RENATO LUIZ BIANCHINI

IMPLANTAÇÃO DE SISTEMA VOIP NA UNIVERSIDADE FEDERAL DE LAVRAS UTILIZANDO SOFTWARES LIVRES

Monografia de graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para a obtenção do título de Bacharel em Ciência da Computação

LAVRAS
MINAS GERAIS - BRASIL
2006

RENATO LUIZ BIANCHINI

IMPLANTAÇÃO DE SISTEMA VOIP NA UNIVERSIDADE FEDERAL DE LAVRAS UTILIZANDO SOFTWARES LIVRES

Monografia de graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para a obtenção do título de Bacharel em Ciência da Computação

Área de Concentração:
Redes de Computadores

Orientador:
Prof. Luiz Henrique Andrade Correia

LAVRAS
MINAS GERAIS - BRASIL
2006

Ficha Catalográfica preparada pela Divisão de Processos Técnico da Biblioteca Central da UFLA

Bianchini, Renato Luiz

Implantação de Sistema VoIP na Universidade Federal de Lavras Utilizando Softwares Livres / Renato Luiz Bianchini. Lavras – Minas Gerais, 2006. 80p : il.

Monografia de Graduação – Universidade Federal de Lavras Departamento de Ciência da Computação

1. Informática 2. Redes de Computadores 3. Voz sobre o Protocolo de Internet

RENATO LUIZ BIANCHINI

IMPLANTAÇÃO DE SISTEMA VOIP NA UNIVERSIDADE FEDERAL DE LAVRAS UTILIZANDO SOFTWARES LIVRES

Monografia de graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para a obtenção do título de Bacharel em Ciência da Computação

Aprovada em 27 de abril de 2006.

_____
Prof. Wilian Soares Lacerda

_____
Prof. Guilherme Bastos Alvarenga

_____
Prof. Luiz Henrique Correia Andrade
(Orientador)

LAVRAS
MINAS GERAIS - BRASIL

AGRADECIMENTOS

Primeiramente agradeço a Deus e meus familiares que fizeram de tudo para que eu pudesse estar concluindo o curso, e a todos que estiveram presentes em minha vida e que de alguma forma me apoiaram nesta caminhada. Deixo aos meus amigos, companheiros de república, professores, a todos do órgão cinufla que me ajudaram a desenvolver este projeto um grande abraço.

Sou muito grato a todos.

RESUMO

IMPLANTAÇÃO DE SISTEMA VOIP NA UNIVERSIDADE FEDERAL DE LAVRAS UTILIZANDO SOFTWARES LIVRES

Este trabalho apresenta a implantação de um sistema de voz sobre o protocolo de internet (VoIP) na Universidade Federal de Lavras (UFLA). A implantação desse sistema foi realizada em parceria com a Rede Nacional de Ensino e Pesquisa (RNP), dentro do projeto fone@RNP. Esse sistema de VoIP tem o objetivo de diminuir os custos da Universidade com as ligações telefônicas locais e interurbanas, pois com o sistema é possível realizar chamadas telefônicas utilizando a rede de dados já existente. O sistema de VoIP utiliza os softwares livres Asterisk, GnuGK, SER, LDAP, FreeRADIUS, PostgreSQL e softphones. Esses softwares funcionando em conjunto, controlam todo o serviço de VoIP, realizando chamadas com os protocolos SIP e H.323.

Palavras Chaves: VoIP, Asterisk, GnuGK, SER, RADIUS, LDAP, Softphone, SIP, H.323.

ABSTRACT

IMPLANTATION OF SYSTEM VOIP IN THE FEDERAL UNIVERSITY OF LAVRAS USING FREE SOFTWARES

The paper presents the implantation of a voice system on the protocol of internet (VoIP) in the Federal University of Lavras (UFLA). The implantation of this system was carried through in partnership with the National Net of Education and Pesquisa (RNP), inside of the project fone@RNP. This system of VoIP has the objective to diminish the costs of the University with the local and interurban telephonic calls, therefore with the system it is possible to carry through called telephonic using the existing net of data already. The system of free VoIP uses softwares Asterisk, GnuGK, SER, LDAP, FreeRADIUS, PostgreSQL and softphones. These softwares functioning in set, control the service of VoIP all, carrying through called with the protocol SIP and H.323.

Keywords: VoIP, Asterisk, GnuGK, SER, RADIUS, LDAP, Softphone, SIP, H.323.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

VoIP - Voice over Internet Protocol

IP - Internet Protocol

QoS - Quality of Service

PSTN - Public Switched Telephonic Network

TI - Tecnologia de Informação

PABX - Private Automatic Branch eXchange

PC - Personal Computer

TCP - Transmission Control Protocol

TCP/IP - Transmision Control Protocol/Internet Protocol

UDP - User Datagram Protocol

SMTP - Simple Mail Transfer Protocol

HTTP - Hypetext Transfer Protocol

LAN - Local Area Network

RTP – Real-Time Transport Protocol

RTPC – Real-Time Transport Control Protocol

SIP - Session Initiation Protocol

MMUSIC - Multiparty Multimedia Session Control

IETF - Internet Engineering Task Force

RFC - Request For Comments

UAC - User Agent Client

UAS - User Client Server

URL - Uniform Resource Locator

DNS - Domain Name Server

SDP - Session Description Protocol

ITU-T - Internation Telecom Union

RAS - Registration, Admission and Status

ISDN - Integrated Services Digital Network

MCU - Multipoint Control Unit

RDSI - Rede Integrada de Serviços Digitais

ASN.1- Abstract Syntax Notation 1

IMTC - International Multimedia Telecommunications Consortium

ASCII - Americam Standard Code for Information Interchange

PCM - Pulse Code Modulation

VPN – Virtual Private Network

PoP - Pontos de Presença

WDM - Wave Division Multiplex

WAN – Wide Area Network

LDAP - Lightweight Directory Access Protocol

ENUM - Eletronic Number Mapping

CAC - Connection Admission Control

DGK - Directory Gatekeeper

SER - SIP Express Router

CDR - Call Detail Recording

SMS - Short Message Service

RADIUS - Remote Authentication Dial In User Service

TDM - Time-division multiplexing

IVR - Interactive Voice Response

ACD - Automatic Call Delivery

DN - Distinguished Name

CN - Common Name

PHP - Personal Home Page

GNU - General Public Licence

SSL - Secure Sockets Layer

NAS - Network Acess Server

SQL – Structured Query Languange

SGBDR - Sistemas de Gerenciamento de Bancos de Dados Relacional

DBA - Data Base Administrator

CC – Country Code

NDC – National Destiny Code

SN – Subcriber Number

1. INTRODUÇÃO

O mercado de telecomunicações brasileiro, representado pelo sistema Telebrás até 1998, sofreu grandes mudanças com a privatização do seu sistema. A abertura do setor de telecomunicações trouxe novas e boas perspectivas para operadoras locais e internacionais. Essas operadoras formaram consórcios e compraram licenças, para exploração do STFC *(Serviço Telefônico Fixo Comutado)*, por prazo indeterminado, nas modalidades local e longa distância da ANATEL *(Agência Nacional de Telecomunicações)* [ANATEL, 1998], a agência reguladora das telecomunicações no Brasil, junto a isso veio uma melhoria no desempenho das conexões destinadas ao uso da internet.

Atualmente as redes de computadores não são usadas somente para o compartilhamento e transferência de arquivos, mas também para a prestação de serviços que antes eram suportados por outros meios de comunicação. Esses serviços, como voz, vídeo e dados exigem novos mecanismos para assegurar o seu funcionamento na rede de uma forma aceitável.

O futuro das telecomunicações está na convergência das redes de dados e das redes de voz. Quando se fala em convergência na área de telecomunicações, refere-se à redução para uma única conexão de rede, fornecendo todos os tipos de serviços, reduzindo gastos nas tarifas telefônicas e infra-estrutura, e na integração de novas aplicações.

As transmissões de voz baseadas na tecnologia IP *(Internet Protocol)* vêm se tornando uma alternativa cada vez mais viável à substituição dos modelos de telefonia tradicional, isso devido ao desenvolvimento de novas tecnologias que permitem dar suporte à transmissão de áudio em tempo real.

Segundo [NUNES, 2003] voz sobre IP é a designação usual do serviço de conversação telefônica suportado numa rede de dados baseada em IP, em geral abreviada para VoIP *(Voice over Internet Protocol)*. Diferentemente das chamadas telefônicas tradicionais, as chamadas realizadas na tecnologia de Voz sobre IP são realizadas através de comutação de pacotes, ou seja, o tráfego de voz é transmitido pelo protocolo IP dentro de uma rede corporativa.

Dessa forma, o uso de VoIP despontou como uma alternativa muito interessante para a implementação de uma série de novos serviços, que podem ser usados com o modelo atual das redes de dados, baseado em IP.

De acordo com [SHULZRINNE, 2000], basicamente três fatores contaram para o crescimento da tecnologia de VoIP: o desenvolvimento e padronização do protocolo que

permite QoS (*Quality of Service*) em redes IP, o desenvolvimento acelerado de métodos de compressão de voz e a explosão da Internet.

1.1. OBJETIVO DO TRABALHO

O objetivo deste trabalho é mostrar como foi implantada a tecnologia de VoIP (*Voice Over Internet Protocol*) no sistema atual de telecomunicações da UFLA (*Universidade Federal de Lavras*). Esse projeto foi desenvolvido em parceria com a RNP (*Rede Nacional de Ensino e Pesquisa*), e foi chamado de fone@RNP.

O CIN (*Centro de Informática*), órgão responsável em fornecer o serviço de Internet para a UFLA, teve a incumbência de implantar esta tecnologia no sistema atual de telecomunicações. Esse projeto foi de grande valor para a universidade, pois reduzirá os custos pago pelo serviço de ligações telefônicas, tanto interurbanas como locais, quando comparado com o modelo de telefonia pública tradicional, chamado de PSTN (*Public Switched Telephonic Network).*

1.2. VANTAGENS

As principais vantagens do uso da tecnologia de VoIP, quando comparado com o sistema de telefonia tradicional, são: a mobilidade, flexibilidade, tendência tecnológica em médio prazo e redução de custos.

- *Mobilidade:* com a tecnologia VoIP, é possível fazer chamadas telefônicas em qualquer lugar do mundo onde haja conectividade com a internet, de preferência banda larga. Permite estender o acesso telefônico a locais onde exista rede de dados, mas inexista a disponibilidade de ramais telefônicos, como por exemplo, em uma montanha.
- *Flexibilidade:* ter tratamento igual para chamadas locais e DDD, além de facilitar a adição de novos serviços e funcionalidades.
- *Tendência tecnológica em médio prazo:* com o grande número de estudos e pesquisas, em um período de curto a médio prazo, haverá um domínio ainda maior

sobre esta tecnologia, e paralelo a isso uma avançada formação de recursos humanos com capacidade de utilização da mesma.

- *Redução de custos:* por meio de uma rede de dados baseado em IP, é possível conversar com qualquer lugar do mundo com tarifas muito menores, além da manutenção da infra-estrutura ter o seu custo também reduzido.

1.3. MOTIVACÃO

Trabalhar com uma tecnologia que vem revolucionando o mundo de TI (*Tecnologia de Informação*), quando o termo VoIP é tratado, a ponto de alguns especialistas na área de telecomunicações, compararem o considerado crescimento do uso da tecnologia de VoIP, ao começo da Internet, no início dos anos 90. Além de poder desenvolver um projeto juntamente com a UFLA, e a RNP, um dos órgãos mais competentes e respeitados no Brasil na área de TI, e que irá abranger 77 instituições federais pertencentes ao MEC *(Ministério da Educação)* e MCT *(Ministério da Ciência e Tecnologia)*, foram duas grandes motivações para que este projeto de conclusão de curso fosse desenvolvido, com o apoio do CIN (*Centro de Informática)* da UFLA.

1.4. ORGANIZAÇÃO DO TRABALHO

O trabalho está organizado em sete capítulos.

No capítulo 2 são mostradas as características do trabalho. São apresentadas as características da tecnologia de VoIP, suas funcionalidades, uso atual e futuro de serviços que dependem desta tecnologia, e descrição de várias formas de como podemos usar os serviços que VoIP nos oferece.

A seguir no capítulo 3 são definidos os protocolos empregados em uma transmissão de áudio em tempo real (VoIP), como é feito a codificação do áudio analógico em áudio digital, parâmetros que influenciam numa qualidade de transmissão de áudio, chamado de QoS *(Quality of Service)* e a questão da segurança na transmissão de áudio.

No capítulo 4 será mostrado mais detalhadamente como foi à implantação dessa tecnologia dentro da UFLA, onde é descrito o ambiente de implantação do sistema, e como funciona o serviço atual de transmissão de dados na UFLA, a especificação do que é o

projeto fone@RNP, desde um histórico, até sua evolução nos dias atuais, junto com uma descrição detalhada do projeto fone@RNP.

Após a descrição do projeto, no capítulo 5, é mostrada a configuração do sistema, onde abrange toda a parte de instalação e configuração dos softwares, que funcionarão em conjunto, para prover serviços da tecnologia de VoIP. Neste capítulo também é mostrado o plano de numeração criado para as chamadas telefônicas usando o serviço de VoIP.

O capítulo 6 descreve os resultados que foram obtidos com está implantação do sistema, até o momento.

E por último, no capítulo 7 são mostradas as conclusões do trabalho e propostas para trabalhos futuros.

2. CARACTERÍSTICAS DA TECNOLOGIA

Neste capítulo será mostrada as funcionalidades da tecnologia de VoIP, o uso desta tecnologia nos dias atuais, e o futuro dentro do mundo de TI proporcionado pelo uso desta tecnologia. Também são descritas as funcionalidades e as características dos vários serviços que podem ser disponibilizados para locais onde o uso de VoIP já esteja implantado.

2.1. FUNCIONALIDADES

A tecnologia VoIP pode facilitar tarefas que podem ser mais difíceis de alcançar usando redes telefônicas tradicionais. O serviço de VoIP pode ser integrado com outros serviços que estão disponíveis na rede de dados IP, como conversação em vídeo, transferências de arquivos em uma conversação, conferência auditiva, dentre outros.

O tráfego da voz sobre pacotes IP pode ser estabelecido por meio de várias configurações entre os seus terminais. Esses terminais podem ser computadores ou mesmo telefones tradicionais. Neste caso, um conversor é necessário para converter os sinais de voz no formato que a rede de telefonia tradicional utiliza. As três formas de interligação que podem acontecer usando VoIP são: PC a PC; PC a telefone; telefone a telefone.

- *PC a PC:* a comunicação entre os dois usuários é feita através da rede IP, portanto a rede telefônica tradicional não é utilizada. A codificação de voz é realizada pelas placas multimídia dos computadores. Segundo [OLIVEIRA, 2001] existem vários softwares para este tipo de aplicação, podendo utilizar um protocolo proprietário ou padrão, permitindo, neste caso a interação de softwares de diferentes fabricantes. Na Figura 2.1 é mostrada uma comunicação PC a PC.

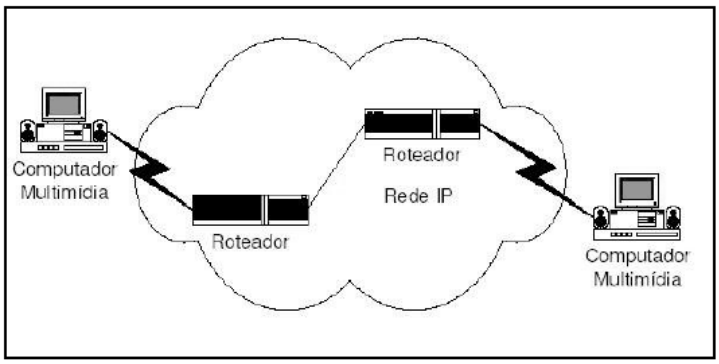


Figura 2.1 - VoIP entre dois PCs

- *PC a telefone:* no ambiente mostrado na Figura 2.2, há a presença de um gateway, equipamento que faz a interface entre a rede de telefonia tradicional e a rede VoIP. O *gateway* é responsável por converter voz (analógico-digital), sinalização e controle da rede telefônica tradicional para a rede IP, permitindo a comunicação entre os usuários dos dois ambientes: rede IP e telefonia tradicional. Os protocolos envolvidos com a tecnologia de VoIP terminam nesse equipamento sendo processados e decodificados. A partir daí, a telefonia tradicional fica responsável pelo tráfego da voz.

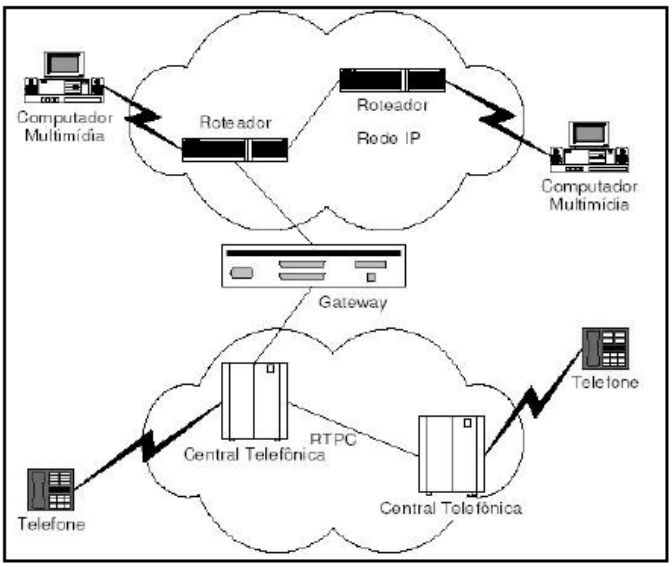


Figura 2.2 - VoIP entre um computador e um Telefone IP

- *Telefone a telefone:* o serviço de VoIP é utilizado para fazer ligação entre dois assinantes da telefonia tradicional, ver Figura 2.3. Sendo assim, a rede IP é utilizada como forma de transporte da voz, com o intuito de reduzir os custos envolvidos em uma ligação, já que a rede baseada na comutação de pacotes caracteriza-se por ser mais barata. As operadoras públicas podem ocasionalmente substituir parte de sua rede tradicional por uma rede IP.

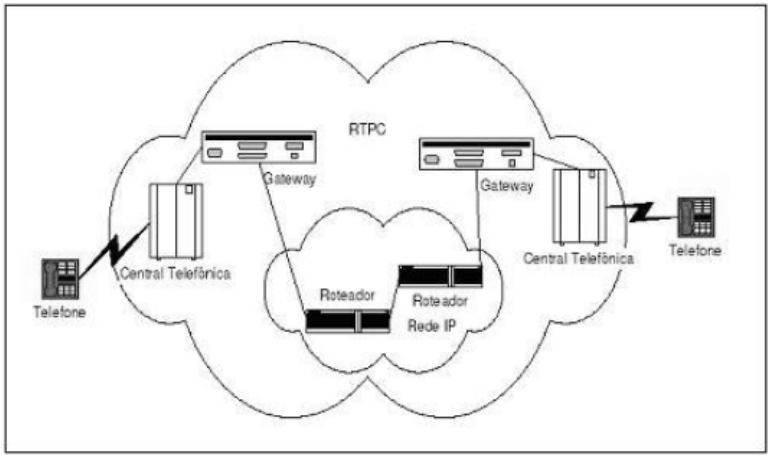


Figura 2.3 - VoIP entre dois Telefones

2.2. CENÁRIO ATUAL E FUTURO DA TECNOLOGIA VOIP

O serviço de VoIP foi desenvolvido ao longo da década de 90. O grande forte dessa tecnologia é a redução de custos que pode ser atingida por uma empresa de telecomunicações, universidades, órgãos públicos ou até mesmo companhias de outros ramos de atividade, que precisam interligar seus escritórios espalhados geograficamente.

As vantagens intrínsecas do VoIP como a qualidade, funcionalidade além do custo, ultrapassarão rapidamente os sistemas analógicos existentes PSTN (*Public Switched Telephonic Network*). Uma implementação de VoIP pode reduzir significativamente o custo das comunicações de voz em tempo real, tornando o uso dessas comunicações e os custos de administração mais previsíveis.

Nos países aonde a tecnologia de Voz sobre IP já chegou à larga escala, a tendência ainda caminha pela não-regulamentação. O grande receio dos reguladores é interferir no

desenvolvimento de uma tecnologia potencialmente vantajosa para os usuários e para o mercado, impondo regras cuja necessidade não se mostra clara e cujos benefícios são incertos.

Algumas das razões apontadas para regular, dizem respeito à padronização de serviços aos usuários e a proteção ao consumidor, que deseja ter acesso a um serviço similar ao telefone tradicional. Os usuários devem ser alertados de que VoIP necessita de energia elétrica para funcionar e os provedores da solução devem oferecer telefones de emergência.

O que se tem observado atualmente é uma generalização da procura resultante da introdução de soluções mais simples e mais baratas no mercado. Embora seja uma tecnologia consolidada, muitas operadoras de telecomunicações ainda encararam os serviços de internet como uma ameaça e não como uma oportunidade de negócio. A não consolidação de uma total qualidade de serviço (QoS) e o fato da internet não ser um meio de transmissão tão seguro como a telefonia tradicional, vem retardando a adoção da tecnologia.

Apesar de ter deixado de ser uma solução futurista e alcançado o patamar de uma alternativa tecnologicamente viável para a solução de comunicação de voz em tempo real, os clientes da área de TI no segmento empresarial não distinguem hoje as diversas abordagens do serviço de VoIP que são oferecidas pelo mercado. Sabem que existem soluções de VoIP que basta possuir um acesso internet, e que em geral, não oferecem quaisquer garantias de qualidade de serviço. Com isso acabam confundindo essas soluções, com soluções empresariais, que por serem aplicações de missão crítica asseguram disponibilidade e qualidade de serviço. A seguir são mostrados os serviços que a tecnologia de VoIP pode disponibilizar.

2.3. SERVIÇOS OFERECIDOS

Entre as muitas possibilidades de arquitetura e de serviços que podem ser agregados a sistemas de VoIP, temos:

- Integração de sistemas com tecnologia VoIP à rede pública de telefonia PSTN.

- Todas as funcionalidades de um PABX.
- Call Center e Voice Mail.
- Sistemas de auto-atendimento.
- Integração com outras aplicações.
- Sistemas de teleconferência.
- Sistemas de chamadas de longa distância.

Esses serviços tornam interessante o uso da tecnologia VoIP, pois por meio do uso de softwares livres, como servidores, banco de dados, softphones, que possibilitem ser configurados para disponibilizar serviços de VoIP, torna-se viável, em relação a custos, implantar soluções para telefonia e para outros serviços que utilizem as conexões de internet, principalmente quando comparado com o serviço de telefonia público tradicional.

2.4. CONCLUSÃO

Diferente de como muitos pensam, a tecnologia de VoIP não está relacionada apenas com transmissão de voz em tempo real, de PC para PC (MSN Messenger[1], Skype[2]), mas é possível que exista uma comunicação mista, tanto de um telefone comum para PC, ou vice-versa. Isso vem chamando muito a atenção dos usuários domésticos, que podem tornar viável esta tecnologia com um custo relativamente baixo.

Existe hoje uma grande preocupação que especialistas no ramo de telecomunicações vem enfrentando, que é a não regulamentação do serviço de VoIP. A um receio tanto das operadoras, quanto dos usuários de VoIP, pois todos temem que uma regulamentação poderia atrapalhar o avanço da tecnologia, e paralelo a isso os benefícios que essa tecnologia nos proporciona.

[1] MSN Messenger - software de comunicação em tempo real, por meio da internet. Disponível em http://messenger.msn.com.br/

[2] Skype - software de comunicação em tempo real, por meio da internet. Disponível em http://web.skype.com/home.pt.html

3. PROTOCOLOS DE COMUNICAÇÃO USADOS EM VOIP

Neste capítulo, são mostrados os principais protocolos usados para uma comunicação de áudio em tempo real, usando redes baseadas no protocolo IP. É descrita uma comparação entre o SIP e o H.323, protocolos principais do serviço de VoIP. São apresentados fatores que comprometem uma qualidade de serviço (QoS) na transmissão de pacotes de dados (áudio) via rede IP.

Uma comunicação de voz em tempo real é possível, desde que, um sinal de áudio analógico (voz humana) seja digitalizado. Essa transformação é feita por meio de algoritmos específicos e codecs, que serão mostrados neste capítulo, junto com fatores importantes de segurança para uma transmissão de áudio em tempo real.

3.1. RTP/ RTCP

Segundo [LOUREIRO, 1999] o uso singular da pilha de protocolo TCP/IP *(Transmission Control Protocol/Internet Protocol)* não atende o exigente tráfego do fluxo de voz, pois não é possível especificar e reservar a quantidade de largura de banda necessária. O uso do protocolo UDP *(User Datagram Protocol)* (não orientado à conexão), adequa-se melhor ao tráfego multimídia, onde o reenvio de dados não se faz necessário, pois pequenas perdas são suportadas pelo sistema ponto a ponto. Por outro lado, o UDP não permite configurar parâmetros de requisitos de largura de banda, podendo o serviço ser prejudicado por um congestionamento. Para integrar esses protocolos com tráfegos multimídia, alguns protocolos de camadas superiores foram propostos, dentre eles o RTP *(Real-Time Transport Protocol)* e o RTCP *(Real-Time Transport Control Protocol)*.

O RTP é um protocolo padrão para transporte de dados com características de tempo real, como o áudio usado na tecnologia de VoIP. Este protocolo atua sobre o protocolo UDP, não garantindo a entrega dos pacotes, nem os requisitos de largura de banda [LOUREIRO, 1999].

Como os fluxos RTP normalmente transportam tráfego de informações em tempo-real é preferível que seja usado com UDP na camada de transporte. Esse protocolo possibilita a especificação de requisitos de tempo, tanto na transmissão quanto na recepção dos pacotes.

Como o RTP não fornecia o monitoramento da comunicação e este era um dos principais requisitos das aplicações multimídias foi desenvolvido o RTCP. Este é um protocolo auxiliar de controle, cuja função é o monitoramento da comunicação, o RTCP implementa funções de controle na troca de informações entre as fontes e os destinos. Sendo assim, utilizado em conjunto com o RTP.

Durante a transmissão dos pacotes de dados, estes podem ser perdidos, ter atrasos variados ou serem entregues fora de ordem. Se um pacote é atrasado em demasia na rede, ele é perdido e técnicas de interpolação podem ser usadas para compensar essa variação de atraso na rede. Essa variação é chamado de *jitter*. Os protocolos RTP e o RTCP não evitam o *jitter* propriamente, mas fornecem parâmetros suficientes para que uma aplicação possa compensar os efeitos do *jitter* na rede, por meio do controle de *buffer* e seqüenciamento apropriados. Além disso, os protocolos fornecem mais informações a respeito da rede de maneira que medidas corretivas apropriadas possam ser adotadas (redundância, codecs, etc).

O projeto do RTP/RTCP permite que esses protocolos sejam usados acima de qualquer camada de protocolos de transporte. No entanto, o RTP e o RTCP são usados principalmente em cima do UDP, uma vez que o esquema de retransmissão do TCP não é adaptado para dados que precisam ser transportados com uma latência muito baixa, como no caso de comunicações interativas. Nesse caso, o RTP é tradicionalmente associado a uma porta UDP de número par e o RTCP à próxima porta UDP de número ímpar.

O SIP e o H.323 são os principais protocolos usados no serviço de VoIP. A seguir veremos o protocolo SIP.

3.2. SIP

O SIP *(Session Initiation Protocol)* é um protocolo de controle da camada de aplicação, que usa como protocolo de transporte o TCP *(Transmission Control Protocol)* ou UDP *(User Datagram Protocol)* (porta 5060). O uso do UDP é preferido, pois ele é

mais rápido, aceita *multicast* e alguns mecanismos de confiabilidade foram adicionados às suas características.

O SIP foi definido pelo grupo de trabalho MMUSIC *(Multiparty Multimedia Session Control)* da IETF (*Internet Engineering Task Force)* e está definido no RFC 3261 (Junho 2002). Dentre algumas funções que o SIP oferece estão, registro e localização de usuário e gerência de sessão.

Na Figura 3.1, é mostrada uma pilha de protocolos associados ao SIP.

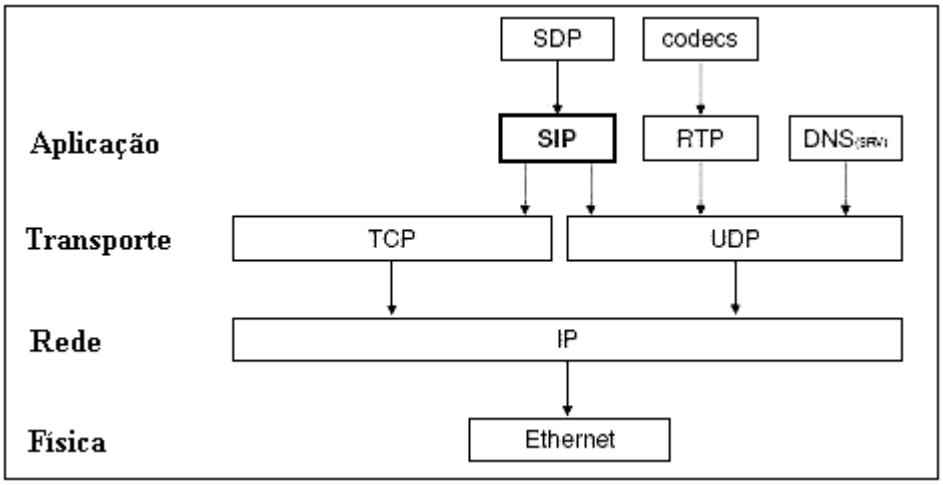


Figura 3.1 - Pilha de protocolos associado ao SIP

O SIP é usado para criar, modificar e terminar sessões (conjunto de fluxos de mídia, onde cada fluxo pode ser de áudio, vídeo, etc.) com um ou mais usuários (participantes). Estas sessões incluem conferências multimídia para internet e chamadas de telefone para internet. Participantes em uma sessão podem se comunicar via *multicast* (enviar uma única cópia da informação para um grupo de endereços) ou *unicast* (envio de uma cópia separada da mesma informação para cada pessoa), com uma combinação de ambos. A configuração da sessão, mudança ou término é independente do tipo de mídia ou aplicação que será usada na chamada. Uma chamada pode utilizar diferentes tipos de dados, incluindo áudio, vídeo e muitos outros formatos. Segundo [OLIVEIRA, 2001] cada requisição SIP consiste de um conjunto de campos de cabeçalho, que descrevem a chamada seguida por uma mensagem, que descreve uma sessão individual que está sendo realizada pela chamada.

Um outro resultado da arquitetura do SIP é a sua adequação natural como um ambiente de colaboração devido às suas habilidades de apresentar múltiplos tipos de dados e aplicações multimídia, com uma ou mais pessoas.

O SIP foi modelado depois de outros protocolos de Internet baseados em texto como o SMTP (*e-mail*) e o http (*páginas da web*). Foi desenvolvido para estabelecer, mudar e terminar chamadas de um ou mais usuários em uma rede IP de maneira totalmente independente do conteúdo de mídia da chamada. Como o HTTP, o SIP leva os controles da aplicação para o terminal, eliminando a necessidade de uma central de troca.

3.2.1. ARQUITETURA DO SIP

Podemos definir os principais componentes da arquitetura do SIP: o Agente do Usuário, Servidor Proxy, Servidor de Redirecionamento, Servidor de Registro.

- *Agente do Usuário SIP*: O agente do usuário é o terminal SIP ou o software de estação final. Ele pode ser um UAC (*User Agent Client*), que envia requisições SIP, ou um UAS (*User Client Server*), que recebe requisições SIP, interpreta e gera respostas aceitando, rejeitando ou redirecionando a requisição para outro UAS. O agente do usuário funciona como um cliente no pedido de inicialização de sessão e também age como um servidor quando responde a um pedido de sessão. Dessa forma, a arquitetura básica é cliente/servidor. O agente do usuário é “inteligente”, com isso ele armazena e gerencia situações de chamada e também faz chamadas com um endereço parecido com o de e-mail ou número de telefone, como por exemplo: SIP:user@proxy.ufla.br. Esse endereço é chamado de URL (*Uniform Resource Locator*) sendo usado para indicar o originador, o destino atual e o receptor final de uma solicitação SIP, e serve também para especificar endereços de redirecionamento. O agente do usuário pode aceitar e receber chamadas de outro agente do usuário sem requerer nenhum componente adicional do SIP.
- *Servidor Proxy SIP*: Um tipo de servidor intermediário do SIP é o Servidor Proxy SIP. O Servidor Proxy SIP passa requisições adiante do agente do usuário para o próximo servidor SIP e também retém informações com a finalidade de

contabilização, faturamento, autenticação e atualização. O servidor proxy SIP tem a capacidade de poder especificar, por exemplo, que seu telefone de desktop SIP, seu telefone celular SIP e suas aplicações de videoconferência de casa SIP possam receber uma chamada todas ao mesmo tempo, e quando o usuário atender de algum delas as outras param de tocar. Essa capacidade recebe o nome de *stateful*. O servidor SIP também pode receber requisições, acessar os serviços de localização e redirecionar as requisições. O servidor proxy SIP pode utilizar múltiplos métodos para tentar resolver o pedido de endereço de *host*, incluindo busca de DNS (*Domain Name Server*), busca em base de dados ou retransmitir o pedido para o próximo servidor proxy SIP. Na Figura 3.2 é mostrado como um servidor proxy SIP funciona.

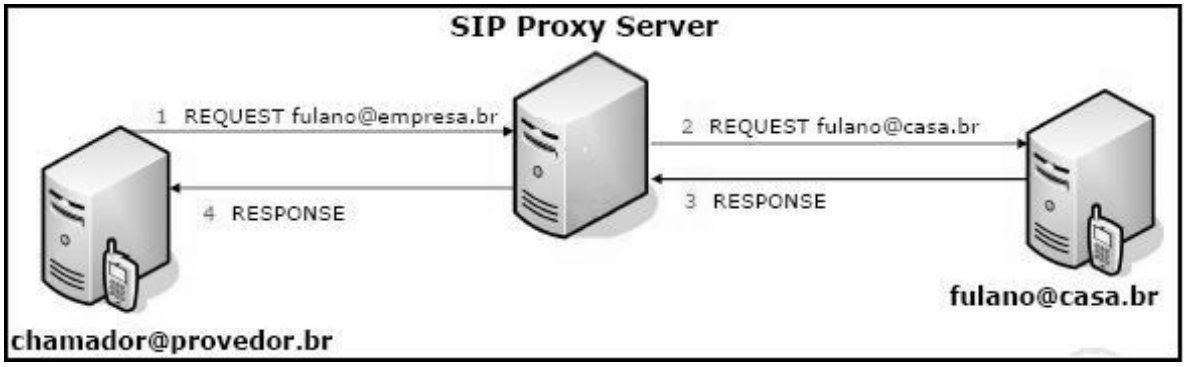


Figura 3.2 - Servidor Proxy
Fonte: RNP 2005 – Treinamento voip4all

- *Servidor de Redirecionamento SIP*: Um outro tipo de servidor intermediário do SIP é o Servidor de Redirecionamento SIP. A função do servidor de redirecionamento SIP é fornecer a resolução de nome e localização do usuário. O servidor de redirecionamento SIP responde ao pedido do agente do usuário fornecendo informações sobre o endereço do servidor para que o cliente possa contatar o endereço diretamente. Na Figura 3.3 é mostrado o funcionamento desse servidor.

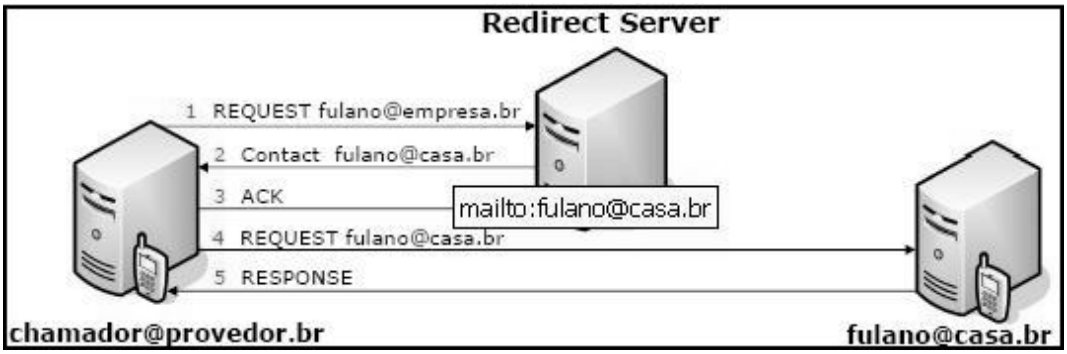


Figura 3.3 - Servidor de Redirecionamento
Fonte: RNP 2005 – Treinamento voip4all

- *Servidor de Registro*: O Servidor de Registro SIP fornece um serviço de informação de localidades. Quando acionado pelo servidor de redirecionamento, ou servidores proxy, ele recebe informações do agente do usuário e armazena essa informação de registro.

A arquitetura do SIP faz uso do SDP (*Session Description Protocol*) que é uma ferramenta de conferência *multicast* via IP desenvolvida para descrever sessões de áudio, vídeo e multimídia. A descrição da sessão pode ser usada para negociar uma aceitação de um conjunto de tipos de mídias compatíveis. O SDP também contém informações necessárias sobre a própria sessão como codecs envolvidos, endereços de transportes, portas. Mas pode conter outras informações sobre a sessão, como horário em que ela começou quem originou a sessão, assunto da sessão e URL contendo maiores informações sobre a sessão.

As sessões podem envolver múltiplos participantes, similar a uma chamada multiponto H.323. O protocolo H.323 é descrito na próxima seção.

3.3. H.323

O H.323 foi definido pelo ITU-T (*Internation Telecom Union*), um órgão que define padrões para redes de computadores e telecomunicações. O H.323 já teve várias versões, mas a versão que é usada atualmente e a versão que iremos tratar será o H.323 v5, Julho 2003.

Podem ser usados em um ambiente H.323 dispositivos físicos ou softwares, podendo ser executados em uma mesma plataforma.

O padrão H.323 provê uma arquitetura de dados multimídia, para redes baseadas no protocolo IP. O H.323 permite que produtos multimídia e aplicações de fabricantes diferentes possam interoperar de forma eficiente e que os usuários possam se comunicar sem preocupação com a velocidade da rede.

Segundo [DOMINGUES, 2000] a recomendação H.323 tem como uma de suas características a flexibilidade, pois pode ser aplicada tanto à voz quanto a vídeo conferência e multimídia. Aplicações H.323 estão se tornando populares no mercado corporativo por várias razões, dentre elas podemos citar.

- O H.323 define padrões de voz para uma infra-estrutura existente, além de ser projetada para compensar o efeito de latência em LANs *(Local Área Network)*, permitindo que os clientes possam usar aplicações de voz sem mudar a infra-estrutura de rede.
- O H.323 provê padrões de interoperabilidade entre LANs e outra redes.
- O fluxo e dados em redes pode ser administrado. Com o H.323, o gerente de rede pode restringir a quantidade de largura de banda disponível para conferências e voz. O suporte à comunicação *multicast* também reduz exigências de largura de banda.

O H.323 provê o uso de terminal computador/cliente onde está implementado o serviço de telefonia IP, atuando como terminal de voz, vídeo e dados, através de recursos multimídia. Esses são os clientes da LAN que fornecem comunicação em tempo real e nas duas direções. Todos os terminais H.323 têm que suportar o H.245, H.225, H.325, Q.931, RAS (*Registration, Admission and Status*). Abaixo estão descritas as características dos protocolos citados acima.

- *H.245* - é responsável pela descrição e controle de mídia, troca de capacidades entre terminais, e controle geral dos canais lógicos que transportam os fluxos de mídia. Um canal H.245 é único para cada chamada entre dois terminais, e é conhecido como canal lógico 0.
- *H.225* - define o formato de mensagens do H.323.

- *H.325* - protocolo responsável em dar confiabilidade às mensagens H.225 ou H.245 entre os pontos finais de uma comunicação na rede, para que o conteúdo de uma mensagem não fique exposto, usa-se chave criptografada.
- *Q.931*- especificação da interface entre rede e usuário dos protocolos ISDN (*Integrated Services Digital Network*), que é a digitalização da rede telefônica para tráfego simultâneo de voz, dados, imagens, aplicações e serviços multimídia e faz o controle básico de chamadas.
- *RAS* (*Registration, Admission and Status*) - é definido pelo padrão H.225, tem como função registrar, admitir, e criar status. Ele é usado entre o servidor e um terminal e entre servidores.

Os terminais H.323 podem incluir o protocolo T.120, para transferência de arquivos e fax, suporte para MCU (*Multipoint Control Unit*), que permite comunicação multiponto usando H.323. Um terminal H.323 pode comunicar com outro terminal, um *gateway* ou um MCU.

Um *gateway* H.323 é um elemento situado entre uma rede IP e outra rede de telecomunicações, como o sistema telefônico convencional, RDSI *(Rede Integrada de Serviços Digitais)*, ou rede de telefonia celular de forma a permitir a interoperabilidade entre as duas redes.

Um *gateway* H.323 é um ponto final da rede que fornece comunicação em tempo real nas duas direções entre terminais H.323 em uma rede IP comutada, ou para outro *gateway* H.323.

Os *gateways* são opcionais em uma LAN onde os terminais se comunicam diretamente, mas quando os terminais precisam se comunicar com um ponto final em outra rede, a comunicação se faz via *gateway* através dos protocolos H.245 e Q.931.

O *Gatekeeper* é o componente mais importante de um sistema H.323 e executa a função de gerente. Ele atua como ponto central para todas as chamadas dentro de sua zona (é a agregação do *Gatekeeper* e dos terminais registrados nela), e fornece serviços aos pontos finais registrados. O potencial do *Gatekeeper* é, entretanto, muito maior do que um simples gerente e um diretório de registro, sendo o local de fato para operacionalizar os serviços da rede H.323. Algumas das funcionalidades que os *Gatekeepers* fornecem são:

- *Tradução de endereços:* tradução de um endereço alias para um endereço de transporte. O endereço alias fornece um método alternativo de endereçamento de um ponto, e pode ser um endereço de e-mail, um número telefônico ou algo similar. Isto é feito usando-se uma tabela de tradução que pode ser atualizada através de mensagens de registro.
- *Controle de admissão:* o *Gatekeeper* pode permitir ou negar acesso baseado em autorização de chamada, endereço de fonte e destino, etc.
- *Sinalização de chamada:* o *Gatekeeper* controla o processo de sinalização entre dois pontos finais que querem se conectar.
- *Autorização de chamada:* o *Gatekeeper* pode rejeitar chamadas de um terminal devido a falhas de autorização através do uso de sinalização H.225. As razões para rejeição poderiam ser acessos restritos durante alguns períodos de tempos ou acesso de certos terminais ou *gateways.*
- *Gerenciamento de largura de faixa:* controle do número de terminais que podem acessar simultaneamente a rede. Através do uso da sinalização H.225, o *Gatekeeper* pode rejeitar chamadas de um terminal devido à limitação de largura de faixa.
- *Gerenciamento da chamada:* o *Gatekeeper* pode manter uma lista de chamadas H.323 em andamento. Essa informação pode ser necessária para indicar que um terminal chamado está ocupado, e fornecer informações para a função de gerenciamento de largura de faixa.

A seguir na próxima seção são mostradas comparações entre o protocolo SIP e H.323.

3.4. COMPARAÇÕES ENTRE OS PROTOCOLOS SIP E H.323

O SIP e o H.323 são ambos protocolos padrões da tecnologia de VoIP. O uso do H.323 tem sido motivado pela sua interoperabilidade com a PSTN (*Public Switched Telephone Network*) e disponibilidade de sistemas/aplicações *desktop* e salas de videoconferência de preço acessível e confiável. Por outro lado o SIP é um protocolo esenvolvido especificamente para Internet e promete grande escalabilidade e flexibilidade.

Um recurso que o SIP utiliza e pode ser considerado como uma vantagem em relação ao H.323 é o uso de URLs como um identificador. A diferença da URL SIP, para um e-mail H.323 é que a URL SIP é flexível, podendo redirecionar uma chamada para servidores diferentes, ao contrário do H.323 que só considera uso do protocolo H.323. Essa flexibilidade facilita a integração de novas aplicações multimídia.

O SIP também possui um campo adicional de priorização de chamadas. Esse campo é adicional, pois alguns países têm exigências legais para priorizar algumas linhas telefônicas. Já no H.323 esse recurso foi ignorado. Além de possuir codificação de texto, a função deste recurso é detectar problemas de interoperabilidade dentro da rede. Isso é considerado como uma vantagem.

O padrão H.323 utiliza canais lógicos para separar os dois tipos de mídias que podem ser enviados ou recebidos em uma chamada. Pelos canais lógicos é definido a capacidade e o tipo de mídia que serão utilizados durante a chamada. O SIP não possui esse tipo de recurso. Ele apenas indica o que os codificadores podem receber.

O padrão H.323 possui ótimos recursos para controle de conferências. Já o SIP não foi projetado para gerenciar esse tipo de controle. Conseqüentemente, muito dos recursos necessários para fazer uma conferência controlada ainda não existem.

Segundo [HERSENT, 2002] as mensagens H.323 trabalham com codificação binária, todas as mensagens são codificadas de acordo com Q.931 para o subconjunto de mensagens H.225. Todas as outras mensagens são codificadas usando-se regras de codificação de pacotes PER *(Packet Encoding Rules)* e ASN.1 *(Abstract Syntax Notation 1)*. Isso gera certa complexidade no H.323, pois misturam dois métodos de codificação com regras totalmente diferentes gerando grandes esforços de programação por parte das empresas.

As organizações de padrões já estão trabalhando com uma interoperabilidade SIP-H.323, prometendo a possibilidade de um período de transição razoável entre as tecnologias H.323 e SIP. Duas organizações que estão especialmente interessadas nesse tópico são a IMTC (*International Multimedia Telecommunications Consortium*), uma corporação sem fins lucrativos com mais de 100 organizações pelo mundo, e também a ETSI (*European Telecommunications Standards Institute*). A Open H.323 Organization já lançou um gateway de trabalho H.323 para SIP.

Na Tabela 3.1 são mostradas diferenças entre os dois protocolos:

Tabela 3.1 – Diferenças entre protocolo SIP e H.323

SIP	H.323
- requisições e respostas baseadas em texto puro (ASCII)	- codificação binária baseada em ASN.1
- protocolo SDP (descreve os tipos de mídia e endereços de transporte da mídia)	- sub-protocolos: H.245, H.225 (Q.931, RAS, RTP/RTCP)
- servidores com diferentes comportamentos: registrar, proxy, redirecionar	- servidor único Gatekeeper H.323
- não foi projetado para gerenciar controle de conferências	- possui ótimos recursos para controle de conferências
- o uso de URLs facilita o redirecionamento de uma chamada para servidores diferentes; essa flexibilidade facilita a integração de novas aplicações multimídia	- uso de e-mail, que só considera uso do protocolo H.323
- ao enviar uma mensagem apenas indica o que os codificadores podem receber	- utiliza canais lógicos para separar dois tipos de mídias que podem ser enviados ou recebidos em uma chamada; pelos canais lógicos é definido a capacidade e o tipo de mídia que serão utilizados durante a chamada

Ter uma qualidade de serviço quando se usa a tecnologia VoIP é um fator necessário para que haja uma conversação de boa qualidade. Fatores que comprometem essa qualidade de serviço e meios para se eliminar esse fatores negativos são mostrados na próxima seção.

3.5. QUALIDADE DE SERVIÇO (QoS)

Existem algumas dificuldades para garantir qualidade na transmissão de voz em redes IP, pois estas redes utilizam comutação de pacotes para a transmissão dos dados, diferente das redes telefônicas que utilizam comutação de circuitos, ou seja, são redes com tecnologias totalmente diferentes. Nas redes IP não há variação dos tipos de dados, independentes de serem pacotes de voz ou vídeo, são tratados de forma igual. Isso causa uma certa dificuldade na transmissão dessas aplicações. Dentre os fatores que causam impacto na qualidade de serviço temos atraso, perda de pacotes, variação de atraso e banda.

Segundo [HERSENT, 2002] o conceito de qualidade de serviço QoS *(Quality of Service)* foi ignorado no projeto inicial do protocolo IPv4, pois inicialmente ele foi

projetado somente para suportar o tráfego de dados e não aplicações multimídia como voz e vídeo. Então a qualidade de serviço que foi considerada era garantir a integridade dos dados trafegados. Atualmente, devido ao grande avanço tecnológico as redes IPv4, essas já suportam o tráfego de aplicações em tempo real. Essas aplicações exigem um controle e gerenciamento da variação do atraso (*jitter)*. O controle do *jitter* é necessário e de extrema importância em aplicações desse tipo, pois sem esse controle não se pode garantir uma boa qualidade na entrega dos pacotes de voz e vídeo.

Os atrasos são fatores críticos para a transmissão de voz, e podem ser agrupados em dois tipos diferentes: atrasos fixos e atrasos variáveis. Os atrasos fixos causam desconforto na conversação, já os atrasos variáveis atrapalham a cadência na transmissão da voz.

Os atrasos fixos são ocasionados por diversos fatores diferentes. Esses fatores são definidos em: compressão, transmissão, buffer, descompressão.

- *Compressão* - tempo gasto na codificação da voz em pacotes.
- *Transmissão* - devido às limitações de velocidade de transmissão da rede
- *Buffer* - método de armazenar pacotes da mensagem, até que outros pacotes atrasados cheguem e seu unam, para que a mensagem não fique picada.
- *Descompressão* - tempo gasto na decodificação da voz em pacotes.

A variação do atraso não é a única preocupação para garantir QoS, a taxa de perda de pacotes é um parâmetro que deve ser levado em consideração. Essa perda acontece quando existe um congestionamento na rota dos dados causando uma sobrecarga no buffer do roteador. Apesar do protocolo TCP *(Transmission Control Protocol)* tentar garantir a recuperação contra congestionamento e perdas, uma garantia maior só é obtida através de uma banda maior disponível, bem como uma melhoria no tempo de processamento.

Os problemas relacionados ao congestionamento e atrasos podem ser solucionados utilizando ferramentas que gerenciam o controle de congestionamento, e realizam atribuição de prioridades nas transmissões. Existem algoritmos de priorização que podem limitar dinamicamente o tamanho dos quadros de dados. Caso haja a existência de pacotes de voz, pode conseguir um enfileiramento de pacotes de dados à frente de qualquer pacote

de voz. Com isso, eles conseguem diminuir os tempos de enfileiramento dos pacotes de voz, garantindo um bom desempenho por parte da transmissão de dados.

Segundo [HERSENT, 2002] a utilização de *buffers* também é um recurso utilizado para gerenciar o controle e a variação de atrasos. O *buffer* armazena dados que chegam mais rápido que o tempo necessário, assim conseguem manter a entrega dos dados em uma taxa constante sem variação. O *buffer* só é usado quando a rede sofre uma queda no tráfego. Ainda existem outros problemas relacionados à garantia de QoS em aplicações multimídias, como a escassez de banda e o eco.

Em uma conversação ocorrem em determinados momentos intervalos de silêncio, esses intervalos podem gerar um desperdício de recursos ao alocar uma possível banda fixa. A solução para este problema de limitação de banda é melhorar o seu desempenho e a utilização de algoritmos de compressão de voz e supressão de silêncio.

Com a compressão, consegue-se obter áudio de boa qualidade com uma banda menor. A codificação PCM (Pulse Code Modulation) é otimizada para a fala, mas ocupa 64Kbps de banda. Outros algoritmos chegam a utilizar uma banda de 16 a 8Kbps. Há também padrões do ITU-T que conseguem taxas mais baixas como os codecs G.729 e G.723 (8Kbps) e o G.723.1, que atinge taxas de 5.3 a 6Kbps, fazendo parte do padrão H.323. Os algoritmos de compressão empregam a supressão de silêncio, eliminando as pausas, que ocupam até 40% da conversação telefônica, e ocupando a banda por outros pacotes quando intervalos de silêncio ocorrem. Entretanto, há que se levar em consideração que com a compressão, os pacotes de voz aumentam a sensibilidade por perdas, donde vemos a importância dos mecanismos que evitam tais características.

Como é feita uma digitalização de um sinal de audio analógico para um sinal de audio digital é mostrado na proxima seção

3.6. DIGITALIZAÇÃO E CODIFICAÇÕ DE ÁUDIO

Segundo [TANENBAUM, 2003] o ouvido humano é surpreendentemente sensível a variações de som que duram milésimos de segundo, ao contrário do olho que não percebe mudanças no nível da luz que durem menos de alguns milésimos. Isso significa que, em uma transmissão multimídia, o atraso afeta mais a qualidade do som percebido do que a qualidade da imagem percebida. Essa condição é o principal fator de limitação da

tecnologia de Telefonia IP, pois a rede IP introduz perdas de pacotes, atraso e *jitter* que degradam sensivelmente a qualidade de voz.

Para que a voz possa trafegar na rede IP ela precisa ser digitalizada, necessitando-se, portanto, de uma conversão analógico-digital (A/D). O processo de conversão A/D pode ser dividido em três fases: amostragem, quantização, compressão.

- *Amostragem* - trata-se do processo de medir valores instantâneos de um sinal analógico em intervalos regulares. O intervalo entre as amostras é determinado pôr um pulso de relógio e a freqüência desse relógio é chamada de Taxa de Amostragem. De acordo com o teorema de Nyquist, para reproduzir fielmente o sinal, a taxa ou freqüência de amostragem deve ser de, pelo menos, o dobro da maior freqüência contida no sinal a ser amostrado [OLIVEIRA, 2000]. Um sinal analógico é convertido em um sinal digital através da captura de uma série de amostras da fonte analógica. A união dessas amostras forma o equivalente digital de uma onda sonora.
- *Quantização* - o sinal amostrado é convertido para valores discretos na quantização, ou seja, é considerada a amplitude deste sinal apenas em níveis discretos. Essa infinidade de valores obtidos do sinal analógico passam a ser representados por uma quantidade finita de bits, para obter um sinal digital. Na Figura 3.4 é mostrado o processo de quantização de uma onda de áudio em valores discretos.

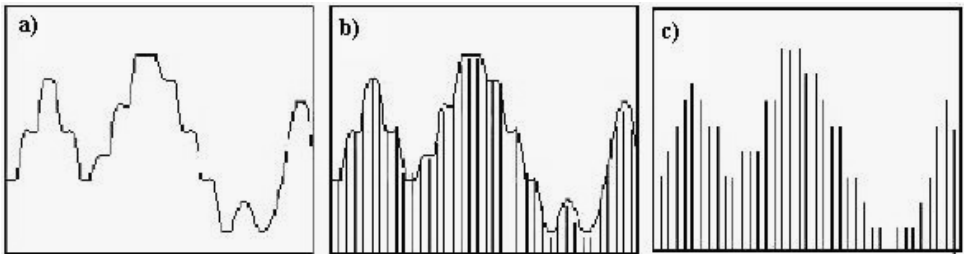


Figura 3.4 – (a) Onda de áudio; (b) Amostragem; (c) Quantização

- *Compressão* - para reduzir a banda do canal necessária para a transmissão de voz digitalizada, são usadas técnicas de compressão de voz que devem acontecer em tempo real para possibilitar a comunicação e a interação. Segundo [OLIVEIRA, 2000] a compressão de sinais é baseada em técnicas de processamento que retiram informações redundantes, imprevisíveis e inúteis.

Os dispositivos responsáveis pela codificação da voz são conhecidos como *voice codecs*, ou simplesmente *vocoders*. Os *vocoders* analisam o conteúdo espectral do sinal da fala e identificam os parâmetros que são entendidos pelo ouvido. Estes parâmetros são transmitidos e usados para sintetizar o padrão de voz. A forma de onda resultante pode não ser semelhante a original, mas as diferenças não são percebidas ou, ainda que o sejam, são consideradas aceitáveis para a aplicação.

Segundo [GUIMARÃES, 1999] os algoritmos de compressão de voz possibilitam uma alta qualidade de voz fazendo um uso eficiente da largura de banda do canal de comunicação. A compressão pode acontecer com ou sem perda de informação. A escolha depende da degradação que se admite para o sinal e do fator de compressão que se deseja atingir. O PCM (*Pulse Code Modulation)* é um padrão de codificação da voz e consume 64Kbps por canal. Existem outros algoritmos de compressão de voz que tentam modelar o PCM mais eficientemente utilizando menos bits. Na Tabela 3.2 são demonstrados os principais *codecs* e suas aplicações segundo recomendações do ITU-T.

Tabela 3.2 - Codecs de Áudio

Recomendação (Ano de Aprovação)	Algoritmo	Taxa de Bit (Kbit/s)	Largura de Banda (Hz)	Delay entre Pontos (ms)	Aplicação
G.711(1972)	PCM	56, 64	300 - 3,4k	< 1	Telefonia GSTN, videoconferência H.320/H.323
G.722(1988)	Sub-ADPCM	48, 56, 64	50 - 7k	< 2	Telefonia e Videoconferência ISDN
G.723.1(1996)	ACELP - 5,3/MP-MLQ - 6,3	5.3, 6.3	300 - 3,4k	67-97	Videotelefonia GSTN,Telefonia H.323,VoIP (básico)
G.728(1992)	LD-CELP	16	300 - 3,4k	< 2	GSTN, Videoconferência H.320
G.729(1992)	CS-ACELP	8	300 - 3,4k	25-35	Telefonia GSTN, Modem GSTN, Videotelefonia H.324 GSTN
G.729 - A(1996)	CS-ACELP	8	300 - 3,4k	25-35	Modem GSTN, Videotelefonia H.324 GSTN

Fonte: Internation Telecom Union - ITU-T

Utilizar o serviço de VoIP com segurança é um fator importante para uma transmissão de áudio em tempo real. Características de como segurança em VoIP é tratada são descritas na próxima seção.

3.7. SEGURANÇA

A comunicação de voz por meio de transmissão de dados por redes de computadores pode sofrer de falta de privacidade. Trata-se de um novo tipo de monitoração, diferente do tradicional grampo. Tendo acesso a um segmento de rede por onde o tráfego de voz é transmitido, seria possível capturar os pacotes e praticamente "gravar" a conversação realizada. Se pensarmos que a voz vai passar a utilizar a rede de dados e que estas redes são tradicionalmente menos seguras que as de voz, podemos antever algumas desvantagens de curto prazo que o tempo e a evolução tecnológica tenderão a resolver. Se a informação não for criptografada, existem riscos de segurança e confidencialidade que normalmente não existem em sistemas tradicionais.

É importante dizer que mecanismos existentes no serviço de VoIP, por si só não garantem a confidencialidade das informações. Alguns usuários possuem a falsa sensação de que teriam uma comunicação segura pelo simples fato de utilizar um telefone IP. Não é verdade. Já existem programas disponíveis livremente na Internet que capturam e remontam chamadas telefônicas realizadas por VoIP, demonstrando apenas a "ponta do iceberg" em produtos e mecanismos existentes. Esse quadro muda sensivelmente com a adoção de criptografia. A voz, neste caso, é tratada como um pacote de dados que pode ser criptografada, utilizando tecnologias de alto nível de segurança.

Projetar bem é fundamental. Usar tecnologias de autenticação forte, *firewall*, VPN *(Virtual Private Network)*, antivírus, prevenção e detecção de intrusos interna e externa e filtragem de conteúdo devem ser utilizadas para proteção da integridade das informações. Um grampo IP, em uma rede sem segurança, é bastante fácil de ser feito, podendo qualquer *sniffer* (pessoas que invadem computadores via internet), por exemplo, capturar e gravar pacotes de voz. Mas uma vez implementando um sistema de segurança eficiente em IP, este com certeza será bastante seguro, mais seguro até do que a telefonia tradicional.

É necessário um conjunto de cuidados para que uma solução de Telefonia IP seja adotada com sucesso, como a infra-estrutura, que precisa ser previamente preparada com requisitos fundamentais como a Qualidade de Serviço, de forma a ser dado tratamento preferencial ao tráfego de voz versus o tráfego de dados. Também o acompanhamento da solução ao nível da segurança, com as atualizações do sistema operacional e versões de

software das aplicações, juntamente com um antivírus, são fatores essenciais ao bom funcionamento da solução.

Muito ainda estar por vir e o cenário mundial está em constante mudança no que diz respeito a voz sobre IP. O importante é que profissionais e usuários de tecnologia precisam ficar atentos aos impactos que podem ser causados em nossa vida profissional e pessoal quando é utilizado VoIP.

3.8. CONCLUSÃO

Podemos considerar que não só os protocolos de transporte (TCP /UDP) e os protocolos específicos da tecnologia de VoIP (SIP/H.323). São essenciais para uma transmissão de áudio em tempo real. Temos outros parâmetros a serem considerados para que uma transmissão de áudio seja de boa qualidade. Os algoritmos, juntamente com os codecs de áudio, são responsáveis pela digitalização do áudio analógico, e desta forma desempenham um papel importante no processo de transmissão de áudio.

O QoS *(Qualidade de Serviço)* também tem um papel importante, pois é um dos maiores desafios que especialistas na área de telecomunicações tem enfrentado, para se adquirir uma comunicação com boa qualidade como a telefonia tradicional. Junto a isso, as incertezas em relação a segurança, que ainda não é um fator que agrada aos usuários desta tecnologia, principalmente quando também é comparada com a telefonia tradicional.

4. DESCRIÇÃO DO AMBIENTE UFLA E PROJETO FONE@RNP

Neste capítulo é apresentada a configuração do ambiente da rede UFLA, desde a sua ligação no PoP-UFMG, até a distribuição dos circuitos pelo campus da Universidade.

É apresentado um histórico dos projetos do GT-VoIP, por meio de uma descrição de como evoluiu os projetos destinados ao estudo do serviço de VoIP, criados pela RNP, até o projeto atual fone@RNP implantado na rede UFLA.

4.1. DESCRIÇÃO DO AMBIENTE UFLA

O backbone, parte de uma rede de comunicações projetada para suportar tráfegos elevados, em geral, emprega meios de transmissão mais rápidos e distâncias mais longas. A rede RNP foi projetada para atender a certos requisitos técnicos, garantindo a largura de banda necessária ao tráfego internet e ao uso de serviços e aplicações avançadas.

Há no Brasil 27 PoPs (*Point of Presence*) instalados em todas as capitais dos estados, interligando cerca de 250 instituições de ensino e pesquisa e algumas iniciativas de redes regionais, principalmente redes estaduais e redes metropolitanas de ensino e pesquisa.

Em 2005, a capacidade de comunicação entre os PoPs começou a ser ampliada com o uso de tecnologia óptica WDM (*Wave Division Multiplex*), o que elevou a capacidades da rede RNP a 10Gbps.

A conexão que é destinada a UFLA, via RNP, tem capacidade de transmissão de 9Mbps. A concessionária de telecomunicações responsável pela chegada do circuito de dados é a Embratel (Empresa Brasileira de Telecomunicações). O circuito de dados usa acesso sem fio através de uma transmissão via rádio. O protocolo de comunicação utilizado na rede da Embratel é o Frame Relay. O circuito de acesso é conectado a sala de equipamentos do CIN, localizado no prédio da Reitoria e, a partir daí, são interligados por meio de cabeamento óptico (fibra óptica) nos prédios da Universidade. Dentre eles, departamentos, biblioteca, banco, alojamentos estudantis, etc. O Campus da UFLA possui

uma área física de 600 ha. com uma área construída de 158.359 m². Atualmente dispõe de 16 departamentos, além de laboratórios e prédios administrativos.

Esses prédios são interconectados por fibras ópticas (monomodo e multimodo), como mostra a Figura 4.1.

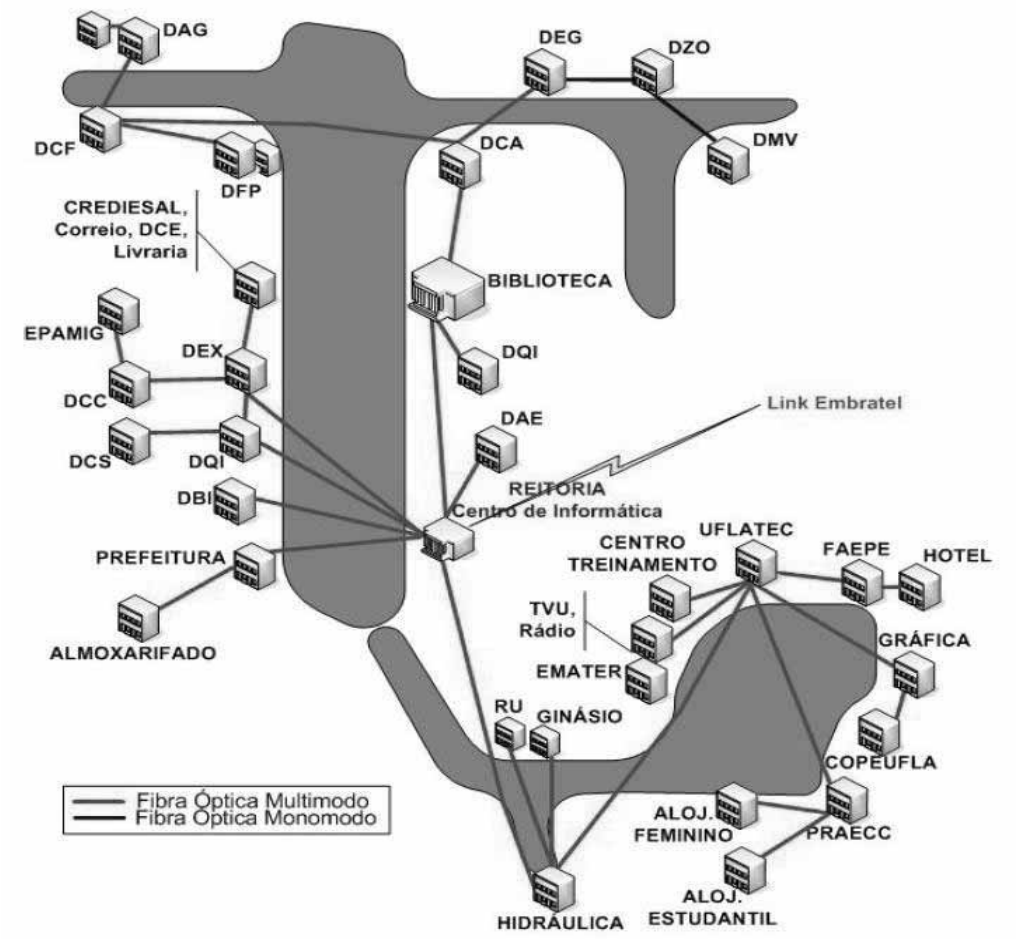


Figura 4.1 – Topologia Rede UFLA[1]

Cada prédio é interconectado ao CIN por cabeamento óptico, e por meio de equipamentos específicos os circuitos de acesso são distribuídos em cada prédio via cabeamento metálico, tornando possível o acesso à internet de todos os computadores que compõem a rede do prédio.

[1] - Fonte: FRINHANI, R. M. D., Projeto de Reestruturação do Gerenciamento e Otimização da Rede Computacional da Universidade Federal de Lavras. 2004.

Toda a estrutura física do campus e os equipamentos utilizados para a transmissão de dados da rede UFLA, acima citados, são utilizados para disponibilizar o serviço de VoIP por toda Universidade.

Na próxima seção é descrito um histórico da evolução do serviço de VoIP, disponibilizado pela RNP.

4.2. HISTÓRICO VOIP - RNP

Nesta seção é apresentado a evolução do serviço de VoIP, por meio do projeto GT-VoIP da RNP. O projeto GT-VoIP evolui durante quase quatro anos de sua criação, e atualmente conta com um alto número de instituições participantes.

4.2.1. GT-VOIP

O projeto GT-VoIP (Grupo de Trabalho – Voz sobre Protocolo de Internet) foi criado em Maio de 2002, porém com primeiras ações em Setembro de 2002, pela RNP e teve como objetivo utilizar o backbone RNP2. Esse projeto foi financiado pelos Ministérios da Ciência e Tecnologia e da Educação e foi concebido para atender com excelência de qualidade à comunidade de ensino e pesquisa brasileira, interconectando instituições e redes regionais em nível nacional e oferecendo circuitos internacionais próprios.

Na primeira fase do projeto GT-VoIP possibilitou capacitar instituições para disseminação do serviço de VoIP através de um piloto H.323 no backbone RNP2. Este piloto teve como participantes instituições federais de ensino superior e unidades de pesquisa do MCT.

Como prioridades do projeto, havia o desenvolvimento de ferramentas para medição ativa e passiva da qualidade de voz, implantar ambiente para gerência e operação do serviço, implantar mecanismos de autenticação e registro seguro de usuários, bem como suporte à operação com Firewall e lançar as bases do serviço.

O GT-VoIP utilizava apenas o protocolo H.323. O cadastro e autenticação de telefones virtuais eram feitos apenas para usuários das instituições, e podiam ser feitos de duas formas: com dois parâmetros, nome do usuário e IP, ou três parâmetros, nome do

usuário, senha e um numero virtual ou alias (identificação alternativa para um objeto, tal como um arquivo ou um conjunto de dados).

Foram criados ambientes integrados de gerência e operação, responsáveis em gerar estatísticas, localizar usuários on-line e de configuração do *Gatekeeper* (ver seção 3.3). Junto a isso foi criado ferramentas de monitoração ativa e passiva, e recomendações de arquiteturas para suporte ao serviço de VoIP.

Ambientes de gerência e operação geram estatísticas de uso do serviço, intensidade de tráfego, duração das chamadas, motivo de término, qualidade das chamadas dentre outras funções. Ferramentas de monitoração ativa geram, coletam e monitoram a qualidade das ligações VoIP, para medições repetitivas a vários pontos.

4.2.2. GT-VOIP AVANÇADO

O projeto GT-VoIP Avançado (Grupo de Trabalho – Voz sobre Protocolo de Internet Avançado) teve seu início oficial, em Julho de 2004, e em conjunto com o serviço fone@RNP, lançado em Maio de 2004, conseguiram uma evolução do primeiro projeto GT-VoIP.

As instituições inscritas para participar dessa segunda fase do projeto GT-VoIP, são instituições federais de ensino superior, unidades de pesquisa do MCT e alguns Cefets.

O objetivo principal do projeto GT-VoIP nesta segunda fase é a implantação escalável do serviço fone@RNP, com suporte a SIP e H.323. Houve um aprimoramento dos ambientes de gerência e medição/monitoração de tráfego, testes de novas formas de localização de usuários com uso de DNS e uso de diretórios nos procedimentos de autenticação e autorização de usuários.

Algumas das metas principais é a de obter um aprimoramento das ferramentas desenvolvidas anteriormente no projeto GT-VoIP. Por exemplo, aprimoramento do processo de autorização e autenticação com uso de LDAP (*Lightweight Directory Access Protocol*). Família de protocolos para acesso a informações de diretórios, configuração automática de clientes, implementação de controle de admissão de chamadas mais complexo, experimentação com ENUM (*Eletronic Number Mapping*), suporte a SIP e operação de gateway H.323/SIP.

A instalação do software utilizado para realizar chamadas de um cliente H.323 foi facilitada. Agora o usuário recebe arquivo .exe, que sendo executado instala automaticamente o cliente H.323 (OpenPhone).

Foram criados outros métodos de autenticação que não sejam conta/senha, como certificados digitais armazenados no LDAP. O padrão para vídeos em videoconferência H.350, por exemplo, cria no LDAP uma descrição das capacidades multimídia do cliente, ou seja, se o Gatekeeper e o cliente suportam H.350, uma configuração automática pode ser feita a cada autenticação do cliente. Isso gera vantagens, pois pode haver uma variação de configuração dinamicamente como escolher Gatekeeper com menor carga para registro, usar diferentes codecs em função do horário e carga da rede, e facilitar gerência alterando parâmetros automaticamente sem participação do usuário, e melhorar segurança e desempenho, forçando uso de uma mesma identificação entre clientes.

O uso de admissão de chamadas com o CAC (*Connection Admission Control*). O intuito do CAC é determinar se a chamada será ou não aceita, esse controle possibilita que o Gatekeeper verifique o número máximo de chamadas já autorizadas.

A integração do Gatekeeper ao DNS (*Domain Name Server)* faz com que a localização de usuários seja feito diretamente pelo Gatekeeper via DNS, tornando o processo de localização semelhante com a forma que o SIP opera para localização de usuários. Foi acrescentado um método para se gerar CDR (*Call Detail Recording*), que equivale aos registros de bilhetagem existentes em uma central telefônica, discriminando os dados das chamadas efetuadas pelos ramais, como data, hora e número chamado com indicação de qualidade.

4.2.3. VOIP4ALL

O projeto VoIP4all, foi criado em Outubro de 2005 e visa criar os meios para que instituições federais, universidades, centros de educação tecnológica e unidades de pesquisa possam implantar internamente uma infra-estrutura de suporte à VoIP e ao mesmo tempo se associarem ao serviço fone@RNP, aumentando a capilaridade e universalizando seu acesso. Essa iniciativa objetiva, também, a capacitação das instituições na tecnologia VoIP, a aquisição dos equipamentos necessários à adesão ao serviço fone@RNP, e o estabelecimento de suporte técnico durante o período de implantação.

4.3. DESCRIÇÃO DO SERVIÇO FONE@RNP

O serviço fone@RNP é fruto do trabalho desenvolvido pelo GT-VoIP (Grupo de Trabalho de Voz sobre IP) para a implantação de voz e telefonia IP no backbone RNP2. Qualquer instituição qualificada como usuária da rede da RNP pode aderir ao serviço. Os procedimentos para filiação ao fone@RNP e recomendações técnicas para implantação do ambiente podem ser encontrados em http://www.rnp.br/voip/.

A utilização de voz sobre IP racionaliza o uso da infra-estrutura de comunicação, possibilitando a convergência de dados e voz pela internet, com diminuição dos custos tradicionais de telefonia, principalmente quando as chamadas completadas são de longa distância. A tecnologia VoIP permite estender o acesso telefônico a locais onde existe a rede de dados, mas inexiste a disponibilidade de ramais telefônicos, além de incorporar o suporte à mobilidade do usuário. O suporte à mobilidade irá permitir que os usuários da instituição possam estar localizados em qualquer ponto do globo e, ainda assim, utilizem o serviço, bastando para tal ter acesso à internet (banda larga) e um software que realize chamadas VoIP configurado corretamente.

Atualmente, o perfil de gasto telefônico de uma instituição típica indica que a maior parcela (em torno dos 60%) das ligações é direcionada para celulares locais. Com a proliferação de celulares em todas as camadas da população, muitas vezes usados apenas com o intuito de receber chamadas, este é, no momento, o ponto fraco de qualquer instituição no Brasil [RNP, 2005].

A economia de custos necessariamente começa pela implementação de políticas de controle que caminhem na direção da limitação de discagem para celulares. Outra conseqüência natural do esforço para redução de custos é a limitação do número de ramais com a capacidade de efetuar DDD e DDI.

Para a comunidade acadêmica, na qual o incentivo a trabalhos cooperativos com instituições nacionais ou internacionais tem sido a tônica nos últimos anos, a restrição de comunicação passa a ter um impacto grande e bastante negativo. Enquanto a troca de e-mails atende integralmente a uma comunicação não interativa, o contato pessoal interativo, na ausência de chamadas telefônicas tradicionais, depende do uso de sistemas de mensagens instantâneas com voz integrada (MSN Messenger, Skype) ou de voz sobre IP.

Com o investimento no gateway (com interface digital ou analógica), a central telefônica institucional poderá ser integrado à Internet, permitindo o acesso ao serviço fone@RNP a partir de qualquer ramal interno. Ligações oriundas de telefones IP ou de ramais internos do PBX são tratadas como chamadas originadas internamente no serviço fone@RNP e tratadas de forma semelhante. Uma instituição que opere esse equipamento de voz poderá, a seu critério, permitir que chamadas originadas dentro da rede VoIP do serviço sejam completadas para a rede pública de telefonia.

Mais ainda, as instituições poderão permitir que chamadas externas, oriundas da rede pública de telefonia, possam acessar o serviço fone@RNP discando para o ramal do serviço. Nesse caso, estas chamadas originadas externamente ao serviço só poderão completar para a rede VoIP, isto é, para telefones IP ou ramais de PBX das instituições participantes.

O serviço fone@RNP está projetado e configurado para impedir que a RNP seja usada para completar chamadas entre telefones da rede pública de telefonia.

O serviço fone@RNP, em sua plenitude, fica restrito à comunidade acadêmica e de pesquisa, embora permita ampla e completa interação desta comunidade com a população em geral, usuária dos provedores de telefonia pública.

A implantação de VoIP dentro de uma instituição irá permitir que o acesso ao serviço fone@RNP seja liberado sem restrições, para qualquer ramal da central telefônica da instituição, visto que todas as chamadas, independente de serem chamadas locais, de longa distância ou internacionais, serão tratadas via Internet, sem custo adicional, como hoje ocorre com o e-mail. Ramais que hoje são de uso restrito passam imediatamente a ter a facilidade de completar chamadas para qualquer instituição ou cidade integradas ao serviço. Esta flexibilidade é muito atraente e conveniente, especialmente no momento atual, quando as instituições estão sendo forçadas a diminuir custos, resultando na habilitação de poucos ramais na instituição com capacidade de fazer DDD ou DDI.

4.3.1. ARQUITETURA FONE@RNP

Na arquitetura do serviço fone@RNP, telefones IP poderão ser disseminados entre os usuários das instituições acadêmicas, com um custo relativamente pequeno de

investimento. Basicamente, será preciso disponibilizar três máquinas com sistema operacional Linux para hospedagem de softwares de domínio público (Open Source) envolvidos e um equipamento para interconexão com a central telefônica da instituição.

O sistema VoIP é heterogêneo, baseado em SIP e H.323. Foram usados apenas softwares livres, dos quais se destacam o GnuGK (Gatekeeper), SER (Servidor Proxy SIP), Asterisk (Gateway SIP/H.323 e Gateway VoIP/PABX), FreeRADIUS (Servidor de autenticação, autorização e contabilização), OpenLDAP (Servidor que implementa o protocolo LDAP, com função de acessar serviços de diretório) e o PostgreSQL (Sistema gerenciador de banco de dados objeto-relacional). Esses softwares e o funcionamento do sistema com eles interligados serão apresentados mais detalhadamente, no próximo capítulo, na seção 5.2.

Na Figura 4.2 abaixo é mostrado a interligação de todos esses softwares, em conjunto com outros softwares, que também desempenham funções no sistema fone@RNP.

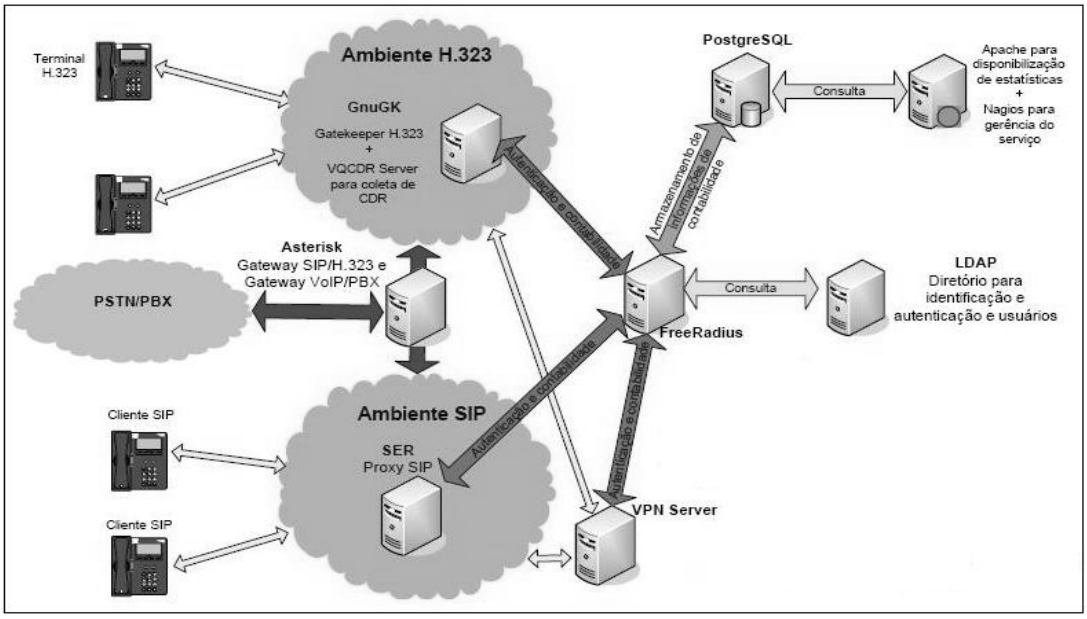


Figura 4.2 - Arquitetura do sistema fone@RNP
Fonte: RNP 2005 - Treinamento voip4all

4.4. CONCLUSÃO

O uso do serviço de VoIP pela Universidade, irá propiciar um melhor aproveitamento da estrutura da rede de dados já existente, além de reduzir gastos destinados as ligações telefônicas realizadas pelo modelo de telefonia tradicional.

A tendência do projeto fone@RNP é evoluir de forma contínua, propiciando cada vez mais uma melhoria do serviço de VoIP e reduzindo custos e mão de obra para a sua manutenção.

5. CONFIGURAÇÃO DO SISTEMA

Neste capítulo são apresentados os oito softwares que compõem o sistema VoIP da Universidade. Estes softwares estão divididos em servidores, banco de dados e softphones, que devidamente configurados e funcionando em conjunto fornecem o serviço de VoIP utilizando os protocolos SIP e H.323.

O capítulo ainda mostra o plano de numeração criado para a Universidade. Este plano, que é definido pela RNP, será usado tanto para as ligações telefônicas internas e externas.

5.1. SOFTWARES UTILIZADOS NA IMPLANTAÇÃO DO SISTEMA

Os softwares utilizados são todos softwares livres e estão divididos em servidores (GnuGK, SER, Asterisk, FreeRadius), banco de dados (PostGreSQL, OpenLDAP) e softphones (X-Lite, OpenPhone).

5.1.1. THE GNU GATEKEEPER – GNUGK

The GNU Gatekeeper é um projeto de código-fonte aberto que implementa um gerente de chamadas H.323, que provê serviços de controle para terminais H.323. Ele representa uma parte importante de muitas instalações de telefonia na internet que são baseadas no padrão H.323.

De acordo com a Recomendação H.323, um Gatekeeper deverá prover os seguintes serviços:

- Tradução de Endereço.
- Controle de Admissão.
- Controle de Banda Passante.
- Gerenciamento da Zona Administrativa.
- Sinalização de Controle das Chamadas.
- Autorização de Chamadas.

- Gerenciamento da Banda Passante.
- Gerenciamento das Chamadas.

The GNU Gatekeeper implementa muitas destas funções providas pela biblioteca OpenH323 que contém a pilha completa dos protocolos. A Recomendação H.323 é um padrão internacional publicado pela ITU (*International Telecommunication Union*), sendo um padrão de comunicação de áudio, vídeo e dados através da internet. O nome formal deste projeto é *OpenH323 Gatekeeper – The GNU Gatekeeper*, e o apelido é *OpenH323GK* ou *GnuGk*.

O GnuGK possui diversas funcionalidades, como tabela de registro, suporte à função proxy H.323, suporte a vários métodos de autenticação, dentre outras características descritas a seguir.

- *Tabela de registro e a tabela de chamadas* – suportam dezenas de milhares de registros e milhares de chamadas concorrentes.
- *Arquitetura GK-routed* – suporte para encaminhamento de H.225/Q.931 e H.245 sem a criação de linhas adicionais. Assim sendo, o limite no número de linhas não restringirá o número de chamadas concorrentes.
- *Função proxy H.323* - suporte para o encaminhamento de todos os canais lógicos, incluindo os fluxos RTP/RTCP dos canais de mídia e os canais de dados T.120. Os canais lógicos abertos pelo tunelamento H.245 e o procedimento de conexão rápida também são suportados. No modo proxy, não existe tráfego direto entre as entidades chamadoras e o chamado.
- *Métodos de autenticação* – suporte a vários métodos de autenticação às requisições RAS, incluindo senha H.235, casamento de padrão por IP ou por prefixo. Bancos de dados MySQL, PostgreSQL e LDAP também são suportados para a autenticação.
- *Suporte a Gatekeepers alternativos* – usado para redundância e balanceamento de carga. Se o GnuGk estiver sobrecarregado, os terminais podem ser redirecionados para outros Gatekeepers.

- *Monitoramento e controle do GnuGk* – monitora e controla o GnuGK via porta de status TCP, incluindo registros e estatísticas da chamada.
- *Impressão de CDR* – CDR é um registro detalhado da chamada, na porta de status para o sistema de contabilização. O CDR contém identificador da chamada, os endereços IPs do chamador e chamado, o inicio e o fim da ligação e a duração da mesma, dentre outras informações.
- *Configurações refeitas em tempo de execução* – é possível realizar mudanças de configuração sem precisar desligar o Gatekeeper. O GnuGk faz a re-leitura das configurações ao receber o comando *reload* via porta de status.

A seguir será mostrado o servidor SER que implementa o protocolo SIP e que tem a função de controlar o processo de chamadas SIP.

5.1.2. SIP EXPRESS ROUTER – SER

O SER (*SIP Express Router*) é um servidor freeware que roda em Linux. O servidor SER tem alto desempenho, sendo extremamente configurável, permitindo criar várias políticas de roteamento, assim como a configuração de serviços novos personalizados. Ele implementa o SIP (*Session Initiation Protocol*) que é um protocolo de sinalização usado para estabelecer chamadas telefônicas com uso de VoIP. Além disso, anuncia a presença de usuários, envia e recebe mensagens e mantém qualquer tipo de sessão, incluindo jogos e chat. Inclui também suporte para atuar como servidor de registro, proxy e redirecionamento.

O SER implementa infra-estruturas de VoIP em larga escala, assegurando alta flexibilidade que lhe permite atuar de forma distinta a satisfazer implementações de serviços variados. Por exemplo, pode atuar como registro de utilizadores e servidor de localização para prover mobilidade aos usuários. Pode também ser utilizado como elemento de controle de acesso, o qual armazena informações sobre gateways PSTN ou outros recursos SIP mais reservados. Pode ser facilmente estendido usando a sua configuração de línguas e suporte a funções particulares usadas para exibição de arquivos

multimídia embutidos, como gateways de messaging de SMS (*Short Message Service*), autenticação e contabilização via RADIUS, LDAP, ENUM entre outros.

O SER tem ainda uma interface de aplicação que permite um fácil acoplamento com outras aplicações que não funcionam com SIP. As aplicações como, interface web ou ferramentas administrativas, podem facilmente monitorar e manipular o estado do servidor e iniciar transações SIP.

Para interligar o GnuGK e o SER, e interligar a rede Ufla ao sistema de telefonia tradicional, é necessário o uso de um software que implementa as características de um PABX, este software é o Asterisk que será detalhado a seguir.

5.1.3. ASTERISK

O Asterisk é um software freeware, que implementa os recursos encontrados em um PABX (*Public Automatic Branch eXchange*) tradicional, utilizando tecnologia de VoIP. Um PABX permite que vários telefones fixos realizem ligações um ao outro, e permite a conexão a outros serviços de telefone, inclusive o PSTN (*Public Switched Telephone Network*).

Asterisk é um PABX híbrido, pois pode interligar diversas tecnologias e tem suporte a muitos *codecs* (codificador e decodificador de sinais de áudio, por exemplo, G.729, G711 e G.726). Na Figura 5.1 é apresentada a integração de vários serviços no Asterisk.

Asterisk tem suporte à tecnologia TDM *(Time-division multiplexing)*, e é um sistema IVR *(Interactive Voice Response)* com funcionalidades ACD *(Automatic Call Delivery)*.

Tecnologia TDM é um padrão na telefonia tradicional, que usa uma técnica para permitir a existência de vários canais de comunicação em um mesmo meio de transmissão. Para uma dada taxa de transmissão em bit/s são alocados alguns *slots* (intervalos) no tempo para cada canal de comunicação. Restrigem chamadas originadas da rede de telefonia pública.

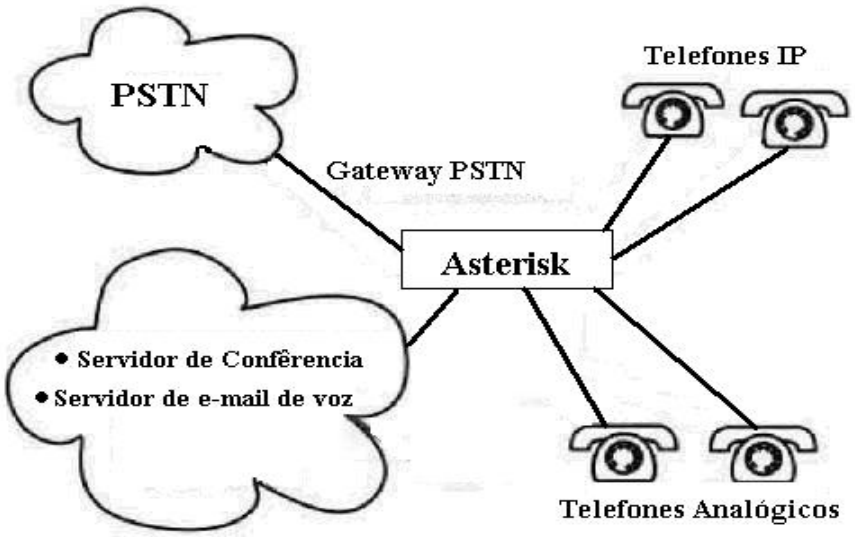


Figura 5.1 - Integração de Serviços no Asterisk

O Asterisk também é um sistema IVR. Este sistema tem características à reprodução (e, em alguns casos, a gravação) de mensagens para o usuário que está do outro lado da linha e pode restringir chamadas originadas da rede de telefonia pública. Pode ser integrado à central telefônica ou ser um equipamento separado. É muito utilizado quando há necessidade de vocalização de informações armazenadas em bancos de dados (por exemplo, em serviços de automação bancária ou no serviço de auxílio à lista). Esse sistema tem como funcionalidade o ACD que consiste num método de alocação de ligações telefônicas, muito utilizados em soluções de *call centers* (centrais onde as chamadas são processadas ou recebidas, com objetivos ligados às funções de vendas, marketing, serviço ao consumidor, telemarketing, suporte técnico e qualquer outra atividade administrativa especializada).

O Asterisk pode fornecer várias funcionalidades, como correio de voz, sala de conferência, discador automático, dentre outras que serão detalhadas abaixo.

- *Correio de voz* – Permite que quando o usuário não atender o telefone por estar ocupado ou ausente, seja enviado um aviso solicitando que o usuário originador da chamada deixe uma mensagem na caixa postal. É semelhante a uma secretária eletrônica ou caixa de mensagens do celular.
- *Sistema de mensagens unificadas* – sistema onde todas as mensagens são direcionadas para um único lugar, por exemplo, a caixa de correio eletrônico do

usuário. Neste caso as mensagens de e-mail, junto com as mensagens do correio de voz e fax seriam encaminhadas para a caixa postal do usuário.

- *Distribuidor automático de chamadas e fila de atendimento* – Em um DAC (ACD), as pessoas normalmente se autenticam em uma fila de atendimento para receber as chamadas. O distribuidor verifica se o usuário está com o telefone livre antes de passar a chamada. Se nenhum operador estiver livre ele segura a chamada na fila com um aviso sonoro e uma mensagem explicativa. No Asterisk isto já é feito de forma automática.
- *Servidor de música em espera* – Quando uma ligação não pode ser completada, por exemplo, num telemarketing, que todos os atendentes estejam ocupados, um dos ramais do servidor poderá conter uma música, para que a pessoa que esteja realizando a ligação fique esperando.
- *Discador automático* – Isto é muito útil em telemarketing, pode se programar o sistema para discar automático e distribuir numa fila.
- *Sala de Conferência* – Permite que vários usuários falem em conjunto. É implementado como sala de conferência, o usúario escolhe um ramal para ser a sala de conferência e todos os que discarem para lá estão imediatamente conectados. Tem várias opções como senha, por exemplo.

Na próxima seção será apresentado o protocolo LDAP, juntamente com o OpenLDAP, software que implementa este protocolo.

5.1.4. OPENLDAP - LDAP

LDAP (*Lightweight Directory Access Protocol*) é um protocolo que roda diretamente sobre a pilha TCP/IP e tem a função de acessar serviços de diretórios [GRAHAM BARR, 2003]. Serviço de diretórios nada mais é que uma base de dados simples, organizada em modelo de árvore, com níveis e subníveis como galhos e suas ramificações. Por isso, é chamado de serviço de diretórios, por que sua estrutura é bastante parecida com a organização de diretórios de um dispositivo de armazenamento, [BRIAN ARKILLS, 2003]. Essa base de dados tem uma estrutura simples, mas que permite alto

desempenho e disponibilidade em grandes volumes de consultas simples. É especialmente otimizada para leituras, consultas e buscas.

Devido a essa estrutura de armazenamento de informações, o LDAP se comporta hierarquicamente como, por exemplo, informações de uma estrutura organizacional (presidência, diretorias, gerências, departamentos, supervisores), informações sobre níveis de acesso de uma determinada aplicação (aplicação, tipo de acesso, grupo de usuários) ou até mesmo uma estrutura geográfica (países, estados, cidades, municípios). A aplicabilidade do LDAP é grande devido à alta flexibilidade de organização das informações por ele armazenadas.

O LDAP pode ser utilizado em várias situações, com grande aplicabilidade na função de autenticação. É um serviço que, basicamente, compara a identificação do solicitante ao seu banco de dados de usuários cadastrados e, baseado nos atributos deste banco de dados, permite ou não a continuidade dos serviços solicitados.

O LDAP fornece esse tipo de serviço, uma vez que pode armazenar informações e atributos de usuários. Além de fornecer o serviço de autenticação, o LDAP se integra a um vasto número de aplicativos, fazendo o papel de autenticador para eles. Esses aplicativos podem ser executados em sistemas operacionais como Unix, Linux e Windows 2000. Podem ser aplicativos de mercado como SGBD *(Sistemas Gerenciadores de Bancos de Dados)* (ORACLE, PostgreSQL, MySQL), Samba, Squid ou aplicações desenvolvidas em linguagens de programação como PHP *(Personal Home Page)* e Java [BRIAN ARKILLS, 2003]. Também é possível uma combinação de ferramentas, como por exemplo, um SGBD que é autenticado através do sistema operacional que, por sua vez, é autenticado no LDAP.

O modelo de informação do LDAP é baseado em "entradas". Uma entrada é uma coleção de atributos e têm um identificador único chamado DN (*Distinguished Name*). O DN é composto por uma seqüência de atributos. Cada um dos atributos tem um tipo e um ou mais valores. Os tipos são: "cn" para "common name" ou "mail" para "mail address", [BRIAN ARKILLS, 2003].

Um exemplo de DN: cn=renato, ou=voip1, o=ufla, c=br. Esta DN indica que existe um cadastramento hierárquico na base do LDAP e sugere a estrutura representada na Figura 5.2.

O acesso à informação no LDAP permite operações para consultar e atualizar sua base de dados. Existem operações para adição, modificação e remoção de uma entrada do

diretório. Funções em várias linguagens já estão disponíveis, facilitando o trabalho dos desenvolvedores. Este projeto se utiliza de funções em PHP para executar autenticação e busca de informações na base LDAP.

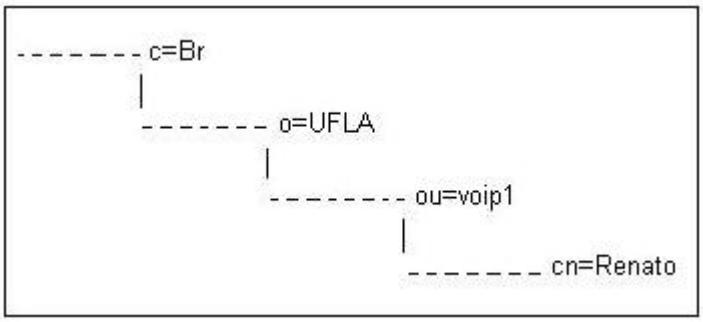


Figura 5.2 – Cadastramento Hierárquico

O OpenLDAP é uma das várias distribuições de LDAP disponíveis. A distribuição da OpenLDAP Foundation, utilizado neste projeto, é licenciada sob a OpenLDAP Public License.

O OpenLDAP oferece um conjunto de funções de apoio à manipulação e administração dos dados, além de sua função básica de autenticação. Em relação à manipulação dos dados, o OpenLDAP traz comandos de busca, inserção, deleção e modificação de entradas na sua porção cliente. O cliente OpenLDAP já está disponível para diversas plataformas. Além da interface texto, disponível como pacote OpenLDAP, muitas interfaces gráficas foram desenvolvidas por terceiros para facilitar a manipulação dos dados hospedados na base OpenLDAP. Podemos citar como exemplo de interface o PhpLDAPAdmin e o FegGK.

O OpenLDAP não oferece em seu pacote original nenhuma interface gráfica para administração. Existem muitos projetos para ferramentas com essa finalidade. Uma delas é o PhpLDAPAdmin. Esse produto permite a execução das tarefas básicas de administração do LDAP como a visualização da árvore, visualização de esquemas, busca, criação, deleção, copia e edição de entradas. Além disso, a grande vantagem do PhpLDAPAdmin é ser desenvolvida para ambiente Web, permitindo a administração da base de autenticação de qualquer estação conectada à rede.

O PhpLDAPAdmin é distribuído sob a General Public Licence (GNU). Sua instalação requer um servidor Web em funcionamento. O servidor usado foi o Apache, que é um software de domínio público para hospedagem de sites.

O FegGK (*Ferramenta de Gerência do GnuGK*) é uma ferramenta utilizada para manipulação da base de dados OpenLDAP via Web. O FegGK também é usado para gerenciar e configurar o GnuGK.

Por meio desta ferramenta é possível alterar as configurações do OpenLDAP, por exemplo, criar, alterar e remover uma conta de um usuário. Na Figura 5.3 é apresentada a tela inicial da ferramenta, onde é possível notar as opções de configuração e gerenciamento que ela dispõe.

O tamanho e a geografia da organização podem exigir a distribuição de bases de autenticação. O OpenLDAP possui as funcionalidades necessárias para a descentralização da autenticação, através dos seus múltiplos servidores.

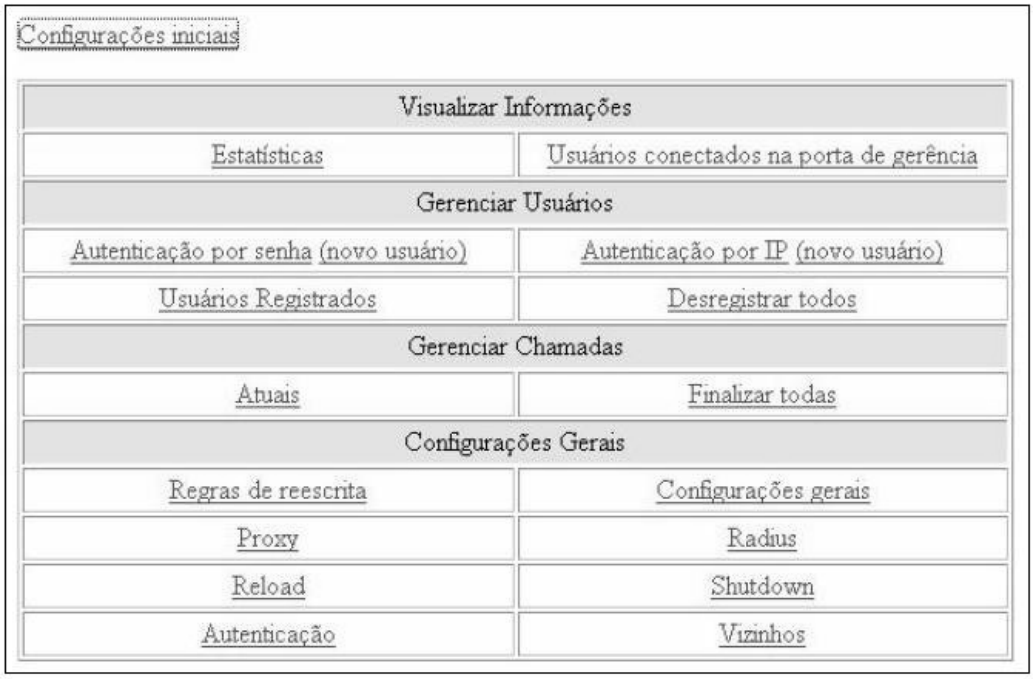


Figura 5.3 – Interface inicial da ferramenta FegGK
Fonte: RNP 2005 – Treinamento voip4all

A segurança dos acessos, evitando que as informações fiquem expostas, é imprescindível. O LDAP fornece métodos para autenticação de clientes que protegem as informações contidas no servidor. Mas a segurança somente da autenticação pode não ser tudo. Dependendo dos dados disponíveis no servidor OpenLDAP, pode ser bastante

interessante proteger toda a transmissão de dados. O uso do SSL (*Secure Sockets Layer*) permite isso, mantendo as informações seguras de intrusos na rede.

Existem versões de servidores LDAP para muitas plataformas, o que o torna bastante popular. É fato que ainda existe a preferência por parte dos desenvolvedores para as plataformas UNIX. Ultimamente, com a popularização do LINUX isto deixou de ser um impeditivo. Ao contrário disso, uma arquitetura bastante encontrada é a hospedagem do servidor LDAP em LINUX com clientes rodando em diversos tipos de ferramentas visuais no Windows.

A flexibilidade é um dos pontos mais fortes do LDAP. Seu poder de integração a várias plataformas, ambientes, aplicações e tecnologias é o que o faz um produto tão interessante.

A seguir é mostrado o FreeRADIUS, software que implementa o protocolo RADIUS, responsável em acessar a base de dados do OpenLDAP, para autenticação, autorização e contabilidade.

5.1.4. FREERADIUS - RADIUS

RADIUS (Remote Authentication Dial In User Service) definido pela RFC 2865, é um protocolo de autenticação, autorização e contabilidade. O RADIUS tem várias características chaves como segurança, confiabilidade e escalabilidade, facilidade de uso, centralização da autenticação e autorização e possui interface com várias bases de dados (LDAP, MySQL, PostgreSQL, etc).

Os serviços do FreeRADIUS são autenticação/autorização e contabilidade. A autenticação/autorização definem os mecanismos para se autenticar e armazenar os perfis dos usuários (privilégios, direitos e restrições). A autenticação tem que garantir que é usuário quem ele diz ser, e a autorização verifica quais são as regras, privilégios para o determinado usuário.

A arquitetura do RADIUS é simples. Usando um NAS (*Network Acess Server*), que no caso específico da UFLA pode ser o Gatekeeper (GnuGK), um usuário (terminal H.323) quando faz uma chamada telefônica, se conecta no NAS. Esse servidor irá negociar com o

RADIUS se ele aceita ou rejeita a sua conexão, através de conferência dos atributos do usuário (login, senha, etc).

O FreeRADIUS foi escolhido para essa implementação do serviço fone@RNP, pois possui várias características que se enquadram nas características do projeto. O FreeRADIUS é um software freeware que permite autenticação via LDAP, serviço de acesso a diretório utilizado pelo projeto fone@RNP, e também possui interfaces com diferentes SGBDs. A Figura 5.4 mostra como é feita a ligação dos servidores SIP e H.323 ao RADIUS, e como ele autentica, autoriza uma ligação no servidor LDAP.

O serviço de contabilização de chamadas é de grande importância, pois são armazenadas informações sobre as chamadas, como duração, origem, destino, motivo de desconexão e a qualidade de voz.

O FreeRADIUS é baseado na coleta de CDR (*Call Detail Record*), que é um conceito herdado de telefonia tradicional. Os equipamentos envolvidos em uma chamada geram CDRs que reportam um relatório relativo à chamada (tempo, local, etc). Os CDRs são enviados para o servidor RADIUS e depois são armazenados no banco de dados PostgreSQL.

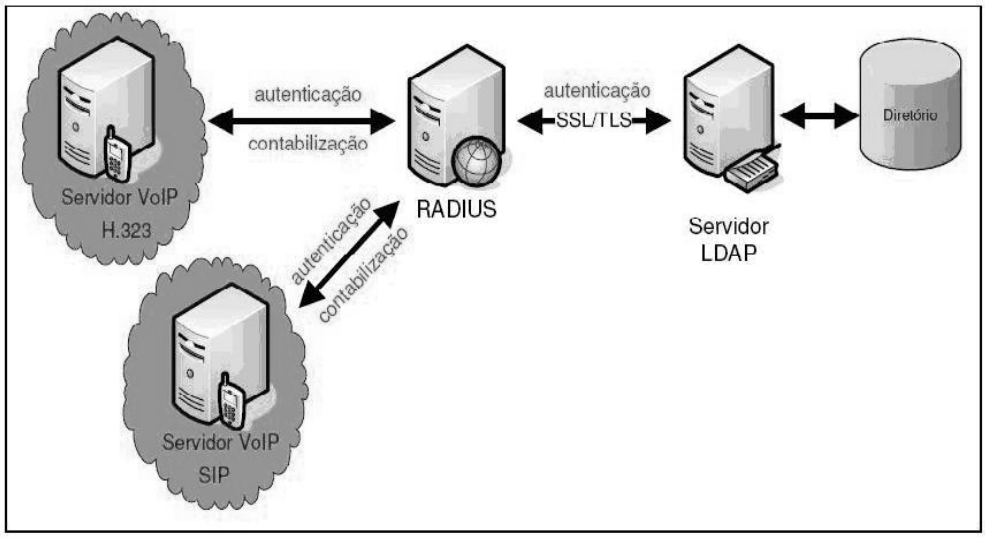


Figura 5.4 – Ligação servidores SIP e H.323 ao FreeRADIUS
Fonte: RNP 2005 – Treinamento voip4all

O CDR RADIUS é composto por 3 tipos de mensagens:

- *Start* - início da chamada
- *Ínterim* - enviadas de tempos em tempos

- *Stop* - fim da chamada

A quantidade de CDR's gerados por chamadas dependerá da trajetória da chamada. Um Gatekeeeper H.323, por exemplo, sempre gera um CDR, mas em uma chamada podem ser gerados de 1 a 6 CDRs. Uma consolidação de CDRs também é feita, essa consolidação reúne as informações mais relevantes dos CDRs envolvidos na chamada. Essas informações mais relevantes podem ser vistas na Tabela 5.1.

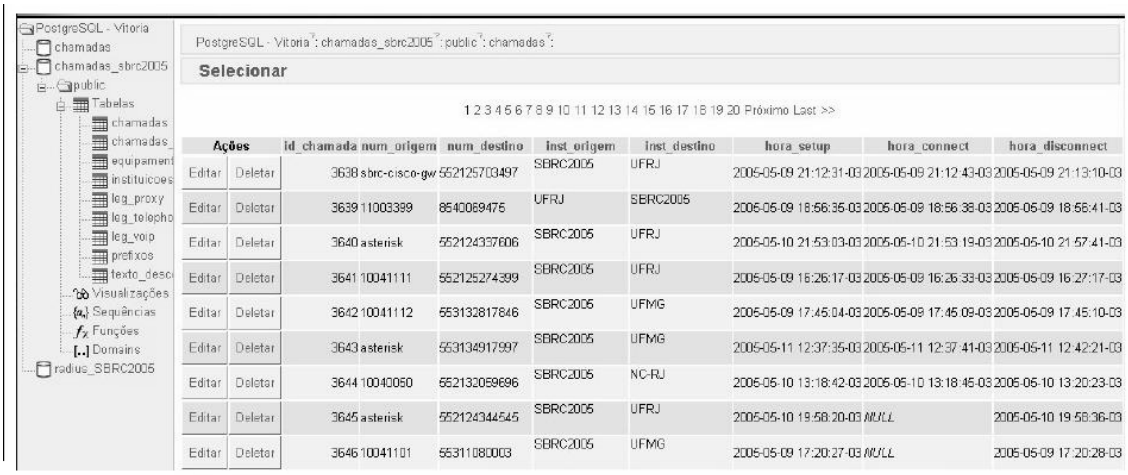
O FreeRADIUS não oferece em seu pacote original nenhuma interface gráfica para administração do banco de dados que armazena os dados de suas autenticações. Uma ferramenta chamada de PhpPGAdmin permite a visualização do banco de dados PostgreSQL, podendo então, visualizar o que está armazenado no banco de dados. Além disso, a grande vantagem do PhpPGAdmin é estar em ambiente WEB, permitindo a administração da base de autenticação de qualquer estação conectada à rede.

Tabela 5.1 – Tabela de CDRs

Objetivo	Informação
Usuários envolvidos	E.164 do originador da chamada
	E.164 do telefone chamado
	IP do originador
	Tipo de telefone do originador
	Tipo de telefone do chamado
Características da Chamada	Identificação da chamada
	Chamada atendida?
	Chamada local?
	Término normal?
	Motivo da desconexão
	Usuário que iniciou desconexão
	Qualidade da chamada
Instituições envolvidas	Instituição do originador
	Instituição do chamado
	IP GK_Origem
	IP GK_Chamado
	IP GW_Origem
Tempos associados	Hora_setup
	Hora_connect
	Hora_disconnect
	Duração

Fonte: RNP 2005 – Treinamento voip4all

O PhpPGAdmin é distribuído sob a *General Public Licence* (GNU). Sua instalação requer um servidor WEB em funcionamento, que no caso deste trabalho, é um servidor Apache. A Figura 5.5 mostra um exemplo de uma análise do banco de dados feita por meio do PhpPGAdmin.



Ações		id_chamada	num_origem	num_destino	inst_origem	inst_destino	hora_setup	hora_connect	hora_disconnect
Editar	Deletar	3638	sbrc-cisco-gw	552125703497	SBRC2005	UFRJ	2005-05-09 21:12:31-03	2005-05-09 21:12:43-03	2005-05-09 21:13:10-03
Editar	Deletar	3639	11003389	8540069475	UFRJ	SBRC2005	2005-05-09 18:56:35-03	2005-05-09 18:56:38-03	2005-05-09 18:56:41-03
Editar	Deletar	3640	asterisk	552124337606	SBRC2005	UFRJ	2005-05-10 21:53:03-03	2005-05-10 21:53:19-03	2005-05-10 21:57:41-03
Editar	Deletar	3641	10041111	552125274399	SBRC2005	UFRJ	2005-05-09 16:26:17-03	2005-05-09 16:26:33-03	2005-05-09 16:27:17-03
Editar	Deletar	3642	10041112	553132817846	SBRC2005	UFMG	2005-05-09 17:45:04-03	2005-05-09 17:45:09-03	2005-05-09 17:45:10-03
Editar	Deletar	3643	asterisk	553134917997	SBRC2005	UFMG	2005-05-11 12:37:35-03	2005-05-11 12:37:41-03	2005-05-11 12:42:21-03
Editar	Deletar	3644	10040050	552132059696	SBRC2005	NC-RJ	2005-05-10 13:18:42-03	2005-05-10 13:18:45-03	2005-05-10 13:20:23-03
Editar	Deletar	3645	asterisk	552124344545	SBRC2005	UFRJ	2005-05-10 19:58:20-03	*NULL*	2005-05-10 19:58:36-03
Editar	Deletar	3646	10041101	55311080003	SBRC2005	UFMG	2005-05-09 17:20:27-03	*NULL*	2005-05-09 17:20:28-03

Figura 5.5 – Análise feita do banco de dados através do PhpPGAdmin
Fonte: RNP 2005 – Treinamento voip4all

Como citado na seção, é usado um banco de dados para armazenamento das estatísticas referentes às chamadas. Este banco de dados é o PostgreSQL, que será mais detalhado na próxima seção.

5.1.5. POSTGRESQL

PostgreSQL é um SGBD (*Sistema Gerenciador de Banco de Dados*) que se destaca atualmente perante a comunidade científica/acadêmica e principalmente comercial.

Como todo Sistema Gerenciador de Banco de Dados, o objetivo básico do PostgreSQL é o armazenamento de dados de modo organizado e gerenciável, permitindo a guarda e o resgate de dados e informações de maneira rápida, segura e eficiente.

O PostgreSQL é um software freeware, desenvolvido pela Universidade de Berkley e hoje mantido por uma grande comunidade de desenvolvedores espalhada pelo mundo. Entre os produtos dessa linha, possui grande vantagem técnica e funcional sobre seus "concorrentes" e está ganhando uma boa fatia do mercado corporativa e concorrendo, inclusive, com produtos comerciais como ORACLE e SQLServer [PEREIRA NETO, 2003].

Fornece suporte às linguagens SQL, além de outras funcionalidades modernas. O PostgresSQL foi pioneiro em muitos conceitos objeto-relacionais que agora estão se tornando disponíveis em alguns bancos de dados comerciais. Os SGBDR (*Sistemas de*

Gerenciamento de Bancos de Dados Relacionais) tradicionais suportam um modelo de dados composto por uma coleção de relações com nome, contendo atributos de um tipo específico. Nos sistemas comerciais em uso, os tipos possíveis incluem número de ponto flutuante, inteiro, cadeia de caracteres, monetário e data. É amplamente reconhecido que este modelo não é adequado para aplicações futuras de processamento de dados. O modelo relacional substituiu com sucesso os modelos anteriores pela sua simplicidade, porém essas simplicidades tornaram a implementação de certas aplicações muito difícil.

O sistema de gerenciamento de banco de dados objeto-relacional, atualmente conhecido por PostgreSQL (e por um breve período de tempo chamado Postgres95), é considerado assim por implementar um conjunto de recursos adicionais ao tradicional modelo SGBDR (*Sistema gerenciador de Banco de Dados relacional*). Dentre os quais podemos destacar; herança, tipos de dados e funções.

Isso sem perder as funcionalidades intrínsecas ao mundo dos bancos de dados relacionais (gatilhos, restrições, regras, papéis, integridade de transações, etc.).

Segundo o [The PostgreSQL Global Development Group, 2002] estas funcionalidades colocam o PostgreSQL dentro da categoria de banco de dados referida como objeto-relacional. Portanto, embora o PostgreSQL possua algumas funcionalidades de orientação a objetos, está firmemente ligado ao mundo dos bancos de dados relacionais.

O PostgreSQL tem características atraentes além da grande vantagem de ser um software freeware. Abaixo são apresentadas essas características.

- *Confiabilidade* - dispõe de funcionalidades internas de auto recuperação que, aliadas a técnicas de segurança como rotinas de *backup*, espelhamento de discos e *cluster*, conferem alta confiabilidade ao produto.
- *Desempenho* - através de técnicas complexas, utilizando-se de algoritmos de busca, indexação, indexação reversa e em cache, o PostgreSQL está entre os primeiros na comparação de performance, só ficando atrás de produtos que não contém funcionalidades essenciais, como integridade referencial e *joins* complexos.
- *Flexibilidade* - por se tratar de um produto de código aberto, suas funcionalidades podem ser alteradas de forma a melhor se compatibilizar com as necessidades do ambiente.

- *Facilidade de administração* - Devido a sua arquitetura, o PostgreSQL é praticamente "auto-administrável". Com exceção das rotinas de *backup* e restauração, as demais tarefas de administração de espaço, controle de estatísticas e outra infinidade de trabalhos tipicamente desenvolvidos por um DBA (*Data Base Administrator*) são automatizados e realizados pelo próprio produto.
- *Baixo consumo de recursos* - o ambiente em que o PostgreSQL melhor se comporta é composto por um servidor de hardware básico com sistema operacional Linux. O consumo de disco rígido é bem menor que um SGBD Oracle, por exemplo, e o consumo de memória é equivalente.

5.1.6. SOFTPHONES – X-LITE E OPENPHONE

O serviço fone@RNP possibilita aos usuários o acesso ao sistema telefônico através de ramais virtuais alocados a um determinado usuário e associado a um usuário e senha. Um ramal virtual é um número de nove dígitos começando com o 0 (zero) e mais oito dígitos quaisquer.

Softphone é um software que pode ser usado tanto em plataforma Linux como Windows. Este software implementa um telefone em um computador, sendo a interface de áudio provido pela placa de som do PC. Com o advento da telefonia IP, o termo passou a designar um aplicativo que transforma o PC num terminal de telefonia IP. Como foram usados dois protocolos da camada de aplicação para implementação do sistema, é usado um softphone para cada protocolo: X-lite para SIP e o OpenPhone para H.323.

Lembrando que, apesar destes softphones trabalharem com protocolos diferentes, eles podem se comunicar devido a interoperação dos protocolos SIP e H.323.

O Suporte ao Gatekeeper (H.323) do OpenPhone é muito simples. Pode ser escolhido um Gatekeeper manualmente ou o próprio OpenPhone detecta na rede automaticamente. O Gatekeeper só é habilitado automaticamente caso haja apenas um Gatekeeper configurado na rede interna ou a certeza que exista algum na rede. A procura pelo Gatekeeper pode ser demorada, e caso não haja nenhum ou tendo ele sido escrito manualmente, pode ocorrer um erro e o OpenPhone ser fechado automaticamente mesmo

antes de ser usado. A seguir mostraremos passo a passo a configuração do OpenPhone para ambiente Windows.

1 - Quando o software é iniciado pela primeira vez, aparece à tela da Figura 5.6, a seguir.

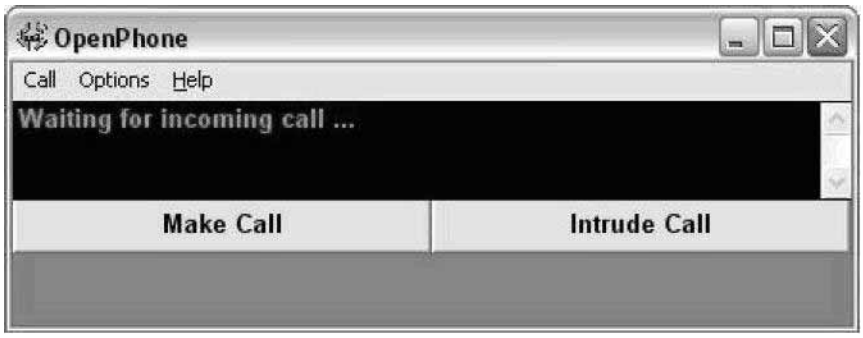


Figura 5.6 – Tela Inicial do Software OpenPhone
Fonte: RNP 2005 – Treinamento voip4all

Repare que ainda nenhum Gatekeeper foi localizado.

2 - Clicando em *Options* aparecerá o item *General,* este item é usado para configurar as informações do usuário, como *Username* e *Alises*. Veja na Figura 5.7.

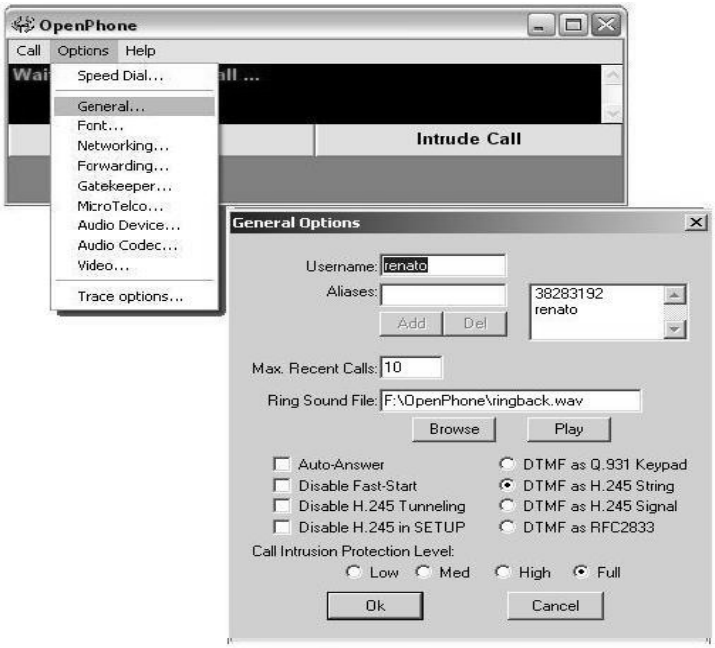


Figura 5.7 – Tela de Configuração do *username e alias*
Fonte: RNP 2005 – Treinamento voip4all

3 - Feito isto, é necessário agora à configuração do Gatekeeper. Novamente na opção de menu *Options* selecione o item *Gatekeeper*, abrirá uma janela e será necessário o preenchimento da *Static Host* (no caso do trabalho, voip1.ufla.br) e colocar a senha de usuário, que já foi criado anteriormente quando o usuário foi cadastrado no sistema, em *H.235 Password*. Veja na Figura 5.8.

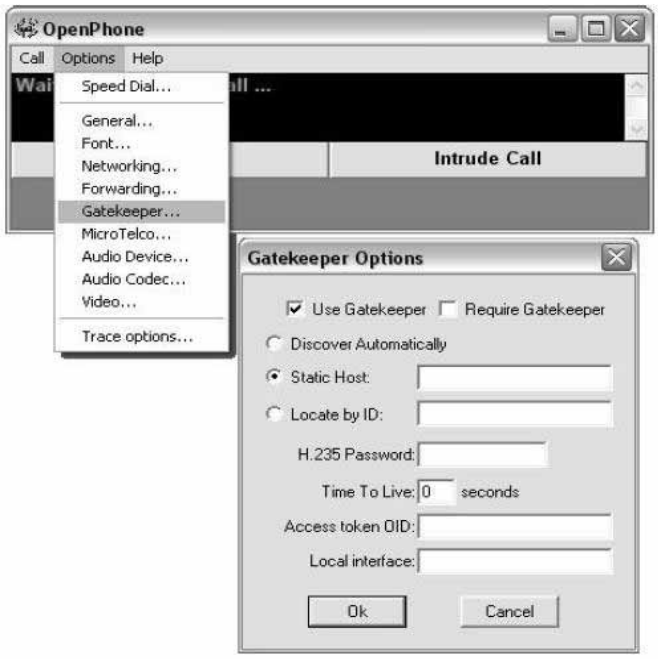


Figura 5.8 – Configurar Gatekeeper e Senha do Usuário
Fonte: RNP 2005 – Treinamento voip4all

Depois de feita essas configurações, a tela do softphone pode ser vista na Figura 5.9. Repare que agora existe um Gatekeeper registrado.

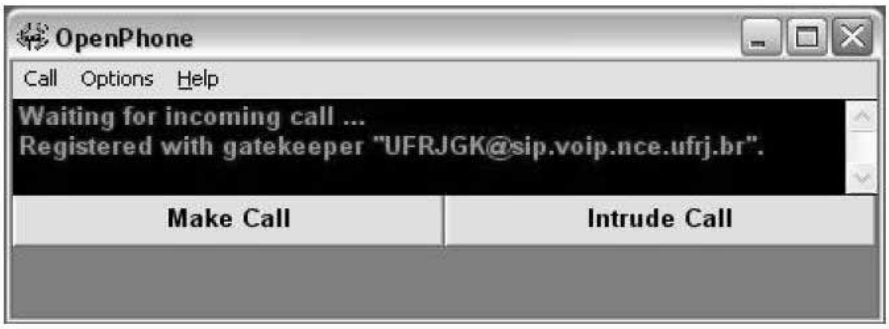


Figura 5.9 – Mostra com qual Gatekeeper o usuário está registrado
Fonte: RNP 2005 – Treinamento voip4all

4 - Para fazer uma ligação é preciso clicar em *Make Call* e configurar o campo *Address* com o alias do usuário que você for ligar, e clicar na opção *Ok*. Ver Figura 5.10 abaixo.

Figura 5.10 – Tela para Realizar a Ligação
Fonte: RNP 2005 – Treinamento voip4all

O softphone X-lite usado para fazer ligações sobre o protocolo SIP, pode rodar em Linux ou Windows. Abaixo será mostrado como fazer a configuração deste softphone passo a passo, para se usar o serviço de VoIP no ambiente Windows.

1 - O X-lite quando iniciado tem o formato apresentado na Figura 5.11 abaixo.

Figura 5.11 – Tela inicial do X-lite
Fonte: RNP 2005 – Treinamento voip4all

2 - Clique no *Menu Button* para configurar o servidor SIP Proxy. Clique em *System Settings* e selecione a opção *SIP Proxy*. Em *Default* defina o servidor, que no caso do trabalho é voip1.ufla.br. Apareça uma tela como a dá Figura 5.12, e será preciso preencher os campos da seguinte maneira (os campos que não forem preenchidos no exemplo, não é preciso preencher):

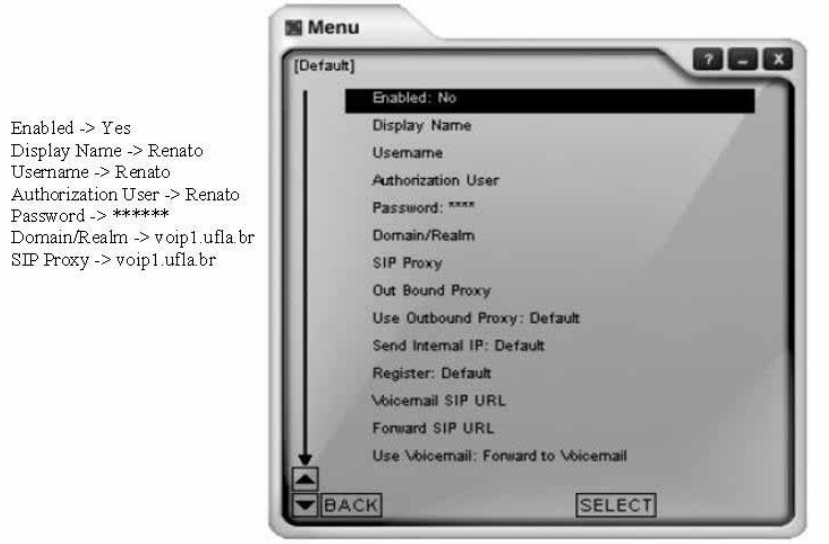


Figura 5.12 – Tela Principal de Configuração do X-lite
Fonte: RNP 2005 – Treinamento voip4all

3 - Pronto, o softphone está configurado e aparecerá na tela principal do programa *Logged in – Enter Phone Number* como mostrado na Figura 5.13 abaixo. Para fazer uma chamada é apenas discar um número, clicando em cima dos números no softphone e clicar em *Dial Button*.

Figura 5.13 – Tela do Programa Indicando que o Usuário está Conectado
Fonte: RNP 2005 – Treinamento voip4all

Com todos os softwares caracterizados, será mostrado na próxima seção como é o funcionamento do sistema, com estes softwares configurados em conjunto.

5.2. FUNCIONAMENTO DO SISTEMA

O sistema de VoIP implantado na UFLA é um sistema híbrido. É possível realizar chamadas telefônicas usando os protocolos da camada de aplicação SIP e H.323. Isto pode ser feito por meio dos softphones X-lite e OpenPhone, respectivamente, sem ser necessário que a chamada seja realizada entre o mesmos softphones. O sistema está configurado para que haja uma interoperabilidade entre os dois protocolos.

Na figura 5.14 a seguir é mostrado um diagrama, onde cada etapa da realização de uma chamada telefônica SIP ou H.323 é demonstrada.

O usuário quando for realizar uma chamada poderá optar por usar X-lite (SIP) ou OpenPhone (H.323), desde que as configurações necessárias para o seu funcionamento já estejam prontas (seção 5.1.6). A chamada telefônica do usuário pode ser destinada tanto para um softphone, análogo ao que foi originada a chamada, ou para um softphone que usa um protocolo de aplicação diferente.

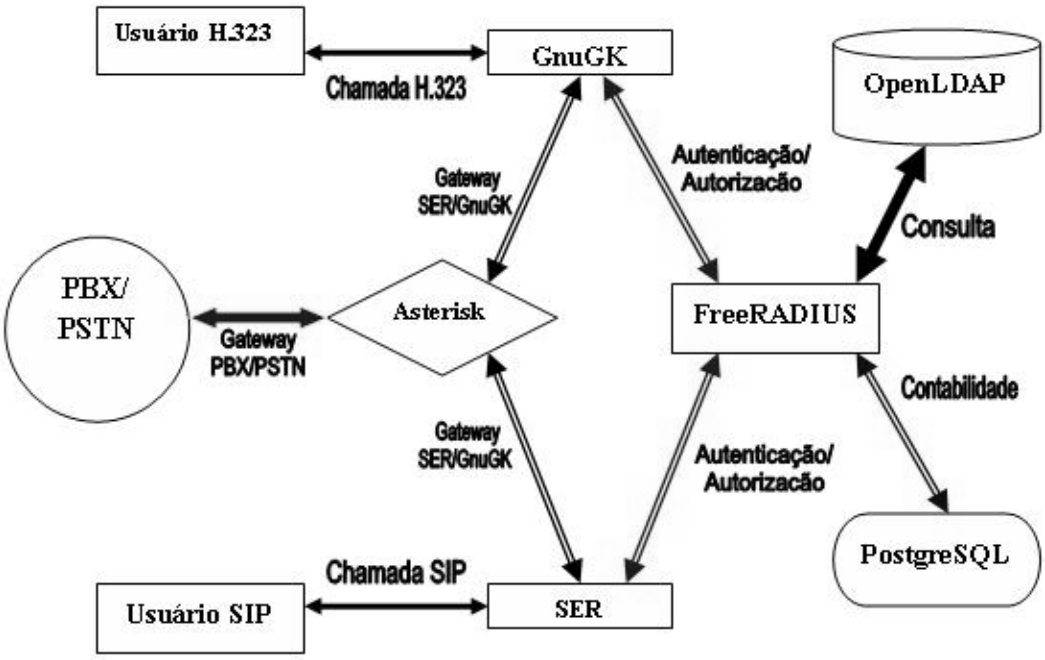


Figura 5.14 – Diagrama das etapas de uma chamada telefônica SIP e H.323

O processo realizado para que uma chamada telefônica seja completada pode ter quatro modelos diferentes: SIP para SIP, H.323 para H.323, SIP para H.323 e H.323 para SIP. Estes quatro modelos são apresentados a seguir.

5.2.1. SIP PARA SIP

O usuário executa o software X-lite, sendo preciso que ele realize seu login no servidor específico de seu protocolo, que no caso é chamado de Servidor Proxy. Feito isso, começa todo um processo para que o usuário se conecte ao servidor corretamente e consiga realizar uma chamada.

Como a ligação será feita pelo X-lite (SIP), o servidor aonde o usuário irá conectar é o SER (*SIP Express Router*), servidor responsável em realizar chamadas SIP. O SER está conectado ao servidor FreeRADIUS, responsável pela autenticação/autorização e contabilidade da chamada. Este servidor é usado para completar a autorização e autenticação do usuário e faz uma consulta ao servidor OpenLDAP, que armazena em diretórios todas as informações de usuários cadastrados no sistema. Essas informações são consideradas como atributos do usuário. A autenticação irá verificar se o usuário é realmente quem ele está dizendo ser, por meio de seu nome de usuário e sua senha que foram configurados no softphone. Feito isso, serão autorizadas as regras e privilégios do usuário. Se ocorrer algum problema no momento dessa autenticação/autorização como, por exemplo, o usuário não ter sido cadastrado anteriormente na base de dados do OpenLDAP, o FreeRADIUS não irá autenticar e autorizar o usuário, e respectivamente o SER também não poderá realizar o login, retornando uma mensagem de erro e não possibilitando então a realização de chamadas por este usuário.

As informações do usuário estando autenticada e autorizada, o login será completado no servidor SER e sendo possível realizar chamadas. Como a ligação irá ser feita para um outro usuário que está utilizando o X-lite (SIP), basta discar um número por meio do teclado virtual do programa e fazer a chamada, que o próprio servidor SER terá a função de completar todo o processo, como verificar número do telefone e tocar o softphone do usuário de destino. O processo que ocorre para uma chamada usando o protocolo H.323 é semelhante, porém ele usa um servidor diferente. Este processo é visto na próxima seção.

5.2.2. H.323 PARA H.323

O usuário executa o software OpenPhone, sendo preciso que ele realize seu login no servidor específico do seu protocolo, que no caso é chamada de Gatekeeper. Feito isso, começa todo um processo para que o usuário se conecte ao Gatekeeper corretamente e consiga realizar uma chamada.

A ligação será feita pelo OpenPhone (H.323). Neste caso, o Gatekeeper aonde o usuário irá conectar é o GnuGK. O Gatekeeper está conectado ao servidor FreeRADIUS, responsável pela autenticação/autorização e contabilidade da chamada. Este servidor irá completar a autorização e autenticação do usuário, fazendo uma consulta ao servidor OpenLDAP, que armazena em diretórios todas as informações de usuários cadastrados no sistema. Essas informações são consideradas como atributos do usuário. A autenticação irá verificar se o usuário é realmente quem ele está dizendo ser, por meio de seu nome de usuário e sua senha, que foram configurados no softphone. Feito isso, serão autorizadas as regras e privilégios do usuário. Se ocorrer algum problema no momento dessa autenticação/autorização como, por exemplo, o usuário não ter sido cadastrado anteriormente na base de dados do OpenLDAP, o FreeRADIUS não irá autenticar e autorizar o usuário. O Gatekeeper também não poderá realizar o login, retornando uma mensagem de erro e não possibilitando então a realização de chamadas.

As informações do usuário estando autenticadas e autorizadas, o login é completado no Gatekeeper e sendo possível realizar chamadas. Como a ligação é feita para um outro usuário que está utilizando o OpenPhone (H.323), basta indicar o *alias* do usuário que irá receber a chamada, que o próprio Gatekeeper completará todo o processo, como verificar o *alias* e tocar o softphone do usuário de destino.

A seguir é mostrado como funciona o processo de uma chamada híbrida, ou seja, quando se usa protocolos diferentes.

5.2.3. SIP PARA H.323

O processo para ser realizada uma chamada telefônica entre softphones que implementam protocolos diferentes (SIP/H.323) torna-se um pouco mais complexa, pois é necessário o uso do software Asterisk, que funcionará como gateway dos dois servidores.

Como a ligação será feita pelo X-lite (SIP), o servidor aonde o usuário irá ter que conectar é o SER (*SIP Express Router*). O SER está conectado ao servidor FreeRADIUS, que é responsável em autenticação/autorização e contabilidade da chamada. Este servidor, para completar a autorização e autenticação do usuário, faz uma consulta ao servidor OpenLDAP. A autenticação irá verificar se o usuário é realmente quem ele está dizendo ser, por meio de seu nome de usuário e sua senha, e logo após será autorizado às regras e privilégios do usuário. Se ocorrer algum problema no momento dessa autenticação/autorização, o FreeRADIUS não irá autenticar e autorizar o usuário, e respectivamente o SER também não poderá realizar o seu login, retornando uma mensagem de erro e não possibilitando então a realização de chamadas.

As informações do usuário estando autenticadas e autorizadas, o login é completado no servidor SER possibilitando a ocorrência de chamadas. Como a chamada será feita para um usuário que está utilizando o OpenPhone (H.323), o servidor SER terá que se conectar com o servidor (Gatekeeper) responsável em realizar chamadas H.323.

Nesse momento é que o Asterisk entra em funcionamento, pois ele servirá de gateway entre o SER e GnuGK. Ele fará as mudanças necessárias nas configurações dos pacotes de dados no formato SIP, para que o GnuGK complete a chamada para o usuário que esteja usando o OpenPhone (H.323).

5.2.4. H.323 PARA SIP

O processo inverso ao anterior tem praticamente o mesmo formato, porém invertendo as ordens dos servidores e softphones, pois a autenticação/autorização e contabilidade são feitas da mesma forma. Nesse caso, o Asterisk fará as mudanças nas configurações dos pacotes H.323, para que da mesma forma o SER possa completar a chamada para o usuário que esteja usando X-lite (SIP).

Em todos os modelos de chamada o FreeRADIUS irá contabilizar as estatísticas das chamadas por meio de CDRs (*Call Detail Record*). Estes CDRs vão conter informações

como: qualidade da chamada, a hora que a chamada se conectou, a hora que a chamada se desconectou, duração das chamadas, dentre outras características. Estes CDRs ficarão armazenados no banco de dados PostgreSQL, que é o gerenciador de banco de dados implementado no projeto de VoIP. O PostgreSQL está conectado ao FreeRADIUS, para que as informações disponibilizadas em cada ligação, sejam armazenadas no banco de dados a todo tempo.

Atualmente o sistema VoIP permite a realização de chamadas telefônicas, tanto SIP como H.323, da rede de dados UFLA para a rede pública (PSTN). Isto é feito por meio de uma conexão do sistema VoIP com o sistema de telefonia tradicional.

O funcionamento deste processo até o momento de autenticação/autorização e contabilidade e armazenamento de estatísticas das chamadas é igual aos modelos que foram descritos anteriormente, porém tanto o servidor proxy SER e o Gatekeeper GnuGK usarão o Asterisk. O Asterisk servirá como um gateway dos servidores SIP e H.323, para a PSTN. Para isso será necessário o uso de uma interface física de conexão de redes, conectada na central telefônica da instituição. Esta interface será configurada para funcionar juntamente com o Asterisk. Desta forma é possível a conexão com a central telefônica da UFLA, e respectivamente ser feito ligações externas usando o sistema VoIP atual.

5.3. PLANO DE NUMERAÇÃO

Um plano de discagem ou plano de numeração descreve os aspectos de endereçamento e roteamento na rede telefônica. O plano identifica números telefônicos que estão associados a regiões e a maneira como é feito o roteamento, por exemplo, por meio de prefixos.

5.3.1. E.164

Existe uma recomendação da ITU-T, denominada de E.164, que define o plano de numeração internacional utilizado na telefonia (PSTN) e em algumas redes de dados. Essa recomendação especifica o formato, a estrutura e a hierarquia administrativa dos números de telefone para três categorias: Áreas Geográficas, Serviços globais e Redes.

A estrutura de números E.164 para áreas geográficas é mostrada na Figura 5.15, onde CC é o código do país; NDC código de destino nacional; SN número do assinante.

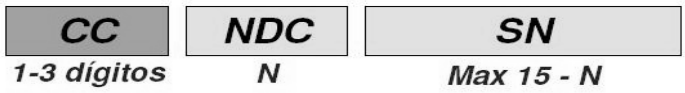


Figura 5.15 – Estrutura de números E.164
Fonte: RNP 2005 – Treinamento voip4all

ENUM (*Eletronic Number Mapping*) é um protocolo padrão IETF que mapeia números de telefone da PSTN em serviços Internet, independente do protocolo de sinalização. A RFC 2916 mostra as facilidades para resolver números E.164, através de entradas no DNS. O domínio "e164.arpa" está sendo utilizado para prover armazenamento de números E.164. O Brasil já tem associado o prefixo cinqüenta e cinco.

O E.164 funciona da seguinte maneira. Associa-se um domínio ao número E.164 e o usuário é localizado por consulta ao DNS. O número E.164 pode representar tanto um telefone IP com um telefone real.

Quando se usa VoIP é associado o uso de DNS com SIP. A RFC 3263, especifica o DNS como mecanismo preferencial para determinar o endereço IP, porta e transporte do hospedeiro para o qual a requisição SIP é enviada. O transporte deve ser determinado, pois requisições SIP podem ser enviadas via UDP, TCP, SCTP ou TLS sobre TCP para sessões seguras e codificadas, diferentemente de outros protocolos mais limitados.

5.3.2. ESPECIFICANDO O PLANO DE NUMERAÇÃO

O Plano de Numeração é responsável em identificar o assinante (professor, aluno, funcionário). É possível que se tenham três configurações de ramais no PABX da instituição. Abaixo os três modelos de número, que pode ter um terminal VoIP.

- Formato internacional - 55 <área> <prefixo> <terminal>

  UFLA: 55 35 1183 xxxx
- Formato abreviado nacional

  UFLA: 0 35 1183 xxxx

- Formato abreviado local: Este formato não é utilizado no encaminhamento ao DGK e pode ser usado numa mesma área

  UFLA: 1183 xxxx

5.3.3. PREMISSAS DO SERVIÇO

Como premissas do serviço podemos citar: endereçamento por número telefônico E.164 e uso de gateways de voz com IVR (*Interactive Voice Response*) para interconectar com o PABX; encaminhamento de chamadas E.164 entre instituições feitas pela sinalização H.323 baseada em estrutura hierárquica com DGK.

5.3.4. RESTRIÇÕES DO PLANO DE NUMERAÇÃO

Algumas restrições foram criadas para que o serviço não seja usado de forma descontrolada, pois há uma legislação a ser seguida. Chamadas externas não são permitidas e para isso foi criado um marcador de chamadas externas, que tem algumas características específicas.

O serviço fone@RNP não pode ser usado pelo público para realizar chamadas de longa distância, começando e terminando na telefonia pública. Se a chamada for de origem externa, o destino desejado, se não for de terminal VoIP, é alterado com inclusão do “1”. Deixando a identificação da chamada dessa forma: 0 <código da área> 1 <número do assinante>. A instituição que recebe a chamada deve rejeitar a chamada que contiver o “1” extra se o destino for à rede pública de telefonia, isto é, se não for PABX ou linha privada da instituição.

5.4. CONCLUSÃO

Todos os softwares utilizados no sistema são freeware, softwares de qualidade e possuem interfaces para funcionarem em conjunto. Isto mostra que é muito viável para uma instituição a implantação do serviço VoIP, pois com um gasto mínimo de infra-estrutura e mão-de-obra, é possível criar um novo modelo de telefonia, que reduzirá os custos com chamadas telefônicas, quando comparado ao modelo tradicional PSTN.

Atualmente, o perfil de gasto telefônico de uma instituição típica indica que a maior parcela (em torno dos 60%) das ligações é direcionada para celulares locais. A proliferação de celulares em todas as camadas da população, muitas vezes usados apenas com o intuito de receber chamadas, é, no momento, o calcanhar-de-aquiles de qualquer instituição no Brasil [RNP, 2005].

6. CONCLUSÕES E TRABALHOS FUTUROS

Diferente de como muitos pensam, a tecnologia de VoIP não está relacionado apenas com transmissão de voz em tempo real, de PC para PC (MSN Messenger, Skype), é possível que exista uma comunicação mista, tanto de um telefone comum para PC, ou vice-versa. O uso do serviço de VoIP pela Universidade, fornece um melhor aproveitamento da estrutura da rede de dados já existente, além de reduzir gastos destinados as ligações telefônicas realizadas pelo modelo de telefonia tradicional.

Atualmente, o perfil de gasto telefônico de uma instituição típica indica que a maior parcela (em torno dos 60%) das ligações é direcionada para celulares locais. Com a proliferação de celulares em todas as camadas da população, muitas vezes usados apenas com o intuito de receber chamadas, este é, no momento, o ponto fraco de qualquer instituição no Brasil.

A tendência do projeto fone@RNP é evoluir de forma contínua, propiciando cada vez mais uma melhoria do serviço de VoIP e reduzindo custos e mão de obra para a sua manutenção.

Todos os softwares utilizados no sistema são *freeware*, softwares de qualidade e possuem interfaces para funcionarem em conjunto. Isto mostra que é muito viável para uma instituição a implantação do serviço VoIP, pois com um gasto mínimo de infra-estrutura e mão-de-obra, é possível criar um novo modelo de telefonia, que reduzirá os custos com as chamadas telefônicas, quando comparado ao modelo tradicional PSTN.

Podemos considerar que não só os protocolos de transporte (TCP/UDP) e os protocolos específicos da tecnologia de VoIP (SIP/H.323), são essenciais para uma transmissão de áudio em tempo real. Temos outros parâmetros a serem considerados para que uma transmissão de áudio seja de boa qualidade. Por exemplo algoritmos, juntamente com os codecs de áudio, que são responsáveis pela digitalização do áudio analógico, e desta forma desempenham um papel imprescindível no processo de transmissão de áudio. A QoS e segurança é um dos maiores desafios que especialistas, na área de telecomunicações, tem enfrentado, para se adquirir uma transmissão de boa qualidade e de forma segura como a telefonia tradicional, provocando incertezas em relação aos usuários em relação ao uso da tecnologia VoIP.

Como trabalhos futuros, pretendemos avaliar o sistema de VoIP implantado na Universidade, realizando chamadas telefônicas distintas. Podendo assim fazer uma análise da qualidade das chamadas, por meio da qualidade da voz.

REFERÊNCIAS BIBLIOGRÁFICAS

BRIAN, Arkills. LDAP Directories Explained, 1. ed. New York: Editora Addison Wesley, 2003. 432 p.

DOMINGUES, Miriam Lúcia Campos Serra. Protocolos de Dados Conferências Multimidia. 2000. Dissertação de Mestrado (Ciência da Computação) - Universidade Federal do Rio Grande do Sul, Porto Alegre.

GRAHAM, Barr em SITE OFICIAL PERL LDAP Documentation, [2003]. Disponível em: <http://ldap.perl.org/>. Acessado em 05 de março 2006.

GUIMARÃES, José Liesse Bollos. Voz sobre IP. Brasil, [1999]. Disponível em: <http://www.gta.ufrj.br/grad/98_2/liesse/relat.html>. Acessado em 18 de outubro 2005.

HERSENT, Oliver; GURLE, David; PETIT, Jean-Pierre. Telefonia IP: comunicação, multimídia baseada em pacotes. São Paulo: Makron Books, 2002. 451 p.

LOUREIRO, Hélio; SAVARIS, Nixon. Protocolos Internet para Comunicação Multimídia, Florianópolis, [1999]. Disponível em: <http://www.lcmi.ufsc.br/redes/redes99/helio/protocolos_multimidia/>. Acessado em 08 junho 2005.

NUNES, Mário Serafim. 4ª Parte - Voz Sobre IP. Disponível on-line em: <http://asterix.ist.utl.pt/ec-ris/textos-aulas/4a%20parte%20VoIP.pdf>. Acessado em 17 de janeiro 2006.

OLIVEIRA, Sérgio. Telefonia IP para ambientes móveis usáveis: Simpósio Brasileiro de Redes de Computadores, 19. 2001, Florianópolis: 2001. p. 542-558.

OLIVEIRA, Sérgio. Telefonia IP para ambientes móveis compactos, Belo Horizonte, [2001]. Disponível <http://www.lecom.dcc.ufmg.br/~sergiool/telefonia/telefoni.htm>. Acessado em 10 julho 2005.

[OpenLDAP Foundation (2004)] OPENLDAP FOUNDATION em SITE OFICIAL OPENLDAP. Manual Pages. Disponível em: http://www.openldap.org/software/man.cgi. Acessado em 02 março 2006.

PEREIRA NETO, Álvaro. PostgreSQL: Técnicas Avançadas - Versões Open Source 7.x 2ª ed. São Paulo: Editora Érica , 2003.

SHULZRINNE, Hennig. Object oriented VoIP library. Página pessoal, Columbia USA, nov. 2000. Disponível em: <http://www.cs.columbia.edu/~hgs/>. Acessado em 08 dezembro 2005.

TANENBAUM, Andrew S. Redes de Computadores, 4. ed. São Paulo: Editora Campus, 2003. 968 p.

THE POSTGRESQL GLOBAL DEVELOPMENT GROUP. Guia do Usuário do PostgreSQL 7.3.4. Disponível em: http://www.postgresql.org.br/usuario/ Acesso em: 25, nov. 2004.

SITES PESQUISADOS

Dígitro Tecnologia. Glossário Tecnológico. Coordenação Eng. Djan de Almeida do Rosário, desenvolvida por Adm. Claudio Brancher Kerber, apresenta termos tecnológicos na área de telecomunicações. Disponível em: http://www.portaldigitro.com.br/novo/glossario_digitro. Acessado em 20 março 2006.

ANATEL 1998. http://www.anatel.gov.br/index.asp?link=/biblioteca/editais/stfc/empresas espelho/edital.htm?Cod=98 CONCORRÊNCIA N.º 001/98/SPB/ANATEL EDITAL SERVIÇO TELEFÔNICO FIXO COMUTADO REGIÕES I, II, III e IV DO PLANO GERAL DE OUTORGAS - 25/03/06. Acessado em 10 de março 2006

http://en.wikipedia.org/wiki/Voice_over_IP#Functionality. Acessado em 08 fevereiro 2006.

http://www.gnugk.org/gnugk-manual-pt.html. Acessado em 11 fevereiro 2006.

http://www.rnp.br/backbone/index.php . Acessado em 13 março 2006.

http://www.gnugk.org/gnugk-manual-pt-1.html. Acessado em 13 março 2006

http://en.wikipedia.org/wiki/Asterisk_PBX#column-one. Acessado em 15 março 2006

http://www.freeradius.org/. Acessado em 14 março 2006

RFC3261. Disponível em ftp://ftp.rfc-editor.org/in-notes/rfc3261.txt. Aceassdo em 10 de março 2006.

RFC2865. Dipsonível em ftp://ftp.rfc-editor.org/in-notes/rfc2865.txt. Acessado em 06 de fevereiro de 2006.

RFC2916. Disponível em ftp://ftp.rfc-editor.org/in-notes/rfc2916.txt. Acessado em 03 de janeiro 2006

RFC3263. Disponível em ftp://ftp.rfc-editor.org/in-notes/rfc3263.txt. Acessado em 12 de março 2006.