, o que requer que os nós de rede sejam capazes de suportar e transportar, com qualidade, este volume de dados.

Além disso, muitas vezes, dada a natureza da aplicação, não é possível tratar estes tráfegos nas redes de pacotes no modo do melhor esforço (mais conhecido pelo termo em inglês *best effort*), sendo necessário o emprego de circuitos ponto a ponto e transparentes a qualquer protocolo.

Diante dessa realidade, novas técnicas foram propostas. Uma delas merece destaque e consiste no emprego de recursos de engenharia de tráfego (TE) baseadas no uso do *Multi-Protocol Label Switching* (MPLS), como forma de solucionar as limitações dos atuais protocolos de roteamento convencionais como OSPF, IS-IS e BGP.

O MPLS integrou os conceitos de encaminhamento de pacotes baseado na troca de rótulos (*labels*) com a camada de roteamento. Os protocolos de roteamento convencionais possuem algoritmos de roteamento ineficientes à medida que os tamanhos das redes e das tabelas de rotas crescem. Assim, para cada decisão de próximo salto (*hop*) do pacote, cada roteador tem que analisar mais informações do que é realmente necessário, repetindo este processo para cada pacote. Como os pacotes pertencentes a um mesmo fluxos têm a mesma origem e destino, a esta escolha de próximo salto baseado no endereço IP de destino, em cada pacote, torna-se ineficiente.

O uso do MPLS possibilitou uma forma mais eficiente e rápida de roteamento e encaminhamento dos pacotes, reduzindo o consumo de recursos como memória e processamento nos roteadores do núcleo da rede. Com a possibilidade da associação de cada fluxo de dados a mais de um LSP (*Label Switched Path*), surgiu também a possibilidade da escolha de diferentes caminhos dentro da rede para um mesmo par de origem e destino. Nesta prerrogativa, surgiu a possibilidade do emprego de diversas técnicas para uso de engenharia de tráfego, em redes do tipo MPLS, que definem formas eficientes na utilização dos circuitos podendo ser escolhidos diversos caminhos para os mesmos fluxos.

No entanto, é sabido que, embora novas técnicas sejam criadas para atender às demandas dos usuários, estas se renovam constantemente.

Tal fato inspirou a criação do Internet2, um consórcio de redes avançadas liderado pelas comunidades educacionais e de pesquisa.

A comunidade Internet2 [32] é uma parceria excepcional envolvendo instituições dos Estados Unidos e de outros países, que são líderes mundiais nos ramos de pesquisa, indústria, acadêmico e governamental. Ela tem contribuído desde 1996 para o desenvolvimento de avançadas tecnologias de rede para suportar as mais exigentes aplicações atuais e futuras, combinando as redes humanas, IP e ópticas.

Em 2005 a Internet2 iniciou o experimento HOPI (*Hybrid Optical and Packet Infrastructure*) [32], para explorar aprovisionamento dinâmico, usando protocolos de sinalização num plano de controle baseado em tecnologia GMPLS [4].

O projeto HOPI demonstrou a viabilidade de usar circuitos dinâmicos, baseado em GMPLS, para contextos intra e interdomínios. Entretanto, a colaboração DICE (Dante-Internet2-Canarie-Esnet) levou ao uso de uma tecnologia SOA (*Service-Oriented Architecture*, que pode ser traduzido como Arquitetura Orientada a Serviços) para comunicação entre domínios.

Assim surgiu a DCN (*Dynamic Circuit Network*, em português Rede de Circuito Dinâmico), que consiste na alocação dinâmica de circuitos determinísticos e gerenciáveis fim a fim para o transporte de serviços que exigem redes de alta capacidade, com ou sem a direta intervenção do usuário final, sendo estabelecidos e mantidos por um tempo limitado.

Inicialmente a DCN foi proposta para atender aos requisitos de aplicações científicas que geram altas taxas de dados para serem transportados através de meios multiprotocolo e

abrangendo múltiplos domínios administrativos. O foco inicial da DCN é o controle dinâmico de aprovisionamento de caminhos baseados em comprimento de onda.

Uma das formas de estabelecimento de DCN que será abordada neste trabalho é o DRAGON (*Dynamic Resource Allocation via Optical Networks*) [3], que se propõe a desenvolver os componentes de *software* necessários para abordar estas questões, além de fornecer um rápido aprovisionamento de LSP inter-domínio, garantindo também autenticação, autorização e contabilização.

O projeto DRAGON hoje já é adotado e existem algumas aplicações *e-Science* específicas que se adaptaram e se beneficiaram diretamente desta infraestrutura experimental. Como exemplo pode ser citado o projeto do Observatório Haystack do MIT chamado de *Very Long Baseline Interferometry* (VLBI), que utiliza esta rede experimental para transportar, em tempo real, os dados dos radiotelescópios de maneira a dar suporte ao corelacionamento e à coordenação efetiva dos seus vários instrumentos de controle. O VLBI combina dados simultaneamente adquiridos a partir de uma matriz global de até 20 radiotelescópios para criar um instrumento único. Os dados gerados pelos VLBI são da ordem de 1 Gigabit/s, sendo, então, armazenados em fitas magnéticas ou em discos e, posteriormente, enviados para um *site* central para o processamento de correlação. Com a possibilidade de aprovisionar circuitos dedicados de alta velocidade, o DRAGON passou a facilitar este processo, desenvolvendo novas características importantes, tais como correlação em tempo real [3].

Outro projeto que utiliza os circuitos criados pelo DRAGON é o UltraGrid, que se iniciou através de uma parceria da NASA com a Universidade de Maryland, visando estudar uma forma de integrar videoconferência em alta definição, sem compressão e com visualização 3D. O sistema UltraGrid permite videoconferência interativa de alta definição (HD) com o mínimo de latência, transportando vídeo não comprimido a uma taxa superior a 1,2 Gigabit/s [3].

É evidente, portanto, que a característica intrínseca à DCN de oferecer largura de banda dedicada para as aplicações mais exigentes, aliada ao fato de os mecanismos para alocação dos circuitos estarem evoluindo continuamente com base em tecnologias e protocolos padronizados, destacam-na como forma adequada para atendimento às crescentes demandas dos serviços, possibilitando, inclusive, o estabelecimento de circuitos de dados dedicados e sob demanda entre usuários finais.

1.1 MOTIVAÇÕES

A Rede Nacional de Ensino e Pesquisa (RNP), em parceria com diversas universidades do país, criou diversos grupos de pesquisa para estudar soluções de DCN. A Universidade Federal Fluminense (UFF) foi convidada a participar de um deles, sendo seus alunos e professores do curso de Mestrado em Engenharia de Telecomunicações integrantes do projeto MonCircuitos [2], que se propõe a estudar, testar e avaliar *softwares* e abordagens relativos ao plano de gerência das DCN e uma proposta da formatação de suporte ao serviço que inclua as necessidades de qualidade de rede e engenharia de tráfego, que possa ser exequível na rede da RNP.

A RNP busca a integração de diferentes instituições de ensino e laboratórios de pesquisa através de uma rede DCN para possibilitar principalmente o desenvolvimento da intercolaboração acadêmica com a criação de novos serviços que esta tecnologia pode suportar. Seu principal objetivo é o de melhorar a infraestrutura de redes em níveis nacional, metropolitano e local, atendendo, com aplicações e serviços inovadores, as demandas de comunidades específicas (telemedicina, biodiversidade, astronomia etc.) e promovendo a capacitação de recursos humanos em tecnologias da informação e comunicação [31]. Atualmente a RNP é composta por equipamentos de última linha e de altíssima capacidade de transmissão e que apresentam suporte e compatibilidade com o plano de controle dos *frameworks* dos principais modelos de DCN.

Numa abordagem inicial para implementação de um novo serviço sempre deverá ser feita uma análise do risco que esta implementação poderá gerar. Toda rede, e isto inclui a RNP, possui características físicas e lógicas que precisam ser levadas em consideração nesta análise. No processo de prestação de serviço existem diversos parâmetros e níveis de qualidade, que são acordados entre o prestador e os clientes, que precisam ser garantidos. Dentre esse parâmetros e características destacam-se disponibilidade, vazão, latência, *jitter*, quantidade de descartes de pacotes etc. Quando um novo serviço é introduzido numa rede que já possui clientes e acordos de qualidade claramente definidos, esta análise de impacto precisa ser profundamente estudada.

Cada rede possui limitações impostas pelos próprios protocolos, meios de transmissão e equipamentos utilizados. Essas limitações devem ser consideradas e avaliadas durante o processo de preparação para o novo serviço. Podem ser citados alguns exemplos dessas limitações, como o emprego de QoS (*Quality of Service*). A forma como cada equipamento

trata e implementa QoS pode ser única e dependente do modelo e do fabricante. Durante o desenvolvimento deste trabalho, com foco para a RNP, evidenciou-se a existência de equipamentos que suportam, por exemplo, apenas quatro filas de QoS enquanto outros suportam oito ou mais. Outro exemplo é a forma na qual os roteadores montam e priorizam os caminhos virtuais criados pela Engenharia de Tráfego. Todas essas informações são fundamentais para o desenvolvimento de uma proposta de implementação de novos serviços em uma rede com características, clientes e necessidades bem definidas e em produção.

O propósito desta dissertação é o de apresentar como a implementação de um serviço baseado em DCN pode ser aplicada em uma rede operativa sem que este interfira nas garantias pré-definidas dos serviços existentes. Serão apresentadas nas propostas de segregação de tráfego algumas técnicas mais usuais de engenharia de tráfego e de QoS específicas e suportadas pelos equipamentos em questão. Para tal, a proposta apresentada utilizará o *framework* DRAGON [3], como parte do plano de controle de alocação de circuitos dinâmicos.

Outro aspecto importante e motivador deste estudo é a proteção, a segurança e a garantia dos serviços atualmente existentes na rede e a sua operação, uma vez que existirão circuitos lógicos sendo continuamente alocados, roteados e liberados de forma automatizada por intermédio de demandas advindas diretamente dos usuários finais do serviço de DCN.

1.2 ORGANIZAÇÃO DO ESTUDO

O Capítulo 1 apresenta o objetivo e as motivações demandadas pela criação de serviço DCN, bem como a necessidade de estudo de técnicas de engenharia de tráfego e QoS para aplicação neste serviço.

No Capítulo 2 são abordados os conceitos de QoS, bem como os tipos de filas, técnicas de escalonamento e o funcionamento do Diffserv nas camadas IP e MPLS.

O Capítulo 3 descreve os princípios básicos do roteamento de pacotes e de comutação de rótulos, detalhando os conceitos do MPLS e do GMPLS.

O Capítulo 4 apresenta uma visão geral das soluções para DCN, detalhando os *framework* DRAGON, que possibilitam a criação e controle de circuitos dinâmicos inter e intradomínios.

O Capítulo 5 apresenta os conceitos principais da engenharia de tráfego em MPLS, bem como os principais protocolos que possibilitam seu funcionamento.

No Capítulo 6 são demonstrados, os resultados, obtidos nas simulações realizadas, de funcionamento do *framework* DRAGON, ensaios em engenharia de tráfego e QoS.

O Capítulo 7 apresenta as premissas e cenários para a criação de um ambiente para suportar o serviço de DCN, bem como a proposta de formatação de alguns destes serviços com o estudo de caso para aplicação na rede da RNP.

No Capítulo 8 são, então, apresentadas as conclusões do presente trabalho e as recomendações para trabalhos futuros.

2. QUALIDADE DE SERVIÇO (QOS)

A Internet desde a sua concepção sempre teve como característica o fato de adotar um modelo de serviço de melhor esforço, ou seja, um serviço em que há a expectativa de que a informação seja entregue ao destino, porém não há nenhuma garantia de entrega nem do tempo para que isto ocorra.

No entanto, com o crescente surgimento de uma variedade de aplicações, principalmente as que produzem fluxos de mídia contínua e que requerem garantias na rede (como alocação de determinada largura de banda, e controle da latência e da variação do retardo, em inglês, *jitter*) é evidente a necessidade de adequação da atual arquitetura da Internet para atendimento a tais requisitos.

Situações comuns são aquelas em que a rede apresenta todos os seus enlaces em sobrecarga, ou quando a carga não está bem distribuída na rede, apresentando alguns enlaces mais congestionados que outros. Embora a rede possa estar bem provisionada, os protocolos convencionais de roteamento dinâmico sempre fazem suas escolhas de caminho com base na melhor métrica, ou seja, no caminho de menor custo até o destino. Essa situação pode ser especulada num cenário em que o caminho mais curto, ou de maior capacidade nominal de banda, entre dois pontos passa por um enlace congestionado, implicando falha no atendimento a certa requisição.

Os Serviços Diferenciados, cujo princípio de funcionamento é a marcação, a classificação e o enfileiramento dos pacotes IP, provêem os requisitos que as aplicações necessitam. Para tanto, o encaminhamento da informação é feito a partir de filas de prioridade, em que os pacotes são classificados com base em determinadas características em cada roteador de um domínio.

Adicionalmente, mecanismos que tratam de questões ligadas ao roteamento podem ser sobrepostas aos Serviços Diferenciados de forma a aperfeiçoar o encaminhamento dos pacotes dentro de um determinado domínio ou entre domínios.

A Qualidade de Serviço, no contexto das redes de pacotes IP, pode ser definida como o tratamento dado pela rede de forma a garantir o funcionamento de cada aplicação para o qual são exigidos que determinados parâmetros estejam dentro de limites bem definidos e minimamente garantidos.

A Qualidade de Serviço especifica um conjunto de características quantitativas e qualitativas de processamento e de comunicação, suportadas por um serviço que permite a provisão da funcionalidade desejada por usuários do ambiente [17]. Essas características são chamadas, normalmente, de parâmetros de especificação da QoS. Em geral, serviços de transporte de dados possuem associados os seguintes parâmetros quantitativos:

- **Disponibilidade do serviço**: quanto tempo determinado serviço está disponível para uso;

- **Retardo ou atraso:** somatório dos atrasos na entrega da informação da origem ao destino;

- **Variação do retardo (*jitter*):** variação no atraso, ou seja, a diferença dos tempos de chegada entre pacotes quando comparados com os intervalos da transmissão original;

- **Vazão:** capacidade de transmissão da informação de um determinado meio por unidade de tempo, normalmente expressa em bits por segundo. Algumas aplicações necessitam de quantidade (vazão) específica de banda para funcionar de acordo com o desempenho esperado;

- **Taxa de perda de pacotes**: quantidade de pacotes não entregues à recepção, calculado em perda de pacotes por segundo ou seu percentual. Desconsiderando-se as perdas por erros nos meios de transmissão, as perdas de pacote em redes IP são definidas como sendo os descartes de pacotes nas filas dos roteadores devido a congestionamento nos enlaces de saída ou por ações de políticas para controle deste congestionamento.

Uma característica qualitativa de um serviço define uma relação comparativa com outro. Um exemplo de parâmetro qualitativo poderia ser a entrega de pacotes com o menor retardo possível. Nesse caso, o parâmetro de QoS especifica uma característica de retardo de um determinado serviço em relação aos demais.

As aplicações possuem formas distintas de apresentação da informação como, por exemplo, uma chamada em videoconferência ou uma transferência de arquivos. A forma em que os dados são transmitidos pelo meio de comunicação implica diretamente o resultado esperado pela aplicação. De acordo com este critério, as aplicações distribuídas podem ser classificadas em aplicações em tempo real e aplicações elásticas [16].

As aplicações em tempo real caracterizam-se por uma forte dependência em relação aos instantes de entrega dos pacotes de informação pela rede. Em geral, envolvem o transporte de mídias contínuas, como a reprodução de um áudio ou vídeo remotamente. Após ser transmitido, um pacote acumula retardos ao longo dos enlaces e dos elementos de comunicação intermediários, normalmente roteadores, antes de ser reproduzido no destino. A maior parcela do retardo total sofrido por um pacote corresponde a um valor fixo: o retardo de propagação nos enlaces. Além deste retardo existe uma parcela chamada de retardo de enfileiramento que depende das condições de congestionamento nas interfaces de saída dos enlaces em cada roteador. Em situações extremas, pacotes podem ser perdidos ou entregues no destino após o instante correto de reprodução e, por conseguinte, descartado. Nesse contexto, aplicações em tempo real são tolerantes à perda de pacotes, uma vez que apesar dos tipos de retardo apresentados podem introduzir distorções na reprodução destas aplicações, elas são até certo grau aceitáveis devido às limitações da percepção humana.

As aplicações elásticas, por sua vez, não dependem tanto dos instantes de entrega dos pacotes, admitindo maiores variações na latência. Por outro lado, perdas de pacotes não são, em geral, admitidas. Para essas aplicações, os parâmetros de QoS mais importantes são a vazão média e a taxa de perda de pacotes. Exemplos de aplicações elásticas são: o correio eletrônico, a navegação WEB, a transferência de arquivos (FTP), o *login* remoto (Telnet), entre outros.

O Quadro 1 compara os diferentes tipos de aplicações com suas exigências de rede para o correto funcionamento.

	Voz	Vídeo	Dados *Best Effort*	Dados Críticos
Banda (*Throughput*)	Baixa a Moderada	Moderada a Alta	Moderada Alta	Baixa a Moderada
Sensibilidade à Perda de Pacotes	Baixa	Baixa	Alta	Moderada a Alta
Sensibilidade ao Atraso	Alta	Alta	Baixa	Moderada a Alta
Sensibilidade ao *Jitter*	Alta	Alta	Baixa	Baixa a Moderada

Quadro 1 – Comparação das necessidades de recurso de rede por aplicação

Em resumo, a necessidade de diferenciação e tratamento de QoS é requisito fundamental, motivado pela convergência de diferentes mídias de informação, que no passado eram transportadas por redes distintas, para o transporte sobre IP, conforme representado esquematicamente na Figura 1.

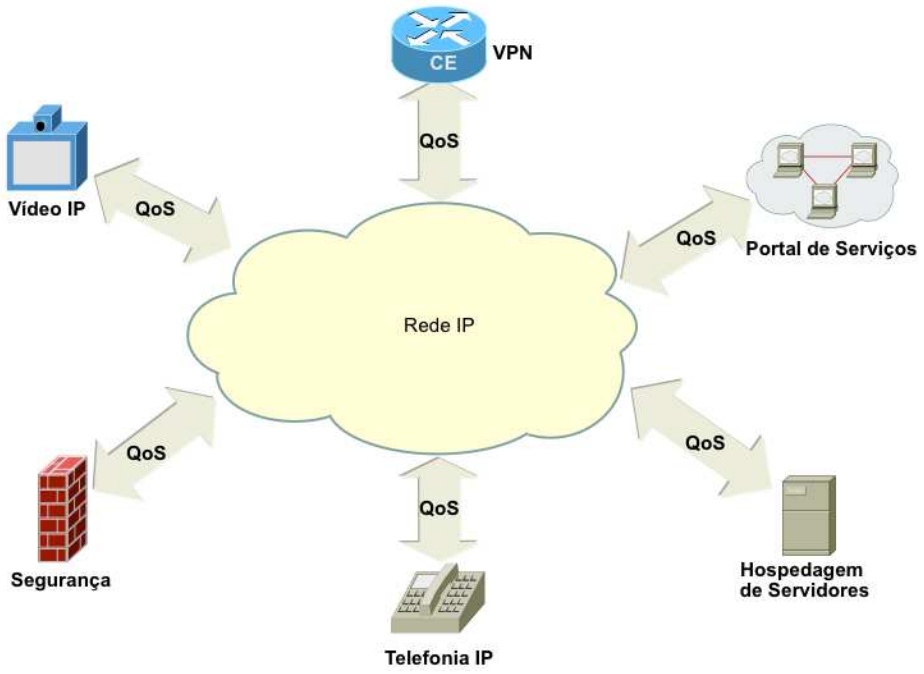

Figura 1 – Convergência de serviços para transporte sobre rede IP

2.1 SERVIÇOS DIFERENCIADOS (DIFFSERV)

Essa proposta do IETF baseia-se na marcação dos pacotes IP no campo de ToS (*Type of Service*), denominado campo DS (*Differentiated Service*), em que, de acordo com o valor, os pacotes são classificados com determinadas prioridades de encaminhamento e descarte [18]. A proposta do Diffserv é a de reduzir o nível de processamento nos roteadores de maneira que os fluxos com determinadas semelhanças e necessidades são classificados da mesma forma e agregados. A tarefa de selecionar e classificar o pacote normalmente ocorre nos roteadores de borda deixando com que os roteadores do núcleo da rede executem apenas o papel de encaminhamento e priorização.

No Diffserv, cada dispositivo da rede desempenha tarefas específicas sobre os pacotes manipulados. Os elementos localizados nas extremidades da rede são normalmente responsáveis pelas tarefas de classificação e marcação do pacote. Dessa forma, são estes elementos que identificam o tráfego, agrupando os fluxos em classes e marcando-os com um identificador para cada tipo de fluxo semelhante.

As tarefas de marcação e classificação são as que normalmente consomem mais recursos dos equipamentos de rede. Por isso que, nas bordas das redes, como a agregação de tráfego é menor, este papel é possível. Nos roteadores de núcleo da rede, que agregam elevado volume de tráfego, esta atividade torna-se quase inviável. Além da classificação e marcação dos pacotes, os roteadores de borda ainda realizam as atividades de policiamento, controle de admissão, e gerenciamento das filas e de congestionamento.

Uma vez estando os pacotes classificados e marcados, os roteadores seguintes têm o papel de enfileirar e priorizar baseados nas políticas de QoS definidas. Essas ações combinadas nos equipamentos de núcleo da rede são denominadas PHB *(Per Hop Behavior)* e são descritas da seguinte forma:

Policing (ou policiamento) - determina se os pacotes estão de acordo com a taxa de transmissão definida pelo administrador da rede e toma as ações correspondentes para sua garantia. Essas ações podem ser marcar, remarcar ou descartar um pacote.

Scheduling (ou escalonamento) - são as técnicas de enfileiramento que definem como determinadas classes de pacotes serão encaminhadas pela interface de saída do elemento de rede.

Forwarding (ou encaminhamento) - é o processo que o roteador realiza de transmissão do pacote com a devida prioridade definida pelo escalonador.

A arquitetura Diffserv, definida na RFC 2474, implementa classes de serviços diferenciadas com base em requisitos de desempenho. As classes de serviços são diferenciadas através de mecanismos que tratam pacotes IP de uma aplicação marcados com um identificador da classe de serviço da aplicação. Esse identificador chamado de DSCP *(Differentiated Services Code Point)* é o campo do pacote IP que recebe as marcações associadas a uma classe de serviço.

Resumidamente, o processo de marcação e processamento do DiffServ ocorre da seguinte forma: cada pacote é processado de acordo com sua marcação. Existem 3 classes de marcação mais utilizadas e difundidas. A primeira é do tipo *Expedited Forwarding* (EF), na qual é normalmente provido o maior nível de priorização. Os pacotes são encaminhados de forma a garantir menor *jitter*, descarte e atraso. A segunda é do tipo *Assured Forwarding* (AF) que possui 4 níveis de prioridade e 3 preferências de descarte por nível de priorização. O terceiro tipo é o pacote sem marcação, ou seja, com todos os bits do capo ToS iguais a zero, este tipo de marcação é comumente conhecida como melhor esforço.

A especificação das classes de serviços, dos DSCP associados às classes, compõe a implementação da Política de QoS. A implementação de QoS deve ser complementada pelo tratamento do tráfego que entra da rede. O tratamento de QoS nas entradas e saídas é chamado de *Traffic Conditioning* e envolve funções de classificação dos pacotes nas classes de serviços e policiamento do tráfego na entrada. A definição do *Traffic Conditioning* é fundamental para a implementação dos PHB.

2.2 GERENCIAMENTO DE FILAS E ESCALONAMENTO

São diversas as possibilidades e técnicas existentes para tratamento dos pacotes dentro de uma rede IP. Os mecanismos de gerenciamento de filas e escalonamento são necessários para acomodar o tráfego quando a taxa de chegadas de pacotes é maior que a capacidade de transmissão [23]. Conceitualmente o gerenciamento de filas define a lógica utilizada para ordenar pacotes nos *buffers* de saídas de uma interface enquanto o escalonamento é o processo de decisão de qual será o próximo pacote a ser transmitido.

Basicamente estas técnicas definem a prioridade de transmissão e de descarte dos pacotes em situações de congestionamento. Os três tipos de filas e técnicas de escalonamento mais conhecidos e que são a base para as diversas implementações são: *First-In-First-Out (FIFO), Priority Queuing (PQ) e Weighted-Fair Queuing (WFQ).* O que ocorre na prática é

que várias das técnicas implementadas pelos grandes fabricantes de roteadores como Cisco® e Juniper®, por exemplo, são combinações destes tipos de fila de maneira a aperfeiçoar a forma de encaminhamento e tratamento de pacotes dentro de uma rede. A seguir são descritas estas principais técnicas.

2.3 *FIRST-IN-FIRST-OUT* (FIFO)

O acrônimo FIFO descreve o princípio de enfileiramento no qual o pacote que vier primeiro será atendido primeiro. Este tipo de fila é o mais básico onde todos os pacotes serão tratados igualmente em uma fila simples e serão encaminhados na ordem em que chegarem.

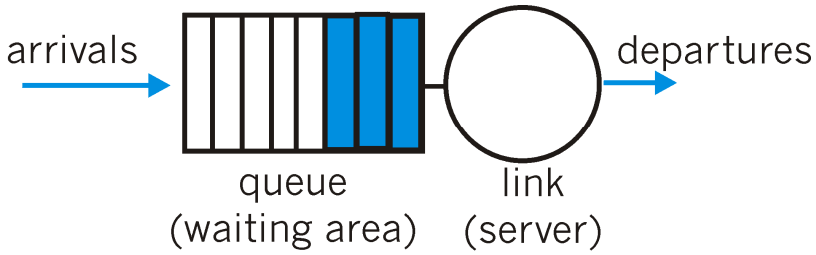

Figura 2 – Fila do tipo FIFO
Fonte: YANG, LEHMAN (2007)

2.4 *PRIORITY QUEUING* (PQ)

O *Priority Queuing* define múltiplas filas de QoS em uma interface de rede onde, para cada fila, é dado um diferente nível de prioridade. A fila com maior prioridade é processada antes das filas de menor prioridade. Se os pacotes de uma fila do tipo PQ causarem congestionamento no roteador, todos os demais pacotes de outras filas serão descartados até que a fila PQ, de maior prioridade, esteja novamente vazia. O tamanho máximo da fila é definido por um limite de comprimento. Quando a fila é maior que este limite, os pacotes são descartados. O risco neste tipo de implementação é a possibilidade da existência de pacotes em filas de baixa prioridade que podem nunca serem transmitidos. Por isso, é usual a definição de um limite na máxima vazão ou comprimento desta fila.

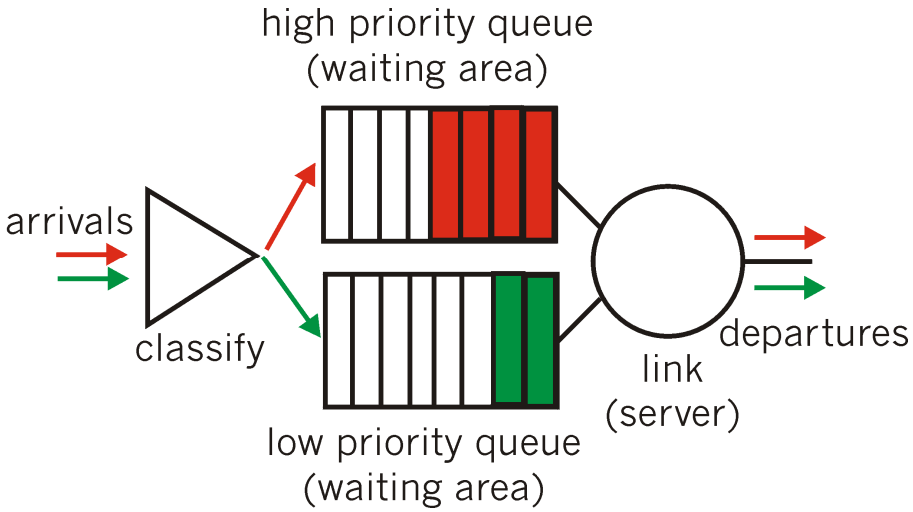

Figura 3 – Fila do tipo PQ
Fonte: YANG, LEHMAN (2007)

2.5 *WEIGHTED-FAIR QUEUING* (WFQ)

No enfileiramento WFQ, os pacotes são separados em classes e encaminhados em diferentes filas de prioridade. Supondo que existam, por exemplo, duas filas, de mesmo peso ou prioridade, o roteador irá encaminhar um pacote de cada fila por vez, alternadamente, até que as filas estejam vazias. Se forem atribuídos pesos ou prioridades diferentes para as filas, o encaminhamento de pacotes acontecerá de forma ponderada ao peso atribuído. Por exemplo, uma fila com peso um e outra com peso dois significa que a cada três pacotes transmitidos um será da primeira fila e dois da segunda.

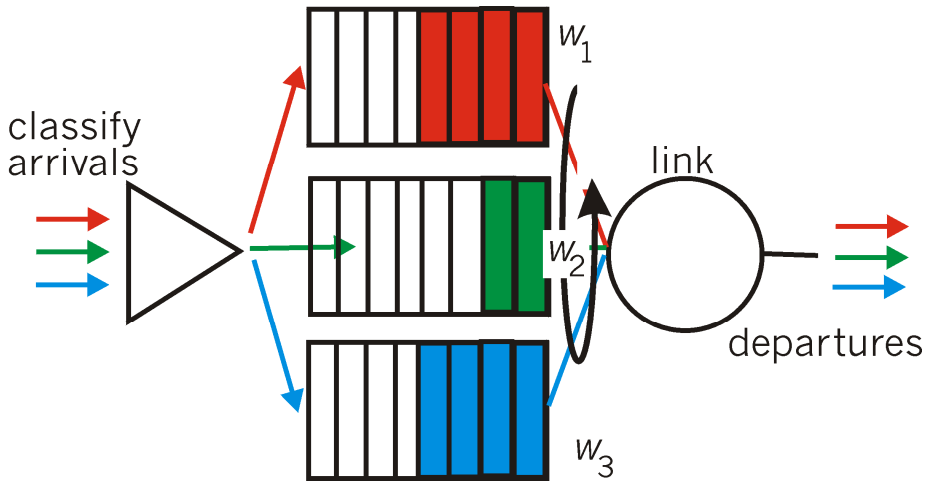

Figura 4 - Fila do tipo WFQ
Fonte: YANG, LEHMAN (2007)

A combinação destas três técnicas básicas de enfileiramento e escalonamento cria a possibilidades de filas mais complexas, das quais podem ser destacadas [23]: a *Class Based Queueing* (CBQ), a *Class Based Weighted Fair Queuing* (CBWFQ) e a *Low Latency Queueing* (LLQ) ou também conhecida como PQ-CBWFQ (*Priority Queueing - Class Based Weighted Fair Queuing).*

3. ROTEAMENTO DE PACOTES

Os protocolos de roteamento são responsáveis pelo encaminhamento dos pacotes com base na troca de informações de alcançabilidade na rede. Os roteadores examinam o endereço IP destino contido no cabeçalho IP de cada pacote que neles chega e consultam sua tabela de roteamento, para determinar como e para onde encaminhar o pacote. Esse processo é executado independentemente em cada roteador ao longo do caminho de origem-destino do pacote.

Apesar de complexo, ele gera diversos cálculos computacionais para escolha do próximo salto baseado no caminho com menor custo ou distância até o destino desejado. Com isso, não é utilizada a totalidade de recursos da rede, onde caminhos diferentes, de maior custo, para o mesmo destino não são usados.

Para possibilitar o roteamento ótimo na rede IP, seria necessária uma conectividade em malha completa entre todos os roteadores. Isso conduziria a uma demanda de $n \cdot (n-1)/2$ conexões interligando todos os roteadores entre si.

Na prática essa topologia não é adotada, pois acarretaria numa grande complexidade operacional, uma vez que sempre que um roteador fosse adicionado, deveria ser configurada uma conexão para cada um dos roteadores da rede.

Além disso, sabe-se que falhas na rede ou mudanças na topologia provocam grandes atualizações no protocolo de roteamento. Cada roteador deve enviar atualizações de roteamento em cada conexão ao qual estiver conectado para informar a seu vizinho a nova situação da topologia na rede. Quanto maior a quantidade de conexões, maior é o tráfego na rede para o envio de atualizações.

3.1 *MULTI-PROTOCOL LABEL SWITCHING* (MPLS)

A ideia básica por trás do funcionamento do MPLS é simples, consistindo no uso de um rótulo, de tamanho fixo, que será usado como argumento para a tomada de decisões de encaminhamento de pacotes. No MPLS, os pacotes IP são encapsulados com estes rótulos pelo roteador de borda do domínio MPLS, denominado LER (*Label Edge Router*). Esse procedimento de análise e seleção de um rótulo é conhecido como classificação de pacotes.

Em todos os nós subsequentes, chamados de LSR (*Label Switching Router*), é o rótulo MPLS e não o cabeçalho IP que será usado na tomada da decisão de encaminhamento do pacote. Finalmente, quando os pacotes deixam o domínio da rede MPLS, outro roteador de borda remove estes rótulos e encaminha o pacote puramente IP. O caminho por onde os pacotes viajam em um domínio MPLS é chamado de LSP (*Label Switched Path*). Para construir dinamicamente um LSP, utiliza-se um protocolo de distribuição de rótulos e, uma vez que o LSP tenha sido estabelecido, os pacotes MPLS podem ser encaminhados com base no rótulo inserido no cabeçalho dos pacotes, conforme exemplificado na Figura 6.

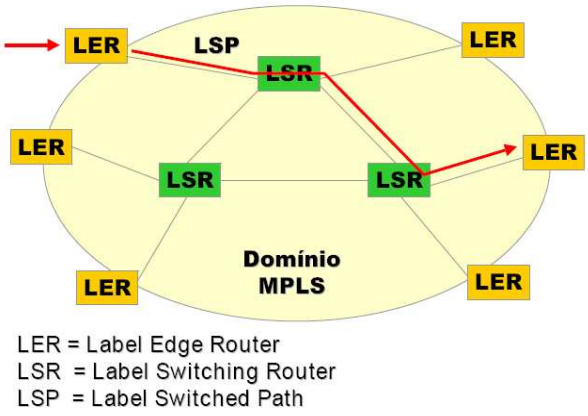

Figura 5 - Elementos da rede MPLS
Fonte: MARQUES (2004)

3.1.1 Histórico

Anteriormente à padronização do atual modelo MPLS pela RFC 3031, várias empresas desenvolveram soluções proprietárias para a comutação de pacotes por rótulos. Dentre essas soluções vale destacar:

- O CSR (*Cell-Switching Router*) desenvolvido pela Toshiba® e apresentado à IETF em 1994.
- O *IP Switching*, desenvolvido pela Ipsilon® foi anunciado no início de 1996 e entregue em alguns produtos comerciais. O *IP Switching* caracterizava-se por usar a presença de fluxos de dados para orientar o estabelecimento de rótulos.
- O *Tag Switching* é a comutação por rótulo desenvolvida pela Cisco®. Em contraste ao CSR e ao *IP Switching*, o *Tag Switching* é uma técnica orientada por controle, que não depende da identificação de um fluxo de dados para estimular a montagem das tabelas de encaminhamento de rótulo.
- O *Aggregate Route-based IP Switching* (ARIS) foi desenvolvido pela IBM® e possuía arquitetura similar ao *Tag Switching*. O ARIS ligava rótulos a rotas agregadas (grupos de prefixos de endereço) ao invés de fluxos individuais (diferententemente de CSR e *IP Switching*).

3.1.2 Arquitetura MPLS

O MPLS é um protocolo de comutação de pacotes baseado em troca de rótulos, que de certa forma, adiciona a característica de "orientação à conexão" às redes IP com a criação dos LSP, cujo conceito poode ser comparado ao de circuitos virtuais do ATM. Ademais, ele é multiprotocolo, ou seja, opera independentemente dos protocolos das camadas 2 (C2 ou L2) e 3 (C3 ou L3), conforme mostra a Figura 7.

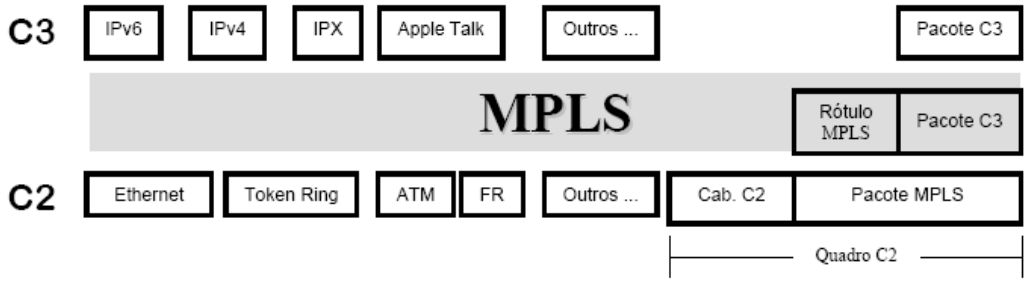

Figura 6 – Característica multiprotocolo do MPLS.

Na arquitetura MPLS dois componentes básicos são definidos: o plano de dados, ou componente de encaminhamento de pacotes, e o plano de controle. Em um roteador a função

de controle envolve o cálculo da rota na qual o roteador recebe informações dos protocolos de roteamento de estado do enlace ou o vetor de distância para criar e atualizar suas tabelas de rotas. O encaminhamento de dados, por sua vez, é uma função totalmente separada. O roteador analisa cada pacote recebido e, com base em seu endereço IP de destino, consulta a tabela de roteamento para determinar qual o próximo nó a encaminhar. Vale ressaltar que, uma vez que o encaminhamento MPLS é baseado em rótulos, é possível separar claramente o plano de encaminhamento (baseado em rótulo) do plano de controle. Assim, cada plano pode ser modificado de forma independente. Com isto, não é preciso modificar o esquema de encaminhamento, por exemplo, para migrar para uma nova estratégia de roteamento.

3.1.3 Plano de Controle

Uma FEC (*Forwarding Equivalency Class*) consiste numa classe de equivalência, ou seja, um conjunto de parâmetros, que irão determinar um caminho para os pacotes dentro da rede MPLS. Os pacotes associados a uma mesma FEC serão encaminhados pelo mesmo caminho. Ao receber um pacote, o roteador de entrada da rede MPLS verifica qual FEC ele pertence e o encaminha através da LSP correspondente. A associação do pacote a uma FEC acontece apenas uma vez, quando o pacote entra na rede MPLS.

O plano de controle do MPLS inclui a distribuição das informações de roteamento entre os LSRs adjacentes e a execução dos procedimentos para criação da tabela de encaminhamento baseada em rótulos.

O componente de controle tem de reagir quando ocorrem mudanças na rede e também é o responsável pelo provimento do mapeamento entre a FEC e o endereço do próximo roteador. Independente do tipo de roteamento adotado a função do componente de controle é responsável pela criação da tabela de encaminhamento por rótulo.

3.1.4 Plano de Dados

Este componente, por sua vez, executa o encaminhamento dos pacotes usando as informações da tabela de encaminhamento. Em um roteador convencional é utilizado, por exemplo, um algoritmo cujo critério de melhor caminho é a comparação entre o endereço de destino no pacote com entradas na tabela de encaminhamento até obtenção da melhor rota

disponível. Todo o processo de tomada de decisão deve ser repetido em cada nó ao longo do caminho da origem ao destino. Em um LSR, um algoritmo de troca de rótulo usa o rótulo no pacote e uma tabela de encaminhamento baseado em rótulo, para obter um novo rótulo e uma interface de saída para o pacote.

Ao chegar um pacote IP o LER executa uma consulta na tabela de encaminhamento IP, classifica o pacote com base no resultado dessa consulta em uma FEC e marca o pacote com o rótulo de saída correspondente à informação obtida. Finalmente, ele encaminha o pacote para a interface de saída com o rótulo apropriado, segundo informações da tabela.

Um LSR recebe o pacote rotulado, usa as tabelas de encaminhamento de rótulo para trocar o rótulo de entrada pelo rótulo de saída correspondente e o encaminha para o próximo nó, conforme informações armazenadas na tabela de encaminhamento.

3.1.5 O Rótulo (*Label*)

A arquitetura MPLS define o rótulo como sendo um identificador, de tamanho fixo. Normalmente, os rótulos MPLS são de significado local ao roteador ao qual pertencem diferentemente do conceito global que possui um endereço IP de rede. Na Figura 8 é apresentado o formato de um cabeçalho de um rótulo, chamado de rótulo SHIM, que pode ser utilizado para encapsular um quadro de enlace que não disponibiliza um campo para inserção de rótulo, a exemplo dos quadros Ethernet.

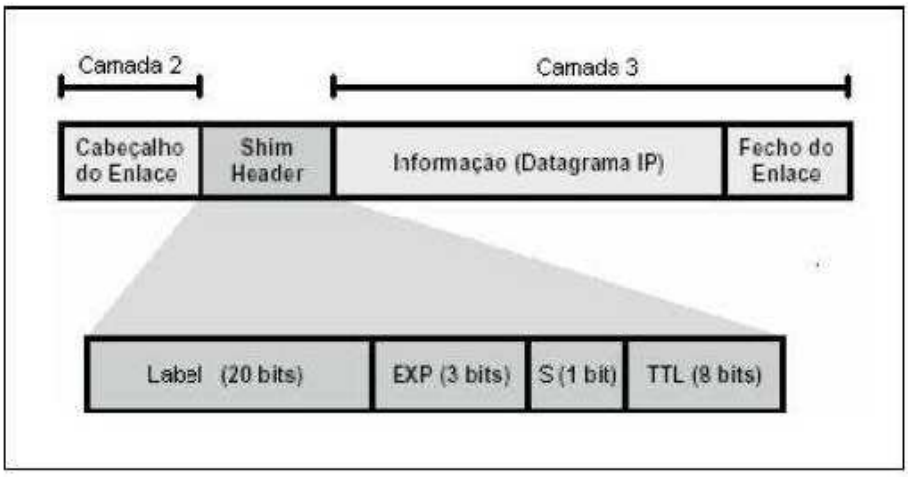

Figura 7 - Formato do cabeçalho MPLS no Ethernet
Fonte: MARQUES (2004)

3.1.6 Tabelas de Encaminhamento por Rótulo

Todos os roteadores MPLS são capazes de processar pacotes com rótulos de entrada, através de uma matriz de comutação ou tabela de encaminhamento. Essas tabelas são constituídas por várias entradas chamadas NHLFE (*Next Hop Label Forwarding Entry*, em português, Entradas de Encaminhamento por Rótulo ao Próximo Roteador). Estas tabelas consistem basicamente de um campo de índice que é preenchido pelo valor do rótulo, uma ou mais entradas, contendo o rótulo de saída, interface de saída e endereço IP do próximo salto (*next hop address*).

Cada NHLFE pode conter as seguintes informações:

- endereço do próximo roteador para o pacote;
- operação a ser feita com a pilha de rótulos de substituição (operação *push*) ou remoção (operação *pop*);
- opcionalmente, o tipo de encapsulamento usado;
- opcionalmente, a codificação da pilha de rótulos.

Um LER de entrada constrói uma tabela que mapeia FEC em NHLFE, que é chamada de Mapa FTN (FEC-To-NHLFE). Essa tabela é usada para encaminhar pacotes que chegam não rotulados ao LER, mas que precisam sair rotulados ao entrar num domínio MPLS. Isso é feito através de uma operação de *push* de entrada. Um LSR constrói uma tabela que mapeia um rótulo em NHLFE, que é chamado de ILM *(Incoming Label Map).* Essa tabela é usada no plano de dados, para encaminhar os pacotes rotulados. Se o ILM mapear um determinado rótulo de entrada em mais de um NHLFE, o LSR deve selecionar uma única entrada para realizar o encaminhamento do pacote. Esse esquema pode ser útil no balanceamento de carga entre múltiplos caminhos de igual custo. A operação prevista nas NHLFEs dessa tabela é geralmente destinada à troca de rótulo (*label swap*), de forma a associar o rótulo de entrada de um pacote que chega através de uma determinada porta de entrada a um rótulo de saída por uma porta de saída do roteador.

3.2 QOS NA CAMADA MPLS

Na camada MPLS, o campo do cabeçalho que permite a marcação de QoS, conhecido como *Experimental Field* (EXP*),* é composto por 3 bits, resultando em apenas 8 possibilidades de diferenciação. A Figura 5 mostra o detalhamento do cabeçalho do rótulo MPLS.

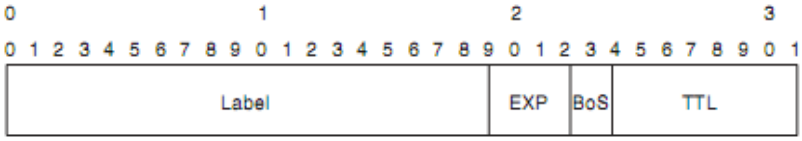

Figura 8 - Detalhamento dos campos do cabeçalho do rótulo MPLS

Os seguintes campos fazem parte do cabeçalho do rótulo MPLS:

- *Label* (20 bits): valor atual do label, identificador de LSP;
- EXP (3 bits): *experimental bits*, usado para o QoS;
- BoS (1 bit): bit de sinalização de fim de pilha de rótulos, este valor é igual a 1 para a última entrada na pilha e a 0 para as demais;
- TTL (8 bits): *Time To Live*, possui a mesma função do TTL do cabeçalho IP.

O funcionamento do QoS Diffserv na camada MPLS é semelhante no mundo puramente IP. Todas as combinações de filas e classes de serviço existentes e descritas neste capítulo são possíveis na camada MPLS. A diferença é que na camada MPLS o campo do pacote usado para análise pelo roteador é o EXP, de apenas três bits, enquanto no IP é o campo TOS, que possui oito bits. Este decréscimo de cinco bits no tamanho do campo destinado a QoS para o MPLS faz com que sejam reduzidas as possibilidades de diferenciação dos pacotes para apenas 8 combinações contra as 256, teoricamente possíveis, combinações do pacote IP. Por padrão, os roteadores ao encapsularem o pacote IP em um rótulo copiam os três bits mais significativos (da esquerda para direita) do campo TOS do cabeçalho IP para o *experimental field*. Dessa forma é necessário um planejamento prévio para definição de um mapeamento dos valores de TOS em EXP para que o QoS possa atuar de forma compatível quando tratado no MPLS.

Os pacotes de sinalização dos protocolos de roteamento e *keepalive* (entre as interfaces do roteador) são fundamentais para o funcionamento do sistema e devem possuir a maior prioridade possível para garantir a operação da rede sob qualquer condição de

congestionamento. Estes pacotes normalmente possuem os valores mais significativos e para o MPLS ocupam o campo EXP, em decimal, com os valores *6 e 7*.

3.3 GENERALIZED MULTIPROTOCOL LABEL SWITCHING (GMPLS)

As redes ópticas atuais transportam tráfegos com informações digitais em comprimentos de onda através da rede, passando por múltiplos estágios intermediários de conversão eletro-óptica-eletro. Redes ópticas futuras certamente realizarão o roteamento de comprimentos de onda em um domínio inteiramente óptico.

Combinando as altas capacidades de largura de banda dos *switches* ópticos com as possibilidades de engenharia de tráfego do MPLS surgiu o GMPLS, permitindo que roteadores, *switches* SONET/SDH, WDM, entre outros, manipulem e realizem o roteamento na camada óptica da mesma forma que roteadores o fazem com pacotes IP, por exemplo.

O MPLS foi projetado para carregar tráfego de camada 3 (IP), usando caminhos estabelecidos com base em IP e associando-os a rótulos. Esses rótulos podem ser configurados explicitamente por um administrador de rede ou dinamicamente por meio de protocolos como LDP ou RSVP-TE.

GMPLS é o conceito generalizado do MPLS, quando define rótulos que atuam na camada 1 (fibras, *slots* de tempo e comprimentos de onda), camada 2 (ethernet, ATM), e na camada 3 (pacotes IP). O principal uso do GMPLS é o de aplicar o conceito do MPLS para equipamentos que não possuem estas características. Dessa forma, é possível implementar nestes equipamentos um plano de controle MPLS incluindo as funcionalidades advindas dos protocolos de roteamento dinâmicos e engenharia de tráfego.

Um importante impacto econômico do GMPLS é possibilitar a habilidade de automatizar o gerenciamento de recursos de rede e o oferecimento de serviços de caminhos com engenharia de tráfego nas redes ópticas, utilizando os princípios de funcionamento do MPLS anteriormente descritos.

Atualmente, nas redes ópticas, o processo de provimento de serviços ocorre de forma manual, lenta e custosa. Como exemplos podem ser citadas as redes SONET/SDH em anel na qual, para se oferecer uma conexão fim-a-fim de alta velocidade, uma prestadora de serviços deverá determinar por quais anéis SONET/SDH a conexão a ser estabelecida passará e, assim, reservar a largura de banda em cada anel de forma manual.

O desenvolvimento de nós (*switches* e roteadores ópticos) com base em GMPLS permite a automatização no oferecimento de serviços e gerenciamento da rede, viabilizando a diminuição do tempo de ativação e recuperação de falhas em várias ordens de magnitude, uma vez que as funcionalidades da engenharia de tráfego serão configuradas e atuarão diretamente nos nós ópticos.

4. SOLUÇÕES DCN

Face a suas características de flexibilidade e suporte a qualidade de serviço e engenharia de tráfego, o MPLS tornou-se um protocolo relevante no desenvolvimento de novas redes e serviços. Originalmente usado para acelerar a comutação de pacotes IP em redes, sua utilização foi estendida a Redes Privadas Virtuais (*Virtual Private Networks* - VPN), a serviços de *Virtual Private LAN* (VPLS) e à resiliência das DCN.

As diversas soluções para DCN existentes baseiam-se na utilização de técnicas desenvolvidas tanto para Engenharia de Tráfego e sinalização, sustentadas por protocolos de roteamento (OSPF ou IS-IS), e por protocolos de sinalização (RSVP-TE ou OSPF-TE). Os LSP são manipulados (criados e removidos) graças a complexos módulos de gerenciamento do plano de controle MPLS ou GMPLS.

Assim, o emprego destes protocolos torna viável que serviços de DCN sejam utilizados sob demanda e de forma transparente. Tal característica é essencial, por exemplo, para o oferecimento de serviços de Internet comercial com alto desempenho.

O DCN permite a criação de circuitos, de forma dinâmica, em redes hibridas apresentando uma solução para um plano de controle de dados GMPLS mesmo para redes onde os equipamentos de transporte de dados sejam totalmente desprovidos destas características. O conceito de dinamismo no DCN está diretamente relacionado a capacidade de prover meios de os usuários finais do sistema possam fazer estas solicitações de circuitos ponto a ponto de forma agendada.

O grande desafio deste trabalho está no emprego do DCN, em uma rede em produção, de forma a garantir a segregação dos serviços de dados transportados, previamente existentes nesta rede, possam conviver sem interferência mútua. O DCN permitirá, além da escolha do circuito dinâmico ideal entre a fonte e os nós de destino, um melhor aproveitamento e a convergência em uma única rede.

Dentre as diversas soluções existentes, que permitem a alocação dinâmica de circuitos, foram estudados os *frameworks* DRAGON [21] e AUTOBAHN [22], por serem os com maior nível de maturação e escopo dos grupos de trabalho demandados pela RNP para o estudo de suporte a serviços DCN.

4.1 DRAGON - *DYNAMIC RESOURCE ALLOCATION VIA GMPLS OPTICAL NETWORKS*

O projeto DRAGON [21] foi iniciado pela *National Science Foundation* (NSF) como sendo um trabalho colaborativo entre as Universidades de *Maryland*, *Mid-Altantic Crossroads*, *Southern California* e *George Mason*. O projeto DRAGON desenvolve tecnologia e a aplica nas infraestruturas das redes para permitir o aprovisionamento dinâmico de circuitos determinísticos em resposta direta à solicitação dos usuários finais.

Com o crescente número de aplicações de alto desempenho que necessitam de redes com características determinísticas, as atuais redes baseadas no melhor esforço não atendem a estes requisitos. Neste contexto, o conceito determinístico implica a definição de garantia de nível de serviço. Estes parâmetros de nível de serviço incluem definições como: um mínimo de largura de banda, taxas de perdas de pacotes controladas, latência e *jitter*. Além disso, estes circuitos devem ser aprovisionados através de domínios de tecnologias heterogêneas entre diversos provedores conforme mostrado na Figura 9.

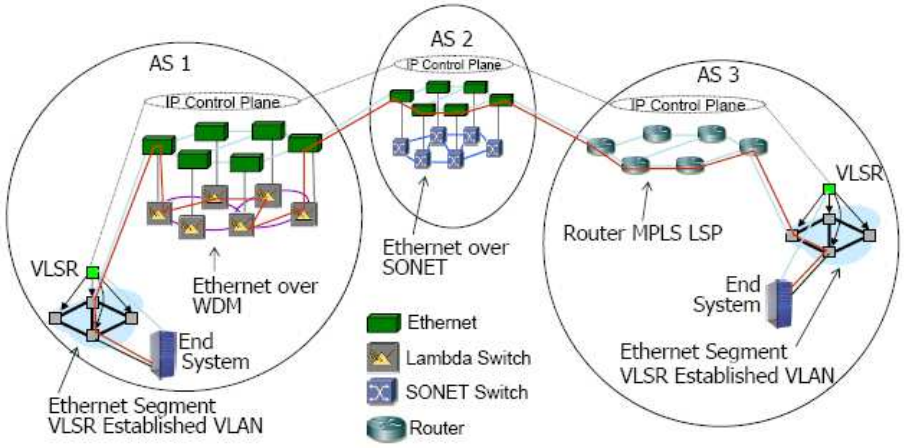

Figura 9 – Complexidade de estabelecimento de um LSP através de uma topologia com diversos domínios e redes heterogêneas.
Fonte: Site dragon.maxgigapop.net (2010)

A contínua evolução das redes ópticas combinadas com mecanismos de aprovisionamento dinâmico como o GMPLS [4] associado a técnicas de engenharia de tráfego possibilita o uso de técnicas de garantia de serviço em redes heterogêneas apresentando roteamento interdomínio, cálculo do circuito fim a fim, sinalização e um avançado esquema de agendamento, autenticação, autorização e contabilização (AAA).

4.1.1 Arquitetura DRAGON

O projeto DRAGON desenvolve uma arquitetura formulada a partir de algumas premissas conforme apresentadas a seguir:

- A infraestrutura deve permitir ações de aprovisionamento solicitadas diretamente pelos usuários finais. O resultado desta solicitação é uma conexão LSP, na nomenclatura do GMPLS.
- Os usuários podem especificar parâmetros associados ao LSP. Estes parâmetros podem ser, por exemplo, origem - destino (*endpoints)*, largura de banda e tempo de vida do LSP. Adicionalmente, parâmetros como latência, *jitter*, controle de perda de pacotes podem ser definidos.
- O aprovisionamento de circuitos pode ser intradomínio, interdomínio, através de topologias heterogêneas e incluir características de AAA e agendamento.
- O tempo necessário para o estabelecimento destes circuitos deve estar em torno de algumas poucas dezenas de segundos.

4.1.2 Componentes da Arquitetura

4.1.2.1 *Network Aware Resource Broker* (NARB)

O NARB é o componente principal do sistema DRAGON. Ele é responsável pelo roteamento, cálculo computacional dos LSP e sinalização interdomínio através de topologias que incluem um conjunto de tecnologias de rede e fabricantes de equipamentos distintos. Além disso, o NARB é o agente que representa o domínio local e atua escutando os protocolos de roteamento intradomínio.

O NARB roda uma versão modificada do protocolo OSPF-TE [5] além de incluir um avançado algoritmo quer permite o cálculo computacional do LSP baseado em múltiplas restrições (*constraints*). Através das vizinhanças do OSPF-TE o NARB pode trocar, entre os domínios, as topologias aprendidas por este protocolo, ou opcionalmente, trocar uma visão "abstrata" da topologia, conforme mostra a Figura 10. Esta visão abstrata protege a real topologia do domínio divulgada a domínios externos, além de reduzir as quantidades de atualizações das bases de dados (*databases*) do protocolo entre os diversos NARBs. Nestas restrições estão incluídos os parâmetros do GMPLS – TE [6] bem como AAA, agendamento e limitações específicas dos fabricantes dos equipamentos de rede.

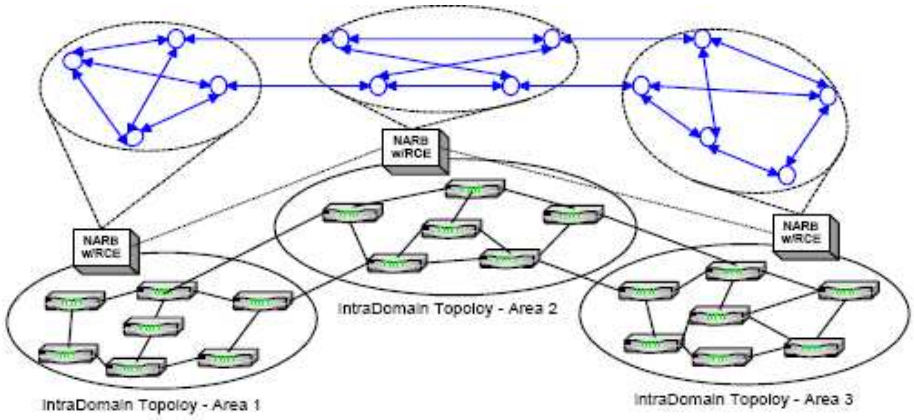

Figura 10 – Visão da topologia de rede complexa x abstrata.
Fonte: Site dragon.maxgigapop.net (2010)

O resultado deste cálculo computacional do LSP é uma *Explicit Route Object* (ERO) [7] que será aplicada nos elementos da rede DCN.

4.1.2.2 *End System Agent (ESA)*

O ESA é o *software* que roda nos terminais dos usuários e define o planejamento e as características do serviço (LSP) a ser aprovisionado. É a camada inicial com a interface com o usuários, características de como dever ser solicitado o LSP, autenticação e níveis de acesso ao sistema são aplicados.

4.1.2.3 *Application Specific Topology Builder (ASTB)*

O elemento ASTB na arquitetura DRAGON é responsável pela coordenação e a resposta para as requisições das aplicações que demandam os LSP. Este elemento é responsável pela criação da visão topológica abstrata para garantir a confidencialidade do *backbone* do sistema autônomo.

4.1.2.4 *Virtual Label Switch Router (VLSR)*

Um importante objetivo da arquitetura DRAGON é a capacidade de aprovisionamento através de redes heterogêneas e composta por diversos fabricantes de equipamentos. Para dar suporte a equipamentos de fabricantes que não suportam o GMPLS foi introduzido o conceito de VLSR. O VLSR é o plano de controle que inclui modificações dos protocolos OSPF-TE e RSVP-TE [8] e atua como um agente *proxy* para dispositivos não GMPLS. Isto permite que estes dispositivos atuem como elementos GMPS e sejam incluídos nas instâncias de criação dos LSP fim a fim. O uso inicial do VLSR no projeto do DRAGON foi para controlar *switches* ethernet via um plano de controle GMPLS, mas este pode ser estendido também para controle de *switches* TDM e ópticos.

4.1.2.5 *3D Resource Computation Model (3D RCM)*

Para o aprovisionamento de um serviço fim a fim entre múltiplos domínios em um ambiente GMPLS são envolvidas três fases para controle deste processo. Na primeira fase, recursos e políticas, como os estados dos circuitos na rede, reserva de recursos e políticas de AAA são trocadas entre os planos de controle tanto intra quanto interdomínio. Na segunda fase, as informações sobre os recursos e políticas serão usadas para determinar de que maneira, quando e como os recursos serão alocados. Esta fase é conhecida como fase computacional e é o momento principal do processo de controle do roteamento GMPLS ou cálculo computacional. Na terceira fase, os resultados e as decisões vindas da fase de cálculo computacional serão aplicadas de forma a aprovisionar o serviço.

O sistema é definido como “3D” RCM devido aos três tipos de recursos e políticas baseados nas redes GMPLS, incluindo o estado dos recursos, agendamento do tempo e as regras de AAA. Estes correspondem às três dimensões das restrições para a alocação dos

recursos, ou seja, restrições de engenharia de tráfego (TE), restrições de tempo (agendamento) e restrições das políticas de AAA.

4.1.2.6 *Resource Computation Engine (RCE)*

Devido à complexidade computacional definiu-se que todas as três dimensões das políticas e recursos estariam disponíveis em um único ambiente computacional que é denominado de RCE na arquitetura DRAGON. O RCE possui as funcionalidades de PCEN (*Path Computation Element Architecture*). As funcionalidades do DRAGON PCEN são similares aos descritos no IETF *Path Computation Element Architecture* [9].

4.2 AUTOBAHN - *AUTOMATED BANDWIDTH ALLOCATION ACROSS HETEROGENEOUS NETWORKS*

Pesquisas nas áreas de astronomia, geologia, física e meio ambiente normalmente precisam de canais dedicados para transportar dados entre pontos a altas taxas, por determinado tempo, com restritivos níveis de garantia de serviço.

As redes baseadas no protocolo IP provêem serviços para a transferência de dados, mas não com a garantia necessária para transferências dados com restrições de tempo a capacidade. Uma solução viável para contornar este problema seriam circuitos fim a fim dedicados que possuem altos custos e geralmente ficam ociosos grande parte do tempo durante a qual não é necessária esta transferência dos dados.

Um serviço de circuito dinâmico (DCN) complementaria as limitações das redes IP com a qualidade oferecida pelos circuitos dedicados de forma a prover níveis de qualidade e quantidade requeridas pelo período necessário de transferência de dados entre os pontos envolvidos [22], a custos relativamente compatíveis com os das redes IP convencionais sem ociosidade de recursos. Dessa forma, quando os circuitos não são mais necessários, eles podem ser liberados para outra potencial transferência entre diferentes pontos usando o mesmo recurso.

O sistema AUTOBAHN [22] provê uma interface amigável para instanciar circuitos dinâmicos através das redes de pesquisa e educação com um piloto elaborado no projeto GN2,

copatrocinado pela Comissão Européia, como parte do 6.º Programa de Desenvolvimento e Pesquisa (FP6).

O sistema AUTOBAHN não atua substituindo o plano de controle, sinalização e aprovisionamento da rede existente. Sua principal característica está no fato de atuar como uma camada integrada ao negócio para coordenar o aprovisionamento interdomínio complementando o plano de controle existente com as funcionalidades de roteamento interdomínio, monitoração e uma infraestrutura de autenticação e autorização. Entende-se como interdomínio a interligação entre redes distintas e administradas por diferentes grupos.

O AUTOBAHN atua como intermediário entre os usuários ou aplicações e a rede, interpretando os pedidos dos usuários (ou aplicações) e traduzindo-os para ações na rede. Este sistema foi desenhado para poder alocar banda de rede para usuário/aplicações tanto imediatamente quanto em data pré-definida. Os recursos são alocados de forma dinâmica, fim a fim, entre múltiplos domínios criando um complexo problema de coordenação e reconfiguração de recursos entre domínios com diferentes administradores. A granularidade da reserva de recursos em termos de banda e a duração são associadas aos parâmetros de QoS.

Atualmente o AUTOBAHN foi desenvolvido para suportar:

- Circuitos comutados Ethernet L2
- Circuitos comutados L1 que podem ser comprimentos de onda ópticos SONET STM-1, 1 GE ou 10 GE.

Cada domínio de rede define suas políticas para uso dos recursos, bem como os parâmetros de qualidade que serão disponibilizados para o DCN através do AUTOBAHN. Através da autenticação, os usuários são identificados e recebem a autorização para executar seu respectivo papel.

O sistema é baseado no *Inter-Domain Manager* (IDM), que é um módulo responsável pelas operações de reservas de circuitos entre diferentes domínios. Isto também inclui a comunicação interdomínio, negociações de recursos com domínios adjacentes, tratamento das requisições e anúncios de topologia. A Figura 11 mostra um resumo de toda arquitetura do sistema AUTOBAHN.

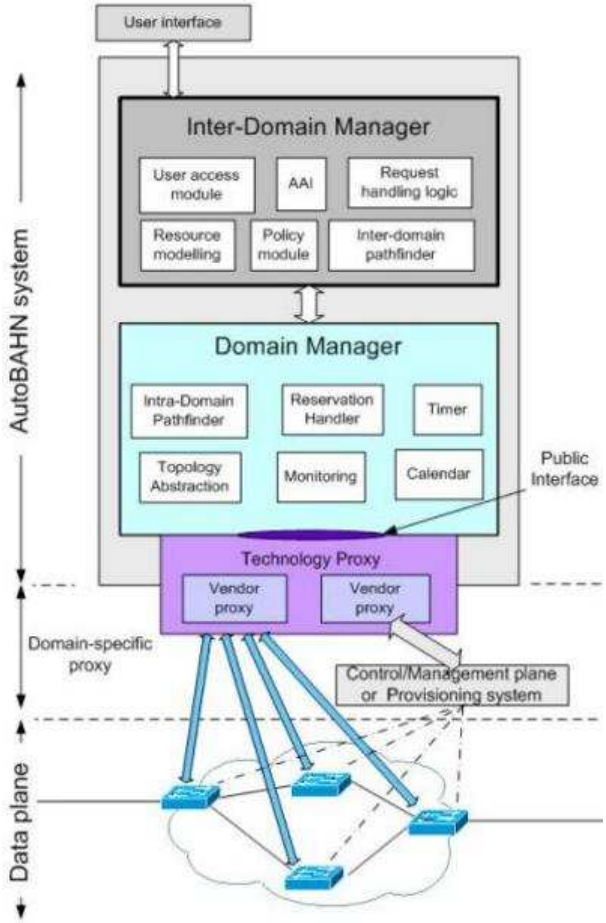

Figura 11 – Arquitetura do sistema AUTOBAHN.
Fonte: Site ist-mupbed.org (2011)

O módulo *Domain Manager* (DM) atua na construção dos circuitos reais fim a fim e também como gestor dos recursos intradomínio. O DM possui uma interface com o IDM local. Em cada domínio, o plano de dados é controlado pelo módulo DM que usa diversas técnicas incluindo interfaces com os Sistemas de Gerenciamento de Rede (NMS), sinalização de protocolos e os próprios elementos. Como parte do DM, um módulo chamado *Technology Proxy* suporta e compatibiliza a comunicação com diversos fabricantes de elementos de rede.

5. ENGENHARIA DE TRÁFEGO

A Engenharia de Tráfego (TE) refere-se ao processo de seleção do caminho usado pelos fluxos de dados, com o objetivo de distribuir ou acomodar a carga na rede de roteadores e *switches*. Pode também ser descrita como sendo o processo através do qual um determinado fluxo de dados é encaminhado pela rede, de acordo com uma visão de gestão dos recursos disponíveis e sua relação com o tráfego real e comportamento esperado. Assim, percebe-se claramente que a TE é mais importante em redes onde existem múltiplos caminhos ligando seus diversos nós de roteamento. A TE fornece os meios necessários para que os administradores de redes definam um melhor uso dos recursos disponíveis, distribuindo a carga entre os circuitos.

Nos últimos anos os administradores de rede têm escolhido protocolos de roteamento que definem o melhor caminho do LSP baseado no menor custo, como o OSPF e o ISIS. Estes protocolos estabelecem caminhos de menor custo, dados os pesos atribuídos aos enlaces. Como, nestes casos, o roteamento é dependente exclusivamente da topologia da rede, não é possível definir caminhos com base, por exemplo, nas demandas de tráfego, utilização e disponibilidade da rede.

Com o surgimento do MPLS novas técnicas de roteamento foram possíveis através do uso de TE permanecendo ainda a indefinição de uma forma dinâmica de escolha de LSP para melhor utilização dos recursos de rede.

O objetivo primário da TE é fazer o melhor uso da infraestrutura de rede enquanto mantém garantias de QoS. Isto é facilitado pela característica de roteamento explícito do MPLS. Há duas formas principais de controle deste roteamento explícito: manualmente, através da ação direta dos administradores da rede, ou de forma automatizada, através de processos que reagem a informações providas pelo estado da rede, restrições específicas e protocolos de roteamento.

Um importante conceito no uso da TE em uma rede MPLS é o roteamento baseado em restrições onde os sistemas de roteamento são usados para selecionar caminhos para fluxos de dados sujeitos às restrições previamente definidas. Os atributos associados ao tráfego e aos recursos, como também os parâmetros associados ao roteamento, coletivamente, representam as variáveis de controle que podem ser modificadas por ação administrativa ou por agentes automatizados que controlam a rede para um estado desejado. Em uma rede em operação, é desejável que estes atributos possam ser dinamicamente modificados por um administrador sem interromper a própria rede.

5.1 ENGENHARIA DE TRÁFEGO BASEADA EM RESTRIÇÕES (*CONSTRAINTS*)

Um dos principais algoritmos para o roteamento baseado em restrições é o *Constrained Shortest Path First* (CSPF). Este protocolo utiliza uma modificação do *Shortest Path First* (SPF) operando com uma base de dados especial, *TE Database* (TED), construída pelos próprios protocolos de *link-state*. As topologias da rede nos protocolos OSPF-TE ou RSVP-TE são alimentadas na TED pelo protocolo de *link-state*. Neste conceito incluem-se a capacidade dos dispositivos que rodam MPLS, suas disponibilidades de banda, prioridades e controles administrativos.

Quando um LSP é definido são enviadas informações para o LER que são passadas pelo CSPF e incluídas na TED. Dessa forma, o algoritmo remove todos os enlaces da rede que não atendem as restrições (*constraints)* definidas, calculando o menor caminho entre os roteadores de entrada e saída da rede MPLS. Em seguida, o LSP é calculado pelo algoritmo tendo como resultado uma *Explicit Route Object* (ERO) detalhando cada salto *(hop)* ao longo do caminho. Este ERO é passado para o RSVP-TE que sinaliza e estabelece o LSP. A habilidade do CSPF em localizar um caminho possível é resultado das informações (ou restrições) contidas na TED.

6. LABORATÓRIO

A principal característica das soluções para DCN está na criação de *Label Switched Paths* alocados dinamicamente e demandados diretamente pelos usuários do serviço. Cada demanda possui requisitos como agendamento, duração, banda, latência e política de QoS. Estes requisitos implementam modificações diretamente na estrutura do *backbone* da rede, no encaminhamento dos pacotes, e na criação ou desconexão de LSP.

Toda rede em produção, seja ela de uso coorporativo, empresarial ou um grande *backbone* de operadora de telecomunicações, possui diversos serviços que precisam operar e interoperar normalmente com a entrada de qualquer novo serviço. Atualmente provedores de serviço, por exemplo, transportam em seus *backbones* tráfego de Internet, para atendimento residencial e corporativo, juntamente com complexas VPN MPLS, transporte de voz de telefonia pública, entre outros. Todos estes exemplos de serviços operam e mantêm seus limiares de funcionamento e qualidade dentro de uma única rede IP/MPLS.

A grande questão por trás da convergência de diversas mídias e serviços em uma única rede está no fato de ser possível seu funcionamento como se transportado por meios dedicados e independentes. Um serviço de DCN, por sua vez, além de incluir novos perfis de tráfego possui a característica de alocação dinâmica de LSP gerando mensagens de protocolos de engenharia de tráfego diretamente no núcleo do *backbone* sem a intervenção direta de seus administradores. Este implementação deste tipo automatizado de aprovisionamento de circuitos é nova e ainda desconhecido para a grande maioria das redes e seus administradores.

Ciente disso, o foco dos ensaios de laboratório, a serem descritos a seguir, será o de apresentar e testar alguns recursos de engenharia de tráfego e QoS apresentando mecanismos que protejam e isolem os tráfegos gerados pelos fluxos de dados das DCN e garantam aos administradores das redes condições mínimas operacionais, independentemente do nível de exigência e autorização que o usuário tenha na solicitação de criação de um LSP dinâmico.

Neste laboratório foram utilizados somente protocolos padronizados ITU-T e IETF para garantir que os resultados possam ter aplicação geral a todo e qualquer fabricante de rede que siga e implemente estes padrões.

Na primeira parte do laboratório foi analisado o funcionamento do *framework* DRAGON com testes de interoperabilidade entre todos os seus componentes.

Na segunda parte foram realizados os testes para atingir o objetivo precípuo do trabalho, tendo sido analisadas as funcionalidades de MPLS-TE e QoS Diffserv em uma rede de roteadores, culminando numa proposta de suporte a serviços de DCN com interoperabilidade com o *framework* DRAGON.

O caderno de testes a seguir, além de apresentar o funcionamento básico do DRAGON e seus componentes, propõe-se a comprovar como os tráfegos de DCN podem ser isolados dentro uma rede operativa sem impacto para os demais serviços. A sequencia de testes, comprovações e resultados esperados são:

1. Interligação dos componentes do DRAGON e criação de um LSP comprovando o funcionamento do *framework* dentro uma topologia simplificada. Espera-se como resultado o funcionamento completo da solução DRAGON e seus subsistemas num ambiente intradomínio, troca de mensagens dos protocolos de TE entre os VLSR e a criação de um LSP entre dois VLSR.
2. A segunda etapa dos testes deverá demonstrar como os LSP são criados, seus principais tipos, proteção em caso de falha, escolha de caminhos baseados em restrições, priorização de LSP de maior hierarquia e limitação de banda. Para isso, espera-se como resultado a criação de LSP que sinalizam caminhos através do protocolo IGP de roteamento da rede, LSP que usam técnicas de ERO (*Explicit Route Object*) para determinação condicional do caminho salto a salto, LSP com caminhos principais e secundários para contingência e com balanceamento de tráfego, limitação de banda e priorização na sinalização para criação e remoção de LSP.
3. A terceira etapa dos testes deverá apresentar como os LSP de camada 2 interligam equipamentos no nível *Ethernet*, mantendo todas as funcionalidades anteriormente apresentadas. Para estes testes o resultado esperado são LSP de camada 2 interligando equipamentos puramente camada 2 como *switches Ethernet*.
4. A quarta etapa apresentará o funcionamento do QoS Diffserv com diferentes tipos de filas e propostas de segregação dos fluxos do serviço DCN e seus LSP dos diversos

outros serviços existentes. Como resultado é esperada a criação de filas e classes de QoS Diffserv, com diferentes níveis de priorização e técnicas de enfileiramento, de maneira a isolar o tráfego gerado pelas DCN dos demais serviços, garantindo qualidade para as diversas mídias a serem transportadas.

6.1 *GRAPHICAL NETWORK SIMULATOR* - GNS3

O GNS3 [25] é um simulador gráfico, código aberto, que permite a simulação de redes complexas, através da emulação dos sistemas operacionais da Cisco® (IOS®) e da Juniper® (Junos®). Este emulador permite que seja executada a grande maioria dos sistemas operacionais destes equipamentos de rede (roteadores, *switches* e *firewalls*) em um ambiente virtualizado.

O GNS3 é um *front-end* gráfico para os produtos Dynamips® [25] e Qemu® [25], que são os programas centrais que permitem a emulação dos sistemas operacionais dos equipamentos de rede. Estes *softwares* criam uma interface amigável onde os usuários podem criar topologias de rede graficamente.

Existem diversos outros simuladores de rede disponíveis na Internet, porém, na grande maioria, não é possível executar todos os tipos de comandos e protocolos existentes nos equipamentos reais por serem apenas uma versão sintetizada dos sistemas operacionais de equipamentos de rede. Este problema não acontece com o GNS3 em virtude de ele executar o *software* real do dispositivo de rede.

O GNS3, além de ser uma ferramenta utilizada para simular redes, também possui a característica de funcionar como um emulador, permitindo que o computador na qual esteja sendo executado interopere com equipamentos reais sem que estes percebam que estão ligados a elementos de um ambiente emulado. Isso garante que a implementação deste laboratório terá total aplicabilidade em redes reais.

O resultado de todo este laboratório poderá ser diretamente usado em dispositivos reais, bastando, para isso, aplicar os arquivos de configuração apresentados nas Figuras desta Seção e no ANEXO deste trabalho.

Neste estudo foi possível apenas simular equipamentos do fabricante Cisco® por exigirem recursos menos agressivos de CPU e memória do computador hospedeiro, quando comparado com a emulação de equipamentos Juniper®. De qualquer forma, esta limitação da

simulação para equipamentos apenas da Cisco® não inviabiliza sua aplicabilidade a outros fabricantes, uma vez que estes equipamentos possuem características similares aos da Juniper® e permitem a execução de todos os testes necessários das técnicas de Engenharia de Tráfego e QoS Diffserv propostas.

6.2 TESTES E SIMULAÇÕES EM LABORATÓRIO

6.2.1 Laboratório do *Framework* DRAGON

Dentre as arquiteturas propostas para estudo foi escolhido o DRAGON para simulação em laboratório como base para a criação dos LSP dinâmicos, uma vez que o AUTOBAHN possui características semelhantes e seus aplicativos ainda estão em um nível de maturidade inferior ao do DRAGON. Foi definido como *testbed* o laboratório de redes da UFF para instalação, configuração e testes desta arquitetura.

O laboratório de redes da UFF, integrado à rede GIGA [13] permite a realização de testes entre vários domínios de diversas universidades do país. Apesar desta possibilidade, este não é o foco deste estudo.

Para a realização dos experimentos foi cedido pela RNP um conjunto de elementos como *racks*, servidores Intel®, *switches* dos fabricantes Cisco® e Extreme®. A lista completa de equipamentos utilizados nos testes é descrita no Quadro 2.

Descrição	**Quantidade**
Servidor Dell® Intel® Core Quad	2
Switch Cisco® 2950	2
Switch Extreme® Summit 24e®	1
Desktop PC modelo Intel® Core 2 Duo	2
Notebook modelo Intel® Core 2 Duo	1
Monitor, teclado e *mouse*	1

Quadro 2 – Lista de equipamentos utilizados no laboratório.

A configuração dos elementos do laboratório iniciou-se com a instalação física dos servidores Dell®. Foi escolhido como sistema operacional para todos os servidores a versão 9 do Linux Ubuntu [14] que, no momento da elaboração deste estudo, era a versão mais recente deste sistema operacional, largamente conhecido como sendo de uso *freeware*. Outros sistemas operacionais baseados em Linux podem ser utilizados desde que possuam todos os módulos e requisitos para o funcionamento do DRAGON e que poderão ser verificados no documento *Virtual Label Switching Router Implementation Guide* [24].

A Figura 12 apresenta a topologia do laboratório onde são representadas as conexões lógicas (setas vermelhas) entre os elementos VLSR e conexões físicas entre os VLSR e *switches* (setas azuis). Após a instalação inicial do DRAGON e comprovação que todos seus módulos como o OSPF, o RSVP-TE, o VLSR e o NARB estavam ativos e funcionando, foi possível o início dos testes de criação de um circuito virtual. O detalhamento com todas as etapas para estabelecimento do circuito virtual e dinâmico pode ser encontrado no documento *Virtual Label Switching Router Implementation Guide* [24]. O resultado deste laboratório foi a criação de um simples LSP camada L2 entre os computadores A e B, conforme representado, comprovando, assim, o funcionamento do DRAGON e de seus módulos.

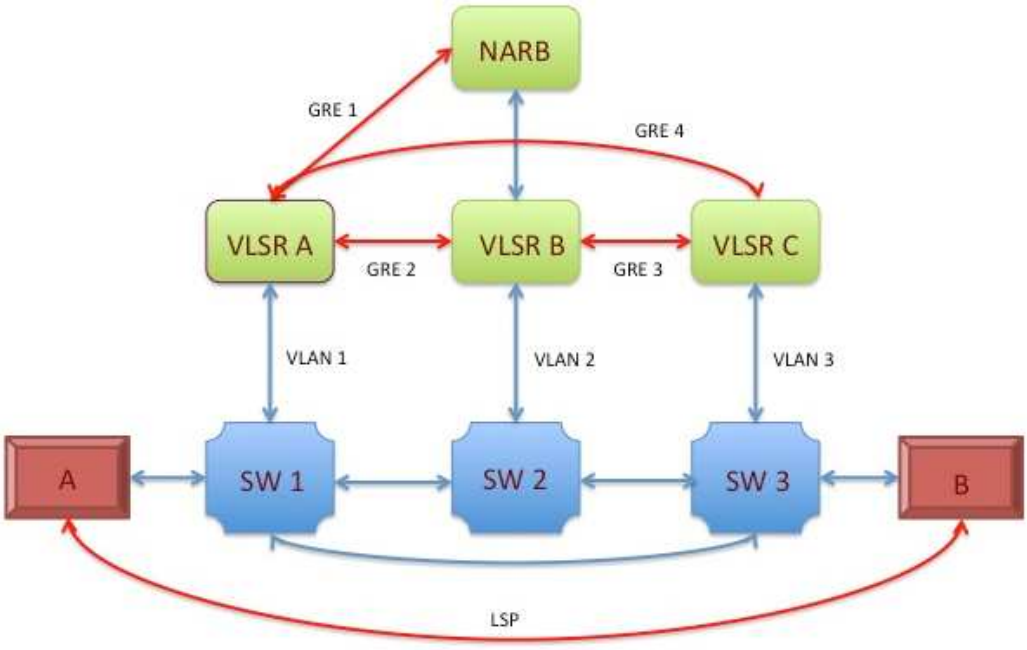

Figura 12– Topologia esquemática do laboratório do framework DRAGON

Na Figura 12, os tuneis GRE interligam o plano de controle de dados do DRAGON e interconectam logicamente os VLSR para troca das sinalizações dos protocolos de roteamento.

6.2.2 Endereçamento IP

O Quadro 3 apresenta a distribuição do endereçamento IP utilizada no laboratório. Faixas específicas de endereços foram separadas para cada segmento, permitindo a interconexão com o laboratório de redes da Engenharia de Telecomunicações da UFF para acesso à Internet, à rede GIGA e demais máquinas do projeto DRAGON nas entidades externas. Esta configuração de endereçamento IP permite que estudos futuros tenham como base inicial uma distribuição de endereçamento e VLAN para simulação com o DRAGON.

Elemento	**Interface**	**Rede**	**Endereço**	**Conexão**
NARB	ETH0	192.168.1.0 /24	192.168.1.104	Rede Lab UFF
NARB	ETH1	10.32.0.0/24	10.32.0.8	NARB - Rede GiGA
NARB	GRE1	10.10.1.0.0/24	10.10.1.1	NARB - VLSRA
VLSRA	ETH0	192.168.1.0 /24	192.168.1.101	Rede Lab UFF
VLSRA	ETH1	192.168.3.0/24	192.168.3.1	VLSRA – SWITCH1
VLSRA	GRE1	10.10.1.0/24	10.10.1.1	VLSRA - NARB
VLSRA	GRE2	10.10.2.0/24	10.10.2.1	VLSRA - VLSRB
VLSRA	GRE4	10.10.4.0/24	10.10.4.1	VLSRA - VLSRC
VLSRB	ETH0	192.168.1.0 /24	192.168.1.102	Rede Lab UFF
VLSRB	ETH1	192.168.4.0/24	192.168.4.1	VLSRB – SWITCH2
VLSRB	GRE2	10.10.2.0/24	10.10.2.2	VLSRB - VLSRA
VLSRB	GRE3	10.10.3.0/24	10.10.3.1	VLSRB - VLSRC
VLSRC	ETH0	192.168.1.0 /24	192.168.1.103	Rede Lab UFF
VLSRC	ETH1	192.168.5.0/24	192.168.5.1	VLSRC – SWITCH3
VLSRC	GRE3	10.10.3.0/24	10.10.3.2	VLSRC - VLSRB
VLSRC	GRE4	10.10.4.0/24	10.10.4.2	VLSRC - VLSRA
SWITCH1	VLAN1	192.168.3.0/24	192.168.3.2	SWITCH1 - VLSRA
SWITCH2	VLAN2	192.168.4.0/24	192.168.4.2	SWITCH2 - VLSRB
SWITCH3	VLAN3	192.168.5.0/24	192.168.5.2	SWITCH3 - VLSRC

Quadro 3 – Lista de distribuição de endereços IP e redes no laboratório.

6.3 LABORATÓRIO MPLS-TE

6.3.1 Implantação e Operação

Toda abordagem na implantação de novas tecnologias de roteamento em uma rede deve sempre considerar como premissas a facilidade de implantação e, principalmente, a baixa complexidade operacional. Neste sentido, as simulações a seguir pretendem incorporar as novas funcionalidades na rede MPLS, de tal forma a permitir que seus administradores possam aproveitar-se das soluções DCN para controlar os recursos alocados pelos LSP dinâmicos e os processos de roteamento.

Inicialmente, a rede deve estar dotada de um protocolo de distribuição automática de rótulos (*labels*). Usualmente o protocolo LDP (*Label Distribution Protocol*) é utilizado, por ser o mais simples de ser configurado e operado. Como o LDP não suporta Engenharia de Tráfego, a sobreposição deste protocolo com o RSVP-TE faz-se necessária, sendo que ambos podem conviver num mesmo domínio sem interferir um no outro. A Figura 13 apresenta um exemplo de rede MPLS, com os roteadores de borda e núcleo, mostrando que o domínio de funcionamento dos protocolos RSVP-TE e LDP é apenas no interior da rede MPLS. Ainda nesta figura, nota-se que estes protocolos convivem simultaneamente dentro de um mesmo domínio, neste caso, representado como AS 1. Esta abordagem facilita a implantação, uma vez que o LDP suportará todos os atuais serviços da rede MPLS (como VPN MPLS, Internet, entre outros) e o RSVP-TE será aplicado apenas nos circuitos (interfaces dos roteadores) onde se pretende usar TE.

Por padrão, nos equipamentos dos fabricantes Cisco® e Juniper® [30], a preferência de escolha das rotas na tabela de roteamento geradas pelo protocolo RSVP-TE é maior quando comparada a do LDP, o que garante que os LSP sinalizados pelo RSVP-TE possuirão sempre maior preferência quando comparados aos LSP criados pelo LDP. Enquanto o LDP define LSP baseados no melhor caminho IP do protocolo IGP utilizado (IS-IS ou OSPF), o RSPV-TE contará com todas as possibilidades de TE disponíveis.

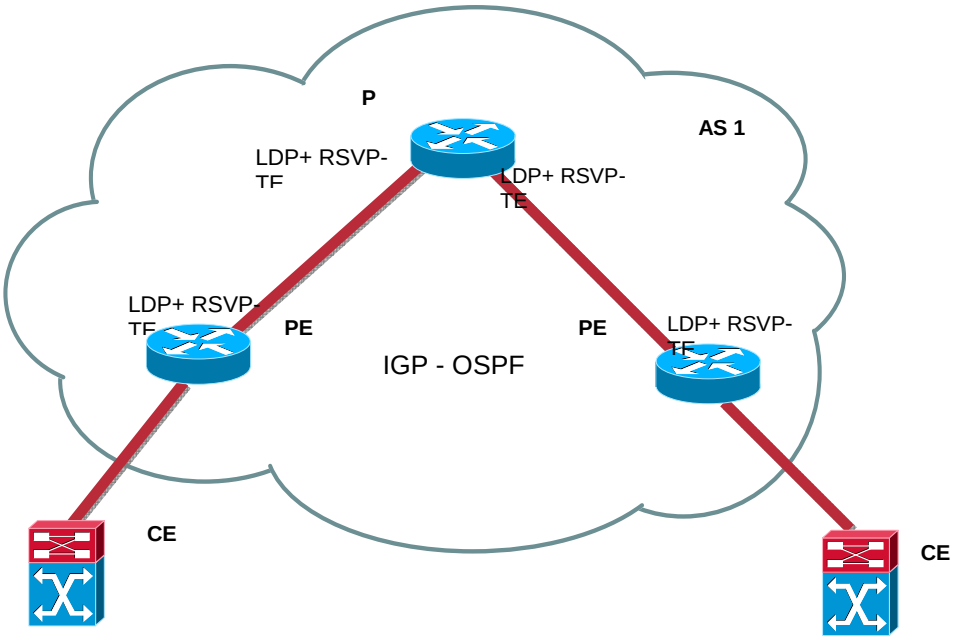

Figura 13 - Uso dos protocolos LDP e RSVP-TE em uma rede MPLS

6.3.2 Experimentos de MPLS-TE

O cenário montado no laboratório foi definido de tal forma a possibilitar a análise do funcionamento de algumas técnicas de Engenharia de Tráfego e QoS, simulando situações de criação de LSP com diferentes níveis de priorização, banda, roteamento explícito ou dinâmico, resultados de falhas em circuitos e elementos, e balanceamento de tráfego.

O *setup* do laboratório foi executado com roteadores Cisco 7206®, emulados no GNS3, com versão de sistema operacional *Advanced Enterprise* 12.2(33) que agrega suporte a todos os protocolos necessários a este estudo, equipados com portas *fastethernet* de 100 Mbit/s e/ou *gigabitethernet* de 1000 Mbit/s. O protocolo IGP *(Interior Gateway Protocol)* escolhido como base para o laboratório foi o OSPF e em todas as interfaces foi utilizado apenas o RSVP-TE para a criação dos LSP de Engenharia de Tráfego. Por se tratar de um laboratório de pequenas proporções não foi necessário o uso do LDP para sinalização automática dos LSP. No caso de um grande *backbone*, a importância do LDP estaria no fato da criação automática de LSP ponto a ponto entre todos os elementos PE da rede, garantindo que tráfegos de quaisquer origens para quaisquer destinos pudessem ser comutados via MPLS.

Para facilitar a configuração e a escolha de caminhos (rotas) que os pacotes seguiriam dentro do *backbone* os custos do protocolo OSPF foram mantidos automáticos, tendo como referência o valor de 1.000.000 bit/s. O custo é calculado pelos roteadores dividindo o valor de referência pela banda nominal da interface. Assim, nos testes realizados, para as interfaces *fastethernet* o custo do OSPF foi calculado como 10 e para as interfaces *gigabitethernet* este valor foi calculado como 1.

A Figura 14 mostra a topologia física de interligação dos equipamentos no simulador do laboratório onde cada equipamento, representado pelo nome Rx, é um equipamento de *backbone* com as características de configuração acima descritas. Esta topologia foi escolhida por ser uma representação simplificada de uma rede com diversos caminhos entre os nós de rede, permitindo a criação de LSP de caminhos diversos e possibilitando a execução do caderno de testes.

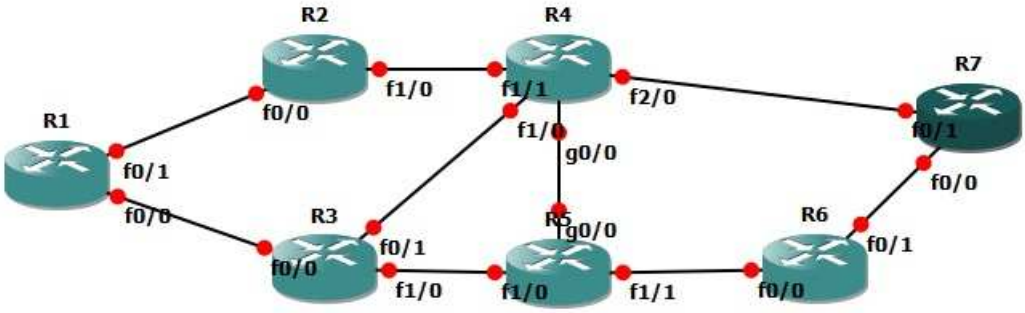

Figura 14 – Topologia de rede no simulador do laboratório

O Quadro 4 apresenta a configuração de endereçamento IP utilizada para a interligação entre as interfaces dos roteadores.

Nome do Roteador	***System Name***	**Interface**	**Endereço IP**
R1	PE1	Fastethernet 0/0	10.1.1.1
R1	PE1	Fastethernet 0/1	10.1.1.5
R1	PE1	Loopback0	10.10.10.1
R2	PE2	Fastethernet 0/0	10.1.1.6
R2	PE2	Fastethernet 1/0	10.1.1.9
R2	PE2	Loopback0	10.10.10.2
R3	PE3	Fastethernet 0/0	10.1.1.2
R3	PE3	Fastethernet 0/1	10.1.1.13
R3	PE3	Fastethernet 1/0	10.1.1.17
R3	PE3	Loopback0	10.10.10.3
R4	PE4	Gigabitethernet 0/0	10.1.1.25
R4	PE4	Fastethernet 1/0	10.1.1.14
R4	PE4	Fastethernet 1/1	10.1.1.10
R4	PE4	Fastethernet 2/0	10.1.1.21
R4	PE4	Loopback0	10.10.10.4
R5	PE5	Gigabitethernet 0/0	10.1.1.26
R5	PE5	Fastethernet 1/0	10.1.1.18
R5	PE5	Fastethernet 1/1	10.1.1.29
R5	PE5	Loopback0	10.10.10.5
R6	PE6	Fastethernet 0/0	10.1.1.30
R6	PE6	Fastethernet 0/1	10.1.1.33
R6	PE6	Loopback0	10.10.10.6
R7	PE7	Fastethernet 0/0	10.1.1.34
R7	PE7	Fastethernet 0/1	10.1.1.22
R7	PE7	Loopback0	10.10.10.7

Quadro 4– Distribuição de endereçamento IP do laboratório

6.3.3 Criação de LSP dinâmicos e explícitos

No detalhamento da Figura 15 é apresentado o *setup* inicial do roteador R1 (PE1) com a ativação dos protocolos OSPF e RSVP-TE, deixando o roteador apto para iniciar a criação de LSP.

```
**************************************************************************
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
ip source-route
!
ip cef
!
multilink bundle-name authenticated
mpls traffic-eng tunnels
!
!
interface Loopback0
 ip address 10.10.10.1 255.255.255.255
```

```
!
interface FastEthernet0/0
 description R1 to f0/0 R3
 ip address 10.1.1.1 255.255.255.252
 load-interval 30
 speed auto
 duplex auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 100000 100000
!
interface FastEthernet0/1
 description R1 to f0/0 R2
 ip address 10.1.1.5 255.255.255.252
 load-interval 30
 speed auto
 duplex auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 100000 100000
!
router ospf 1
 router-id 10.10.10.1
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 network 0.0.0.0 255.255.255.255 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
ip classless
!
no ip http secure-server
!
!
!
!
!
control-plane
```

```
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
```

Figura 15 – Ativação dos protocolos OSPF e RSVP-TE no R1

Todos os demais roteadores do laboratório possuem configurações semelhantes à apresentada para o roteador R1, com variações no endereçamento IP das interfaces, conforme Quadro 4. As configurações básicas dos roteadores de R2 a R7 são apresentadas no ANEXO.

Inicialmente todas as interfaces foram mantidas ativas com uma reserva de banda para o protocolo RSVP-TE no valor nominal igual ao da interface, ou seja, para interfaces de 100Mbit/s o valor permitido para o RSVP-TE sinalizar um túnel era de 100Mbit/s, assegurado pelo comando "*ip rsvp bandwidth 100000 100000*" aplicado em cada uma das interfaces dos roteadores.

Foram criados dois túneis de MPLS-TE. O primeiro (tunnel 1) estabelecia um LSP entre os roteadores R1 e R7, com as seguintes características:

- Banda de 30Mbit/s
- Destino R7
- Roteamento dinâmico (usa o melhor caminho do IGP)
- Prioridade de estabelecimento igual a 5

O segundo túnel (tunnel 2) estabelecia um LSP entre os roteadores R1 e R6, com as seguintes características:

- Banda de 30Mbit/s
- Destino R6

- Roteamento explícito (caminho definido passando pelos seguintes equipamentos R1>R2>R4>R7>R6 independente do melhor caminho do IGP)
- Prioridade de estabelecimento igual a 1

```
**********************************************************************
interface Tunnel1
 description TE to PE7
 ip unnumbered Loopback0
 tunnel destination 10.10.10.7
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 5 5
 tunnel mpls traffic-eng path-option 1 dynamic
 tunnel mpls traffic-eng record-route
 tunnel mpls traffic-eng bandwidth 30000
!
interface Tunnel2
 description TE to PE6 EXPLICIT
 ip unnumbered Loopback0
 tunnel destination 10.10.10.6
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 30000
 tunnel mpls traffic-eng path-option 1 explicit name TUNNEL2_TO_PE6
 tunnel mpls traffic-eng record-route
 tunnel mpls traffic-eng fast-reroute
ip explicit-path name TUNNEL2_TO_PE6 enable
 next-address 10.1.1.6
 next-address 10.1.1.10
 next-address 10.1.1.22
 next-address 10.1.1.33
**********************************************************************
```

Figura 16 – Criação dos LSP 1 e 2

Pode ser observado pela Figura 17 que os túneis foram estabelecidos *(status "up").* Como o protocolo RSVP-TE possui métrica menor que a do OSPF, o caminho escolhido pelo roteador para envio dos pacotes do R1 para os roteadores R6 e R7 foram os túneis de TE (1 e 2), como comprovado pelo resultado do comando apresentado na Figura 18.

```
**********************************************************************************
PE1#show ip int brief
Interface          IP-Address      OK? Method      Status          Protocol
FastEthernet0/0    10.1.1.1        YES NVRAM       up              up
FastEthernet0/1    10.1.1.5        YES NVRAM       up              up
Loopback0          10.10.10.1      YES NVRAM       up              up
Tunnel1            10.10.10.1      YES TFTP        up              up
Tunnel2            10.10.10.1      YES TFTP        up              up

PE1#show ip route 10.10.10.7
Routing entry for 10.10.10.7/32
  Known via "ospf 1", distance 110, metric 31, type intra area
  Last update from 10.10.10.7 on Tunnel1, 00:10:13 ago
  Routing Descriptor Blocks:
  * 10.10.10.7, from 10.10.10.7, 00:10:13 ago, via Tunnel1
      Route metric is 31, traffic share count is 1

PE1#show ip route 10.10.10.6
Routing entry for 10.10.10.6/32
  Known via "ospf 1", distance 110, metric 31, type intra area
  Last update from 10.10.10.6 on Tunnel2, 00:10:40 ago
  Routing Descriptor Blocks:
  * 10.10.10.6, from 10.10.10.6, 00:10:40 ago, via Tunnel2
      Route metric is 31, traffic share count is 1
**********************************************************************************
```

Figura 17 – Situação dos túneis de TE em *status up*

```
**********************************************************************************
PE1#show mpls traffic-eng tunnels tunnel 1
Name: TE to PE7                    (Tunnel1) Destination: 10.10.10.7
  Status:
    Admin: up        Oper: up     Path: valid       Signalling: connected
    path option 1, type dynamic (Basis for Setup, path weight 30)
      RSVP Path Info:
      My Address: 10.1.1.5
      Explicit Route: 10.1.1.6 10.1.1.9 10.1.1.10 10.1.1.21 10.1.1.22 10.10.10.7

PE1#show mpls traffic-eng tunnels tunnel 2
Name: TE to PE6 EXPLICIT           (Tunnel2) Destination: 10.10.10.6
  Status:
    Admin: up        Oper: up     Path: valid       Signalling: connected
    path option 1, type explicit TUNNEL2_TO_PE6 (Basis for Setup, path weight 40)
    RSVP Path Info:
      My Address: 10.1.1.5
      Explicit Route: 10.1.1.6 10.1.1.9 10.1.1.10 10.1.1.21 10.1.1.22 10.1.1.34 10.1.1.33
10.10.10.6
**********************************************************************************
```

Figura 18 – Criação dos LSP 1 e 2

6.3.4 Balanceamento de tráfego entre LSP

Outra característica importante da engenharia de tráfego é a possibilidade de balanceamento de tráfego entre LSP.

Para comprovação da capacidade de balanceamento de tráfego foi criado um segundo LSP para o roteador R6, desta vez do tipo dinâmico. Através dos comandos apresentados na Figura 19 foi configurado o balanceamento de tráfego.

Com isso passaram a existir, portanto, dois LSP direcionados ao roteador R6. O primeiro (tunnel 2), possuindo um caminho explícito através do caminho R1>R2>R4>R7>R6, e o segundo (tunnel 3), possuindo um caminho dinâmico, seguindo o IGP (que, pelas métricas definidas, adotava o caminho R1>R3>R5>R6).

A análise da tabela de roteamento permitiu comprovar que os pacotes seriam roteados de forma balanceada entre os LSP por possuírem métricas e destinos iguais.

Após tal verificação foi adicionada a funcionalidade de reroteamento rápido (*Fast Reroute*) para garantir uma rápida comutação entre LSP.

```
**********************************************************************************
PE1#show run int tunnel 3
Building configuration...
interface Tunnel3
 description TE to PE6 DYNAMIC
 ip unnumbered Loopback0
 mpls traffic-eng tunnels
 tunnel destination 10.10.10.6
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 2 2
 tunnel mpls traffic-eng bandwidth 30000
 tunnel mpls traffic-eng path-option 1 dynamic
 tunnel mpls traffic-eng record-route
 tunnel mpls traffic-eng fast-reroute
end
**********************************************************************************
```

Figura 19 – Segundo LSP para R6 para balanceamento de tráfego

```
**********************************************************************
PE1#show ip route 10.10.10.6
Routing entry for 10.10.10.6/32
  Known via "ospf 1", distance 110, metric 31, type intra area
  Last update from 10.10.10.6 on Tunnel2, 00:16:50 ago
  Routing Descriptor Blocks:
    10.10.10.6, from 10.10.10.6, 00:16:50 ago, via Tunnel3
      Route metric is 31, traffic share count is 1
  * 10.10.10.6, from 10.10.10.6, 00:16:50 ago, via Tunnel2
      Route metric is 31, traffic share count is 1
**********************************************************************
```

Figura 20 – Balanceamento de trafego entre LSP

6.3.5 Criação de LSP Camada 2

Complementando as técnicas apresentadas, introduziu-se a possibilidade de criação de LSP em camada 2 (L2), os quais permitem a emulação e o transporte de circuitos, neste caso, baseados em *Ethernet*.

No laboratório foi criado um LSP L2 interligando o roteador R1 e R7 através de um dos túneis de engenharia de tráfego. Com isso assegurou-se que, além de emular um circuito L2, seriam mantidas todas as funcionalidades apresentadas de engenharia de tráfego. No exemplo a seguir, o circuito L2 utiliza o túnel de TE número 1 (tunnel 1).

A Figura 21 apresenta a ligação de dois *switches Ethernet* SW1 e SW2 por meio deste circuito virtual em camada 2. Para os switches esta ligação é completamente transparente, semelhante à ligação física utilizando-se cabos *Ethernet* convencionais.

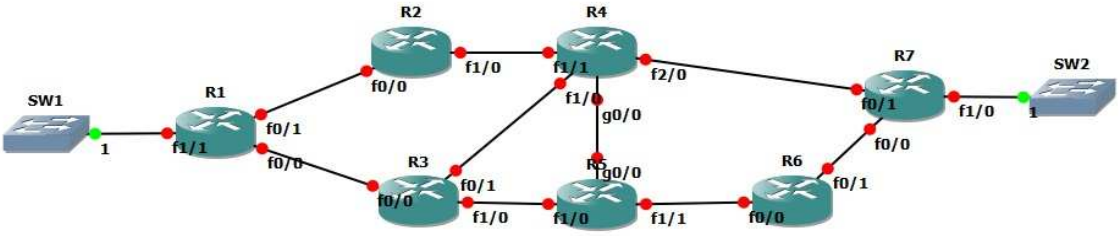

Figura 21 – Topologia de rede no simulador para testes de LSP L2

A Figura 22 apresenta os comandos necessários para a criação do LSP L2 entre os roteadores R1 e R7, ligando os switches ethernet SW1 e SW2.

```
**************************************************************************
PE1#show run
Building configuration...
!
hostname PE1
!
pseudowire-class LSP_L2
 encapsulation mpls
 preferred-path interface Tunnel1
!
interface Tunnel1
 description TE to PE7
 ip unnumbered Loopback0
 tunnel destination 10.10.10.7
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 5 5
 tunnel mpls traffic-eng path-option 1 dynamic
 tunnel mpls traffic-eng record-route
 tunnel mpls traffic-eng auto-bw min-bw 10000
!
interface FastEthernet1/1
 no ip address
 speed auto
 duplex auto
 xconnect 10.10.10.7 100 pw-class LSP_L2
!
**************************************************************************
```

Figura 22 – LSP L2 ligando SW1 e SW2

O resultado dos comandos a seguir comprova a criação do circuito L2 entre os roteadores R1 e R7 através do túnel de TE 1.

```
**********************************************************************************
PE1#show xconnect all
Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down          AD=Admin Down      IA=Inactive
  SB=Standby  RV=Recovering      NH=No Hardware
XC ST  Segment 1                    S1 Segment 2                    S2
------+---------------------------------+--+---------------------------------+--
UP     ac   Fa1/1(Ethernet)           UP mpls 10.10.10.7:100          UP


PE1#show mpls l2transport summary
Destination address: 10.10.10.7, total number of vc: 1
  0 unknown, 1 up, 0 down, 0 admin down, 0 recovering, 0 standby
  1 active vc on MPLS interface Tu1


PE1#show mpls l2transport vc
Local intf     Local circuit            Dest address    VC ID      Status
-------------  ------------------------- --------------- ---------- ----------
Fa1/1          Ethernet                 10.10.10.7      100        UP
**********************************************************************************
```

Figura 23 – Criação do LSP L2 entre SW1 e SW2

6.4 RESULTADOS OBTIDOS PELOS ENSAIOS DOS LABORATÓRIOS

A partir dos ensaios de laboratório realizados, foi possível comprovar o funcionamento do *framework* DRAGON e de seus subsistemas, além de atestar a correta sinalização e a criação de um LSP interligando os VLSR existentes na topologia simplificada, montada para validação.

Intencionava-se integrar os protocolos de sinalização de TE e roteamento do DRAGON com os sistemas operacionais dos roteadores Cisco® emulados no GNS3. No entanto, não foi possível alcançar tal objetivo, em virtude das dificuldades encontradas para compatibilizar os *daemons* de RSVP-TE e OSPF-TE existentes no DRAGON com os protocolos implementados nos equipamentos Cisco®.

Embora fosse contribuir para o enriquecimento do presente trabalho, os esforços necessários para a resolução do problema identificado canalizariam a atenção para outro foco diferente do cerne deste estudo. Por este motivo, e, diante do fato de que não era imprescindível para a comprovação dos resultados, optou-se por relegar a idéia de integração supracitada, mas a mesma será, *a posteriori*, apresentada como sugestão para trabalhos futuros.

Face ao exposto, os experimentos com TE e QoS foram realizados de maneira a comprovar a possibilidade de segregação de tráfegos de dados utilizando-se implementações existentes nos equipamentos Cisco®, que, mesmo emulados, suportam protocolos existentes em redes reais.

Os resultados obtidos e destacados neste capítulo atestam o sucesso das técnicas mencionadas e ofereceram embasamento técnico para as propostas de suporte e segregação ao serviço de DCN apresentadas no Capítulo 7.

7. SUPORTE AO SERVIÇO DCN

QoS e Engenharia de Tráfego (TE) são técnicas conhecidas e aplicadas em redes há mais de uma década. O QoS tem como principal característica garantir os recursos mínimos de rede necessários para que determinada aplicação possa operar dentro de seus limiares de funcionamento. Por outro lado, o uso de TE basicamente define que os fluxos de dados, dessas aplicações, possam seguir por caminhos específicos e definidos a partir de determinadas priorizações ou por políticas aplicadas pelo administrador da rede.

É usual, nos dias atuais, redes que usem o QoS para a garantia dos recursos a determinado fluxo de dados e TE para escolha de caminhos específicos, balanceamento de tráfego, proteção de circuitos, entre outras coisas. O que se espera neste trabalho de suporte ao serviço DCN é o de apresentar algumas propostas do uso de QoS combinado com TE para resolver o problema específico da inclusão deste novo serviço DCN em uma rede já operacional.

Os dados transportados por DCN possuem normalmente a característica de serem grandes consumidores de recurso, principalmente largura de banda. O *backbone* que transporta o DCN deve ser capaz de suportar e tratar essas características, além de atender às necessidades dos demais fluxos de dados existentes.

A proposta de solução para este problema, apresentada neste trabalho, utilizará o QoS para segregar e garantir o DCN e demais aplicações, e em conjunto com o TE, criará limites e priorizações aos LSP, uma vez que uma característica forte do DCN é a de que o usuário final possa solicitar e agendar diretamente o LSP conforme sua necessidade.

Durante o processo de análise e definição de como suportar um novo serviço faz-se necessário considerar como fator limitante as características intrínsecas de cada equipamento e a rede propriamente dita, com seus *links*, capacidades e topologia.

O QoS, e como este é suportado em cada equipamentos de rede, é um importante fator decisório na hora de definir como segregar fluxos de dados dentro de uma *backbone* IP. Como

a proposta deste trabalho é o de apresentar modelos aplicáveis numa rede real, deverão ser considerados modelos de segregação, na visão do QoS, tanto para os casos de equipamentos que suportam uma menor quantidade de filas quanto para os que possuem uma maior granularidade. Com foco no caso motivacional deste trabalho, a rede da RNP possui diferentes tipos e modelos de equipamentos que suportam, por exemplo, apenas quatro filas de QoS. As possibilidades de segregação de diferentes fluxos de dados em apenas quatro filas serão limitadas uma vez que os serviços previamente existentes à implementação do DCN certamente demandam essa quantidade mínima de separação de tráfego. Por outro lado, nesta mesma rede, existem modelos de equipamentos que suportam até oito filas, aumentando, assim, as possibilidades de segregação.

Neste capítulo serão apresentadas algumas propostas e modalidades de inclusão de um serviço de criação de circuitos dinâmicos em uma rede com equipamentos e QoS com diferentes quantidades e tipos de filas. Serão considerados equipamentos que suportam pelo menos quatro filas de QoS e para equipamentos que suportam até oito filas.

Realizando uma análise de impacto da entrada de novos fluxos de dados baseados no serviço DCN, o estudo das propostas e modalidades deste serviço deverá considerar que os serviços existentes não sofrerão perdas ou degradações de qualidade. A forma como serão alocados dinamicamente estes circuitos, limitações de banda para controle do número máximo de LSP criados e a banda consumida serão fatores determinantes para o sucesso da implementação do DCN.

Associando o uso dos controles de alocação dos LSP no nível da Engenharia de Tráfego e a separação destes LSP em diferentes filas de Qos será possível que, mesmo em situações de grandes demandas, sejam mantidos os níveis de serviço. Para essa segregação na camada do MPLS será possível a definição de limites para a alocação de circuitos, o que garantirá que o DCN não utilizará mais banda do que a definida pelo administrador da rede.

Neste Capítulo será apresentado como a combinação de QoS e TE poderá suportar o serviço DCN segregando-o dos demais tráfegos de dados mesmo em situações onde existem limitações técnicas para uma maior granularidade para esta segmentação.

7.1 QUALIDADE DE SERVIÇO PARA SUPORTE A DCN

Atualmente é impossível pensar em Engenharia de Tráfego sem considerar o uso simultâneo de alguma técnica de QoS.

O QoS, além de proporcionar o atendimento a requisitos necessários ao funcionamento de diversas aplicações IP, torna possível o acondicionamento dos LSP dentro do *backbone* de maneira a segregar diferentes serviços.

Esta facilidade propiciada pelo QoS gera um novo desafio para os administradores, que é o de garantir que o serviço de LSP dinâmicos não interfira em outros serviços já existentes.

Com este intuito, serão apresentados a seguir alguns possíveis cenários de suporte ao serviço DCN, cuja definição baseou-se na premissa de poder prover diferentes serviços de transporte IP em camadas 2 e 3 (L2 e L3), com diferentes níveis de qualidade , segregando os serviços existentes na rede.

A RFC 4594 [26], que define uma proposição de uso de QoS, é atualmente uma referência para a indústria de equipamentos, sendo adotada como melhores práticas para definição de QoS em uma rede [27]. Em tal RFC define-se que todas as aplicações podem ser classificadas em uma dentre as doze diferentes descritas a seguir:

1. Telefonia VoIP;
2. Difusão de vídeo;
3. Serviços de tempo real interativos;
4. Conferência multimídia;
5. *Streaming* multimídia;
6. Fluxos de controle de rede ou dados do plano de controle;
7. Sinalização de voz e vídeo;
8. Operação e manutenção da rede;
9. Dados de baixa latência;
10. Dados de alto *throughput*;
11. *Best effort*;
12. Dados de baixa prioridade.

Ainda que a RFC 4594 proponha um modelo de 12 classes de serviço, alguns fabricantes reconhecem que nem todos as redes estão prontas para desenvolver um QoS tão

complexo. Dessa forma, nas implementações de mercado, é recomendado que as políticas de QoS adotadas nas redes tenham início com um modelo simples, com apenas poucas classes, e evoluam a um modelo de, no máximo 12 classes [27]. Em outras palavras, o modelo de 12 classes, definido pela RFC 4594, é adotado como um limitante superior, não devendo ser excedido, face à proporcionalidade direta entre a complexidade e a quantidade excessiva de classes.

Partindo destes princípios, boas práticas e recomendações de fabricantes de equipamentos, iniciou-se o estudo com uma proposição de 4 filas de QoS, com algumas opções de classes com base no documento *Quality of Service Design Overview* [28].

Além de ser uma boa prática iniciar o estudo com apenas 4 filas de QoS, equipamentos de comutação IP (roteadores e *switches*) mais antigos normalmente possuem esta limitação de suporte a apenas 4 filas de QoS. Por outro lado, os equipamentos mais recentes e de grande porte, que ocupam em grande parte a função de núcleo das redes, podem suportar até 8 filas de QoS.

Com a necessidade de propor uma forma simplificada de QoS com 4 filas, adaptado às necessidades de segregação dos serviços de DCN, foi considerado como base o modelo apresentado na Figura 24.

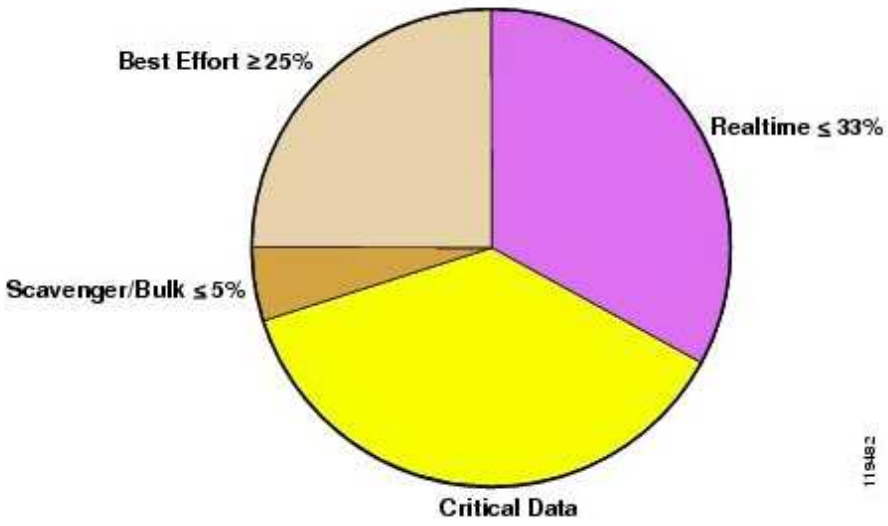

Figura 24 – Modelo de 4 filas de QoS

Fonte: www.cisco.com [28]

Os percentuais mostrados na Figura 24 são proposições que, segundo o fabricante Cisco®, seriam as melhores práticas recomendadas para dimensionamento da fila através de um método de escalonamento de QoS ponderado [28].

Com este modelo da RFC 4594 adaptado pela Cisco® na qual a fila *Scavenger/Bulk* é utilizada para transporte de fluxos de dados de baixa importância e com menos prioridade que o melhor esforço. É proposto, neste estudo, a substituição da fila *Scavenger/Bulk* por uma fila específica para transporte dos LSP do serviço DCN. Dessa forma, tem-se um modelo inicial aplicável a redes que necessitam de segregação do serviço DCN dos demais existentes, estando o QoS limitado a 4 filas.

O tráfego de dados do tipo *Scavenger/Bulk*, por ser predominantemente de baixa prioridade, pode ser somado à classe *best effort* sem causar prejuízo na separação de serviços em classes de mesmas características. Com essa mudança, o uso de 3 filas de QoS seria suficiente para atendimento às necessidades da maioria dos serviços previamente existentes na rede, destinando-se a quarta fila para uso e segregação do serviço DCN. Além disso, e reforçando o uso de um modelo com menor número de filas, deve-se considerar que equipamentos de *backbone* tratam várias dezenas de gigabytes por segundo durante o processo conhecido como PHB. Assim, o aumento do número de filas e classes aumenta proporcionalmente a complexidade operacional e o processamento nos equipamentos.

Nesta proposta foram usadas 3 filas para distinguir e segregar 3 tipos de serviço bem díspares, além do serviço DCN na quarta e exclusiva fila. Dessa forma:

1. A primeira classe destina-se ao tratamento de fluxos de tráfegos interativos e de tempo real como voz, vídeo, TV interativa, videoconferência, entre outros. Fica claro que para este tipo de tráfego o tratamento dado aos pacotes deve ser o de menor tempo de espera dentro do equipamento, sendo, por este motivo, associados a uma fila do tipo *Priority Queue (PQ),* que possui a mais alta prioridade de encaminhamento.
2. A segunda classe de fluxos merecedores de tratamento diferenciado refere-se aos tráfegos considerados de alta importância ou de missão crítica. Para estes fluxos existe uma associação a uma fila de alta prioridade que normalmente possui alguma técnica de escalonamento de pacotes ponderada que pode ser do tipo WFQ ou CBWFQ.
3. A terceira classe de fluxos corresponde aos que não são merecedores de diferenciação e normalmente não recebem qualquer tipo de marcação no campo

DSCP ou EXP (no MPLS), ficando este igual a zero. Estes dados são transportados pelo melhor esforço e sempre que há banda disponível para encaminhamento dos pacotes. Os fluxos e serviços oriundos da Internet e dados de baixa prioridade como o *Scavenger/Bulk* são exemplos de tráfegos que são tratados como melhor esforço dentro dos *backbones*.

4. E a quarta seria exclusivamente dedicada ao transporte dos fluxos de dados gerados pelo serviço DCN, podendo ser do tipo ponderada ou *priority* e será definida a partir da natureza dos dados a serem transportados.

A Figura 25 apresenta o modelo de 12 classes proposto pela RFC 4594 e resume sua distribuição em 4 filas de QoS.

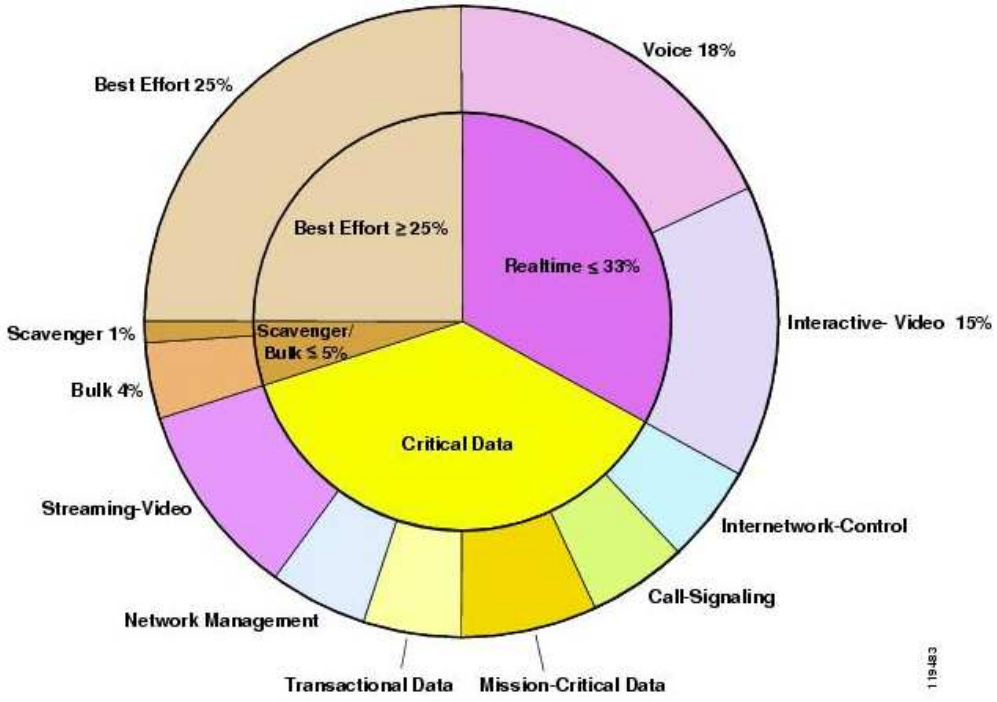

Figura 25 - Modelo de 4 filas e até 12 classes de serviço para QoS
Fonte: cisco.com [28]

Em resumo, pode-se definir que a estratégia de implementação de QoS visa a:

- Maximizar a utilização da rede;
- Maximizar o tempo de vida da rede, pois aplicações críticas terão recursos garantidos;
- Controlar rajadas, taxa de perda de pacotes e *jitter*, proporcionando suporte a aplica-

ções de tempo real;

- Garantir recursos para aplicações críticas;
- Possibilitar a dedicação de banda para aplicações;
- Gerenciar o congestionamento através da sinalização para as aplicações;
- Gerenciar a utilização de recursos por classes, segregando os diferentes serviços;
- Proteger os recursos de rede para as aplicações críticas.

7.1.1 Mapeamento do campo TOS em EXP

Como apresentado anteriormente, o campo TOS do cabeçalho IP possui oito bits de extensão enquanto o EXP possui apenas três bits. Assim, a quantidade possível de diferenciações de fluxo na camada MPLS é reduzida e limitada a 8 diferentes classes (de 000 a 111, no sistema binário). Para este estudo, apresenta-se no Quadro 5 uma proposta para mapeamento do QoS de IP para MPLS. Os roteadores de borda do MPLS (LER ou PE) seguem este mapeamento automaticamente, copiando os 3 bits mais significativos do campo TOS no EXP. Este modelo proposto segue o mapeamento padrão de DSCP para EXP apresentado na RFC 3270 [29].

Per Hop Behavior (PHB)			**DiffServ Code Point (DSCP)**		**EXP FIELD**
Default			0		**0**
Assured Forwarding		**Low Drop Probability**	**Medium Drop Probability**	**High Drop Probability**	
	Class 1	AF11	AF12	AF13	**1**
		1010	**1100**	**1110**	
	Class 2	AF21	AF22	AF23	**2**
		10010	**10100**	**10110**	
	Class 3	AF31	AF32	AF33	**3**
		11010	**11100**	**11110**	
	Class 4	AF41	AF42	AF43	**4**
		100010	**100100**	**100110**	
Expedited Forwarding		EF			**5**
		101110			

Quadro 5– Mapeamento de TOS em EXP

7.1.2 Propostas de QoS para suporte ao serviço DCN

De maneira a diferenciar e proteger os tráfegos de dados gerados pelos DCN dos serviços legados existentes na rede, foi definida uma primeira proposta de marcação dos pacotes e enfileiramento de QoS. A Figura 26 apresenta a marcação diferenciando os fluxos de dados dos LSP do serviço DCN. Nesta proposta é criada uma fila específica de QoS Diffserv para os LSP, na qual todos os seus fluxos terão a marcação do campo TOS no grupamento AF1X, onde X pode ser igual a 1, 2 ou 3, dependendo da preferência de descarte. Dessa forma, objetiva-se que o serviço DCN não interfira nos outros serviços da rede e vice versa.

Conforme apresentado, são reservadas bandas percentuais de dados para cada fila e tipo. As bandas percentuais apresentadas nas propostas de QoS são apenas proposições iniciais. A partir das medições e monitorações dos consumos dos fluxos de dados dos serviços na rede em operação faz-se necessário o ajuste para implantação em definitivo. Há o tipo de fila CB-WFQ, para as filas de tráfegos normais, não *real time*, por exemplo, e há o tipo LLQ (PQ), para os serviços de baixa latência.

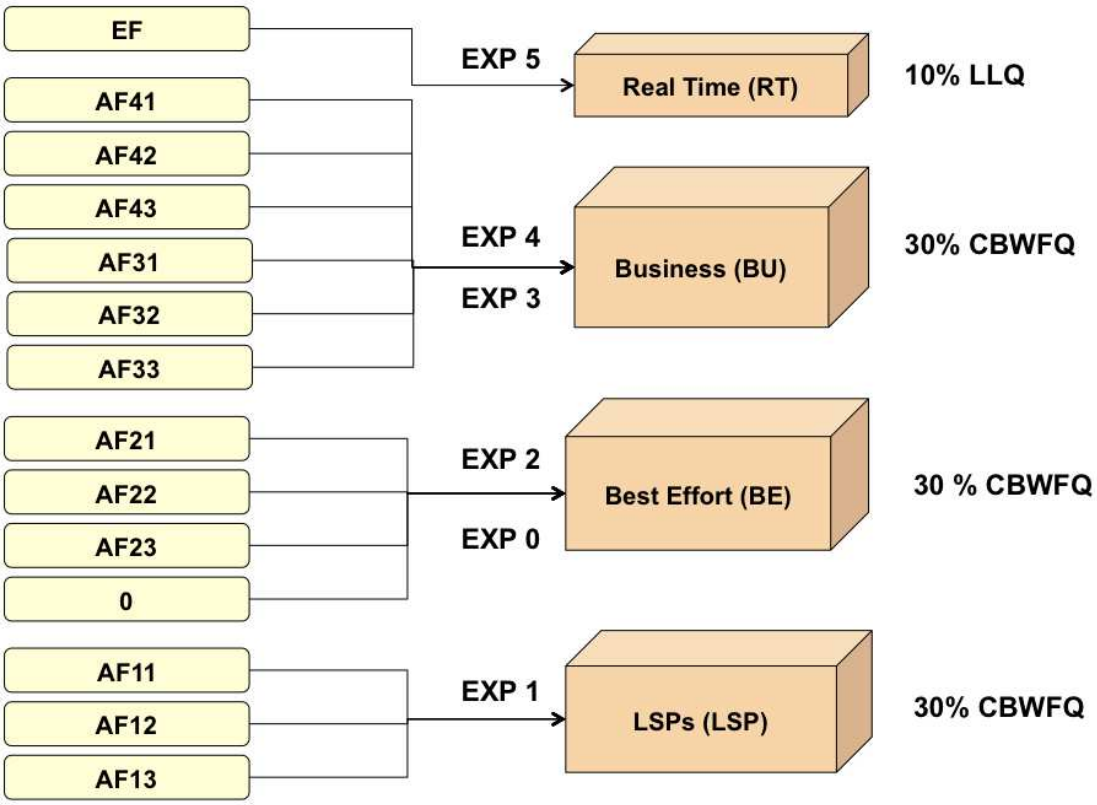

Figura 26 – Proposta 1 de QoS Diffserv para segregação do DCN.

A proposta de QoS DiffServ na camada MPLS da rede apresentada na Figura 27 foi configurada em laboratório com o objetivo de retratar a efetiva separação de todo o tráfego gerado pelos LSP da DCN em uma fila específica, tendo esta recebido a marcação do campo EXP igual a 1.

A premissa desta proposta é a de que todo o tráfego gerado pelo serviço DCN seja tratado da mesma forma e respeite o modelo de apenas 4 filas de QoS.

```
**********************************************************************************
class-map match-any BU
description Bussines
match mpls experimental topmost 3 4
class-map match-any LSP
description LSP
match mpls experimental topmost 1
class-map match-any BE
description Best-Effort
```

```
match mpls experimental topmost 0 2
class-map match-any RT
description Real-Time
match mpls experimental topmost 5
policy-map QOS_Backbone
description Policy QOS_Backbone
class RT
priority percent 10
class BU
bandwidth percent 30
random-detect dscp-based
class BE
bandwidth percent 30
random-detect dscp-based
class LSP
bandwidth percent 30
random-detect dscp-based
**********************************************************************
```

Figura 27 – QoS para atendimento ao serviço de DCN de mesma classe.

A segunda proposição apresentada para a diferenciação de tráfego dos LSP considerou que nem todos os fluxos de dados dentro do serviço DCN possuem as mesmas características e necessidades e que, por conseguinte, não devem ser tratados da mesma forma. Para esta segunda proposta, faz-se necessário que os equipamentos suportem mais de 4 filas de QoS. Uma vez sendo possível o uso de pelo menos mais uma fila de QoS, criou-se uma nova, do tipo LLQ, para segregação dos serviços de tempo real oriundos das DCN. Para este cenário inicial, esta nova fila teria 10%, podendo ser dimensionado conforme necessidade, de banda reservada e utilizaria a marcação EXP igual a 6.

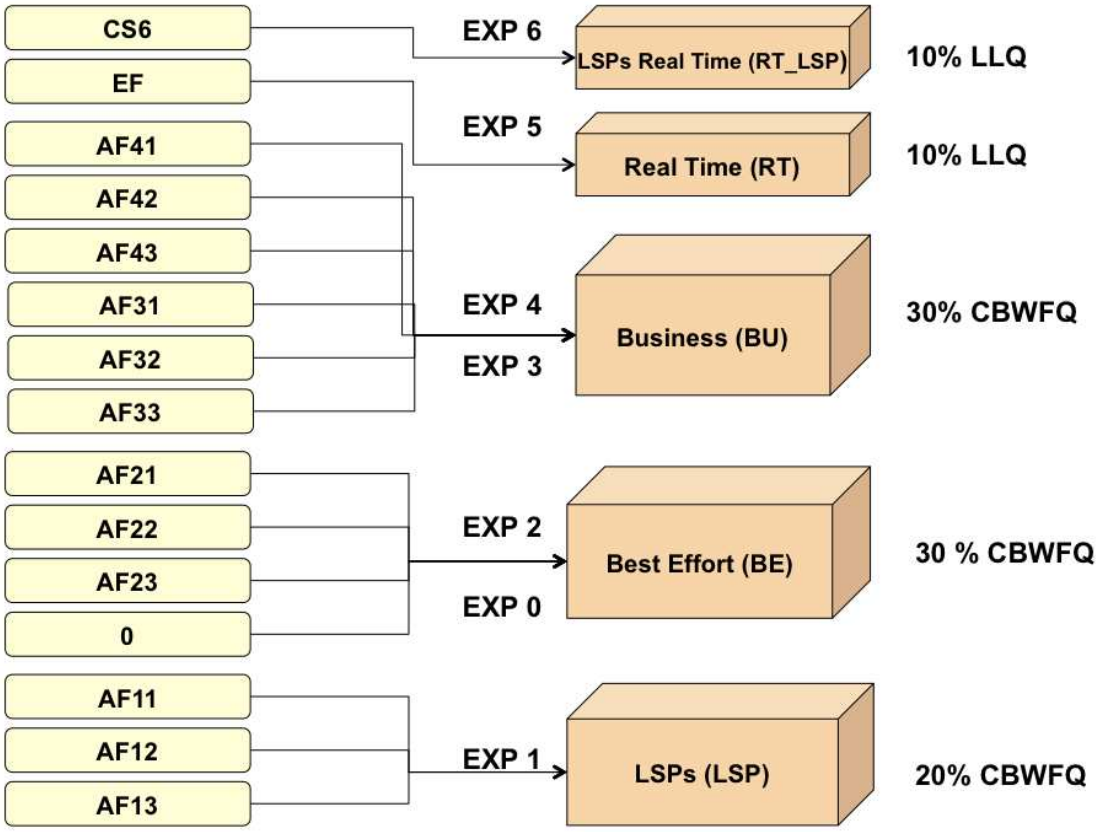

Figura 28 - Proposta 2 de QoS Diffserv para segregação do DCN.

Conforme apresentado na Figura 28, fica explicitado que haverá distinção entre os LSP para tráfego que necessita de tratamento de tempo real e aqueles para os tráfegos que não necessitam. Mesmo assim, os demais serviços da rede continuam imunes a interferências do serviço DCN.

A grande limitação deste modelo proposto é a aplicabilidade apenas a equipamentos que suportam mais de 4 filas de QoS.

A Figura 29 apresenta as configurações do laboratório comprovando o funcionamento e a aplicabilidade desta proposta.

```
**************************************************************************
class-map match-any BU
description Bussines
match mpls experimental topmost 3 4
class-map match-any LSP
description LSP
match mpls experimental topmost 1
```

```
class-map match-any BE
description Best-Effort
match mpls experimental topmost 0 2
class-map match-any RT
description Real-Time
match mpls experimental topmost 5
class-map match-any RT_LSP
description Real-Time for LSP
match mpls experimental topmost 6
policy-map QOS_Backbone
description Policy QOS_Backbone
class RT
priority percent 10
class RT_LSP
priority percent 10
class BU
bandwidth percent 30
random-detect dscp-based
class BE
bandwidth percent 30
random-detect dscp-based
class LSP
bandwidth percent 20
random-detect dscp-based
**************************************************************************
```

Figura 29 - QoS para atendimento ao serviço de DCN de diferentes classes.

7.2 PROPOSTA DE SUPORTE A DCN E ESTUDO DE CASO

A proposta a seguir de suporte a DCN será usada no estudo de caso da rede da RNP, mas, de maneira geral, seu resultado pode ser considerado como aplicável a qualquer *backbone* no qual seja desejada uma similar separação entre serviços.

Para a definição de uma proposta de suporte ao serviço DCN são assumidas algumas premissas a serem atendidas, sendo elas: o gerenciamento, a segurança operacional e da rede, a segregação entre os fluxos gerados pelos LSP da DCN e os serviços existentes, e características inerentes ao próprio serviço proposto aos usuários finais.

Um detalhe importante levado em consideração é que todo o serviço de criação dos LSP da DCN está contido no próprio domínio da RNP. Outros *backbones* e redes de instituições externas são, assim, considerados clientes, podendo usar do serviço sem interação direta com o processo de engenharia de tráfego e QoS existente na rede da RNP.

A Figura 30 apresenta o *backbone* da RNP, com sua topologia e capacidades dos links. Tal *backbone* é conhecido como rede Ipê [12] e seu detalhamento pode ser encontrado na própria página da RNP na Internet [12], como abaixo transcrito. Neste *backbone* foram previstas, e atualmente implementadas, modificações importantes de capacidade de circuitos e equipamentos para suporte a novos serviços, dentre eles o de DCN.

"O *backbone* da rede Ipê foi projetado para atender a certos requisitos técnicos, garantindo não só a largura de banda necessária ao tráfego Internet de produção como o uso de serviços e aplicações avançadas e a experimentação. A infraestrutura engloba 27 Pontos de Presença (PoPs), um em cada unidade da federação, além de ramificações para atender mais de 600 institutos de ensino e pesquisa em todo o país.

Atualmente a capacidade multigigabit da rede Ipê está disponível em 10 PoPs, com enlaces de 2,5 e 10 Gbps. Na nova geração, os enlaces de 3 e 10 Gbps chegarão a 24 PoPs.

Até o fim de 2010, a rede Ipê passará por um grande salto qualitativo, atingindo a capacidade agregada de 233,2 Gbps, um aumento de 280% em relação à capacidade agregada atual. A ampliação é resultado de acordo de cooperação com a empresa de telecomunicações Oi, que proverá à RNP infraestrutura de transmissão em fibras ópticas para uso não-comercial e participará de projetos de pesquisa & desenvolvimento de interesse comum."

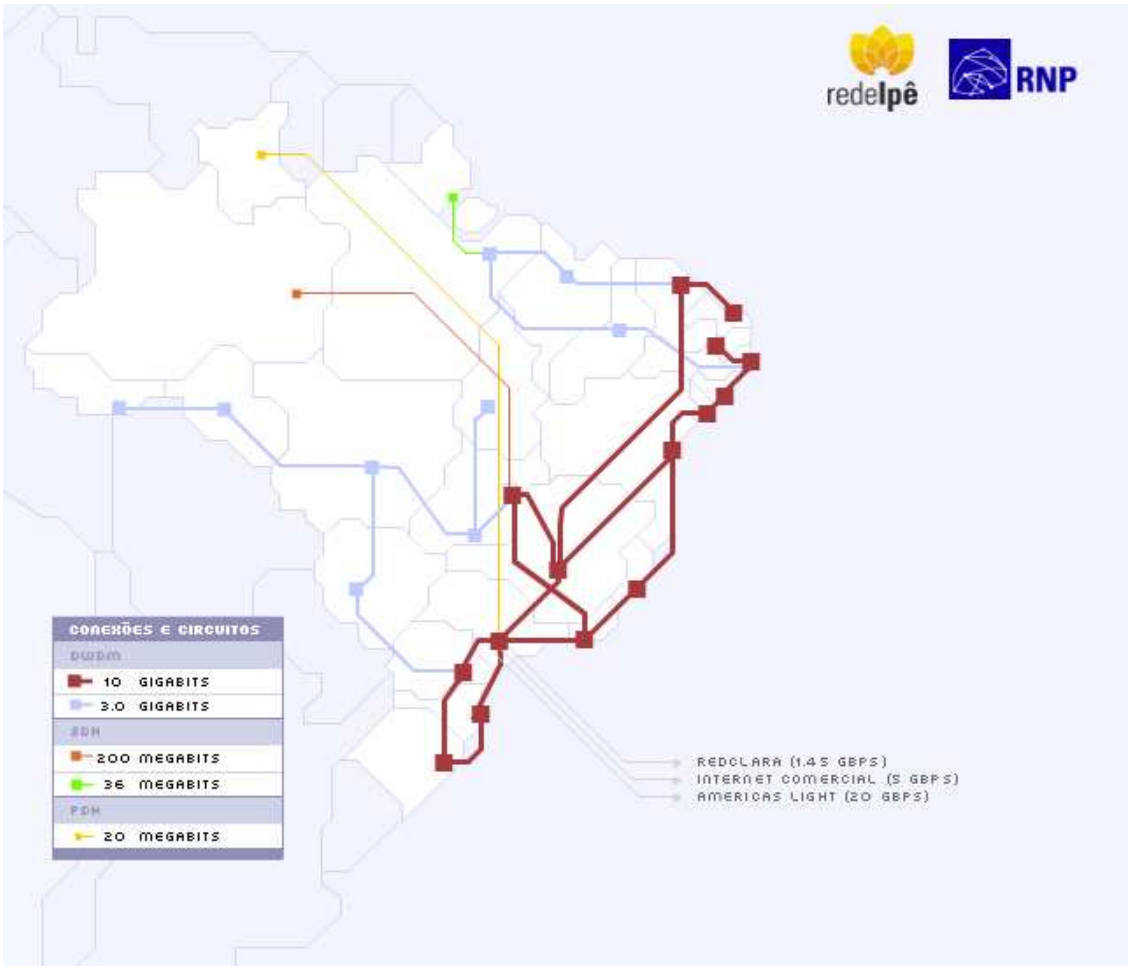

Figura 30 – Topologia do *backbone* da RNP [12].
Fonte: Site rnp.br (2011)

7.2.1 Equipamentos envolvidos

Os equipamentos de rede considerados nesta proposta de suporte a serviço DCN são roteadores do fabricante Juniper®, série MX®, que suportam todos os ensaios de laboratório anteriormente descritos. Os equipamentos envolvidos suportam os protocolos abertos e padronizados de roteamento, virtualização, engenharia de tráfego, autenticação, SNMP e QoS, e ainda possuem total interoperabilidade com os equipamentos utilizados no laboratório deste trabalho.

7.2.2 Segurança e gerenciamento da rede

Outro ponto de grande relevância está relacionado à garantia e ao controle operacional da rede uma vez que existirão elementos fazendo interface com os roteadores e interagindo diretamente com os protocolos de roteamento MPLS do *backbone*.

Uma das possíveis maneiras de garantir este controle é a de limitar os comandos que podem ou não ser executados nos elementos de rede. Desta forma, os *scripts* de configuração gerados pelos cálculos computacionais de criação de LSP serão limitados a executar apenas o permitido. Os equipamentos envolvidos possuem suporte aos protocolos *RADIUS* [11] *e TACACS+* [11] e poderiam ser utilizados para este tipo de controle de acesso.

Do ponto de vista da segurança entre os serviços, o QoS Diffserv, RSVP-TE e a virtualização de equipamentos são as alternativas mais completas para impedir a interferência gerada pela implantação de um novo serviço de DCN juntamente aos demais serviços existentes.

Para a garantia de qualquer serviço é fundamental uma gerência efetiva. Para o escopo deste trabalho, um sistema de gerenciamento que consiga ler e interpretar as MIB SNMP dos roteadores envolvidos deverá ser capaz de suportar as características mais importantes na operação dos serviços DCN dentro do domínio de rede da RNP.

7.2.3 Segregação de serviços dentro do *backbone*

Além da garantia mínima para o serviço de LSP, segregado em uma ou mais filas de QoS específicas, são necessárias a diferenciação, a garantia e a priorização dos próprios LSP. Uma das possíveis técnicas consiste no uso do protocolo RSVP-TE com uma limitação percentual da banda, por interface dos roteadores, para a criação destes LSP. Como proposta no presente estudo, está sendo alocada 30% da banda, da capacidade nominal de cada interface, para uso no serviço DCN. Dessa forma, se para uma interface é limitada a criação de LSP até 30% da banda, apenas poderão ser criados LSP até este limite. Uma vez estando a ocupação em 30%, o próximo LSP não conseguirá ser sinalizado pelo protocolo, liberando, por conseguinte, o restante da banda deste circuito para outros serviços.

A priorização de LSP também deverá ser definida. Esta priorização permitirá que LSP concorrentes sejam ativados ou desativados conforme seu grau de prioridade. O grau de prioridade garante que LSP de maior nível de importância sejam sinalizados e caso não exista banda disponível reservada, os LSP de menor prioridade sejam rerroteados ou mesmo removidos, até que exista banda novamente disponível para sua sinalização fim a fim.

Inicialmente os LSP podem ser divididos em três classes de prioridade, sendo estas alta, média ou baixa.

LSP de baixa prioridade podem ficar indisponíveis por alguns segundos, enquanto os de média prioridade correspondem aos que podem ser rerroteados desde que um novo LSP seja estabelecido e, então, o antigo poderá ser removido. Na prática, este processo tem impacto reduzido na qualidade das comunicações e pode introduzir algumas perdas de pacote no momento da comutação de LSP.

Os LSP de alta prioridade, por sua vez, nunca serão removidos ou rerroteados.

Por definição, nesta proposta, cada LSP será rerroteado através do processo de estabelecimento de um novo LSP, ou seja, comutação para o novo e remoção do antigo. Frisa-se, contudo, que, eventualmente, será necessário provocar algumas desconexões para que o objetivo ótimo seja alcançado.

Tomando-se como base apenas LSP de média prioridade, este método não é considerado totalmente satisfatório. Se, por um lado, são permitidas interrupções de LSP, quando necessário, por outro, o número de rerroteamentos pode ser igual ou superior ao número de LSP existentes. Este número pode ser elevado, o que implica complexidade no gerenciamento da rede, podendo provocar impacto com maiores interrupções de serviço.

Em particular, os LSP de média prioridade não podem ser interrompidos sem que os novos estejam estabelecidos e o número máximo de possíveis reroteamentos deve ser controlado. Dadas estas restrições, o objetivo é alcançar o melhor esquema de roteamento.

Os parâmetros de QoS levados em consideração serão largura de banda, latência, *jitter* e taxa de descarte de pacotes. Para garantir um melhor QoS, é interessante o uso de caminhos curtos de forma a reduzir a possibilidade de aumento da latência e da taxa de descarte de pacotes e, consequentemente, o *jitter*. Além disso, o administrador da rede deverá, também, manter um controle da banda de rede disponível, haja vista os novos fluxos que entrarão na rede e as constantes variações de tráfego.

Tais técnicas de priorização são possíveis com o uso RSVP-TE e permitem um grau maior de controle por parte da equipe de administração do *backbone*.

7.3 CARACTERÍSTICAS DO SERVIÇO

Uma vez apresentadas as técnicas de engenharia de tráfego e QoS possíveis e simuladas em laboratório, o próximo passo é o de definir como estas podem ser integradas e oferecidas com um serviço funcional aos usuários finais.

Basicamente são alguns passos a serem seguidos, iniciando com a solicitação, passando pelo agendamento do circuito DCN e a preparação da infraestrutura de rede para suportar e garantir a operacionalidade do serviço, até a entrega final ao usuário.

Primeiramente, o serviço deverá possuir uma interface amigável para a solicitação do usuário. Esta deverá conter todas as possibilidades e combinações do serviço, que, ao serem solicitadas, transformar-se-ão em ações que irão aprovisionar o circuito DCN na rede. Nesta interface do usuário deverá ser possível a identificação dos mesmos, carregando automaticamente todas suas permissões para determinado serviço.

O AAA, apresentado no *framework* DRAGON, seria um dos possíveis mecanismos usados para garantir a identificação do usuário, o nível de autorização e o histórico do uso para futuras auditorias e bilhetagem.

Antes da apresentação de propostas de alguns possíveis cenários e tipos de DCN permitidos na rede, faz-se necessário definir o quanto de recurso de rede estará disponível para este serviço e como estes serão usados de maneira a não afetar os demais serviços existentes. Para isso, deve-se ter uma definição inicial quanto à banda que será reservada, à forma de alocação, à priorização e aos protocolos envolvidos. Neste cenário inicial, poderão ser

definidos alguns dos requisitos e características já apresentadas nos testes de laboratório desde estudo. Para este cenário foram consideras as seguintes premissas:

- Escolha de um *framework* DCN como sendo o plano de controle, autenticação e aprovisionamento do serviço na rede;
- RSVP-TE como sendo o protocolo de engenharia de tráfego no *backbone* MPLS;
- A proposta 2 de segregação de QoS, na qual criam-se 2 filas para o DCN, do tipo DiffServ, sendo uma para serviços de baixa latência e *jitter* e outra para os demais serviços advindos dos LSP da DCN, com total de banda dedicada a estas filas de 30% da banda total nominal de cada enlace;
- Reserva inicial de 30% da banda nominal de cada enlace via protocolo RSVP-TE para a alocação dos serviços DCN;
- Definição de três níveis de priorização dos LSP (*preemption*) dentro do serviço DCN, sendo eles de prioridade 1, 3 e 5, respectivamente, da maior para a menor prioridade de sinalização.
- Os LSP podem ser dos tipos camada 2 (L2) e camada 3 (L3);

Partindo-se destas premissas, podem ser propostas algumas modalidades de suporte ao serviço DCN. Dependendo das especificidades das políticas internas de prestação de serviço, o administrador da rede poderá criar variações das modalidades apresentadas para que fique aderente à expectativa do oferecimento do serviço DCN aos usuários finais.

A seguir são propostas três modalidades do serviço, cada uma com suas características de priorização, disponibilidade, QoS, taxa, e camada de transporte. Estas modalidades podem ser combinadas e, para um mesmo cliente, podem ser oferecidas quantas forem necessárias para atendimento a suas necessidades, de acordo com as aplicações a serem transportadas. O Quadro 6 apresenta o resumo das propostas de modalidades de suporte a serviços DCN que serão apresentadas. Nele são apresentados os 3 tipos de modalidades de suporte ao serviço DCN, sendo que os LSP gerados podem ser do tipo camada 2 ou 3 (L2 ou L3), influenciando na forma de QoS. Além disso, cada modalidade possui diferentes características quanto aos mecanismos de proteção de LSP.

	CARACTERÍSTICA DO SUPORTE AO SERVIÇO DCN								
MODALIDADE DO SERVIÇO	LSP L2	LSP L3	QoS L3	QoS EXP	LSP Standby Ativo	LSP Standby Passivo	*Fast Reroute*	Prioridade do LSP	Exemplos de Aplicabilidade
TIPO 1	X			6	X		X	1	Emulação de circuitos transparentes ethernet, transporte de dados não TCP/IP de alta prioridade e baixo descarte, voz e vídeo
		X	X	1 e/ou 6	X		X	1	Transporte de diversos serviços IP de alta prioridade como voz, vídeo e automação industrial, simultaneamente
TIPO 2	X			1		X		3	Emulação de circuitos transparentes com media probabilidade de descarte, transporte de dados não TCP/IP não interativos ou de tempo real
		X	X	0 e/ou 1		X		3	Transporte de diversos serviços IP de média prioridade como aplicações de missão crítica não interativas ou de tempo real
TIPO 3	X			1				5	Emulação de circuitos transparentes com alta probabilidade de descarte, transporte de dados não TCP/IP de baixa prioridade
		X	X	0 e/ou 1				5	Transporte de diversos serviços IP de baixa prioridade que podem ser descartados preferencialmente

Quadro 6 - Modalidades de suporte ao serviço DCN e suas características.

7.3.1 Modalidade de Serviço TIPO 1

No TIPO 1 do serviço são criados LSP de mais alta prioridade, com valor de *preemption* igual a 1.

Sabe-se que o valor 0 (zero) de *preemption* ou prioridade é o de mais alta ordem, porém recomenda-se que este valor seja deixado disponível para a necessidade de criação de LSP estratégicos de manutenção operacional em momentos de recuperação de falhas, uma vez que este LSP assumirá a maior prioridade dentro do *backbone*.

Esta modalidade define LSP que assumem a mais alta hierarquia de sinalização dentro da rede. Os LSP criados para esta modalidade nunca serão rerroteados por necessidade de estabelecimento de outros LSP do serviço DCN. O uso de técnicas de recuperação rápida, como o *fast reroute*, podem ser empregadas e sempre haverá um LSP de contingência para rápida comutação em caso de falha de algum segmento ou nó de rede por onde o caminho principal deste LSP passar. O consumo de recurso de rede (banda) reservada pelo protocolo RSVP-TE será sempre o dobro da banda solicitada pelo usuário do serviço, uma vez que existirá um LSP primário e outro de contingência, de mesma banda, para rápida recuperação.

Nesta modalidade poderão ser definidos LSP de camada 2, basicamente Ethernet modo transparente com priorização única de QoS, ou camada 3, com mais de um nível de priorização, ou classe, no QoS.

Recomenda-se a prestação do TIPO 1 de serviço para atendimento a necessidades de transporte de informações de missão crítica, que necessitam de alto grau de disponibilidade e confiabilidade, aliados a um baixíssimo tempo de comutação dentro dos nós da rede.

Como exemplo de serviço que poderia ser atendido por tal modalidade pode ser citado o transporte de voz, videoconferência e automação industrial, que se caracterizam como aplicações que demandam menor tempo de comutação dentro dos nós de rede, e recuperação de falha na ordem de poucas dezenas de milissegundos.

7.3.2 Modalidade de Serviço TIPO 2

No TIPO 2 do serviço são criados LSP de média prioridade, com valor de *preemption* igual a 3.

Esta modalidade define LSP que assumem médio nível de priorização de sinalização dentro da rede. Os LSP criados para esta modalidade serão apenas rerroteados por necessidade de estabelecimento de outros LSP da modalidade TIPO 1 do serviço DCN. Haverá sempre a sinalização de um segundo LSP, no modo *standby*, que permitirá a comutação do serviço em caso de falha ou preempção de outro LSP de mais alta prioridade. Dessa maneira, o consumo de banda desta modalidade será de apenas uma vez a banda solicitada pelo usuário e o recurso de comutação rápida não estará disponível.

Nesta modalidade poderão também ser definidos LSP de camada 2, *Ethernet* modo transparente com priorização única de QoS, ou camada 3, com mais de um nível de priorização, ou classe, no QoS.

Recomenda-se a prestação do TIPO 2 para o transporte de informações de missão crítica e que necessitam de qualidade no transporte dos dados. A recuperação de uma falha de rede na ordem de alguns segundos é tolerável e ainda assim mantém o alto grau de confiabilidade aliado a uma garantia de banda nos enlaces da rede.

7.3.3 Modalidade de Serviço TIPO 3

No TIPO 3 do serviço são criados LSP de baixa prioridade, com valor de *preemption* igual a 5.

Esta modalidade define LSP que assumem baixo nível de priorização de sinalização dentro da rede. Os LSP criados para esta modalidade serão sempre a primeira escolha e rerroteados por necessidade de estabelecimento de outros LSP das modalidades TIPO 1 e 2 do serviço DCN. Não haverá a sinalização de um segundo LSP para contingenciamento.

Nesta modalidade poderão também ser definidos LSP de camada 2, *Ethernet* modo transparente com priorização única de QoS, ou camada 3, com mais de um nível de priorização, ou classe, no QoS. Exclui-se desta modalidade a opção de uso da fila do tipo PQ.

Recomenda-se a prestação do TIPO 3 para o transporte de informações de baixo nível de priorização e que não exigem muito da qualidade no transporte dos dados. A recuperação de uma falha de rede na ordem de alguns segundos é tolerável e mantém o grau de confiabilidade existente na rede. Em outras palavras, o uso desta modalidade é recomendado para serviços que geram, normalmente, grandes volumes de transferências de dados sem a necessidade de garantia de transporte e para os quais a perda de pacotes é tolerada, como é o caso de aplicações semelhantes ao FTP.

8. CONCLUSÃO E RECOMENDAÇÕES

A DCN permite a criação dinâmica de circuitos ponto-a-ponto, podendo prover uma conexão dedicada, com largura de banda específica, entre uma origem e um destino. Tal característica, aliada ao fato de que os circuitos podem ser estabelecidos por um período limitado de tempo, caracterizam-se como uma das principais vantagens da DCN, uma vez que permitem o transporte de grandes volumes de dados, sem desperdiçar recursos de rede. Ou seja, o recurso permanece alocado somente durante o período de uso.

Face às características inerentes às redes DCN, estas podem ser empregadas de diversas formas e com diferentes objetivos. Dentre os exemplos de aplicabilidade podem ser citados: o oferecimento, por provedores, de serviços de Internet comercial com alto desempenho; o uso por pesquisadores para acesso remoto, a altas taxas, a servidores de processamento e armazenamento, de forma mais eficaz; e a possibilidade de uso, em um mesmo meio, de tecnologias de transporte alternativas, diferentes do tradicional TCP/IP, permitindo total utilização da largura de banda oferecida.

A versatilidade e o conjunto de facilidades oferecidas pelo emprego das redes DCN motivou o estudo desenvolvido no presente trabalho, que se iniciou a partir da demanda de criação de mecanismos para suportar o serviço de DCN, usando os *frameworks* DRAGON como base para o plano de controle de alocação de circuitos.

Foram apresentadas técnicas mais usuais de engenharia de tráfego e QoS, definidas a partir de necessidades do uso de aplicações que demandam aumento de confiabilidade, eficiência e qualidade na rede. Levou-se em consideração também a proteção, a segurança e a garantia dos serviços ora existentes, haja vista a característica do serviço e a alocação contínua de circuitos, de forma automatizada, por intermédio de demandas advindas diretamente dos usuários finais. Tais demandas podem possuir requisitos como agendamento, duração, banda, latência e política de QoS e podem implementar modificações diretamente na estrutura do *backbone* da rede e no encaminhamento dos pacotes.

Foi considerada, no caso da RNP, a existência de equipamentos de rede que possuem limitações quanto à quantidade máxima de filas de QoS possíveis. De certa forma, essa limitação impediu uma separação ideal entre os fluxos de dados dos serviços existentes daqueles gerados pelo DCN. Mesmo com essas limitações foi possível criar e definir níveis de garantia e priorização que permitiram, dentro de certas possibilidades, a existência conjunta de diferentes serviços.

Outro aspecto relevante na definição das técnicas estudadas foi a facilidade de implantação e principalmente de operação, garantindo aos seus administradores controle total dos recursos.

A partir dos resultados obtidos nos ensaios de laboratório, foi possível concluir que todas as propostas apresentadas e emuladas, em equipamentos do fabricante Cisco® possuem total empregabilidade e aplicabilidade em redes reais. As configurações apresentadas no ANEXO e ao longo deste trabalho reproduzem as linhas de comando usadas na execução do laboratório, e são fidedignas às necessárias para implementação em equipamentos reais do citado fabricante, e seu emprego em um caso prático exigiria apenas a adaptação dos planos de endereçamento IP e bandas reservadas pelos protocolos de engenharia de tráfego e QoS.

O estudo levou em consideração também o uso de QoS associado a engenharia de tráfego que, além de proporcionar as conhecidas garantias e requisitos para o funcionamento das aplicações IP, tornou possível o acondicionamento dos LSP da DCN dentro do *backbone* e a segregação completa dos diferentes serviços. Além disso, comprovou-se que, com o emprego do protocolo RSVP-TE, é possível garantir uma melhor acomodação do tráfego, escolha de caminhos baseados em restrições, limitação de banda para o serviço, qualidade de serviço, além de possibilitar uma rápida convergência em caso de falha.

Em suma, foi possível constatar que o emprego de QoS e TE, simultaneamente, propicia resultados satisfatórios, assegurando a maximização e o melhor uso da rede, possibilitando garantia de tráfego para aplicações de missão crítica, controle para as de menor prioridade e gerência de congestionamento, de tal modo a assegurar o uso dos recursos disponíveis de forma otimizada independentemente do serviço transportado.

Foram apresentadas três propostas de suporte ao serviço DCN, com diferentes níveis de qualidade, priorização e disponibilidade. Estas propostas foram inicialmente apresentadas para aplicação às necessidades da RNP, mas podem ser facilmente generalizadas. Nestas propostas foram apresentadas características de suporte baseadas em QoS e TE, que garantem, de forma geral, que os diferentes tipos de serviço providos pelos circuitos dinamicamente

gerados sejam segregados dos tráfegos existentes nas redes. A combinação das modalidades de suporte ao serviço podem gerar uma gama de serviços, que certamente atenderá às necessidades dos usuários da RNP.

O presente trabalho teve como foco a análise e o suporte ao serviço de criação dos LSP da DCN apenas no intradomínio. Assim, sugere-se que a análise seja ampliada para um ambiente multidomínios, envolvendo redes de diversos provedores e domínios administrativos distintos. Tal análise é considerada importante, pois o emprego em ambientes multidomínios permitirá que serviços baseados em DCN sejam aprovisionados em redes de dimensões continentais.

É de bom alvitre destacar que, embora o ambiente simulado usado tenha sido extremamente útil para validar todas as proposições e atestar seu correto funcionamento, seria interessante realizar testes de integração total dos protocolos RSVP-TE e OSPF-TE do DRAGON com os dos roteadores reais. Novos trabalhos poderiam ser desenvolvidos, portanto, tendo como foco o estudo de novos *deamons* destes protocolos no sistema operacional hospedeiro compatíveis com os implementados pelos fabricantes de equipamentos de rede.

Outro aspecto importante é o gerenciamento do serviço. Estudos posteriores a este trabalho podem avaliar ou desenvolver ferramentas que forneçam a visão do serviço fim a fim para suporte à operação, à configuração, à bilhetagem e às gerências de desempenho e de falha, considerando ainda as características multidomínios do serviço. Mais ainda do que a simples monitoração da rede, o desenvolvimento de um sistema ou algoritmo que seja capaz de analisar e tomar decisões de TE baseadas nos resultados das medições em tempo real dos parâmetros importantes da saúde da rede, como ocupação dos enlaces, latência e erros, por exemplo. Tal sistema aumentaria ainda mais o uso e a distribuição de tráfego dentro da rede, garantindo uma otimização que análises feitas por administradores de rede não conseguem alcançar. Este sistema ainda poderia ser capaz de realizar os cálculos computacionais necessários para a definição da ordem de criação de LSP baseados em suas prioridades e com completa interação com os subsistemas do DRAGON e AUTOBAHN e, por conseguinte, com os elementos de rede.

Finalmente, visando a alavancar o serviço, um estudo considerado extremamente importante concerne à definição de um sistema com interface amigável (baseada em WEB) para a solicitação do serviço pelos usuários. Este sistema asseguraria ao usuário a possibilidade de solicitar e disponibilizaria informações completas do serviço e de seu

funcionamento, além de garantir o controle e a segurança de quem acessa, usa e altera suas características.

9. REFERÊNCIAS

[1] RFC3031, ROSEN, E., VISWANATHAN, A., and R. CALLON, "*Multiprotocol Label Switching Architecture*", IETF.ORG, Janeiro de 2001

[2] SURUAGY, "MonCircuitos - Monitoração de Circuitos e Engenharia de Tráfego", http://wiki.rnp.br/display/futura/MonCircuitos, Agosto de 2010

[3] YANG, LEHMAN, "*Policy-Based Resource Management and Service Provisioning in GMPLS Networks", INFOCOM 2006 - 25th IEEE International Conference on Computer Communication,* Abril de 2006.

[4] RFC3945, MANNIE, E., "*Generalized Multiprotocol Label Switching (GMPLS) Architecture*", IETF.ORG, Outubro de 2004.

[5] RFC3630, KATZ, D., KOMPELLA, K., and D. YEUNG, "*Traffic Engineering (TE) Extensions to OSPF Version 2*", IETF.ORG, Setembro de 2003.

[6] RFC4203, KOMPELLA, K. Ed. and Y. REKHTER, Ed., "*OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*", IETF.ORG, Outubro de 2005.

[7] RFC 4736, JP. VASSEUR, Y. IKEJIRI, R. ZHANG, "*Reoptimization of Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Loosely Routed Label Switched Path (LSP)*", IETF.ORG, Novembro de 2006.

[8] RFC 3209, D. AWDUCHE, L. BERGER, T. Li, V. SRINIVASAN and G. Swallow "*RSVP-TE: Extensions to RSVP for LSP Tunnels*", IETF.ORG, Dezembro de 2001.

[9] DASGUPTA, S., de OLIVEIRA, J.C.; VASSEUR, J.-P., "*Path-Computation-Element-Based Architecture for Interdomain MPLS/GMPLS Traffic Engineering: Overview and Performance*", IEEE Network pages 38-45, Agosto de 2007.

[10] "*Frequently Asked Questions about Internet2*", Internet2.edu, Disponível em:< http://www.internet2.edu/resources/i2faq.pdf>, Acesso em: 27/10/2010.

[11] "*Authentication Protocols - TACACS+ and RADIUS Comparison*", Cisco.com, Disponível em: <http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml>, Acesso em: 23/04/2011.

[12] "Mapa do Backbone da rede Ipê", RNP.BR, Disponível em: < http://www.rnp.br/backbone/>, Acesso em: 30/04/2011.

[13] "Rede GiGA", giga.org.br, Disponível em: <http://www.giga.org.br/home>, Acessado em 12/01/2011.

[14] "Linux Ubuntu Versão 9", Ubunto-br.org, Download Disponível em: http://www.ubuntu-br.org/download-avancado/, Acessado em 12/07/2009.

[15] "*MX SERIES 3D UNIVERSAL EDGE ROUTERS*", Juniper.net, Disponível em:< http://www.juniper.net/us/en/local/pdf/datasheets/1000208-en.pdf>, Acesso em: 21/02/2011.

[16] MARQUES, Ricardo Rodrigues, "Análise das Tecnologias MPLS e GMPLS e suas Aplicações em Redes de Comunicação", Universidade de Brasília UNB, Distrito Federal, 2004.

[17] SITOLINO C., ROCHOL, J., "Voz sobre IP (VoIP): Um estudo experimental.", Universidade Federal do Rio Grande do Sul – UFRGS, PortoAlegre, 2002.

[18] KIM Y., "*Discrete Event Simulation of the DiffServ-over-MPLS with NIST GMPLS Lightwave Agile Switching Simulator (GLASS)" National Institute of Standards and Technology (NIST)*, Korea, 2002.

[19] MOHAMMAD Mirza, GOLAM Rashed, MAMUN Kabir , "*A Comparative Study of Different Queuing Techniques in Voip, Video Conferencing And File Transfer*" Department of ETE, Daffodil International University, 2010.

[20] KUROSE and Keith ROSS, "*Scheduling and Policing Mechanisms*", Book *Multemedia Networking*, Capítulo 7, 2000.

[21] DRAGON, "*Dynamic Resource Allocation via GMPLS Optical Networks*", Disponível em: http://dragon.maxgigapop.net., Acessado em: 23/10/2010.

[22] Jacek LUKASIK, Ophelia NEOFYTOU, Afrodite SEVASTI, Stella-Maria THOMAS, Sue TYLEY, "AUTOBAHN - *Automated Bandwidth Allocation across Heterogeneous Networks*", Agosto de 2008.

[23] SANTANA, Sílvio Fernando, "Proposta de referência para projetos de qualidade de serviço (QoS) em redes corporativas", Universidade Salvador - UNIFACS, Maio de 2006.

[24] "*Virtual Label Switching Router Implementation Guide"*, Disponível em http://dragon.east.isi.edu, Acessado em: 23/06/2011.

[25] "GNS3 - *Graphical Network Simulator",* versão 0.7.4, *Download* disponível em http://www.gns3.net/download, Acessado em 12/08/2010.

[26] RFC 4594, J. Babiarz, K. Chan, "*Configuration Guidelines for DiffServ Service Classes*", IETF.ORG, Agosto de 2006.

[27] "*QoS Design Strategy"*, Cisco.com, Disponível em: "http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/qosmrn.html", Acessado em 11 de Junho de 2011.

[28]"*Quality of Service Design Overview"*, Cisco.com, Disponível em: "http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoSIntro.html", Acessado em 12 de Junho de 2011.

[29] RFC 3270, F. Le Faucheur, L. Wu, B. Davie, "*Multi-Protocol Label Switching (MPLS) Support of Differentiated Services*", IETF.ORG, Maio de 2002.

[30]"*Default Route Preference Values"*, Juniper.net, Disponível em: "http://www.juniper.net/techpubs/software/junos/junos94/swconfig-routing/default-route-preference-values.html", Acessado em 18/07/2011.

[31] "Qualidade de rede e serviços inovadores para a comunidade científica brasileira", RNP.br, Disponível em: "http://www.rnp.br/rnp/" , Acessado em 19/07/2011.

[32] "*Hybrid Optical and Packet Infrastructure Project*", Internet2.edu, Disponível em: "www.internet2.edu/pubs/HOPIInfosheet.pdf", Acessado em 11/08/2011.

ANEXOS

Anexo A: Configuração básica inicial do roteador R2

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
ip source-route
!
!
!
!
ip cef
!
```

```
!
multilink bundle-name authenticated
mpls traffic-eng tunnels
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.10.2 255.255.255.255
!
interface FastEthernet0/0
 description R2 to f0/1 R1
 ip address 10.1.1.6 255.255.255.252
 speed auto
 duplex auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 100000 100000
!
interface FastEthernet0/1
 no ip address
 shutdown
 speed auto
 duplex auto
!
```

```
interface FastEthernet1/0
 description R3 to f1/1 R4
 ip address 10.1.1.9 255.255.255.252
 speed auto
 duplex auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 100000 100000
!
interface FastEthernet1/1
 no ip address
 shutdown
 speed auto
 duplex auto
!
router ospf 1
 router-id 10.10.10.2
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 network 0.0.0.0 255.255.255.255 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
ip classless
!
!
no ip http server
no ip http secure-server
!
!
```

```
!
!
control-plane
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
end
```

Anexo B: Configuração básica inicial do roteador R3

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
```

```
ip source-route
!
!
!
!
ip cef
!
!
multilink bundle-name authenticated
mpls traffic-eng tunnels
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.10.3 255.255.255.255
!
interface FastEthernet0/0
 description R3 to f0/0 R1
 ip address 10.1.1.2 255.255.255.252
 speed auto
 duplex auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 100000 100000
```

```
!
interface FastEthernet0/1
 description R3 to f1/0 R4
 ip address 10.1.1.13 255.255.255.252
 speed auto
 duplex auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 100000 100000
!
interface FastEthernet1/0
 description R3 to f1/0 R5
 ip address 10.1.1.17 255.255.255.252
 speed auto
 duplex auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 100000 100000
!
interface FastEthernet1/1
 no ip address
 shutdown
 speed auto
 duplex auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 speed auto
 duplex auto
!
```

```
interface FastEthernet2/1
 no ip address
 shutdown
 speed auto
 duplex auto
!
router ospf 1
 router-id 10.10.10.3
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 network 0.0.0.0 255.255.255.255 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
ip classless
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
line con 0
 stopbits 1
line aux 0
line vty 0 4
```

```
!
end
```

Anexo C: Configuração básica inicial do roteador R4

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE4
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
ip source-route
!
!
!
!
ip cef
!
!
multilink bundle-name authenticated
mpls traffic-eng tunnels
!
!
```

```
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.10.4 255.255.255.255
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 description R4 to g0/0 R5
 ip address 10.1.1.25 255.255.255.252
 media-type gbic
 speed 1000
 duplex full
 negotiation auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 100000 100000
!
interface FastEthernet1/0
 description R4 to f0/1 R3
 ip address 10.1.1.14 255.255.255.252
```

```
 speed auto
 duplex auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 100000 100000
!
interface FastEthernet1/1
 description R4 to f1/0 R2
 ip address 10.1.1.10 255.255.255.252
 speed auto
 duplex auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 100000 100000
!
interface FastEthernet2/0
 description R4 to f0/1 R7
 ip address 10.1.1.21 255.255.255.252
 speed auto
 duplex auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 100000
!
interface FastEthernet2/1
 no ip address
 shutdown
 speed auto
 duplex auto
!
router ospf 1
 router-id 10.10.10.4
 log-adjacency-changes
```

```
 auto-cost reference-bandwidth 1000
 network 0.0.0.0 255.255.255.255 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
ip classless
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
end
```

Anexo D: Configuração básica inicial do roteador R5

```
version 12.2
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE5
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
ip source-route
!
!
!
!
ip cef
!
!
multilink bundle-name authenticated
mpls traffic-eng tunnels
!
!
!
!
!
!
!
!
```

```
!
!
interface Loopback0
 ip address 10.10.10.5 255.255.255.255
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 description R5 to g0/0 R4
 ip address 10.1.1.26 255.255.255.252
 media-type gbic
 speed 1000
 duplex full
 negotiation auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 100000 100000
!
interface FastEthernet1/0
 description R5 to f1/0 R3
 ip address 10.1.1.18 255.255.255.252
 speed auto
 duplex auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 100000 100000
!
interface FastEthernet1/1
```

```
 description R5 to f0/0 R6
 ip address 10.1.1.29 255.255.255.252
 speed auto
 duplex auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 100000 100000
!
interface FastEthernet2/0
 no ip address
 shutdown
 speed auto
 duplex auto
!
interface FastEthernet2/1
 no ip address
 shutdown
 speed auto
 duplex auto
!
router ospf 1
 router-id 10.10.10.5
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 network 0.0.0.0 255.255.255.255 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
ip classless
!
!
```

```
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
line con 0
 stopbits 1
line aux 0
line vty 0 4
!
end
```

Anexo E: Configuração básica inicial do roteador R6

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE6
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
```

```
ip subnet-zero
ip source-route
!
!
!
!
ip cef
!
!
multilink bundle-name authenticated
mpls traffic-eng tunnels
!
!
!
!
!
!
!
!
!
!
!
interface Tunnel2
 description TE to PE1 EXPLICIT
 bandwidth 50000
 ip unnumbered Loopback0
 tunnel destination 10.10.10.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng path-option 1 explicit name TUNNEL2_TO_PE1
```

```
 tunnel mpls traffic-eng path-option 2 dynamic
 tunnel mpls traffic-eng record-route
!
interface Loopback0
 ip address 10.10.10.6 255.255.255.255
!
interface FastEthernet0/0
 description R6 to f1/1 R5
 ip address 10.1.1.30 255.255.255.252
 speed auto
 duplex auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 100000 100000
!
interface FastEthernet0/1
 description R6 to f0/0 R7
 ip address 10.1.1.33 255.255.255.252
 speed auto
 duplex auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 100000 100000
!
interface FastEthernet1/0
 no ip address
 shutdown
 speed auto
 duplex auto
!
interface FastEthernet1/1
```

```
 no ip address
 shutdown
 speed auto
 duplex auto
!
router ospf 1
 router-id 10.10.10.6
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 network 0.0.0.0 255.255.255.255 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
ip classless
!
!
no ip http server
no ip http secure-server
!
ip explicit-path name TUNNEL2_TO_PE1 enable
 next-address 10.1.1.34
 next-address 10.1.1.21
 next-address 10.1.1.9
 next-address 10.1.1.5
!
!
!
!
control-plane
!
```

```
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
end
```

Anexo F: Configuração básica inicial do roteador R7

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE7
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
ip source-route
!
!
!
!
ip cef
```

```
!
!
multilink bundle-name authenticated
mpls traffic-eng tunnels
!
!
!
!
pseudowire-class LSP_L2
 encapsulation mpls
 preferred-path interface Tunnel1
!
!
!
!
!
!
!
interface Tunnel1
 description TE to PE1
 bandwidth 20000
 ip unnumbered Loopback0
 tunnel destination 10.10.10.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng path-option 1 dynamic
 tunnel mpls traffic-eng record-route
!
```

```
interface Loopback0
 ip address 10.10.10.7 255.255.255.255
!
interface FastEthernet0/0
 description R7 to f0/1 R6
 ip address 10.1.1.34 255.255.255.252
 speed auto
 duplex auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 100000 100000
!
interface FastEthernet0/1
 description R7 to f2/0 R4
 ip address 10.1.1.22 255.255.255.252
 speed auto
 duplex auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 100000 100000
!
interface FastEthernet1/0
 no ip address
 shutdown
 speed auto
 duplex auto
!
interface FastEthernet1/1
 no ip address
 speed auto
 duplex auto
 xconnect 10.10.10.1 100 pw-class LSP_L2
```

```
!
router ospf 1
 router-id 10.10.10.7
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 network 0.0.0.0 255.255.255.255 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
ip classless
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
end
```