UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE TECNOLOGIAS E GEOCIÊNCIAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

ANÁLISE DO TRÁFEGO DE VOZ EM REDES MPLS

Elaborado por:

Marcos Antonio Alves Gondim

Junho de 2009

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE TECNOLOGIAS E GEOCIÊNCIAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

ANÁLISE DO TRÁFEGO DE VOZ EM REDES MPLS

por

MARCOS ANTONIO ALVES GONDIM

Dissertação submetida ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Pernambuco como parte dos requisitos para a obtenção do grau de Mestre em Engenharia Elétrica.

ORIENTADOR: PROF. RAFAEL DUEIRE LINS, Ph.D.

Recife, Junho de 2009.

© Marcos Antonio Alves Gondim, 2009

G637a **Gondim, Marcos Antônio Alves.**
Análise do tráfego de voz em Redes MPLS / Marcos Antônio Alves Gondim. – Recife: O Autor, 2009.
xv, 98 folhas, il : figs., tabs.

Dissertação (Mestrado) – Universidade Federal de Pernambuco. CTG. Programa de Pós-Graduação em Engenharia Elétrica, 2009.

Inclui Referências.

1. Engenharia Elétrica. 2.VoIP. 3.MPLS. 4.Telefonia. I. Título.
UFPE

621.3 **CDD (22. ed.)** **BCTG/2009-218**

PPGEE
UFPE

Ata da sessão de defesa da 173ª Dissertação do Mestrado Acadêmico de **MARCOS ANTONIO ALVES GONDIM** do Programa de Pós-Graduação em Engenharia Elétrica do Centro de Tecnologia e Geociências/Escola de Engenharia de Pernambuco da Universidade Federal de Pernambuco, realizada no dia 15 de junho de 2009.

Aos quinze dias do mês de abril de dois mil e nove, no Laboratório Valdemar Rocha do Departamento de Eletrônica e Sistemas do Centro de Tecnologia e Geociências/Escola de Engenharia de Pernambuco, sob a presidência do prof. Rafael Dueire Lins, reuniu-se a Comissão Examinadora aprovada "ad referendum" do Colegiado e homologada pela Pró-Reitoria Para Assuntos de Pesquisa e Pós-Graduação (Proc. nº 23076.011806/2009-91) composta pelos professores: 1º Examinador e Orientador: Rafael Dueire Lins, DES/UFPE (PhD-Canterbury-Inglaterra); 2º Examinador: Valdemar Cardoso da Rocha Júnior, DES/UFPE (PhD-Kent-Inglaterra); 3º Examinador: Carmelo José Albanez Bastos Filho, DSC/UPE (Doutor-Recife-Brasil); Suplente Interno: Joaquim Ferreira Martins Filho, DES/UFPE (PhD-Glasgow-Escócia) e Suplente Externo: Maria Lencastre Pinheiro de Menezes Cruz, DSC/UPE (Doutor-Recife-Brasil. Às nove horas, o Sr. Presidente abriu a sessão de defesa de dissertação do mestrando **Marcos Antonio Alves Gondim** sob o título *"Análise do Tráfego de Voz em Redes MPLS"*. Após exposição do candidato e, por decisão da Comissão Examinadora, o mesmo foi **APROVADO**. Nada mais havendo a tratar foi encerrada a sessão, da qual, eu, Andréa Tenório Silveira, secretária do Programa de Pós-Graduação em Engenharia Elétrica, lavrei a presente ata que vai por mim assinada e por quem de direito. Recife, 15 de junho de 2009.

ANDRÉA TENÓRIO SILVEIRA
Secretária do PPGEE

RAFAEL DUEIRE LINS
Orientador e Membro Titular Interno

VALDEMAR CARDOSO DA ROCHA JÚNIOR
Membro Titular Interno

CARMELO JOSÉ ALBANEZ BASTOS FILHO
Membro Titular Externo

CONFERE COM O ORIGINAL DE ACORDO COM O DEC. 83936/79 EM 17/06/2009
Andréa Tenório Secretária Programa de Pós-Graduação em Engenharia Elétrica da UFPE

Programa de Pós-Graduação em Engenharia Elétrica
Depto. de Eletrônica e Sistemas-CTG/UFPE, Rua Acadêmico Hélio Ramos s/n
Cidade Universitária, Recife - PE 50.740-530
Tel: (0xx81)2126-8210/11/12, ramal 266, Fax: (0xx81)2126-8215
E-mail: andrea@ee.ufpe.br, http://www.ee.ufpe.br/ppgee/

Resumo da Dissertação apresentada à Universidade Federal de Pernambuco como parte dos requisitos necessários à obtenção do grau de Mestre em Engenharia Elétrica.

ANÁLISE DO TRÁFEGO DE VOZ EM REDES MPLS

MARCOS ANTONIO ALVES GONDIM

Junho / 2009

Orientador: Rafael Dueire Lins, Ph.D.

Área de concentração: Telecomunicações.

Linha de Pesquisa: Redes de Computadores.

Palavras-chave: VoIP, MPLS, Telefonia, Qualidade de Serviço.

Número de páginas: 113

É comum associar a telefonia IP somente a aplicativos tais como: Skype, Gizmo e MSN. Entretanto um segmento muito mais expressivo na área de telefonia IP começa a despontar: as redes de alto tráfego de voz e com exigência de altíssima disponibilidade e qualidade de serviço.

Há hoje o interesse real e crescente em se reduzir custos com equipamentos e com ligações telefônicas. Esta dissertação contempla a análise do tráfego de voz através de enlaces Multiprotocol Label Switching (MPLS) buscando-se boa qualidade de voz e a disponibilidade de 99,999%, já alcançada pela Rede Pública de Telefonia (PSTN). As redes MPLS tornam possível a interoperabilidade entre o roteamento de pacotes e a comutação de circuitos, além de reduzir o consumo de recursos dos roteadores permitindo obter um melhor desempenho da rede.

Os experimentos efetuados no desenvolvimento desta dissertação indicam que pode-se obter a disponibilidade e qualidade de serviço necessárias para substituir as soluções convencionais de telefonia, utilizando-se o protocolo IP para o tráfego de voz sobre uma rede MPLS.

Abstract of Dissertation presented to UFPE as a partial fulfillment of the requirements for the degree of Master in Electrical Engineering.

AN ANAYSIS OF VOICE TRAFFIC IN MPLS NETWORKS

MARCOS ANTONIO ALVES GONDIM

June / 2009

Supervisor: Rafael Dueire Lins, Ph.D.

Area of Concentration: Telecommunications

Line of Research: Computer Networks.

Keywords: VoIP, MPLS, Telephony, Quality of Service

Number of pages: 113

It is common to associate IP telephony with applications such as: Skype, Gizmo and MSN. However, a far more expressive segment in IP telephony area is starting to gain importance: the high traffic voice networks, which should provide a close to integral disponibility and high quality of service.

There is today growing interest in reducing the costs of equipment and phone calls. This dissertation presents an analysis of voice traffic trough the Multiprotocol Label Switching (MPLS) networks targeting good voice quality and at 99,999% system availability a standard already reached by the Public Switched Telephone Network (PSTN). MPLS networks allow the interoperability between routing packets and circuit switching, besides reducing the demand for resources of routers allowing for a better network throughput.

The experiments performed in the development of this dissertation indicate that it is possible to obtain the availability and quality service needed to replace the conventional telephone solutions, using the IP protocol for voice traffic on a MPLS network.

Dedico este trabalho ao meu avô, João Alves da Silva,
pelo amor, exemplo e força que sempre recebi.

Agradecimentos

Primeiramente dou graças a Deus por todas as bênçãos e oportunidades recebidas. Agradeço também a minha família, especialmente a minha mãe Eugenia Alves da Silva, ao meu tio Laudelino Alves da Silva, a minha irmã Luciana Maria Alves Gondim e aos meus avós João Alves e Maria de Lourdes.

De uma forma igualmente especial agradeço pelo amor e pela força recebidos da minha noiva, Gemma Gonçalves de Araújo, que sempre me acompanhou sendo uma companheira fiel.

Agradeço ao meu orientador, professor Rafael Dueire Lins, pela confiança depositada em mim e por partilhar seu conhecimento e experiência. Aos componentes da banca examinadora, professores Carmelo José Albanez Bastos Filho e Valdemar Cardoso da Rocha Júnior pelas observações, contribuições e críticas construtivas.

Por fim agradeço a todos os amigos e pessoas que torceram e se felicitaram pelo êxito na conclusão do curso. Muito obrigado a todos.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Acrônimos

ADSL - Assymmetric Digital Subscriber Line

AS - Autonomous System

ATM - Asynchronous Transfer Mode

BGP - Border Gateway Protocol

CE - Customer Edge

CODEC - Coder / Decoder

CSR - Cell Switching Routers

DEP - Densidade Espectral de Potência

EIGRP - Enhanced Interior Gateway Routing Protocol

FAC - Função de Autocorrelação

FDP - Função Densidade de Probabilidade

FEC - Forwarding Equivalency Class

IETF - Internet Engineering Task Force

IP - Internet Protocol

IS-IS - Intermediate System-to-Intermediate System

ITU-T - International Telecommunications Union – Telecommunications

LBI - Label Base Information

LBS - Label Based Switching

LDP - Label Distribution Protocol

LSP - Label Switched Path

LSR - Label Switch Router

MPLS - Multiprotocol Label Switching

OSI - Open Systems Interconnection

OSPF - Open Shortest Path First

P2P - Peer-to-Peer

PABX - Private Automatic Branch Exchange

PCM - Pulse Code Modulation

P - Provider Routers

PE - Provider Edge Routers

PSTN - Public Switched Telephone Network

SNR - Signal-to-Noise Ratio

SNR_Q - Quantization Signal to Noise Ratio

QoS - Quality of Service

RFC - Request for Comments

RSVP - Reservation Protocol

RTCP - Real Time Control Protocol

RTP - Real Time Protocol

RTSP - Real-Time Streaming Protocol

TCP - Transport Control Protocol

TCP/IP - Transport Control Protocol / Internet Protocol

TDM - Time Division Multiplexing

TTL - Time to Live

UDP - User Datagram Protocol

UMTS - Universal Mobile Telecommunication System

VAD - Voice Activity Detector

VoIP - Voice over IP

VPN - Virtual Private Network

VR – Virtual Routers

VRF - VPN Routing and Forwarding

WAN - Wide Area Network

WCDMA - Wideband Code Division Multiple Access

WiMAX - Worldwide Interoperability for Microwave Access

1. **Introdução**

Com o advento da telefonia IP, que se iniciou na década de 1990, e que agora no início do século XXI tem o seu momento mais expressivo, pessoas e empresas esperam pagar menos pelo serviço de comunicação telefônica. Costuma-se associar a telefonia IP com os aplicativos de conversação usados em computadores, tais como: Skype, Gizmo e MSN, que são utilizados geralmente para realizar ligações interurbanas ou internacionais com um menor custo, ou às vezes gratuitas desde que os interlocutores tenham o mesmo software de conversação instalado em seus computadores. Entretanto, um segmento muito mais expressivo na área de telefonia IP começa a se erguer de forma menos evidente aos olhos daqueles que não estão diretamente envolvidos com a área de tecnologia, que são as redes de alto tráfego de voz e com exigência de total disponibilidade e qualidade de serviço.

No caso de grandes empresas com suas dezenas de pontos de representação espalhados por um país ou no caso de *call centers* com suas centenas de pontos de atendimento, as soluções citadas no parágrafo anterior não atendem à demanda e as necessidades dessa parcela do mercado. O tráfego elevado de chamadas e a necessidade de uma conversação totalmente inteligível são características indispensáveis à solução de telefonia de uma empresa de grande porte e por isso se faz necessário uma solução mais robusta e inteligente que garanta a qualidade do serviço.

Pode-se perguntar então o que há de errado com o sistema telefônico convencional ou PSTN (*Public Switched Telephone Network*) para que se busque novas soluções de telefonia visto que este já é para um sistema amplamente utilizado e amadurecido. Quanto a PSTN não há nada de errado, seja na qualidade de voz, seja quanto à confiabilidade da

rede. Na verdade ela representa robustez e segurança, porém a qualidade da voz somente parece não ser mais suficiente para satisfazer um mercado crescente e cada vez mais complexo e exigente quanto à diversidade de serviços procurados. A mudança de necessidades do mercado empresarial e residencial apontam para novas características e capacidades telefônicas.

Como fruto desta evolução no mercado das telecomunicações, é realizada a convergência de tecnologias de voz, dados e vídeo em um único produto oferecido pelas operadoras chamado *triple play* e para cada avanço tecnológico que aumenta a capacidade técnica das operadoras de telecomunicações, surge uma nova aplicação que consome os ganhos de desempenho.

1.1. **Motivação**

Baseando-se no fato do interesse real e crescente em se reduzir custos com equipamentos e com ligações é que este trabalho contempla a análise e o estudo do tráfego de voz através de enlaces dedicados com alta qualidade de voz e também almejando a disponibilidade de 99,999% já alcançada pela telefonia convencional. Utilizando-se dos benefícios trazidos pela tecnologia das redes *Multiprotocol Label Switching* (MPLS), que tornou possível a interoperabilidade entre o roteamento de pacotes e a comutação de circuitos, do protocolo de roteamento para grandes redes *Border Gateway Protocol* (BGP) e dos *codecs* com grande capacidade de compressão de voz, pretende-se mostrar que se pode obter a disponibilidade e qualidade de serviço muito semelhante à que as redes PSTN (*Public Switched Telephone Network*) oferecem, utilizando-se o meio IP para o tráfego de voz.

1.2. **Objetivo**

O objetivo desta dissertação é propor e analisar o desempenho de uma solução de telefonia IP confiável, escalável e segura, baseando-se em um meio de transmissão MPLS que possa substituir confiavelmente as soluções de telefonia convencional (PSTN) existentes a um menor custo e sem perdas de qualidade.

As soluções de telefonia IP mais difundidas utilizam a *Internet* como meio para o tráfego de voz na forma de pacotes IP. Entretanto existem nestas soluções alguns pontos negativos que inviabilizam o uso destas soluções em determinadas situações tais como serviço de atendimento ao cliente (SAC) e central de vendas de uma empresa, pois existem regras rígidas que devem ser seguidas para o atendimento nestes casos. Soluções VoIP que utilizam a *Internet* como meio de comunicação concorrem com o tráfego de pacotes das mais diversas aplicações tais como: *e-mail*, transferência de arquivos, acesso a sites dentre outros. O fato de não haver gerência do meio de transmissão, propicia perda na confiabilidade da entrega dos pacotes e vulnerabilidade quanto à segurança das informações.

Finalmente também é objetivo deste trabalho superar os pontos de vulnerabilidade das aplicações VoIP que utilizam a *Internet* e assim mostrar que a solução de telefonia IP pode substituir confiavelmente a telefonia convencional em aplicações que requerem maior rigor quanto aos quesitos de segurança, disponibilidade e qualidade nas ligações.

1.3. **Organização da Dissertação**

Além deste capítulo introdutório, esta dissertação é composta de mais quatro capítulos cujos conteúdos são descritos a seguir:

Capitulo 2 – Telefonia IP

Apresenta uma idéia geral do que são Sistemas de Voz sobre IP e prepara o leitor para um melhor entendimento do projeto do sistema telefônico proposto neste trabalho.

Capítulo 3 – Redes MPLS

Apresenta a estrutura, o modo de funcionamento e as principais características de uma rede MPLS. Também neste capítulo é justificada a escolha da rede MPLS como a base do projeto do sistema de telefonia apresentado nesta dissertação.

Capítulo 4 – Experimento

Apresenta a idealização, montagem e execução dos testes realizados para a análise da rede MPLS com o objetivo de se trafegar voz sobre IP.

Capítulo 5 – Conclusões e trabalhos futuros

Apresenta uma análise dos resultados dos testes das ligações utilizando-se a rede MPLS e as compara com os resultados das ligações realizadas com a rede VoIP sobre rede par-a-par. O capítulo apresenta também sugestões para trabalhos futuros.

2. **Telefonia IP**

Este capítulo apresenta os fundamentos da telefonia IP com o objetivo de possibilitar o melhor entendimento dos próximos capítulos. São descritos os principais codificadores de voz utilizados em soluções VoIP, a importância da implementação da Qualidade de Serviço e uma breve abordagem da recomendação H.323 que foi utilizada no projeto da rede VoIP sobre MPLS apresentada nesta dissertação no capítulo 4.

2.1. **Fundamentos da Telefonia IP**

A Rede Pública de Telefonia é uma rede comutada por circuitos destinada ao serviço de telefonia, sendo administrada pelas operadoras de serviço telefônico. Inicialmente foi projetada como uma rede de linhas fixas e analógicas, porém atualmente é digital e inclui também dispositivos móveis como os telefones celulares. De uma forma simplificada, o acesso do assinante nesse modelo de sistema telefônico, é feito por meio das centrais telefônicas que oferecem o serviço básico de telefonia através de telefones residenciais comuns ou sistemas digitais de PABX (*Private Automatic Branch Exchange*) como solução de telefonia para empresas [1].

Já em uma rede de telefonia IP, temos o sinal de voz transformado em informação digital e trafegando através de uma rede como pacotes IP. As questões de segurança, confiabilidade e qualidade dos serviços prestados pelas operadoras de telefonia convencional e as operadoras de telefonia que fornecem a solução de voz sobre IP tem aspectos bastante distintos, porém alguns pontos são comuns entre eles tais como: a

necessidade de digitalizar o sinal analógico da voz, contornar o problema de ecos nas ligações e a qualidade de serviço da rede utilizada para o tráfego das conversações.

A seguir, será exposta de forma simplificada a técnica utilizada para o processamento e a conversão analógico/digital de sinais de voz. As seções 2.3 e 2.4 apresentam uma explanação sobre codificadores. Na seção 2.5 é apresentado um estudo sobre a qualidade de serviço exigida em uma rede IP para o tráfego de voz.

2.2. **Processamento da voz**

A voz humana possui diversas características que podem ser utilizadas para a construção de codificadores mais eficientes [10, 58]. Algumas dessas características tais como: a não-uniformidade da função distribuição de probabilidade das amplitudes da voz; a correlação não-nula entre amostras de voz sucessivas; o espectro de voz não-plano; a existência de segmentos vocais e não-vocais na fala são fortemente exploradas nesse aspecto e permitem o uso de técnicas de quantização eficientes [10].

Uma característica fundamental do sinal de voz é a de poder ser considerado de banda limitada, pois embora possua componentes de amplitude não-nula por uma faixa relativamente larga do espectro, a maior parte de sua energia encontra-se concentrada em frequências abaixo de 4 kHz, sendo essa frequência considerada um limite prático. De acordo com o critério de Nyquist, essa característica permite que o sinal de voz seja amostrado a uma taxa finita [10], correspondente ao dobro de sua máxima frequência e reconstruído a partir de suas amostras. O sinal de voz é modelado através de ferramentas estatísticas.

A Função Densidade de Probabilidade

A não-uniformidade da função densidade de probabilidade (fdp) da fala é uma de suas características mais exploradas. A fdp de um sinal de voz possui amplitudes muito altas perto do zero de freqüência, decrescendo monotonicamente com o aumento da freqüência até se tornar praticamente nula em frequências altas. A fdp de longo prazo de um sinal com qualidade telefônica pode ser aproximada por uma distribuição exponencial Laplaciana definida por [59]:

$$p_{it}(x) = \frac{1}{\sqrt{2\sigma_x}} e^{-\frac{\sqrt{2}|x|}{\sigma x}}. \quad (1)$$

Para modelar a fdp de curto prazo é utilizada a distribuição Gaussiana definida por:

$$p_{st}(x) = \frac{1}{\sqrt{2\pi\sigma_x^2}} e^{-\frac{(x-m_x)^2}{2\sigma_x^2}}, \quad (2)$$

com m_x sendo a média e σ_x^2 a variância das distribuições. Ambas as distribuições possuem um pico em zero devido à presença frequente de segmentos de fala de baixa intensidade.

A Função de Autocorrelação

A função de autocorrelação (fac) determina uma medida quantitativa do grau de similaridade entre duas amostras de um sinal de voz em função da separação temporal *k* entre as mesmas. A fac para sinais de tempo discreto é definida pela expressão [59]:

$$C[k] = \frac{1}{N} \sum_{n=0}^{N-|n|-1} \{x[n].x[n+|k|]\}. \quad (3)$$

A função de autocorrelação é geralmente normalizada com a variância do sinal de voz e excursiona entre valores do intervalo [−1,1] com C[0] =1. Isso implica que em cada amostra existe uma grande quantidade de informação que é facilmente previsível a partir dos valores das amostras anteriores com um pequeno erro aleatório. Valores típicos da função de autocorrelação entre amostras consecutivas C[1] de um sinal de voz estão entre 0,85 e 0,9.

A Função Densidade Espectral de Potência

A função densidade espectral de potência (dep) é a representação frequencial via transformada de Fourier da função de autocorrelação, segundo o teorema de Wiener-Kintchine [2]. A função densidade de potência espectral da fala é não-plana. Assim, é possível se obter uma compressão significativa codificando o sinal no domínio da freqüência. Tal característica do sinal de voz é simplesmente uma manifestação no domínio da freqüência do fato da função de autocorrelação ser não-nula [10]. Típicas

distribuições da função densidade de potência espectral mostram que as componentes de alta freqüência de um sinal de voz contribuem muito pouco para a energia total do sinal, no entanto, carregam informações importantes sobre o mesmo, devendo ser adequadamente representadas no sistema de codificação.

A análise e a síntese de voz são as duas etapas que constituem o processamento da voz, onde a análise constitui a parte do processamento da voz que é capaz de converter a voz humana em uma forma digital, possibilitando assim o seu armazenamento ou transmissão em computadores. Quanto à etapa da síntese da voz, é realizado o processo inverso, pois convertem-se os dados de voz digital em uma forma similar a da voz original, que seja capaz de ser reproduzida em um transdutor [2, 3].

Um *codec* (codificador-decodificador) é um dispositivo capaz de realizar as funções de análise e síntese de voz. O *codec* é dividido em três partes básicas: amostragem, quantização e codificação. A amostragem e quantização são etapas da conversão analógico-digital que tem como finalidade converter o sinal de voz em uma forma que possa ser entendida e processada por um computador digital. A função da codificação é comprimir e proteger os dados, ou seja, representar o sinal de voz digitalizado utilizando o menor número de bits possível, de forma a economizar memória durante o armazenamento e largura de banda, durante a transmissão do mesmo e possibilitar que possíveis erros sejam detectados e corrigidos [55].

Um conversor analógico-digital (conversor A/D) é um dispositivo que recebe como entrada um sinal de tempo contínuo e amplitude contínua (sinal analógico) e produz como saída um sinal de tempo discreto e amplitude discreta (seqüência discreta). Dois processos estão envolvidos nessa tarefa: a amostragem (discretização no tempo) e a quantização (discretização na amplitude) [56].

De um modo geral, no conversor A/D, o sinal analógico é convertido em uma seqüência de amostras que o representam no domínio digital. Uma seqüência produzida pelo conversor A/D, portanto, representa a informação de entrada com um determinado grau de precisão, o qual depende da freqüência com que o sinal é amostrado (resolução no tempo) e da quantidade de bits utilizados para representar cada amostra (resolução na amplitude).

O processo de amostragem consiste em colher periodicamente o valor instantâneo do sinal, o qual é geralmente realizado a uma taxa constante conhecida como freqüência de amostragem de acordo com o teorema de Shannon-Nyquist [57]. Os valores das amostras

em cada instante são obtidos utilizando a técnica conhecida como *sample-and-hold* na qual o valor do sinal em um dado instante é carregado e mantido em um capacitor até que a amostragem de um novo trecho do sinal seja realizada.

Como resultado do processo de amostragem, tem-se um sinal de tempo discreto, cujos valores só são definidos em pontos discretos do eixo temporal, mas com uma amplitude que ainda varia no contínuo. A próxima etapa da conversão A/D é a discretização do eixo das amplitudes do sinal através da quantização. A quantização é um processo não-linear que tem como objetivo mapear o valor da amplitude do sinal que varia no *continuum* em um número finito de valores discretos (geralmente números binários).

Existem várias técnicas de quantização, a seguir serão abordadas a **quantização uniforme, a quantização não-uniforme, a quantização adaptativa e a quantização vetorial**.

2.2.1. **Quantização Uniforme**

Na técnica de quantização uniforme a máxima excursão do sinal R é dividida em 2^n segmentos iguais, sendo cada um deles representado por uma única palavra-código de n bits. O passo de quantização s é o comprimento de cada segmento e é definido através da expressão:

$$R = s.(2^n). \tag{4}$$

Haverá um ceifamento do sinal caso o valor da amostra de entrada seja maior que R. O processo de quantização é inerentemente um processo com perdas. A diferença entre o valor real da amostra $x[n]$ e a sua representação discreta (quantizada) $Q\{x[n]\}$ produz um erro não-linear $e[n]$, conhecido como ruído de quantização e dado por:

$$e[n] = x[n] - Q\{x[n]\}. \tag{5}$$

A função de mapeamento da quantização uniforme é ilustrada através do exemplo da figura 2.1.

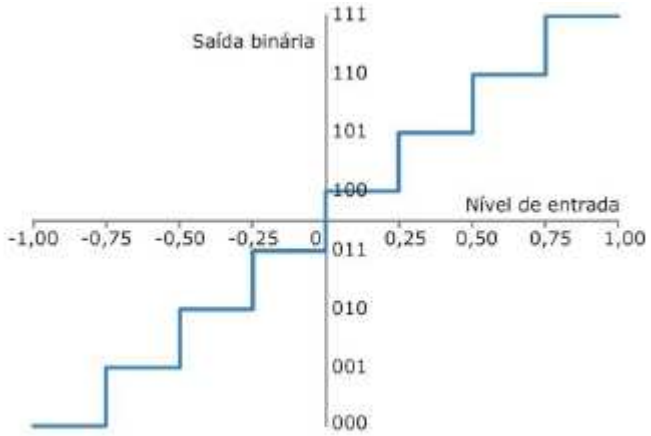


Figura 2.1 – Quantização Uniforme.

A não linearidade é introduzida pelas aproximações sucessivas por arredondamento ou truncamento em sistemas realimentados e podem gerar padrões repetitivos ou ciclos-limite [2] causando tons audíveis indesejados em sistemas de áudio.

Para os casos de um sinal de banda larga como o de voz, que flutua rapidamente entre todos os níveis de quantização, cruzando vários deles de uma amostra para outra, a análise pode ser realizada de forma bastante precisa através de ferramentas de estatística [2].

Essa análise consiste em substituir a fonte não-linear do ruído de quantização por uma fonte estocástica linear equivalente cuja função densidade de probabilidade é uniforme no intervalo de quantização. O quantizador pode ainda utilizar uma estratégia de aproximação por truncamento ou arredondamento da amostra. Sendo m_e a média e σ_e^2 a variância da fonte de ruído linear equivalente, para uma palavra de (B+1) bits, tem-se que:

Para aproximação por arredondamento:

$$\begin{cases} -\frac{1}{2}2^{-B} < e[n] \leq \frac{1}{2}2^{-B} \\ m_e = 0 \\ \sigma_e^2 = \frac{2^{-2B}}{12} \end{cases} . \tag{6}$$

Para aproximação por truncamento:

$$\begin{cases} -2^{-B} < e[n] \leq 0 \\ m_e = -\frac{2^{-B}}{2} \\ \sigma_e^2 = \frac{2^{-2B}}{12} \end{cases} . \tag{7}$$

A razão entre a energia do sinal e a energia do ruído dada em decibéis (dB) é definida com a *relação sinal-ruído*. Para um total de *N* amostras, a relação sinal-ruído é dada por:

$$SNR_{dB} = 10 \log . \left(\frac{\sum_{n=1}^{N} x^2[n]}{\sum_{n=1}^{N} e^2[n]} \right). \tag{8}$$

Se o valor do *SNR* for baixo a voz perde inteligibilidade. O patamar aceito para voz com qualidade telefônica corresponde a um sinal de voz cuja relação sinal-ruído se mantém acima de 30 dB [3].

Além disso, cada acréscimo/diminuição de 1 bit na palavra digital do quantizador faz com que a relação sinal-ruído devido à quantização SNR_Q melhore ou piore em aproximadamente 6 dB conforme a expressão:

$$SNR_Q = 6{,}02n + \alpha, \tag{9}$$

onde n representa o número de bits e α é um escalar que assume os valores α =0 para SNR_Q médio e α = 4,77 para SNR_Q de pico [59].

2.2.2. **Quantização Não-Uniforme**

Na quantização uniforme, a relação sinal-ruído é dependente da amplitude do sinal, sendo pior para sinais de entrada de baixa amplitude e melhor para sinais de entrada com maiores amplitudes [10]. Assim, com o objetivo de minimizar os efeitos do ruído de quantização e manter uma relação sinal-ruído constante em todos os níveis de amplitude do sinal, uma técnica de quantização não-uniforme deve ser empregada. Os quantizadores não-uniformes alocam mais níveis de quantização para as regiões com alta probabilidade e menos níveis para as regiões com baixa probabilidade, otimizando assim o processo de quantização.

A forma mais popular de quantização não-linear é a quantização logarítmica. Com o uso da quantização logarítmica, ao invés de se quantizar a amostra propriamente dita $Q\{x[n]\}$, codifica-se o seu logaritmo $Q\{y[n]\}$ através da expressão:

$$y[n] = h + k.log\ x[n]\ , \tag{10}$$

sendo h e k constantes positivas. Essa expressão é válida apenas para valores positivos de $x[n]$ e uma aproximação linear por partes deve ser utilizada para abranger valores nulos ou negativos, como mostra a figura 2.2.

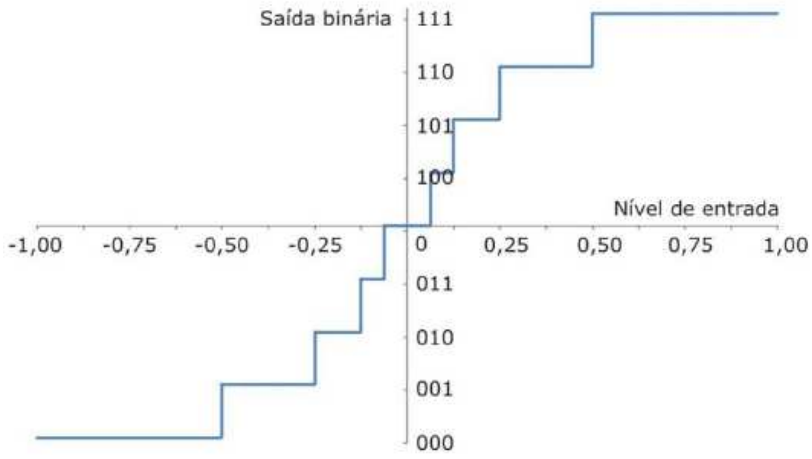


Figura 2.2 – Quantização Logarítmica.

Uma operação de expansão através da função exponencial é necessária para se recuperar o sinal no receptor. O ciclo completo é geralmente chamado de *companding* formado a partir da junção das palavras do inglês para compressão e expansão (*compressing/expanding*).

2.2.3. **Quantização Adaptativa**

Os sinais de voz possuem uma característica de não-estacionariedade que implica em diferenças entre suas funções densidade de probabilidade de curto e longo prazo. De fato, esse aspecto faz com que a variação de um sinal de voz possa excursionar numa escala de 40 dB ou mais [10].

Através da quantização adaptativa é possível explorar essa característica de forma a obter uma melhor relação sinal-ruído na voz digitalizada final. A quantização adaptativa

consiste em adequar dinamicamente o passo de quantização a cada trecho do sinal, expandindo-o à medida que o sinal aumenta de intensidade e vice-versa.

Existem várias formas de quantização adaptativa que podem usar tanto quantizadores uniformes quanto não-uniformes (*adaptative PCM, feed foward adaptative PCM, feedback adaptative PCM*) e todas tentam balancear o acréscimo no passo de quantização com a diminuição na relação sinal-ruído associada. Tais quantizadores são conhecidos como quantizadores de bloco, pois aspectos como: energia de curto prazo, variância, faixa dinâmica são calculados sobre um bloco de *N* amostras para o ajuste do passo de quantização. Os quantizadores podem ainda ser divididos em instantâneos ou silábicos, dependendo da taxa com a qual novas informações sobre o trecho de voz são adquiridas e novos parâmetros de adaptação calculados. Os quantizadores silábicos diferem dos instantâneos porque suas características são atualizadas com uma taxa próxima a da ocorrência das sílabas em um trecho de fala. A quantização adaptativa funciona como se cada trecho do sinal de voz possuísse um quantizador próprio, feito sob medida para as suas necessidades, diminuindo o desperdício e aumentando a eficiência do sistema, como mostrado na figura 2.3.

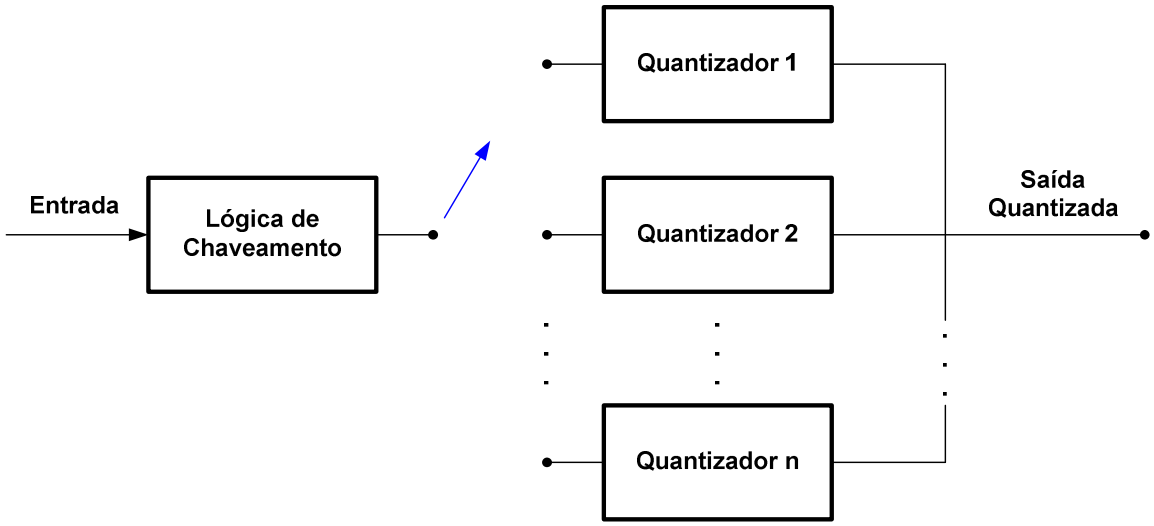


Figura 2.3 – Quantização Adaptativa.

Para sistemas com palavras com mesmo número de bits, quantizadores que utilizam a quantização adaptativa apresentam um ganho na relação sinal-ruído em comparação aos que não a utilizam de aproximadamente 6 dB, ou seja, funcionam como se possuíssem virtualmente um bit a mais na palavra de quantização [2].

2.2.4. **Quantização Vetorial**

A quantização vetorial é uma técnica na qual um grupo de vetores de entrada que possuem certa “proximidade” são agrupados e mapeados em um único vetor que representa todos os membros desse conjunto [2].

Os diversos vetores de entrada são mapeados em um vetor do dicionário de acordo com a região do espaço na qual estejam localizados. Ou seja, a quantização vetorial é uma técnica de divisão do espaço composto pelos possíveis sinais de entrada (em partes geralmente disjuntas), seguida da escolha de um representante para cada uma das partições nas quais o espaço foi dividido.

Esses vetores de representação são escolhidos após sessões de treino periódicas por um algoritmo de treinamento, de forma que sejam os melhores representantes da coleção de sinais de cada conjunto através de algum critério (e.g. erro mínimo quadrático).

Em seguida, os vetores de representação são agrupados em um dicionário (*codebook*) e associados a um dado índice. Durante a operação normal, após receber um vetor de entrada da fonte, o quantizador decide a qual conjunto ele pertence e o substitui pelo vetor de representação deste conjunto (ou pelo seu respectivo índice no dicionário). Dessa forma, o ruído de quantização é definido pela “distância” entre o vetor de entrada e o seu respectivo vetor de representação presente no dicionário [2]. O desempenho da quantização vetorial é função da eficiência do algoritmo de treinamento para construção de seu dicionário.

2.2.5. **Reconstrução do sinal**

Na conversão analógico-digital, um número discreto de amostras deve ser colhido do sinal analógico original. O bom-senso intuitivamente levaria a crer que um número demasiadamente pequeno de amostras resultaria em uma reconstrução imperfeita do sinal original devido à perda de informação entre amostras.

Por outro lado, se poderia pensar que, quanto mais freqüentemente fossem colhidas as amostras, mais perfeita seria a reconstrução, dado que os espaços entre amostras seriam menores. Esse fato se estenderia indefinidamente com a diminuição dos espaços ente as amostras, porém, sempre alguma perda seria esperada.

No entanto, o Teorema de Shannon-Nyquist mostra que, dadas algumas condições, um conjunto de amostras indexadas nos inteiros, podem sim representar perfeitamente um sinal que varia no continuum sem nenhuma perda de informação. O teorema é anunciado como segue:

Seja um sinal $f(t)$ de banda limitada, ou seja, cujo espectro de freqüências via transformada de Fourier $F(j\Omega)$ é nulo para freqüências acima de certa freqüência máxima Ω_M. Para que nenhuma informação seja perdida no processo de amostragem, deve-se amostrar esse sinal com uma taxa maior ou igual que o dobro da máxima frequência presente em seu espectro de Fourier [5, 113]. Essa freqüência Ω_S é chamada freqüência de Nyquist ou freqüência de amostragem do sinal.

$$\text{Se: } f(t) \leftrightarrow F(j\Omega), \text{ e } \Omega>\Omega_M \rightarrow F(j\Omega)=0, \text{ então: } \Omega_S \geq 2\Omega_M.$$

O critério por trás do teorema de Shannon-Nyquist é bastante sutil, mas de uma enorme aplicação prática. Ocorre que um sinal não pode ser ao mesmo tempo limitado nos domínios do tempo e da freqüência. O sinal de voz é de tempo finito, logo ele possui infinitas componentes no domínio da frequência. No entanto, a amplitude das componentes de alta frequência tornam-se cada vez menores a partir de certo ponto que define a banda efetiva do sinal, podendo assim ser desprezadas. Desse modo, na prática filtra-se o sinal levando suas componentes espectrais de alta freqüência tão próximas de zero quanto possível através dos filtros anti-*aliasing*. Ou seja, os filtros anti-*aliasing* forçam o sinal a ter banda limitada para que o teorema possa ser aplicado normalmente.

A voz humana possui componentes espectrais até uma freqüência de aproximadamente 12 kHz, no entanto, uma grande parcela dessas componentes não contribuem de forma essencial para a formação do sinal de voz. A maior parcela da energia do sinal de voz encontra-se até os 4 kHz, portanto, em aplicações de telefonia por exemplo, o sinal de voz é filtrado em 3,3 – 4 kHz e amostrado em PCM a uma taxa de 8.000 amostras por segundo (de acordo com o teorema de Shannon-Nyquist). Desse modo, tem-se não só um sinal inteligível, mas também a possibilidade de reconhecimento do interlocutor.

2.3. **Codificadores de Voz**

Todo canal de comunicação possui uma capacidade limitada de transportar informação. Os *codecs* (codificadores-decodificadores) são sistemas que permitem representar sinais de voz (ou vídeo) de forma eficiente através de um número mínimo de bits, reduzindo a largura de banda necessária para sua transmissão e a quantidade de memória necessária para seu armazenamento [4]. Os codificadores de voz podem ser divididos em três grupos: codificadores Forma de Onda, Paramétricos e Híbridos [5]. A tabela 2.1 enumera os codificadores de acordo com suas características.

Tabela 2.1 – Tipos de codificadores de voz.

Codificador	Taxa de Codificação
Forma de Onda	32 a 64 kbits/s
Paramétrico	1,2 a 9,6 kbits/s
Híbrido	4,8 a 16 kbits/s

2.3.1. **Codificador Forma de Onda**

Os codificadores de Forma de Onda procuram reproduzir a forma de onda do sinal original, amostra por amostra, de modo que o sinal reproduzido possua a maior semelhança possível com o sinal original. São codificadores de alta qualidade, baixo atraso e pequena complexidade de implementação. Para sinais de voz, estes codificadores só devem ser escolhidos para taxas superiores a 16kbit/s, uma vez que para taxas inferiores a essa existem soluções mais atrativas tais como os codificadores paramétricos. Os codificadores de forma de onda são baseados quase que exclusivamente no teorema de Shannon-Nyquist, embora outras técnicas sejam usadas para minimizar o número de bits necessários para a representação do sinal. A mais comum dessas técnicas é a codificação diferencial, que ao invés de representar o valor de uma amostra, representa a diferença entre amostras sucessivas. O codificador de forma de onda mais simples é o *Pulse Code Modulation* (PCM).

2.3.2. **Codificador Paramétrico**

Ao invés de tentar copiar tão fielmente quanto possível a forma de onda de um sinal de voz, os codificadores de fonte ou codificadores paramétricos representam a fala através de um conjunto de características associados a um modelo simplificado de produção de voz, permitindo assim sua implementação com um custo computacional adequado. Baseados na noção de que o trato vocal muda lentamente e seu estado e configuração podem ser representados por um pequeno conjunto de parâmetros, os codificadores paramétricos extraem e transmitem periodicamente as principais características do sinal de voz.

No entanto, devido à complexidade do processo de geração da voz humana, as modelagens, simplificações e aproximações utilizadas nos codificadores paramétricos introduzem perdas e distorções que acabam por tornar a qualidade da voz obtida nos mesmos inferior àquela obtida em codificadores de forma de onda. Os *vocoders* ou codificadores vocais atingem níveis de compactação consideráveis (operando normalmente entre 1,2 e 9,6 kbps), com uma taxa de transmissão média de 2,4 kbps [6]. Esses codificadores são uma solução em sistemas que possuem restrições de qualidade da voz ou pouca largura de banda disponível, tais como em alguns sistemas de comunicação móvel.

2.3.3. **Codificador Híbrido**

Os codificadores híbridos combinam a qualidade dos codificadores de forma de onda com a eficiência dos codificadores paramétricos. Operam com taxas de transmissão de 4,8 a 16 kbps.

2.4. **Principais codificadores de voz**

A seguir serão descritas as principais recomendações da ITU (*International Telecommunication Union*) dos codificadores de voz estudados na seção 2.3. Serão

abordados aspectos históricos e principais característica das recomendações enumeradas na tabela 2.2.

Tabela 2.2 – Principais Codificadores de Voz.

Referência	Codificador	Taxa de bits (kbps)	Tamanho do quadro (ms)
G.711	PCM	64	0,125
G.722	SB-ADPCM	56	0,125
G.726	ADPCM	32	0,125
G.727	E-ADPCM	32	0,125
G.728	LD-CELP	16	0,625
G.729	CS-ACELP	8	10

2.4.1. **G711**

O G.711 é uma recomendação que foi desenvolvida pelo ITU-T em 1972. Este padrão define um codificador de forma de onda que utiliza PCM (*Pulse Code Modulation*) com quantização logarítmica [7].

As principais formas de compressão logarítmica utilizadas são: μ-Law, utilizada na América do Norte e Japão, e A-Law utilizada na Europa e Brasil [8]. Nos sistemas μ-Law, sinais fracos são amplificados e sinais fortes são comprimidos [9].

O PCM é uma das formas mais simples de se digitalizar voz, sendo usado em redes ISDN e na maioria dos *backbones* de telefonia digital. O espectro de voz utilizado em telefonia possui uma banda de 4 kHz [10], desse modo, segundo o teorema de Shannon-Nyquist, deve-se coletar 8.000 amostras por segundo desse sinal para se obter uma reconstrução perfeita. O G.711 quantifica essas amostras em 256 níveis, utilizando palavras com oito bits de comprimento. A transmissão é realizada com 8.000 amostras por segundo, cada uma com oito bits, totalizando 64 kbps de taxa de transmissão do PCM [10].

2.4.2. **G.722**

O G.711 possui uma qualidade excelente, porém, parte do espectro de voz (acima de 4 kHz) é perdido [10]. Padronizado pelo ITU-T em 1988, o G.722 foi proposto para

aplicações de áudio de alta qualidade codificando a voz no espectro de 50 a 7.000 Hz através do uso do codificador de forma de onda SB-ADPCM (*Sub-Band Adaptive Differential Pulse Code Modulation*) [11]. A codificação em sub-bandas (SBC) subdivide o espectro de voz em um pequeno número de faixas de freqüência (sub-bandas) e os codifica individualmente. As melhorias alcançadas no uso desta técnica residem no fato das sub-bandas poderem ser transladadas no espectro possibilitando o uso de menores taxas de amostragem.

A codificação adaptativa (*Adaptive Coding*) provê melhorias ajustando dinamicamente o passo de quantização ao nível de excursão do sinal, fazendo com que virtualmente cada trecho do sinal possua um quantizador próprio, dimensionado para as suas características. Os quantizadores adaptativos utilizados no G.722 são atualizados em uma taxa próxima a taxa silábica. Dado que amostras sucessivas de um sinal de voz possuem uma alta correlação entre si, permitindo estimativas com razoável nível de acerto, o ADPCM utiliza um preditor linear para estimar o valor da próxima amostra do sinal de acordo com as amostras passadas.

Por sua vez, a quantização diferencial (*Differencial Coding*) explora as características de variação temporal do sinal de voz para codificar o sinal diferença entre o sinal estimado pelo preditor e o sinal que efetivamente é recebido na entrada do codificador, utilizando um menor número de bits em relação ao necessário para codificar o sinal propriamente dito. O G.722 faz uso da combinação dessas técnicas, tornando possível a transmissão de voz de alta qualidade com taxas de 48, 56 e 64 kbps.

2.4.3. **G.726**

Padronizado pelo ITU-T em 1990, o G.726 utiliza um codificador de forma de onda ADPCM (*Adaptive Differential Pulse Code Modulation*) [11]. Projetado para ser uma evolução do G.711, operando em taxas de transmissão mais baixas, o sistema ADPCM do G.726 incorpora três características em relação ao PCM do G.711: predição linear, quantização adaptativa e codificação diferencial. No G.726 os sinais codificados em μ-Law ou A-Law são convertidos em PCM uniforme e a diferença entre este sinal e o seu valor estimado é codificada adaptativamente em uma palavra com comprimento entre cinco e dois dígitos binários, permitindo a operação em 40, 32, 24 ou 16 kbps.

O ADPCM possui um tamanho de passo e um preditor que rastreiam e se adaptam as características estatísticas variantes no tempo da fala. O preditor pode ser pós-alimentado (*feedback adaptive*) ou pré-alimentado (*feed forward adaptive*).

Nos preditores pós-alimentados, cada amostra é quantizada com um passo de quantização resultante das *N* amostras anteriores. Após o recebimento de um bloco de *N* amostras, o passo de quantização é calculado em função dos seus valores e é utilizado na quantização das próximas *N* amostras, e assim por diante. Ou seja, nesse tipo de preditor o passo de quantização é calculado a partir de um bloco de amostras, mas só é aplicado no próximo bloco.

Por sua vez, nos preditores pré-alimentados o bloco de *N* amostras é recebido, os cálculos para determinação do passo de quantização adequado são realizados e estas próprias amostras são quantizadas através dos parâmetros calculados. Ou seja, o passo de quantização é calculado sobre um bloco de amostras e aplicado a este mesmo bloco de amostras.

Os preditores pré-alimentados necessitam acumular o bloco de *N* amostras na memória a fim de realizar as computações necessárias implicando um atraso associado à acumulação das mesmas. Outra desvantagem é que a informação em relação ao passo de quantização deve ser enviada juntamente com as amostras (geralmente uma vez a cada bloco).

No entanto, esse esquema de predição possui a vantagem de seus passos de quantização não são afetados pelo ruído de quantização, já que eles são calculados a partir de amostras não-quantizadas e passados explicitamente ao decodificador. Por outro lado, os preditores pós-alimentados possuem a vantagem de serem instantâneos, porém, as estimativas dos passos de quantização sofrem influência do ruído de quantização já que o decodificador precisa computá-lo a partir de amostras já quantizadas.

2.4.4. **G.727**

Padronizado pelo ITU-T em 1990, o G.727 utiliza um codificador de forma de onda E-ADPCM (*Embedded ADPCM*) capaz de operar a 40, 32, 24 e 16 kbps fazendo uso de 5, 4, 3 ou 2 bits por amostra respectivamente [12].

O sistema foi desenvolvido para converter um sinal PCM 64 kbps em um sinal de taxa variável e vice-versa. Os algoritmos embarcados (*Embedded Algorithms*) são algoritmos de taxa de bit variável com a capacidade de descartar bits externamente aos blocos do codificador e decodificador em qualquer ponto da rede sem a necessidade de uma coordenação entre o transmissor e o receptor. Eles consistem em uma série de algoritmos nos quais os níveis de decisão dos codificadores de taxas baixas são subconjuntos dos níveis de decisão dos codificadores de taxas mais altas.

O G.727 é uma extensão do G.726 e é recomendado para o uso no PVPs (*Packetized Voice Protocol*) definido na recomendação G.764. O PVP possui a capacidade de alterar o tamanho dos pacotes de voz quando necessário. Utilizando a propriedade do algoritmo, os bits menos significativos de cada palavra-código pode ser descartada em qualquer ponto da rede atingindo em momentos de congestionamento um melhor desempenho que o dos algoritmos que descartam pacotes inteiros de voz.

2.4.5. **G.728**

Definido pela ITU-T em 1992, o padrão G.728 estabelece os aspectos de codificação de voz a 16 kbps utilizando um codificador híbrido de baixo atraso com predição linear excitada a código LD-CELP (*Low-Delay Code-Excited Linear Prediction*) [13]. A essência dos algoritmos de procura em dicionários de código (*codebook searching*) CELP é mantida no LD-CELP, no entanto, este último utiliza uma abordagem adaptativa no cálculo do ganho e dos coeficientes do preditor.

O CELP é um codificador otimizado para voz [14] no qual, uma coleção de C possíveis sequências de comprimento L é armazenada nos dicionários do codificador e decodificador. Este codificador trabalha com um bloco (vetor) de cinco amostras, cada uma com um atraso de 0,125 ms totalizando um atraso no algoritmo de apenas 0,625 ms.

Após os sinais de entrada serem convertidos de PCM μ-Law ou A-Law para PCM uniforme, segmentados em vetores de cinco amostras e passados através do filtro de síntese e da unidade de escalonamento, o G.728 os compara com cada um dos 1.024 vetores de seu dicionário. O sistema então identifica o candidato que minimiza o erro médio quadrático em relação ao sinal de entrada e transmite o seu respectivo índice de 10 bits ao

decodificador (daí a taxa de operação desse sistema, de um total de 8.000 amostras coletadas por segundo são transmitidos 10 bits a cada cinco amostras, totalizando 16 kbps).

O melhor vetor-código é então passado pela unidade de escalonamento e pelo filtro de síntese para estabelecer os novos parâmetros a serem utilizados no próximo vetor-sinal de entrada. Os ganhos dos filtros são atualizados a cada vetor, mas os seus coeficientes são atualizados a cada quatro vetores transmitidos, ou seja, 20 amostras PCM ou 2,5 ms. Os parâmetros do preditor são atualizados a partir das amostras de voz que já foram quantizadas anteriormente.

A análise de desempenho do LD-CELP foi publicada em 1995 no apêndice II do G.728. Segundo esse documento, em uma transmissão livre de erros a qualidade do LD-CELP 16 kbps é inferior à alcançada com o PCM 64 kbps, mas equivalente ao ADPCM 32 kbps [14].

2.4.6. **G.729**

Padronizado em 1996 pelo ITU-T, o G.729 é um codificador paramétrico ou vocoder. O padrão descreve uma técnica para codificação de voz a 8 kbps utilizando predição linear de estrutura conjugada excitada por código algébrico CS-ACELP (*Conjugate-Structure Algebraic-Code-Excited Linear Prediction*) [15]. O sistema foi concebido para codificar voz com qualidade total a 8 kbps para uso em comunicações sem-fio e circuitos cabeados transoceânicos [16]. No G.729 o sinal de entrada é filtrado em banda telefônica (4 kHz), amostrado a 8.000 amostras por segundo (PCM 64 kbps) e convertido para PCM linear 16 kbps. Baseado no codificador CELP, o CS-ACELP opera com quadros de voz com 10 ms de duração, ou seja, um bloco 80 amostras. A cada 10 ms, o sistema extrai os parâmetros do modelo CELP (coeficientes do filtro preditor linear e índices e ganhos dos dicionários fixos e adaptativos), codificando-os e transmitindo-os.

Os coeficientes gerados por seus filtros são calculados através do método de autocorrelação por uma janela deslizante de 240 amostras de comprimento que é deslocada a cada 80 amostras (10 ms). Essa janela é composta por duas partes: a primeira (120 amostras) é formada pela metade de uma janela de Hamming e a segunda (120 amostras) por um quarto de ciclo da função cosseno. A janela possui um comprimento total de 240 amostras, divididas em 120 amostras dos quadros passados, 80 amostras do quadro atual e

40 amostras do próximo quadro em um esquema de previsão das próximas amostras (*look-ahead*), resultando num tempo de atraso total de 15 ms para o algoritmo.

Ainda em 1996, o ITU-T publicou os anexos A e B para o G.729. O primeiro reduziu a complexidade computacional e os requisitos de memória do CS-ACELP através de simplificações no modo de operação dos filtros e da forma com a qual a busca é realizada no dicionário de vetores, mantendo no entanto a interoperabilidade com o sistema original. O segundo descreve o detector de voz ativa (VAD – *Voice Activity Detector*) e o gerador de ruído de conforto (CNG – *Comfort Noise Generator*), utilizados na supressão e compactação de silêncio no G.729 e G.729A.

2.5. **Qualidade de Serviço**

O conceito de Qualidade de Serviço (QoS) no projeto inicial do *Internet Protocol* ou IP não foi levado em consideração, afinal a concepção inicial na construção do protocolo era o transporte de dados e não se concebia ainda, a idéia de se transportar voz ou vídeo pela rede. Para a análise e aplicação da QoS em redes IP alguns parâmetros devem ser bem conhecidos [17]:

- Flutuações no tempo do tráfego de pacotes (*jitter*);
- Perda de Pacotes;
- Largura de Banda;
- Latência.

Para se alcançar a qualidade necessária para o transporte de pacotes de aplicações em tempo real, é necessário a caracterização e o controle das flutuações no tempo do tráfego de pacotes na rede, também conhecido como *jitter*. Como uma das medidas de solução para a problemática das variações de tempo do tráfego de pacotes em uma rede IP, surgiu o "*buffer* de pior caso" que tem a função de garantir a entrega dos pacotes. Estes *buffers* são elementos de armazenamento utilizados para garantir um entrega de dados em uma taxa constante, armazenando dados que chegam mais rápidos que o tempo inicialmente estipulado e utiliza esta reserva quando ocorre uma degradação da rede gerando atrasos no tráfego de pacotes.

Um outro elemento importante na análise dos elementos que influenciam a qualidade de serviço em uma rede IP é a perda de pacotes. Uma das causas mais comuns para a perda de pacotes é o tráfego gerado acima da capacidade do link de dados, que gera uma sobrecarga no *buffer* e consequentemente o descarte de pacotes. Outros fatores que podem gerar perda de pacotes são: má qualidade do meio físico de transmissão dos dados gerando atenuação degenerativa do sinal, conectores mal feitos, equipamentos de rede trabalhando em altas temperaturas e alta utilização das CPUs dos roteadores da rede.

Os efeitos da perda de pacotes em uma rede IP podem ser desastrosos em alguns casos devido à lentidão gerada na rede. Mesmo utilizando o UDP (*User Datagram Protocol*), as aplicações de mídia podem utilizar um esquema de correção de erro ou confirmação de recebimento de pacotes. Neste caso, a cada pacote não recebido, o protocolo pára de transmitir a seqüência de dados e retransmite o pacotes perdido, gerando lentidão na conexão.

Um terceiro fator na análise da qualidade de serviço em redes IP que deve ser levado em consideração é a largura de banda disponibilizada para suprir a necessidade de cada aplicação. Uma solução aparentemente simples pode ser sugerida para se contornar este problema, aumentar a largura de banda disponível até que se tenha o necessário para se obter um nível adequado de qualidade de serviço. Porém, algumas questões devem ser levadas em consideração neste momento. Qual o custo financeiro para a obtenção da largura de banda necessária para se obter a qualidade desejada e se cada usuário terá assegurada uma parte justa da largura de banda total?

De todos os elementos que devem ser considerados para o estudo de qualidade de serviço, sem dúvida a latência dos pacotes é o problema mais difícil de ser contornado. A latência é o período de tempo que um pacote de dados leva para ser transmitido da origem até ao seu destino. Em conjunto com a largura de banda, define a capacidade máxima e velocidade de uma rede. Em muitos casos é comum se afirmar que as redes IP são inadequadas para o transporte de dados com latência controlada, porém isto não é verdade.

2.5.1. **Técnicas de Enfileiramento para QoS**

Analisando-se o tráfego de pacotes em uma rede, sabe-se que a cada nó da rede todo pacote que é recebido por um roteador deve ser processado e posteriormente encaminhado para o seu destino de acordo com as regras predefinidas na tabela de

roteamento. Desta forma, o atraso é inserido como uma das variáveis que influenciam na qualidade final de um determinado serviço que utiliza tal rede. O atraso entre o ponto de transmissão e o de recepção é altamente variável, podendo ser muito longo caso haja congestionamento na rede ou se um pacote muito grande estiver sendo transmitido, e caso contrário, se somente um pacote pequeno estiver sendo transmitido em um determinado momento teremos um atraso pequeno.

Buscando minimizar os atrasos inerentes à natureza da própria rede de pacotes IP, algumas técnicas e estudos de enfileiramento de pacotes foram criadas permitindo a alocação de uma parte justa da largura de banda para cada fluxo existente. Abaixo são enumeradas algumas destas técnicas que cuidam da ordenação do pacote nas filas de saída [18]:

FIFO (First In First Out): também chamado de primeiro a chegar primeiro atendido (FCFS – *First Come First Served*), simplesmente emite os pacotes na ordem em que foram recebidos. Se não houver espaço suficiente no *buffer* para guardar o pacote que chega, a política de descarte de pacotes da fila então determinará se o pacote será descartado ou se outros pacotes serão retirados da fila para dar espaço ao pacote que está chegando.

Enfileiramento Prioritário: a regra seguida neste caso é que os pacotes que chegam ao enlace de saída são classificados em classes de prioridade na fila de saída. A classe de prioridade de um pacote pode depender de uma marca explícita que ele carrega em seu cabeçalho, do endereço IP de origem e destino ou do número da porta do seu destino. Cada classe de prioridade tem sua própria fila. Ao escolher um pacote para transmitir, a disciplina de enfileiramento prioritário transmitirá um pacote de classe de prioridade mais alta. A escolha entre pacotes da mesma classe de prioridade é feita, tipicamente pelo método FIFO.

Varredura Cíclica e Enfileiramento Justo Ponderado: No enfileiramento por varredura cíclica, pacotes são classificados do mesmo modo que no enfileiramento prioritário. Porém, havendo uma prioridade de serviço entre as classes, um escalonador de varredura cíclica alterna serviços entre as classes. Uma disciplina de enfileiramento de conservação de trabalho nunca permitirá que o enlace fique ocioso enquanto houver pacotes de qualquer classe enfileirados para transmissão. Quando uma varredura cíclica de conservação de trabalho procura um pacote de uma dada classe e não encontra nenhum, verifica imediatamente a classe seguinte da seqüência da varredura cíclica.

No enfileiramento justo ponderado (WFQ - *Weighted Fair Queuing*) os pacotes que chegam são classificados e enfileirados por classe em suas áreas de espera apropriadas. Como acontece no escalonamento por varredura cíclica, um programador WFQ atende às classes de modo cíclico. A WFQ é também uma disciplina de enfileiramento de conservação de trabalho, assim ao encontrar um classe de fila vazia esta imediatamente passa a classe seguinte na seqüência de atendimento.

O WFQ é diferente da varredura cíclica, pois cada classe pode receber uma quantidade de serviço diferenciado a qualquer intervalo de tempo. Em particular, a cada classe *i* é atribuído um peso w_i. O WFQ garante que em qualquer intervalo de tempo durante o qual houver pacotes da classe *i* para transmitir, a classe *i* receberá uma fração de serviço igual a $w_i/(\Sigma w_j)$, onde o denominador é a soma de todas as classes que também têm pacotes enfileirados para transmissão. No pior caso mesmo que todas as classes tenham pacotes na fila, a classe *i* ainda terá garantido o recebimento de uma fração $w_i/(\Sigma w_j)$ da largura de banda. Assim, para um enlace com taxa de transmissão *R*, a classe *i* sempre conseguirá um vazão de no mínimo $R \cdot w_i/(\Sigma w_j)$.

2.6. **Recomendação H.323**

Uma rede de telefonia necessita de diversos protocolos para poder funcionar, nesse aspecto, o H.323 é muito mais uma avaliação da arquitetura da telefonia IP do que um protocolo específico [2]. Desenvolvida pelo ITU-T em 1996 e tendo recebido diversos melhoramentos e revisões até 2006, a recomendação H.323 define terminais e outras entidades que oferecem serviços de comunicação de multimídia sobre redes comutadas a pacotes que não garantem a qualidade de serviço oferecida [19].

O projeto do H.323 foi bastante referenciado na filosofia de operação do sistema de telefonia convencional PSTN, focando o esforço nos aspectos de brevidade e disponibilidade do sistema. Os sinais do H.323 são curtos e a rede é utilizada o mínimo possível para transportar sinalização de chamadas e ao máximo para transportar voz [20].

O H.323 faz referência a um grande número de protocolos específicos para codificação de voz, estabelecimento e configuração de chamadas, sinalização, transporte de dados e outros.

2.6.1. **Entidades que compõem o H.323**

O padrão H.323 é composto por quatro entidades principais: terminais, *gateways*, *gatekeepers* e unidades de controle de multiponto (MCU – *Multipoint Control Unit*). Todos esses elementos são necessários quando se almeja uma interação entre uma rede H.323 e uma outra rede de comunicação. A seguir são descritos os elementos que compõem uma rede H.323.

Terminal: Este atua como terminal de voz, vídeo e dados através de recursos multimídia. O terminal pode ser uma estação multimídia ou um telefone IP capazes de realizar uma comunicação bidirecional com outra entidade H.323. Os terminais H.323 devem dar suporte obrigatório aos protocolos responsáveis pela codificação de áudio (G.711, G.728, G.729), sinalização, configuração e controle de chamadas (Q.931, H.245 e H.225 – RAS) e transporte de mídia em tempo real (RTP e RTCP).

Gateway: Este é um dispositivo localizado na fronteira da rede H.323. Ele é capaz de realizar os serviços de interface e tradução bidirecional em tempo real entre terminais H.323 localizados em uma rede comutada a pacotes e outros terminais ITU pertencentes à uma rede comutada a circuitos, ou mesmo a outro gateway H.323. O gateway H.323 situa-se entre a rede IP e uma outra rede de telecomunicações (RTCP, PBX, ISDN, GSM, UMTS), realizando a compatibilização dos procedimentos de chamada e formatos de transmissão, bem como a conversão dos protocolos de sinalização e codificadores de voz das duas redes.

Gatekeeper – Este é um dispositivo que fornece os serviços de tradução de endereços e controle de acesso dos terminais, *gateways* e MCUs à rede H.323 de forma centralizada. Tipicamente um *gatekeeper* é uma aplicação implementada em software em um PC, podendo, no entanto, ser incorporada em um gateway ou terminal H.323. Uma coleção de terminais, *gateways* e MCUs sob responsabilidade de um único *gatekeeper* é chamada de zona. Uma zona pode conter desde terminais separados por poucos metros de distância até terminais localizados em continentes diferentes, desde que sejam gerenciados por um único *gatekeeper*. Algumas vezes pode existir um segundo *gatekeeper* apenas para fins de backup ou balanceamento de carga. O *gatekeeper* é responsável pelas funções de tradução de endereços (roteamento), controle de admissão e gerenciamento de zona, podendo opcionalmente realizar as funções de controle de sinalização e autorização das

chamadas, gerenciamento de largura de banda, serviços de diretório e localização de *gateways*. *Gateways* que desejam se comunicar em uma zona controlada por um *gatekeeper* precisam se registrar no mesmo para poder realizar a troca de mídia entre si [23].

2.6.2. **Protocolos e Canais que compõem o H.323**

Os principais protocolos que compõem o H.323 são descritos a seguir.

- H.225 – Tem como função a sincronização dos dados, estabelecimento e controle de chamadas através do RAS (Registro, Autenticação e Status);
- Q.931 - Trata dos aspectos de sinalização, estabelecimento e encerramento de conexões, geração de tons de chamada e de discagem para a interoperabilidade com o sistema de telefonia padrão PSTN;
- H.245 – Este protocolo é responsável pela negociação dos sistemas de codificação utilizados e da taxa de transmissão da comunicação;
- G.7xx – Responsável pela codificação utilizada na mídia;
- RTP – Realiza o transporte de mídia em tempo real;
- RTCP – Controla o protocolo de transporte de mídia (RTP).

O H.323 também define diversos protocolos para prestação de serviços auxiliares. Dentre eles se incluem os seguintes:

- T.12x – Oferecem serviços interativos de comunicação de dados para multiconferências;
- H.450 – Oferece serviços suplementares como chamada em espera, transferência de chamadas e outros;
- H.26x – Protocolos utilizados para a codificação de vídeo;
- H.246 – Protocolo utilizado para interoperação com sistemas de comutação de circuitos (RTPC);
- H.235 – Protocolo que confere aspectos segurança ao sistema (autenticação, integridade e privacidade).

Os dispositivos que compõem o padrão H.323 se comunicam uns com os outros através de três canais lógicos principais definidos nas especificações H.225.0 e H.245 [21]. A especificação H.225.0 descreve como informações de áudio, vídeo, dados e controle

podem ser gerenciadas numa rede de pacotes para proporcionar serviços de conversação em equipamentos H.323 [22]. Esta especificação possui duas partes principais: a sinalização de chamadas e o RAS (*Registration, Admission and Status*). O canal de sinalização é utilizado para configurar conexões entre terminais ou entre um terminal e um *gatekeeper*. O padrão recomenda que as mensagens que trafegam nesse canal utilizem o padrão Q.931 de sinalização e sejam transportadas através do protocolo confiável TCP.

O canal RAS do H.225.0 é utilizado para a comunicação entre um terminal ou um gateway com um *gatekeeper*. O RAS realiza as operações de registro, controle de admissão, ajustes de banda, status e desconexão e deve ser aberto em uma comunicação H.323 antes de qualquer outro canal lógico. O canal H.245 tem a função de realizar o controle das chamadas do H.323. Ele é o responsável pelo controle de fluxo, determinação do mestre e escravo, controle de conferências, cifragem, controle de jitter, negociação de capacidades e pela negociação, abertura e fechamento dos canais lógicos RTP/RTCP que carregam os fluxos de mídia. As mensagens de controle H.245 sempre são confirmadas pelo receptor. O H.245 possui a capacidade de ser tunelado em mensagens de sinalização H.225.0, o que facilita a transposição de *firewalls*.

3. **MPLS**

Este capítulo apresenta a estrutura e o funcionamento das redes que utilizam o MPLS (*Multi Protocol Label Switching*). Inicialmente é realizado um breve histórico sobre a tecnologia e são apresentadas as motivações para o uso deste protocolo e os benefícios trazidos por ele. Posteriormente são estudadas as principais características, a estrutura e os elementos necessários para a construção de uma rede MPLS.

3.1. **Protocolos Anteriores ao MPLS**

A demanda crescente por largura de banda de usuários que utilizam cada vez mais serviços do tipo vídeo conferência, transferência de dados com alto desempenho, multimídia, biblioteca de vídeos, educação à distância e telemedicina movimentou pesquisadores e o mercado de tecnologia a estudar e desenvolver métodos de encaminhamento de pacotes cada vez mais rápidos e eficientes [24].

Uma das tecnologias desenvolvidas foi o ATM (*Asynchronous Transfer Mode*) que ao ser lançado, esperava-se que dominasse o cenário mundial de redes devido às suas altas velocidades, suprindo assim o consumo crescente por banda. Contudo, a tecnologia ATM não era compatível com o IP, o protocolo de rede mais difundido no mundo, sendo necessário o desenvolvimento de uma solução nada simples e muito menos trivial, que integrasse o ATM ao IP. Esta deficiência da rede ATM inviabilizou a sua popularização restringindo-a aos *backbones* das operadoras [34].

Por outro lado, o fato das redes ATM não terem alcançado o sucesso que se esperava alimentou ainda mais a busca por uma tecnologia que satisfizesse as novas necessidades dos usuários de enlaces dedicados de dados. Este trabalho se concentrou na inclusão de um rótulo (*label*) no início de cada pacote e na execução do roteamento baseado no rótulo e não no endereço de destino. Ao se utilizar esta técnica, o roteamento pode ser realizado muito mais rapidamente. Esta técnica se aproxima da tecnologia de circuitos virtuais, pois o X.25, o ATM e o *Frame Relay*, também inserem um identificador do circuito virtual em cada pacote e efetuam o roteamento baseando-se em uma tabela de rótulos, entretanto existem muitas outras peculiaridades que diferenciam esta nova idéia de comutação de pacotes das outras tecnologias de comutação de circuitos tradicionais.

Como resultado foi criada a tecnologia LBS - *Label Based Switching*, que possibilitou a utilização do que há de melhor das redes baseadas em pacotes (como as redes IP) e das redes orientadas a conexão (como as redes ATM). LBS usa rótulos pequenos e de tamanho fixo, que são adicionados aos pacotes quando entram numa rede LBS. Os pacotes etiquetados podem ser agrupados em categorias, e os pacotes de uma mesma categoria vão seguir um mesmo caminho virtual, através da infra-estrutura LBS. Muitas implementações comerciais proprietárias de LSB foram criadas: o IP Switching da Nokia; o CSR - Cell Switching Routers da Toshiba; o TAG Switching da Cisco; o ARIS da IBM; o IP Navigator da Ascend; o Fast IP da 3Com. Cada fabricante tem implementações próprias de LBS, dificultando a interoperabilidade entre eles. Para obter uma solução aberta, inter-operável e independente de protocolos foi padronizado o protocolo MPLS (*Multi Protocol Label Switching* – comutação de rótulos multiprotocolo) pelo IETF através da RFC 3031 [25].

3.2. **Motivações para o uso de Redes MPLS**

No universo do protocolo de endereçamento de pacotes mais popular do planeta, o IP, o roteamento consiste resumidamente, que cada roteador que compõe o caminho entre a origem e o destino do trajeto do pacote, analise o cabeçalho do pacote IP e o encaminhe de acordo com a sua tabela de roteamento. Esta forma de roteamento resulta em um consumo elevado dos elementos de hardware do roteador, tais como processador e memória. Um dos

benefícios trazidos pelo protocolo MPLS é justamente a minimização da utilização desses elementos de hardware.

Numa rede MPLS, somente os roteadores de borda, analisam o cabeçalho IP do pacote, criando um caminho para este dentro da rede MPLS atribuindo ao pacote um rótulo. Assim, os demais roteadores que compõem o núcleo da rede irão somente fazer um chaveamento de rótulos até que o pacote chegue ao seu destino. Desta forma a parte pesada do processamento dos pacotes é feita nas bordas da rede, diminuindo o processamento no núcleo. Como a taxa de pacotes no núcleo da rede é maior que a taxa de pacotes nas bordas, agiliza-se assim o processo [26].

Em relação a aplicações que exigem tempo real, a rede MPLS oferece a implementação de QoS, que se pode definir como sendo um requisito das aplicações para a qual se exige que determinados parâmetros (atrasos, vazão, perdas, variação de atrasos ou jitter, largura de banda) e que estes estejam dentro de limites bem definidos. Com a implementação do QoS pode-se diferenciar diversos tipos de tráfegos e tratá-los de forma distinta, dando prioridades às aplicações mais sensíveis. Outro fator importante numa rede MPLS é a facilidade da implementação de engenharia de tráfego, onde tem-se a opção de distribuir a carga de um enlace saturado, podendo por exemplo, escolher caminhos mais rápidos, porém com custo mais elevado, para pacotes de maior prioridade e desta forma melhorar o desempenho da rede.

Resumidamente uma rede MPLS além de acelerar o processo de encaminhamento dos dados, fornece diversas aplicações tais como suporte à QoS e Engenharia de Tráfego favorecendo a utilização do tráfego de pacotes de voz sobre IP em link de dados [27]. Além disso, é facilmente escalonável e possui interoperabilidade, ou seja, suporta redes com tecnologias distintas (*Ethernet*, ATM, Frame *Relay*, entre outras), pois é capaz de calcular caminhos tanto para pacotes como para células.

3.3. **O Cabeçalho MPLS**

No projeto do protocolo MPLS um dos desafios foi descobrir uma forma de se colocar o rótulo na estrutura do pacote, tendo-se em vista que os pacotes IP não foram projetados para os circuitos virtuais e que na estrutura do cabeçalho do pacote IP não há um espaço reservado para números de circuitos virtuais. A solução encontrada foi

adicionar um novo cabeçalho MPLS antes do cabeçalho IP. O rótulo foi então definido como um identificador curto, de tamanho fixo (32 bits) e significado local, onde cada pacote que venha a entrar na rede MPLS receberá um rótulo e os roteadores por sua vez somente se basearão nesses e não mais no endereço IP de destino para encaminhar o pacote. O rótulo pode ser descrito como na figura 3.1.

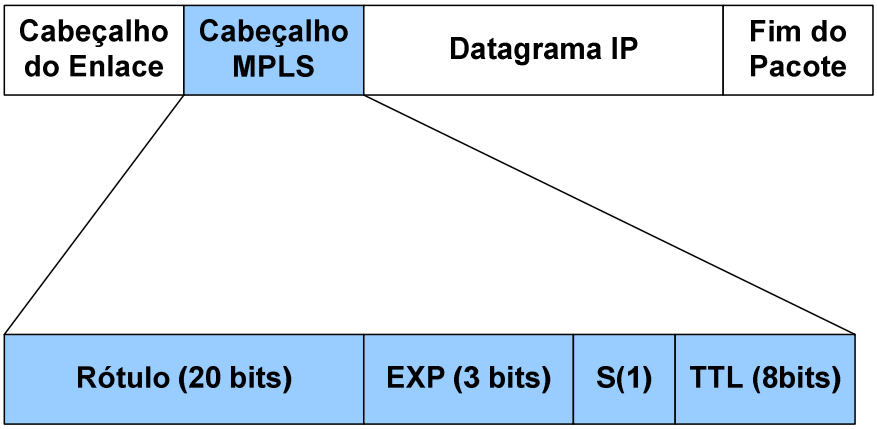


Figura 3.1 - Cabeçalho MPLS.

Descrição dos campo do cabeçalho [25]:

- Campo Rótulo (20 bits): guarda o valor atual do rótulo;
- Campo EXP (3 bits): indica a classe de serviço do pacote, ou seja, que prioridade este pacote terá na rede;
- Campo S (1 bit): o *stack* indica se há suporte ou não de enfileiramento, para os casos em que se recebe mais de um rótulo por vez;
- Campo TTL (*Time to Live*): tem o mesmo papel que no IP, contar por quantos roteadores o pacote passou, num total de 255. No caso do pacote viajar por mais de 255 roteadores, ele é descartado para evitar possíveis *loops*.

Como os cabeçalhos MPLS não fazem parte do pacote da camada de rede ou do quadro da camada de enlace de dados, considera-se o MPLS independente dessas camadas. Podemos interpretar essa propriedade como sendo possível construir comutadores MPLS que podem encaminhar tanto pacotes IP quanto células ATM, o que justifica a palavra multiprotocolo no nome MPLS.

Observando-se o tráfego de um pacote em uma rede MPLS, percebemos que um pacote ou célula, ao chegar a um roteador que suporte o protocolo MPLS, usará o rótulo como um índice para uma tabela a fim de determinar qual caminho seguir e também qual

será o novo rótulo. A troca de rótulos será realizada em todas as sub-redes de circuitos virtuais porque os rótulos tem significado apenas local, e dois roteadores diferentes podem inserir o mesmo valor de rótulo em pacotes (representado pelo quadrado amarelo) não relacionados que trafeguem em uma mesma linha como mostra a figura 3.2 [2].

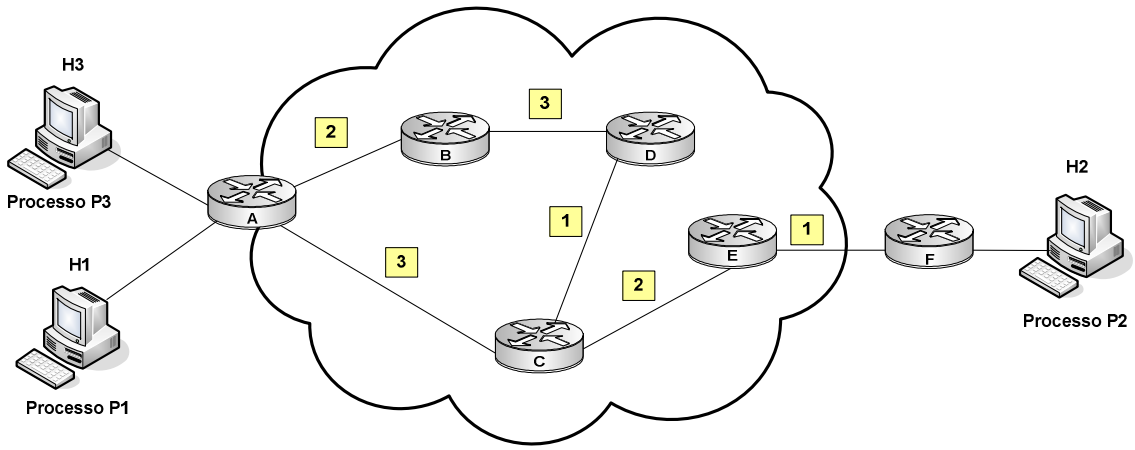


Figura 3.2 – Roteamento de rótulos em uma rede MPLS.

3.4. **Label Switch Router (LSR)**

De uma forma simples, o LSR é um roteador que suporta o protocolo MPLS, o que significa que o mesmo entende, encaminha e transmite rótulos MPLS através de enlaces de dados. Existem três tipos de LSR em uma rede [28,29]:

- LSR de entrada: são roteadores que recebem o pacote ainda sem o rótulo, realizam a inserção do mesmo no pacote e o encaminha através do link de dados.
- LSR de saída: são roteadores que recebem o pacote com o rótulo, realizam a retirada do mesmo e o encaminha através do link de dados. Os LSRs de entrada e saída podem ser considerados LSRs de borda.

- LSR intermediário: são roteadores que recebem e encaminham os pacotes com rótulo dentro de uma rede MPLS.

3.5. **Label Switched Path (LSP)**

Podemos visualizar uma LSP como sendo uma seqüência de roteadores comutadores de rótulos formando um caminho dentro de uma rede MPLS, como mostra a figura 3.3.

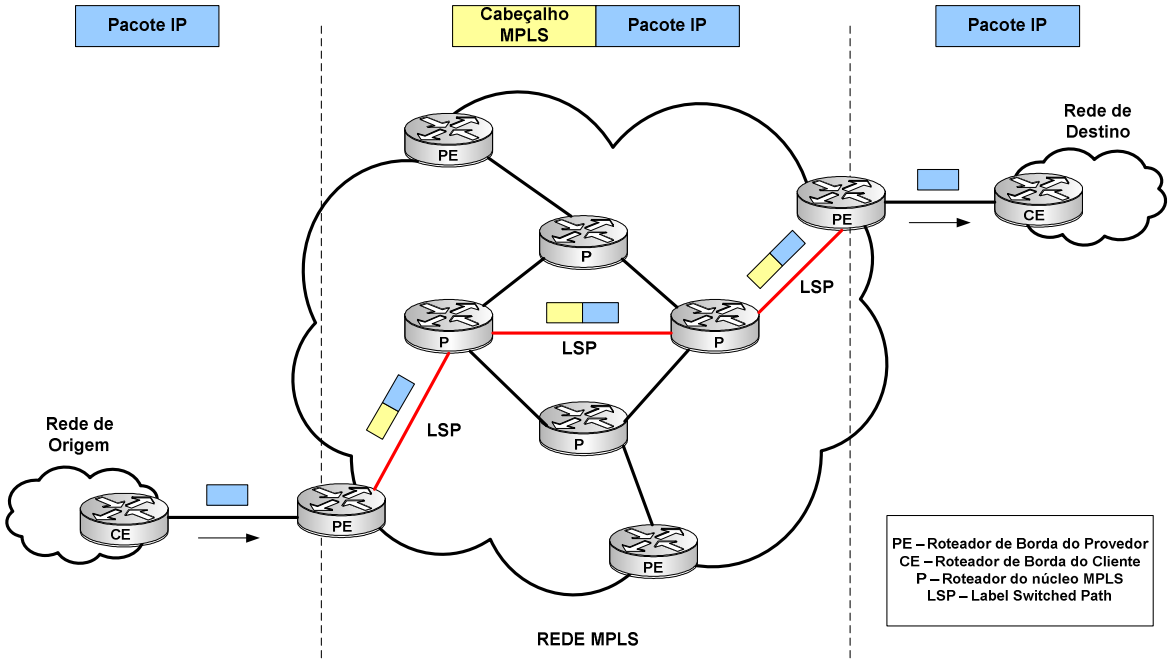


Figura 3.3 – Exemplo de uma LSP em uma rede MPLS.

É importante salientar que a LSP é unidirecional, fazendo-se necessárias duas LSPs para a comunicação entre dois elementos através das redes MPLS e que a criação do caminho a ser percorrido pelo pacote MPLS é determinado no momento da sua entrada na rede, ou seja, os LSRs do núcleo irão somente chavear os rótulos encaminhando o pacote de acordo com a LSP pré-determinada, não precisando mais fazer um roteamento dos pacotes [30, 32].

3.6. **Forwarding Equivalency Class (FEC)**

Uma Classe de Equivalência de Encaminhamento (FEC-*Forwarding Equivalency Class*) pode ser descrita como sendo uma classe de equivalência, que fará um grupo ou um fluxo de pacotes serem roteados por um mesmo caminho desde que estes se enquadrem em um mesmo conjunto de parâmetros ou características. Todos os pacotes pertencentes a uma mesma FEC terão o mesmo rótulo, entretanto pacotes com um mesmo rótulo nem sempre pertencerão a uma mesma FEC. Isto porque o campo EXP do cabeçalho MPLS pode assumir valores diferentes exigindo um tratamento diferenciado para estes pacotes, levando-os a pertencer a FECs diferentes [31].

O roteador que decide a qual FEC o pacote pertencerá será o LSR de entrada, pois é este elemento de rede que tem a responsabilidade de inserir o rótulo nos pacotes. A seguir apresenta-se através da figura 3.4 o funcionamento das FECs.

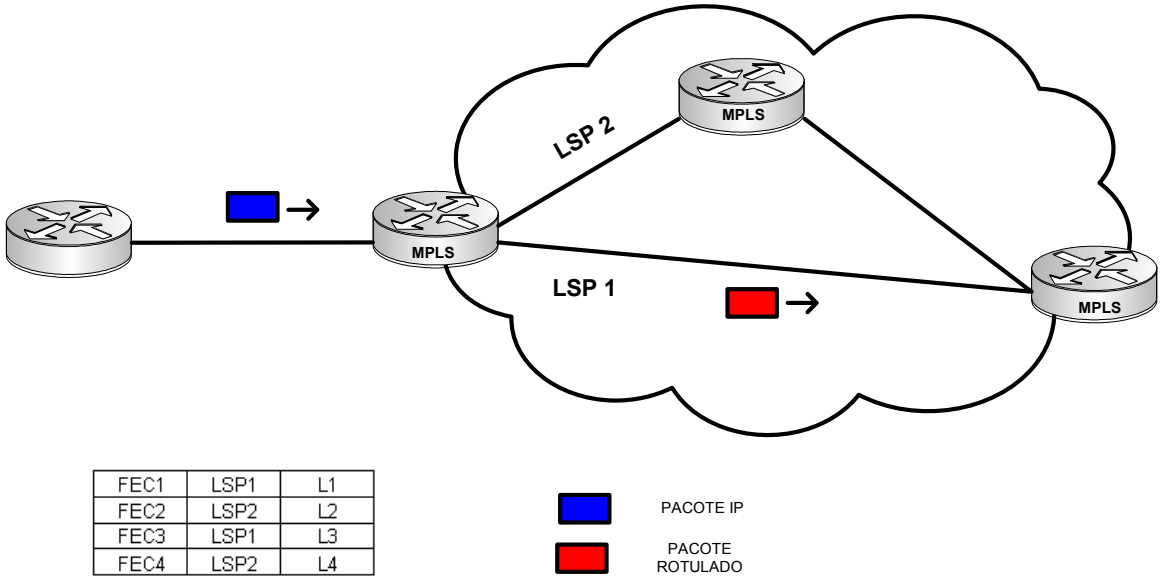


Figura 3.4 – Esquema de associação entre pacote-rótulo-FEC-LSP.

Podemos determinar uma FEC através de um ou vários parâmetros, são alguns deles [32]:

- Qualidade de Serviço (QoS);
- IP de origem e IP de Destino;
- Pacotes de *multicast* pertencentes a um mesmo grupo de *multicast*;
- Pacotes de camada 3 com os mesmos endereços IP de destino pertencentes a uma rede BGP;
- Número da porta de origem e destino.

3.7. **Distribuição de Rótulos**

Na viagem realizada pelos pacotes dentro de uma rede MPLS, a cada salto ou passagem por um roteador, a pilha de rótulos de um pacote é alterada. O rótulo do topo da pilha que foi inserido pelo LSR de entrada, é mudado a cada salto pelos LSRs intermediários, com o intuito de mostrar qual caminho o pacote deve seguir até o roteador de saída da rede MPLS.

Como exemplo é feita uma análise de um projeto de rede em que se planeja trafegar IPv4 sobre MPLS. Para isto, se faz necessário que os LSRs que compõem a rede, além de permitirem o tráfego de rótulos, também suportem os protocolos de roteamento interior ou IGP (Interior Gateway Protocol) tais como: *Open Shortest Path First* (OSPF) e *Enhanced Interior Gateway Routing Protocol* (EIGRP).

Para ilustrar a dinâmica da inserção e troca de rótulos, será feita uma breve análise do que ocorre com um pacotes IP ao entrar e sair de um rede MPLS. A princípio teremos os pacotes IP chegando à rede MPLS através do LSR de entrada, o mesmo analisará qual o endereço IP de destino do pacote e acrescentará um rótulo ao mesmo. Posteriormente, o LSR de entrada encaminhará o pacote ao próximo roteador da rede MPLS. O próximo LSR, ou LSR intermediário, receberá o pacote e trocará o rótulo de entrada por um outro rótulo de saída, repetindo o processo até que o pacote chegue ao último roteador da rede MPLS ou LSR de saída. Neste último roteador, o rótulo será retirado do pacote e este será encaminhado como um pacote IP convencional ao seu destino.

Para que isto funcione corretamente é necessário que o protocolo utilizado para o roteamento dos pacotes tanto suporte realizar a distribuição de rótulos quanto às

informações de roteamento IP simultaneamente. Para a distribuição dos rótulos na rede MPLS é utilizado o Protocolo de Distribuição de Rótulos ou LDP.

3.8. **Label Distribution Protocol - LDP**

O Protocolo de Distribuição de Rótulos (LDP-*Label Distribution Protocol*) é descrito pela RFC 2283 [33]. A criação do LDP trouxe vantagens ao projeto de uma rede MPLS. Uma delas é que o protocolo foi pensado e projetado com a finalidade de realizar a distribuição de rótulos em redes MPLS, sendo assim eficiente, escalável e confiável, diferentemente do caso da adoção de uma adaptação de outros protocolos semelhantes para a realização desta tarefa. Um outro benefício do LDP é que o mesmo é um protocolo aberto, e isto favoreceu a sua popularização. Hoje, o LDP se faz presente em todos os equipamentos de rede MPLS disponíveis no mercado.

O LDP realiza três funções principais [34]:

- Descoberta de LSRs vizinhos que rodem o LDP;
- Manutenção e estabelecimento de sessões com outros roteadores;
- Atualização da tabela de rótulo.

Quanto à primeira funcionalidade, pode-se dizer que quando dois ou mais LSRs utilizam o LDP e estão conectados por enlace de dados entre eles, a descoberta dos elementos vizinhos da rede são feitas através de pacotes "*Hello*" que são enviados periodicamente. Os pacotes "*Hello*", são datagramas de pequeno tamanho que são trocados entre elementos de rede para o reconhecimento de vizinhos.

A segunda funcionalidade está relacionada com o estabelecimento de sessões através de conexões TCP. Através destas conexões é que o LDP consegue atualizar o mapeamento de rótulos entre dois pares de roteadores que rodam o LDP.

As mensagens de atualização para as tabelas de rótulos são também de grande importância, pois estas podem mudar, retratar ou anunciar a mesma, melhorando o roteamento de rótulo e assim otimizando a rede MPLS.

Quanto ao funcionamento do LDP, cada roteador MPLS cria uma tabela relacionando um valor de rótulo a um caminho dentro da rede, esta tabela é chamada de

Base de Informações de Rótulo (LBI – *Label Base Information*). Assim, quando o pacote entra no LSR, este verifica para qual interface esse pacote deve ser encaminhado através da tabela LIB. Posteriormente realiza-se a troca do rótulo de entrada por um rótulo de saída, para que o pacote possa alcançar o próximo nó assim como mostra a figura 3.5.

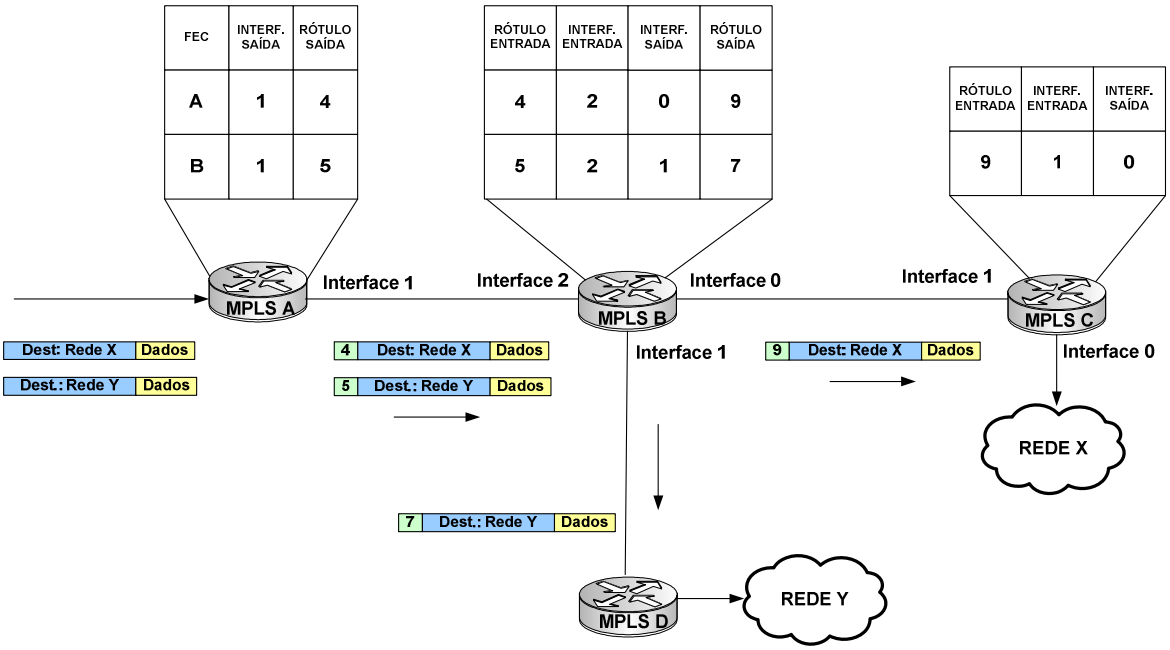


Figura 3.5 – Funcionamento do LDP.

Quando o pacote entra no LSR, este verifica para qual interface esse pacote deve ser encaminhado, através da LIB. Sendo assim, realiza a troca do rótulo de entrada por um rótulo de saída, para que o pacote possa alcançar o próximo nó [32, 34].

3.9. **Rede Privada Virtual sobre MPLS**

Uma VPN é definida como um conjunto de políticas que controlam a conectividade e qualidade de serviço de uma rede privada. construída em cima de uma rede de comunicações pública como por exemplo: a *Internet*. O tráfego de dados é levado pela rede pública utilizando protocolos padrão, não necessariamente seguros. A VPN provê comunicação entre as camadas 2 e 3 do modelo OSI e geralmente conecta vários ponto da rede de uma mesma instituição ou empresa [36]. As VPNs podem ser implementadas de três maneiras distintas: *Intranet* VPN, *Extranet* VPN e VPN de Acesso Remoto. A seguir são descritas as principais características de cada uma delas [37, 38].

Intranet VPN

Uma *Intranet* VPN é uma VPN que conecta máquinas de uma rede de computadores de uma mesma rede local ou LAN (*Local Área* Network) ou também conecta filiais, matriz e outras unidades de uma mesma unidade organizacional. Um exemplo de *Intranet* VPN é a comunicação entre departamentos de uma mesma empresa, onde um dos quesitos básicos a considerar é a necessidade de uma criptografia rápida, para não sobrecarregar a rede.

No exemplo apresentado na figura 3.6, seis diferentes pontos são incorporados pela rede do *backbone* do provedor de serviço. Os pontos A, B e C pertencem a uma mesma empresa e os pontos X,Y e Z pertencem a uma outra empresa. Os pontos A, B e C podem compartilhar conectividade IP entre si porque eles fazem parte do mesmo subconjunto de políticas, ou seja, eles estão na mesma VPN (VPN ABC). Os pontos X,Y e Z são partes de uma outra VPN, pois compartilham um conjunto de políticas diferente daquele associado à VPN ABC.

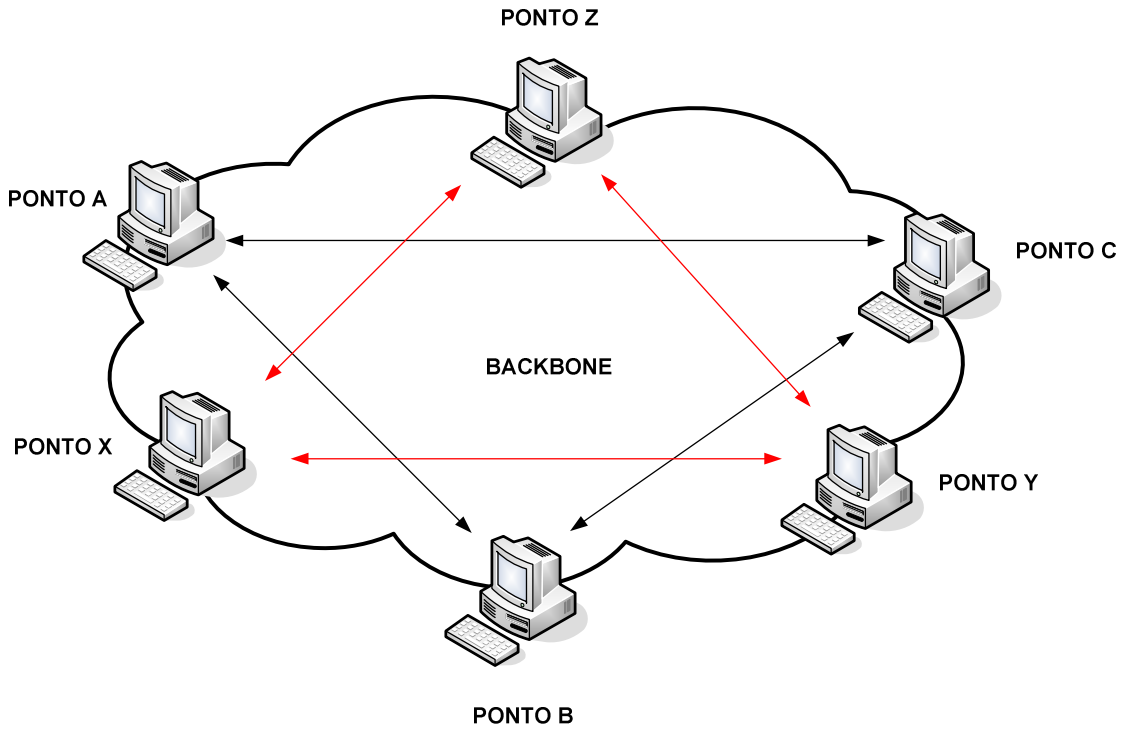


Figura 3.6 – Modo de Interconexão *Intranet* VPN

A primeira VPN que conecta os pontos A, B e C e a segunda VPN que conecta os pontos X, Y e Z ilustram o modo de Interconexão de uma *Intranet* VPN.

Extranet VPN

Extranet VPN é implementada para conectar uma empresa à seus sócios, fornecedores e clientes. Para isso é necessário uma solução aberta, para garantir a interoperabilidade com as várias soluções que as empresas envolvidas possam ter em suas redes privadas. Outro ponto muito importante a se considerar é o controle de tráfego, o que minimiza o efeitos dos gargalos existentes em possíveis nós entre as redes, e também garantir uma resposta rápida e suave para aplicações críticas.

Esta é uma solução voltada para a colaboração, compartilhamento de aplicações e comércio eletrônico entre empresas. A figura 3.7 ilustra o funcionamento de uma *Extranet* VPN.

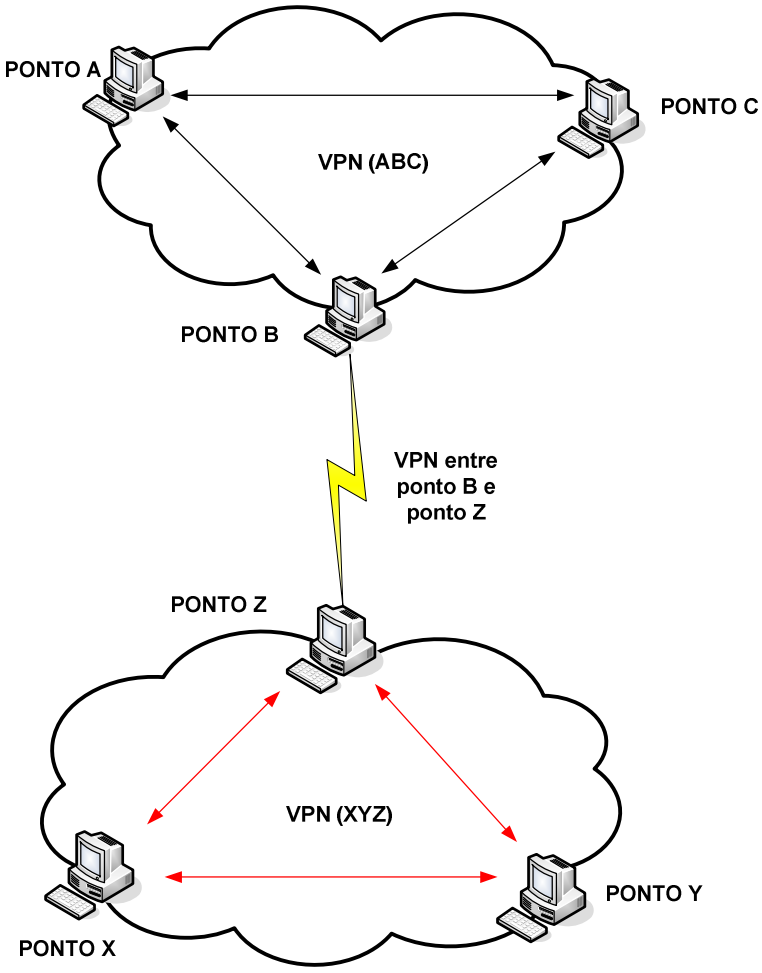


Figura 3.7 – Modo de Interconexão *Extranet* VPN

VPN de Acesso Remoto

Uma VPN de acesso remoto conecta usuários que estejam distantes fisicamente de uma rede de computadores que precisa ser acessada. Neste caso, torna-se necessário um software cliente de acesso remoto. Uma autenticação rápida e eficiente, que garanta a identidade do usuário remoto é de fundamental importância para o correto funcionamento de uma VPN de Acesso Remoto. Outro fator importante é a necessidade de um gerenciamento centralizado desta rede, já que ao mesmo tempo, pode-se ter muitos usuários remotos acessando a rede através da VPN, o que torna necessário que todas as informações sobre os usuários, para efeitos de autenticação por exemplo, estejam centralizadas num único lugar.

As duas topologias, *Intranet* VPN e *Extranet* VPN, apresentadas anteriormente são possíveis de ser implementadas com a tecnologia VPN MPLS - RFC 2574bis [39]. Uma VPN MPLS consiste de duas redes: a rede do provedor e a rede do cliente. A rede do provedor é constituída de roteadores de borda (PE) que provêem serviços de VPN e conectividade para as redes dos clientes. As redes dos clientes são normalmente constituídas, fisicamente, por diferentes pontos de acessos. Os roteadores dos clientes que se conectam aos provedores dos serviços das VPNs são chamados de *Router Customer Edge* (CE). Existem basicamente dois modelos de VPN existentes: o modelo *Overlay* e o modelo *Peer*. Nas seções a seguir serão explanadas as suas principais características e seus modos de funcionamento.

3.9.1. **Modelo Overlay**

As técnicas mais comuns para prover serviços VPN são baseadas no modelo *Overlay* [36, 40]. Neste modelo, cada ponto de acesso do ambiente do usuário tem um roteador que é conectado, através de enlaces ponto a ponto, a outro roteador remoto do usuário. O ambiente do usuário pode ter um ou mais roteadores que podem ser conectados a todos os outros pontos ou a um subconjunto destes.

As tecnologias utilizadas para oferecer enlaces ponto a ponto são: linhas dedicadas ponto a ponto, *Frame Relay* e ATM. A rede formada por estes enlaces juntamente com os roteadores formam um "*Backbone* Virtual". É nesse *backbone* virtual que os provedores de serviços formam as VPNs para interligar os pontos das redes dos usuários.

O roteador concentrador da rede privada virtual é responsável pelo mapeamento e visibilidade da rede como um todo. Este modelo tem na sua essência um problema de escalabilidade ou crescimento da rede. Com um número grande de pontos interligados através de uma VPN *Overlay*, a gerência e administração da rede torna-se muito trabalhosa.

A quantidade de configuração necessária para inclusão de um novo ponto em uma VPN existente cresce juntamente com a rede. Para uma VPN que requer conectividade completa entre todos os pontos, cada novo ponto acrescido na rede necessita de uma conexão e roteamento ponto a ponto com todos os outros pontos da VPN.

A seguir, na figura 3.8 é ilustrada de forma simplificada a estrutura de uma VPN *Overlay*.

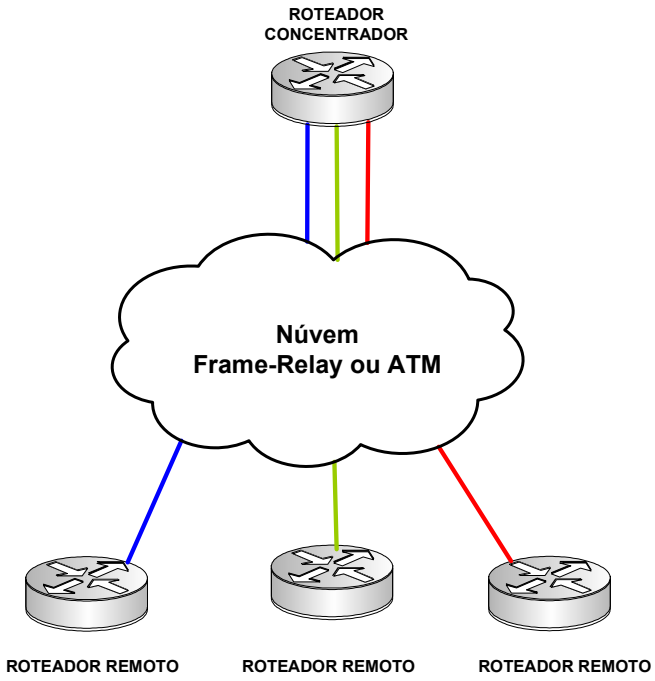


Figura 3.8 – Modelo de uma VPN *Overlay*.

Uma variação do modelo *overlay* é o modelo em que o provedor de serviço utiliza roteadores que são capazes de atuar como Roteadores Virtuais (VR). Nesse caso, um simples roteador atua como uma coleção de roteadores virtuais. Um “VR” é funcionalmente equivalente a um roteador convencional, exceto pelo fato de que compartilha a CPU, largura de banda e recursos de memória com outros roteadores virtuais.

Um Roteador Virtual é conectado a outro, via enlaces ponto a ponto. Para reduzir o número de enlaces ponto a ponto requerido, é possível fazer a multiplexação de várias

conexões em um único enlace por meio de *Frame Relay* ou ATM, através da introdução de alguma forma de multiplexação do cabeçalho do pacote. Cada ambiente do usuário possui um roteador conectado em um roteador virtual. Nesse caso, o *backbone* virtual é composto de tais roteadores virtuais e os enlaces que os interligam.

Uma das vantagens do uso do Roteador Virtual é que ele reduz a quantidade de equipamentos físicos que um provedor necessita disponibilizar. O uso do roteador virtual não altera o modelo; ele permite simplesmente que um único roteador seja fisicamente compartilhado por vários roteadores virtuais.

3.9.2. **Modelo Peer**

A principal contribuição do modelo *Peer* é proporcionar escalabilidade a rede de uma forma bem mais simples e eficiente quando comparada com o modelo *Overlay*. O roteamento das redes que integram uma mesma VPN também é bastante simples, pois o roteador do cliente troca informações de roteamento com poucos roteadores de borda do provedor.

Outra característica interessante deste modelo é a simplicidade na adição de um novo ponto à rede. Para isto, é necessário somente adicionar um enlace com um roteador cliente e configurar o protocolo de roteamento entre o roteador cliente e o roteador do provedor. No modelo *Overlay* de VPN, o provedor de serviço deverá aprovisionar um conjunto inteiro de circuito virtuais desde a origem até o destino.

A implementação de VPN baseada no modelo *Peer* em uma rede MPLS tem duas possibilidades de implementação:

Método com roteador compartilhado: Nesse método, os usuários compartilham o mesmo roteador PE (*Provider Edge*) ou roteador de borda do provedor;

Método com roteador dedicado: Nesse método, cada usuário tem um roteador PE dedicado. O modelo com roteador dedicado usa protocolos de roteamento para criar tabelas de roteamento para cada VPN nos roteadores do provedor do serviço. Estas tabelas contêm somente as rotas anunciadas pela VPN conectada, resultando em uma perfeita isolação entre as mesmas.

3.10. **VPN BGP-MPLS (RFC 2547bis)**

A RFC-2547bis [39] define o padrão que os provedores de serviço devem utilizar em seu *backbone* para prover serviço de VPN para seus clientes. A RFC-2547bis é também conhecida como VPN BGP-MPLS porque o BGP é o protocolo utilizado para a distribuição das tabelas de roteamento das VPNs e pela utilização do MPLS no estabelecimento dos circuitos virtuais e encaminhamento do tráfego.

Os principais objetivos da RFC 2547bis são: oferecer serviços de simples implementação proporcionando escalabilidade e flexibilidade, além de segurança e privacidade quanto as informações que trafegarão na rede.

3.10.1. **Elementos de uma VPN BGP-MPLS**

Na arquitetura tradicional de roteamento IP há uma clara distinção entre rotas externas e internas. Na visão de um provedor de serviço, rotas internas incluem todos os enlaces internos do provedor. Essas rotas internas são trocadas com outras rotas na rede, por meio de protocolos IGP (*Interior Gateway Protocol*) tais como: OSPF (*Open Shortest Path First*) ou IS-IS (*Intermediate System-to-Intermediate System*). Todas as rotas aprendidas na *Internet* por meio de pontos de troca de tráfego (*peering*) ou de pontos de clientes são classificadas como rotas externas e são distribuídas por meio do protocolo EGP (*Exterior Gateway Protocol*), tal como o BGP (*Border Gateway Protocol*).

Uma rede cliente é conectada pelo provedor do serviço por uma ou mais portas, sendo que o provedor de serviço associa cada porta com uma tabela de roteamento da VPN. Na RFC 2574bis, a tabela de roteamento VPN é chamada VPN *Routing and Forwarding* (VRF). Os elementos que compõem a estrutura provedor/cliente em uma VPN BGP-MPLS são ilustrados na figura 3.9:

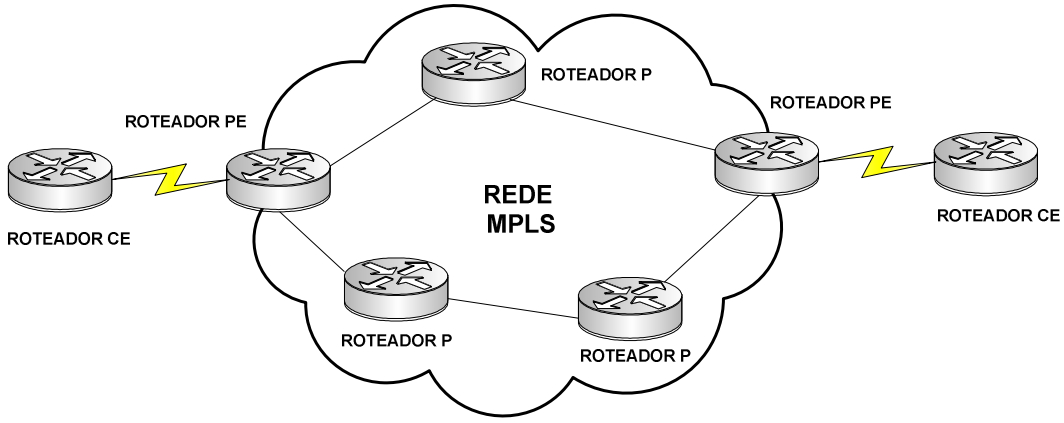


Figura 3.9 – Elementos de uma VPN BGP-MPLS

Customer Edge (CE): Provê acesso do cliente até o provedor de serviço de rede. Tipicamente, o equipamento CE é um roteador que estabelece uma conexão diretamente com o roteador do provedor do serviço (PE). Depois de estabelecida a conexão, o roteador CE anuncia as rotas dos pontos da VPN local para o roteador PE e obtém as rotas das outras redes que compõem a VPN.

Provider Edge Routers (PE): É o equipamento de borda do provedor. Os roteadores PE trocam informação de roteamento com os roteadores CE através de roteamento estático ou dinâmico. Esse modelo de VPN realça a escalabilidade da RFC 2574bis porque elimina a necessidade dos roteadores PE manterem rotas VPN com todos os roteadores PE do Provedor de Serviço. Cada roteador PE mantém uma VRF para cada ponto conectado diretamente. Observa-se que múltiplas interfaces do roteador PE podem ser associadas com uma única VRF se todos os pontos de acesso participam da mesma VPN. Após aprender as rotas das VPNs locais dos roteadores CE, um roteador PE troca informação de roteamento com os outros roteadores PE através do BGP. Quando foi concebido o BGP para as VPN MPLS, foi definido que todos os roteadores PE de uma rede que utilizam BGP necessitam de uma comunicação direta entre si. Para melhorar a escalabilidade e simplificar a configuração, foi criado o *Route Reflector*, onde todos os roteadores estabelecem uma sessão BGP somente com estes elementos da rede desta forma não é necessário que todos os roteadores tenham conexão direta entre si, como ilustram as figuras 3.10 e 3.11.

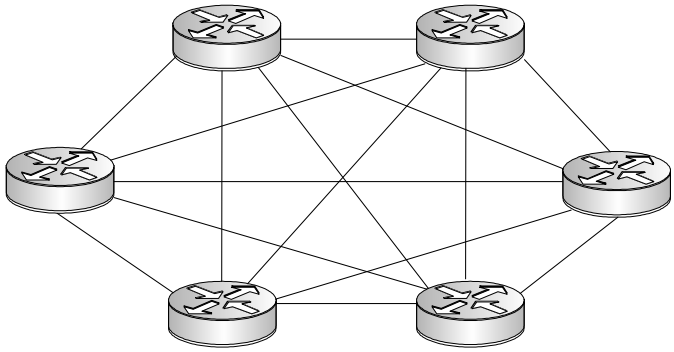


Figura 3.10 – Conexão entre roteadores dois a dois.

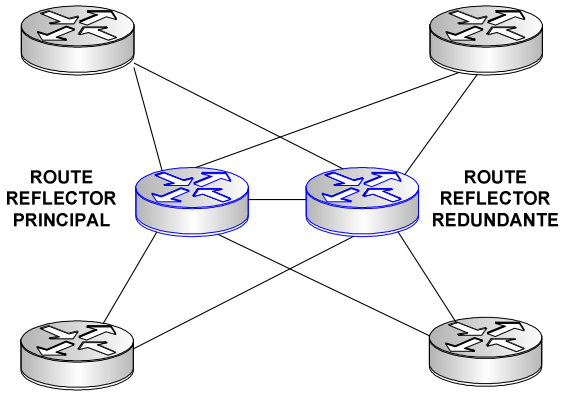


Figura 3.11 – Conexão entre roteadores usando Route Reflector.

Provider Routers (P): Um *Router Provider* é um roteador na rede do provedor que não troca informação diretamente com o equipamento CE. A função dos roteadores do provedor P é encaminhar tráfego de dados para os roteadores PE, desde que o tráfego seja encaminhado por meio do *backbone* MPLS. Os roteadores P são utilizados para manter rotas para os roteadores PE, eles não são necessários para manter informação de roteamento específico para cada acesso do cliente.

Tabela de Roteamento e Encaminhamento (VRF): Um conceito chave na arquitetura VPN BGP/MPLS é o elemento chamado de tabela de Encaminhamento e Roteamento dos roteadores PE. A VRF é uma tabela de encaminhamento e roteamento para cada VPN dentro dos roteadores PE. Uma VRF privada é acessível unicamente pelas interfaces que fazem parte da VPN correspondente. Todos os pontos conectados no roteador PE devem fazer parte de uma VRF. Todas as informações das VPNs são refletidas na VRF e os pacotes que viajam através daquele ponto serão roteados e encaminhados com base unicamente na informação encontrada na VRF correspondente.

3.11. **Considerações sobre VPN BGP/MPLS**

O maior objetivo das VPNs BGP/MPLS é simplificar a operação da rede para os usuários, enquanto permite ao provedor de serviço oferecer escalabilidade e serviços de valor adicionado. As VPNs BGP/MPLS têm muitos benefícios, alguns deles são:

• Não há restrição do plano de endereços utilizados em cada VPN do usuário. O usuário pode usar outros endereços, globais ou privados. Na perspectiva do provedor do serviço, clientes diferentes podem ter endereços sobrepostos (*Overlapping*).

• Os roteadores CE de cada ponto de presença do usuário não trocam informação de roteamento diretamente com outros roteadores CE. Os usuários não têm de se preocupar com questões de roteamento entre redes porque estas são de responsabilidade do provedor de serviço.

• Usuários não precisam administrar o *backbone* virtual e nem gerenciar acessos para os roteadores PE ou P.

• Provedor de Serviço não tem um *backbone* separado ou virtual para administrar cada VPN do usuário.

• Segurança equivalente ao *Frame Relay* e ATM.

• Provedor de Serviço pode utilizar uma infra-estrutura comum para entregar serviços de conectividade *Internet* e VPN.

• Flexibilidade e Escalabilidade para serviços de QoS são suportadas por meio do uso do EXP no cabeçalho MPLS ou pelo uso de engenharia de tráfego.

3.12. **Serviço Integrado e Diferenciado**

O serviço integrado (*Intserv*) [41] foi desenvolvido pela IETF (*Internet* Engineering *Task Force*) para fornecer garantias de qualidade de serviço específicas às sessões de aplicações individuais. Já o serviço diferenciado (*Diffserv*) [42] tem como objetivo prover a capacidade de manipular diferentes classes de tráfego de modos diferentes. O *Inteserv* e o *Diffserv* representam a solução do IETF para prover qualidade de serviço.

3.12.1. **Regulação**

No estudo da qualidade de serviço, a regulação é o ajuste da taxa com a qual é permitido que um fluxo injete pacotes na rede. Este elemento é fundamental para qualquer arquitetura que utilize QoS. A seguir são enumerados três critérios importantes de regulação diferentes entre si pela escala de tempo que o pacote é regulado:

Taxa Média: É comum se desejar limitar a taxa média durante um período de tempo com o qual os pacotes de um fluxo podem ser enviados. Porém é importante observar o intervalo de tempo durante o qual a taxa média será regulada. Por exemplo: um fluxo cuja taxa média está limitada a 100 pacotes por segundo é mais restringida do que um outro fluxo limitado por 6000 pacotes por minuto, mesmo que ambos tenham a mesma taxa média durante um intervalo de tempo suficientemente longo, pois a limitação de 6000 pacotes por minuto permitiria que um fluxo enviasse 1000 pacotes em um dado intervalo de tempo de um segundo de duração enquanto a limitação de 100 pacotes por segundo não permitiria este comportamento de envio em momento algum.

Taxa de Pico: Enquanto a limitação da taxa média restringe a quantidade de tráfego que pode ser enviada para uma rede durante um período de tempo relativamente longo, uma limitação de taxa de pico restringe o número máximo de pacotes que podem ser enviados durante um período de tempo mais curto. Usando o mesmo exemplo do parágrafo anterior, a rede pode regular um fluxo a uma taxa média de 6000 pacotes por minuto e ao mesmo tempo limitar a taxa de pico em 1500 pacotes por segundo.

Tamanho da Rajada: A rede também pode limitar o número máximo de pacotes, ou rajada de pacotes, que podem ser enviados durante um intervalo de tempo extremamente curto. À medida que o comprimento do intervalo se aproxima de zero o tamanho da rajada limita o número de pacotes que podem ser enviados instantaneamente.

O mecanismo *leaky bucket* é uma abstração que pode ser usada para caracterizar esses limites da regulação. Como ilustrado na figura 3.12 um *leaky bucket* é um balde que pode conter até *b* permissões. Novas permissões que potencialmente podem ser adicionadas ao balde, estão sempre sendo geradas a uma taxa de *r* permissões por segundo. Se o balde estiver com um número de permissões menor que o seu limite *b* a permissão recém gerada será adicionada ao balde, caso contrário ela será ignorada.

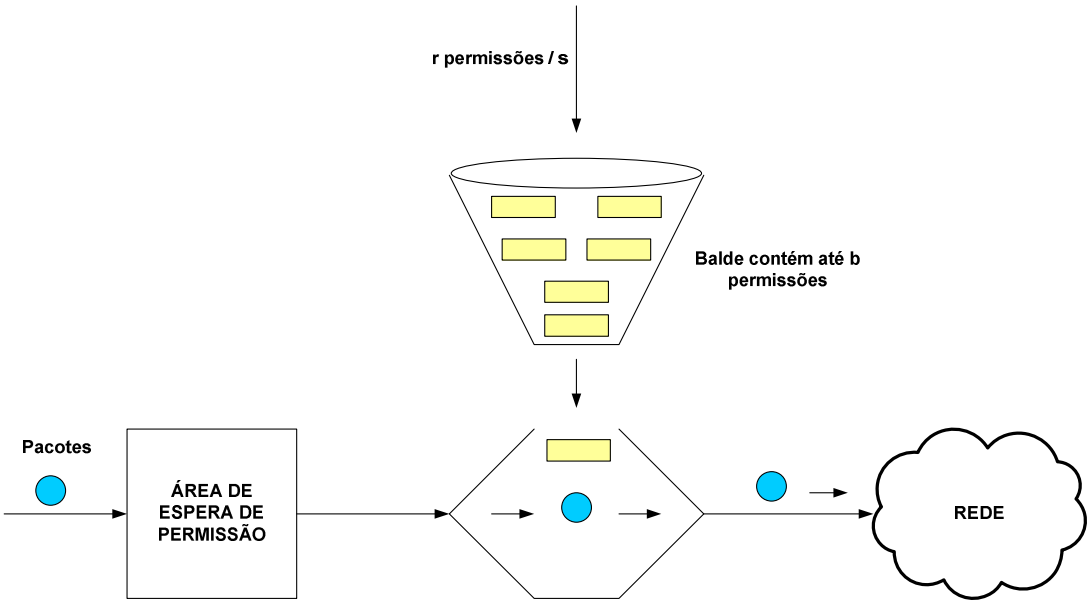


Figura 3.12 – Funcionamento do *leaky bucket.*

O uso do *leaky bucket* pode ser aplicado para regular fluxo de pacotes. Supondo que um pacote antes de ser transmitido tenha que retirar uma permissão de dentro do balde, se o balde estiver vazio o pacote terá que esperar por uma permissão. Como pode haver no máximo *b* permissões no balde, o tamanho máximo da rajada para um fluxo regulado pela técnica do *leaky bucket* é de *b* pacotes. E se a taxa de geração de permissões é *r*, o número máximo de pacotes que pode entrar na rede para qualquer intervalo de tempo *t* é *rt* + *b*. Assim a taxa de geração de permissões *r* serve para limitar a taxa média de longo período com a qual os pacotes podem entrar na rede. Também é possível usar o *leaky bucket* para regular a taxa de pico de um fluxo e a taxa média por um período de tempo.

3.12.2. **Intserv**

A arquitetura Intserv tem duas características fundamentais:

Recursos Reservados: Um roteador tem que saber a quantidade de seus recursos (*buffers*, largura de banda) que já está reservada para sessões em andamento.

Estabelecimento de chamadas: Em uma sessão onde se deseja implementar QoS, faz-se necessário habilitar a reserva de recursos em cada roteador desde a origem até o destino. Esse processo do estabelecimento da chamada exige a participação de todos os roteadores integrantes da sessão. Cada roteador deve determinar os recursos locais exigidos

pela sessão, considerar a quantidade de recursos que já estão comprometidos com outras sessões em andamento e determinar se tem recursos suficientes para suprir as exigências de QoS dada uma sessão que já foi aceita. As etapas do estabelecimento de chamadas seguem as etapas descritas a seguir:

1. Caracterização do tráfego e especificação da QoS desejada: Para que um roteador determine se os seus recursos são suficientes ou não para atender as exigências da QoS de uma sessão. Na arquitetura *Intserv,* a *Rspec* define a QoS específica que está sendo requisitada por uma conexão, a *Tspec* caracteriza o tráfego que a origem estará enviando a rede. A *Rspec* é definida na RFC 2215 [43] e a *Tspec* é definida na RFC 2210 [44].
2. Sinalização para o estabelecimento da chamada: ATspec e a Rspec deverão ser transportadas para os roteadores nos quais serão reservados recursos para uma determinada sessão. O protocolo RSVP definido pela RFC 2210 [44] é o protocolo responsável pelo transporte da sinalização.
3. Aceitação de chamada por elemento: Tendo o roteador recebido a *Tspec* e a *Rspec*, o mesmo determinará se pode ou não receber a chamada. Essa decisão de aceitação da chamada dependerá da especificação do tráfego, do tipo de serviço exigido e do comprometimento dos recursos existentes para sessões em andamento.

A arquitetura *Intserv* define duas classes de serviço: serviço garantido e serviço de carga controlada. Esta duas classes são descritas a seguir:

Serviço Garantido: Esta classe de serviço é descrita na RFC 2212 [45] estabelece limites rígidos, que podem ser provados matematicamente, para os atrasos de fila que um pacote sofrerá em um roteador. A caracterização do tráfego de uma fonte é dada por um *leaky bucket* com os parâmetros (*r,b*) e o serviço requisitado é caracterizado por uma taxa de transmissão *R*. O que é buscado pela sessão requisitante do serviço é que seja garantida uma taxa de transmissão *R* aos seus pacotes.

Serviço de rede de carga controlada: Uma sessão que está recebendo serviço de carga controlada receberá uma qualidade de serviço que se aproxima muito da QoS que o mesmo fluxo receberia de um elemento da rede que não tivesse carga [46]. Com isto se quer dizer que uma grande quantidade de pacotes passará com sucesso pelo roteador sem ser descartado e sofrerá atraso próximo de zero na fila do roteador. Vale observar que o

serviço de carga controlada não dá garantias quantitativas de desempenho. O foco deste serviço são as aplicações multimídia desenvolvidas para a *Internet*, onde as aplicações funcionam muito bem quando não há carga na rede, porém o seu desempenho cai à medida que a rede fica carregada de tráfego.

3.12.3. **Diffserv**

A capacidade de requisitar e reservar recursos por fluxo faz com que seja possível que a estrutura *Intserv* forneça qualidade de serviço a fluxos individuais. No entanto, existem dificuldades associadas ao *Intserv* quanto a reserva de recursos por fluxo.

Escalabilidade: A reserva de recursos por fluxo implica a necessidade de um roteador para processar reservas de recursos o que pode representar uma sobrecarga significativa em redes de grande porte.

Modelos de serviço flexíveis: A estrutura *Intserv* atende a um pequeno número de classes de serviços pré-especificados. O conjunto específico de classes de serviço não comporta definições mais qualitativas ou relativas para as diferenças entre as classes.

A arquitetura *Diffserv* visa promover diferenciação de serviço escalável e flexível, ou seja, a capacidade de manipular diferentes classes de tráfego de maneiras diferentes dentro da rede. Esta arquitetura é flexível no sentido de que não define serviços específicos nem classes de serviço específicas ao contrário do *Inteserv*.

Na arquitetura *Diffserv* existem dois conjuntos de elementos funcionais:

Função de Borda: Na borda de entrada da rede os pacotes que chegam são marcados, mais especificamente o campo DS (*Differentiated Service*) do cabeçalho do pacote é configurado para um valor. A marca que um pacote recebe identifica a classe de tráfego à qual ele pertence. Assim, diferentes classes de tráfego receberão serviços diferenciados dentro do núcleo da rede.

Função Central: Quando um pacote marcado com DS chega a um roteador habilitado para *Diffserv*, ele é repassado até seu próximo salto de acordo com o comportamento por salto associado à classe do pacote. O comportamento por salto influencia a maneira pela qual os *buffers* e a largura de banda de um roteador são compartilhados entre as classes de tráfego concorrentes.

Outro elemento fundamental na arquitetura *Diffserv* é o comportamento por salto ou PHB (*Per Hop Behavior*) realizado pelos roteadores. O PHB é definido na RFC 2475 [47] como uma descrição do comportamento de envio de um nó *Diffserv* que possa ser observado externamente aplicado a um comportamento agregado *Diffserv* em particular.

Um PHB pode resultar no recebimento de diferentes desempenhos por diferentes classes de tráfego, isto é, comportamentos de envio diferentes que possam ser observados externamente. E embora um PHB defina diferenças de desempenho entre classes, ele não determina nenhum mecanismo específico para conseguir esses comportamentos. Desde que os critérios de desempenho observados externamente sejam cumpridos, quaisquer mecanismos de implementação e quaisquer políticas de alocação de *buffer* e largura de banda podem ser usados.

Existem definições para dois tipos de PHB: o PHB de repasse acelerado (EF – *Expedited Forwarding*) [48] e o PHB de repasse assegurado (AF – *Assured Forwarding*) [49].

O PHB de repasse acelerado especifica que a taxa de partida de uma classe de tráfego de um roteador deve ser igual ou maior do que um taxa configurada. Ou seja, durante qualquer intervalo de tempo fica garantido que a classe de tráfego receba largura de banda suficiente de modo que a taxa de saída do tráfego seja igual ou maior do que essa taxa mínima configurada.

O PHB de envio assegurado é mais complexo. O AF divide o tráfego em quatro classes e garante a cada classe AF o fornecimento de alguma quantidade mínima de largura de banda e de *buffer*. Dentro de cada classe os pacotes ainda são divididos em uma das três categorias de descarte preferencial. Quando ocorre um congestionamento dentro de uma classe AF, um roteador pode então descartar pacotes com base em seus valores de descarte preferencial.

3.13. **RSVP**

Para que uma rede forneça garantias de QoS é preciso que haja um protocolo de sinalização para que as aplicações reservem recursos. O *Reservation Protocol* (RSVP) [53] é o protocolo de sinalização mais utilizado em redes de computadores para a garantia de QoS. O protocolo RSVP permite que aplicações reservem largura de banda para fluxos de dados. Este protocolo é também utilizado pelos roteadores para repassar requisições de

reserva de largura de banda. Para implementar o RSVP, um *software* RSVP de estar presente nos receptores, remetentes e roteadores. As duas principais características do RSVP são:

1. O protocolo fornece reservas de largura de banda em árvores *multicast*.
2. O protocolo RSVP é orientado para o receptor, pois é o receptor do fluxo de dados que inicia e mantém a reserva de recursos.

Estas duas características são exibidas na figura 3.13, onde o diagrama mostra uma árvore *multicast* com dados fluindo do topo da árvore para as estações da base. Embora os dados se originem do remetente as mensagens de reserva se originam nos receptores. Quando um roteador transmite uma mensagem de reserva na direção do remetente, ele pode consolidar a mensagem de reserva com outras mensagens de reserva que estão chegando da corrente inferior.

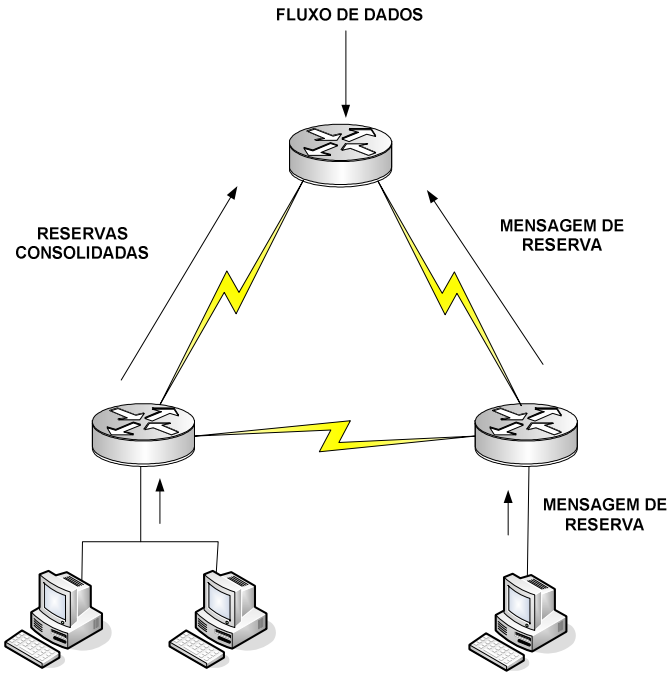


Figura 3.13 – Funcionamento do RSVP.

O padrão RFC 2205 [42] não especifica como a rede fornece largura de banda reservada aos fluxos de dados. Este é meramente um protocolo que permite que as aplicações reservem a largura de banda necessária de um enlace. Uma vez realizadas as reservas o fornecimento da largura de banda reservada aos fluxos de dados passa a ser tarefa dos roteadores através de mecanismos de escalonamento tais como: escalonamento

prioritário e enfileiramento justo ponderado. O RSVP não é um protocolo de roteamento e ele não determina os enlaces nos quais as reservas devem ser feitas. Em vez disso, ele depende de um protocolo de roteamento subjacente para determinar as rotas dos fluxos. Assim que as reservas estejam em vigor, os escalonadores de pacotes do roteador devem realmente fornecer aos fluxos de dados a largura de banda reservada. Em síntese o RSVP é um protocolo que as estações de uma rede utilizam para estabelecer e encerrar reservas de fluxos de dados.

O RSVP também traz uma solução para o caso de receptores heterogêneos em uma rede. Considere uma rede na qual alguns receptores podem receber um fluxo à taxa de 29 kbps, outros a uma taxa de 128 kbps e por fim receptores que possam receber um fluxo de dados à taxa de 10 Mbps. Se um remetente estiver enviando um vídeo para um grupo de receptores heterogêneos, a qual taxa ele o fará? Se o vídeo for codificado para a taxa de 10 Mbps somente os usuários com essa taxa de acesso poderão assistí-lo. Por outro lado, se o vídeo for codificado a 29 kbps os usuários que tem acesso à taxa de 128 kbps e 10 Mbps serão obrigados a ver a imagem a uma resolução abaixo da qualidade possível.

Para se resolver esse problema a sugestão é codificar áudio e vídeo em duas camadas: uma camada base e uma camada de realce. A camada base poderia ter um taxa de 20 kbps e a camada de realce ter uma taxa de 100 kbps. Assim receptores com acessos de 29 kbps poderiam receber a imagem com menor qualidade da camada de base e os receptores com acesso de 128 kbps e 10 Mbps poderiam receber a imagem com melhor qualidade fundindo ambas as camadas. O remetente não precisa conhecer as taxas de recepção de todos os receptores, ele precisa apenas saber a taxa máxima dos receptores. O remetente codifica o áudio e vídeo em várias camadas e envia todas elas para a árvore *multicast* à taxa máxima e daí, os receptores escolhem a camada que são adequadas às suas taxas de recepção.

O RSVP opera em duas fases. Uma fonte transmissora anuncia seu conteúdo enviando mensagens de caminho RSVP por meio de uma árvore *multicast*, indicando a largura de banda requerida pelo conteúdo e as informações sobre o caminho até o remetente. Cada receptor envia uma mensagem de reserva RSVP à árvore *multicast*. Essa mensagem de reserva especifica a taxa a qual o receptor gostaria de receber os dados provenientes da fonte. Quando a mensagem de reserva chega a um roteador, este ajusta seu escalonador de pacotes para atender àquela reserva. Por isto, o RSVP é orientado para o

receptor, pois o receptor de um fluxo de dados inicia e mantém a reserva de recursos usada para um determinado fluxo.

3.14. **Fundamentos do BGP**

O BGP é um protocolo de roteamento dinâmico, utilizado para comunicação entre sistemas autônomos (AS). Baseados nessas informações, os sistemas autônomos conseguem trocar informações e determinar o melhor caminho para as redes que formam a *Internet*. Tal papel é muito importante, sabendo-se que a todo momento as redes podem sofrer alterações, podem ocorrer quedas de suas conexões, receber anúncios inválidos, aplicar políticas, manter a conectividade por outros caminhos, adaptando-se rapidamente e mantendo a consistência de seus anúncios de forma eficiente.

A divulgação das informações de roteamento BGP [54] é feita entre roteadores que estabelecem uma relação de “vizinhança”, sempre na forma de pares. Tendo essa relação, são trocadas as informações contidas nas tabelas de roteamento BGP de cada um desses. Para estabelecer uma relação de vizinhança é necessário que dois roteadores tenham uma conexão direta entre eles, ou que algum protocolo IGP (*Interior Gateway Protocol*) trate de garantir a alcançabilidade. Essa relação de vizinhança pode definir aos roteadores uma relação de pares (*peers*).

Sendo um protocolo que requer confiabilidade em sua comunicação, para garantir a alcançabilidade entre redes, é necessário que seja utilizada uma forma confiável de troca de informações deste protocolo. Isso é obtido pela utilização do protocolo TCP entre dois roteadores que trocam informações do protocolo BGP. A porta utilizada para a comunicação é 179.

Para diferir e identificar univocamente em cada sistema autônomo (AS), esse será associado a um número que o identifica mediante os demais sistemas. Esse número varia entre 1 e 65.535, sendo que a faixa entre 64.512 e 65.535 é destinada a uso privado.

3.14.1. **SESSÃO BGP**

Antes do estabelecimento de uma sessão BGP, os roteadores vizinhos trocam mensagens entre si para entrar em acordo sobre quais serão os parâmetros da sessão. Não havendo discordância e nem erros durante a negociação dos parâmetros entre as partes, a

sessão BGP é estabelecida. Caso contrário, serão enviadas mensagens de erro e a sessão não será aberta.

Quando a sessão é estabelecida entre os roteadores, são trocadas mensagens contendo todas as informações de roteamento, ou seja, todos os melhores caminhos previamente selecionados por cada um, para os destinos conhecidos. Posteriormente, eles trocarão mensagens somente de atualização das informações de roteamento de forma incremental. Essa técnica mostrou-se um avanço no que se refere à diminuição da carga das CPUs dos roteadores e na economia da banda dos enlaces, quando comparada a outros protocolos que, ao comunicarem suas atualizações, enviam, periodicamente, a totalidade de rotas instaladas em suas tabelas.

3.14.2. **Mensagem BGP**

As mensagens trocadas em sessões BGP têm o comprimento máximo de 4.096 bytes, e mínimos 19 bytes. Todas as mensagens são compostas de, no mínimo, um cabeçalho e, opcionalmente, uma parte de dados. O formato do cabeçalho das mensagens BGP está apresentado na figura 3.14.

Figura 3.14 – Cabeçalho de mensagem BGP.

A funcionalidade do “Campo Marcador” é verificar a autenticidade da mensagem recebida e se houve perda de sincronização entre os roteadores vizinhos BGP.

O “Campo Comprimento” deve conter um número que representa o comprimento total da mensagem, incluindo o cabeçalho. Como pode haver mensagens que não possuem dados após o cabeçalho, a menor mensagem BGP enviada é de 19 bytes.

Finalmente, o “Campo Tipo”, contém um número que representa o código de um tipo de mensagem. Os tipos de mensagens são: KEEPALIVE, NOTIFICATION, OPEN e UPDATE.

A mensagem do tipo OPEN é enviada para se iniciar a abertura de uma sessão BGP entre os vizinhos BGP. A mensagem do tipo NOTIFICATION é enviada no caso da

detecção de erros durante ou após o estabelecimento de uma sessão BGP, com o propósito de verificar se a comunicação entre os vizinhos está ativa. A mensagem do tipo KEEPALIVE é composta apenas de cabeçalho padrão das mensagens BGP, sem dados transmitidos após o cabeçalho. O tempo máximo permitido para o recebimento da mensagem KEEPALIVE é definido pelo *hold time*. Por fim, a mensagem UPDATE é enviada quando há mudanças na rede. Essa mudança pode ser uma nova rede disponível e propagada através do BGP ou a necessidade de se remover uma rota que aponta para uma rede desativada.

4. **Análise do tráfego de voz em redes MPLS**

Com o objetivo de se analisar a qualidade de serviço do tráfego de pacotes de voz em uma rede MPLS foi projetado um ambiente de testes buscando-se coletar o máximo de evidências possíveis que pudessem ser utilizadas como elementos de pesquisa. Neste capítulo serão descritos a idealização, montagem e análise do ambiente de testes.

4.1. **Etapas do Experimento**

No primeiro momento do experimento foi realizado o projeto e montagem física da rede MPLS de testes que serviu como fonte de dados para a análise do tráfego de voz. Foi feito um levantamento dos equipamentos necessários para a montagem da rede e o estudo técnico necessário a realização da configuração dos mesmos.

Em seguida, foi iniciada a análise de desempenho da rede MPLS, que consistiu em realizar a troca de pacotes entre a origem e o destino e verificar o percentual de perdas no meio, a análise da latência no tráfego dos pacotes e o mapeamento dos roteadores que compunham o caminho entre a origem e o destino.

Montada a rede de testes, foram realizadas ligações com a finalidade de se coletar informações e posteriormente analisar a qualidade das mesmas. Concluído os testes de ligações com a rede MPLS, foi percebido que uma análise comparativa entre a rede testada e uma outra solução de telefonia IP tornaria o experimento mais preciso na análise da qualidade das ligações.

4.2. **Cenário de Teste**

Para a montagem e configuração da rede MPLS de testes foram enumerados os equipamentos necessários para a realização desta tarefa. No total foram necessários dois roteadores, dois switches, dois telefones IP e um computador. A seguir estão as especificações técnicas de tais equipamentos.

4.2.1. **Roteadores**

Os roteadores utilizados foram o Cisco 3700 Series com versão do Sistema Operacional 12.3 (22), com um processador de 350 MHz, 256 Mbytes de memória RAM e memória Flash de 128 Mbytes além de duas interfaces *FastEthernet*/IEEE 802.3. O roteador utilizado é ilustrado na figura 4.1.

Figura 4.1 – Roteador Cisco 3700 Series.

4.2.2. **Switches**

Foi utilizado também, em cada uma das localidades um *switch* Cisco 3560G de 48 portas Gigabit Ethernet com versão do Sistema Operacional 12.2 (25r) SEE4, processador de 230 MHz, 128 Mbytes de memória RAM e 64 Mbytes de memória Flash. O *switch* utilizado é ilustrado na figura 4.2.

Figura 4.2 – *Switch* Cisco 3560.

4.2.3. **Telefones IP**

Conectado a uma das portas do *Switch* estava um telefone IP Modelo 4621SW IP da Avaya. Na figura 4.3 a seguir é ilustrado o telefone IP utilizado no experimento.

Figura 4.3 – Telefone IP 46SW IP.

4.2.4. **Computador**

O computador utilizado teve a finalidade de coletar e analisar os pacotes de voz e sinalização que trafegaram na rede. A máquina utilizada para a coleta destas informações foi um Pentium III 1.2 GHz com 256 Mbytes de memória RAM e HD de 20 GigaBytes.

4.3. **Topologia da rede MPLS de Testes**

A topologia da rede utilizada para o estudo do tráfego de voz sobre MPLS, consistiu em se conectar duas redes, uma localizada na cidade de Recife - PE e a outra localizada em São Paulo – SP como mostra a figura 4.4 a seguir. O enlace MPLS utilizado para teste tinha uma taxa de transmissão de 2048 kbps determinístico e simétrico. O enlace era simétrico porque as taxas de *upload* e download do enlace eram iguais e determinístico porque a taxa de 2048 kbps era garantida. A escolha das duas localidades (Recife e São Paulo) para a realização dos testes foi motivada pelo interesse de medir a qualidade de uma

ligação entre locais geograficamente distantes. Afinal, um dos grandes atrativos das ligações usando-se voz sobre IP é a realização de chamadas de longa distância a um baixo custo. Outro ponto de motivação é que a grande distância entre a origem e o destino traria condições não ideais ao experimento tais como: aumento no tempo de resposta dos pacotes e um número de roteadores intermediários maior do que se a origem e o destino estivessem localizados em uma mesma cidade.

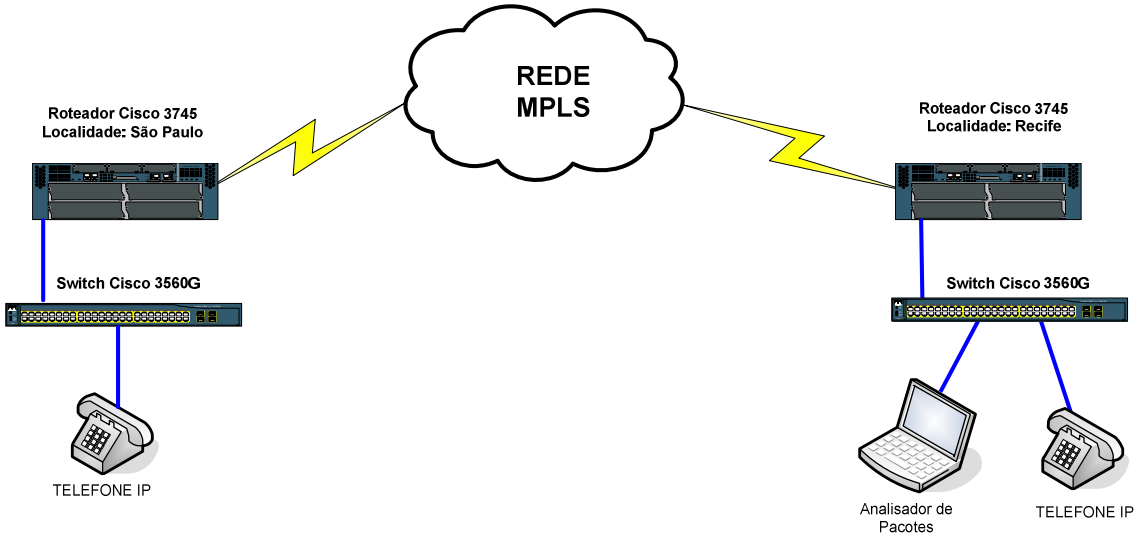


Figura 4.4 – Diagrama da rede MPLS de testes.

4.4. **Análise de Desempenho da Rede MPLS**

O enlace MPLS que conecta Recife a São Paulo utilizou o *backbone* MPLS da Embratel para conectar as duas localidades. Foi necessário avaliar a confiabilidade, disponibilidade e a qualidade do meio de transmissão utilizado, por ser este um ponto determinante na qualidade das ligações. A análise e testes do enlace foram realizadas conforme as etapas descritas a seguir:

- **Primeiro Teste de Tráfego de Pacotes:** este teste consistiu em enviar 10^6 pacotes com tamanho de 500 bytes cada, tendo como origem o roteador localizado em Recife e destino o roteador de São Paulo. A finalidade desse teste foi identificar a latência e estatísticas de perdas de pacotes na rede.

- **Segundo Teste de Tráfego de Pacotes:** este teste consistiu em enviar 10^6 pacotes com tamanho de 500 bytes cada, tendo como origem o roteador localizado em São Paulo e destino o roteador de Recife.
- **Mapeamento do núcleo da rede MPLS:** este teste consistiu em realizar o mapeamento dos roteadores que compunham o *backbone* da rede MPLS da Embratel que conectou as redes entre Recife e São Paulo.
- **Disponibilidade do enlace MPLS:** este teste consistiu em realizar a avaliação da disponibilidade do enlace MPLS utilizado nos testes.

4.4.1. **Primeiro Teste de Tráfego de Pacotes**

A troca de pacotes entre a origem e destino da rede MPLS teve como objetivo mensurar a confiabilidade da entrega dos pacotes. Em uma conversação telefônica via IP não há o reenvio de pacotes perdidos, por isto a confiabilidade do meio de transmissão na entrega dos pacotes de voz é de fundamental importância para que se tenha uma boa qualidade nas ligações. Neste primeiro teste, foram enviados a partir do roteador de Recife com destino o roteador de São Paulo, 1.000.000 de pacotes. Cada pacote tinha o tamanho de 500 bytes.

A ferramenta de testes de envio e recebimento de pacotes utilizada foi a ferramenta já disponível no sistema operacional do roteador que funciona da seguinte forma. O roteador envia um pacote IP para o destino e aguarda uma resposta do mesmo com a confirmação de recebimento do pacote. Caso esta resposta não seja recebida dentro de um limite de tempo configurado, o pacote enviado é dado como perdido. Este tempo de resposta máximo, para que a partir dele o pacote seja dado como perdido, é chamado de *timeout*, Neste primeiro teste o *timeout* foi configurado com o tempo de dois segundos. O resultado do teste foi uma taxa de sucesso de cem por cento, onde dos 1.000.000 pacotes enviados 1.000.000 foram recebidos.

Outra informação relevante disponibilizada como resultado do teste é o tempo de resposta no envio de cada pacote. É recomendado pela Cisco Systems, que o tempo de resposta dos pacotes não exceda 150 ms para que não haja perda na qualidade das ligações [27]. Um tempo de resposta alto pode ocasionar cortes ou metalização da voz do interlocutor no decorrer de um ligação.

Dentre a totalidade de pacotes que trafegaram na rede o que teve o menor tempo de resposta apresentou um atraso de 35 ms, o que apresentou o maior atraso teve 72 ms de atraso e a média dos atrasos dos 1.000.000 pacotes foi de 40 ms.

Como conclusão do primeiro teste de tráfego de pacotes entre os roteadores da rede MPLS, foi observado um tempo de resposta médio bem abaixo do exigido como requisito mínimo para se obter uma conversação de voz inteligível. A rede também se demonstrou ser confiável, pois dos 1.000.000 pacotes enviados, nenhum foi perdido.

4.4.2. **Segundo Teste de Tráfego de Pacotes**

No segundo teste a origem foi o roteador de São Paulo e destino o roteador de Recife. Neste teste também foram enviados 1.000.000 pacotes com o tamanho de 500 bytes cada e tendo como tolerância máxima de atraso, ou *timeout*, o tempo de dois segundos. Como resultado foi obtida uma taxa de sucesso de cem por cento, onde 1.000.000 de pacotes foram enviados e 1.000.000 foram recebidos. Dentre a totalidade de pacotes que trafegaram na rede o que teve o menor tempo de resposta apresentou um atraso de 34 ms, o que apresentou o maior atraso teve 72 ms de atraso e a média dos atrasos dos 1.000.000 de pacotes foi de 39 ms.

No segundo teste também foi obtida uma média de atraso bem abaixo dos 150 ms exigidos e a rede se demonstrou bem estável quanto à confiabilidade no tráfego de pacotes. Pelo fato do enlace ser simétrico, tendo taxas iguais de *download* e *upload* e também ser dedicado ao tráfego de voz, os valores dos atrasos dos pacotes foram bem aproximados tanto no primeiro teste como no segundo teste de tráfego de pacotes.

4.4.3. **Mapeamento do núcleo da rede MPLS**

Mapear o caminho que os pacotes percorrem na rede desde a origem até o destino é um ponto de grande importância e influência na qualidade das ligações. O número de saltos, ou o número de roteadores pelos quais os pacotes passam, influencia diretamente no tempo que o pacote de voz leva para chegar ao seu destino. Cada vez que um pacote chega a um roteador da rede, seu cabeçalho é aberto, analisado e encaminhado para o próximo roteador. Esta tarefa leva algum tempo e caso haja muitos roteadores no intermédio entre a

origem e o destino dos pacotes o atraso inserido no tráfego dos pacotes pode degradar a qualidade da ligação.

Através de uma ferramenta do sistema operacional do roteador, chamada *traceroute* [50], pode-se obter a informação de quantos saltos (entenda-se como salto a passagem do pacote por um roteador) o pacotes deu até o seu destino e quanto tempo levou em cada salto entre os roteadores. No primeiro teste utilizando-se o *traceroute* tendo-se como origem o roteador de Recife e destino o roteador de São Paulo foi obtido o caminho expresso na tabela 4.1 a seguir:

Tabela 4.1 – Saltos entre Recife e São Paulo.

Salto	Endereço IP do roteador
1	200.249.11.77
2	200.244.167.133
3	200.244.40.94
4	200.178.73.9
5	200.178.73.10

A partir do resultado obtido pelo *traceroute* entre Recife e São Paulo, pode-se ter uma melhor visibilidade dos elementos que compõem o núcleo da rede MPLS utilizada. A figura 4.5 ilustra o caminho que os pacotes que tem como origem a rede de Recife e destino a rede de São Paulo realizam.

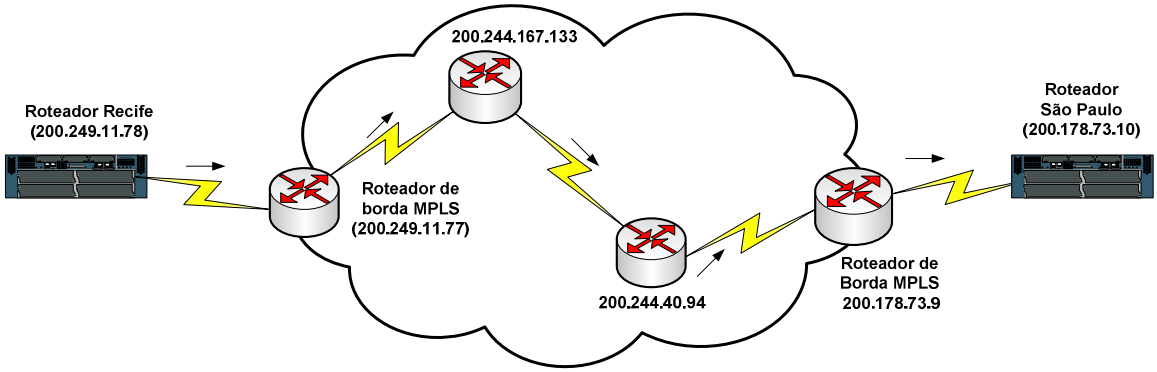


Figura 4.5 – Topologia do *backbone* MPLS Recife-SãoPaulo.

O teste utilizando o *traceroute* foi repetido, porém a origem do teste passou a ser a rede de São Paulo e o destino a rede de Recife. A justificativa de se realizar novamente o teste invertendo origem e destino é o fato de que os roteadores de *backbone* da Embratel utilizarem roteamento dinâmico. Daí a necessidade de saber se o caminho de ida dos

pacotes ser necessariamente igual ao de volta e se o número de saltos dado pelo pacote aumentou, diminuiu e ou permaneceu o mesmo. A seguir é apresentado o resultado do teste ilustrado pela tabela 4.2.

Tabela 4.2 - Saltos entre São Paulo e Recife.

Salto	Endereço IP do roteador
1	200.178.73.9
2	ebt-c1-core03.spo.embratel.net.br (200.230.242.18)
3	ebt-p7-3-dist04.rce.embratel.net.br (200.244.40.85)
4	200.249.11.77
5	200.249.11.78

A partir desse resultado, com a origem do teste em São Paulo e destino em Recife, pode-se ter uma melhor visibilidade dos elementos que compõem o núcleo da rede MPLS utilizada, que é ilustrada na figura 4.6:

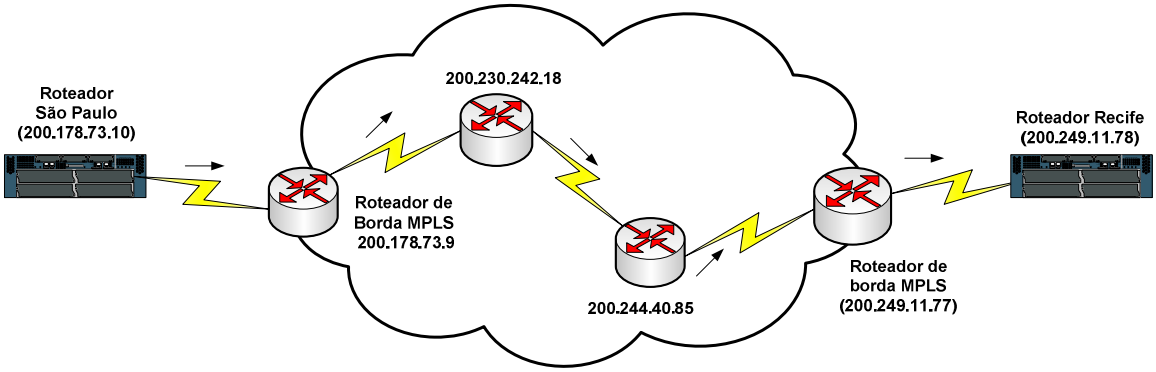


Figura 4.6 – Topologia do *backbone* MPLS São Paulo-Recife.

Como conclusão dos testes verificou-se que os caminhos ou roteadores utilizados como nós do núcleo da rede MPLS, que encaminham os pacotes entre Recife-São Paulo e São Paulo-Recife não são necessariamente os mesmos. Fica a cargo do protocolo de roteamento dinâmico, escolher o melhor caminho, que não será necessariamente o mesmo. O critério da escolha dos caminhos é feita a partir da análise de métricas de rede tais como: largura de banda disponível entre os enlaces que conectam os roteadores, atraso dos pacotes, congestionamento do enlace, entre outros.

4.4.4. **Disponibilidade do enlace MPLS**

O que todo usuário de qualquer serviço telefônico espera ao discar para um número em seu telefone é que o serviço esteja disponível e que sua chamada seja completada. Para competir em nível de igualdade com o sistema de telefonia convencional, os sistemas de voz sobre IP devem atingir o grau de disponibilidade conhecido por “cinco noves” (99,999% disponível) oferecido atualmente pela telefonia convencional (PSTN).

A disponibilidade do serviço de telefonia IP está diretamente ligada a disponibilidade do meio de transmissão dos pacotes de voz. Utilizar um enlace que frequentemente está indisponível torna impossível a oferta de um serviço de qualidade.

Para avaliar a disponibilidade do enlace MPLS utilizado como meio de transmissão dos pacotes de voz, foi utilizada uma ferramenta do próprio roteador que contabiliza o tempo em que o enlace MPLS está funcionando ininterruptamente. Desde o início da análise, quando foi zerado o contador que mede o tempo de disponibilidade do enlace até o fim da análise, foi observado que o enlace MPLS de testes permaneceu disponível durante sete semanas e seis dias ininterruptamente, sem apresentar nenhum tipo de intermitência ou indisponibilidade.

Através desta informação pode-se observar que se tratando de disponibilidade a solução proposta atendeu as expectativas. O fato do enlace permanecer 1.320 horas disponível não garante que o serviço jamais terá problemas ou que não haverá indisponibilidade, porém trouxe a segurança e tempo necessário para a realização dos experimentos sem nenhum contratempo devido a problemas de disponibilidade no enlace ou degradação da qualidade do mesmo.

4.5. **Recomendação H.323 e Codec G.729**

Concluída a ativação e análise de desempenho do link MPLS, dois pontos importantes do projeto foram definidos, qual o protocolo e qual *codec* seriam utilizados na rede VoIP proposta nesta dissertação.

Uma rede de telefonia necessita de diversos protocolos para poder funcionar, nesse aspecto, o H.323 é muito mais uma avaliação da arquitetura da telefonia IP do que um protocolo específico. O H.323 é considerado um padrão “guarda-chuva” que faz referência

a um grande número de protocolos específicos para codificação de voz, estabelecimento e configuração de chamadas, sinalização, transporte de dados e outros. Devido a características tais como: pacote de mensagens compacto e sinalização extremamente rápida, a recomendação H.323 foi escolhida para ser utilizada na rede VoIP proposta nesta dissertação.

O CODEC é o responsável por transformar a voz humana, um sinal analógico, em sinal digital para transmissão numa rede de dados. Nos equipamentos que funcionam como *gateways* VoIP, esses *codecs* são implementados através de um componente chamado DSP (*Digital Signal Processor*). Cada *codec* provê certa qualidade de voz. Alguns dos *codecs* mais utilizados são: G.711, G729, G726, G723.1. Devido a sua grande capacidade de compressão da voz e baixa utilização de banda o CODEC G.729 foi escolhido para aplicação da rede VoIP proposta. Por padrão, utilizando-se o G.729 uma conversação telefônica consumiria 8kbit/s de banda.

Através do Software Wireshark - Version 0.99.6a [51] instalado em um computador Pentium III 1.2 GHz com 256 Mbytes de memória RAM e HD de 20 GB foi monitorado o tráfego dos pacotes de voz da rede MPLS. O intuito da monitoração destes pacotes é constatar que o protocolo e o CODEC escolhidos estão funcionando como o determinado no projeto da rede. A seguir, na figura 4.7, é ilustrada a captura dos pacotes de voz durante uma ligação através do software de capturas de pacotes Wireshark.

No.	Time	Source	Destination	Protocol	Info
46	11.605443	10.81.14.10	10.81.12.66	SNMP	get-request
47	11.720315	10.81.14.35	10.81.12.10	H.225.0	CS: empty
48	11.747345	10.81.12.10	10.81.14.35	H.225.0	CS: empty
49	11.794536	10.81.12.22	10.81.14.35	UDP	Source port: 16900 Destination port: 16496
50	11.795219	10.81.14.35	10.81.12.22	ICMP	Destination unreachable (Port unreachable)
51	11.795412	10.81.12.22	10.81.14.35	UDP	Source port: 16901 Destination port: 16497
52	11.796585	10.81.14.35	10.81.12.22	ICMP	Destination unreachable (Port unreachable)
53	11.807726	10.81.14.35	10.81.12.10	TCP	6488 > 1720 [ACK] Seq=43 Ack=62 Win=8192 Len=0 TSV=1018911 TSER=13220405
54	11.808955	10.81.12.10	10.81.14.35	H.225.0	CS: empty CS: empty CS: empty CS: facility OpenLogicalChannel
55	11.809778	10.81.14.35	10.81.12.10	TCP	6488 > 1720 [ACK] Seq=43 Ack=312 Win=7946 Len=0 TSV=1018911 TSER=13220405
56	11.814510	10.81.12.22	10.81.14.35	RTP	PT=ITU-T G.729, SSRC=0x2B124204, Seq=2, Time=160
57	11.815226	10.81.14.35	10.81.12.22	ICMP	Destination unreachable (Port unreachable)
58	11.834502	10.81.12.22	10.81.14.35	RTP	PT=ITU-T G.729, SSRC=0x2B124204, Seq=3, Time=320
59	11.838869	10.81.14.3	224.0.0.2	HSRP	Hello (state Active)
60	11.854517	10.81.12.22	10.81.14.35	RTP	PT=ITU-T G.729, SSRC=0x2B124204, Seq=4, Time=480
61	11.855418	10.81.12.22	10.81.14.35	RTCP	Sender Report Source description
62	11.874515	10.81.12.22	10.81.14.35	RTP	PT=ITU-T G.729, SSRC=0x2B124204, Seq=5, Time=640
63	11.890822	10.81.14.2	224.0.0.2	HSRP	Hello (state Standby)
64	11.894521	10.81.12.22	10.81.14.35	RTP	PT=ITU-T G.729, SSRC=0x2B124204, Seq=6, Time=800
65	11.914532	10.81.12.22	10.81.14.35	RTP	PT=ITU-T G.729, SSRC=0x2B124204, Seq=7, Time=960
66	11.915428	10.81.12.22	10.81.14.35	RTCP	Sender Report Source description
67	11.934491	10.81.12.22	10.81.14.35	RTP	PT=ITU-T G.729, SSRC=0x2B124204, Seq=8, Time=1120
68	11.954526	10.81.12.22	10.81.14.35	RTP	PT=ITU-T G.729, SSRC=0x2B124204, Seq=9, Time=1280
69	11.974505	10.81.12.22	10.81.14.35	RTP	PT=ITU-T G.729, SSRC=0x2B124204, Seq=10, Time=1440
70	11.975417	10.81.12.22	10.81.14.35	RTCP	Sender Report Source description
71	11.994518	10.81.12.22	10.81.14.35	RTP	PT=ITU-T G.729, SSRC=0x2B124204, Seq=11, Time=1600
72	12.014525	10.81.12.22	10.81.14.35	RTP	PT=ITU-T G.729, SSRC=0x2B124204, Seq=12, Time=1760
73	12.022079	10.81.14.35	10.81.12.22	RTP	PT=ITU-T G.729, SSRC=0x3095FE5, Seq=12274, Time=150400
74	12.034531	10.81.12.22	10.81.14.35	RTP	PT=ITU-T G.729, SSRC=0x2B124204, Seq=13, Time=1920
75	12.041973	10.81.14.35	10.81.12.22	RTP	PT=ITU-T G.729, SSRC=0x3095FE5, Seq=12275, Time=150560

Figura 4.7 – Captura de pacotes de voz durante uma ligação telefônica.

4.6. **Coleta e armazenamento de informações técnicas**

Em busca da maior quantidade possível de elementos que pudessem expressar a qualidade da rede VoIP sobre MPLS, foi utilizado um recurso dos telefones IP utilizados na montagem da rede em que foi possível coletar informações técnicas sobre a rede, armazená-las e construir um gráfico com as informações em função do tempo.

Para que isto fosse possível foi disponibilizado um computador que funcionou exclusivamente para coletar as informações e gerar os gráficos. As informações enviadas pelo telefone para a geração dos gráficos foram: perda de pacotes, atraso dos pacotes e *jitter*. o servidor de *syslog* coletou e armazenou estas informações e as esboçou através de gráficos com as estatísticas obtidas como mostra a figura 4.8 a seguir.

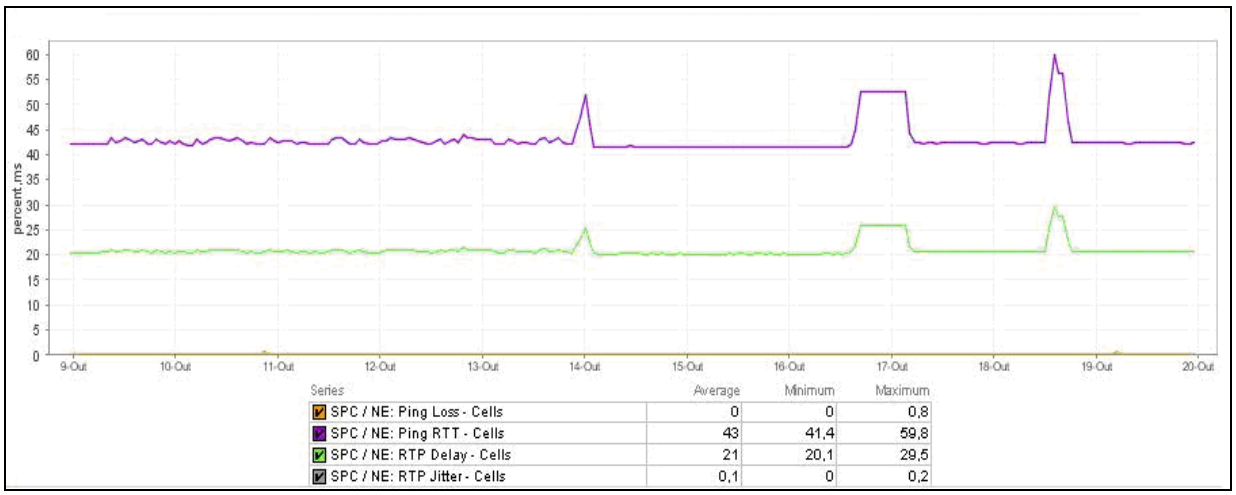


Figura 4.8 – Estatísticas da rede MPLS.

4.7. **Estudo comparativo**

No processo do estudo da qualidade das ligações utilizando-se a rede MPLS, a comparação da solução proposta com uma outra solução VoIP foi de grande importância. A análise comparativa entre as informações técnicas e subjetiva das ligações VoIP sobre MPLS e ligações VoIP sobre uma outra solução trouxe um ponto de referência que ajudou a observar se houve um ganho ou não de qualidade com a utilização da rede MPLS para o

tráfego de pacotes de voz. Para isto a solução a ser comparada com a rede MPLS deveria apresentar boa qualidade nas ligações e preferencialmente ser bem conhecida. O Skype [60] é uma solução VoIP sobre redes Par-a-Par e atende estes requisitos. Outro ponto que justifica a escolha do Skype como solução VoIP a ser comparada com a rede MPLS é o fato deste já ter sido objeto de pesquisa em estudos anteriores pelo autor desta dissertação.

4.7.1. **O Skype**

O Skype é um serviço de telefonia muito popular na *Internet*, que usa a tecnologia VoIP de modo P2P, esse também é reconhecido como um dos aplicativos VoIP que proporcionam maior qualidade de ligações. A versão do Skype utilizada para análise foi a 3.8.0.180. Porém a sua análise não é simples, pois a implementação do Skype (aplicações, protocolos e arquitetura) são proprietárias, além disso, o mesmo utiliza criptografia de ponta a ponta para que se proporcione comunicação segura nas ligações.

Cada computador que tem o software cliente do Skype é chamado de nó ou par (*peer*), onde a maioria dos nós são simples nós clientes da rede, porém cada nó tem o potencial de se tornar um super nó na rede P2P do Skype. O ambiente de teste montado para a análise da rede Skype está exibido na figura 4.9 a seguir.

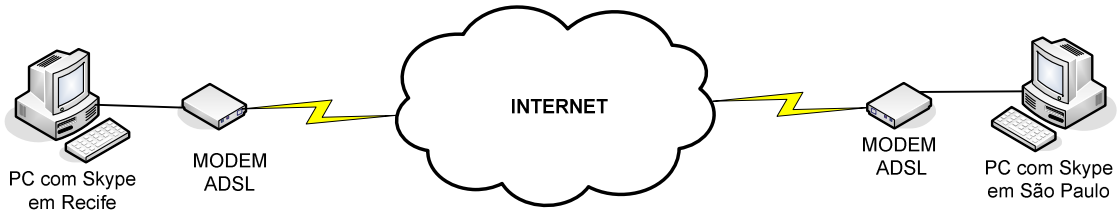


Figura 4.9- – Topologia da rede de testes Skype.

Foram utilizados dois computadores com Sistema Operacional Windows XP, tendo já instalado o software do Skype (versão 3.8.0.180). Um dos computadores estava localizado em Recife e outro em São Paulo, ambos conectados a um modem ADSL. Com as máquinas localizadas nas mesmas cidades dos testes realizados com a rede MPLS, foi pretendido se manter a máxima semelhança entre os dois testes.

4.8. **Análise de Desempenho da Rede Par-a-Par**

A conectividade entre os dois usuários Skype foi mantida através de dois enlaces ADSL um localizado em Recife com uma banda disponível de 2.048 kbps e o outro localizado em São Paulo com uma banda disponível de 2.048 kbps. Foi necessário avaliar a confiabilidade, disponibilidade e a qualidade do meio de transmissão utilizado, por ser este um ponto determinante na qualidade das ligações.

A análise e testes do enlace foram realizados conforme as etapas a seguir:

- **Primeiro Teste de Tráfego de Pacotes:** este teste consistiu em enviar pacotes com tamanho de 500 bytes cada, tendo como origem a rede localizada em Recife e destino a rede de São Paulo.
- **Segundo Teste de Tráfego de Pacotes:** este teste consistiu em enviar pacotes com tamanho de 500 bytes cada, tendo como origem a rede localizada em São Paulo e destino a rede de Recife.
- **Mapeamento dos roteadores entre origem e destino:** este teste consistiu em realizar o mapeamento dos roteadores pelos quais os pacotes de voz passaram no decorrem das ligação utilizando o Skype entre as localidades de Recife e São Paulo.
- **Disponibilidade dos enlaces ADSL:** este teste consistiu em realizar a avaliação da disponibilidade do enlace MPLS utilizado nos testes.

4.8.1. **Primeiro Teste de Tráfego de Pacotes**

A seqüência de testes realizada na rede MPLS foi mantida nos testes com a rede utilizada pelo Skype. A troca de pacotes entre a origem e destino utilizando-se os enlaces de *Internet* sobre ADSL, teve como objetivo medir a confiabilidade da entrega dos pacotes. Neste primeiro teste, foram enviados a partir da rede de Recife para a rede de São Paulo, 1.000.000 de pacotes. Cada pacote tinha o tamanho de 500 bytes.

A ferramenta de testes de envio e recebimento de pacotes utilizada neste teste foi a disponibilizada pelo *Prompt* de Comandos do próprio Sistema Operacional Windows XP.

Nesta etapa dos teste pôde-se observar as estatísticas de perdas de pacotes na rede entre os dois computadores e se o atraso máximo de 150 ms dos pacotes seria respeitado.

No primeiro teste foram enviados 1.000.000 pacotes a partir do computador de Recife com destino ao computador de São Paulo, todos com o tamanho de 500 bytes e tendo como tolerância máxima de atraso (ou *timeout*) o valor de dois segundos. Do total de pacotes, 22.751 pacotes foram perdidos e o tempo médio do atraso dos pacotes foi de 121 ms. O pacote com menor atraso teve um tempo de resposta de 89 ms e o pacote com maior atraso teve o valor de 212 ms.

Como conclusão do primeiro teste de tráfego de pacotes, foi observado um tempo médio de atraso dos pacotes abaixo dos 150 ms, porém próximo ao exigido como requisito mínimo para se obter uma conversação de voz com boa qualidade. Quanto à confiabilidade, o acesso ADSL não se mostrou tão confiável quanto a rede MPLS, porém isto já era esperado visto que não há garantia de banda no acesso a *Internet* através dos enlaces ADSL, além do fato da *Internet* não ser um meio seguro, nem confiável. Com um percentual de perda de pacotes de 2,3%, o acesso ADSL não pôde ser caracterizado como confiável.

4.8.2. **Segundo Teste de Tráfego de Pacotes**

No segundo teste a origem foi a rede de São Paulo e destino a rede de Recife. Neste teste também foram enviados 1.000.000 pacotes com o tamanho de 500 bytes cada e tendo como tolerância máxima de atraso, ou *timeout*, o tempo de dois segundos. Do total de pacotes, 19.418 pacotes foram perdidos Dentre a totalidade de pacotes que trafegaram na rede o que teve o menor tempo de resposta apresentou um atraso de 76 ms, o que apresentou o maior atraso teve 183 ms de atraso e a média dos atrasos dos 1.000.000 de pacotes foi de 101 ms.

No segundo teste também foi observado que o tempo médio de atraso dos pacotes ficou abaixo dos 150 ms exigidos para que se tenha uma ligação com boa qualidade de voz. Porém quanto a confiabilidade na entrega dos pacotes enviados a partir de São Paulo com destino a rede de Recife, também neste teste, o meio de transmissão não se demonstrou confiável quanto a entrega de pacotes, pois apresentou um percentual de perda de pacotes de 1,9%.

4.8.3. **Mapeamento dos roteadores entre origem e destino**

Para se mapear por quais roteadores os pacotes passaram da origem até o destino no decorrer de uma chamada usando-se o Skype, se utilizou uma ferramenta do *Prompt* de Comandos do próprio Windows XP (na mesma máquina onde foi instalado o Skype para a realização de teste) chamado *traceroute*. O primeiro teste foi realizado a partir da máquina com IP 189.70.178.140 localizada em Recife tendo como destino à máquina com IP 200.145.0.42 em São Paulo. Como resultado do teste é informado pela ferramenta quantos saltos foram dados pelo pacotes da origem até o destino e qual o IP dos roteadores por onde os pacotes passaram. A seguir é exibido na tabela 4.3 o número de saltos dados a partir da rede de Recife com destino a São Paulo juntamente com os IPs dos roteadores pelos quais os pacotes passaram.

Tabela 4.3 – Caminho percorrido pelos pacotes a partir de Recife para São Paulo.

Saltos	Endereço IP do roteador
1	200.217.255.216
2	200.164.180.13
3	pos5-1-1-arc-rj-rotn-01.telemar.net.br [200.223. 131.205]
4	200.223.254.109
5	as1916.rj.ptt.br [200.219.138.101]
6	so-0-1-0-r1-sp.bkb.rnp.br [200.143.252.21]
7	200.143.254.185
8	143.108.254.49
9	143.108.254.121
10	200.136.37.4
11	200.145.255.238
12	200.145.0.42

Visto que o caminho percorrido pelos pacotes que saíram da rede montada em Recife com destino a rede de São Paulo pode não ser necessariamente o mesmo caminho que os pacotes farão com a origem e destino forem invertidos, foi realizado um segundo teste tendo-se a rede de São Paulo como origem e Recife como destino. O fato de que os pacotes podem percorrer caminhos diferentes se deve ao fato de que a *Internet* utiliza protocolos dinâmicos de roteamento.

A seguir, na tabela 4.4 é exibido o caminho dos pacotes a partir da rede de São Paulo com destino a rede de Recife.

Tabela 4.4 – Caminho percorrido pelos pacotes a partir de São Paulo para Recife.

Saltos	Endereço IP do roteador
1	200.145.0.42
2	200.145.0.33
3	200.145.255.237
4	200.136.37.1
5	200.136.34.24
6	200.223.44.185
7	pos12-0-hga-mg-rotn-01.telemar.net.br (200.223.131.42)
8	so-6-1-3-0-bvg-pe-rotn-01.telemar.net.br (200.223.43.246)
9	bvg-pe-rotd-02.telemar.net.br(200.164.204.131)
10	pos6-0-bdea-ba-rotn-01.telemar.net.br (200.223.131.49)
11	200.164.180.14
12	189.70.178.140

4.8.4. **Disponibilidade dos enlaces ADSL**

A avaliação da disponibilidade dos enlaces ADSL não teve a mesma precisão que a avaliação realizada na rede MPLS. O acesso a *Internet* através de modem ADSL é realizado através de discagem a partir de um provedor e ocorre a cada momento que há necessidade de acesso por parte do usuário, diferentemente do enlace MPLS que após sua ativação o mesmo permanece ativo e disponível todo o tempo não havendo necessidades de discagem nem provedores para acesso. Pelo fato de não haver ferramentas de monitoração do enlace, nem pelo *firmware* do próprio modem nem através de software, não se pode questionar a disponibilidade dos enlaces ADSL.

4.9. **Comparações técnicas entre Skype e a rede VoIP sobre MPLS**

Além dos indicadores técnicos de rede, é importante observar outros pontos que diferenciam os dois tipos de soluções VoIP aqui apresentados. Alguns destes pontos são: o controle de acesso, autenticação de rede, disponibilidade do serviço e protocolos VoIP utilizados nas duas soluções.

4.9.1. **Controle de acesso**

O controle de acesso certifica-se que somente pessoas ou dispositivos autorizados tenham permissão de acesso a dados do usuário final que estejam transitando num elemento da rede ou enlace de comunicação. Como o Skype utiliza a *Internet* como meio de transmissão, os pacotes são misturados com outros pacotes que não são os de voz.

Tendo os protocolos VoIP sido concebidos, sem a opção de utilização de criptografia, para que a integridade das informações dos pacotes VoIP fossem mantidas foram feitos acréscimo aos padrões originais para se permitir conexões seguras. O Skype utiliza criptografia em todas as conexões oferecendo controle de acesso aos dados em trânsito. Além da criptografia, a Versão 3.8.0.180 do Skype oferece a identidade digital, que busca proteger os usuários de falsos interlocutores fazendo-se passar por outras pessoas.

Em contrapartida, a rede MPLS tem o controle de acesso feito de forma física, onde o telefone IP é conectado a um *switch* e a porta do mesmo é configurada de modo que somente o tráfego de pacotes com o endereço MAC da placa de rede do telefone IP seja permitido. Este modo de controle de acesso, além do fato de que a rede MPLS é uma linha privativa para o tráfego de voz, retira a necessidade de criptografia nas conversações para garantir a confiabilidade, o que influencia substancialmente na melhoria da qualidade das conversações.

4.9.2. **Autenticação**

Na autenticação se verifica a identidade da pessoa ou dispositivo que tenta ter acesso aos dados do usuário final que está transitando num elemento de rede ou em um enlace de comunicação. No casa da rede P2P do Skype a autenticação utilizada é do tipo usuário/senha.

No momento do *login* de um usuário Skype, através de capturas feitas com o Wireshark foi observado que o Skype se comunica primeiramente com o servidor cujo DNS cadastrado na *Internet* é o **163-158.static.quiettouch.com [204.9.163.158]** e está localizado na cidade Nova Iorque - EUA. Este servidor pertence a Quite Touch, que é uma empresa canadense que presta serviço de Segurança em TI. Através de vários testes foi observado que o IP 204.9.163.158 sempre é contatado no momento do login, o que nos faz acreditar que este funcione como um dos servidores de autenticação dos clientes Skype, porém não há evidências suficientes através dos testes realizados para que se possa afirmar que este seja o único servidor de autenticação.

Já para a rede MPLS proposta nesta dissertação a autenticação do telefone IP é realizada no momento em que o telefone é ligado em um servidor de autenticação localizado na mesma rede dos telefones IP de testes. O tipo de autenticação usuário/senha também é utilizada. O fato do servidor de autenticação estar localizado em uma rede privativa propicia mais segurança aos usuários da rede de telefonia IP sobre MPLS proposta, diferentemente do Skype que tem que enviar as informações através da *Internet*, que é considerado um meio inseguro.

4.9.3. **Disponibilidade**

A disponibilidade da rede se resume ao usuário poder usar o serviço em qualquer instante, com uma probabilidade aceitável. A disponibilidade da PSTN chega à porcentagem de 99,999% e as pessoas estão acostumadas à idéia de pegar o telefone e o mesmo estar disponível para utilização.

No caso da rede P2P do Skype, foi utilizado um acesso ADSL à *Internet*, que hoje representa a grande maioria dos enlaces de acesso à *Internet* no Brasil. Embora existam aparelhos telefônicos dedicados a funcionar com uma linha Skype, na grande maioria dos

casos, os usuários preferem a solução gratuita do *softphone* Skype instalado em um computador, tendo apenas que adquirir um microfone para utilizar o aplicativo.

O fato de utilizar o computador também como um equipamento para telefonia pode prejudicar o desempenho e qualidade do aplicativo. Por exemplo, se o sistema operacional ou algum outro programa instalado na máquina realizar atualizações automáticas em *background*, utilizando recursos de banda e processamento do computador, isto pode gerar degradação e em alguns casos quedas na ligação. *Downloads* realizados concomitantemente a chamadas em curso, são um outro fator comum que pode gerar interferência prejudicial nas ligações. Em uma situação real, a queda, indisponibilidade ou a degradação das chamadas podem interferir no rendimento do trabalho de usuários que optem pela solução Skype em sua empresa, se cuidados não forem tomados ao se realizar a ligação.

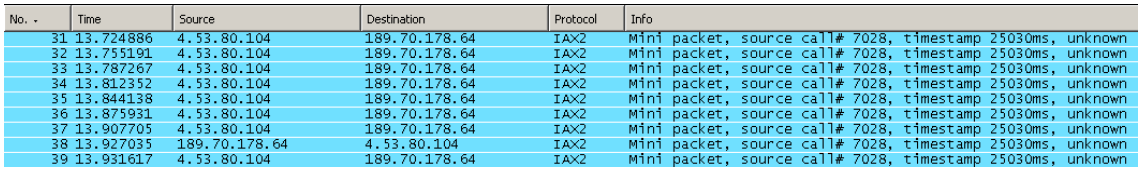
A idéia de se projetar uma rede privativa e dedicada, contempla justamente o fato de que nenhum tráfego além do de voz estaria presente na rede, com isto se buscou o máximo de qualidade, segurança e disponibilidade aos usuários da rede proposta. Vale salientar também que a utilização de um telefone IP na rede MPLS ao invés de um computador com um *softphone*, assim como o Skype, foca todos os recursos de hardware e software do equipamento exclusivamente a ligações, eliminando assim atividades concomitantes que pudessem afetar a qualidade das ligações.

4.9.4. **Protocolos**

Na rede MPLS estudada o protocolo utilizado foi o H.323. Uma das vantagens da utilização deste protocolo é que o H.323 possui um pacote de mensagens compacto e sua sinalização é extremamente rápida, especialmente se comparado ao SIP, que em termos comparativos utiliza pacotes de mensagens bem mais longos. Um outro fator motivador para a utilização do H.323 foi o fato deste ter se referenciado na filosofia de operação do sistema de telefonia convencional PSTN, focando o esforço nos aspectos de brevidade e disponibilidade do sistema. Os sinais do H.323 são curtos e a rede é utilizada o mínimo possível para transportar sinalização de chamadas e ao máximo para transportar voz.

Já na rede Skype, foi necessária uma pesquisa e avaliação para se descobrir qual protocolo o mesmo utiliza para o tráfego de voz. Através do Wireshark [51] (software de

análise de pacotes) foi constatado que o protocolo IAX2 [52], é atualmente utilizado pelo Skype 3.8.0.180 como mostra a figura 4.10 a seguir.



No.	Time	Source	Destination	Protocol	Info
31	13.724886	4.53.80.104	189.70.178.64	IAX2	Mini packet, source call# 7028, timestamp 25030ms, unknown
32	13.755191	4.53.80.104	189.70.178.64	IAX2	Mini packet, source call# 7028, timestamp 25030ms, unknown
33	13.787267	4.53.80.104	189.70.178.64	IAX2	Mini packet, source call# 7028, timestamp 25030ms, unknown
34	13.812352	4.53.80.104	189.70.178.64	IAX2	Mini packet, source call# 7028, timestamp 25030ms, unknown
35	13.844138	4.53.80.104	189.70.178.64	IAX2	Mini packet, source call# 7028, timestamp 25030ms, unknown
36	13.875931	4.53.80.104	189.70.178.64	IAX2	Mini packet, source call# 7028, timestamp 25030ms, unknown
37	13.907705	4.53.80.104	189.70.178.64	IAX2	Mini packet, source call# 7028, timestamp 25030ms, unknown
38	13.927035	189.70.178.64	4.53.80.104	IAX2	Mini packet, source call# 7028, timestamp 25030ms, unknown
39	13.931617	4.53.80.104	189.70.178.64	IAX2	Mini packet, source call# 7028, timestamp 25030ms, unknown

Figura 4.10 – Capturas de pacotes de voz utilizando-se o Skype.

O IAX2 (*Inter Asterisk eXchange*) é um protocolo desenvolvido pela Digium com o objetivo de estabelecer comunicação entre servidores Asterisk. O IAX é um protocolo de transporte, tal como o SIP, no entanto faz uso apenas de uma única porta UDP (4569) tanto para sinalização como para *streams* RTP e o fato de se utilizar apenas uma porta é uma vantagem em cenários que existem Firewalls ou NATs entre os interlocutores.

Uma outra vantagem do IAX2 é a utilização do *jitter buffer*. Este é uma área de dados compartilhada onde os pacotes de voz são coletados, armazenados e enviados para o processador de voz em intervalos de tempos uniformemente espaçados.

Existem dois tipos de *jitter buffer*, o estático e o dinâmico. O estático é baseado em hardware e é configurado pelo fabricante do equipamento, já o dinâmico é baseado em software e pode ser configurado pelo administrador da rede que adequará o mesmo conforme os tempos de resposta dos pacotes.

4.10. **VoIP sobre MPLS versus Skype**

Após uma análise individual das características técnicas das duas soluções de telefonia sobre o protocolo IP, foram realizados testes de ligações através da rede MPLS e através do Skype para se analisar a qualidade das mesmas. Esperou-se através desta etapa do estudo obter o quanto se ganhará em qualidade quando utilizamos a solução MPLS em comparação a uma solução VoIP que utiliza a *Internet* como meio de transmissão dos pacotes.

A metodologia desta etapa dos testes é descrita a seguir:

1. Foram realizadas 45 ligações entre as cidades de Recife e São Paulo utilizando a rede MPLS e outras 45 ligações utilizando-se a solução Par-a-Par (Skype) totalizando 90 ligações de testes.
2. As ligações foram distribuídas em três grupos de 30, onde 15 ligações foram feitas utilizando-se a rede MPLS e as outras 15 utilizando-se o Skype. Cada grupo de 30 ligações foi realizada em três dias diferentes. Esperava-se assim capturar o comportamento da rede MPLS e do enlace de *Internet* ADSL utilizado pelo Skype em momentos diferentes.
3. A realização de cada ligação aconteceu da seguinte forma. Completada a ligação, o interlocutor em Recife leu primeiramente um texto gerando assim um tráfego de pacotes com origem em Recife e destino São Paulo e ao final da leitura o interlocutor de São Paulo leu o mesmo texto gerando assim um fluxo de pacotes que tinham como origem São Paulo e destino Recife.

4. Com as leituras finalizadas os interlocutores responderam conjuntamente ao questionário da tabela 4.5 e tabela 4.6, exibidas a seguir, sobre a qualidade das ligações com a ressalva de que se um ou mais itens da tabela 4.5 fossem assinalados como Sim na tabela 4.6 a classificação da qualidade da chamada só poderia ser assinalada como Regular, Ruim ou Muito Ruim.

Tabela 4.5 - Questionário utilizado na análise subjetiva das ligações.

O áudio estava cortando em algum momento	A chamada estava com ruídos e/ou ecos	A chamada estava com atraso na voz	A chamada foi interrompida indesejadamente
Sim ou Não	Sim ou Não	Sim ou Não	Sim ou Não

Tabela 4.6 – Avaliação da qualidade das ligações.

O interlocutor considerou a chamada:	**Muito Boa**	**Boa**	**Regular**	**Ruim**	**Muito Ruim**
Assinale apenas uma das opções	( )	( )	( )	( )	( )

5. Paralelamente foram coletadas informações técnicas importantes na definição da qualidade das ligações tais como: atraso médio, *jitter*, pacotes transmitidos, perda de pacotes, pacotes transmitidos por segundo e tamanho médio dos pacotes de voz

como ilustra a tabela 4.7 a seguir. As informações técnicas do Skype foram obtidas através do registro de informações técnicas disponibilizadas pelo próprio software e as informações técnicas sobre as ligações feitas pela solução MPLS foram obtidas através do registro de informações gerados pelo aparelho de telefonia IP utilizado no experimento. De forma complementar, todos os pacotes que trafegaram durante o experimento foram capturados por um analisador de pacotes (Wireshark).

Tabela 4.7 – Informações Técnicas obtidas das ligações.

Delay médio (ms)	Jitter (ms)	Pacotes transmitidos	Perda de pacotes	Pacotes transmitidos por segundo	Tamanho médio dos pacotes (bytes)

6. Finalizados os testes, os resultados foram consolidados e analisados.

A seguir, na seção 4.11, serão esboçados os resultados dos testes de ligações utilizando o Skype e a rede MPLS realizados em três dias. Os resultados estão divididos por dia, onde foram realizados 15 ligações/dia durante 3 dias.

4.11. **Resultado dos testes**

Primeiro dia de testes

No primeiro dia de testes foram realizados primeiramente quinze ligações utilizando-se o Skype e posteriormente quinze ligações utilizando-se a solução baseada em MPLS. A seguir é mostrado através das tabelas 4.8 e 4.9 as informações técnicas e subjetivas respectivamente da solução Par a Par (Skype) e as tabelas 4.10 e 4.11 ilustram as informações técnicas e subjetivas respectivamente da solução MPLS.

Tabela 4.8 – Análise Técnica das chamadas com Skype (1º dia)

1º Dia de Testes	ANÁLISE TÉCNICA DAS CHAMADAS						
	Teste	Delay médio (ms)	Jitter (ms)	Pacotes transmitidos	Perda de pacotes	Pacotes transmitidos por segundo	Tamanho médio dos pacotes (bytes)
SOLUÇÃO P2P	1	98	20,4	1098	4,10%	22	160
	2	125	22,1	784	2,20%	23	161
	3	89	17	908	1,90%	24	155
	4	93	17,8	840	1,50%	23	158
	5	90	16,5	767	2,00%	25	160
	6	112	10,1	780	5,70%	24	161
	7	101	10,7	828	0,80%	23	159
	8	95	10,0	780	3,80%	23	162
	9	90	9,7	811	2,90%	25	160
	10	88	4,2	814	1,10%	25	160
	11	121	13,3	981	4,20%	23	152
	12	118	11,9	924	5,00%	23	157
	13	100	12,8	897	4,70%	24	158
	14	108	15,7	1019	3,30%	25	162
	15	125	14,9	911	1,70%	24	163
	Média	103,5	13,6	876	2,99%	24	159

Tabela 4.9 – Análise Subjetiva das chamadas com Skype (1º dia)

1º Dia de Testes	ANÁLISE SUBJETIVA DAS CHAMADAS					
	Teste	O áudio estava cortando em algum momento	A chamada estava com ruídos e/ou ecos	A chamada estava com atraso na voz	A chamada foi interrompida indesejadamente	Classificação da chamada
SOLUÇÃO P2P	1	Sim	Não	Não	Não	Ruim
	2	Sim	Sim	Não	Não	Ruim
	3	Não	Não	Não	Não	Muito Boa
	4	Não	Não	Não	Não	Muito Boa
	5	Não	Não	Não	Não	Muito Boa
	6	Sim	Não	Não	Não	Regular
	7	Sim	Sim	Não	Não	Regular
	8	Não	Não	Não	Não	Muito Boa
	9	Não	Não	Não	Não	Boa
	10	Não	Não	Não	Não	Muito Boa
	11	Não	Sim	Não	Não	Ruim
	12	Sim	Não	Não	Não	Regular
	13	Não	Não	Não	Não	Muito Boa
	14	Não	Sim	Não	Não	Regular
	15	Não	Sim	Sim	Não	Ruim

Tabela 4.10 – Análise Técnica das chamadas com MPLS (1º dia).

1º Dia de Testes	ANÁLISE TÉCNICA DAS CHAMADAS						
	Teste	Delay médio (ms)	Jitter (ms)	Pacotes transmitidos	Perda de pacotes	Pacotes transmitidos por segundo	Tamanho médio dos pacotes (bytes)
SOLUÇÃO MPLS	1	25	1,2	920	0,00%	31	74
	2	32	0,8	1199	0,00%	33	74
	3	20	1	1014	0,00%	35	74
	4	23	0,7	1072	0,00%	30	74
	5	19	0,8	977	0,00%	36	74
	6	24	1,3	991	0,00%	37	74
	7	25	1,1	1010	0,00%	32	74
	8	20	0,9	969	0,00%	31	74
	9	33	1,5	1088	0,00%	35	74
	10	27	1,1	971	0,00%	33	74
	11	21	0,8	1045	0,00%	30	74
	12	22	1,1	1131	0,00%	31	74
	13	25	1	1205	0,00%	35	74
	14	33	0,6	913	0,00%	36	74
	15	28	1,2	897	0,00%	35	74
	Média	25,1	1,0	1026,80	0,00%	33,33	74

Tabela 4.11 – Análise Subjetiva das chamadas com MPLS (1º dia).

1º Dia de Testes	ANÁLISE SUBJETIVA DAS CHAMADAS					
	Teste	O áudio estava cortando em algum momento	A chamada estava com ruídos e/ou ecos	A chamada estava com atraso na voz	A chamada foi interrompida indesejadamente	Classificação da chamada
SOLUÇÃO MPLS	1	Não	Não	Não	Não	Muito Boa
	2	Não	Não	Não	Não	Muito Boa
	3	Não	Não	Não	Não	Muito Boa
	4	Não	Não	Não	Não	Muito Boa
	5	Não	Não	Não	Não	Muito Boa
	6	Não	Não	Não	Não	Muito Boa
	7	Não	Não	Não	Não	Muito Boa
	8	Não	Não	Não	Não	Muito Boa
	9	Não	Não	Não	Não	Muito Boa
	10	Não	Não	Não	Não	Muito Boa
	11	Não	Não	Não	Não	Muito Boa
	12	Não	Não	Não	Não	Muito Boa
	13	Não	Não	Não	Não	Muito Boa
	14	Não	Não	Não	Não	Muito Boa
	15	Não	Não	Não	Não	Muito Boa

Segundo dia de testes

No segundo dia de testes foi mantida a mesma metodologia do primeiro dia de testes.

Tabela 4.12 – Análise Técnica das chamadas com Skype (2º dia).

2º Dia de Testes	ANÁLISE TÉCNICA DAS CHAMADAS						
	Teste	Delay médio (ms)	Jitter (ms)	Pacotes transmitidos	Perda de pacotes	Pacotes transmitidos por segundo	Tamanho médio dos pacotes (bytes)
SOLUÇÃO P2P	1	78	8,2	813	1,20%	28	148
	2	95	11,9	915	0,60%	23	162
	3	89	10,2	784	1,10%	25	138
	4	112	18,7	968	6,50%	26	158
	5	87	9,1	827	1,90%	27	112
	6	101	19,3	1012	1,70%	28	149
	7	93	6,4	956	2,10%	21	155
	8	114	16,3	876	0,90%	22	163
	9	215	33,9	318	10,10%	21	153
	10	92	5,6	794	0,70%	23	169
	11	99	14,1	933	4,20%	25	154
	12	106	21,2	1112	1,40%	26	158
	13	84	14	915	0,80%	24	161
	14	121	19,7	871	3,10%	21	144
	15	112	23,6	1042	2,70%	28	142
	Média	106,5	14,6	876	2,60%	25	151

Tabela 4.13 – Análise Subjetiva das chamadas com Skype (2º dia).

2º Dia de Testes	ANÁLISE SUBJETIVA DAS CHAMADAS					
	Teste	O áudio estava cortando em algum momento	A chamada estava com ruídos e/ou ecos	A chamada estava com atraso na voz	A chamada foi interrompida indesejadamente	Classificação da chamada
SOLUÇÃO P2P	1	Não	Não	Não	Não	Boa
	2	Não	Não	Não	Não	Muito Boa
	3	Não	Não	Não	Não	Muito Boa
	4	Sim	Sim	Não	Não	Muito Ruim
	5	Não	Sim	Não	Não	Regular
	6	Sim	Não	Não	Não	Regular
	7	Não	Não	Não	Não	Boa
	8	Não	Não	Não	Não	Muito Boa
	9	Não	Não	Sim	Sim	Muito Ruim
	10	Sim	Não	Sim	Não	Ruim
	11	Não	Não	Não	Não	Boa
	12	Não	Não	Não	Não	Muito Boa
	13	Não	Não	Não	Não	Muito Boa
	14	Sim	Não	Sim	Não	Ruim
	15	Não	Sim	Não	Não	Regular

Tabela 4.14 – Análise Técnica das chamadas com MPLS (2º dia).

2º Dia de Testes	ANÁLISE TÉCNICA DAS CHAMADAS						
	Teste	Delay médio (ms)	Jitter (ms)	Pacotes transmitidos	Perda de pacotes	Pacotes transmitidos por segundo	Tamanho médio dos pacotes (bytes)
SOLUÇÃO MPLS	1	31	0,8	875	0,00%	29	74
	2	21	0,7	942	0,00%	31	74
	3	25	0,7	988	0,00%	35	74
	4	26	0,9	1042	0,00%	33	74
	5	22	0,3	954	0,00%	32	74
	6	30	1,1	877	0,00%	36	74
	7	19	0,7	946	0,00%	28	74
	8	20	1	899	0,00%	34	74
	9	31	2,1	971	0,00%	31	74
	10	29	1,6	934	0,00%	32	74
	11	22	0,5	1012	0,00%	28	74
	12	18	0,6	1007	0,00%	29	74
	13	27	1,2	974	0,00%	30	74
	14	31	1,2	845	0,00%	27	74
	15	29	0,9	876	0,00%	34	74
	Média	25,4	1,0	942,80	0,00%	31,27	74

Tabela 4.15 – Análise Subjetiva das chamadas com MPLS (2º dia).

2º Dia de Testes	ANÁLISE SUBJETIVA DAS CHAMADAS					
	Teste	O áudio estava cortando em algum momento	A chamada estava com ruídos e/ou ecos	A chamada estava com atraso na voz	A chamada foi interrompida indesejadamente	Classificação da chamada
SOLUÇÃO MPLS	1	Não	Não	Não	Não	Muito Boa
	2	Não	Não	Não	Não	Muito Boa
	3	Não	Não	Não	Não	Muito Boa
	4	Não	Não	Não	Não	Muito Boa
	5	Não	Não	Não	Não	Muito Boa
	6	Não	Não	Não	Não	Muito Boa
	7	Não	Não	Não	Não	Muito Boa
	8	Não	Não	Não	Não	Muito Boa
	9	Não	Não	Não	Não	Muito Boa
	10	Não	Não	Não	Não	Muito Boa
	11	Não	Não	Não	Não	Muito Boa
	12	Não	Não	Não	Não	Muito Boa
	13	Não	Não	Não	Não	Muito Boa
	14	Não	Não	Não	Não	Muito Boa
	15	Não	Não	Não	Não	Muito Boa

Terceiro dia de testes

No terceiro dia de testes foi mantida a mesma metodologia do primeiro e segundo dia de testes. A seguir é mostrado através das tabelas 4.16 e 4.17 as informações técnicas e subjetivas da solução Par a Par (Skype) e as tabelas 4.18 e 4.19 ilustram respectivamente as informações técnicas e subjetivas da solução MPLS.

Tabela 4.16 – Análise Técnica das chamadas com Skype (3º dia).

3º Dia de Testes	ANÁLISE TÉCNICA DAS CHAMADAS						
	Teste	Delay médio (ms)	Jitter (ms)	Pacotes transmitidos	Perda de pacotes	Pacotes transmitidos por segundo	Tamanho médio dos pacotes (bytes)
SOLUÇÃO P2P	1	105	15,2	714	0,80%	30	132
	2	92	10	815	1,30%	22	128
	3	84	11,3	912	0,50%	26	141
	4	112	9,4	1007	4,10%	28	146
	5	103	16,1	852	1,00%	24	150
	6	87	12,2	968	0,60%	21	127
	7	92	9,7	817	1,20%	27	120
	8	83	11,9	845	1,10%	22	149
	9	86	13,5	831	1,70%	23	158
	10	91	17,1	802	2,30%	31	117
	11	78	8,3	901	0,40%	29	160
	12	98	7,2	1032	1,80%	25	158
	13	84	9,8	800	0,70%	28	151
	14	131	10,7	915	5,10%	24	155
	15	78	13,1	844	0,90%	26	159
	Média	93,6	11,8	870	1,57%	26	143

Tabela 4.17 – Análise Subjetiva das chamadas com Skype (3º dia).

3º Dia de Testes	ANÁLISE SUBJETIVA DAS CHAMADAS					
	Teste	O áudio estava cortando em algum momento	A chamada estava com ruídos e/ou ecos	A chamada estava com atraso na voz	A chamada foi interrompida indesejadamente	Classificação da chamada
SOLUÇÃO P2P	1	Não	Não	Não	Não	Boa
	2	Não	Não	Não	Não	Muito Boa
	3	Não	Não	Não	Não	Muito Boa
	4	Não	Não	Não	Não	Muito Boa
	5	Não	Não	Não	Não	Muito Boa
	6	Sim	Não	Não	Não	Ruim
	7	Não	Não	Não	Não	Boa
	8	Não	Não	Não	Não	Muito Boa
	9	Não	Não	Não	Não	Muito Boa
	10	Não	Não	Não	Não	Muito Boa
	11	Não	Não	Não	Não	Boa
	12	Não	Não	Não	Não	Muito Boa
	13	Não	Não	Não	Não	Muito Boa
	14	Sim	Não	Sim	Não	Ruim
	15	Não	Sim	Não	Não	Muito Ruim

Tabela 4.18 – Análise Técnica das chamadas com MPLS (3º dia).

3º Dia de Testes	ANÁLISE TÉCNICA DAS CHAMADAS						
	Teste	Delay médio (ms)	Jitter (ms)	Pacotes transmitidos	Perda de pacotes	Pacotes transmitidos por segundo	Tamanho médio dos pacotes (bytes)
SOLUÇÃO MPLS	1	38	0,7	917	0,00%	33	74
	2	40	0,4	689	0,00%	31	74
	3	22	0,1	711	0,00%	30	74
	4	19	0,9	818	0,00%	25	74
	5	38	0,2	998	0,00%	31	74
	6	33	1,4	1002	0,00%	24	74
	7	26	0,6	883	0,00%	29	74
	8	27	0,8	930	0,00%	28	74
	9	32	1,9	877	0,00%	22	74
	10	33	0,7	894	0,00%	25	74
	11	40	0,9	856	0,00%	26	74
	12	15	0,7	964	0,00%	31	74
	13	16	0,6	1018	0,00%	29	74
	14	20	1,5	811	0,00%	33	74
	15	30	1,1	799	0,00%	34	74
	Média	28,6	0,8	877,80	0,00%	28,73	74

Tabela 4.19 – Análise Subjetiva das chamadas com MPLS (3º dia).

3º Dia de Testes	ANÁLISE SUBJETIVA DAS CHAMADAS					
	Teste	O áudio estava cortando em algum momento	A chamada estava com ruídos e/ou ecos	A chamada estava com atraso na voz	A chamada foi interrompida indesejadamente	Classificação da chamada
SOLUÇÃO MPLS	1	Não	Não	Não	Não	Muito Boa
	2	Não	Não	Não	Não	Muito Boa
	3	Não	Não	Não	Não	Muito Boa
	4	Não	Não	Não	Não	Muito Boa
	5	Não	Não	Não	Não	Muito Boa
	6	Não	Não	Não	Não	Muito Boa
	7	Não	Não	Não	Não	Muito Boa
	8	Não	Não	Não	Não	Muito Boa
	9	Não	Não	Não	Não	Boa
	10	Não	Não	Não	Não	Muito Boa
	11	Não	Não	Não	Não	Muito Boa
	12	Não	Não	Não	Não	Muito Boa
	13	Não	Não	Não	Não	Muito Boa
	14	Não	Não	Não	Não	Muito Boa
	15	Não	Não	Não	Não	Muito Boa

4.12. **Análise dos resultados**

Para facilitar a análise dos dados obtidos, as informações técnicas e subjetivas foram consolidadas e ilustradas através de gráficos. Primeiramente, foram analisados os dados técnicos.

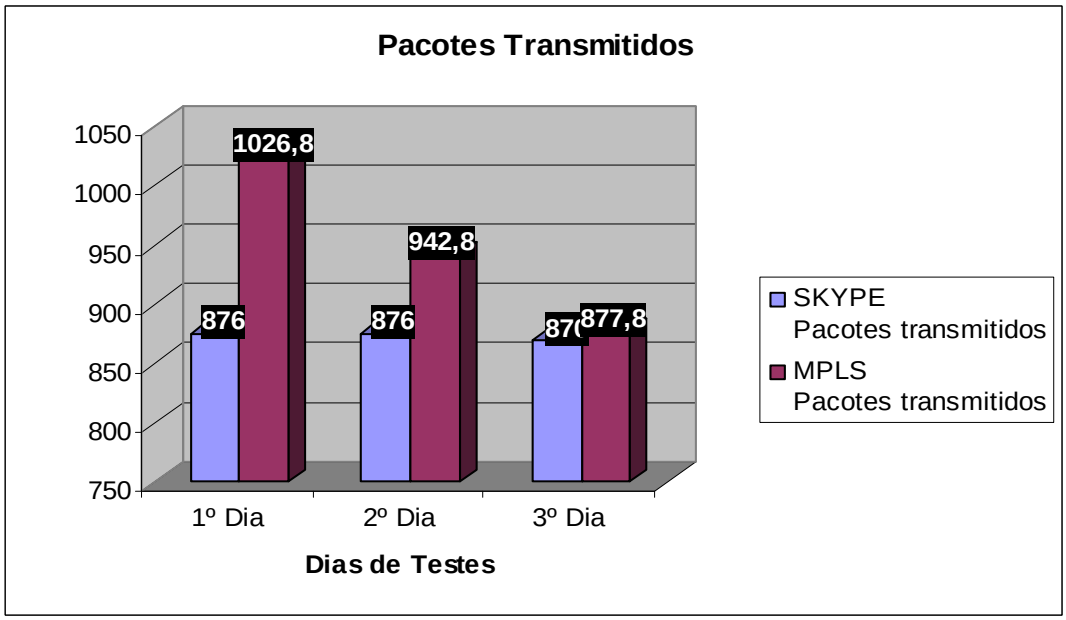
Pacotes Transmitidos

Pôde-se observar que o número médio de pacotes transmitidos numa ligação utilizando-se a solução MPLS foi maior do que o número médio de pacotes transmitidos em uma ligação utilizando-se o Skype.

A maior quantidade de pacotes transmitidos pela solução MPLS é justificado pela utilização do *codec* G.729 que utiliza pacotes com tamanhos menores (em média 74 bytes) e consequentemente numa maior quantidade em relação ao Skype que utiliza o *codec Speex* onde o tamanho dos pacotes são maiores (em média 120 bytes).

A média de pacotes transmitidos por dia de teste é ilustrado na figura 4.20.

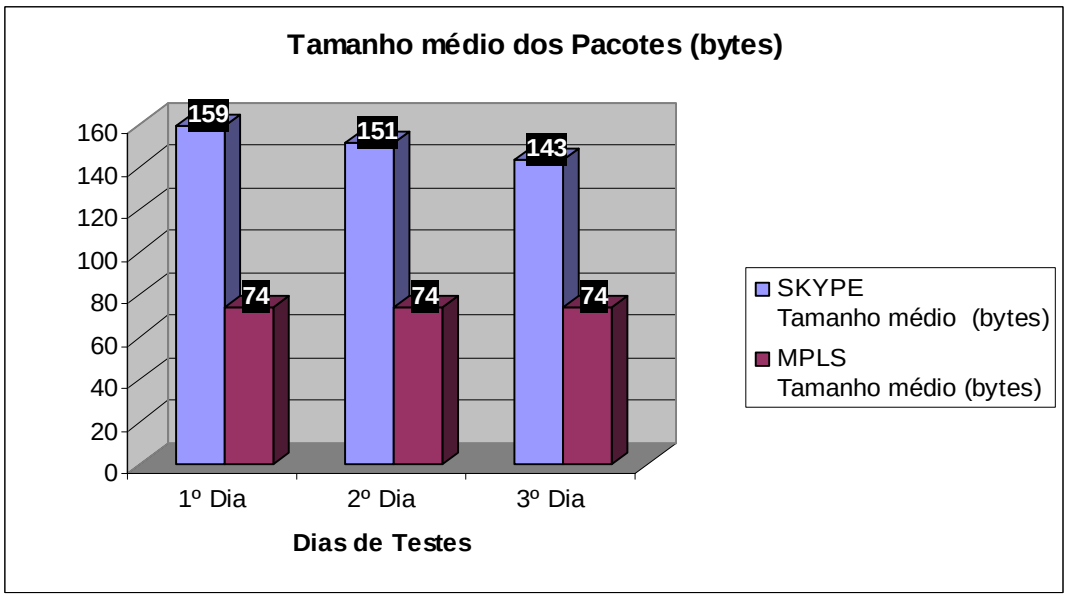
Figura 4.11 – Médias dos pacotes transmitidos por dias de testes.



Tamanho médio dos pacotes transmitidos por ligação

Embora a solução MPLS transmita uma maior quantidade de pacotes por ligação o tamanho dos pacotes são menores em relação aos pacotes transmitidos em uma ligação utilizando-se o Skype como mostra a figura 4.12.

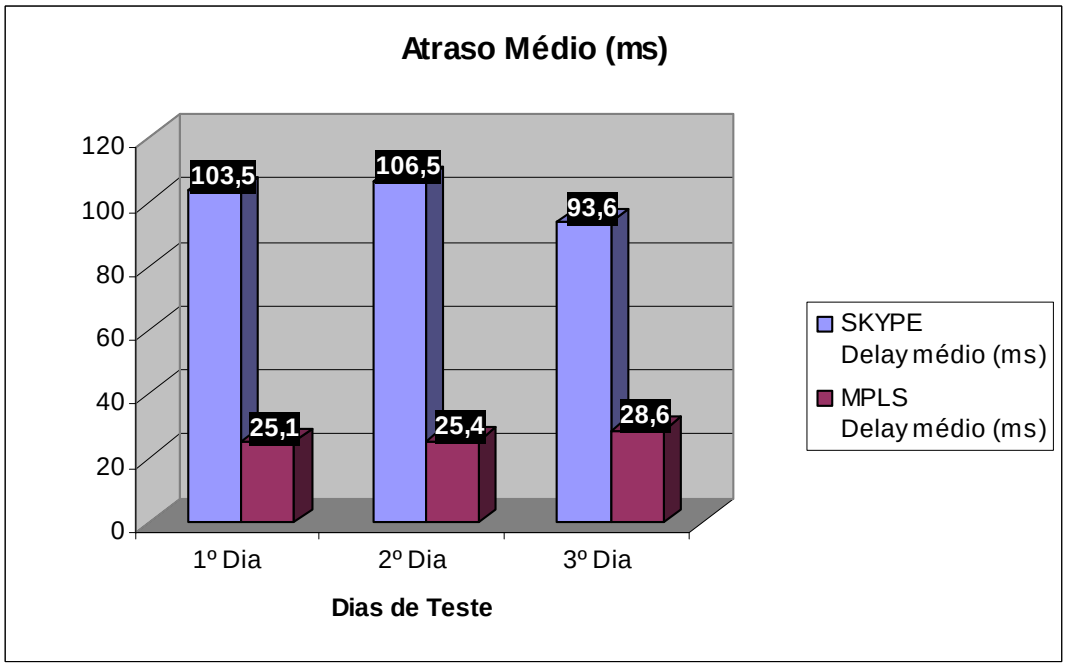
Figura 4.12 – Tamanho médio dos pacotes em bytes.



Atraso médio dos pacotes

O atraso dos pacotes de voz em uma ligação VoIP não deve exceder o valor de 150ms [27]. Tanto nas ligações utilizando-se o MPLS quanto nas ligações utilizando-se VoIP, o valor médio do atraso não excedeu o valor recomendado, porém os atrasos médios dos pacotes que trafegaram na rede MPLS nos três dias de testes, foram bem menores em relação aos pacotes do Skype como é ilustrado na figura 4.13. A diferença explica-se pelo fato do Skype utilizar a *Internet* como meio de transmissão para os pacotes de voz, onde não há gerência nem a possibilidade de implementação de qualidade de serviço (QoS). Em contrapartida a solução MPLS nesta dissertação foi projetada com dedicação exclusiva ao tráfego de voz.

Figura 4.13 – Atraso médio dos pacotes de voz durante as ligações.

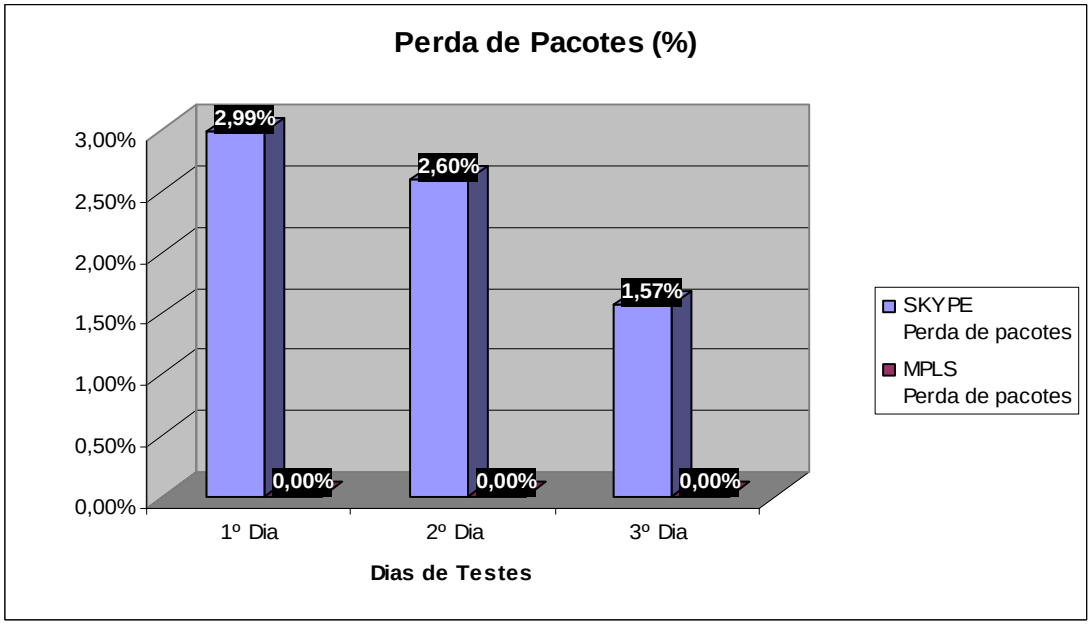


Perdas de pacotes

A confiabilidade e qualidade das ligações dependem diretamente da certeza na entrega dos pacotes a sua origem.Utilizando-se a rede MPLS as perdas de pacotes foram de 0%, ou seja, todos os pacotes de voz no decorrer das ligações nos três dias de testes foram entregues ao seu destino.

Utilizando-se o Skype houve perdas de pacotes em todas as ligações realizadas nos três dias de testes o que influenciou na perda de qualidade nas ligações como é ilustrado na figura 4.14.

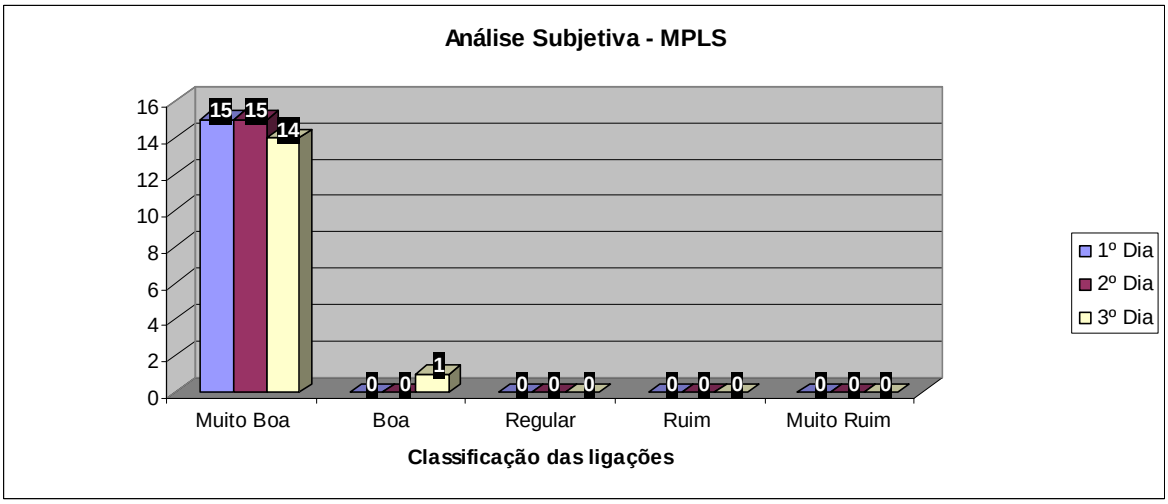
Figura 4.14 – Perda de pacotes.



Análise subjetiva das ligações utilizando MPLS

Os resultados das análises subjetivas dos interlocutores para as ligações utilizando MPLS são ilustrados na figura 4.15. Observa-se que todas as ligações utilizando-se o MPLS foram classificadas como Muito Boa ou Boa.

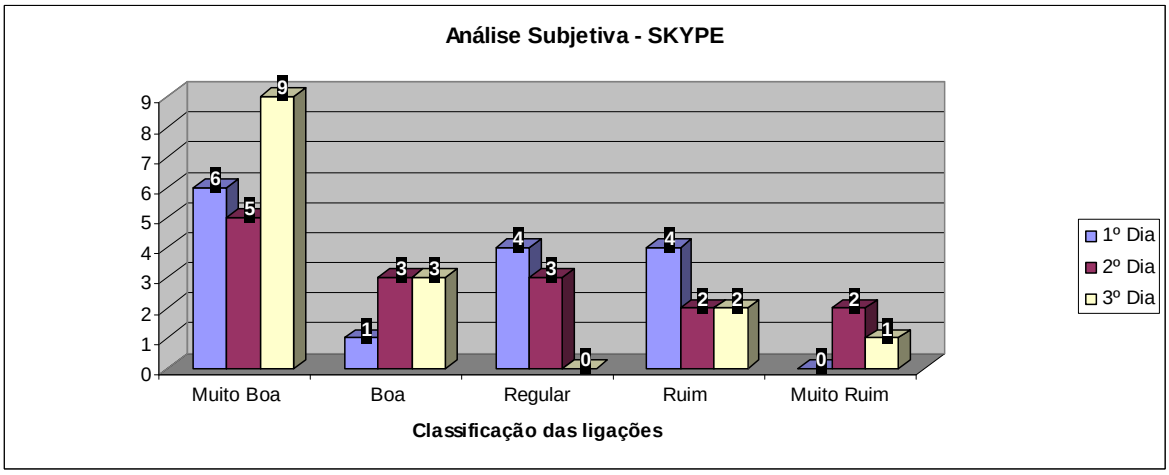
Figura 4.15 – Análise subjetiva usando-se MPLS.



Análise subjetiva das ligações utilizando Skype

Os resultados das análises subjetivas dos interlocutores para as ligações utilizando Skype são ilustrados na figura 4.16. Observa-se que as ligações foram classificadas de forma mais heterogênea comparando-se com o MPLS, onde as ligações foram avaliadas de forma mais distribuída como Muito Boa, Boa, Regular, Ruim e Muito Ruim.

Figura 4.16 – Análise subjetiva usando-se Skype.



5. **Conclusões e trabalhos futuros**

São desafios da telefonia sobre IP oferecer aos seus usuários níveis de qualidade de voz similares aos experimentados no sistema de telefonia convencional PSTN (*Public Switched Telephone Network*), confiabilidade e segurança, tudo isto em tempo real através de uma rede de pacotes IP que não foi inicialmente projetada para esse fim. Para algumas soluções de telefonia principalmente no meio corporativo a substituição dos circuitos de voz convencionais por enlaces IP que sirvam como meio de transmissão da voz reduziriam significativamente o custo operacional no que se refere a telefonia.

O estudo do tráfego de voz sobre redes MPLS realizado nesta dissertação buscou avaliar o quanto este protocolo traria a qualidade, confiabilidade e segurança necessárias para a substituição da telefonia convencional pela telefonia IP em situações em que a degradação e a não inteligibilidade das conversações telefônicas podem ser desastrosas.

Empresas de telefonia no Brasil seguem regras rigorosas regidas pela Agência Nacional de Telecomunicações (Anatel). O uso da voz sobre IP pode representar um ganho significativo para estas empresas, tanto financeiramente como tecnicamente, desde que a qualidade do serviço prestado não seja inferior ao mesmo serviço experimentado no sistema de telefonia convencional PSTN.

Nesta dissertação foi montada uma rede MPLS de testes que foi utilizada como meio de transmissão para o tráfego de voz. Aspectos técnicos e subjetivos foram observados e analisados nas ligações realizadas entre as cidades de Recife e São Paulo. Porém, após a coleta e processamento dos dados, foi percebido que uma análise comparativa com uma outra solução de voz sobre IP tornaria as conclusões do experimento mais claras e completas. Daí, foi escolhida uma solução VoIP bastante difundida e com reconhecida qualidade de ligações para se parametrizar o ganho obtido com a utilização de uma rede MPLS para o tráfego de voz. Por isso, a solução escolhida para ser comparada com a rede MPLS foi o Skype [60].

A realização dos testes de ligações, utilizando-se o Skype e utilizando-se a rede MPLS projetada para os estudos desta dissertação trouxe uma maior clareza dos benefícios trazidos pelos esforços de se utilizar uma rede privativa e dedicada ao tráfego de voz. Seria muito simples, porém pouco eficiente e bastante oneroso, aumentar mais e mais a capacidade do enlace de acesso para suprir a necessidade de banda e assim garantir a qualidade de ligações. Do contrário se optou utilizar o protocolo MPLS, que ao comutar pacotes de voz através de rótulos ao invés de comutar pacotes utilizando a análise dos endereços IP, trouxe benefícios com a redução do consumo de recursos de rede e de hardware dos roteadores envolvidos.

O intuito de se comparar a rede P2P do Skype utilizando um acesso ADSL com a rede MPLS dedicada ao tráfego de voz, não foi mostrar que uma rede é melhor ou pior que a outra. O foco do estudo foi mostrar com maior clareza, que a tecnologia VoIP, dependendo de quanto esforço e investimento se deseje fazer, pode sim substituir a rede de telefonia tradicional a altura seja qual for a finalidade do usuário ao utilizar o serviço VoIP. Desde ligações para usuários residenciais até o uso de chamadas telefônicas de missão crítica tais como: central de atendimentos a clientes, centrais de atendimento de serviços públicos entre outros, a tecnologia VoIP é hoje, uma opção estável, segura, confiável e menos onerosa que a telefonia tradicional.

Observou-se então que a segurança, confiabilidade e qualidade da rede MPLS como *backbone* para a rede de voz foi satisfatório atendendo as expectativas iniciais quanto à eficiência do protocolo MPLS na otimização do transporte de pacotes de voz.

Com base nos resultados obtidos através dos experimentos apresentados nesta dissertação, pode-se estender a pesquisa para trabalhos futuros realizando:

- Testes de chamadas a partir da rede VoIP sobre MPLS com destino a PSTN.
- Implementar e analisar o fluxo mútuo de voz e vídeo em redes IP sobre MPLS.
- Aumentar a distância geográfica entre os interlocutores e observar os efeitos sobre as ligações.
- Interação entre a rede MPLS e outras tecnologias e sistemas tais como: VoIP sobre WiFi, WiMax, UMTS.

Referências

[1] TANENBAUM, A. Redes de Computadores, Tradução da Quarta Edição. Editora Campus, 2003.

[2] OPPENHEIM, A. V.; SCHAFER, R. W. Discrete-Time Signal Processing. 2. ed. USA: Prentice-Hall, 1999.

[3] PELTON, G. E. Voice Processing. 1. ed. USA : McGraw-Hill, 1992.

[4] ABRAMSON, N. Information Theory and Coding. USA: McGraw-Hill, 1963.

[5] COLLINS, D. Carrier Grade Voice Over IP. USA: Mc Graw-Hill, 2001.

[6] SILVA JUNIOR, J. Uma Aplicação de Voz Sobre IP Baseada no Session Initiation Protocol. Recife, 2003. Dissertação de Mestrado. Programa de Pós-Graduação em Engenharia Elétrica. UFPE.

[7] INTERNATIONAL TELECOMMUNICATIONS UNION – TELECOMMUNICATION STANDARDIZATION SECTOR (ITU-T). Pulse Code Modulation (PCM) of Voice Frequencies, Recommendation G.711.

[8] FERNANDES, N. Relação Entre a Qualidade das Respostas das Recomendações G.723.1 e G.729 e o Comportamento da Rede IP de Suporte. Rio de Janeiro, 2003. Dissertação (Mestrado em Engenharia de Sistemas e Computação). COPPE, UFRJ.

[9] SMITH, J. I. Instantaneous Companding of Quantized Signals. Bell System Technical Journal, v. 36 p. 653-709. 1957.

[10] RAPPAPORT, T. S. Wireless Communications – Principles and Practice. USA: Prentice-Hall, 1996.

[11] INTERNATIONAL TELECOMMUNICATIONS UNION – TELECOMMUNICATION STANDARDIZATION SECTOR (ITU-T). 7 kHz Audio-Coding Within 64 kbit/s, Recommendation G.722. 1988.

[12] INTERNATIONAL TELECOMMUNICATIONS UNION – TELECOMMUNICATION STANDARDIZATION SECTOR (ITU-T). 5-, 4-, 3- and 2-bits Sample Embedded Adaptive Differential Pulse Code Modulation (ADPCM), Recommendation G.727. 1990.

[13] INTERNATIONAL TELECOMMUNICATIONS UNION – TELECOMMUNICATION STANDARDIZATION SECTOR (ITU-T). Coding Speech at 16 kbits/s Using Low-Delay Code Excited Linear Prediction, Recommendation G.728. 1992.

[14] HERSENT, O.; GUIDE, D.; PETIT, J-P. Telefonia IP. Addison-Wesley, 2002.

[15] INTERNATIONAL TELECOMMUNICATIONS UNION – TELECOMMUNICATION STANDARDIZATION SECTOR (ITU-T). Coding of Speech at 8 kbits/s Using Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (CS-ACELP), Recommendation G.729. 1996.

[16] SILVA, J. Aplicações VoIP Utilizando o Teleporto da Rede Metropolitana da Prefeitura Municipal de Manaus. Recife, 2004. Dissertação de Mestrado. Programa de Pós-Graduação em Engenharia Elétrica. UFPE.

[17] GOMES, A.T.A., COLCHER, S., SOARES, L.F.G. "Modeling QoS Provision on Adaptable Communication Environments", In: IEEE International Conference on Communications (ICC 2001), Helsinki, Finlândia, junho de 2001.

[18] MOTA, O., " IPQoS: Uma Interface em Java para Solicitação de Serviços com QoS na *Internet*", Projeto Final de Programação, Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro, Janeiro de 2001.

[19] INTERNATIONAL TELECOMMUNICATIONS UNION – TELECOMMUNICATION STANDARDIZATION SECTOR (ITU-T). Visual Telephone Systems and Terminal Equipment for Local Area Networks which Provide a Non-Guaranteed Quality of Service, Recommendation H.323. 1996.

[20] INTERNATIONAL TELECOMMUNICATIONS UNION – TELECOMMUNICATION STANDARDIZATION SECTOR (ITU-T). Terminals and Others Entities that Provide Multimedia Communications Services over Packet Based Networks which May Not Provide a Guaranteed Quality of Service, Recommendation H.323. 2006.

[21] INTERNATIONAL TELECOMMUNICATIONS UNION – TELECOMMUNICATION STANDARDIZATION SECTOR (ITU-T). Call Signaling Protocols And Media Stream Packetization for Packet-Based Multimedia Communication Systems, Recommendation H.225.0. 2003.

[22] INTERNATIONAL TELECOMMUNICATIONS UNION – TELECOMMUNICATION STANDARDIZATION SECTOR (ITU-T). Control Protocol for Multimedia Communication, Recommendation H.245. 2006.

[23] WALLINGFORD, T. Switching for VoIP. USA : O"Reilly, 2005.

[24] SAZIMA, R. Análise, projeto e implementação de uma plataforma para experimentos som MPLS com suporte a QoS. Campinas, 2004. Dissertação de Mestrado. Departamento de Engenharia e Computação e Automação Industrial.Universidade Estadual de Campinas.

[25] INTERNET ENGINEERING TASK FORCE (IETF). Multiprotocol Label Switching Architecture, RFC 2960. 2000.

[26] XIAO, X., A. HANNAN, B. BAILEY. Traffic Enginnering wiyth MPLS in the *Internet*. IEEE Network Magazine. 2000.

[27] DAVIDSON, J., PETERS, J. Voice Over IP Fundamentals – A Systematic Approach to Understanding the Basics of Voice Over IP. Indianapolis: Cisco Press, 2000.

[28] GUEIN,L. MPLS Fundamentals. Indianapolis: Cisco Press, 2007.

[29] BLACK, U., " MPLS and Label Switching Networks" Prentice Hall Series 2001

[30] OSBORNE, E., "Engenharia de Tráfego com MPLS" Cisco Press 2003

[31] ROSEN, E., CALLON, R., VISWANATHAN, A., RFC 3031, "Multiprotocol Label Switching Architecture," 2001.

[32] JAMOUSSI, B., ANDERSSON, L., CALLON, R. and DANTU, R.. "Constraint-Based LSP Setup using LDP", RFC 3212, 2002

[33] INTERNET ENGINEERING TASK FORCE (IETF). Multiprotocol Extensions for BGP-4, RFC 2283. 1998.

[34] JAMOUSSI, B. Constraint-Based LSP Setup using LDP, [draft-ietf-mpls-crldp-05.txt], Jan 2001.

[35] HEINANEN, Juha, RFC 1483, "Multiprotocol Encapsulation over ATM Adaptation Layer 5," 1993.

[36] GUICHARD, J., PEPELNJAK, I. MPLS and VPN Architectures: A Practical Guide to Understanding, Designing and Deploying MPLS and MPLS-Enabled VPNs Cisco Press, 2000.

[37] INTERNET ENGINEERING TASK FORCE (IETF). A Core MPLS IP VPN Architecture , RFC 2917. 2000.

[38] GUIMARÃES, A., LINS, R., G., OLIVEIRA, R. . Segurança em Redes Privadas Virtuais. Editora Brasport Livros e Multimídia. 2006.

[39] INTERNET ENGINEERING TASK FORCE (IETF). BGP/MPLS VPNs. RFC 2574. 1999.

[40] DAVIE, B. MPLS Technology and Applications. Morgan Kaufmann Publishers. 2000.

[41] INTERNET ENGINEERING TASK FORCE (IETF). An Architecture for Differentiated Services, RFC 2475. 1998.

[42] INTERNET ENGINEERING TASK FORCE (IETF). Resource ReServation Protocol (RSVP) – Version 1, Functional Specification, RFC 2205. 1997.

[43] INTERNET ENGINEERING TASK FORCE (IETF). The Use of RSVP with IETF Integrated Services, RFC 2215. 1997.

[44] INTERNET ENGINEERING TASK FORCE (IETF). General Characterization Parameters for Integrated Service Network Elements, RFC 2210. 1997.

[45] INTERNET ENGINEERING TASK FORCE (IETF). Specification of Guaranteed Quality of Service, RFC 2212. 1997.

[46] INTERNET ENGINEERING TASK FORCE (IETF). Specification of the Controlled-Load Network Element, RFC 2211. 1997.

[47] INTERNET ENGINEERING TASK FORCE (IETF). An Architecture for Differentiated Services, RFC 2475. 1998.

[48] INTERNET ENGINEERING TASK FORCE (IETF). An Expedited Forwarding PHB (Per-Hop Behavior), RFC 3246. 2002.

[49] INTERNET ENGINEERING TASK FORCE (IETF). Assured Forwarding PHB Group, RFC 2597. 1999.

[50] Traceroute. Microsoft homepage. Disponível em: < http://www.microsoft.com> Acesso em: 26 abr. 2009.

[51] WIRESHARK. Wireshark homepage. Disponível em: <http://www.wireshark.org/>. Acesso em: 27 dez. 2008.

[52] INTERNET ENGINEERING TASK FORCE (IETF). IAX: Inter-Asterisk eXchange Version 2, RFC 5456. 2009.

[53] INTERNET ENGINEERING TASK FORCE (IETF). Resource ReSerVation Protocol (RSVP), RFC 2205. 1997.

[54] INTERNET ENGINEERING TASK FORCE (IETF). BGP OSPF Interaction, RFC 1403. 1993.

[55] ALENCAR, M. S. de. Sistemas de Comunicações, 9ª Edição. Editora Érica, 2004.

[56] TOCCI, R.; WIDMER, N. Sistemas Digitais. 8ª Edição. Editora Pearson, 2003.

[57] Nyquist, H. Certain topics in telegraph transmission theory, vol. 47, Abril. 1928.

[58] FLANAGAN, J. L. SCHROEDER, M.; ATAL, B. et al. Speech Coding. IEEE Transactions on Communications, v. 27, n. 4, p. 710-737, Abr. 1979.

[59] JAYANT, N. S.; NOLL, P. Digital Coding of Waveforms, Prentice-Hall, Englewood Cliffs, New Jersey, 1984.

[60] SKYPE. Skype homepage. Disponível em: <http://www.skype.com>. Acesso em: 27 Abr. 2009.