UNIVERSIDADE ESTADUAL DO MARANHÃO
CENTRO DE CIÊNCIAS TECNOLÓGICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE
COMPUTAÇÃO E SISTEMAS

FILIPE HILUY LIMA

ANÁLISE DE REDE CORPORATIVA COM INSERÇÃO DE TRÁFEGO IPTV

São Luís
2015

FILIPE HILUY LIMA

ANÁLISE DE REDE CORPORATIVA COM INSERÇÃO DE TRÁFEGO IPTV

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia de Computação da Universidade Estadual do Maranhão, como parte dos requisitos para obtenção do título de Mestre em Engenharia de Computação na área de concentração Tecnologia da Informação.

Orientador: Prof. MSc. Henrique Mariano Costa do Amaral
Coorientador: Denílson Moreira Santos

São Luís

2015

Lima, Filipe Hiluy.
Análise de rede corporativa com inserção de tráfego IPTV / Filipe Hiluy Lima.–São Luís, 2015.

82f

Dissertação (Mestrado) – Curso de Engenharia de Computação, Universidade Estadual do Maranhão, 2015.

Orientador: Prof. Msc. Henrique Mariano Costa do Amaral

1.QoS. 2.MPLS. 3.IPTV. 4.Engenharia de tráfego. 5.MPLS-TE. I. Título

CDU: 004.7:621.39

FILIPE HILUY LIMA

ANÁLISE DE REDE CORPORATIVA COM INSERÇÃO DE TRÁFEGO IPTV

Dissertação apresentada ao Programa de Pós Graduação em Engenharia de Computação e Sistemas da Universidade Estadual do Maranhão, para obtenção do grau de Mestre em Engenharia de Computação.

Aprovada em: _____/_____/_____.

BANCA EXAMINADORA

_____

Profº MSc. Henrique Mariano Costa do Amaral (Orientador)

Universidade Estadual do Maranhão

_____

Profº Dr. Denílson Moreira Santos (Coorientador)

Universidade Federal do Maranhão

_____

Profº Dr. Rogério Moreira Lima da Silva

Universidade Estadual do Maranhão

_____

Prof° Dr. Carlos Henrique Rodrigues de Oliveira

Universidade Estadual do Maranhão

AGRADECIMENTOS

A Deus de inteligência suprema que rege e permanece em todas suas criações e criaturas.

À minha família. Em especial, aos meus pais Afonso Henrique Lima e Jacira Hiluy Lima e ao meu irmão Henrique Hiluy Lima, pelo apoio durante esse projeto e sempre.

À minha esposa, Huaina Guimarães Vieira Ribeiro, fonte de todo amor, esperança, admiração e motivação necessárias ao trabalho.

Ao meu amigo Elias por todas as orientações dadas durante todo esse tempo de vida.

Ao meu professor e orientador, Henrique Mariano, por acreditar na minha capacidade e pelos ensinamentos, acadêmicos ou não, passados durante todo o tempo do mestrado.

Ao meu coorientador, Denílson Moreira Santos, por acreditar na minha capacidade e pelos ensinamentos, acadêmicos ou não, passados durante todo o tempo do mestrado.

Ao Programa de Pós-Graduação em Engenharia da Computação e a todos os seus professores, pelo aprendizado.

Muito obrigado a todos.

RESUMO

Este trabalho apresenta estudos sobre a tecnologia IPTV iniciando pela sua motivação que acarretou seu aparecimento e sua grande e atual utilização. A fundamentação teórica da dissertação apresentará a descrição dos mecanismos, padrões e os principais protocolos utilizados para garantir uma qualidade de serviço necessária para implantação das aplicações IPTV. Dentre eles, cita-se o MPLS-TE. Foi feito um estudo de caso englobando uma rede corporativa de uma grande empresa corporativa de mineração, que simulará o coração da rede provedora entre filiais concentradoras de dados. O objetivo dessa simulação é analisar o comportamento da rede após inserção de tráfegos IPTV's com base nos requisitos de qualidade de serviço e engenharia de tráfego da rede, servindo de base para que se obtenha as conclusões acerca da possibilidade de implantações de novas aplicações utilizando essa tecnologia. A metodologia de trabalho foi validada por meio das simulações de várias instâncias para fluxos IPTV's. As simulações foram realizadas de forma sequencial para que se observasse em qual delas havia um limite nos parâmetros de qualidade medidos. A partir disso, se tornou possível visualizar o crescimento e disputa que esse novo tráfego gerou na rede corporativa, fundamentando as análises a respeito das decisões de implantação desta nova plataforma de serviço.

Palavras-chave: QoS, MPLS, IPTV, Engenharia de Tráfego, MPLS-TE.

ABSTRACT

This work presents studies on IPTV technology starting with the motivation which led to its appearance and its great and current use. The theoretical basis of the dissertation presents the description of the mechanisms, standards and key protocols used to ensure a quality of service required for deployment of IPTV applications. Among them, it cites the MPLS-TE. A case study was made encompassing a corporate network of a large corporate mining company, which will simulate the heart of the provider network between branches concentrator data. The purpose of this simulation is to analyze the network behavior after insertion IPTV's traffic based on quality of service requirements and network traffic engineering, serving as a base in order to obtain conclusions about the possibility of new applications deployments using this technology. The methodology was validated through simulations of multiple instances for IPTV's flows. The simulations were performed sequentially to be observed in which one was a limit on the measured quality parameters. From this it became possible to see the growth and dispute that this new traffic generated on the corporate network, basing the analysis regarding the implementation of decisions of this new service platform.

Keywords: QoS, MPLS, IPTV, traffic engineering, MPLS-TE.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

1 INTRODUÇÃO

Com o avanço da tecnologia e uma competição comercial cada vez mais acirrada, percebe-se que atualmente, quase a totalidade de processos das grandes corporações está totalmente dependente de uma disponibilidade maior de acesso à rede de comunicação e dados. Empresas de grande porte que possuem unidades de negócios em várias regiões do país ou até mesmo em regiões internacionais, precisam estreitar essas longas distâncias fazendo com que a única rede controladora e compartilhadora dessas informações pareçam únicas e locais.

A rede de comunicação de uma empresa corporativa se torna ferramenta fundamental para implementações de padrões, divulgação de políticas internas, treinamento de funcionários e até mesmo sistemas que controlam máquinas que operam *full-time* (o tempo todo). Com todo esse aumento exponencial de informações trafegando por toda essa rede, é imprescindível que haja um planejamento mínimo na hora de sua construção para que todas as "vias" por onde passarão essas informações, obtenham o maior rendimento possível, traduzindo-se em rapidez de resposta, balanceamento do tráfego, boa escalabilidade (aumento de serviços), menor número de colisões e maior economia financeira para a empresa.

Para que uma informação ou um dado chegue ao seu destino a partir de sua origem, é percorrido um trajeto que possui vários equipamentos de rede (cabos, fibras ópticas, *hubs, switchs*, roteadores), por isso, a melhor disposição desses equipamentos ao longo da malha (caminho) lógica, acarretará maior aproveitamento da infraestrutura desta empresa.

Apesar da existência de vários protocolos de encaminhamento de dados, a Cisco Systems[1] implementa em seus equipamentos (roteadores), um mecanismo padronizado pela IETF[2] de livre utilização chamado MPLS (*Multi Protocol Label Switching*) que possui diversas aplicações na engenharia de tráfego, que se mostra eficaz para alcançar os objetivos acima expostos.

[1] *Cisco Systems, Inc.* é uma companhia multinacional sediada em São José Califórnia, Estados Unidos da América. A atividade principal da Cisco é o oferecimento de soluções para redes e comunicações quer seja na fabricação e venda.

[2] *Internet Engineering Task Force* é uma comunidade internacional ampla e aberta (técnicos, agências, fabricantes, fornecedores, pesquisadores) preocupada com a evolução da arquitetura da Internet e seu perfeito funcionamento.

O protocolo MPLS possui uma arquitetura que proporciona a agregação de outras tecnologias de forma otimizada, pois sua utilização compreende na formação de vários componentes ou elementos ao longo da rede que propiciaram a abertura de um ambiente capaz de ser utilizado por outros protocolos, garantindo um melhor rendimento e um novo paradigma na engenharia de tráfego. Por isso foi criado o protocolo RSVP-TE (*Resource ReSerVation Protocol – Traffic Engineering*) que se utiliza de um desses elementos do MPLS para criar túneis virtuais, fundamentais na implementação da engenharia de tráfego de redes.

1.1 Justificativa

A transmissão de vídeo digital de alta qualidade se tornou muito requerida por diversas empresas e usuários comuns. Isto foi possibilitado pelo grande acesso e disponibilização de uma infraestrutura mais robusta por parte das operadoras de serviços de telecomunicações. Com essa demanda crescente, percebeu-se que dados, voz e vídeos, poderiam ser transmitidos juntos com uma versão de banda larga. Este serviço, no entanto, foi denominado conceitualmente de *triple play*.

Entende-se por IPTV (*Internet Protocol TeleVision*) a transmissão de programação contínua de Televisão, estruturada em canais da mesma forma que os serviços de Televisão aberta e à cabo, através da internet ou redes corporativas (Shihab and Cai, 2007). Consequentemente, houve um aproveitamento desta tecnologia para que fosse aplicada nas mais diversas áreas como, por exemplo: segurança, entretenimento, automação, comércio, negócios, marketing etc. Em ambientes corporativos, o serviço *triple play* ganhou mais força com este conceito de IPTV principalmente para aplicações de videoconferências e monitoramento de áreas remotas, onde é feita uma transmissão de programação contínua. Com isso, o tempo de decisões gerenciais tende a ser menor, justificando e demonstrando a importância estratégica de tal investimento.

Apesar da expansão da infraestrutura dos provedores desse serviço, há um consumo diferente da largura de banda em comparação aos serviços tradicionais como a *web* (imagens e texto), transferência de arquivos via correio eletrônico, etc. Atualmente os serviços de vídeos por demanda, chamados (*VoD*), mesmo utilizando uma resolução baixa, são responsáveis por um aumento considerável na ocupação de redes de distribuição (Uzunalioglu, 2009). No IPTV, a demanda por largura de banda de uma programação que por ventura utilize HDTV (*High Definition TeleVision*) aumenta

aproximadamente 25 vezes em relação à das aplicações multimídias atuais (Yarali and Cherry, 2005; Gill et al., 2007).

Por isso, a implementação deste serviço acarreta em um desafio maior para planejar e executar uma engenharia de tráfego de dados e outros mecanismos com o objetivo de alcançar uma qualidade de serviço satisfatória, analisando protocolos adequados para tal finalidade. A distribuição *unicast, multicast* são os principais mecanismos considerados em estudos que visam otimizar as transmissões em um sistema IPTV (Gill et al., 2007; She et al., 2009; Uzunalioglu, 2009).

1.2 Objetivos

1.2.1 Objetivo Geral

Este trabalho tem como objetivo simular a topologia lógica de rede WAN (*Wide Area Network*) de uma empresa corporativa, gerenciada por uma provedora de serviços, com a finalidade de analisar seus parâmetros de qualidade de serviço - QoS (*Quality of Service*) necessários à transmissão de aplicações IPTV (*Internet Protocol TeleVision*). Após isso, serão feitas inserções de fluxos de pacotes IPTV para uma avaliação da possibilidade de implementação por parte da empresa. Para tal, utilizaremos as ferramentas de simulação NS2 (*Network Simulator 2*), NS2 *Analyzer* e a ferramenta *Tracegraph*. Com este trabalho apresenta-se uma análise prática por meio de uma ferramenta que possibilite o tráfego seguro de informações na rede.

Além disso, será apresentada a importância do MPLS no desenvolvimento de uma engenharia de tráfego de uma rede corporativa para garantir certos níveis de serviços de forma agregada com o protocolo RSVP-TE, específico na criação de túneis virtuais em uma topologia de grandes redes corporativas.

1.2.2 Objetivos Específicos

(1) Elaborar o cenário lógico com parâmetros de QoS compatíveis com políticas da empresa, possibilitando sua implementação e análise;
(2) Apresentar as funcionalidades básicas do protocolo RSVP-TE;
(3) Apresentar conceitos e funcionalidades do protocolo IPTV e suas aplicações;

(4) Modelar e simular a topologia lógica da rede corporativa, levando em consideração os requisitos de segurança, financeiros e legais da empresa;
(5) Fazer uma demonstração da utilização da rede com a geração e inserção do tráfego IPTV;
(6) Analisar os resultados com base nas recomendações mínimas de QoS para o bom funcionamento deste novo serviço na rede.

1.3 Estrutura do texto

Esta dissertação encontra-se estruturada em 6 (seis) capítulos. Apresentou-se no capítulo 1 a introdução necessária ao restante dos capítulos que compõe o trabalho.

No capítulo 2, apresenta-se uma fundamentação teórica sobre engenharia de tráfego em redes e QoS com suas arquiteturas, bem como as diversas gerências onde ela é aplicada.

No capítulo 3, explicam-se novos conceitos e o funcionamento do protocolo IPTV e seu tráfego, serviços *tripleplay*, arquitetura da plataforma, bem como a utilização agregada dos dois para o desenvolvimento da engenharia de tráfego.

No capítulo 4, é demonstrado o estudo de caso, a metodologia utilizada, a codificação utilizada e ferramentas executoras da simulação que fazem referências a uma empresa de grande porte possuidora de uma estrutura consolidada em tecnologia da informação. Por isso, esta se torna capaz de desenvolver constantemente a engenharia de tráfego em sua rede de comunicação através da tecnologia apresentada no capítulo 2. Além disso, são apresentados os cenários construídos e os pacotes capturados após a configuração dos equipamentos necessários.

No capítulo 5, são apresentados os resultados obtidos através da simulação do ambiente e suas análises em detrimento do comportamento gerado e desempenho após as inserções do novo tráfego.

No capítulo 6, por fim, apresentam-se as considerações finais conclusivas a respeito da possibilidade de implantação ou não deste novo serviço na corporação, além disso, as sugestões de trabalhos futuros referentes a esta pesquisa também serão explanados.

2. ENGENHARIA DE TRÁFEGO E MPLS-TE

A engenharia de tráfego é a utilização de princípios tecnológicos e científicos para a medição, caracterização, modelagem e controle do tráfego com o objetivo de avaliação e otimização do desempenho das redes IP (Awduche *et al.*, 2000).

Com o crescimento e desenvolvimento de uma determinada empresa que possui uma rede de informação, como área estratégica de maior produção, cresce também a necessidade de um maior rendimento e eficácia dessa rede. Com isso, a engenharia de tráfego dessas informações que passarão na rede se torna alvo de constante planejamento, execução e otimização para alcançar resultados mais positivos e rentáveis para a empresa.

O principal objetivo da engenharia de tráfego é controlar e otimizar o fluxo de informações, uniformemente, por todos os caminhos que a rede possui, para que os recursos implantados sejam melhores aproveitados. A figura 1(a) demonstra uma situação que evidencia a não implementação da engenharia de tráfego na rede, cujos pacotes seguem por uma única alternativa de caminho pré-estabelecido. Já a situação mostrada na figura 1(b), de forma simples, há uma implementação de engenharia de tráfego, cujos pacotes possuem opções de tráfego dos pacotes. As ações de engenharia de tráfego podem ser construídas, em longo prazo, como planejamento de crescimento contínuo de uma rede, mas poderá ter ações em tempo real, como recuperação de um caminho bloqueado por um tráfego intenso gerado por um sistema online.

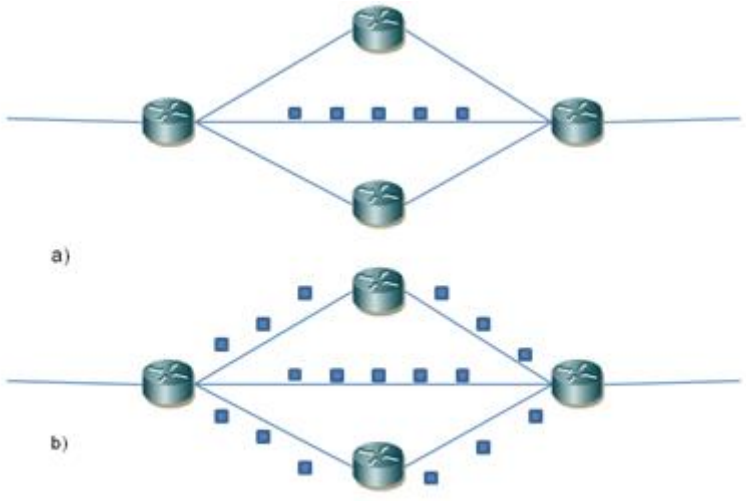

Figura 1: a) Sem engenharia de tráfego; b) Com engenharia de tráfego.

Fonte: Lima, Filipe (2015).

2.1 Visão geral da engenharia de tráfego

Há alguns anos, a percepção dos usuários acerca do tempo de resposta da rede passava a ser o principal parâmetro de desempenho considerado pelos gerentes da rede. Porém, a cada dia, é notório o aparecimento de vários outros parâmetros de análise para o provedor desse serviço como, por exemplo, o maior tempo de disponibilidade para que um determinado processo alocado, solicitado pela empresa, possa ser executado.

Desde o planejamento de implantação de redes locais ou metropolitanas, a principal meta dessas redes, principalmente para grandes empresas, é transmitir os pacotes de dados a partir de nós de ingresso (onde se originam) até os nós de egresso (onde encontram seu destino) de forma rápida, eficaz, econômica e sem perdas. Além disso, atualmente as empresas de grande porte estão utilizando tecnologias cada vez mais dependentes de uma boa infraestrutura em suas redes, separadas por várias classes de serviços como o *Diffserv*[3]. Por isso, em um ambiente que possui os pacotes de informação pertencentes a diferentes classes, é natural que ocorra uma concorrência de recursos tornando-se necessário obter uma configuração na qual esses pacotes enfrentem um menor número de possíveis interferências advindas dessa competição pelos serviços.

Como consequência do contínuo dinamismo que a rede possui, o processo de engenharia de tráfego perdura por toda sua existência dentro da corporação. Com isso, surge a necessidade de criação de políticas adequadas para a realização de certas mudanças estruturais e lógicas que causam impacto significativo no desempenho da rede, trazendo vantagens ao prover certas habilidades de controle da rede como um todo, ao invés de controlar interfaces e dispositivos individualmente. Porém, qualquer decisão a ser tomada em sentido de gerenciamento de controle por uma empresa dependente da rede lógica, é necessário um estudo prévio, sobretudo da topologia alocada aos componentes, englobando a rede na sua total extensão, analisando o fluxo conjunto com as funções de comutação e roteamento de pacotes.

O controle e o gerenciamento da rede corporativa na engenharia de tráfego assumem papel de fundamental importância, tendo em vista este dinamismo do fluxo dos pacotes, alternando as fontes de possíveis gargalos e consequentes degradações nos

[3] *Diffserv* é um serviço de rede disponível capaz de separar os pacotes de dados em determinadas classes e prioridades através de identificações contidas no cabeçalho do protocolo IP.

recursos aplicados. Por isso, empresas de grande porte seguem duas principais linhas para controle do tráfego: o controle pró-ativo e o reativo.

No caso do controle pró-ativo, há um controle preventivo no sentido de poder prever possíveis eventos desfavoráveis inesperados ou até minimizar os eventos já previstos. Isso pode ser feito com a constante análise da rede como um todo, verificando as origens de tráfego mais significantes, os sistemas mais críticos juntamente com a sobrecarga gerada em algum ponto da rede com a finalidade de saná-la a curto ou longo prazo.

Para restringir o acesso a recursos da rede que estejam congestionados e/ou regular a demanda para diminuir a situação de sobrecarga, devem ser definidas certas políticas para a aceitação, estabelecimento e manutenção de conexões (Awduche; Rekhter, 2001 apud Maia, Nilton, 2006).

No caso do controle reativo, como o nome já diz, reage de forma a corrigir eventos desfavoráveis, ou falhas que já aconteceram na rede em curto prazo.

2.2 Tipos de gerência de redes.

Para se conseguir uma eficiência razoável na engenharia de tráfego de dados em uma rede, a gerência dela se torna uma grande aliada a partir do momento em que são feitas medições, análises de pacotes, *delay* nos equipamentos, porcentagem de disponibilidade etc.

Com todas essas informações disponibilizadas, é possível traçar metas de intervenções cada vez mais adaptativas para maior eficiência da engenharia de tráfego.

No contexto de uma empresa de grande porte, o gerente de rede se torna o principal responsável pelo desempenho e pela eficácia da manutenção da engenharia de tráfego, possuindo total poder de decisão em relação a mudanças.

Apesar de cada empresa possuir sua metodologia de gerência de rede diferente, é possível separá-la em três grandes domínios de ação: Gerência de Desempenho e Planejamento, Gerência de Incidentes ou Falhas/Segurança, Gerência de Configuração.

2.2.1 Gerência de desempenho e planejamento

O principal objetivo da gerência de desempenho é a avaliação de desempenho da rede como um todo, com o objetivo de buscar uma melhor performance, ou seja, envolve atividades a fim de obter uma maior otimização do fluxo dos dados.

Um bom gerenciamento de desempenho de uma rede pode ser obtido através do gerenciamento e planejamento da capacidade desta rede, analisando-a por completo juntamente com seu contínuo tráfego. O gerenciamento de planejamento da capacidade da rede inclui um estudo dos recursos computacionais a serem implantados como largura de banda dos enlaces, configurações dos servidores, *buffers* etc. Em redes corporativas, esse gerenciamento se torna muito importante com análises muito frequentes, pois o crescimento da demanda é muito grande, o que pode comprometer o desempenho se não houver uma melhora constante.

O gerenciamento de tráfego atua basicamente nos nós da rede (roteador, *hubs, access points, swicths*) que são responsáveis pelo transporte de pacotes. Esse controle pode ser efetivado por medições ou funções que demonstram o rendimento de cada um desses nós, apontando o atraso e eficácia de transmissão dos pacotes, possibilitando uma análise mais detalhada de pontos ou trechos da rede que são candidatos a ter congestionamentos, o que significa uma antecipação na resolução de problemas de indisponibilidade dos recursos.

2.2.2 Gerência de incidentes ou falhas/segurança

Uma boa engenharia de tráfego engloba também uma gerência de falhas devido à dependência de uma constante monitoração em busca de qualquer evento que impeça a disponibilidade da rede.

O objetivo da gerência de falha é descobrir a raiz do problema, coletando os dados monitorados e que se mostram potencialmente capazes de gerar alguma falha no transporte normal ou ótimo do fluxo de pacotes. Identificado o problema, é importante tomar uma decisão para saná-la de forma que posteriormente seja possível solucioná-lo definitivamente de modo imperceptível para os usuários da rede.

Outro ponto importante para o impedimento de falhas em uma rede é a implementação de uma segurança robusta, ou seja, quanto menor as chances de pontos de ataques em uma grande malha lógica, menor será a quantidade de falhas geradas por algum agente externo ou mesmo interno. Como toda e qualquer rede empresarial possui um caráter privado, ou seja, não há permissão de conexões externas com seus servidores ou com qualquer nó, normalmente quando se percebe uma ameaça ativa, poderá ser acionado um *plugin* (aplicativo computacional) específico para tentar impedir de

alguma forma a vulnerabilidade que o ataque proporcionou, degradando o desempenho normal.

Por isso, tanto as falhas que acontecem de forma natural ou aquelas ocasionadas por fatores externos, devem ser gerenciadas ao longo do processo da engenharia de tráfego para garantir acordos de disponibilidade firmados. Por outro lado, faz-se necessário incluir como parâmetro o intervalo temporal que cada falha diferente necessita para ser corrigida. Isto decorre das diferentes políticas que cada empresa implementa.

2.2.3 Gerência de configuração

A última das principais gerências e não menos importante é a gerência de configuração. Ela se caracteriza pela uniformidade de configuração que alguns ou todos os equipamentos relacionados da rede possuem. Configuração de uma rede corporativa pode se dá em nível topológico, em que se mantém um mapa da arquitetura que, como os nós (equipamentos), estão interligados uns aos outros e em nível lógico, onde todas as configurações feitas no sistema operacional de cada equipamento são guardadas a fim de que facilite operações de mudanças, recuperação de enlaces comprometidos e otimizando o processo de escalabilidade. Essas informações são melhores administradas, acumulando-as em uma base de dados chamada *baseline*.

É muito importante tornar a consulta à *baseline* confiável e atualizada, ou seja, qualquer modificação feita, como novo padrão adotado pela empresa, ela deverá ser atualizada.

Por isso, uma gerência de configuração dos dispositivos da rede demonstra-se como um grande aliado na hora em que se precisa tomar medidas ou intervenções na otimização da engenharia de tráfego.

2.3 Modelagem, análise e medição.

Atualmente, há um crescente aumento de padronização no gerenciamento de serviços de TI, porém de forma que o gerente tenha grande liberdade de implementação dentro da sua área de negócio. Por isso, cada empresa adota uma política ou modelo para que se desenvolva uma engenharia de tráfego dos seus dados na rede.

Os principais parâmetros norteadores para que se consiga implementar uma engenharia de tráfego são disponibilizados através de processos experimentais, como a medição de fluxos, velocidade de respostas, capacidade de transportes etc. A partir dessas informações, é necessário que seja feita uma análise para que se tenha uma conclusão no comportamento dessa rede.

2.3.1 Modelagem para engenharia de tráfego

Atualmente não existe um modelo de processo padrão para o desenvolvimento de uma engenharia de tráfego em redes computacionais. Por isso, cada empresa possui um modelo próprio dependendo de suas características e objetivos. Apesar dessa falta de um modelo, cada qual possui etapas para sua construção que se assemelham bastante e se destacam por ter as seguintes características:

a) A primeira etapa possui uma característica de definição de políticas de controle mais amplo, dependendo de parâmetros, como objetivos da empresa, atividade de negócio, custo estrutural da rede, níveis de serviço, restrições, permissões etc;
b) A segunda fase consiste basicamente em uma aquisição de dados de *feedback* (dados gerados pela rede) para a análise através da rede operacional. Dependendo da política de segurança da empresa, esses dados poderão ser de difícil acesso, necessitando-se de uma análise feita com simuladores, o que reflete o comportamento da rede estimando valores bem aproximados da realidade;
c) A terceira e mais trabalhosa fase consiste na investigação de pontos críticos, pontos potenciais de gargalos, pontos problemáticos existentes e também na investigação do equilíbrio existente das concentrações dos fluxos de dados e sua distribuição;
d) A quarta fase é a otimização da rede. Uma empresa pode possuir técnicas próprias para alcançar a melhor performance no fluxo de dados de uma rede. Isto pode ser feito em nível topológico, parâmetros de roteamento em determinado trecho, mudanças dinâmicas para atender certo gargalo em um ponto, métricas de protocolos configurados etc. Uma boa otimização tem seu início desde planejamento da topologia até as configurações de equipamentos que visam o crescimento atual e futuro da empresa.

2.3.2 Análise e medições

A análise pormenorizada de uma rede corporativa começa a partir da coleta de dados específicos, através de medições feitas com sistemas apropriados para tal fim e que ajudam a dar suporte à engenharia de tráfego em grandes redes IP corporativas, de forma a assegurar aspectos dessa engenharia, como planejamento, dimensionamento, gerenciamento (controle) e otimização de desempenho.

As bases para uma medição de rede podem ser os fluxos, interfaces, desempenho dos equipamentos, topologia da rede, enlaces etc. A partir dessas bases, há a formação das entidades de medição que se identificam pelos resultados ou desempenho do funcionamento das bases utilizadas como parâmetro. Essas entidades podem ser o atraso dos pacotes em algum enlace, retardo de processamento de algum equipamento, banda disponível e utilizada em alguma parte da topologia, tempo gasto em algum fluxo específico e utilização dos recursos.

É importante notar que essas informações em conjunto com outras, como por exemplo, as configurações da *baseline* e outros dados estatísticos obtidos com as entidades de medição são importantes para se obter uma melhor engenharia de tráfego.

Atualmente, há alguns *frameworks* (aplicativo para reconhecimento de medidas) capazes de identificar componentes de medição para a engenharia de tráfego. Dentre esses componentes, alguns apresentam maiores relevâncias para uma análise mais eficaz, tais como escalas de tempo, bases para medição, interfaces, medição baseada em MPLS[4] e entidades de medição, as quais serão comentadas a seguir:

- Escalas de tempo: para cada tipo de gerenciamento existente na rede, pode-se atribuir uma escala de tempo diferente. Como exemplo, a gerência de planejamento de rede possui uma escala de tempo grande ou muito grande, pois uma mudança na configuração requer uma constante avaliação, cuja alteração dure dias ou meses a fim de não ocorrer impactos significativos ou perda de desempenho.

Já na gerência de capacidade, onde os *SLA's*[5] (*Service Level Agreement*) entram em evidência, há uma necessidade de obter uma rotina de análises, cujas alterações

[4] *MPLS* (*Multiprotocol Label Switching)* é um protocolo de roteamento baseado em pacotes rotulados, onde cada rótulo representa um índice na tabela de roteamento do próximo roteador.
[5] *SLA(Service Level Agreement)* ou acordo de nível de serviço é a parte do contrato de serviços entre duas ou mais entidades no qual o nível da prestação de serviço é definido formalmente

acontecem em um espaço de tempo não muito longo a fim de atender demandas estratégicas da corporação ou reverter algumas falhas toleráveis. Possuindo uma gerência de controle, há informações que se modificam muito rapidamente, necessitando de mudanças cujas alterações possuem um tempo muito menor do que nos outros tipos de gerências, objetivando a recuperação de falhas e perdas de dados importantes em serviços diferenciados obtidas por falhas de infraestrutura, reequilibrando a carga e retornando o funcionamento de todos os nós e enlaces o mais rápido possível.

- Bases para a medição: é importante notar que, dentre vários pontos da rede, haverá uma diferença enorme na coleta de dados entre esses pontos devido ao maior e menor fluxo de dados que passarão nas mais diferentes interfaces de coletas. Por exemplo, em roteadores de borda ou concentração (roteadores responsáveis pela entrada de todos os dados em uma determinada rede) haverá um fluxo muito grande de dados, porém, em roteadores de qualquer outro ponto, haverá uma quantidade menor e um fluxo totalmente diferente. Por isso, o fluxo de um dado ponto da rede, compreendendo uma origem e um destino, servirá como base de medição para uma engenharia de tráfego.
- As interfaces e nós alocados por toda a extensão da rede podem servir também como base de medição na engenharia a partir do momento em que esses equipamentos detêm todas as rotas definidas dos pacotes que por eles ultrapassarem. Daí se torna necessária uma análise estatística da quantidade perdida e processada desses pacotes, contribuindo como informação relevante nas medições.
- Medição baseada em caminhos MPLS. De forma semelhante ao do fluxo, o caminho sugere uma análise de uma forma mais abrangente pelo fato de que, por esse caminho MPLS, poderão percorrer diversos fluxos, ou seja, de um nó de origem para um nó de destino, não se observa apenas um fluxo simples, mas é necessário considerar o conjunto deles.
- Entidades de medição: definidas as bases de medição, a análise pode ser iniciada com as medições propriamente ditas, possuindo nomenclaturas e unidades

diferentes. Dentre essas entidades, as mais conhecidas são a vazão (*throughput)*, a variação de retardo (*jitter*) e a matriz de tráfego[6].

Por isso, qualquer valor estatístico observado por um tempo e que possui uma unidade caracterizadora de uma rede lógica, poderá servir como uma entidade de medição na engenharia de tráfego. Obviamente que serão determinados limiares norteadores sobre a operacionalidade normal da rede em questão.

2.4 *Multiprotocol Label Switching –Traffic Engineering*

Com a crescente exigência de aplicações de tempo real, voz e vídeo, houve uma motivação em agilizar o processo de roteamento para suportar o tráfego cada vez maior. Como esse processamento era feito baseado nos pacotes IP, o tempo de roteamento se tornava muito elevado para esta tecnologia. A partir dessa necessidade, o IETF padronizou o MPLS, baseado na combinação de três tecnologias apresentadas por três principais empresas, Ipsilon (tecnologia *IP Switching*), Toshiba (tecnologia *Cell Switching Router*) e a Cisco (tecnologia *Tag Switching*), demonstrando o conceito de comutação dos pacotes IP de forma mais rápida que os processos anteriores.

O principal objetivo desta tecnologia é a solução dos problemas de redes atuais como velocidade, escalabilidade, qualidade dos serviços e engenharia de tráfego (TE). Por isso, uma das vantagens, está na relação do aumento no rendimento da rede, uma vez que existe uma facilidade de implementação dessa engenharia, escolhendo caminhos com maior velocidade e prioridades para distribuição da carga de um enlace congestionado.

O MPLS é utilizado principalmente em *backbones*[7] e sua principal aplicação consiste na utilização em conjunto com a tecnologia IP, o que se torna possível a interoperabilidade de roteamento dos pacotes com a comutação de circuitos. Outra aplicação muito significativa que esta tecnologia pode implementar é a construção de *VPN's* (*Virtual Private Network*) de grande abrangência, onde os dados conseguem

[6] *Throughput* é a taxa a que os dados são enviados entre dois pontos da rede em um período determinado de tempo; *Jitter* é uma variação estatística do atraso na entrega dos dados de uma rede ou enlace; Matriz de tráfego é o conjunto de informações existentes a respeito de análises feitas da rede obtidas pelas medições.

[7] *Backbone* significa "espinha dorsal", e é o termo utilizado para identificar a rede principal pela qual os dados de todos os clientes passam.

trafegar pelo túnel MPLS de forma segura em uma rede aberta, sem serem descobertos por terceiros.

Por tudo isso, esta tecnologia se torna responsável por dar suporte a diversas aplicações que necessitam de um serviço diferenciado com qualidade sobre a infraestrutura de redes.

2.4.1 Elementos de uma rede MPLS

Para o entendimento do funcionamento de uma rede de domínio MPLS, é necessário conhecer o significado e o papel de cada elemento pertencente a essa rede. Fisicamente, uma rede MPLS é formada por um conjunto de roteadores camada três, ou seja, roteadores que suportam o protocolo de distribuição de rótulos para comutação.

Dependendo da topologia e da localização de cada um desses roteadores dentro da rede, pode-se ter uma denominação e um conceito diferente para cada um deles. Os principais elementos de uma rede MPLS são: *Label Switching Routers* (LSR), *Label Switch Path* (LSP), *Forward Equivalence Label* (FEC), *Label Edge Routers* (LER), *Labels* (Rótulos) e *Label Information Base* (LIB). A figura 2 ilustra a distribuição desses elementos ao longo de uma rede MPLS.

Os LSR's são roteadores que se encontram no interior da rede e são fundamentais para a comunicação com outros roteadores, aonde irão se certificar de informações sobre os enlaces, efetuando a expedição de pacotes com seus rótulos a um ritmo de níveis elevados, gerando um caminho chamado LSP (*Label Switching Path*), ligando a origem (roteador localizado na borda de entrada do fluxo) ao destino (roteador localizado na borda de saída do fluxo).

Na fronteira da rede MPLS, estão os roteadores chamados LER que, por se localizarem na entrada e saída da rede, implementam as políticas de acesso determinadas pelo administrador da rede, além de inserir os rótulos (roteadores de entrada) e retirar rótulos (roteadores de saída) nos pacotes que trafegam por esta rede.

Uma FEC (*Forward Equivalence Class*) é um conjunto de pacotes que foram tratados pelo roteador de entrada para expedição, no sentido de classificar esses pacotes, aplicando alguns processamentos nos campos de cabeçalho: requisitos de *QoS*, tipo de aplicação, identificador de *AS/VPN*, as sub-redes de origem/destino e grupos de *multicast*, gerando um rótulo distinto apropriado para cada requisição associada.

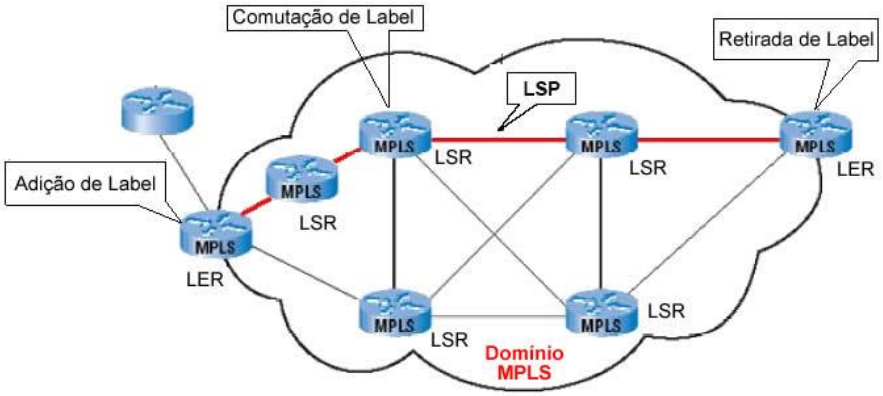

Figura 2: Elementos de uma rede MPLS

Fonte: Memória, Carlos (2004).

Algumas características presentes na FEC são importantes para que se faça engenharia de tráfego eficientemente como, por exemplo, a atribuição de várias FEC's associadas ao mesmo caminho LSP e vários caminhos LSP associados à mesma FEC, gerando assim, uma melhora da agregação dos fluxos desses pacotes. Outra importante característica é a possibilidade de configuração explícita dos caminhos LSP atribuídos a cada FEC relacionada, executando-se de forma administrativa pelo gerente da rede ou de acordo com as necessidades de recursos requisitadas, baseadas em restrições.

O *Label* ou rótulo MPLS também chamado de *Shim Header*, geralmente é encapsulado em um pequeno cabeçalho localizado entre a camada 2 e a camada 3, permitindo assim o suporte a vários outros protocolos e qualquer tecnologia da camada de ligação (Veiga, 2009). Dentro de uma rede MPLS os rótulos são pequenos identificadores colocados nos pacotes durante seu tráfego pela rede. Eles são inseridos pelos roteadores de entrada e removidos definitivamente pelos roteadores de saída. Os rótulos possuem a seguinte estrutura:

|-20bits Label-|-3bits CoS-|-1bit Stack-|-8bits TTL-|

Os três bits de *CoS* (*Class of Service*) são usados para determinação de classes de enfileiramento e descarte de pacotes, podendo-se utilizar prioridades para certos pacotes. O bit *Stack* é usado para a criação de uma pilha de rótulos, usada de forma

hierárquica, ou seja, durante a movimentação dos pacotes pela rede, os rótulos mais externos dessa pilha, serão removidos e os mais internos, atravessarão os roteadores que formam o caminho LSP até chegar aos roteadores de saída, removendo-os definitivamente.

A *Label Information Base* (LIB), nada mais é do que uma tabela que contém informações acerca dos rótulos de entrada e saída de cada um dos roteadores localizados no interior da rede, estruturada em campos como índices dos rótulos, interface de entrada e saída, e o IP do próximo *hop* (salto). Assim que um caminho LSP é criado, a relação entre interface e rótulo é armazenada na LIB.

2.4.2 Distribuição de rótulos

Cada roteador localizado no interior de uma rede MPLS irá atribuir um rótulo para cada caminho LSP formado. Por isso, um roteador localizado mais próximo à origem do fluxo do tráfego, deverá conhecer qual o rótulo que o roteador que está localizado mais distante dele utiliza para identificar esse caminho LSP.

O responsável pela distribuição dos rótulos em uma rede MPLS é um protocolo denominado LDP (*Label Distribution Protocol*). O funcionamento deste protocolo se dá com a troca de mensagens entre os roteadores localizados no interior da rede, sobre informações de mapeamento do caminho LSP e a FEC respectiva. Isto é feito de forma bidirecional entre eles, abrindo uma sessão de comunicação, cujas informações de controle e alcance dos rótulos são trocadas. Atualmente o LDP foi modificado para que este consiga suportar o encaminhamento de rótulos com restrições, o que é fundamental para implementação de serviços diferenciados e engenharia de tráfego de rede. Por serem configurados nos roteadores localizados na fronteira das redes MPLS, os LER devem possuir um desempenho muito alto devido à distribuição dos rótulos na entrada e a retirada desses na saída da rede.

2.5 Encaminhamentos com restrições e MPLS-TE

Os protocolos IGP[8] convencionais implementados dentro da rede MPLS, por si só não atendem todas as necessidades de recursos e nem otimizam os cálculos de

[8] IGP protocolos utilizados no interior de uma rede. Composto de três protocolos (RIP, Hello, OSPF).

métrica escalares (como por exemplo, o número de saltos). Para administrar métricas do IGP no encaminhamento entre dois pontos, se torna bastante difícil na medida em que o estado da ligação e a forma como são manipuladas no domínio MPLS, são diferentes das métricas utilizadas na arquitetura de serviços integrados (arquitetura *IntServ)* de uma rede IP tradicional. Por isso, os protocolos de encaminhamento baseados em restrições, buscam encontrar uma rota que otimize uma certa métrica e ao mesmo tempo não viole alguma restrição solicitada (como por exemplo, largura de banda mínima). Sendo assim, torna-se necessário a sinalização para implementação desses serviços utilizando-se as métricas IGP.

As principais soluções desenvolvidas para esta tarefa de sinalização são: *Constraint Based Label Distribution Protocol* (CR-LDP) e o protocolo *Resource Reservation Protocol* (RSVP) que atualmente já possui extensões de engenharia de tráfego com MPLS, chamando-se *Resource Reservation Protocol with Traffic Engineering* (RSVP-TE).

2.5.1 *Constraint Based Label Distribution* (CR-LDP)

O CR-LDP é construído sobre o LDP, que já é parte do MPLS. Embora os estudos do *IETF MPLS Working Group* tenham sido abandonados, este protocolo possui resultados satisfatórios e não implica a implementação de um novo protocolo, com o consequente aumento na carga de processamento, tal como acontece com o preferido RSVP-TE (Veiga, 2009).

As principais características do protocolo são: o uso de um esquema de codificação parecida com o LDP tradicional de redes MPLS denominado TLV *(Type-Lenght-Value)* que são mensagens passadas pela rede, possuindo três campos diferentes. O campo *type* (define o tipo da mensagem), o campo *length* (especifica o tamanho em bytes do campo *value*), o campo *value* (codifica a mensagem que é interpretada de acordo com o tipo). Com a manipulação desses três campos, pode-se implementar a engenharia de tráfego na rede MPLS. Outra característica deste protocolo é o suporte explícito de encaminhamentos do tipo *stric* e *loose*, onde no primeiro tipo, o caminho completo a ser seguido se torna fixo e o segundo tipo, somente alguns nós ou roteadores do caminho todo se tornam fixos. Além dessas características, para descobertas de novos nós em uma rede MPLS, o CR-LDP usa o protocolo *User Datagram Protocol* (UDP) e para realização de controle e gestão, mensagens *label request e label mapping*.

2.5.1 Funcionamento do CR-LDP

O funcionamento da sinalização usando o CR-LDP se dá basicamente através das mensagens *label request* e *label mapping.* Todo o processo de distribuição e solicitação do estabelecimento de rota se inicia no LSR de borda quando é gerado um *label request* que é o possuidor de campos indicadores dos parâmetros de recursos requeridos. Após a reserva desses recursos requeridos para o novo caminho LSP, a mensagem para estabelecimento de comunicação é encaminhada para o próximo nó (*router*) numa sessão TCP. Este processo é feito de nó em nó até que o LSR de saída pertencente ao LSP receba esta mensagem, e a partir daí é gerado um *label mapping* que fará com que percorra por todos os nós anteriores, chegando ao roteador de entrada que concluirá informações dos recursos reservados para o LSP, alocando-os.

Existem diversos objetos característicos deste protocolo: o ER (*Explicit Route*) é um campo das mensagens CR-LDP que especifica o caminho que um LSP deve tomar no momento em que está a ser estabelecido. É composto por um ou mais *ER-Hops* que constituem a especificação dos *routers* que fazem parte do caminho definido para o LSP (Veiga, 2009).

Para controlar erros por falta de recursos ou outro tipo de falha no estabelecimento de um CR-LSP, o protocolo possui notificação de mensagens que carregam o campo *Status TLV's* que identificam os eventos sinalizados. Se um LSR receber uma mensagem de notificação, este deverá desalocar todo o recurso previamente alocado para tal caminho e ainda propagar para o LSR anterior se estes recursos estiverem associados a ele. Essas notificações são propagadas até o roteador de entrada, o qual gerou o *label request message*. A figura 3 ilustra o funcionamento básico de troca de mensagens entre os roteadores de um caminho LSP implementado com o protocolo CR-LDP.

Apesar das boas referências expostas deste protocolo, há uma diferença que motiva a preferência do IETF (*Internet Engineering Task Force*) pelo RSVP-TE, presente no fato do CR-LDP ser do tipo *Hard State* caracterizando o fechamento do circuito virtual somente após um pedido expresso de desconexão enviado, ao passo que o RSVP-TE é do tipo *Soft State* que se caracteriza por envios de mensagens periódicas acerca do estado operacional dos circuitos virtuais, podendo ser fechados se ultrapassarem algum tempo determinado de resposta.

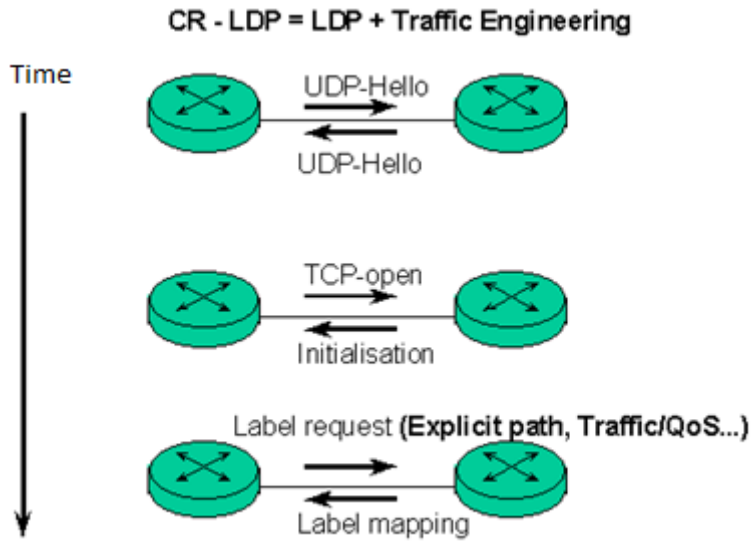

Figura 3: Funcionamento da troca de mensagens do protocolo CR-LDP.

Fonte: Benbella Benduduh et Jean Marc Fourcade, 2001.

2.5.2 *Resource Reservation Protocol with Traffic Engineering* (RSVP-TE)

O protocolo RSVPv1 foi desenvolvido para contornar congestionamentos de rede, pela inteligência proporcionada aos roteadores para decidir, antecipadamente, qual o caminho que atenderia às necessidades do fluxo de tráfego de uma aplicação e então reservar os recursos necessários (Amorim & Silva, 2007). Assim como o CR-LDP, o RSVP é uma técnica de sinalização usada para reservar recursos através de uma rede, portanto não possui a capacidade de roteamento dos pacotes. O protocolo RSVP-TE é na verdade uma extensão do protocolo RSVP original, suportando o estabelecimento de LSP's que utilizam redes MPLS[9].

O protocolo RSVP-TE possui várias mensagens que são utilizadas nas operações de formação de túneis, são elas: *Path, Resv, PathTear, ResvTear, PathErr, ResvErr, ResvConf, ResvTearConf* (proprietária da *Cisco Systems*) e *Hello*. Para iniciar o estabelecimento de um caminho, as mensagens *Path message* e *Resv message* se tornam fundamentais para a troca de informações entre origem e destino.

A estrutura do protocolo RSVP-TE é alicerçada com a troca de mensagens e objetos utilizados entre os roteadores definidos para implementação da qualidade de

[9] Descrito na *Request for Comments* (RFC3209). RFC é um documento que descreve os padrões para cada protocolo da internet previamente a ser considerado um padrão.

serviço em uma rede MPLS. O quadro 1 mostra um resumo das funções definidas que as mensagens do protocolo possuem:

Quadro 1: Resumo das funções definidas

Tipo de Mensagem	Descrição
Path	Usada para configurar e manter reservas
Resv (abreviação de Reservation)	Enviado em resposta a mensagens Path, mas usada para remover reservas da rede.
PathTear	Semelhante a mensagens Path, mas usado para remover reservas da rede.
ResvTear	Enviado para mensagens Resv, mas usado para remover reservas da rede.
PathErr	Enviado por um destinatário de uma mensagem Path, que detecta um erro nessa mensagem.
ResvErr	Enviado por um destinatário de uma mensagem Resv, que detecta um erro nessa mensagem.
ResvConf	Opcionalmente enviado de volta ao emissor de uma mensagem Resv, para confirmar que determinada reserva realmente foi instalada.
ResvTearConf	Uma mensagem proprietária da Cisco para um ResvConf. Usado para confirmar que determinada reserva foi removida da rede.
Hello	Uma extensão definida na RFC 3209, que permite *keepalives* locais do enlace entre dois vizinhos RSVP conectados diretamente.

Fonte: OSBORNE, Eric 2003

Cada tipo de mensagem possui uma identificação única definida previamente para o processo de comunicação. As mensagens *Path* e *Resv* que são trocadas entre a origem e o destino para o estabelecimento do caminho LSP, possuem objetos que são transportados por elas, carregando as informações e características de qualidade de serviço, banda disponível, reservas, possíveis *loops*, rotas explícitas e etc. Além disso, esses objetos fazem parte da constituição de um pacote RSVP-TE juntamente com um cabeçalho (Amorim & Silva, 2007).

Os objetos utilizados pelas mensagens *Path Message* e *Resv Message* são: *Label Request Object, Label Object, Flowspec Object, Explicit Route Object, Record Route Object, Session Object, Sender_Template Object, Filter_Spec Object* e *Session_Atribute Object*.

É importante esclarecer que além dos objetos serem separados por classes, dentro de cada classe, há outra separação por tipo de classes, definida como Tipo C do objeto, criando assim, uma espécie de hierarquia de tipos.

O objeto *Label Request Object* é basicamente utilizado por uma mensagem do tipo *Path Message* para que um roteador da rede MPLS reserve um *label* de um caminho LSP. Outra característica importante desse objeto está no fato de se poder identificar um protocolo de nível 3 como, por exemplo, o protocolo de roteamento OSPF, BGP-4.

O *Label Object* é utilizado em mensagens do tipo *Resv Message*, confirmando a alocação de um recurso solicitado e posteriormente atualiza a LIB do roteador. Por ter essa característica, na pilha de *labels*, o objeto contém apenas um identificador referenciando o respectivo recurso local da interface onde é percorrido o LSP.

O objeto *Flowspec* é importante pela sua função de especificação da qualidade de serviço que a aplicação requisitará. Alguns requisitos são: nível de QoS, banda a ser alocada, atraso, taxas de perdas e etc. É claro que, em muitos casos, não se precisa definir esses requisitos por não se tratar de um LSP que necessite desses recursos diferenciados, por isso, caso isso aconteça, o objeto *Flowspec* não possuirá nenhuma informação e o tráfego irá ser associado ao tipo *best effort* (melhor esforço) convencional.

Há situações em que é possível configurar rotas explícitas independente dos protocolos implementados dentro da rede como o IGP. Além disso, existe a possibilidade de manter um nível de QoS nesse caminho LSP através do uso do protocolo RSVP-TE com o objeto *Explicit Route Object* associado a essa rota. Para garantir que isto aconteça, é necessário que a origem conheça todo o caminho por onde irá passar o tráfego (somente por roteadores com o RSVP-TE configurado) e que possui características necessárias para o atendimento desses requisitos de recursos.

O *Explicit Route Object* possui vários sub-tipos de classe, onde é garantido o suporte a vários elementos de rede como o IPv4, IPv6, *Autonomous System Number* e Terminação MPLS LSP.

Outro objeto de grande importância e de fundamental implementação é o *Record Route Object* (RRO), capaz de gravar e identificar cada elemento de rede por onde as mensagens *PATH e RESV Messages* passam, por isso, é utilizado por elas. Porém, o RRO possui um número limitado de elementos a ser gravado e por isso, quando esse limite for ultrapassado, será enviado um *PathErr* ou um *ResvErr* no intuito de retirar o RRO da mensagem. É possível aplicar este objeto de forma a descobrir loops de roteamento e loops de rotas explicitas que não obtiveram êxito em suas implementações (Amorim & Silva, 2007). Esse objeto possui atualmente dois subtipos de classe, sendo um para o IPv4 tradicional e o novo IPv6.

Há outros tipos de objetos com funções específicas como, por exemplo: *Session Object* utilizado pelo *Path Message* para identificar um LSP; *Sender_Template Object* também utilizado pela Path Message para informar o formato dos dados; *Filter_Spec Object* que define em conjunto com o *Session Object*, o fluxo de dados que possuirá as características definidas pelo *Flowspec Object* e o *Session_Atribute Object* que controla a prioridade do caminho LSP em casos de preempção (interrupções temporárias) utilizado pela mensagem *Path Message*, podendo ajustar as sessões baseado nas prioridades antigas e atuais e com valores maiores e menores.

Esse objeto em específico se torna muito importante para implementação de engenharia de tráfego na medida em que há circuitos virtuais com reservas similares de recursos, podendo-se determinar a política e estratégia de utilização da banda em períodos críticos de solicitações.

2.5.2 Funcionamento do RSVP-TE

O funcionamento do protocolo é baseado em operações que ocorrem nos túneis LSP's, sendo essencialmente constituídas por troca de mensagens entre a origem e o destino do túnel. As reservas que o protocolo faz, necessita ser atualizada de tempos em tempos, tornando-lhe não rígido. Uma requisição solicitada, somente irá desaparecer se for explicitamente pedido ou tiver seu tempo de vida esgotado.

Com base na figura 4 mostra-se uma rede MPLS com seus roteadores de fronteira (LER's) e os de *backbone* (LSR's) configurados com o protocolo RSVP-TE. É importante notificar que, além da arquitetura MPLS, há um protocolo de roteamento (IGP) dentro da rede, responsável por definir caminhos para a comunicação entre a origem e o destino.

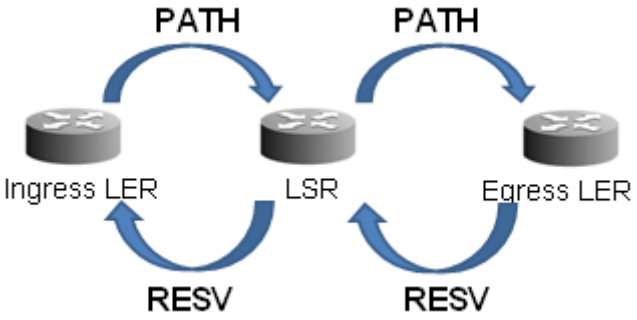

Figura 4: Funcionamento da troca de mensagens do protocolo RSVP-TE.

Fonte: Dominique Revuz, 2000.

A estação de origem requisita um caminho com qualidade de serviço para alcançar a estação de destino enviando uma mensagem do tipo *Path Message*, contendo todas as informações referentes ao tipo de recurso, tráfego e qualidade de serviço a ser utilizado.

A mensagem do tipo *Resv Message* é enviada da estação destino para a estação de origem percorrendo o mesmo caminho seguido pela mensagem *Path Message* reservando todos os recursos de QoS requisitados, estabelecendo o caminho de túnel LSP. Por isso, o protocolo RSVP-TE é dito orientado pelo destinatário ou *Receiver Oriented*. Devido à troca de mensagens do tipo *Path Message* e *Resv Message* ser feita periodicamente entre os roteadores, o protocolo é do tipo *softstate*, possibilitando o rápido re-roteamento dos caminhos LSP's.

A verificação da disponibilidade de recursos e a alocação de um *label* para o LSP são duas tarefas que serão realizadas em todos os nós (*routers*) do túnel. Porém, se algumas dessas duas tarefas não puderem ser efetivadas, haverá uma mensagem de erro chamada *PathErr* ou *ResvErr* (dependendo do sentido da requisição) e o túnel não será estabelecido.

Um *PathErr* é enviado quando um label não pode ser alocado para um *Path Message* devido uma indisponibilidade de faixa para alocação. O código padrão para este tipo de procedimento é: *Routing Problem* e com o valor: MPLS *label allocation failure*. Além do formato normal do *label request*, há outros que especificam faixas de valores para VPI e VCI em redes ATM e DLCI para redes *Frame Relay*, demonstrando o poder de utilidade em pacotes de diferentes tecnologias de redes.

Diante dos principais tipos de objetos utilizados no mecanismo de alocação de recursos, há três possibilidades de se reservar tais recursos. A primeira forma é chamada

de *Fixed Filter* (FF), como o nome já diz, não há uma mobilidade de recursos, se trata de uma forma fixa para um único par origem-destino, sem compartilhamentos. A segunda forma é chamada de *Shared Explicit* (SE), permitindo que a origem solicitante do recurso, compartilhe com elementos diferentes e com necessidades diferentes. Nesse modelo de reserva, é utilizado o conceito de *make-before-break* que significa a realocação de recursos de um LSP danificado (com interrupções de tráfego ou queda de performance) para outro LSP antes que o primeiro seja desativado (Amorim & Silva, 2007). A terceira forma de reserva é chamada de *Wildcard Filter* (WF) e compartilha apenas um único recurso reservado não podendo assim ter atributos de engenharia de tráfego e por isso não é utilizado pelo RSVP-TE.

2.6 Classes de serviços e MPLS-TE

Um campo de 8 bits chamado DS (*Differentiated Services*), presente no protocolo IP, dá o suporte a arquitetura de serviços diferenciados de forma a inserir informações (classificação) nos pacotes para que sejam analisados. Todas as informações de classificação estão inseridas nos primeiros 6 bits do campo, denominado DSCP (*Differentiated Services Codepoint*). O modelo DiffServ não necessita de um protocolo próprio (como no caso do RSVP, usado no IntServ), pois aqui se utiliza um campo do próprio datagrama IP. Tudo que um roteador precisa fazer é examinar o campo DSCP de cada pacote para determinar qual tratamento a ser dado ao mesmo. (Teixeira, 2000).

A primeira tarefa ao implementar serviços diferenciados é ter a capacidade de classificar os pacotes. Isto nada mais é do que fazer uma análise para saber sobre qual o tipo de regra que cada um deles será executada.

Os pacotes com a tecnologia MPLS são classificados apenas comparando o valor do campo EXP de 3 bits, presente nos rótulos, ou seja, não há forma de comparação distinta, pois o MPLS encapsula o protocolo IP. Além disso, somente os rótulos encontrados no topo da pilha serão comparados, uma vez que são os únicos visíveis para os roteadores, decorrentes de sua hierarquia.

Para que os serviços sejam classificados através desses pacotes, é preciso que seja feito um tratamento na pilha de rótulos, especialmente no campo EXP, uma vez que haverá um encapsulamento de vários rótulos com o campo referido.

O primeiro caso a ser considerado, é observado nos pacotes IP que entram em uma rede MPLS, conhecido como *ip-para-mpls* e normalmente escrito como *ip2mpls*. Quando os pacotes IP entram numa rede MPLS, há uma operação de empilhamento (*push*), ou seja, os rótulo MPLS é empilhado sobre o pacote IP não rotulado.

Por padrão, quando o software da Cisco empilha rótulos sobre um pacote IP, os bits mais significativos no campo DiffServ (os *bits IP Precedence*[10]) são copiados para o campo EXP de todos os rótulos empilhados (Osborne, 2003).

O segundo caso a ser considerado, é observado em pacotes MPLS que estão trafegando num domínio MPLS, ou seja, pacotes que já possuem rótulos sendo empilhados por outros rótulos. Isto é conhecido como *mpls-para-mpls* ou *mpls2mpls*. Quando ocorre a operação de empilhamento, o campo EXP do rótulo mais abaixo da pilha é copiado para o rótulo mais acima da pilha. Essa troca é chamada de caminho (*path*) *mpls2mpls*. No entanto, por existir uma pilha de rótulos, três ações são possíveis de ser manipuladas nesse âmbito:

- Empilhar (*Push*): rótulos MPLS são acrescentados a um pacote que já possui rótulo;
- Trocar (*Swap*): rótulos que se localizam no topo da pilha, é trocado por outro rótulo;
- Desempilhar (*Pop*): rótulos mais externos são removidos, mas pelo menos um rótulo ainda permanece na pilha;

O último caso é observado quando a pilha de rótulos é completamente removida, resultando apenas num pacote IP tradicional. Isto é chamado de *mpls-para-ip* ou *mpls2ip*. A única operação presente é a de desempilhar (pop) todos os rótulos da pilha, resultando em um pacote IP tradicional.

O suporte do MPLS para serviços diferenciados possui uma particularidade devido à limitação encontrada nesta tecnologia. Isto se deve ao fato de que o rótulo MPLS, com seu campo EXP (utilizado para marcação de pacotes) de três bits, foi definido anteriormente ao DSCP (utilizado para classificação de serviços em pacotes IP) de seis bits. Em consequência disso, serviços diferenciados sem o uso do MPLS, poderão ter 64 possibilidades de classificação DSCP, e com esta tecnologia, somente oito possibilidades de classificação. Por isso, foram desenvolvidos dois métodos para

[10] *IP Precedence* é a referência para os três dos seis *bits* presentes no cabeçalho IP que são copiados para o rótulo.

aliviar tal problema. O primeiro método chamado de E-LSP possui a ideia de que se a rede possui até oito classificações de serviços diferenciados, o campo EXP do pacote MPLS é suficiente para mapear e transmitir os valores deste campo para essas classificações, utilizando o DSCP normalmente. Porém, se a rede possuir mais de oito classificações de serviços, o método chamado L-LSP utiliza tanto o campo EXP de três bits como o próprio rótulo MPLS para definir essas diferentes classificações.

2.7 Proteção e restauração

Apesar da implementação de toda uma engenharia de tráfego em uma rede corporativa, sempre haverá momentos que tudo ou parcialmente não funcionará devido alguma falha física ou lógica. Partindo para o foco no núcleo dessas redes (roteadores), podemos ter falhas de enlace (caracterizando-se na ligação desses roteadores) e falhas de nó (o próprio roteador). Uma falha no enlace pode ser uma fibra cortada, cabos mal conectados e etc. Já uma falha no nó pode ser representada por falta de alimentação do roteador, problemas administrativos ou desligamentos preventivos.

Acontece que a MPLS-TE e sua capacidade de direcionar o tráfego para fora do caminho mais curto, derivado pelo IGP, ajuda a aliviar a perda de pacotes associadas a falhas de enlace ou nó na rede. A capacidade da MPLS-TE de fazer isso é conhecida como *Fast Reroute* (FRR) ou simplesmente MPLS-TE *Protection* (OSBORNE, 2003).

A proteção para alguma eventualidade de falha está relacionada à perda mínima de pacotes após esse evento. Os recursos a serem protegidos podem ser físicos (roteadores ou fibras/cabos) e lógicos (caminhos LSP's). O termo proteção deverá estar associado ao fato de que recursos de backup são pré-estabelecidos e não são sinalizados depois que uma falha tenha ocorrido.

Se os recursos de proteção não fossem pré-estabelecidos, eles teriam que ser configurados depois da detecção da falha; nesse caso, seria tarde demais (OSBORNE, 2003).

A seguir, serão explicitados os conceitos básicos sobre a nova plataforma de serviços IPTV, os requisitos necessários para que se transmita esses dados com a devida qualidade e suas relações com a importância do uso protocolo MPLS-TE para provimento de uma rede mais otimizada para adequação deste serviço.

3. INTERNET PROTOCOL TELEVISION (IPTV)

O novo conceito de IPTV surgiu quando foram possíveis e viáveis os serviços de voz, vídeos e dados trafegarem juntos na mesma infraestrutura de internet já existente. A partir daí ofereceu-se uma nova plataforma de serviço, a transmissão de conteúdo televisivo "ao vivo" pela rede lógica.

Este serviço se torna diferente dos modelos de televisão existentes pelo fato de que há a possibilidade de interatividade e controle de conteúdo personalizado grande com os telespectadores. Além disso, possibilita outros serviços já oferecidos pelos servidores, como o *VoD* (vídeo sob demanda). Porém, como o serviço *tripleplay* se mostra bem mais sensível aos requisitos de qualidade da rede como, por exemplo, o *delay, jitter* e etc, obriga-se a revisão de toda a infraestrutura de configuração da rede para que não haja degradação deste novo serviço.

Esta revisão se enquadra na implementação de protocolos que garantem qualidade de serviços de forma eficiente, resiliente e otimizado com engenharia de tráfego de rede.

O *IPTV* é um sistema multimídia no qual canais de TV digital são disponibilizados através de uma rede IP, mantendo um nível satisfatório de QoS (Quality of Service) e QoE (Quality of Experience). A QoE refere-se à percepção do usuário sobre a qualidade de um serviço *IPTV*. "Uma rede de distribuição que atenda seus clientes com essa modalidade de serviço, acrescida dos serviços convencionais de dados e voz, é conhecida como *triple play*". (Lee, 2007, apud Follador Neto, Arlindo, 2009).

Os termos *Internet TV* e *IPTV* são muitas vezes utilizados como sinônimos, uma vez que ambos são serviços que fornecem conteúdo de vídeo tanto em tempo real como em tempo não real, transmitem o conteúdo de vídeo em multicast e a rede *IP* (Internet Protocol) é utilizada como meio de transporte do conteúdo de vídeo. Contudo, na realidade são termos que descrevem dois tipos de serviços diferentes. O conceito apresentado, de acordo com Altged et al, Taylor & Francis Group identifica essas diferenças.

> "O que diferencia estes dois serviços é o fato do serviço Internet TV necessitar de um computador e uma aplicação de mídia para o usuário final poder visualizar o conteúdo de vídeo enquanto que o serviço *IPTV* apenas requer um *STB* (Set-Top-Box) para decodificar o conteúdo mídia e permitir a visualização do conteúdo de vídeo

> diretamente na televisão. Outra diferença encontra-se na qualidade da imagem, pois o serviço *IPTV* oferece uma qualidade de imagem muito superior à do serviço Internet TV". (Altgeld et al, 2005, Taylor & Francis Group,2007, apud Follador Neto, Arlindo, 2009).

Uma das vantagens trazidas pela transmissão de televisão através da rede de dados é justamente a possibilidade de grandes transferências de arquivos e a sua seleção. Por isso, representa um novo paradigma ao passar todo o controle de interatividade para o cliente final.

Por outro lado, há algumas limitações deste serviço que se faz necessário observar como, por exemplo, a perda de pacotes na rede distribuidora dos pacotes, acarretando numa degradação natural da imagem. Além disso, as configurações devem estar alinhadas a suprirem dificuldades dos *codecs* (programas que codificam e decodificam arquivos de mídia, favorecendo a compactação para armazenagem), das grandes distâncias físicas e etc.

A implementação desse serviço pode ocorrer de formas variadas, porém dentro de sua arquitetura, existem elementos comuns que sempre estarão presentes. O foco deste trabalho está na camada de rede de distribuição, onde teremos que aplicar a qualidade de serviço adequada para distribuir o conteúdo de forma otimizada.

3.1 Padrões, Arquitetura e Protocolos.

Para que se crie um sistema de televisão sobre IP, é preciso que sua arquitetura esteja separada em algumas camadas necessárias para agrupamento de serviços e arquivos bem definidos. Atualmente, essas camadas são cobertas por padrões, refletindo em um esforço de interoperabilizar vários sistemas IPTV do mercado.

Os padrões são especificamente entendidos como codificação dos vídeos que serão enviados. A entrega de serviços de multimídia, tanto interativas quanto personalizadas, são objetos de padronização por várias instituições, como por exemplo, *International Telecommunication Union-Telecommunication* (ITU-T) e *Open IPTV Forum*. (Yarali,A and Cherry, A, 2005).

A instituição ITU-T possui um grupo formado para realizar a missão de padronizar globalmente serviços de IPTV. Esse grupo tem por base a arquitetura cliente-servidor com o adicional de plataforma de entrega de serviços, considerando as

áreas de registro de direitos digitais, qualidade de serviço (*QoS*) e qualidade de experiência (*QoE*). A qualidade de serviço se apresenta como um conjunto de atividades que garantem a otimização da rede lógica para entrega dos pacotes IPTV, em função de perda de pacotes, velocidade de entrega e atraso fim-a-fim. Dentre essas atividades, enquadram-se desde implementações de protocolos específicos como o MPLS e os protocolos *Multicast*, até políticas de priorização de tráfegos ou arquiteturas de serviços integrados e diferenciados. Já a qualidade de experiência, traduz todos os esforços técnicos aplicados na rede através da percepção global do usuário desse serviço.

Uma instituição muito importante e inserida no processo dessa padronização é TISPAN (*Telecoms & Internet Converged Services & Protocols for Advanced Networks*) que é um grupo de trabalho do ETSI (*European Telecommunications Standards Institute*), onde definiu o serviço IPTV como próxima geração de redes, ou seja, NGN (*Next Generation Networks*). Outra importante contribuição desse processo está na inclusão por parte do *Open IPTV Forum* das arquiteturas de rede legadas, integralizando a totalidade das redes cabeadas (Zeadally,S and Moustafa,H, 2011).

Uma importante ação para provimento do IPTV é o empacotamento dos conteúdos pelos provedores deste serviço, a fim de minimizar a quantidade de dados existentes em arquivos de vídeos. As camadas superiores do modelo são responsáveis por serviços diversos, como codificação de vídeo e empacotamento de conteúdo. Os níveis mais baixos deste modelo são responsáveis pelo transporte de funções direcionadas como roteamento, endereçamento controle de fluxo e entrega física. (OBARIDOA, et al. 2009).

Para a transmissão de serviços IPTV, faz-se menção importante ao DVB (*Digital Vídeo Broadcast*), documento padrão que especifica os primeiros intentos de especificação para transmissão de vídeos e rádios ao vivo, possuidores ou não de interações para seu controle. O *codec* (algoritmo de codificação) mais aceito popularmente e aberto para melhorias é o MPEG-2 *Systems* (tecnologia de compressão de vídeo), onde é focado na combinação de fluxos elementares de áudio e vídeo produzidos pela arquitetura IPTV. Entretanto, o MPEG trabalha em diferentes especificações bastante relevantes para o IPTV como o MPEG-E, MPEG-7 e o MPEG-21. Além disso, possui uma vertente em consideração ao melhoramento na gestão de recursos de multimídias para consumo, proteção e criação (Zeadally,S and Moustafa,H, 2011).

A arquitetura de uma plataforma de IPTV pode se enquadrar nas seguintes camadas:

1) Uma rede doméstica (*home network*): Essa rede está do lado do usuário onde possui um equipamento *Gateway* (máquina que interliga redes) servindo como uma espécie de modem para conectar um ou mais Set-Top-Boxes (conversores), para então decodificar canais de IPTV para exibição e controle no acesso;

2) Uma rede de acesso (*access network*): A rede de acesso serve como fornecedor da conectividade para a rede doméstica dos usuários. Nessa rede são encontrados os equipamentos de camada de enlace como *switches* de redes *Ethernet* a fim de executar funções melhoradas de interoperabilidades, suporte a protocolos de multicast e etc. Existem várias técnicas de acesso como opção de linha de assinante digital de alta velocidade (*SW VDSL*);

3) Redes de agregação regional: São redes representadas por grandes provedores de dados, ou seja, rede constituída por uma grande malha de equipamentos de comunicações de pacotes ou dados, principalmente da camada de rede. Esses equipamentos são principalmente representados pelos roteadores capazes de interligar sistemas autônomos de outras redes facilitando os tráfegos de informações.

A figura 5 demonstra a representação de uma arquitetura básica de uma rede IPTV.

A partir dela, pode-se identificar claramente cada uma das camadas básicas que uma arquitetura ou plataforma da tecnologia IPTV precisa para poder oferecer serviços de vídeos.

3.2 Funcionamento da tecnologia IPTV

Nesta seção são apresentados alguns pontos chaves necessários ao entendimento sobre o funcionamento desta nova tecnologia. Semelhante à transmissão de sinal através de satélites ou a cabo, o IPTV é enviado com uma linha digital de alta velocidade.

A figura 6 demonstra o sentido do fluxo de uma transmissão de sinal IPTV, iniciando com o centro de dados que recebe os metadados (dados referentes a outros dados) de seu gerador com os áudios, vídeos e dados. Após a solicitação de uma

conexão, o fluxo é enviado através do roteador de borda, atravessando toda a extensão do provedor até chegar ao destino final, onde possui um decodificador do sinal para acesso das imagens de alta qualidade.

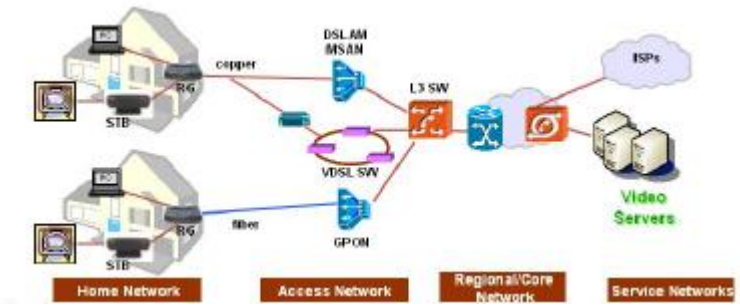

Figura 5: Arquitetura de uma rede IPTV.

Fonte: Wang, Ya.,et al, 2010.

A simulação da pesquisa se deterá a estudar tráfegos inseridos na rede regional de agregação, ou seja, na rede "core" de dados. Será feita uma simulação da capacidade requerida ao provedor por parte da empresa em estudo e inserção posterior dos tráfegos IPTV para análise de capacidade. Será analisado se o roteador localizado na borda da localidade estudada terá capacidade de transmissão desse novo fluxo de dados, garantindo os mínimos requisitos de qualidade de serviço para o adequado funcionamento.

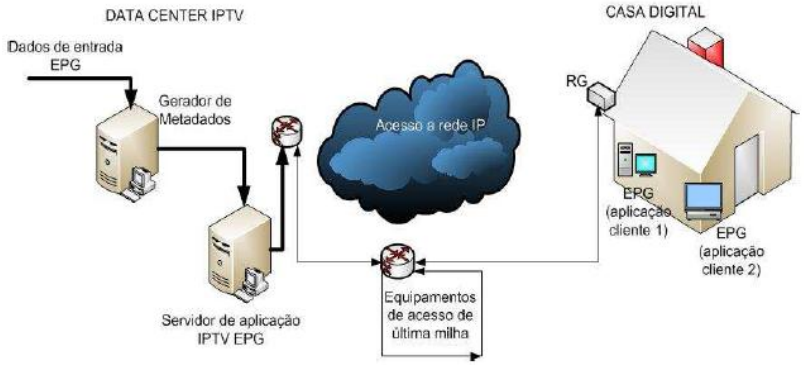

Figura 6: Fluxo de transmissão IPTV.

Fonte: O'Driscoll, 2008

Apresentada a arquitetura básica de IPTV, é necessário que se faça menção a alguns conceitos chaves sobre entidades necessárias ao funcionamento desta tecnologia.

1- Central de Dados (*IPTV Data Center*)

A central de dados de IPTV é responsável pelo processamento e preparo do conteúdo para distribuição. Tal estrutura conta, não só com switches e roteadores, mas também com servidores de armazenamento necessários para suportar os serviços de vídeo, programação, com base local e etc. (Agrawal; Bisdikian; Lee, 2007). A central recebe conteúdo de uma variedade de fontes: vídeo local, conteúdos agregadores, conteúdo de produtores, canais terrestres, satélite e cabo (Minoli, 2008). A central de dados IPTV tem sua localização ditada pela infraestrutura de rede usada pelo provedor de serviços. (O'Driscoll 2008).

2- Redes de transporte

A rede de transporte é de fundamental importância para transmissão de pacotes oriundos da tecnologia IPTV. Isto se deve pelo fato da existência de múltiplas formas de implementação dos protocolos disponíveis para garantir a qualidade de serviço e consequentemente a qualidade de experiência para o usuário final. No caso de grande emprego de IPTV, o número de conexões *one-to-one* aumenta significativamente e as demandas, em termos de largura de banda na infraestrutura de rede, podem ser bem grandes. (Han; Nehib,2008).

3- Set-top-Box

Pode-se entender como um equipamento que tem a funcionalidade de decodificar os sinais de televisão. São provedores da conectividade entre a TV e o acesso às redes banda larga de internet. Dos diversos dispositivos de consumo que estão disputando uma cota do emergente mercado de IPTV, hoje a maior parte das implantações de uso residencial ou corporativo são os gateways IP e os set-top-boxes. (Graziano, 2009).

4- Redes Domésticas

A rede doméstica possibilita a conexão da tecnologia IPTV entre os diversos equipamentos eletrônicos disponíveis do usuário final. Neste caso, a rede é representada pela intranet da empresa, onde possui uma malha complexa entre todos seus prédios de funcionamento administrativo e operacional.

5- Protocolos Utilizados

A Qualidade de Serviço pode ser alcançada por diversas técnicas e protocolos implementados. As principais são através das arquiteturas IntServ (*Integrated Services*, solução que provê QoS com a reserva de recursos com o protocolo *RSVP* – Resource Reservation Protocol), na qual é garantida através de mensagens nativas do protocolo *PATH* e *RESV* trocadas por toda a extensão do circuito com QoS (todos os equipamentos devem possuir recursos para este tipo de conexão). Isto é feito com um controle de admissão que verifica se a rede possui condições necessárias para tal investida. Em grandes grupos com *multicast* implementados, a reserva pelo protocolo RSVP é realizada a partir do destinatário onde o Set-Top-Box efetuaria a solicitação compatível com suas necessidades. Já na arquitetura *DiffServ* (Differentiated Services, solução com priorização de pacotes), o fluxo de dados ou os pacotes são selecionados em prioridades através do campo DSCP (*Differentiated Services Codepoint*), ou seja, não há reserva de recursos da rede como no IntServ, apenas prioriza os pacotes que irão trafegar. Esse mecanismo se torna uma implementação mais simples e escalável, pois pode-se tratar pacotes de diferentes fluxos de dados. Diante da política de informação das empresas, essa arquitetura se torna bem gerenciável. A solução DiffServ está definida pelo IETF através da RFC 2475 (Reis, B. and Sodré, M, 2012).

O *Multiprotocol Label Switching* se tornou uma tecnologia largamente utilizada por empresas provedoras de serviços e grandes corporações que implementam redes WAN's (*Wide Area Networks*). Isto é possível, pois implementa uma técnica de comutação de pacotes através de pequenos *labels* (rótulos), possibilitando encaminhamento mais rápido entre os nós, evitando pesquisas gigantescas de endereçamento IP em tabelas. Outra grande vantagem do MPLS vem da sua possibilidade de encapsular pacotes de diversos protocolos de rede, suportando uma variedade de tecnologias. Além de servir como mecanismo para engenharia de tráfegos de rede, simplifica a função dos roteamentos e diminui drasticamente o *overhead* e latência dos pacotes.

O MPLS, juntamente com as tecnologias e protocolos presentes nas duas arquiteturas citadas, atuam de forma complementar, agregando vantagens do roteamento e da comutação, onde cabe ao administrador escolher a priorização e tecnologia para sua configuração de melhor rendimento da aplicação.

Como consequência da aplicação de qualidade de serviço na rede, surge um conceito muito importante chamado QoE (*Quality of Experience*), ou seja, traduz a percepção do usuário com base nas experiências obtidas anteriormente nessas

aplicações. Apesar de a QoE ser bastante subjetiva, existem parâmetros numéricos e estatísticos acerca desses fluxos ao longo da rede capazes de indicar o limite superior ou inferior da qualidade esperada. Os requisitos mais relevantes de QoS capazes de demonstrar e indicar esses limites, são o *troughput* (consumo de banda pela aplicação), *delay* (tempo máximo de entrega origem – destino), *jitter* (variação no retardo da entrega) e perda de pacotes (limites de tolerância para a aplicação).

De acordo com a tabela 1, os requisitos para que se assegure uma boa QoE nas diferentes categorias de aplicações IPTV são os seguintes (Barros, *apud* Mello, 2011):

Tabela 1: Serviços e requisitos de vazão, delay, jitter e perda de pacotes.

Serviços/Requisitos	Vazão	Delay (s)	Jitter (s)	Perda de pacotes (%)
VoD	384Kbps até 1,5Mbps	4 e 5 (s)	300ms	<0,1%
Vídeo (IPTV)	1 Mbps	3 e 5 (s)	30ms	<0,5%
Videoconferência	64Kbps até 8Mbps	150ms	30ms	<0,5%
Voz (Telefonia)	90Kbps	150ms	<=150ms	<=0,25%

O requisito vazão varia em função do codificador que é utilizado na aplicação, por exemplo, o MPEG-2 necessita em média de 4 Mbps por canal SDTV. Já o MPEG-4 utiliza 2 Mbps por canal. A perda de pacotes se torna muito relevante na análise uma vez que esse requisito compromete diretamente na qualidade de transmissão. Por isso, a porcentagem menor que 0,5% se torna satisfatória sem grandes prejuízos para aplicações *IPTV*.

A qualidade de serviço é mantida quando os valores desses requisitos acima não são ultrapassados. Quando os requisitos mínimos são atingidos, há uma boa transmissão deste serviço, com uma qualidade satisfatória para o cliente final e consequentemente há uma boa qualidade de experiência, perceptível nas imagens, nos sons e no restante dos dados enviados.

No quarto capítulo, será apresentado o estudo de caso referente à empresa corporativa Vale S.A, uma das maiores mineradoras do mundo e muito influente no mercado de minério de ferro. Além disso, será feito um detalhamento das etapas da metodologia utilizada para realização da simulação e testes da rede de dados da empresa, demonstrando sua topologia com arquitetura MPLS e dados dos requisitos fornecidos pela sua provedora.

4. ESTUDO DE CASO

No estudo de caso proposto neste trabalho, será apresentada a forma estrutural da área responsável pelo gerenciamento da rede como um todo, englobada por uma área de negócio chamada TI de uma empresa multinacional que possui escritórios em várias localidades do Brasil e do mundo. Além disso, será apresentado o histórico e a evolução da implantação do protocolo MPLS e da engenharia de tráfego através dos SLA's para interligar esses sites corporativos, analisando a estrutura atual desta tecnologia, correlacionando com a parte gerencial. Por fim, serão apresentadas duas ferramentas (NS2, NS2 Analyzer e TraceGraph*)*, utilizadas para demonstrar a emulação dos cenários extraídos da própria realidade da empresa, os serviços implementados com a tecnologia MPLS-TE, suas configurações e as análises de pacotes de tráfego desta rede que serão capturados.

4.1 Evoluções da estrutura de telecomunicações da empresa

Na década de 80, mesmo com unidades de negócios espalhadas geograficamente pelo país, a empresa analisada não possuía meios eletrônicos de comunicação, controlando todos seus processos por meio de documentos oficiais, principalmente através de malotes de correios. Com o advento do avanço na telefonia, passou-se a utilizar um sistema de conexão de máquinas de escrever elétricas a uma rede telefônica, chamado Telex.

Por isso, o único *link* de dados era utilizado através desta ferramenta, o que limitava muito a quantidade de informações que se pretendia trafegar. Paralelo a isso, os links de voz existentes ainda resistiam em serem os principais meios de comunicação e de informações, uma vez que a central de telefonia com toda a sua infraestrutura era gerida e administrada pela própria empresa.

Com o passar do tempo, a empresa se expandiu, tornando-se necessária a implantação dos mainframes (computadores de grande porte) de informações em cada localidade, que passaram a ser ligados ponto-a-ponto através de um sistema de rádio de frequência analógico, com faixas de frequências do tipo SHF (*Super High Frequency*). Esse sistema continha uma antena capaz de capturar os sinais analógicos e um multiplexador em cada lado da conexão, distribuindo esses sinais para os modems transformarem em sinais digitais. Por atravessar por toda essa infraestrutura, as taxas de

transmissão para o tráfego eram muito baixas entre as localidades que possuíam esses mainframes.

Por ser utilizada uma estrutura de mainframe principal, ainda não existia a ideia de hosts (computadores pessoais), utilizando-se apenas os terminais burros (terminais com funcionalidades limitadas) que operavam como se estivessem diretamente neles.

Após o sistema de rádio, foi adotada a ligação com fibra óptica na década de 90, quando as antenas responsáveis pela captura dos sinais foram substituídas pelos conversores eletro-ópticos, juntamente com os multiplexadores digitais. Porém os links continuaram a ser diretos e toda essa infraestrutura continuava a ser provida pela própria empresa.

Com o avanço da tecnologia e o oferecimento de uma melhor infraestrutura, a empresa passou a contratar links de telecomunicação, pagando por altos valores para provedores desse serviço (justificados pela novidade tecnológica da época), devido à grande dispersão geográfica dos sites no país. Com isso, foram criadas as redes locais, com servidores locais, em que se rodavam aplicações também locais (não possuíam aplicações padrão para todos os sites) no modelo cliente-servidor, gerando o deslocamento do mainframe de informações para a sede da empresa.

Com o crescimento da empresa e do número de clientes que passaram a utilizar a informática como ferramenta de trabalho, a área de Tecnologia da Informação (TI) ganhou uma importância maior e houve a necessidade de se criar uma área (gerência) que intermediasse todas as necessidades dos empregados, com a implementação de novas aplicações e de novos equipamentos de telecomunicações, a fim de atender a demanda, a qualidade e a continuidade dos serviços.

Em consequência disso, a gerência de projetos de TI alavancou toda a infraestrutura da empresa e o número sistemas, causando um “boom” de mais de 300 novas aplicações, gerando, assim, uma quantidade muito grande de acessos por parte dos empregados aos servidores. Isso era feito de forma desordenada e isolada do resto das unidades de negócios, atendendo apenas as necessidades locais. Em contrapartida, foi observada uma consequente lentidão contínua na rede, justamente por esse crescimento, apontado como principal motivo do gargalo.

Na tentativa de acabar com o gargalo no número de aplicações que eram desenvolvidas de forma separadas, foi feita a adoção e a implantação de um sistema único, muito grande e segmentado por módulos, em que as principais aplicações de várias áreas de negócios da empresa (recursos humanos, financeiro, sistemas

operacionais, voz sobre IP) pudessem ser atendidas por qualquer site distribuído pelo mundo. A partir daí, esse novo sistema passou a ter um nível muito alto de criticidade, pois qualquer falha significaria uma perda considerável de trabalho e de rendimento. Por isso, a área de telecomunicações da empresa passou a ser vista como ponto crítico de seu funcionamento. Porém, como a estrutura do Data Center era centralizada na sede e havia apenas um único canal para acessar essas aplicações, gerou-se um problema de tráfego difícil de ser diagnosticado.

Uma das medidas, para que o problema desse gargalo na rede pudesse ser sanado, foi a adoção de uma política de hospedar as aplicações em um Data Center, ou seja, replicar virtualmente em uma localidade diferente, forçando a distribuição de acesso entre a sede e o novo centro de processamento. Além dessa solução, observou-se a necessidade de ajustar o contrato com a provedora do link de comunicação, com a finalidade de garantir uma qualidade de serviço para links específicos, restritos e críticos, indicados pela empresa. Com isso, foi feito um mapeamento de todos os processos prioritários e não prioritários, apontando quais aplicações necessitariam de implementações de qualidade de serviços, a fim de firmar os *SLA's* correspondentes.

Consequentemente à implantação de uma réplica do Data Center, os sites mais distantes geograficamente pelo país passaram a se interligar através da VPN/MPLS (nuvem MPLS), administrada pela provedora. De forma equivalente, os sites localizados em regiões fora do país, se interligam através da nuvem MPLS internacional, administrada por uma empresa provedora internacional.

Atualmente a empresa possui uma infraestrutura de contingência lógica e física, ou seja, existem dois *links* principais providos por empresas diferentes. Fisicamente, ela ainda não implantou esta redundância, consistindo apenas em um *switch-core*. Como os principais links atualmente são implementados com a tecnologia MPLS, a área gestora de TI monitora todos os enlaces através de um aplicativo gráfico, chamado *Cacti* (é uma ferramenta software livre administrativa de rede, que recolhe e exibe informações sobre o estado de uma rede de computadores através de gráficos), analisando todo o volume de tráfego nos feixes de ligações entre os *sites.*

4.2 Metodologia

A simulação se baseia na inserção de tráfegos IPTV em uma rede corporativa de dados para se avaliar tecnicamente o impacto que isto acarretará no seu comportamento

e desempenho. Trata-se de um estudo de caso de uma grande corporação para inserção de nova plataforma de serviços de tecnologia, a IPTV. O foco da implementação residirá no core provedor da rede, ou seja, nas redes de agregação da arquitetura IPTV.

Para que isto fosse viável, a metodologia utilizada para realizar este trabalho seguiu uma sequência de etapas bem definidas e dependentes entre si. A seguir, será feito a descrição de cada atividade concretizada nessas etapas.

4.2.1 Coleta de requisitos *in loco*

A metodologia do trabalho foi realizada em etapas distintas e sucessivas. A primeira etapa consistiu na coleta de requisitos e parâmetros diretamente com o responsável pela gestão técnica da infraestrutura de TI (Tecnologia da Informação) e pela gestão do SLA (*Service Level Agreement*) com o provedor de serviços. Entre esses requisitos, está a topologia utilizada pela empresa para prover o *link* do *backbone* (rede de transporte), figura 7, a largura de banda utilizada nos principais enlaces, localização da nuvem *MPLS* e os tráfegos que mais são utilizados na carga total de banda passante da rede.

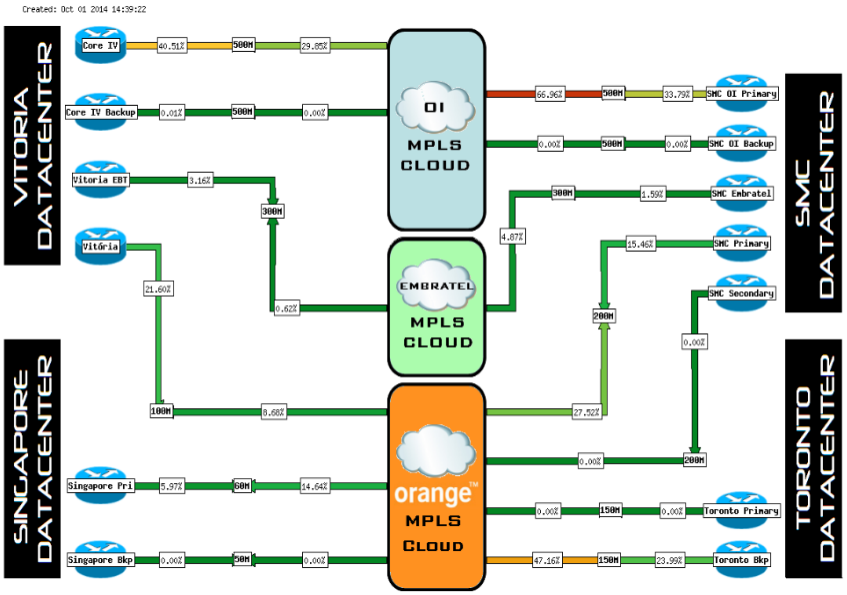

Figura 7: Topologia Corporativa.

Fonte: Vale S.A

A topologia vista na figura 7 demonstra os principais roteadores de borda dos principais centros de dados que incluem rótulos antes de chegar à nuvem MPLS até

chegar seus destinos. Além disso, mostra também a capacidade e carga de cada link provido pelas empresas contratadas para atender essa demanda.

Os requisitos de maior relevância para a simulação desta topologia são: largura de banda que interliga duas localidades principais da empresa, tipo de tráfegos mais utilizados pelos funcionários, eficiência dos serviços oferecidos pela provedora de telecomunicações, horário de maior tráfego de dados da empresa e etc.

A coleta dos dados da rede foi realizada por amostras em determinados intervalos de tempo e com uma frequência de semanas para avaliar qual variação existia durante o tempo medido. A figura 8 mostra um gráfico extraído pela aplicação de monitoramento da rede em um determinado horário de maior fluxo de dados. Um dos mais relevantes requisitos coletados está na vazão do link principal da rede de São Luís. O que foi relatado pelo gerente de tecnologia da informação é de que o principal gargalo encontrado atualmente pelos gestores é que o tráfego intenso de vídeo apresenta picos de grandes volumes de pacotes.

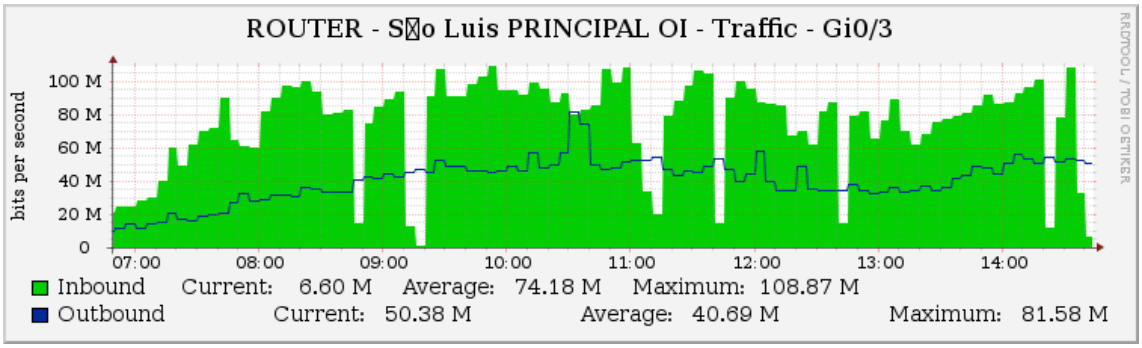

Figura 8: Tráfego de dados.

Fonte: Vale S.A

A figura 8 nos mostra que há um determinado tempo que a rede sofreu um aumento na transmissão de seu volume de dados, chegando a quase 70% de sua capacidade, o que confirma a informação obtida anteriormente.

Essa informação se torna muito relevante para implementação da simulação, pois poderão ser inseridos tráfegos oriundos de vídeos e dados juntos até o limite de ocupação mencionado, independentemente da largura de banda do link que será codificado. Protocolo utilizado para interligar a rede da empresa com seu *backbone* também foi apresentado como requisito necessário à pesquisa. O MPLS é a principal

tecnologia utilizada pelos provedores do link de interligação, tanto o principal (representado pela empresa Oi) quanto pelo link secundário ou de backup (representado pela empresa Embratel).

4.2.2 Ferramentas Utilizadas

Para a codificação e simulação da rede da Vale S.A, foi escolhida a ferramenta chamada NS2, versão 2.35 *standallone*. A escolha da ferramenta utilizada baseou-se na possibilidade de implementação de maior aproximação entre a rede real e a computacional através da execução por eventos discretos. Segundo Pereira (2009), em uma simulação discreta, considera-se somente os eventos onde há alteração do sistema, ou seja, o tempo decorrido entre alterações do estado do sistema não é relevante para obtenção dos resultados da simulação, embora o tempo nunca pare. Por isso, a maior vantagem neste modelo é a capacidade de simular e analisar por um curto período de tempo, os eventos mais relevantes no tráfego da rede, que neste caso seria o comportamento após a inserção dos novos tráfegos IPTV.

O network Simulator é uma ferramenta resultante de um projeto chamado VINT (*Virtual InterNetwork Testbed*), composto pelas instituições DARPA, USC/ISI, Xerox PARC, LBNL e também pela Universidade de Berkeley. Uma grande vantagem está no fato da possibilidade de adaptação a qualquer situação de rede, pois é uma ferramenta *freeware* e de código fonte aberto. Além disso, ela permite a implementação de uma gama muito grande de tecnologias, entre elas a sem fio e a engenharia de tráfego como o protocolo RSVP.

A ferramenta NS-2 é executada no ambiente Linux/Unix, mas também é possível ser executado no ambiente Windows através da utilização da aplicação *Cygwin*. O componente *xgraph* corre na plataforma Unix com o XWindows, no entanto, o suporte para esta componente no Windows não está disponível (Rodrigues, 2009).

Para melhorar a eficiência do tempo de simulação, este simulador utiliza a linguagem de programação C++ para implementar os modelos de objetos e a programação de eventos. O usuário define e configura os detalhes da rede tais como a topologia, as aplicações, os tipos de tráfego, os pontos de início e fim das simulações e outros parâmetros. Utiliza também a linguagem *Object* Tcl (OTcl) que não necessita de ser compilada. Assim, são utilizadas duas linguagens, a linguagem C++ que permite criar e personalizar a arquitetura do protocolo e a linguagem OTcl que é utilizada para

variar os parâmetros e configurações da simulação de uma forma fácil. (Rodrigues, 2009).

A simulação do NS-2 cria um arquivo tipo ficheiro chamado *trace* que contém a informação detalhada da topologia e todos os eventos ocasionados ao longo do caminho dos pacotes, sendo demonstrados de forma gráfica e dinâmica no ambiente de animação chamado NAM. O NAM (*Network Animator*) [Chung et al, 1999] é uma ferramenta de animação para visualizar os *traces* da simulação. Desta forma a visualização em tempo real não é possível. O pacote de *software* NS-2 contém uma componente opcional chamada *xgraph*. Este componente é um programa utilizado para criar representações gráficas dos resultados de simulação. A análise do ficheiro *trace* pode ser efetuada através da linguagem Perl ou da linguagem AWK.

A arquitetura do simulador pode ser ilustrada na figura 9 a seguir, onde são mostradas as diferentes camadas de execução das linguagens.

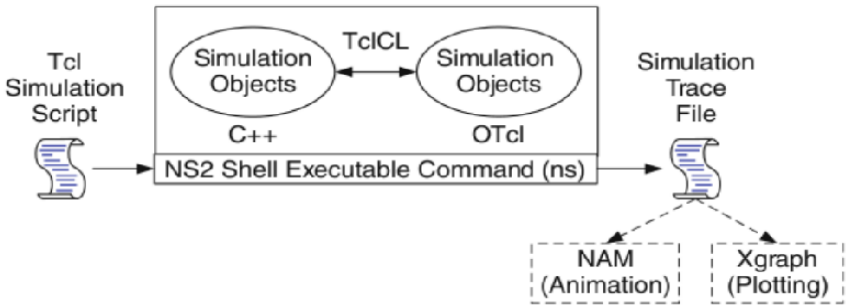

Figura 9: Arquitetura da ferramenta NS2.

Fonte: Coutinho, 2012

A topologia, tipos de tráfegos e programação de execução da simulação são feitas através da linguagem declarativa chama OTCL desenvolvida pelo MIT (Massachusetts Institute of Technology). Após esta camada, o arquivo do tipo .tcl é chamado por um comando do tipo ns para execução no simulador. Este comando monta toda a estrutura codificada anteriormente e registra cada milissegundo da simulação, onde existem todos os eventos dos pacotes enviados e recebidos, com pacotes transmitidos, perdidos, tipos de protocolos utilizados, roteadores ativos, rotas explícitas

e etc. Este ficheiro possuidor de todas essas informações é chamado pelo animador gráfico NAM e de forma gráfica pode-se observar toda a simulação que mantém sua execução pelo tempo descrito e seus pacotes oriundos dos diferentes protocolos são visualizados desde a sua origem até seu destino final.

Entretanto, os pacotes descartados ao longo do trajeto ou em filas e gargalos nos roteadores em pontos de acesso também são percebidos graficamente. A figura 10 mostra um exemplo de arquivos gerados pelo simulador após a execução. O arquivo é dividido em colunas, onde cada uma delas significa alguma característica do comportamento da rede em cada milissegundo.

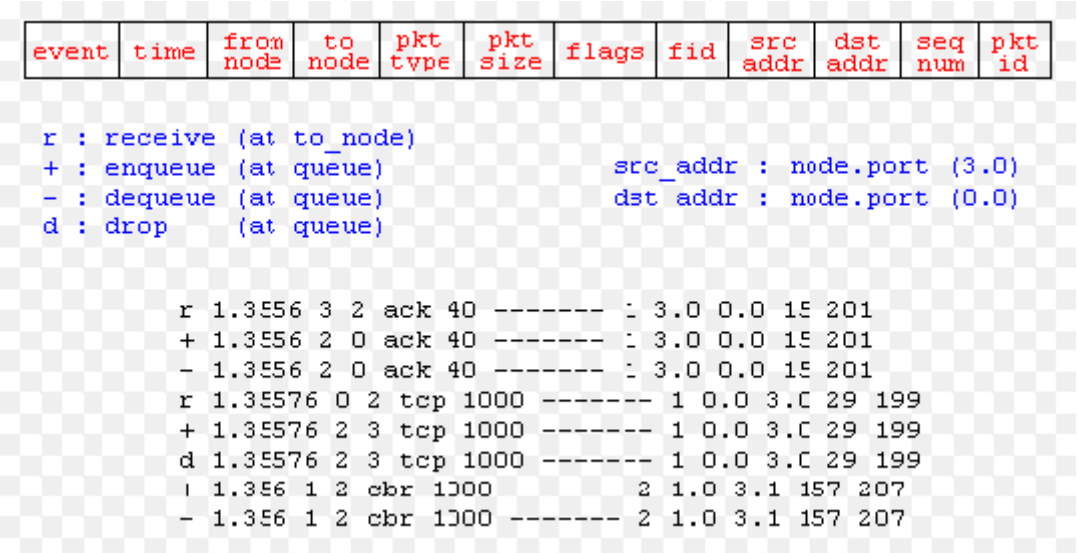

Figura 10: Exemplo de arquivo trace.

O primeiro campo identifica o tipo de operação (evento) naquele determinado tempo, onde há possibilidade de ser recebimento, enfileiramento ou perda. O segundo campo identifica o tempo correto deste evento. A seguir há a identificação do nó de origem, nó de destino, o tipo de pacote, as etiquetas utilizadas pelos protocolos, a sequencia de números dos pacotes e a identificação de cada pacote na rede.

Este arquivo possui um grande volume de dados, onde ferramentas específicas são capazes de realizarem a leitura correta para a construção de gráficos e cálculos sobre requisitos de qualidade de serviços da rede simulada.

Para essas leituras técnicas, foram utilizadas duas ferramentas específicas. Uma chamada *NS2 Analyzer* que ofereceu todos os números referentes aos requisitos de QoS pertinentes e necessários para os resultados da pesquisa. Além dessa, o *TraceGraph* foi

utilizado para construção de gráficos que auxiliaram na conclusão da evolução dos fluxos durante o tempo de simulação. O arquivo *.tr* possui uma estrutura matricial, por isso, essas duas ferramentas auxiliares suportam as bibliotecas do MATLAB específicas para este tipo de arquivo.

Por isso, as ferramentas *NS2 Analyzer e TraceGraph*, foram utilizadas no trabalho, de forma complementar para que os dados estatísticos e gráficos fossem gerados com maior facilidade e acessibilidade analisando os ficheiros de *trace*.

Apesar da ferramenta *NS2 Analyzer* se mostrar como uma poderosa aliada na simulação e amplamente utilizada, os dados a serem analisados ainda não possuem fácil interpretação. Esta ferramenta se torna fundamentalmente importante para complementar a simulação, pois o NS2 não possui e fornece quaisquer gráficos e dados estatísticos a respeito dos pacotes de forma nativa. Para isso, há a necessidade de implementação através da codificação da linguagem tcl ou scripts awk capazes de construir gráficos específicos, porém subjetivos.

NS2 Analyzer foi desenvolvido pelo laboratório de comunicações e telemática (LCT) do Centro de Informática e Sistemas da Universidade de Coimbra com o objetivo de ser bem amigável, simples e autônomo, porém com análises complexas em relação aos fluxos registrados pelos arquivos de *trace*.

A figura 11 abaixo ilustra a interface da ferramenta onde há o local de inserção do arquivo de simulação *trace*.

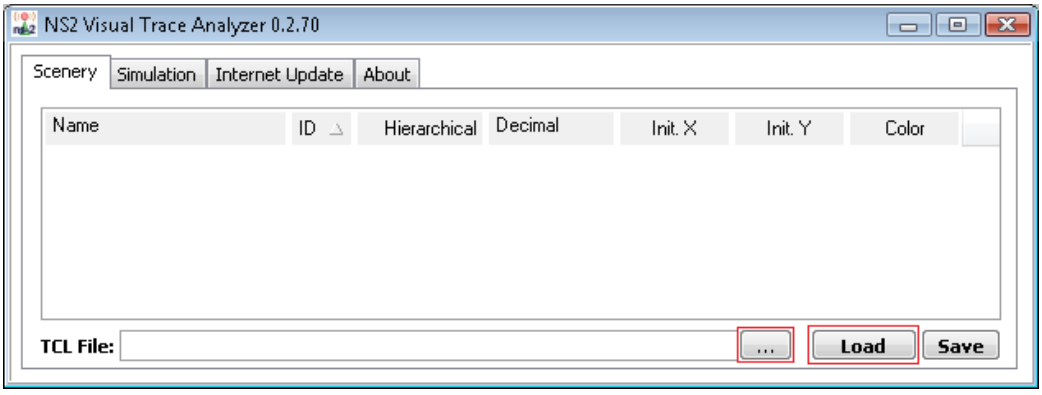

Figura 11: Interface da ferramenta NS2 *Analyzer.*

Fonte: Rocha, 2010

Após a inserção e leitura do arquivo de simulação, a ferramenta gera o cenário e propriedades estatísticas sobre todos os fluxos dos pacotes gerados e recebidos. A figura 12 ilustra as propriedades descritas na ferramenta.

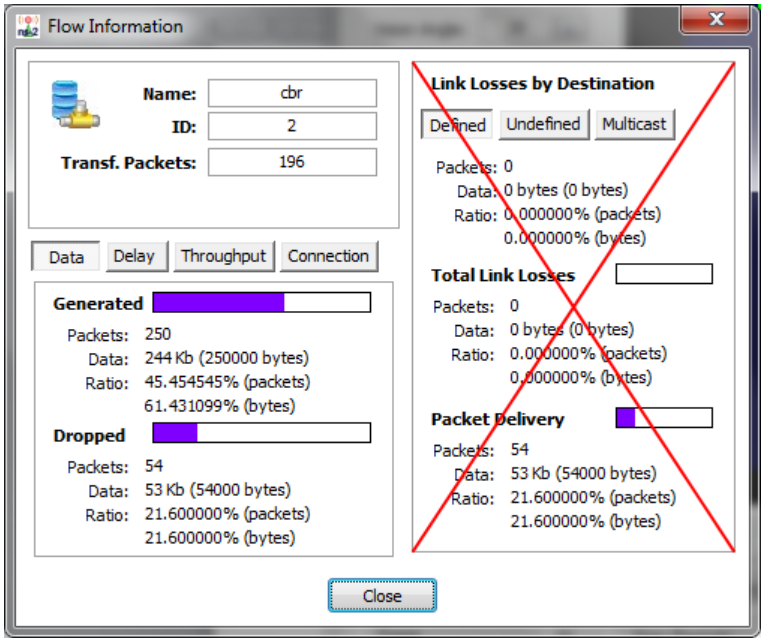

Figura 12: Exemplo de dados estatísticos de cada nodo.

Fonte: Rocha, 2010

Após a etapa de escolha das ferramentas que serão utilizadas, inicia-se a etapa de execução com a codificação e geração de resultados. A seção 4.2.3 seguinte detalhará essa fase.

4.2.3 Execução

De posse dos requisitos relevantes e da escolha da ferramenta, a última etapa da metodologia de trabalho se concretizou com a execução da simulação e com análises dos ficheiros com os respectivos resultados.

Foram construídos vários gráficos sobre os tipos de tráfegos que trafegaram conjuntamente pela rede durante a simulação. Com base nesses gráficos e cálculos realizados acerca dos parâmetros de QoS, foi possível a interpretação do comportamento da rede sobre a degradação ou não de outros serviços e dados ao longo do aumento no fluxos de IPTV.

Após as ações anteriores, será feito um detalhamento sobre a codificação da topologia e dos fluxos, ilustrando como foi construída toda a rede através da linguagem declarativa da ferramenta, sua capacidade, ligações entre os roteadores e programação

dos eventos. No quinto capítulo serão feitas as análises de acordo com os resultados obtidos pela execução realizada.

4.3 Codificação e geração de tráfegos

O objetivo do trabalho de simulação nesta dissertação é apresentar o comportamento da rede de uma empresa corporativa após a inserção de um novo tipo de tráfego, o IPTV ou *Triple Play*. Em contexto com as redes *Triple Play*, o encaminhamento ótimo ou quase ótimo é aquele que permite reduzir a taxa de perda de pacotes e a latência nas redes que suportam o serviço *Triple Play*.

Os serviços VoIP e IPTV pertencentes ao serviço *Triple Play* são intolerantes à perda de pacotes. Por isso, a topologia da empresa simulada ajuda a compreender o funcionamento dela está apta para se tornar uma rede *Triple Play*, com as suas exigências e seus limites. Os cenários apresentados também ajudam a perceber como o MPLS, a Engenharia de Tráfego e os métodos de enfileiramento e envio de pacotes podem melhorar o desempenho e a eficiência da rede IP existente. A arquitetura MPLS é utilizada nas simulações para obter a QoS para os clientes em redes *Triple Play*, e através da análise do seu funcionamento, é possível explicar os fatores, o desempenho, os problemas relacionados com a qualidade de serviço, as vantagens e limitações. Desta forma, as simulações permitem prever situações futuras de escalonamento de acordo com o aumento de adesões ao serviço *Triple Play* (Rodrigues, 2009).

A figura 13, ilustra a topologia utilizada na simulação já implementada na ferramenta NS2.

Os roteadores são identificados través dos números e os links pelas linhas que fazem essas ligações. Os roteadores de número 0, 1, 10 e 11 representam as localidades ou filiais da empresa. Já os roteadores que possuem o formato hexagonal representam aqueles que estão inseridos na nuvem MPLS e implementam esta tecnologia, ou seja, são através desses que irão ser trocadas as etiquetas ou rótulos de comutação.

A simulação da rede MPLS fornecida pela operadora de telecomunicações, no caso a Oi, está representada pelo conjunto de roteadores de números 2, 3, 4, 5, 6, 7, 8, 9, onde será configurado o protocolo de qualidade de serviço RSVP, trocando e alocando recursos (banda) ao longo do caminho (todos os roteadores pertencentes ao caminho) explicitado em forma de rótulos, capazes de formar um túnel reservado de capacidade, separando e balanceando a carga da rede com engenharia de tráfego.

No caso, o roteador número 2 representa a borda da rede de entrada e saída para a localidade de São Luís e o de número 8 a borda da localidade de Vitória, onde reside o *backbone* de toda a rede MPLS no Brasil.

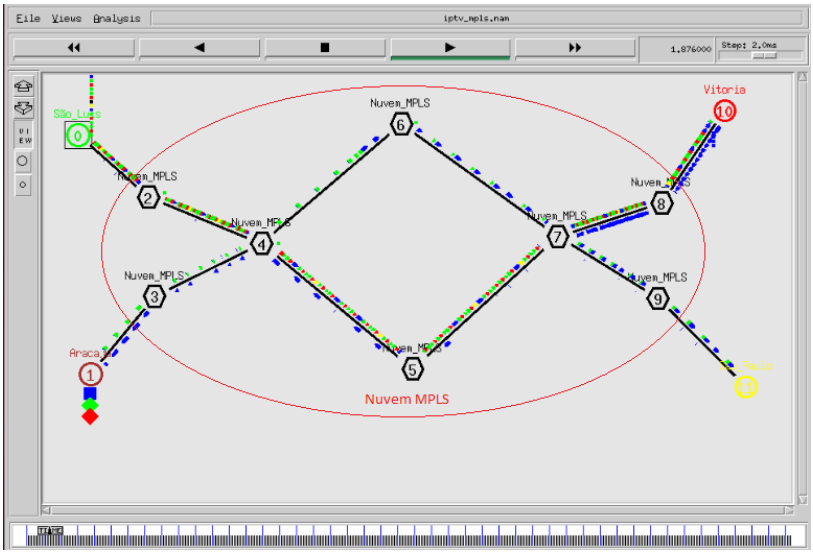

Figura 13: Topologia da empresa implementada na ferramenta.

Fonte: Lima, Filipe (2015).

É importante destacar que nesses roteadores de borda, é requerido uma capacidade de processamento bem maior devido o grande fluxo de dados que são enviados e recebidos, além da inserção e retirada dos rótulos MPLS nos cabeçalhos do pacotes IP's da rede e outros protocolos robustos para esse tipo de serviço como o *Border Gateway Protocol* (protocolo de roteamento dinâmico entre as bordas dos nós MPLS).

As linhas tracejadas e coloridas representam cada tipo de fluxo que trafegam através dos enlaces entre os roteadores, como também as filas dos pacotes e os perdidos identificados pelos quadrados em cima e embaixo de cada roteador.

A ferramenta NS2 possui um módulo chamado MNS_V2 que possibilita a criação da rede com roteadores implementados com o MPLS. Através da codificação declarativa da linguagem OTCL, é possível toda a configuração da topologia. O quadro 2 mostra os comandos utilizados para a criação dos roteadores e seus enlaces com suas respectivas capacidades e tipo de fila utilizada para envio dos pacotes.

Quadro 2: Declaração da rede e dos roteadores MPLS

Declaração da Rede

```
# Criação dos Nos da Rede e estabelecimento dos Nos de Domínio MPLS

set n0 [$ns node]
set n1 [$ns node]
$ns node-config -MPLS ON
set LSR2 [$ns node]
set LSR3 [$ns node]
set LSR4 [$ns node]
set LSR5 [$ns node]
set LSR6 [$ns node]
set LSR7 [$ns node]
set LSR8 [$ns node]
set LSR9 [$ns node]
$ns node-config -MPLS OFF
set n10 [$ns node]
set n11 [$ns node]

# Definição dos rótulos para os Nos IP e MPLS

$n0 label "São_Luis"
$n1 label "Aracaju"
$LSR2 label "Nuvem_MPLS"
$LSR3 label "Nuvem_MPLS"
$LSR4 label "Nuvem_MPLS"
$LSR5 label "Nuvem_MPLS"
$LSR6 label "Nuvem_MPLS"
$LSR7 label "Nuvem_MPLS"
$LSR8 label "Nuvem_MPLS"
$LSR9 label "Nuvem_MPLS"
$n10 label "Vitoria"
$n11 label "São_Paulo"
```

O quadro 2 mostra a criação dos roteadores juntamente com seus rótulos. A partir da declaração $ns node-config -MPLS ON-OFF, o módulo é invocado e os

roteadores MPLS declarados entre esses comandos são criados e passam a ser denominados de LSR (*Label Switch Router*), ou seja, roteadores possuidores de rótulos na rede.

Para uma simulação com mais clareza, foram adicionados os nomes de cada roteador da topologia para que se identificassem as ligações entre cada um deles. O comando para realizar esta tarefa é: $LSR9 label "Nuvem_MPLS".

Após a criação dos roteadores da rede é necessária realizar os enlaces entre eles, o que define e dá formato para a disposição desses elementos. O quadro 3 ilustra a codificação para a estruturação desses enlaces com suas respectivas capacidades e tipos de filas que serão implementadas em cada um.

Quadro 3: Codificação dos enlaces entre roteadores

```
# Definição dos Enlaces

$ns duplex-link $n0 $LSR2 20Mb 8ms DropTail
$ns duplex-link $n1 $LSR3 10Mb 8ms DropTail
$ns duplex-link $LSR2 $LSR4 20Mb 12ms DropTail
$ns duplex-link $LSR3 $LSR4 20Mb 12ms DropTail
$ns duplex-link $LSR4 $LSR5 20Mb 12ms DropTail
$ns duplex-link $LSR4 $LSR6 20Mb 12ms DropTail
$ns duplex-link $LSR6 $LSR7 20Mb 12ms DropTail
$ns duplex-link $LSR5 $LSR7 20Mb 12ms DropTail
$ns duplex-link $LSR7 $LSR9 20Mb 12ms DropTail
$ns duplex-link $LSR7 $LSR8 20Mb 12ms DropTail
$ns duplex-link $LSR9 $n11 20Mb 8ms DropTail
$ns duplex-link $LSR8 $n10 20Mb 8ms DropTail
```

A declaração primeiramente especifica o tipo do *link* entre os roteadores, declarando quais os roteadores que serão ligados juntamente com sua capacidade de largura de banda e algoritmo do tipo de fila que será utilizado.

O link é da forma duplex, ou seja, permitindo a ida e volta dos dados. A capacidade é de 20 MB para o tráfego de dado, possuindo um atraso médio de 12 e 8 ms com o tipo de fila com algoritmo *DropTail*. Este algoritmo é utilizado pela grande maioria de roteadores de internet para decisão de quando serão descartados os pacotes

da rede. Em camadas de aplicação, algumas requisições à servidores podem ser descartadas, por isso, quando a fila apresenta-se abaixo do limite pré-estabelecido ainda poderão ser aceitas, descartando somente aquelas que ultrapassarem tal limite.

O quadro 4 ilustra a definição para mensagens entre todos os roteadores do domínio MPLS. Estes comandos são importantes para que se efetuem de fato os pares para trocas dos rótulos. Cada nó pertencente ao laço *for*, será identificado como um par entre todos os roteadores implementados com a tecnologia MPLS. Isto é feito pela combinação de todos os roteadores, ou seja, os rótulos serão distribuídos a todos dentro de um conjunto de nós pré-estabelecidos e serão anexados e retirados ao longo da simulação.

Quadro 4: Implementação de pares LDP's

```
#Definição de mensagens LDPs em todos os Nós do domínio MPLS

for { set i 2} {$i < 10} {incr i} {
for {set j [expr $i+1]} {$j < 10} {incr j} {
set a LSR$i
set b LSR$j
eval $ns LDP-peer $$a $$b
}
}
[$LSR2 get-module "MPLS"] enable-control-driven
[$LSR3 get-module "MPLS"] enable-control-driven
[$LSR4 get-module "MPLS"] enable-control-driven
[$LSR5 get-module "MPLS"] enable-control-driven
[$LSR6 get-module "MPLS"] enable-control-driven
[$LSR7 get-module "MPLS"] enable-control-driven
[$LSR8 get-module "MPLS"] enable-control-driven
[$LSR9 get-module "MPLS"] enable-control-driven
```

O comando [$LSR2 get-module "MPLS"] enable-control-driven permite que os roteadores troquem rótulos de maneira de controle conduzido, ou seja, permite de forma clara e perceptível como um gatilho disparado cada rótulo inserido na rede.

Depois de feito o design da topologia e definido toda a estrutura de enlaces dos nós, é necessária a implementação dos protocolos e geração dos tráfegos entre a origem e o destino dos pacotes.

Para isso, abre-se uma conexão entre dois nós escolhidos através de agentes de conexão. Cada conexão necessita de um agente para originar o tipo de protocolo que será utilizado no envio do pacote e uma resposta diferente a esse agente. Por exemplo, o agente do protocolo TCP entre dois nós, necessita de uma resposta do tipo SINK para que haja troca de mensagens e dados entre eles. O quadro 5 ilustra esse tipo de conexão entre dois nós e a geração do tráfego.

Quadro 5: Agentes criadores de tráfego

```
#Criando a primeira conexão TCP entre os nos 0 e 10


set tcp0 [new Agent/TCP]
$tcp0 set packetSize_ 1400
set tcpsink0 [new Agent/TCPSink]
$ns attach-agent $n0 $tcp0
$ns attach-agent $n10 $tcpsink0
$ns connect $tcp0 $tcpsink0
$tcp0 set class_ 2
```

Para que o agente tcp0 [new Agent/TCP] envie dados do tipo TCP para o nó 10 é necessário que o destino possua um tipo de resposta como tcpsink0 [new Agent/TCPSink]. Além disso, o tamanho de cada pacote é descriminado através do comando $tcp0 set packetSize_ 1400.

Essa forma de geração de tráfego é utilizada com todos os protocolos suportados pela ferramenta. A seguir serão feitas algumas considerações sobre os tráfegos TCP IPTV.

4.3.1 Tráfego IPTV

O *codec* H.264 é o mais utilizado na transferência de vídeo sobre a rede IP. A sua taxa de transferência é de 384 Kbps num *stream* de vídeo de 30 *frames/s*, apresentado em (Salah et al, 2006 apud Rodrigues, 2009).

É utilizado o gerador de tráfego *Exponencial* ON/OFF para o conteúdo de IPTV. O tráfego *Exponencial* é acionado e desligado (*Exponencial* ON/OFF) em intervalos de tempo estipulados. Durante o período de "ON", os pacotes são enviados numa taxa de transferência fixa e durante o período "OFF" nenhum pacote é enviado (Rodrigues, 2009).

São exigidas variáveis para o objeto *Exponencial* tais como o tamanho do pacote, o tempo "ON", o tempo "OFF" e a taxa de transferência. O Tráfego utilizado para simular o IPTV é criado a partir das seguintes variáveis:

- PacketSize_ 1402 (gerado pacotes constantes do mesmo tamanho);
- burst_time_ 0ms (tempo médio em que são enviados pacotes);
- idle_time_ 0ms (tempo médio em que não são enviados pacotes);
- rate_ 4907k (taxa de transferência durante o tempo em que está ativo);

O tamanho do pacote "PacketSize_" é dado em *bytes*, os tempos em milissegundos e a taxa de transferência em Kbps.

Como o tráfego IPTV é não orientado à conexão, ele é implementado na ferramenta através do protocolo UDP, necessitando uma resposta do tipo *null* para cada conexão. O quadro 6 ilustra os comandos para iniciar um tráfego do tipo IPTV.

Quadro 6: Agentes IPTV

```
# Inserção de tráfego IPTV1 - Exponential na terceira conexão UDP2 0-10

set udp2 [new Agent/UDP]
set null2 [new Agent/Null]
$ns attach-agent $n0 $udp2
$ns attach-agent $n10 $null2
$ns connect $udp2 $null2
$udp2 set class_ 4
set vbr1 [new Application/Traffic/Exponential]
$vbr1 set packetSize_ 700
$vbr1 set rate_ 600k
$vbr1 set burst_time_ 0ms
$vbr1 set idle_time_ 0ms
$vbr1 attach-agent $udp2
```

Os comandos “set udp2 [new Agent/UDP]” e “set null2 [new Agent/Null]” orientam um fluxo de dados no sentido da origem e destino respectivamente. Já o comando “set vbr1 [new Application/Traffic/Exponential]” inicia as características de cada pacote gerado deste tipo na rede, indicando os valores de tamanho, tempo entre envio de cada um e tempo de não envio deles.

4.3.2 Criação de LSP’s e programação da simulação

A criação de caminhos entre os roteadores que utilizam o protocolo RSVP-TE para reservarem recursos na rede e transmitir pacotes específicos são importantes e necessários na implementação de engenharia de tráfego em redes IPTV.

Foi criado um caminho específico para que os tráfegos de IPTV ficassem separados dos outros tráfegos de dados de aplicações utilizados pela empresa. Assim, o novo fluxo de dados passou a trafegar junto com os tráfegos de vídeos comuns e voz como o Voip, utilizados pela corporação.

Isto foi feito para se avaliar o verdadeiro impacto que teria a inserção e implantação desta nova plataforma de serviço nos serviços mais importantes oferecidos pela operadora e regidos pelo acordo de nível de serviço (*SLA*).

O quadro 7 demonstra os comandos necessários para a criação dos canais LSP’s que implementam o protocolo de reserva de recursos.

Quadro 7: Criação de canais LSP’s

```
# Criação de LSP para o tráfego de áudio

$ns at 0.15 "[$LSR8 get-module MPLS] ldp-trigger-by-withdraw 10 -1"
$ns at 0.1 "[$LSR2 get-module MPLS] make-explicit-route 8 2_4_5_7_8 1000 -1"
$ns at 0.25 "[$LSR2 get-module MPLS] flow-erlsp-install 10 -1 1000"

# Criação de LSP para o tráfego de vídeo

$ns at 0.15 "[$LSR8 get-module MPLS] ldp-trigger-by-withdraw 10 -1"
#$ns at 0.15 "[$LSR8 get-module MPLS] ldp-trigger-by-routing-table"
$ns at 0.1 "[$LSR2 get-module MPLS] make-explicit-route 8 2_4_5_7_8 1001 -1"
```

```
$ns at 0.25 "[$LSR2 get-module MPLS] flow-erlsp-install 10 -1 1001"

#Criação de LSP para tráfego TCP

$ns at 0.15 "[$LSR9 get-module MPLS] ldp-trigger-by-withdraw 11 -1"
#$ns at 0.15 "[$LSR9 get-module MPLS] ldp-trigger-by-routing-table"
$ns at 0.1 "[$LSR3 get-module MPLS] make-explicit-route 9 3_4_6_7_3 1002 -1"
$ns at 0.25 "[$LSR3 get-module MPLS] flow-erlsp-install 11 -1 1002"
```

O quadro acima ilustra a codificação para que os roteadores pertencentes ao caminho LSP troquem rótulos entre si referentes à reserva de recursos e encaminhamento diferencial dos pacotes oriundos de aplicações IPTV em um determinado tempo pré-estabelecido pela programação.

Os caminhos ditos LSP's foram criados com o intuito de priorizar os tráfegos mais necessitados de recursos como o IPTV e TCP, que neste caso foram tratados como prioridade e analisados juntos. Além disso, houve naturalmente a aplicação de uma engenharia de tráfego através do balanceamento na transmissão de todos os fluxos oriundos do roteador de SLZ em direção ao roteador de VIT. Ao separar tráfegos de vídeos comuns, de voz e dados comuns, acarretou em um melhor throughput na rede lógica.

Para inicialização e partida dos tráfegos na rede, é necessário que se faça uma programação de quando (tempo determinado) serão disparados na rede simulada. O quadro 8 demonstra como pode ser realizada esta ação.

Quadro 8: Programação da simulação

```
#Determinação de Tempo de Simulação
set timesimu 60.0

# Programação da simulação
$ns at 0.1 "$cbr0 start"
$ns at 0.1 "$cbr1 start"
$ns at 0.1 "$cbr2 start"
$ns at 0.1 "$cbr3 start"
```

```
$ns at 0.1 "$cbr4 start"
$ns at 0.1 "$cbr5 start"
#$ns at 0.1 "$cbr6 start"
$ns at 0.1 "$vbr1 start"
$ns at 0.1 "$vbr2 start"
$ns at 0.1 "$vbr3 start"
…
```

Após a criação dos tráfegos, eles são programados para entrarem em ação em determinado tempo da simulação através dos comandos do quadro 8. Primeiro é determinado qual o intervalo de tempo máximo da simulação, que no caso foi de 60 segundos, considerado um tempo muito satisfatório para uma simulação de eventos discretos.

Após isso, cada fluxo criado deve ser inicializado com sua identificação declarada e em qual tempo exato do intervalo isto deve ocorrer. Como o intuito é analisar a concorrência desses fluxos, todos os tráfegos foram inicializados bem no começo da simulação aos 0,1 milissegundos e parados no limite final atribuído. O quadro 9 ilustra os comandos para a finalização deles e da simulação como um todo.

Quadro 9: Finalização dos tráfegos

```
$ns at timesimu "$vbr1 stop"
$ns at timesimu "$vbr2 stop"
$ns at timesimu "$vbr3 stop"
$ns at timesimu "$ftp0 stop"
$ns at timesimu "$ftp1 stop"
$ns at timesimu "$ftp2 stop"
$ns at timesimu "$ftp3 stop"
$ns at timesimu "$ftp4 stop"
$ns at timesimu "$ftp5 stop"
$ns at timesimu "$ftp6 stop"
$ns at timesimu "$ftp7 stop"
#$ns at timesimu "$ftp8 stop"
# Chamando procedimento final
$ns at [expr $timesimu] "finish"
```

```
# Iniciando a simulação
$ns run
```

Definida toda a programação, a simulação é executada e os arquivos de trace são gerados para futura análise dos acontecimentos da simulação.

No quinto capítulo, serão mostrados os resultados obtidos após a execução da simulação e as análises serão feitas em relação aos parâmetros de qualidade de serviço necessários ao serviço IPTV, onde os acontecimentos mais relevantes que foram percebidos quando outros tráfegos também disputaram a banda ofertada pela provedora. Além disso, poderá ser concluído se há possibilidade de implantação desse serviço sem degradação daqueles já em operação e quais os limites para o transporte desses dados novos.

5. RESULTADOS E ANÁLISES

Os resultados foram obtidos a partir do processamento dos arquivos *trace* gerados pela ferramenta de simulação NS2. A cada instância para um novo fluxo de tráfego IPTV inserido foi realizado um processamento para cálculo de requisitos de QoS juntamente com seus respectivos gráficos associados.

O objetivo do aumento no número de fluxos inseridos é a verificação e validação do limite máximo de tráfegos IPTV que a rede suporta em condições atuais de funcionamento.

A cada novo fluxo de tráfego IPTV declarado e executado na simulação foi analisado o arquivo *trace* de saída correspondente para avaliar o impacto gerado por esta ação e fazer uma comparação com os limites estabelecidos por (Barros, *apud* Mello, 2011) vistos na tabela 01, para uma transmissão IPTV satisfatória na rede.

Através das propriedades gráficas da ferramenta de análise, pode-se verificar os resultados dos requisitos de QoS após o primeiro fluxo inserido.

A ferramenta é capaz de trazer informações a respeito dos fluxos Exponenciais utilizados como tráfego IPTV. A partir da figura, algumas informações relevantes são demonstradas como: transferências de pacotes, identificação do roteador, nome do fluxo, pacotes gerados e pacotes perdidos.

Após a inserção do primeiro fluxo IPTV, verificou-se que foi gerado um total de 2871 pacotes e que **nenhum pacote** foi perdido pela fila de concorrência durante a transmissão e recebimento neste roteador. De acordo com o modelo e método de análise realizado para o primeiro fluxo, servirá base para demonstração dos demais fluxos, uma vez que estão disponíveis nos demais requisitos como *delay, throughput.* Os outros requisitos de QoS obtidos para um primeiro fluxo trás uma média de *delay* (atraso) dos pacotes IPTV de 0,07301283 segundos. O *jitter* (variação de atraso) por sua vez, possui uma média de 0,0016033182 segundos.

O último requisito mostrado pela ferramenta é o throughput que mede a quantidade de dados de um determinado fluxo que são gerados recebidos pelo roteador analisado. A figura 14 demonstra a medição deste parâmetro.

O throughput dos pacotes IPTV para um primeiro fluxo de transferência e geração pelo roteador são demonstrados pela figura acima gerada pela ferramenta. A partir do conjunto dos dados de qualidade de serviço e a devida comparação com os

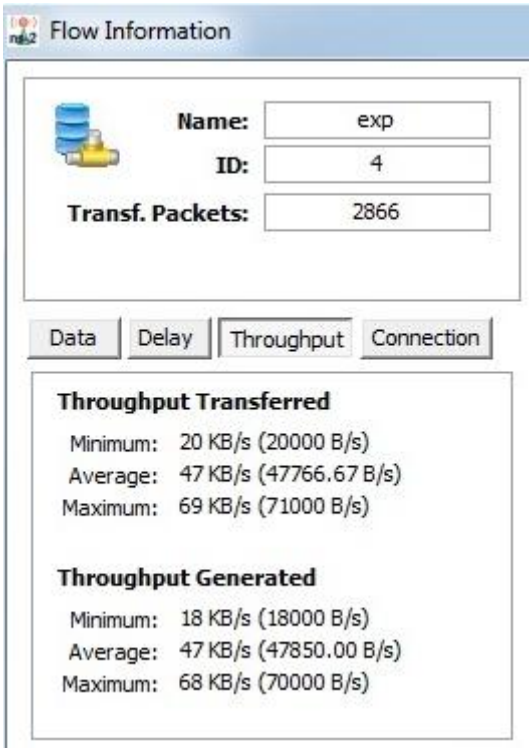

Figura 14: Throughput IPTV primeiro fluxo

Fonte: Lima, Filipe (2015).

requisitos mínimos de transmissão, pode-se concluir que para a inserção de uma primeira instância de tráfego IPTV, a rede consegue manter um nível satisfatório para oferecer esta nova plataforma tecnológica aos gestores da empresa sem alterar acordos de nível de serviços.

Para cada nova inserção de uma instância IPTV foi realizado o mesmo procedimento de análise e extração de informações através da ferramenta. Os dados estatísticos gerados após a inserção do segundo fluxo IPTV na rede possui os seguintes valores para os requisitos de QoS: 5521 pacotes do tipo *exp* gerados, 10 pacotes perdidos ou **0,181127%** deles, um *delay* de 0,084917 segundos e 0,012151 de variação de atraso (*jitter*). A figura 15 ilustra o throughput gerado por esse roteador com transmissão dos dois fluxos inseridos.

Como o valor dos pacotes perdidos é vital para o funcionamento correto e nessa instância ainda se encontra dentro do limite estabelecido pela tabela de referência, a rede ainda mantém a qualidade necessária para transmissão dessa nova aplicação.

Prosseguindo com as inserções de novos fluxos, percebesse que o número de pacotes perdidos para um terceiro fluxo aumenta para **24 (vinte e quatro)** em um total

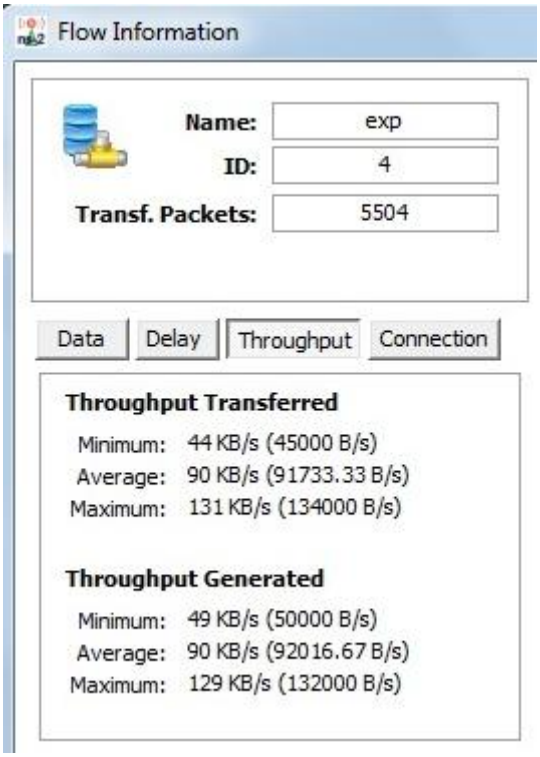

Figura 15: Throughput IPTV segundo fluxo

Fonte: Lima, Filipe (2015)

de 8233 pacotes gerados por esse nó. Isto significa que a porcentagem de perdas é de: **0,291510%**, o que indica estar dentro do limite referencial, garantindo uma qualidade de transmissão. Além disso, os outros requisitos também se mostram satisfatórios para tal necessidade com números de 0,86252 segundos para *delay* e 0,010249 segundos para *jitter*. A figura 16 ilustra o throughput IPTV gerado por este roteador com três fluxos inseridos.

Ao inserir **quatro (04)** fluxos destes pacotes, pode-se perceber que os requisitos de qualidade de serviço obtidos possuíam um valor limite à tabela de referência, ou seja, a rede tinha capacidade de processamento de quatro fluxos IPTV, porém com uma pequena concorrência natural e uma degradação de outros serviços já em operação.

Isto pôde ser observado devido aos números dos requisitos coletados onde a quantidade de pacotes IPTV perdidos após a simulação com os quatro fluxos é de **55 (cinquenta e cinco)** de um total de 10889 pacotes.

A porcentagem de pacotes perdidos é **0,505097%**, ou seja, no limite imposto pela tabela de referência (tabela 1) para uma boa qualidade.

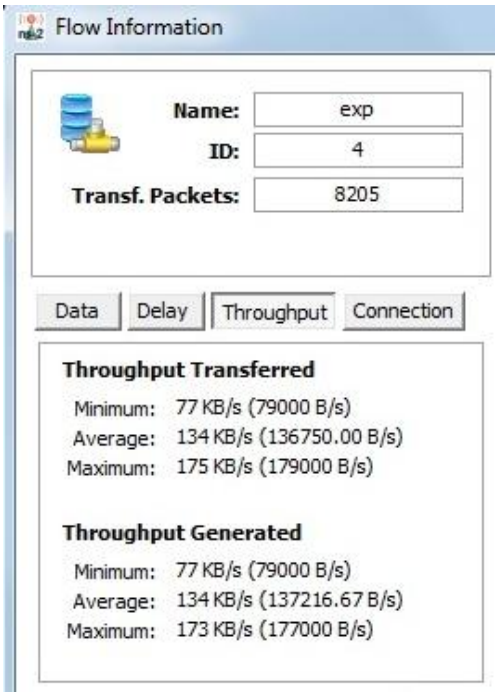

Figura 16: Throughput IPTV três fluxos

Fonte: Lima, Filipe (2015).

Além disso, nessa instância, podemos observar que os outros requisitos de QoS ainda se mantém com valores baixos como 0,86174 segundos de *delay* e 0,009645 segundos de *jitter*.

A figura 17 ilustra o throughput gerado nesse nó com geração de tráfegos com os quatro fluxos IPTV´s.

A partir de mais inserções na simulação, houve uma degradação maior e os valores de referência já começam a ultrapassar os limites aceitos. Para uma maior análise acerca das inserções de fluxos e suas respectivas análises, foram inseridos até o sétimo fluxo IPTV para que o comportamento dos requisitos de qualidade de serviço fosse verificado. A tabela 2, mostra a grade de resultados para cada instância de fluxo IPTV inserido na rede, associado ao requisito de QoS correspondente. Após isso, pôde-se retirar uma relação entre as perdas evolutivas de pacotes e qual o grau e intervalo que isto ocorre.

Todos os valores coletados e mostrados na tabela referem-se aos pacotes específicos dos fluxos de aplicações IPTV que foram analisados juntamente com outros tipos de pacotes oriundos das demais aplicações disputando a banda passante.

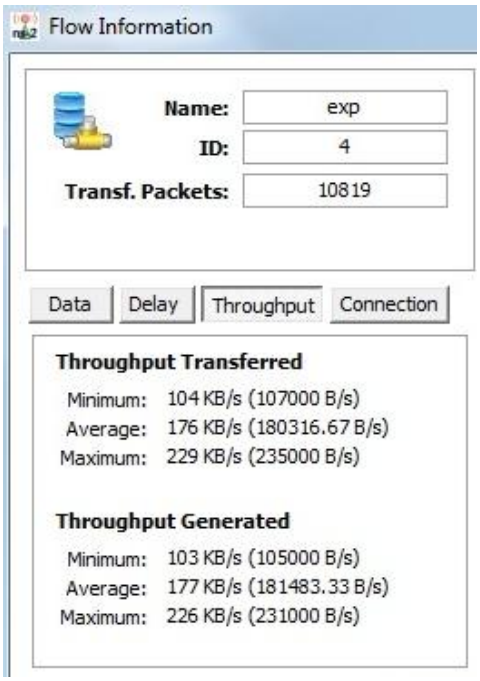

Figura 17: Throughput IPTV quatro fluxos

Fonte: Lima, Filipe (2015).

O requisito de maior relevância para este estudo são os pacotes perdidos, pois eles representarão degradações na transmissão de vídeos. Uma vez perdido, dificilmente poderão ser recuperados, acarretando problemas de visualização do usuário final e influenciando a sua qualidade de experiência.

Tabela 2: Resultados da Simulação

Instância (Fluxos IPTV)	Throughput (B/s)	Delay (s)	Jitter (s)	Perda de pacotes	Perda de pacotes (%)
1 Fluxo de IPTV	71000 B/s	0,084798 s	0,01333 s	0	0,00000
2 Fluxos de IPTV	134000 B/s	0,084917 s	0,012151 s	10	0,18113
3 Fluxos de IPTV	179000 B/s	0.086252 s	0,010249 s	24	0,29151
4 Fluxos de IPTV	235000 B/s	0,086174 s	0,009645 s	55	0,50510
5 Fluxos de IPTV	287000 B/s	0,086839 s	0,011041 s	88	0,64408
6 Fluxos de IPTV	333000 B/s	0,085712 s	0,008577 s	123	0,75082
7 Fluxos de IPTV	374000 B/s	0,088193 s	0,008141 s	176	0,91896

Entretanto, pode-se realizar uma comparação entre a quantidade de pacotes perdidos e o throughput dos tipos de pacotes da rede. A seguir, será feita uma análise da vazão entre os pacotes concorrentes IPTV e TCP (os mais relevantes para a pesquisa).

5.1 Análises

Pelos resultados obtidos após uma série de fluxos inseridos na rede, uma análise de comparação e relação entre as perdas das instâncias mostra que a evolução se dá de forma exponencial. A figura 18 ilustra o gráfico evolutivo de perdas de pacotes IPTV ao longo das inserções na rede.

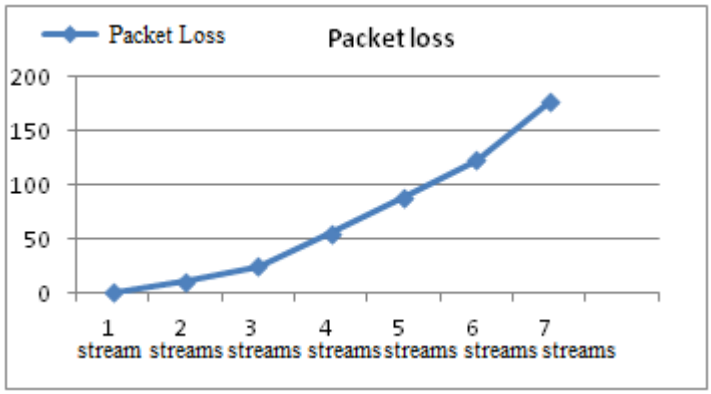

Figura 18: Curva de pacotes perdidos

Fonte: Lima, Filipe (2015).

A figura 18 oferece uma informação relevante para possíveis planejamentos de implantação dessa nova plataforma na empresa, uma vez que analisa qual a relação e evolução no aumento deste tipo de tráfego. Com isso, a gerência de capacidade poderá ter um conhecimento prévio do comportamento com cenários futuros, acarretando tomadas de decisões respaldadas tecnicamente.

Diante das informações obtidas e apresentadas, podemos afirmar primeiramente que a rede corporativa analisada possui uma tolerância e capacidade de processar até 03 (três) fluxos IPTV, garantindo os requisitos mínimos para se possuir uma transmissão de boa qualidade. Após a inserção de 04 (quatro) fluxos de IPTV na rede atual da empresa corporativa, haverá uma concorrência natural com outras aplicações de forma que poderá acontecer degradação na transmissão desses pacotes IPTV e possivelmente

uma defasagem na qualidade da transmissão do vídeo, apesar de estar dentro do intervalo recomendado para uma qualidade satisfatória.

Após essa quantidade inserida, é perceptível que, a partir da instância de 05 (cinco) fluxos de IPTV há uma porcentagem de perda significativa dos pacotes IPTV, eliminando qualquer investimento para esse número de conexões.

A concorrência entre as aplicações inseridas na rede corporativa será ponto chave para que se tome uma medida de investimento mais robusto do ponto de vista a priorizar algumas delas. Através da figura 19, fica claro que como a quantidade do novo tráfego inserido é pequeno, os outros serviços ainda ocupam faixas bem distintas da largura de banda total da rede. Porém, na figura 20, fica evidente que o tráfego IPTV concorre bastante com as outras aplicações de dados convencionais, representados pelos fluxos de protocolo TCP.

O gráfico apresenta o throughput dos pacotes das aplicações IPTV e TCP. Esse gráfico faz referência à inserção de apenas um fluxo IPTV, onde se pode perceber que a concorrência ainda não se tornou evidente para essa instância e a ocupação da banda segue em faixas bem distintas, o que não gera a degradação dos pacotes de cada aplicação.

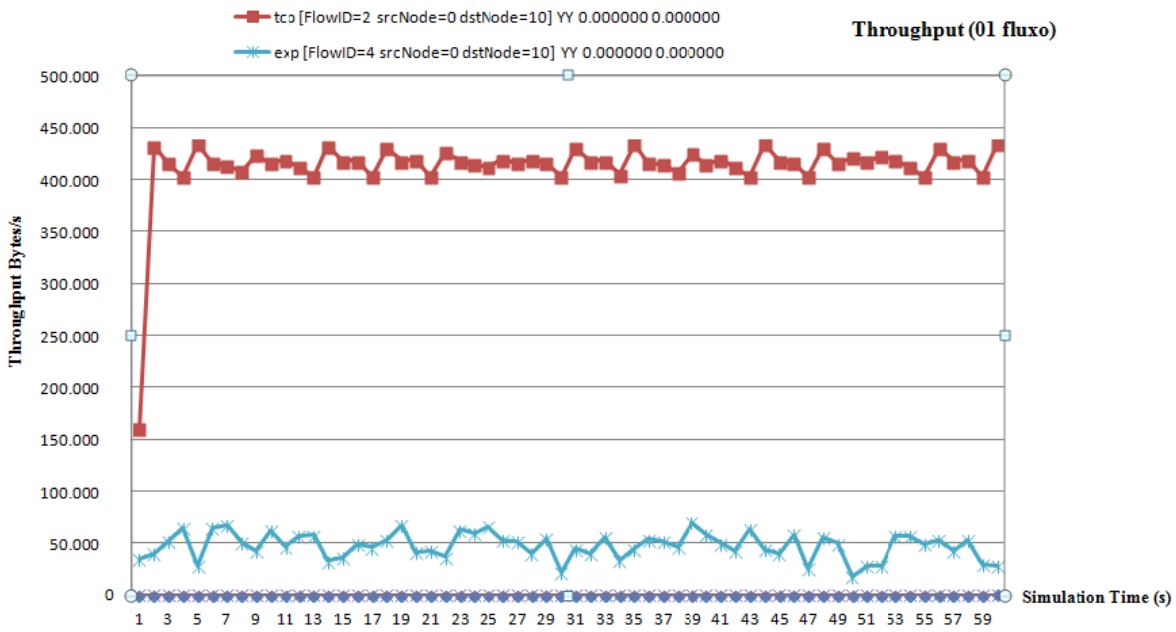

Figura 19: Throughput IPTV x TCP (um fluxo)

Fonte: Lima, Filipe (2015).

Já na figura 20, a percepção dessa concorrência já é muito mais evidente, ou seja, na instância limite para a qualidade de transmissão satisfatória da rede, a concorrência da banda pelos pacotes IPTV com os pacotes de dados gerais se torna mais acirrada, causando uma degradação para o serviço e ocupando limites de faixas de transmissão.

Com a inserção da última instância de 07 (sete) fluxos de aplicações IPTV, há uma degradação ainda maior do throughput dos pacotes TCP, sendo inclusive ultrapassado na vazão de envio.

A figura 21 comprova este fato, ou seja, quanto mais fluxos deste tipo forem inseridos na rede, maior será a concorrência da largura de banda oferecida pela empresa provedora, apesar da implementação de uma engenharia de tráfego na rede.

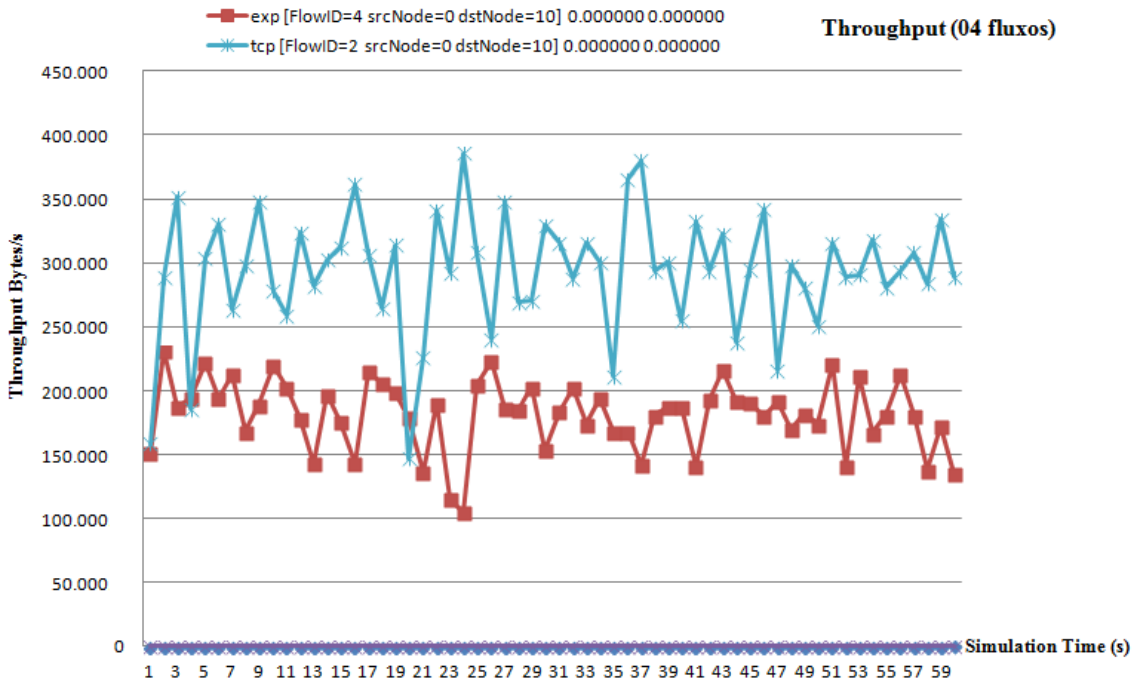

Figura 20: Throughput IPTV x TCP (4 fluxos)

Fonte: Lima, Filipe (2015).

A vazão do tráfego TCP, que são dados prioritários de transações da empresa, teve uma queda na ordem de 250.000 bytes por segundo ao longo dos sete fluxos inseridos. Isto significa uma perda muito sensível para realização do volume de dados que a empresa necessita no seu dia a dia.

Com o aumento na ocupação da rede em detrimento dos pacotes TCP, as aplicações às quais a empresa já operava de forma satisfatória diante de seus clientes,

poderá sofrer perdas de disponibilidade, instabilidades e até inconsistências de dados. Por outro lado, a nova tecnologia IPTV pode garantir maiores retornos produtivos do ponto de vista de aumento de possibilidades tecnológicas.

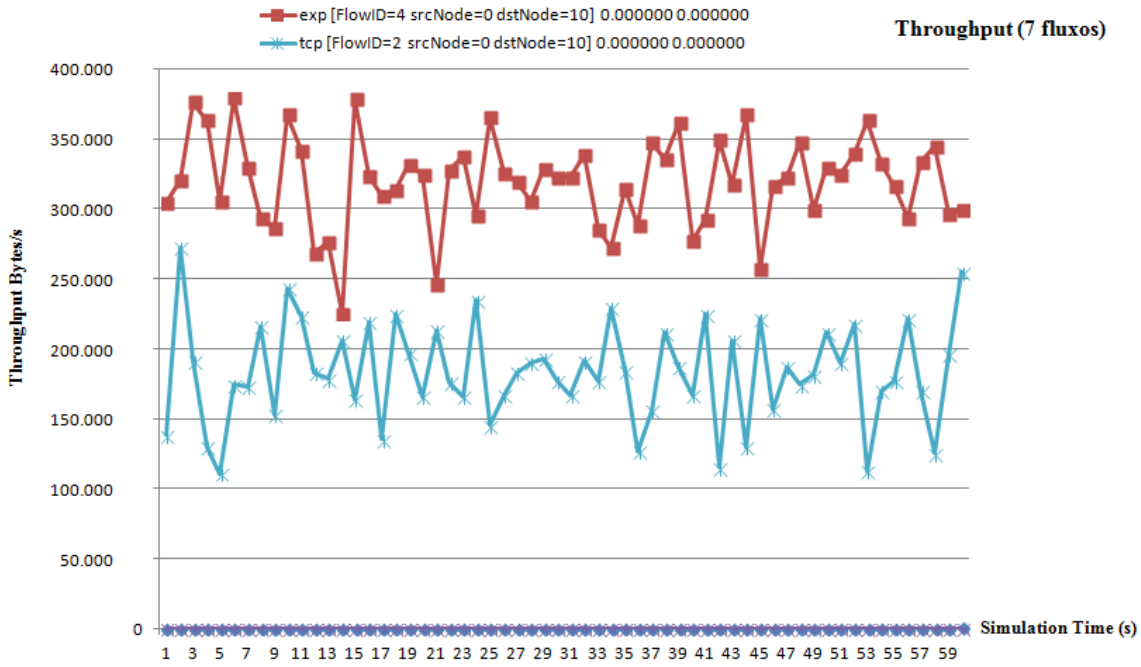

Figura 21: Throughput IPTV x TCP (7 fluxos)

Fonte: Lima, Filipe (2015).

No capítulo a seguir, pode-se tirar algumas conclusões a respeito da viabilidade de implantação desta nova plataforma de serviço na rede da empresa, de acordo com os resultados obtidos e análises realizadas.

6. CONCLUSÃO

É perceptível que cada vez mais há o aumento de exigências por parte dos clientes sobre o uso de mídias e serviços complementares de voz e dados. Os serviços de televisão são oferecidos de forma não digital de alta qualidade e sem interatividade com os consumidores. Por isso, a tecnologia tem um peso importante no que diz respeito à modernidade e desenrolar de tendência para o futuro.

A motivação do trabalho foi baseada à possibilidade de aplicação desta plataforma tecnológica no meio industrial. Por isso, abriu-se a possibilidade de monitoramento de áreas operacionais remotas sem perder qualidades de informações de forma mais ágil e com maior disponibilidade.

Além disso, a viabilidade desse novo serviço poderá acarretar na diminuição no tempo de decisões gerenciais, uma vez disponibilizada para cargos estratégicos dentro da empresa.

O trabalho proposto teve a finalidade de verificar a viabilidade ou não de inserção de tráfegos IPTV's na rede corporativa que pudesse atender a transmissão de televisão ao vivo, de forma satisfatória e sem perdas significativas de outras aplicações já existentes na rede lógica de dados.

Os resultados levam a uma conclusão de que até a inserção de três fluxos IPTV's, a rede da empresa mantém um nível de qualidade aceitável para implantação e operacionalizar o novo serviço sem a degradação dos outros serviços já em operação.

Após a inserção do quarto fluxo, a rede inicia um processo de degradação dos outros tipos de pacotes essenciais para os processos administrativos e de controle geral.

Após os dados coletados e análises realizadas a partir dessas métricas, pode-se concluir que, obedecendo ao cenário atual da empresa, é viável a inserção dessa nova tecnologia e plataforma. Porém, é importante notar que há uma limitação bem aparente na escalabilidade desses fluxos. Se houver necessidade de aumento no número de aplicações IPTV, fatalmente será necessário um investimento na infraestrutura local e na espinha dorsal dessa rede. Além disso, outras estratégias de Qualidade de Serviço serão requisitadas para cobrir as novas necessidades de transmissão dos pacotes.

Por isso, os trabalhos de pesquisas e simulações prévias têm uma importância muito grande antes da operacionalização desses serviços. Além disso, será necessário

um estudo do custo/benefício de implantação diante da empresa terceirizada que provê o backbone da rede lógica através de um SLA específico.

Por fim, a transmissão de televisão por meio da rede de dados se tornou uma realidade na grande maioria de empresas de grande porte para amparar diversas áreas de negócio. Isso significa que haverá possibilidades reais de aproximar ainda mais os gerentes e as áreas operacionais, uma vez que se abrirão possibilidades de tecnologias inovadoras como, por exemplo, os aplicativos de IPTV em *smartphones* (telefone móvel com funcionalidades avançadas como, por exemplo, conexão à internet). Consequentemente, a viabilidade de implantação dessa plataforma na empresa, não só abre um leque amplo de possibilidades de novos serviços como também porá a empresa em um nível de destaque de inovação e inclusão digital.

Como trabalhos futuros, propõe-se primeiramente aumentar o número de localidades com a plataforma IPTV o teste dos modelos gerados em outros dados sísmicos reais para avaliar os resultados. Caso estes se mostrem inferiores aos apresentados neste trabalho, um treinamento pode ser realizado novamente para incluir novas informações fornecidas por especialistas e tornar o método mais generalizável.

Outra proposta é a seleção da base e das características que gerem um modelo ótimo de classificação. Como a seleção das amostras de treinamento foi realizada de forma aleatória, não existe a garantia de que estas amostras sejam as mais representativas de todo o volume. Buscas pela melhor base com o auxílio, por exemplo, de algoritmos genéticos, podem ser realizadas.

7. REFERÊNCIAS

Administrator Guide for Cisco Unified Videoconferencing 3515 MCU12 and MCU24 Release 5.0, (2003). Cisco Systems, Inc.

Alves Cruz, Elifranio (2012); "Aprovisionamento avançado de recursos em redes convergentes sensíveis ao contexto", UFC.

Alves de Sousa dos Santos, Ricardo (2004); "QoS sobre redes de pacotes utilizando H.323".

Amorim, Leonardo Gomes; SILVA, Danilo José. RSVP-TE. Universidade Federal do Rio Grande do Norte, 2007.

Anacom. (2011), (Autoridade Nacional de Comunicações), "Avaliação da QoS dos Serviços de Voz, Videotelefonia e Cobertura Radioelétrica GSM e WCDMA, nos principais Aglomerados Urbanos e Eixos Rodoviários de Portugal Continental".

Awduche, D. et al. *Requirements for Traffic Engineering over MPLS.* RFC 2702, 2000.

Barros, Jorge Luis Silva, (2011); "Proposta de Método para Análise Técnica de Rede para Implantação de Serviços IPTV", Escola Politécnica de São Paulo.

Benbella Benduduh et Jean Marc Fourcade, (2001). MPLS <http://www.frameip.com/mpls/>. Acesso em maio de 2014.

Blog CCNA. Disponível em: <http://www.ccna.com.br>.GNS3, Comunidade. Disponível em: <http: //http://www.gns3.net/>.

Cisco Systems Inc. (2007). IPTV Solutions for Wireline Carriers - IP Multicast Technical Overview. <http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6552/prod_white_ paper0900aecd804d5fe6_ns610_Networking_Solutions_White_Paper.html> Acesso em outubro de 2009.

Comer, Douglas E. Redes de computadores e internet: abrange transmissão de dados, ligações inter - redes, web e aplicações. 4.ed. Portto alegre: Bookman, 2007. 640 p. Inclui CD - ROM. ISBN 9788560031368.

Coutinho L. W. Rodolfo. (2009). "Network Simulator – ns2". Universidade Federal de Minas Gerais.

De Queiroz, Osmar Leonardo.; VPN (REDE PRIVADA VIRTUAL): VPN/MPLS. UNIFACS, 2000 Disponível em: <http://pt.scribd.com/doc/56980705/Artigo-VPN-Mpls> Acesso em: 18 de maio. 2015.

Dominique Revuz, (2000). Les réseaux IP/MPLS. <http://www-igm.univ-mlv.fr/~dr/XPOSE2007/ykarkab_MPLS/mpls_services.html#rsvp> Acesso em 17 de maio de 2015.

Evans, John, Filsfil, Clarence. Developing IP and MPLS QoS for multiservice networks – Theory and Pratice: Morgan Kaufman, 2007.

Filippetti, Marco Aurélio. CCNA 4.1: Guia completo de estudo. Florianópolis: Visual Books, 2008.

Follador Neto, Arlindo (2009); "Uma avaliação dos mecanismos de transmissão de tráfego para IPTV", UFMG.

Freitas, Leandro Alexandre (2011); "QoS-RRC: Um mecanismo de orquestração de Sobre-provisionamento de recursos e balanceamento de carga para roteamento orientado a QoS na Internet do Futuro".

Gill, P., Arlitt, M., Li, Z., and Mahanti, A. (2007). YouTube traffic characterization: a view from the edge. In IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement, pages 15–28, New York, NY, USA. ACM.

Goll, Maicon, (2007). "Processo de simulação - uma abordagem com estudo de caso da ferramenta network simulator 2", Sociedade Educacional de Santa Catarina – Sociesc.

Gonçalves, Emerson Carlos, (2011); "Tecnologia Voip: Estudos das Falhas; Centro Universitário de Maringá".

Kurose, J. F., Ross, K. W., Redes de Computadores e a Internet - Uma nova abordagem, 3a Edição, São Paulo: Addison Wesley, 2006.

Lotito, Alberto. Engenharia de tráfego entre domínios de redes distintas. 119f Dissertação (Mestrado em Engenharia Elétrica) – Pós-Graduação em Gestão de Redes de Telecomunicações. – PUC, Campinas 2007.

Mateus Farinha, Diogo Miguel, (2008). "Arquitecturas de Rede para oferta de serviços de Vídeo a Pedido e IPTV". Universidade Técnica de Lisboa.

Memória, Carlos, (2007). "Introdução as Redes de Computadores com Serviços Diferenciados: O Protocolo MPLS". Universidade Federal do Maranhão.

Mokarzel, Marcos Perez. (2010). "Redução do tempo do zapping em serviços IPTV sobre redes GPON utilizando vídeos escaláveis." USP, Departamento de Engenharia Elétrica.92f. Dissertação.

Neto Gonçalves, Miguel, (2009); "IPTV 2.0"; Universidade de Aveiro.124f. Dissertação.

Osborne, Eric. Engenharia de tráfego com MPLS. CiscoPress: Editora Campus, 2003.

Oswald Vieira, Gabriel Maurício (2010), "Ferramenta para mapear a qualidade percebida pelo usuário em requisitos de QoS em ambiente convergente e heterogêneo", USP .

Reis Correa, Bruno; Sodré dos Reis, Marcelo (2012); "IPTV: Protocolos Utilizados, Congresso de iniciação científica do INATEL-INCITEL, 2012, p. 178-182".

RFC 2362: Protocol Independent Multicast - Sparse Mode.,1998.

Rodrigues, Sandy Carmo. (2009). "Encaminhamento Óptimo do Tráfego em redes *Triple Play*." Universidade da Madeira. 162f Dissertação (Mestrado em Engenharia Eletrônica e Telecomunicações).

Shihab, E. and Cai, L. (2007). IPTV Distribution Technologies in Broadband Home Networks. Electrical and Computer Engineering, 2007. CCECE 2007. Canadian Conference on , vol., no., pp.765- 768, 22-26.

Solis Barreto, Priscila. Uma metodologia de Engenharia de Tráfego Baseada na Abordagem Auto-Similar para a Caracterização de Parâmetros e a Otimização de Redes Multimídias. Tese (Doutorado em Engenharia Elétrica). – Departamento de Engenharia Elétrica, Universidade de Brasília, 164f, 2007.

Tanenbaum, A. S. Redes de computadores. 5 ed. Rio de Janeiro: Editora Campus, 2011.

Teixeira, Mario Antônio Meireles. Suporte a serviços diferenciados em servidores web: modelos e algoritmos. São Carlos, SP: 2004. Tese (Doutorado em Ciências: Área Ciências da Computação e Matemática Computacional). Universidade de São Paulo. São Carlos, SP, 2004.

Uzunalioglu, H. (2009). Channel change delay in IPTV systems. Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE, pages 1–6.

Veiga, Miguel Ângelo. Simulação de redes MPLS: Uma perspectiva pedagógica. 2009 115f Dissertação (Mestrado em Engenharia Eletrônica e Telecomunicações) – Departamento de Eletrônica, Telecomunicações e Informática. – Universidade de Aveiro, Portugal 2009.

Wang, Ya-Shian e et al, (2010); “Quality-Assured Provisioning of IPTV Services in Ethernet-Based Broadband Networks”, Network Operations Laboratory Chunghwa Telecom Laboratories, Taoyuan county, Taiwan, R.O.C.

Weissheimer Júnior, Carlos Alfredo (2012). “Desenvolvimento de um algoritmo híbrido utilizando metaheurísticas aplicado a uma plataforma de Internet Protocol TeleVision – IPTV”.

Yarali, A. and Cherry, A. (2005). Internet Protocol Television (IPTV). Proceedings of the TENCON 2005 - IEEE International Region 10 Conference., pages pp.1–6.

Zeadally, Sherali; Moustafa, Hassnaa, (2011); “Internet Protocol Television (IPTV): Architecture, Trends, and Challenges”, IEEE System Journal, Vol.5 n°4, December 2011, p. 518-526.