FUNDAÇÃO DE ENSINO "EURÍPIDES SOARES DA ROCHA"
CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA – UNIVEM
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

GIULIANNA MAREGA MARQUES

UTILIZAÇÃO DE VOIP SOBRE PLATAFORMA OPEN SOURCE

MARÍLIA
2005

GIULIANNA MAREGA MARQUES

UTILIZAÇÃO DE VOIP SOBRE PLATAFORMA OPEN SOURCE

Trabalho de Conclusão de Curso (TCC), apresentado ao Centro Universitário Eurípides de Marília – UNIVEM, mantido pela Fundação de Ensino Eurípides da Rocha, como requisito parcial para obtenção do Título de Bacharel em Ciência da Computação.

Orientador:
Prof°. Ms. Ricardo Petruzza do Prado

MARÍLIA
2005

GIULIANNA MAREGA MARQUES

UTILIZAÇÃO DE VOIP SOBRE PLATAFORMA OPEN SOURCE

Banca examinadora do Trabalho de Conclusão de Curso (TCC), apresentado ao Centro Universitário Eurípides de Marília – UNIVEM, mantido pela Fundação de Ensino Eurípides da Rocha – F.E.E.S.R, como requisito para obtenção do Título de Bacharel em Ciência da Computação.

Nota: 9,0 (Nove)

Orientador: Ricardo Petruzza Do Prado

1º Examinador: Marcos Luiz Mucheroni

2º Examinador: Marcos Roberto Bombacini

Marília, 05 de dezembro de 2005.

À Deus, pela serenidade, força e sabedoria atribuída a mim.

Ao meu namorado, por todo apoio, confiança e colaboração.

Aos meus amigos, pela confiança, paciência e incentivo.

Aos professores, pelas experiências compartilhadas.

À minha família, pela motivação, confiança
e ensinamentos que me auxiliaram no
crescimento pessoal e profissional.

A todos que colaboraram com o
desenvolvimento deste trabalho.

Faz da tua alma um diamante.

Por cada novo golpe uma nova face,

para que um dia ela seja toda luminosa.

(Rogelio Stela Bonilla)

RESUMO

A convergência de tecnologias, o grande crescimento da implantação de redes IP, tanto local como remota, e o desenvolvimento de técnicas avançadas de digitalização de voz, mecanismos de controle, priorização de tráfego e protocolos de transmissão em tempo real, assim como o estudo de novos padrões que permitam a qualidade de serviço em redes IP, tem criado condições em que há possibilidade de transmissão de voz sobre IP. O VoIP tem o auxilio do padrão H.323 para estabilizar conexões multimídia, e este, possui um elemento chamado *Gatekeeper,* o qual é considerado um dos elementos mais importantes do padrão, pois possui suporte a aplicações de videoconferência e de voz sobre IP. O trabalho visou demonstrar evolução das tecnologias utilizadas para implementação e implantação de VoIP, suas arquiteturas, seus padrões, cita detalhes sobre qualidade de serviço em telefonia IP, e abordou as vantagens de utilizar plataformas *open source*.

Palavras-Chave: VoIP. Padrão H.323. *Gatekeeper.*

ABSTRACT

The dawn of technology's convergence, the IP networks' implementation growth, local and remote, and the development of advanced techniques of voice digitalization, control mechanisms, traffic prioritization and real time transmission protocols, the study of new standards that allows quality in IP network services, bring conditions for voice over IP transmissions. VoIP is supported by the H.323 standard for stable multimedia connections, and it has an element called Gatekeeper, that acts as the manager of all the calls inside a determined H.323 zone. It's considered one of the most important elements of the standard, because it supports videoconference and voice over IP applications. The work bellow demonstrates the evolution of technologies in use for VoIP implementation, their architectures and standards, showing QoS details in IP telephony, and explains the advantages of open source platforms for that matter.

Keywords: VoIP. H.323. *Gatekeeper.*

LISTA DE ILUSTRAÇOES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CODEC	*Encoder-Decoder*
ACF	*Admission Confirmation*
ARJ	*Admission Rejection*
ARQ	*Admission Request*
ATA	*Analog Telephone Adaptor*
ATM	*Asyncronous Transfer Mode*
AVT	*Audio/Video Transport*
CoS	*Class of Service*
DARPA	*Advanced Research Projects Agency*
DNS	*Domain Name System*
DoS	*Denial of Service*
DRQ	*Disengage Request*
DSL	*Digital Subscriber Line*
EAD	*Distance Learning*
FDDI	*Fiber Distributed Data Interface*
FPC	*Flexible PIC Concentrator*
FTP	*File Transfer Protocol*
GCF	*Gatekeeper Confirmation*
GK	*Gatekeeper*
GRJ	*Gatekeeper Rejection*
GRQ	*Gatekeeper Request*

HDLC	*High-level Data Link Control*
HTTP	*Hypertext Transfer Protocol*
IETF	*Internet Engineering Task Force*
IMTC	*International Multimedia Teleconferencing Consortium*
IP	*Internet Protocol*
ISDN	*Integrated Services Digital Network (ver RDSI)*
ISO	*Intenational Standards Organization*
ITU	*International Telecommunications Union*
LAN	*Local Area Network*
LD-CELP	*Low-Delay Code Excited Linear Prediction*
MAN	*Metropolitan Area Network*
MB	*Megabytes*
Mb	*Megabit*
MCU	*Multipoint Control Unit*
MGCP	*Media Gateway Control Protocol*
MPL	*Mozilla Public License*
MTP	*Message Transfer Part*
OSI	*Open System Interconnetion*
P2P	*Peer-to-peer*
PABX	*Private Automatic Branch Exchange*
PBX	*Private Branch Exchange*
PC	*Personal Computer*
PCM	*Pulse Code Modulation*

POP3	*Post Office Protocol*
PPP	*Point-to-Point Protocol*
PSTN	*Public Switched Telephone Network*
PVC	*Permanent Virtual Circuit*
QoS	*Quality of Service*
RAS	*Registration Admission and Status*
RDSI	*Redes Digitais de Serviços Integrados*
RED	*Random Early Detection*
RFC	*Request for Comments*
RRQ	*Registration Request*
RSVP	*Resource Reservation Protocol*
RTCP	*Real-time Transport Control Protocol*
RTP	*Real-time Transport Protocol*
RTPC	*Rede de Telefonia Pública Comutada*
SDP	*Session Description Protocol*
SigTran	*Signaling Transport*
SIP	*Session Initiation Protocol*
SLA	*Service-Level Agreement*
SLIP	*Serial Line Internet Protocol*
SMTP	*Simple Mail Transfer Protocol*
SS7	*Signaling System Seven*
SSP	*Signaling Switch Point*
STFC	*Serviço Telefônico Fixo Comutado*

STP	*Signal Transfer Points*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
UML	*Unified Modelling Language*
URL	*Universal Resource Locator*
URQ	*Unregister Request*
VOCODER	*Voice coder-decoder*
VoIP	*Voice over IP*
WAN	*Wide Area Network*

SUMÁRIO

INTRODUÇÃO

Desde a criação do telégrafo por volta de 1830, para cada nova mídia de comunicação adotada era criada uma rede distinta para torná-la disponível a seus usuários. Com evolução da Internet houve um grande desenvolvimento de novas tecnologias que fossem capazes de suportar o grande tráfego de informações sob vários formatos (dados, voz e vídeo), originado em diferentes topologias de rede, desde pequenas LAN's (*Local Area Network*) até WAN´s (*Wide Area Network*).

A utilização de redes distintas para transmissão de cada formato de informação, tornou-se algo de difícil administração, além de exigir um grande investimento de capital para estruturá-las.

Para facilitar a interação de informações, reduzir custos, e gerenciar segurança, a convergência de tecnologias tornou-se uma opção vantajosa para as empresas estruturarem suas redes corporativas. A convergência é um tema discutido desde os anos 80, quando foi reconhecida pela primeira vez a importância e necessidade da comunicação entre computadores.

Com a digitalização da rede de telefonia, a voz passou a ser transmitida como dados entre as centrais telefônicas, mantendo-se a rede de terminais analógicos para os usuários finais. Para a extensão do canal de voz digital até o usuário final, substituindo seu antigo telefone analógico por um aparelho digital, foi proposta a criação da Rede Digital de Serviço Integrados (RDSI, em inglês seria ISDN), que levaria ao usuário uma única conexão (digital), podendo ser usada indistintamente para voz (telefonia) e comunicação de dados até 128 Kbps (kilobits por segundo).

Quando a criação da rede RDSI foi proposta, os *modems* da época possuíam velocidades baixas, devido a isso, ficou disponível ao mercado apenas no final dos anos 90, quando já existiam *modems* de 56 Kbps e alternativas ainda mais rápidas.

O grande crescimento da implantação de redes IP (*Internet Protocol* ou Protocolo Internet), tanto local como remota, e o desenvolvimento de técnicas avançadas de digitalização de voz, mecanismos de controle, priorização de tráfego e protocolos de transmissão em tempo real, assim como o estudo de novos padrões que permitam a qualidade de serviço em redes IP, tem criado condições onde há possibilidade de transmissão de voz sobre IP. A seção 1.3 faz a explanação sobre o assunto.

Voz sobre IP (VoIP) é uma tecnologia que permite a digitalização e codificação da voz e o empacotamento destes dados em pacotes IP para transmissão em uma rede que utilize o protocolo TCP/IP (*Transmission Control Protocol/ Internet Protocol* – Protocolo de Controle de Transmissão/ Protocolo Internet).

As soluções VoIP vão desde a simplicidade e eficiência dos comunicadores por voz, que realizam o bate-papo gratuito e em bom som a qualquer distância, até sistemas que dispensam o computador e permitem telefonar para outra cidade, país ou continente com tarifas abaixo do custo das operadoras de telefonia convencional, conforme a explanação na seção 1.1.

As principais formas de comunicação VoIP podem envolver softwares, hardwares especiais e até mesmo as operadoras de telefonia convencional. Em alguns casos, não é necessário um computador para falar pela Internet, basta tirar o aparelho de telefone do gancho e discar.

O VoIP tem o auxílio do padrão H.323 para estabilizar conexões multimídia. Desde sua primeira especificação em 1996, englobou e ainda engloba uma grande variedade de aplicações multimídia.

No capítulo 2 é enfatizado este elemento mais importante do padrão H.323, o *Gatekeeper*, o qual age como um ponto central para todas as chamadas dentro de uma determinada zona H.323. E essa alcunha se deve a inúmeros fatores, que de fato são muito importantes em aplicações de videoconferência e de voz sobre IP.

O trabalho a seguir demonstra a evolução das tecnologias utilizadas para implementação e implantação de VoIP, suas arquiteturas, seus padrões, cita detalhes sobre qualidade de serviço em telefonia IP, e aborda as vantagens de utilizar plataformas *open source.*

1 FUNDAMENTAÇÃO CONCEITUAL

São abordados neste capítulo conceitos sobre a tecnologia VoIP, suas arquiteturas, e os modelos de referencia OSI e TCP/IP, devido ao fato da importância destes conceitos para o entendimento do projeto.

1.1 Voz sobre IP

A tecnologia Voz sobre IP, cujo nome deriva do inglês *Voice over Internet Protocol* (VoIP), consiste em transmissão de voz em uma rede TCP/IP em forma de pacotes de dados IP.

A telefonia convencional conhecida como RTPC (Rede de Telefonia Pública Comutada) ou STFC (Serviço Telefônico Fixo Comutado), utiliza comutação de circuitos (*Circuit Switching*) para estabelecer uma conexão, e o VoIP tem como vantagem a utilização de comutação de pacotes (*Packet Switching*).

Para esclarecer qual é a vantagem de se utilizar à comutação de pacotes, é necessário ter conhecimento das diferenças básicas entre ambas as formas de comutação, conforme ilustra a Figura 1.

Em uma rede STFC, ao efetuar uma ligação, é estabelecida uma conexão física com o circuito, e esta, permanece ativa durante toda a chamada, mesmo que não haja conversação. Isso torna impossível que outros usuários usem esta conexão durante os momentos vagos. Já na telefonia com comutação por pacotes, não existe um circuito dedicado entre dois pontos, os dados de voz são convertidos em pacotes à medida que vão

sendo criados e são transmitidos pelo caminho disponível na rede naquele instante. Os pacotes podem seguir caminhos diferentes pela rede, mas todos chegarão ao destino pelo caminho livre naquele instante (PENNO, 1999).

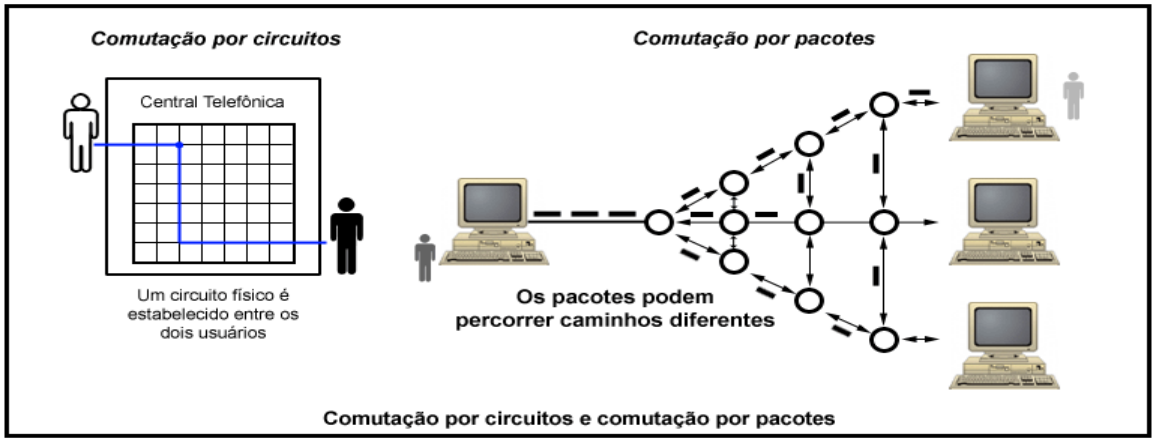


Figura 1: Comutação por circuitos e comutação por pacotes (PENNO, 1999)

Outras vantagens:

- Convergência de redes (dados, voz e vídeo);
- Utilização de *softphones* – uso em PC;
- Utilização de *hardphones* – telefone IP;
- Entroncamento IP entre os PABXs;
- Expansão da opção de comunicação de voz além dos limites do PABXs;
- Custo reduzido em ligação DDD e DDI;
- Largura de banda mínima através de compressão (*codec*);
- Amortização dos investimentos em poucos meses.

Pode-se dizer que a arquitetura de VoIP ainda está em desenvolvimento e não existe uma padronização de protocolos e equipamentos como na telefonia fixa, o que pode acarretar algumas dificuldades ou mesmo algumas desvantagens, mas que tendem a serem sanadas proporcionalmente com sua popularização e evolução.

Algumas desvantagens:

- Dependendo dos recursos utilizados, a voz fica metalizada;
- Atrasos de pacotes (problemas de *bufferização* dos equipamentos);
- Os dispositivos VoIP possuem valores elevados (exemplos: telefones IP e *gateways*);
- Não possui regulamentação.

Conforme o Coordenadoria de Tecnologia da Informação da USP, para evitar maiores problemas com estas desvantagens e obter uma boa comunicação utilizando rede VoIP, deve-se seguir as seguintes condições (CTI USP, 2005):

- *Delay* < 150ms;
- *Jitter* < 30ms - atraso excessivo da voz;
- Perda de Pacotes < 1% - eco;
- Largura de Banda:
  - 18 Kbps para *codec* G.723.1;
  - 70,2 a 82,7 Kbps para *codec* G711;
  - 7,3 a 36 Kbps para *codec* G729a;

Os ítens anteriores são abordados com mais detalhes no capítulo 3, e a seguir serão apresentadas as principais arquiteturas básicas aplicadas a VoIP.

1.2 Arquiteturas Básicas

O VoIP possui três arquiteturas básicas, que são descritas a seguir.

1.2.1 Arquitetura PC a PC

A porta de entrada para a telefonia pela Internet são os comunicadores com recurso de conversa com voz, como *Skype, MSN Messenger, Yahoo! Messenger e ICQ*. Todos são gratuitos e fáceis de usar, basta instalar o software desejado em um PC (*Personal Computer*) que possua microfone e alto-falantes e criar uma conta no respectivo serviço, para conversar pela Internet com outros usuários do programa a custo zero.

O microfone e alto-falantes podem ser substituídos ou utilizados juntos com um *headset*, peça que combina fone de ouvido e microfone para deixar as mãos livres, ou com *handset*, acessórios com o formato de um fone de um aparelho telefônico normal ou mesmo de um celular, como pode ser visto na Figura 2.

Uma conexão em banda larga não é obrigatória para a conversa pelos comunicadores, mas é desejável. Afinal, a qualidade da ligação depende diretamente das condições da conexão dos usuários que estão nos dois lados da linha. Em banda estreita, o atraso ou perda dos pacotes de dados pode causar ruídos e interferências no som. Como o

tráfego da voz convertida em dados é feito integralmente pela Internet, não há qualquer tipo de tarifa.

Nesta arquitetura a conexão é *Peer-to-peer* (Ponto a Ponto), todo o tratamento de voz (amostragem, compressão e empacotamento) ocorre nos PCs. As chamadas de voz são estabelecidas com base no endereço IP do receptor ou nomes associados que serão convertidos para endereço IP.

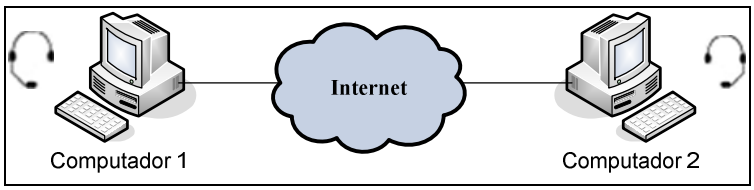


Figura 2: Arquitetura PC a PC

1.2.2 Arquitetura Gateway

Telefonar do computador para um número da rede telefônica convencional, isto é, para um telefone fixo ou celular, é possível, mas não é gratuito. A vantagem é que, dependendo do destino da chamada, a tarifa da ligação é muito mais baixa do que as cobradas pelas operadoras de telefonia de longa distância. Para fazer ligações por VoIP do computador para telefones convencionais, é necessário algum serviço como o *SkypeOut* (SkypeOut, 2005), *Net2Phone* (Net2Phone, 2005) e *Nikotel* (Nikotel, 2005), instalar o programa recomendado e comprar créditos para o pagamento das ligações.

Nessa modalidade de VoIP, a chamada feita do computador do usuário é roteada através do provedor VoIP pela Internet até o ponto mais próximo possível de seu destino,

neste ponto, através de um *gateway*, ela é transformada em voz e transferida para a rede STFC, que completa a chamada para o aparelho fixo ou celular da pessoa desejada.

Alguns serviços como o *SkypeIn* (SkypeIn, 2005) e o *WebFone* Virtual, da GVT (GVT, 2005), também permitem receber no computador ligações originadas em telefones fixos ou celulares, é como se o usuário comprasse uma linha telefônica virtual com número.

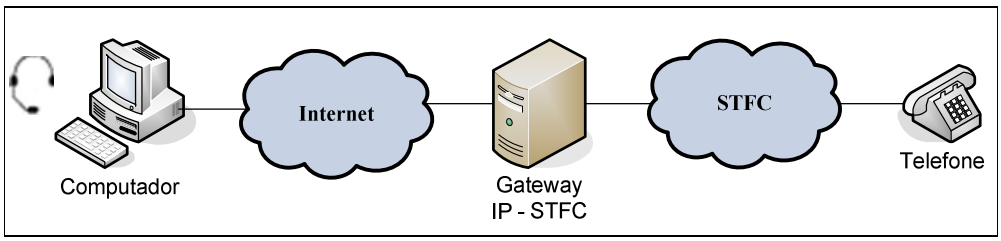


Figura 3: Interconexão da rede IP com a STFC

1.2.3 Arquitetura Híbrida

A arquitetura hibrida tem como característica ser utilizada, na maioria das vezes, em redes corporativas, pois o custo entre filiais pode chegar à zero, dependendo do acordo feito com a operadora de telefonia IP adotada, além de disponibilizar valores mais acessíveis, comparado às operadoras de telefonia convencional, para ligações interurbanas e internacionais, assim o valor do investimento será retribuído com a economia gerada ao longo do tempo.

A transmissão de pacotes pode utilizar LANs, rede Internet, e a rede STFC, e as opções de comunicação disponíveis são: através do computador, utilizando de softwares conhecidos como *softphones*, pelo telefone IP, telefone comum conectado a um adaptador

chamado ATA (*Analog Telephone Adaptor*), ou mesmo, através do PABX (*Private Automatic Branch eXchange*). A Figura 4 demonstra a estrutura destas opções.

O telefone IP traz embutido o programa e as configurações do serviço VoIP, e quando conectado no modem de banda larga ou no roteador, oferece uma grande facilidade de utilização, pois é só retirar o fone do gancho para atender ou iniciar uma ligação.

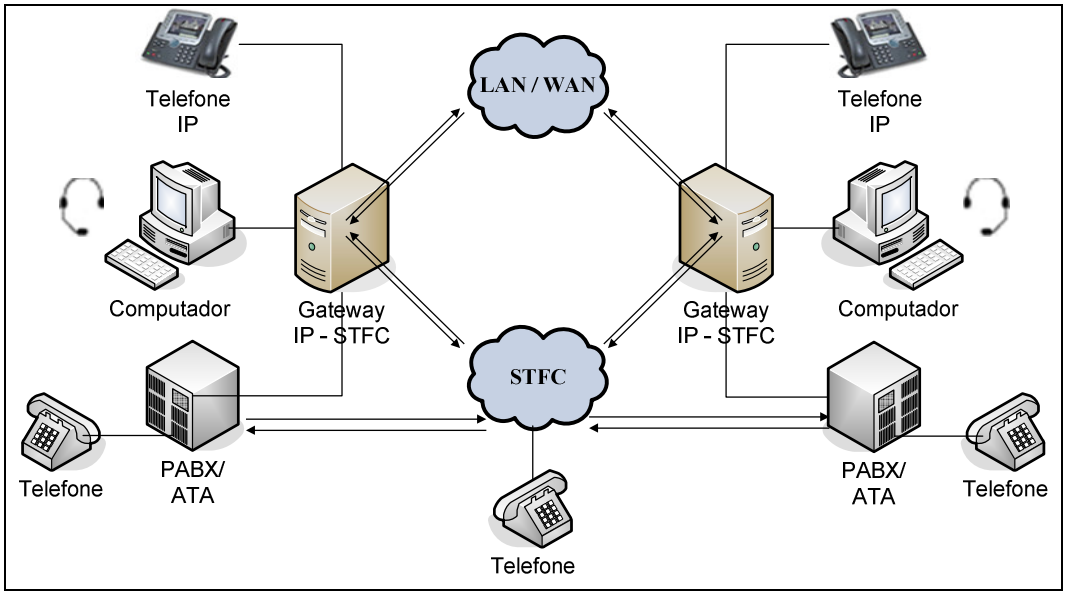


Figura 4: Arquitetura Híbrida

Os ATAs são adaptadores que devem ser conectados no modem de banda larga ou no roteador e a um aparelho de telefone normal, que passará a ser utilizado para fazer e receber as ligações pela rede IP. O ATA é de fácil transporte devido seu tamanho reduzido, e esta vantagem pode-se aplicar a quem viaja e se hospeda em um hotel com acesso a banda larga nos quartos, basta conectar o ATA ao ponto de rede, e no mesmo, o aparelho de telefone comum, com isso o usuário estará conectado a um ramal VoIP de sua empresa no local de hospedagem.

Devido ao crescimento das soluções de telefonia IP, órgãos internacionais desenvolveram padrões para permitir a interoperabilidade entre implementações de desenvolvedores diferentes. No cenário mundial, o padrão ITU H.323 é o mais utilizado pelas aplicações de voz, descrito no capítulo 2.

1.3 Modelos de Referências OSI e TCP/IP

O modelo de referência serve como uma diretriz útil para dividir tarefas de comunicação, e reduzir a complexidade no projeto de protocolos. Antes cada fabricante tinha seu próprio protocolo que muitas vezes não era compatível, impossibilitando a interoperabilidade.

Protocolos são regras e convenções utilizadas pelos dispositivos de rede de modo que eles consigam se entender, isto é, trocar informações entre si.

Para descrever a arquitetura do conjunto de protocolos da Arquitetura TCP/IP geralmente é utilizado um modelo conceitual de camadas. As camadas interagem somente com as camadas diretamente ligadas a ela, imediatamente acima e imediatamente abaixo.

Existem dois modelos que fazem a organização de camadas: o modelo OSI de sete camadas da ISO (*International Standards Organization*) e o modelo DARPA de quatro camadas.

1.3.1 Modelo ISO/OSI

Para facilitar a interconexão de sistemas de computadores, a ISO (*International Standards Organization*) desenvolveu um modelo de referência chamado OSI (*Open System Interconnetion*), para que os fabricantes pudessem criar protocolos a partir desse modelo (TANENBAUM, 2003).

Este modelo trata da interconexão de sistemas abertos à comunicação com outros sistemas, na transmissão de um dado, cada camada pega as informações passadas pela camada superior, acrescenta informações pelas quais ela seja responsável e passa os dados para a camada imediatamente inferior, esse processo é conhecido como encapsulamento.

Conforme a Tabela 1, o modelo OSI possui sete camadas conhecidas como:

Tabela 1: Modelo de Referência OSI (TANENBAUM, 2003).

7	Aplicação
6	Apresentação
5	Sessão
4	Transporte
3	Rede
2	Enlace
1	Física

Camada 1- Física: trata da transmissão de sinais elétricos ou pulsos de luz através de um canal de comunicação;

Camada 2- Enlace de Dados: transforma um canal de comunicação em uma linha livre de erros para a transmissão transformando os dados em quadros;

Camada 3- Rede: controla o modo como os pacotes são roteados da origem ao destino;

Camada 4- Transporte: divide os dados em unidades menores para passá-los à camada de rede garantindo que cheguem corretamente à outra extremidade;

Camada 5- Sessão: permite que usuários de diferentes máquinas estabeleçam sessões entre si;

Camada 6- Apresentação: codifica os dados conforme a sintaxe e semântica das informações transmitidas;

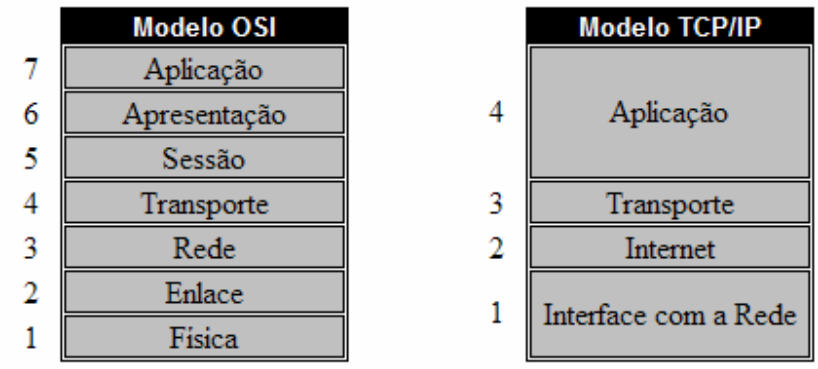
Camada 7- Aplicação: responsável pelas aplicações específicas do protocolo.

O modelo OSI acabou servindo de base para a criação de outros protocolos. Embora seja mundialmente reconhecido, o padrão aberto e histórico da Internet é o TCP/IP.

1.3.2 Modelo TCP/IP

O modelo TCP/IP constitui uma arquitetura de camada especificada pela *Internet Enginnering Task Force* (IETF) e patrocinada *pela Advanced Research Projects Agency* (DARPA) modelado em um conjunto de quatro camadas.

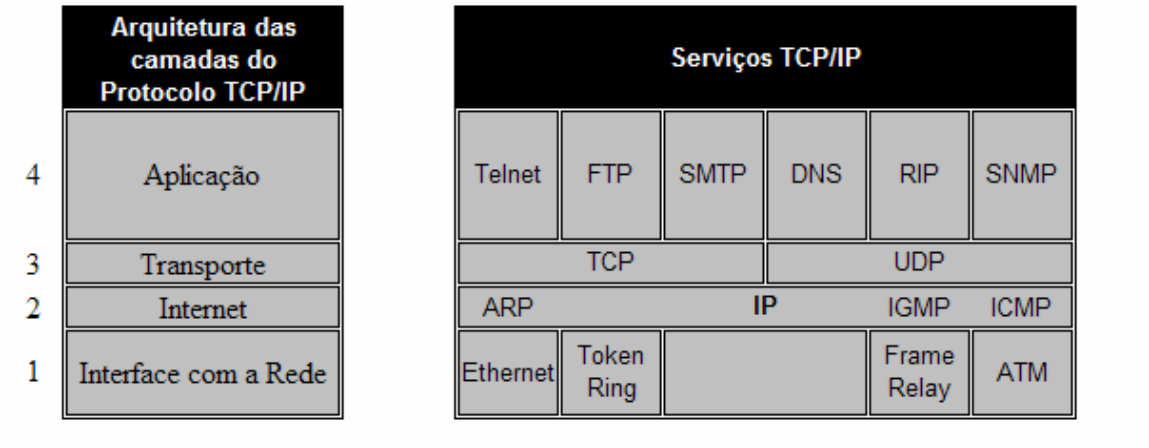
Tabela 2: Modelo OSI comparado ao modelo TCP/IP (TANENBAUM, 2003)



O nome TCP/IP é originário dos nomes dos protocolos mais importantes desta pilha: *o Internet Protocol* (IP) e o *Transmission Control Protocol* (TCP). O modelo TCP/IP quando comparado com o modelo OSI, tem duas camadas que se formam a partir da fusão de algumas camadas, são elas: as camadas de Aplicação (Aplicação, Apresentação e Sessão) e Rede (Link de dados e Física). Pode ser visto na Tabela 2 a comparação

A Tabela 3, ilustra o modelo TCP/IP com suas camadas, seus protocolos e sua ligação física, e em seguida, tem-se uma breve explicação de cada uma delas:

Tabela 3: Arquitetura e Serviços do modelo TCP/IP



Camada 1- Interface com a Rede:

Esta camada é equivalente às camadas 1 e 2 (Física e Enlace) do modelo OSI, considerada camada de abstração de hardware, é responsável por enviar o datagrama recebido pela camada de Internet em forma de um quadro através de diversos tipos de redes (X.25, ATM, FDDI, Ethernet, Token Ring, Frame Relay, PPP e SLIP). Por causa da grande variedade de tecnologias de rede, ela não é normatizada pelo modelo, o que provê a possibilidade de interconexão e interoperação de redes heterogêneas.

Camada 2- Internet:

Essa camada é a primeira normatizada do modelo, é responsável pelo endereçamento, roteamento e controle de envio e recepção. Ela não é orientada à conexão, se comunica através de datagramas. O protocolo IP situa-se nesta camada. É o protocolo responsável pelo roteamento e controle de congestionamento. Seu objetivo é a entrega dos pacotes a qualquer destino independente da tecnologia de transmissão utilizada.

Camada 3- Transporte:

Camada fim-a-fim, considerada uma entidade desta camada que só se comunica com a sua entidade-par do *host* destinatário. É nesta camada que se faz o controle da conversação entre as aplicações intercomunicadas da rede. Reúne os protocolos que realizam as funções de transporte de dados, que consideram apenas a origem e o destino da comunicação, sem se preocupar com os elementos intermediários. A camada de transporte possui dois protocolos: o *User Datagram Protocol* (UDP) e *Transmission Control Protocol* (TCP).

O protocolo UDP não possui confirmação de entrega dos dados, isto é, não é orientada a conexão. Já o protocolo TCP possui uma série de funções para tornar a comunicação entre origem e destino mais confiável, isto é, orientado a conexão. O acesso das aplicações à camada de transporte é feito através de portas que recebem um número inteiro para cada tipo de aplicação.

Camada 4- Aplicação:

É formada pelos protocolos utilizados pelas diversas aplicações do modelo TCP/IP, fornecem serviços de comunicação ao sistema ou ao usuário. Os serviços definidos

utilizam a arquitetura de distribuição cliente-servidor. Os servidores são processos que oferecem o serviço e estabelecem um endereço (*host, port*) para sua disponibilização. Não possui um padrão comum, o padrão é estabelecido por cada aplicação, isto é, o FTP (File Transfer Protocol) possui seu próprio protocolo, assim como o TELNET, SMTP (Simple Mail Transfer Protocol), HTTP (Hypertext Transport Protocol), POP3 (Post Office Protocol), DNS (*Domain Name System*) entre outros.

Como visto na seção 1.1, o VoIP é uma tecnologia que permite a digitalização e codificação da voz e o empacotamento de dados em pacotes IP para transmissão em uma rede que utilize o protocolo TCP/IP. O TCP é um protocolo da camada de transporte confiável, ele é baseado em conexão encapsulada no IP. O TCP garante a entrega dos pacotes, assegura o "seqüenciamento" dos pacotes, e providencia um *checksum* que valida tanto o cabeçalho, quanto os dados do pacote. No caso da rede perder ou corromper um pacote TCP/IP durante a transmissão, é tarefa do TCP retransmitir o pacote faltoso ou incorreto. Essa confiabilidade torna o TCP/IP o protocolo escolhido para transmissões baseadas em sessão, aplicativos cliente-servidor e serviços críticos.

Os cabeçalhos dos pacotes TCP requerem o uso de bits adicionais para assegurar o correto "seqüenciamento" da informação, bem como um *checksum* obrigatório para garantir a integridade do cabeçalho e dos dados. Para garantia da entrega dos pacotes, o protocolo requisita que o destinatário, informe através do envio de um *acknowledgement*, para que seja confirmado o recebimento.

O protocolo UDP é a segunda opção da camada de transporte, sendo que ele não é confiável, pois não implementa *acknowledgements*, "janelas" e nem "seqüenciamentos", o único controle feito é um *checksum* opcional que está dentro do seu próprio *header* (cabeçalho), ele é utilizado por aplicações que não vão gerar altos volumes de tráfego na

Internet.

O IP é o protocolo da camada Internet. Ele é encarregado da entrega de pacotes para todos os outros protocolos da família TCP/IP. Ele oferece um sistema de entrega de dados sem conexão. Isto é, os pacotes IP não são garantidos de chegarem ao seu destino, nem de serem recebidos na ordem em que foram enviados. O *checksum* do IP confirma apenas a integridade do cabeçalho do pacote.

O endereço IP é formado por um número de 32 bits no formato "nnn.nnn.nnn.nnn" onde cada "nnn" pode variar de 0 até 255 (1 octeto = 8 bits). Os endereços possuem uma classificação que varia de acordo com o número de sub-redes e de *hosts*. Tal classificação tem por finalidade otimizar o roteamento de mensagens na rede.

Mais informações e detalhes sobre os modelos e funcionalidades podem ser encontrados em materiais complementares a este.

2 PADRÃO MULTIMÍDIA H.323

Antigamente, no início das redes de computadores, as necessidades de utilização estavam ligadas diretamente ao transporte puro e simples de dados e informações. Com a melhoria gradativa da qualidade dessas redes, novas aplicações foram surgindo. Uma delas é referente ao transporte de informações em tempo real.

Segundo Comer, (COMER, 1998) as "novas aplicações" sobre redes de comutação de pacotes, referindo-se principalmente as redes TCP/IP, trazem inúmeros problemas, tendo em vista que suas estruturas básicas não foram projetadas para esse fim. Mesmo com a evolução das redes TCP/IP e das demais redes de comutação de pacotes, ainda existem muitos problemas relacionados ao transporte de dados quando esses são sensíveis ao atraso. De fato, a evolução propriamente dita foi mais no aspecto da velocidade e eficiência da transmissão, que na maneira como a transmissão ocorre. O envio de informações na rede Internet continua tendo como princípio a simples emissão de dados de uma parte a outra, não importando por onde eles passem. Caso algum caminho esteja congestionado, os dados devem percorrer uma rota alternativa que os levem ao destino desejado. Em qualquer circunstância, em cada nó da rede, todos os pacotes são transmitidos ao próximo nó na maior velocidade possível, obedecidas às restrições de capacidade do enlace de saída, capacidade de armazenamento e processamento desses pacotes (COMER, 1998).

Em outras palavras, redes que possuem esse princípio de transmissão, como as redes TCP/IP, são baseadas na idéia do "melhor esforço".

Quando começou a se pensar em transmitir outros tipos de informações sobre a rede que não fossem meramente dados, como voz e vídeo em tempo real, mecanismos alternativos tiveram de ser implementados a fim de adaptar a rede TCP/IP e o paradigma de

“melhor esforço”, a transmitir esse tipo de informação. Essa adaptação é necessária, tendo em vista que voz e vídeo possuem outros requisitos de transmissão diferentes daqueles originalmente ligados ao simples envio de dados. Tais requisitos são decorrentes da natureza de “tempo real” das comunicações por voz e vídeo presentes em algumas aplicações, sendo os mais importantes deles: a necessidade de largura de banda mínima e a manutenção de atrasos constantes e perdas reduzidas. Ou seja, um fluxo de dados de voz ou vídeo necessita chegar o mais próximo possível, no receptor, dos moldes em que foram criados.

Para solucionar os problemas referentes à transmissão de informações em tempo real, têm-se utilizado canais de transmissão dedicada de dados, onde apenas o tráfego de voz e vídeo de uma videoconferência, por exemplo, estará presente. Na prática, essa solução propicia uma ótima qualidade da transmissão desses dados, porém vem se apresentado como uma alternativa muito cara para a maior parte dos usuários de serviços de tempo real.

Outra solução, muito mais acessível, é utilizar toda a estrutura das redes TCP/IP já instaladas para transmissão dos dados em questão. Porém, como já mencionado anteriormente, essas redes são do tipo “melhor esforço”, ou seja, inadequadas à transmissão de voz e vídeo em tempo real: nessas redes, esses pacotes de mídia não teriam nenhuma prioridade de processamento e transmissão em relação aos outros dados não sensíveis ao atraso.

Para tratar dos problemas supracitados, muitos estudos sobre este tema foram e ainda são feitos com o intuito de melhorar, num aspecto global, a transmissão dos dados sensíveis ao atraso em redes TCP/IP. Como resultado, muitos padrões foram elaborados para permitir a viabilidade de aplicações como VoIP e videoconferência sobre IP. Órgãos

relacionados à área, como o *International Telecommunication Union* (ITU), e muitas universidades, especificam e elaboram padrões que são utilizados para transmissão de dados em tempo real. Entre esses padrões destacam-se aqueles da série H do ITU-T (subgrupo do ITU), como o padrão H.323, destinado às comunicações multimídias sobre a Internet.

O H.323 é uma recomendação do ITU para transmissão de voz e vídeo sobre redes TCP/IP, mais precisamente sobre aquelas redes que operem sobre *Ethernet, Fast Ethernet, Gibabit Ethernet e Token Ring*. Esse padrão foi aprovado em 1996 pelo grupo de estudos 16 do ITU.

Devido à necessidade de um padrão para voz sobre IP, o H.323 foi revisado e surgiu a versão 2, adotada em janeiro de 1998. Na versão 3, foi adicionado suporte à comunicação *Gatekeeper-Gatekeeper*, ao fax sobre redes de pacotes e aos mecanismos de conexão rápidos. A versão 4 teve como foco importantes áreas como confiabilidade, escalabilidade e flexibilidade. A versão 5 desse padrão possui poucas mudanças em relação a sua versão anterior, sendo a versão atual.

Tabela 4: Recomendações da ITU-T

RECOMENDAÇÕES ITU-T	
Caracteristicas de Sistemas de Telefonia Visual Infraestrutura de Serviços Audiovisuais	H.100–H.199
Geral	H.200–H.219
Transmissão, multiplexação e sincronização	H.220–H.229
Aspectos do Sistema	H.230–H.239
Procedimentos de comunicação	H.240–H.259
Codificação de video em movimento	H.260–H.279
Aspectos relacionados ao sistema	H.280–H.299
Sistemas e Equipamentos Terminais para Serviços Audiovisuais	H.300–H.399
Serviços Suplementares para Multimidia	H.450–H.499

A Tabela 4 possui alguns padrões do ITU-T (setor de padronização do ITU). Deve-se verificar que o padrão H.323 está localizado no grupo de padrões para serviços audiovisuais (multimídia). Outros padrões relacionados ao H.323, como o H.245, discutido na seção 2.2.2, também podem ser aqui localizados.

Concernindo agora os padrões para comunicações multimídia, podemos verificar na Tabela 5 a seguir os padrões do ITU utilizados para esses fins, destacando o H.323 como empregado nas redes TCP/IP.

Tabela 5: Padrões para comunicações multimídia

PADRÕES PARA COMUNICAÇÕES MULTIMIDIA		
Padrão	**Data**	**Descrição**
H.310	1996	Video conferência MPEG-2 sobre ATM com alta qualidade
H.320	1997	Video conferência sobre RDSI (Redes digitais de serviços integrados)
H.321	1996	Video conferência sobre ATM com boa qualidade
H.322	1996	Sistemas de video-fone para redes locais com qualidade de serviço
H.323	1996	Video conferência sobre redes TCP/IP sobre Ethernet e Token Ring
H.324	1996	Video Conferência sobre sistema telefônico

2.1 Características do padrão H.323

O padrão H.323 é completamente independente dos aspectos relacionados à rede. Dessa forma, podem ser utilizadas quaisquer tecnologias de enlace, podendo-se escolher livremente entre as que dominam o mercado atual como *Ethernet, Fast Ethernet*, FDDI, ou *Token Ring*. Também não há restrições quanto à topologia da rede, que pode consistir tanto de uma única ligação ponto a ponto, de um único segmento de rede, ou ainda serem complexas, incorporando vários segmentos de redes interconectados (HERSENT, 2002).

Conceitualmente, o padrão H.323 estabelece padrões para codificação e decodificação de fluxos de dados de áudio e vídeo, garantindo que produtos baseados no padrão H.323 de um fabricante opere com produtos H.323 de outros fabricantes.

A aplicabilidade desse padrão é muito extensa. Na verdade, o padrão H.323 consiste em uma solução baseada em padrões para sistemas de comunicação que inclui, desde uma simples telefonia ponto-a-ponto, até uma sofisticada conferência multimídia com compartilhamento de dados. Ele tem sido amplamente utilizado em aplicações de VoIP, videoconferência em *desktop*, computação colaborativa, ensino a distância, aplicações de *helpdesk* e suporte, e *shopping* interativo (RNP, 2005).

Uma das grandes vantagens do padrão H.323 é a sua flexibilidade, podendo ser aplicada tanto para voz quanto para vídeo. Dessa maneira, pode-se ter uma variedade de formas de comunicação, envolvendo áudio apenas (telefonia IP), áudio e vídeo (videoconferência), áudio e dados e, por fim, áudio, vídeo e dados.

O *International Multimedia Teleconferencing Consortium* (IMTC), uma organização que conduz testes de compatibilidade e interoperabilidade de produtos e serviços, estabeleceu um objetivo para assegurar vendedores de produtos e serviços que os mesmos sejam interoperáveis. Tal garantia é guiada pelo cumprimento das recomendações estabelecidas para o padrão H.323.

O H.323 é um padrão extremamente popular. As razões para isso são inúmeras e algumas delas são comentadas a seguir:

O H.323 define padrões de voz e vídeo para uma infra-estrutura existente (redes TCP/IP, mundialmente utilizadas) permitindo que os clientes possam usar aplicações sobre esses dados sem mudar a infra-estrutura de rede atual.

As redes baseadas em IP estão ficando mais velozes. Isso inclui redes locais dominantes do mercado, como a *Ethernet*, que estão aumentando sua largura de banda, formando as já conhecidas *Fast Ethernet e Gigabit Ethernet*. Dessa forma, as aplicações H.323 adquirem uma melhor qualidade, diminuindo a distância entre elas e as aplicações de padrões para redes com qualidade de serviço ou mesmo para canais dedicados.

O H.323 provê padrões de interoperabilidade entre LANs e outra redes, bem como suas aplicações. Além disso, o padrão é independente do tipo de enlace utilizado, como já mencionado.

O suporte à comunicação *multicast* reduz exigências de largura de banda. O padrão foi definido para que fosse totalmente destinado a aplicações *multicast*, embora também possa ser usada para tráfego *unicast*.

A especificação H.323 tem o apoio de muitas empresas de comunicação e organizações de informática em geral, incluindo a Intel®, Microsoft®, Cisco® e IBM®. Os esforços destas companhias estão gerando um nível mais alto de confiança no mercado em relação às aplicações de videoconferência e voz sobre redes TCP/IP.

O H.323 é independente de plataforma, possui suporte a gerenciamento de rede e suporte a conferência multiponto. Qualquer aplicação H.323 pode se comunicar com qualquer outra aplicação implementando este padrão, não importando a plataforma em que estejam. Além disso, as organizações envolvidas com o padrão implementam os elementos H.323 para todas as plataformas mundialmente difundidas, como Unix, Linux e Windows. Mesmo assim, as aplicações não comerciais estão abrindo o seu código fonte a qualquer um que queira implementar algum elemento H.323 em determinada plataforma não tão difundida, a ponto de possuir uma implementação oficial.

O padrão provê mecanismos de gerenciamento que permitem delimitar a quantidade de conferências simultâneas, bem como a quantidade de largura de banda destinada às aplicações H.323. Isso é necessário devido à característica de "consumidora de banda" das aplicações de tempo real.

O H.323 também provê mecanismos de contabilidade de uso dos recursos da rede, que pode ser usado para fins de cobrança. Para tanto, pode-se utilizar o elemento H.323 *Gatekeeper* (seção 2.5.2).

2.2. Pilha de protocolos

O ITU-T também desenvolve outras recomendações que estendem as funcionalidades do H.323 ou adicionam novos serviços. Essas recomendações, como as exibidas a seguir, não serão aqui detalhadas na íntegra. A idéia é descrever sucintamente a finalidade apenas dos padrões mais importantes.

- H.225 para gerenciamento de conexão;
- H.245 para controle e estabelecimento de mídia;
- H.335 para segurança;
- H.235 para criptografia para Série H;
- H.246 para interoperabilidade com RTCP;
- Série H.450.x para serviços suplementares.

A pilha de protocolos do padrão H.323 é apresentada na Figura 5 de forma simplificada. Embora o RTP e o RTCP não façam parte do padrão H.323, esses protocolos são recomendados na implementação de aplicações seguindo esse padrão.

<table>
<tr><td colspan="2">Vídeo</td><td colspan="2">Audio</td><td colspan="3">Control</td><td>Data</td></tr>
<tr><td colspan="2">H.261
H.263</td><td colspan="2">G.711
G.722
G.723
G.728
G.729</td><td rowspan="2">H.225

Terminal to gatekeeper signaling</td><td rowspan="2">H.225
Call signaling</td><td rowspan="2">H.245</td><td rowspan="2">T-120
(Multipoint data transfer)</td></tr>
<tr><td>RTP</td><td>RTCP</td><td>RTP</td><td>RTCP</td></tr>
<tr><td colspan="4">Unreliable transport (UDP)</td><td colspan="4">Reliable transport (TCP)</td></tr>
</table>

Figura 5: Pilha de Protocolos H.323 (PRYCKER, 2005).

2.2.1 Sinalização de chamadas - H.225.0

Esse protocolo define o procedimento inicial para o estabelecimento de uma chamada H.323. É a partir desse padrão que os terminais informam, a um destino chamado, sobre suas intenções de comunicação.

O padrão H.225.0 é de fato muito extenso, com inúmeras particularidades. Ele teve sua concepção muito influenciada pelo padrão Q.931 das redes RDSI, tendo em vista não só sua eficiência no estabelecimento dos tipos de conexões pretendidas, mas também o desejo de tornar o H.225 compatível com essas redes. E, de fato, as mensagens de comunicação de ambos os padrões são muito semelhantes.

As mensagens H.225.0 mais importantes, subconjunto do Q.931, são as seguintes:

- *SETUP*
- *ALERTING*
- *CONNECT*
- *RELEASE COMPLETE*

Existem outras mensagens no H.225.0, porém são de caráter opcional. Considerando as mensagens acima, existem muitos detalhes a respeito do funcionamento de cada uma delas, detalhes esses fora do escopo desse projeto. De uma maneira geral, apenas o imprescindível para o entendimento de cada mensagem será abordado. Sendo esse projeto destinado ao atendimento das operações básicas do H.323, grande parte dos detalhes será evitada ao máximo. Numa versão posterior desse projeto, detalhes maiores deverão ser incluídos.

Para iniciar uma comunicação, uma mensagem *SETUP* é enviada para o terminal destino na porta TCP 1720. Informações importantes presentes nessa mensagem são os identificadores, responsável pelas associações de mensagens. Respostas possíveis para essa mensagem são *RELEASE COMPLETE, ALERTING, CONNECT* ou *CALL PROCEEDING* (opcional). Uma observação crucial é a existência de contadores que regulam o tempo máximo que uma resposta pode ser recebida.

A mensagem *ALERTING* indicará ao emissor do *SETUP* que essa mensagem foi recebida. Após o *ALERTING*, um *CONNECT* aceita e estabelece a comunicação.

2.2.2 Sinalização de controle - H.245

O H.245 é o protocolo de controle de mídia que os sistemas H.323 utilizam depois que a fase de estabelecimento da chamada foi completada. Em outras palavras, o H.245 especifica o conjunto de comandos e requisições que cada terminal deve seguir, a fim de obter uma comunicação satisfatória com outro terminal.

O H.245 é usado para negociar e estabelecer todos os canais de mídia conduzidos pelo RTP/RTCP. Esses dois últimos protocolos são os responsáveis pela transmissão do fluxo de dados de tempo real e do controle da conferência nesse nível, respectivamente, e serão tratados na seção 2.2.2.

Com o H.245, os terminais podem negociar a taxa de transmissão de bits, os formatos das imagens e do áudio transmitidos e os algoritmos usados para codificação e decodificação. Toda essa negociação ocorre dinamicamente. Com isso, uma comunicação H.323 consegue se adaptar às mudanças ocorridas, tanto em relação às disponibilidades da rede, quanto em relação às capacidades atuais dos elementos H.323 participantes dessa comunicação.

Todo o processo de controle é feito por um “canal H.245”. Esse canal é o canal lógico 0 (zero) e está permanentemente aberto, ao contrário dos canais de mídia. Através desse canal, um elemento H.323 pode informar a outro elemento qual é a sua capacidade de transmissão e de recepção atuais, evitando que o primeiro desgaste o último com processamento além das suas capacidades. Os canais de mídia criados, a partir do canal padrão zero, recebem identificadores distintos.

Para haver a comunicação de controle é necessário que haja uma troca de mensagens pré-definidas para esse fim. Essas mensagens, além de permitir a

compatibilidade entre elementos H.323 distintos, permitem que canais lógicos sejam abertos ou fechados.

Um terminal pode ter o "controle H.245". Esse controle é a função que provê ao terminal a habilidade de enviar mensagens fim-a-fim para negociar o uso e a capacidade do canal.

Em resumo, as informações carregadas e gerenciadas pelas mensagens supracitadas são:

- Mecanismo de gerenciamento de capacidades dos terminais H.323;
- Abertura e fechamento de canais de transmissão de fluxo de media;
- Mensagens de controle de fluxo;
- Comandos adicionais e indicações.

A primeira tarefa do canal H.245 é trocar informações sobre a capacidade de cada terminal. Para tanto, cada terminal emite nesse canal, através de mensagens H.245, informações sobre os *codecs* (EnCOder/DECoder) que suporta. Nessa lista há uma ordem de prioridade e a escolha é feita seguindo a idéia do maior denominador comum. Caso não haja esse denominador, a comunicação não é estabelecida. A mensagem enviada para esse fim é a *TerminalCapabilitySet*. Deve-se lembrar que há *codecs* que são considerados obrigatórios, tanto para áudio quanto para vídeo.

Após a troca de capacidades, com o final do estabelecimento do(s) *codec(s)* comum(s), inicia-se a fase de estabelecimentos dos canais lógicos. Esses canais lógicos transportarão as mídias da comunicação: áudio, vídeo e dados (protocolo T.120). O canal de áudio é obrigatório, sendo os outros canais opcionais. Outro comentário importante é

que os canais de áudio e vídeo são unidirecionais, enquanto os canais de dados são bidirecionais.

A mensagem H.245 para abrir um canal lógico é o *OpenLogicalChannel*. A confirmação dessa mensagem ocorre com um *OpenLogicalChannelAck*. O terminal que desejar transmitir mídia para o outro terminal na mesma comunicação deve seguir o mesmo procedimento. Após esse procedimento, os pacotes RTP e RTCP podem começar a ser enviados entre os terminais (HERSENT, 2002).

2.2.3. Estabelecimentos de chamadas H.323 simples

Para o estabelecimento de uma chamada H.323 fim-a-fim, são necessárias duas conexões TCP entre os dois terminais. Uma dessas conexões é destinada ao estabelecimento da chamada, enquanto a outra é responsável pelo controle da conferência H.323, bem como a troca de informações de capacidades entre os terminais.

Considerando a conexão TCP inicial, essa é estabelecida entre o terminal chamador e o terminal chamado. Nessa conexão, mensagens H.225.0 serão trocadas entre esses terminais. Devido à semelhança desse padrão com o Q.931, costuma-se chamar esse canal de canal Q.931, ou, para fins mais didáticos, canal de sinalização de chamadas.

Ao analisar esse princípio de comunicação, uma dúvida comum surge ao analisar a criação da conexão TCP inicial. Devido essa conexão ser iniciada a partir de um terminal, com um destino na outra extremidade da comunicação, o terminal chamador deve ter conhecimento não só do endereço de rede do destino, mas também da respectiva porta TCP. De fato, a porta TCP para essa finalidade foi padronizada: a porta TCP 1720. Dessa forma,

faz-se claro a necessidade de todos os terminais H.323 em “escutar” essa porta para tratar eventuais pedidos de abertura de conexão H.225.0.

A porta TCP 1720 foi padronizada para a comunicação inicial (*setup*). Contudo, nenhuma porta foi padronizada para a segunda comunicação TCP criada entre os terminais: o canal H.245. A porta TCP para estabelecimento desse canal é de caráter dinâmico.

Para que o terminal chamador saiba qual porta TCP usar para estabelecer o canal H.245 com o terminal chamado, existe um artifício na comunicação H.225.0 sendo criada previamente. Durante essa troca inicial de mensagens, o terminal chamado indica ao chamador a porta TCP a ser utilizada na abertura do canal H.245.

As funções desses dois padrões já foram mencionadas nas seções anteriores e uma diagramação dessas comunicações será apresentada nas discussões sobre os testes da ferramenta. Muitas opções de comunicação são possíveis no H.323, entretanto, devido ao objetivo do trabalho, não serão comentadas aqui.

Caso o terminal esteja anexado a um *Gatekeeper*, ele deve pedir autorização ao *Gatekeeper* para efetuar a chamada. Mais detalhes sobre essa operação são apresentados na seção 2.5.2.

2.2.4. Encerramento de chamadas H.323

O primeiro passo para terminar uma ligação é encerrar todos os canais lógicos H.245. Isso é feito através da mensagem H.245 *CloseLogicalChannel*. Após isso, o canal H.225.0 (Q.931), se ainda não tiver sido fechado (situação comum após a abertura do canal H.245), deve ser encerrado por um mensagem H.225.0 *ReleaseComplete*.

Caso o terminal esteja conectado a um *Gatekeeper*, o próximo passo é encerrar a comunicação com ele através das mensagens DRQ (*Disengage Request*) e URQ (*Unregister Request*) do protocolo RAS (*Registration Admission and Status*). Essas mensagens serão discutidas na seção 2.5.2.

2.2.5. Opções de chamada H.323

Muito já foi melhorado no padrão H.323 em relação ao tempo de conexão. De fato, a troca de mensagens necessárias antes do inicio efetivo da comunicação constitui-se em umas das grandes críticas a esse padrão. Tão prejudicial era inicialmente essa característica que o padrão IETF SIP, introduzido após o H.323, possui um esquema de operação onde a comunicação efetiva ocorre logo "de início". E isso se tornou uma das vantagens desse padrão em relação ao H.323.

Alguns esquemas adicionais foram desenvolvidos desde a primeira especificação do H.323 em 1996. Os mais importantes entre eles são o "*Fast Connect*" e o tunelamento H.245.

O procedimento "*Fast Connect*" permite que haja uma comunicação de áudio bidirecional após o recebimento da mensagem H.225.0 *CONNECT*. Para tanto, uma relação das capacidades (*codecs*) do terminal é enviada na mensagem *SETUP*. Dessa maneira, o *overhead* antes de ocorrer à comunicação efetiva é diminuído.

O tunelamento H.245 consiste no encapsulamento de mensagem desse padrão em mensagens *SETUP* H.225.0. Dessa forma, o canal H.225.0 deve permanecer aberto durante toda a chamada. Existem inúmeras vantagens em se utilizar essa técnica, sendo de grande

utilidade para terminais que estejam por trás de um *"firewall"*, pois apenas uma porta bem conhecida, a TCP 1720, será necessária.

2.3 Codificadores e Decodificadores (voz e vídeo)

Um dos papéis do H.323 é definir codificadores e decodificadores de áudio e vídeo padrões para as aplicações multimídia. Com isso, as implementações de determinado fabricante que utilizem as recomendações H.323 serão compatíveis com implementações de outros fabricantes, desde que sigam esta especificação. Dessa forma, a interoperabilidade, uma das características marcantes do padrão H.323, é garantida.

Os codificadores e decodificadores, também chamados de *codecs* (*encoder - decoder*), definem o formato em que as informações de áudio e vídeo serão codificadas e, opcionalmente, comprimidas para transmissão na rede.

Um *codec* de áudio codifica o sinal de áudio proveniente do microfone do terminal transmissor e decodifica o áudio recebido que é então enviado para as saídas de som. Como o áudio é o serviço mínimo fornecido pelo padrão H.323, todos os terminais H.323 devem suportar pelo menos um *codec* de áudio. Vale ressaltar que a utilização do *codec* G.711 para áudio é obrigatório nas implementações H.323 e o suporte aos outros padrões de áudio especificado pelo H.323 é opcional.

O G.711 é reconhecido internacionalmente, largamente utilizado na conversão de sinais de voz analógicos para transmissão em redes digitais. A qualidade resultante é adequada para sinais de voz (*toll quality*), mas não é considerada boa para sinais de áudio. Opera em um esquema de modulação por codificação de pulso (PCM - *Pulse Code*

Modulation), numa taxa de amostragem de 8kHz, como 8 bits por amostra, com taxa de transmissão de 64 Kbps. Os terminais H.323 são capazes de enviar e receber dados codificados por algoritmos codificadores *A-Law* e *μ-Law*, os dois variantes do G.711. A diferença entre eles é que o *A-law* representa os sinais de freqüências menores com mais fidelidade.

Tabela 6: Codecs de voz

Padrão	Algoritmo	Bit Rate (Kbit/s)	Recursos de CPU	Delay (ms)	Qualidade da voz
G.711	PCM	48, 56, 64	Não requerido	<<1	Excelente
G.723.1	MPE/ACELP	5.3, 6.3	Moderado	67-97	Boa(6.3), Razoável(5.3)
H.728	LD-CELP	16	Muito alto	<<2	Boa
G.729	CS-ACELP	8	Alto	25-35	Boa
G.729 annex A	CS-ACELP	8	Alto	25-35	Boa
G.722	Sub-band ADPCM	48, 56, 64	Alto	<<2	Boa
G.726	ADPCM	16,24,32,40	Baixo	60	Boa(40), Razoável(24)
G.727	AEDPCM	16, 24, 32, 40	Baixo	60	Boa(40), Razoável (24)

Um *codec* de vídeo codifica vídeo proveniente de uma entrada de vídeo (câmera, por exemplo) no transmissor e decodifica o vídeo recebido, enviando-o ao display de vídeo

no receptor. Como o suporte a vídeo é opcional, um terminal H.323 pode não processar *codecs* de vídeo se assim for desejado.

Há muitas características relevantes em relação a estes *codecs*, porém elas não são aqui abordadas. Tais características, como geração de ruído de conforto e esquemas de supressão de silêncio, podem ser encontradas na literatura apropriada (HERSENT, 2002).

O H.323 especifica que os pacotes de voz sejam encapsulados no Protocolo RTP (*Real-Time Transport Protocol*) e transportados no UDP (User Datagram Protocol). Para gerenciar a qualidade da comunicação de voz na rede, utiliza-se o protocolo RTPC (*Real-Time Control Protocol*).

A parte de controle do H.323 também utiliza o UDP como protocolo de transporte para estabelecer conexões entre os terminais H.323 e o *Gatekeeper*, que é basicamente um servidor de acesso remoto (RAS – *Remote Access Server*) da rede H.323, e o TCP para sinalização de chamada e canal de controle. Os protocolos H.225, que é um subconjunto do protocolo Q.931 (protocolo de sinalização da RDSI) e H.245 definem toda a operação de controle da arquitetura H.323.

2.4. RTP e RTCP

O TCP é o protocolo de transporte mais usado na Internet; entretanto, existem alguns fatores que fazem com que o TCP não seja adequado para aplicações de tempo real. Primeiro, o TCP foi construído para permitir retransmissão de pacotes perdidos.

Como num fluxo de tempo real a perda de alguns pacotes não causa um impacto relevante na comunicação, seria um problema a retransmissão desses pacotes. Segundo, o

TCP não suporta “multicast”. Por último, não há informações de tempo nesse protocolo, um problema já que a maioria das aplicações de tempo real necessita de tais informações.

O UDP, outro protocolo de transporte amplamente utilizado, não possui qualquer informação de tempo.

Dessa forma, o IETF (*Internet Engineering Task Force*) criou o RTP (*Real Time Protocol*). Desde então, o AVT (Áudio/Vídeo *Transport*) *Working Group* tem sido o maior fórum de discussão sobre o RTP.

A ITU (*International Telecommunication Union*) adotou o RTP como o protocolo de transporte de tempo real (multimídia) padrão. O padrão ITU H.323 utiliza o RTP como o protocolo padrão para transporte de dados multimídia.

O RTP é um protocolo de transporte da pilha de protocolos H.323, sendo definido pela RFC 1889. Conceitualmente, o RTP provê transporte de dados fim a fim necessário a aplicações de tempo real, tais como áudio e vídeo. Em outras palavras, esse protocolo tem como objetivo fornecer um mecanismo para levar dados sensíveis ao atraso, por exemplo, vídeo e áudio, de uma extremidade a outra da rede, em “tempo real”. Em relação a esse aspecto de transporte, o RTP atua como uma espécie de “intermediador” entre os dados a serem transmitidos e os meios que efetivam a transmissão. De uma forma mais direta, esse protocolo funciona como uma interface entre as aplicações de tempo real e os protocolos da camada de transporte.

Apesar de funcionar como uma “interface” entre camadas, o RTP foi designado para ser independente das camadas de rede e de transporte. Sendo independente, o RTP pode ser implementado sobre qualquer protocolo dessas camadas. Na realidade, as aplicações geralmente utilizam o RTP sobre o UDP, para o envio de áudio e vídeo (fluxo de tempo real) e o RTP sobre o TCP para transmissão de arquivos (não sensíveis ao tempo).

Com a utilização de UDP, além das vantagens obtidas com a simplicidade do protocolo, dois serviços de extrema importância são disponibilizados: a multiplexação e a detecção de erros (*checksum*).

Como o RTP necessita dos recursos oferecidos pelos protocolos das camadas inferiores, ele não utiliza qualquer mecanismo para assegurar a entrega de dados em ordem ou com atraso constante. É de se esperar que serviços como estes sejam fornecidos pelos protocolos nos quais o RTP está encapsulado. Em adição, o RTP não fornece qualquer tipo de reserva de recursos, não garantindo qualidade de serviço (QoS) em aplicações de tempo real.

O RTCP (*Real Time Control Protocol*) foi criado pelo IETF para ser um protocolo de controle que auxiliasse o RTP na sua tarefa de transmissão de dados em tempo real. Seu objetivo primário é a disponibilização de "*feedback*" QoS para que os participantes de uma conferência multimídia possam se adaptar dinamicamente a problemas na rede. Contudo, o RTCP possui outras aplicações como a troca de informações de usuários e a associação de mídias provenientes de diferentes sessões de comunicação. Apenas como um parêntese, cada mídia é transmitida em *sessões* RTP distintas, tendo cada uma dessas sessões um fluxo RTP e um RTCP.

Um pacote RTCP é um pacote de controle consistindo de um cabeçalho fixo seguido por elementos estruturados, variando de acordo com o tipo de pacote RTCP. Esse protocolo é baseado na transmissão periódica de pacotes de controle para todos os participantes numa sessão, usando os mesmos mecanismos de comunicação utilizados para os dados. O protocolo da camada inferior deve fornecer multiplexação dos dados e dos pacotes de controle, usando, por exemplo, número de portas distintas.

Todos os participantes devem enviar pacotes RTCP. Dessa forma, deve existir uma maneira de controlar a taxa de envio desses pacotes. De uma certa maneira, quanto mais pacotes RTCP forem enviados, melhor será a obtenção de dados estatísticos confiáveis. Entretanto, maior é o consumo da banda da sessão. Para tanto, é esperada que, no máximo, 5% da banda da sessão RTP seja destinada à transmissão de pacotes RTCP.

Tipicamente, múltiplos pacotes RTCP são enviados juntos como um só pacote RTCP composto, dentro de um único pacote da camada inferior (geralmente UDP). A contagem do número de pacotes deve ser feita pelo protocolo dessa camada.

De uma certa forma, os pacotes de relatório podem fazer com que um emissor mude a taxa de envio dos pacotes RTP, numa adaptação às variações da rede. Além disso, a taxa de envio de pacotes RTCP é ajustada de acordo com o número de usuários, uma vez que dependendo do número de participantes da conferência, o tráfego gerado pelos pacotes RTCP poder ser grande.

2.5 Elementos H.323

Na prática, uma rede H.323 não é um novo tipo de rede, mas sim uma rede tipicamente IP, que possui serviços especiais voltados para as comunicações multimídia. Tais serviços especiais são implementados através da implantação, em uma rede IP, de MCUs (*Multipoint Control Unit*), *Gatekeepers* e *gateways*. Logo, diz-se que uma rede H.323 é uma rede IP que fornece, via MUCs, *Gatekeepers* e *gateways*, serviços multimídia aos terminais H.323 a ela conectados.

MCUs e *gateways* não precisam estar presentes em todas as situações de comunicação multimídia, uma vez que apresentam funções específicas: um *gateway* só se faz necessário quando terminais de padrões diferentes do H.323 precisam se comunicar com terminais H.323 e um MCU só será necessário numa conferência multiponto.

No projeto, dois elementos H.323 básicos foram utilizados: o terminal H.323 e o *Gatekeeper*. Sua descrição mais detalhada é apresentada a seguir.

2.5.1 Terminal H.323

De uma maneira geral, os terminais H.323 são todos os equipamentos que podem se comunicar utilizando a pilha de protocolos desse padrão.

Por padrão, todos os terminais H.323 devem suportar o H.245, Q.931, RAS e RTP. Os terminais H.323 podem também incluir o protocolo de conferência de dados T.120, codificadores de vídeo e suporte para MCU. Um terminal H.323 pode se comunicar com outro terminal, um *gateway* ou um MCU.

Os terminais são os pontos iniciais e finais das comunicações multimídia. Embora possa se considerar um servidor de vídeo como gerando tráfego em tempo real, é totalmente aceitável considerá-lo como um terminal. É comum que os terminais apresentem comunicação bidirecional, sendo essa a forma mais presente.

De fato, os terminais H.323 podem ser encontrados na forma de um microcomputador ou como um dispositivo específico. Como exemplo deste último, existem telefones H.323 que implementam todas as funcionalidades requerentes às aplicações de

VoIP. Outros exemplos muito comuns são as câmeras digitais que já possuem as implementações necessárias às videoconferências.

A função principal de um terminal H.323 é a de se comunicar com outros terminais multimídia, que tanto podem ser outros terminais H.323 como terminais de outros padrões. Neste último caso, faz-se necessária a utilização de um *gateway* para compatibilizar a comunicação entre terminais diferentes.

2.5.2 Elemento *Gatekeeper*

O *Gatekeeper* é um elemento H.323 que age como um ponto central para todas as chamadas dentro de uma determinada zona H.323. Esse conceito de *zona* refere-se muito mais à gerência do *Gatekeeper* do que qualquer outra entidade H.323.

O *Gatekeeper* (GK) é considerado como o componente mais importante de uma rede H.323. E essa alcunha se deve a inúmeros fatores, que de fato são muito importantes em aplicações de videoconferência e de voz sobre IP.

Agindo como um ponto central de uma zona H.323, ele pode oferecer uma série de serviços aos seus "clientes" cadastrados. Entre esses serviços, podemos destacar o controle da sinalização de chamada.

O *Gatekeeper*, fazendo uso do H.245, realiza funções de negociação de "capacidades" quando uma chamada é estabelecida. Capacidades aqui podem ser consideradas como sendo a banda de transmissão e/ou de recepção disponíveis ou mesmo o tamanho do *"buffer"* destinado à comunicação tanto no transmissor quanto no receptor. Em

qualquer momento pode haver a troca de capacidades, sendo o *Gatekeeper* o gerenciador desta tarefa.

Após a negociação de capacidades, descrita acima, os terminais podem abrir ou fechar um canal lógico de mídia. Esse canal lógico, detalhado a seguir, é por onde a comunicação efetiva dos dados ocorrerá, tendo para tanto numeração e esquemas de configuração próprios.

Uma zona H.323 é o conjunto de dispositivos finais (terminais, *gateways* e MCUs) que são gerenciados por um *Gatekeeper*. Os dispositivos H.323 se registram nos *Gatekeepers* para enviar e receber chamadas. Os *Gatekeepers* oferecem serviços de rede para os componentes da zona que gerenciam. As suas principais funções são:

- Tradução de endereços *aliases* para endereços IP ou IPX;
- Gerenciamento de largura de banda, permitindo a definição da quantidade máxima permitida para os recursos da conferência;
- Roteamento de chamadas H.323;
- Controle do número e do tipo de conexões permitidas;
- Controle de admissão de acesso em uma rede local;
- Gerenciamento de zona, executando todas as funções nos dispositivos finais desta.

Muitas das atribuições ligadas ao *Gatekeeper* são essenciais à comunicação H.323 na Internet. Os usuários não desejam, por exemplo, trabalhar com endereços de rede, mas sim nomes que sejam facilmente associáveis às pessoas. Além disso, é de se esperar que

existam mecanismos que permitam ou não a "anexação" de determinado usuário ao *Gatekeeper*.

De uma maneira geral, as funções de registro, admissão e estado do *Gatekeeper* são desempenhadas pelo protocolo RAS (*Registration, Admission and Status*).

A mensagem RAS básica é a GRQ (*Gatekeeper* Request). Nessa mensagem são enviados os *aliases* que o terminal deseja possuir, sendo escolhido aquele de maior prioridade e que já não esteja em uso por outro terminal. Contudo, na ferramenta desenvolvida, foi utilizado apenas um alias. Caso este já esteja em uso, uma mensagem de "rejeição" é retornada pelo GK. Essa mensagem é o GRJ (*Gatekeeper Rejection*). Caso contrário, é retornado um GCF (*Gatekeeper Confirmation*). Informações comuns para um GRQ são o endereço em que o terminal espera receber a resposta e o tipo do terminal, sem esquecer da lista de *aliases*. Deve-se lembrar também que o *Gatekeeper* pode recusar um pedido de registro por inúmeros motivos, dependendo da política de registro adotada pelo GK.

Com o intuito de aumentar a segurança na comunicação com o *Gatekeeper*, pode-se utilizar o protocolo H.235. Entretanto, devido ao objetivo desse trabalho, a abordagem desse protocolo foi deixada de lado.

Após receber uma resposta GCF, o registro do terminal é pedido através do envio de uma mensagem RRQ (*Registration Request*), na porta UDP 1719. Nessa mensagem segue uma importante informação: o endereço de transporte para a sinalização de chamadas pelo terminal. Se o GK aceita o pedido de registro, uma mensagem RCF é enviada ao terminal. Uma informação importante dessa mensagem é um identificador único utilizado em todas as mensagens RAS subseqüentes.

Considerando agora que o terminal deseja fazer uma chamada e estando ele registrado num *Gatekeeper*, este deve pedir autorização ao GK. Para isso, é utilizada uma mensagem ARQ (*Admission Request*). Nessa mensagem está presente o alias destino da chamada. Caso o *Gatekeeper* aceite o pedido feito, uma mensagem ACF (*Admission Confirmation*) é enviada para o terminal. Nessa mensagem, o endereço de transporte do alias destino é retornado (capturado a partir de um RRQ enviada previamente pelo terminal destino da chamada). Um ARJ (*Admission Rejection*) impede o terminal de realizar a chamada. Com o endereço de transporte retornado pelo GK, o terminal realiza a chamada diretamente a esse endereço (modelo de comunicação direto).

As mensagens ARQ e ACF carregam muitas informações importantes à conferência, como largura de banda máxima e o modelo de chamada. Tais informações terão valores padrões na implementação da ferramenta, já que esta não fará qualquer tratamento dessas informações.

Por fim, o desregistro junto ao GK é feito através de um URQ (*Unregister Request*). Porém, antes dessa mensagem e caso o terminal esteja em processo de encerramento da chamada, deve haver o envio da mensagem DRQ (*Desingage Request*), que, entre outras coisas, informa ao GK que a banda da comunicação encerrada foi liberada. Caso o GK queira encerrar a comunicação, ele também pode enviar uma mensagem DRQ aos terminais que estejam nessa comunicação.

Esses cinco grupos de mensagens constituem apenas o básico da comunicação com o *Gatekeeper*. De fato, há muitas outras mensagens RAS com diferentes objetivos, porém o tratamento dessas mensagens pela ferramenta não é realizado diretamente.

Para localizar um *Gatekeeper* pode-se utilizar diversas maneiras; entretanto duas delas foram utilizadas pela ferramenta e apenas essas duas serão aqui abordadas. Mais

detalhes e métodos de localização podem ser encontrados na documentação oficial do H.323 (PACKETIZER, 2005).

O primeiro método de localizar um *Gatekeeper* é através do seu endereço de rede, na porta UDP 1719 (porta padrão). Uma outra maneira é utilizar mensagens *multicast*, numa localização dinâmica.

Tipo de operação do *Gatekeeper*

Existem três tipos de operações do *Gatekeeper*: direta, roteada e *proxy*. No primeiro esquema de operação, o *Gatekeeper* realiza principalmente a função de tradução de *aliases* em endereços. Todos os canais de comunicação, tanto de controle como de dados, são estabelecidos diretamente entre os terminais.

O modo de operação roteado estabelece os canais de dados entre os terminais diretamente, porém o *Gatekeeper* localiza-se como ponto central dos canais de sinalização. Nesse modo de operação, o *Gatekeeper* executa um maior controle e gerência das comunicações.

Por último, no modo *proxy* todos os canais estabelecidos entre terminais comunicantes possuem o *Gatekeeper* como ponto intermediário. Inúmeras aplicações são possíveis nesse modo de operação, principalmente em relação a problemas com *firewall*.

Na ferramenta implementada, tendo em vista o objetivo do projeto, apenas o modo de comunicação direto foi utilizado nos testes. Considerando o *Gatekeeper* utilizado, basta a alteração no modo de operação deste para que a ferramenta opere da maneira desejada.

3 QUALIDADE DE SERVIÇO

A qualidade de serviço (QoS - *Quality of Service*) em redes é um importante aspecto de implantação e operação tanto para redes de pacotes como um todo, como para redes IP em particular (CLAUDE, 2002).

As redes TCP/IP, ou simplesmente redes de IP possuem uma grande base instalada, e seu crescimento e aceitabilidade se dão por dois fatores: o crescimento da Internet e a aceitação pelas empresas da base TCP/IP como plataforma de suporte às aplicações em rede. E para os próximos anos esse cenário não tende a mudar, pois teremos cada vez mais computadores utilizando o TCP/IP para comunicação via Internet.

Em um âmbito geral, as redes IP foram desenvolvidas e têm como uma de suas premissas básicas, o poder de ser utilizadas com diversos tipos de meios físicos e tecnologias existentes, de forma a viabilizar a comunicação entre as aplicações fim-a-fim em redes.

Para o cenário atual, a utilização das redes IP demanda que “qualquer aplicação” possa executar com qualidade sobre o IP. Dessa forma, a questão que segue vem a ser a identificação das eventuais limitações do IP e procedimentos necessários para adequá-lo à realidade de utilização das redes.

O desafio para utilização do IP como plataforma principal para aplicações em redes é: o protocolo IP sem qualquer garantia de qualidade de serviço e as dificuldades de mudanças de protocolo, por causa da grande base IP instalada (SILVA, 2000).

A primeira questão é de caráter técnico, e diz respeito ao paradigma previsto para o protocolo que enfatiza a simplicidade de concepção. Um exemplo disso é o protocolo IP, que não tem nenhuma garantia de vazão constante para uma aplicação em particular. Além

disso, uma aplicação não pode obter do IP nenhuma garantia de entrega dos próprios pacotes que eventualmente são descartados ou perdidos sem que nenhum tipo de correção ou ação seja tomada. Não existe também nenhuma garantia de tempo de entrega para os pacotes (YAMADA, 2001).

Pode-se dizer que a proposta de novos algoritmos com mecanismos de tratamento de deficiências são algumas das formas de se sanar as "deficiências" do IP, e permitirem o suporte efetivo de qualquer tipo de aplicação sobre redes IP.

O IP possui uma grande base instalada e a tendência é que ele suporte as aplicações em rede, tais como: Telefonia e Fax sobre IP (VoIP – *Voice over IP*); Comércio eletrônico (*E_commerce*); Vídeo sobre IP; Educação a distância (EAD) (*Distance Learning*); Vídeo conferência; Aplicações de grupo; Aplicações multimídia; Aplicações em tempo real.

Para obtenção de uma QoS, o entendimento dos seus princípios, parâmetros, mecanismos, algoritmos e protocolos são de grande importância, pois a qualidade de serviço (QoS) nas redes é um aspecto fundamental para o desempenho fim-a-fim das aplicações (VoIP, multimídia,...).

3.1 Princípios de Qualidade de Serviço (QoS)

Pode-se dizer, que Qualidade de Serviço é um conjunto de padronizações que impõem limites (valores mínimos e máximos) para determinados parâmetros (perdas, atrasos, vazões, etc).

A QoS é garantida pela rede, seus componentes e equipamentos utilizados. Do ponto de vista dos programas de aplicação, a QoS é expressa em termos de uma "solicitação de serviços" ou "contrato de serviços". Esse contrato é denominado de SLA (Service Level Agreement) (McCABE, 1998).

Algumas aplicações, como as de multimídia, são as que normalmente exigem os parâmetros de QoS mais satisfatórios. Entretanto, em aplicações multimídia, envolvendo dados, gráficos e arquivos com animação (vídeo...), em que não há necessidade de sincronização ou aplicação de QoS. Por outro lado, em uma aplicação envolvendo áudio, somente garantir a vazão não é o suficiente. Para este caso, os atrasos e as perdas influenciam tanto na interação com o usuário, como nos recursos das redes, exigindo-se assim uma maior necessidade de suporte da qualidade de serviço da rede.

Na seqüência, algumas considerações sobre os parâmetros de QoS em aplicações multimídia são feitas para identificar suas exigências.

3.1.1 Erros de seqüenciamento

Congestionamentos nas redes por comutação de pacotes podem levar os pacotes a tomar rotas diferentes para o mesmo destino. Os pacotes podem então chegar fora de ordem resultando numa fala distorcida.

3.1.2 Latência (Atraso)

Latência é o atraso de tempo fala gerado pelo sistema de VoIP. É medida de tempo entre o momento que em que se fala até o momento que realmente o interlocutor escuta.

Esta é a latência num sentido, a latência percebida pelos usuários do sistema. A latência total é a soma das latências nos dois sentidos.

No sistemas de telefonia pública tradicional, esta latência para chamadas nacionais está quase sempre abaixo de 150 ms, que é o valor desejado para todos os sistemas de telefonia, uma vez que, neste nível, a latência não é percebida.

Muitas chamadas internacionais, especialmente as via satélite as vezes apresentam latência de até 1 segundo, sendo bastante desconfortável.

Faixa de aceitação de latência:

- De 0 a 150ms = Excelente
- De 150ms a 300ms = Boa;
- De 300ms a 450ms = regular;
- Acima de 450ms = Inaceitável.

A latência é causada principalmente no processamento de dados no Gateway: demora no manuseio dos pacotes, bufferização, empacotamento, latência do buffer de Jitter, latência da interface de rede, latência do processamento de sinais, latência na criação dos quadros e tempo de processamento. A latência ocorrida na rede é classificada como latência no acesso ao meio, latência no roteamento, firewalls e servidores Proxy.

3.1.3 Jitter

Jitter é o efeito causado por pacotes com tempos de latência diferentes entre si, ou seja pacotes enviado a taxa constante e igualmente espaçados chegam no destino em intervalos irregulares. Muito jitter torna a voz difícil de entender. O jitter é calculado

baseado no intervalo de tempo de chegada dos pacotes. Para uma sinal de alta qualidade o intervalo médio de chegada de pacotes tem que ser igual ao do transmissor e o desvio padrão deve ser o menor possível.

Buffers de jitter são usados para aliviar o efeito de flutuações na rede e garantir uma fluxo suave e constante de pacotes no receptor. Para isso o sistema utiliza as informações provenientes dos cabeçalhos do RTP e do RTCP.

3.1.4 Perda de pacotes

A perda de pacotes é normal numa rede de comutação por pacotes e pode ocorrer devido a links sobrecarregados, colisão na rede, erros num meio físico entre outros fatores.

Os CODECs levam em consideração essa possibilidade e têm uma série de recursos para que uma perda ocasional de pacotes não seja notada pelo usuário, podendo repetir um pacote anterior ou até mesmo fazer uma interpolação.

Quando as perdas de pacotes ultrapassam 5% ou se dão em rajadas, mesmo os melhores CODECs não conseguem mais resolver, resultando numa degradação da qualidade do sinal de voz.

4 DESENVOLVIMENTO E TESTES DA FERRAMENTA

Nos capítulos anteriores foram citados os padrões utilizados em comunicações multimídia, em especial na Telefonia IP. Contudo, deve-se lembrar que apenas uma pequena parcela desses padrões foi mais extensamente abordada, uma vez que um detalhamento mais completo foge do escopo desse trabalho.

Os objetivos principais são englobados pelo projeto são: O primeiro deles é auxiliar na auxiliar na configuração da ferramenta de áudio de fácil utilização, de interface amigável ao usuário e gratuita, *Gnomemeeting*. O segundo objetivo, sem dúvida o mais importante de todos, é fornecer informações ao usuário sobre a operação do padrão H.323, mostrando a troca de mensagens entre os terminais, utilizando o elemento *Gatekeeper*. Por fim, o terceiro objetivo é disponibilizar um código fonte de fácil compreensão, para que interessados na tecnologia VoIP e na utilização do padrão H.323, possam dar continuidade ao trabalho aqui apresentado. A fim de atingir esse último objetivo, o código fonte da ferramenta é apresentado no apêndice.

Nas seções seguintes são detalhadas as questões referentes à implementação da ferramenta.

4.1 Características gerais – Identificação dos requisitos

A ferramenta de comunicação utilizada, *Gnomemeeting* (DAMIEN SANDRAS, 2005), possui características como efetuar e receber chamadas e, em relação ao padrão

H.323, interagir basicamente com o *Gatekeeper*, executando os procedimentos de registro e desregistro de um usuário junto a esse elemento .

Todas as mensagens H.323 enviadas e recebidas pela ferramenta, bem como mensagens de informações ao usuário, devem ser disponibilizadas em um "*buffer* de saída". Esse *buffer* deve ser nada mais que uma área de texto onde as informações são apresentadas. Como opção, as mensagens podem ser salvas em um arquivo de *log* padrão, após o encerramento da aplicação. Nesse *log*, indicações de tempo a respeito do momento dos envios e recepções de mensagens são registradas.

4.2 Modelagem de uma solução

Para realização da modelagem de uma solução que atenda os requisitos expostos na seção anterior, utilizou-se a UML (Unified Modelling Language). Contudo, apenas algumas ferramentas dessa linguagem foram empregadas, tendo em vista as características do projeto desenvolvido, que é utilização de bibliotecas de código livre para construção das principais funcionalidades de um *Gatekeeper*.

4.2.1. Diagrama de Casos de Uso

O Diagrama de Casos de Uso que descreve as funcionalidades da ferramenta, apresentado na Figura 6, seguido pela descrição dos casos de uso e seus procedimentos

normais de execução. Não são mencionados os casos alternativos de operação para simplificar a descrição da ferramenta.

Como forma de tornar os casos de uso mais fáceis de serem compreendidos, cada procedimento de operação dos casos de uso será acompanhado por um diagrama de seqüência correspondente, que ilustra os passos envolvidos.

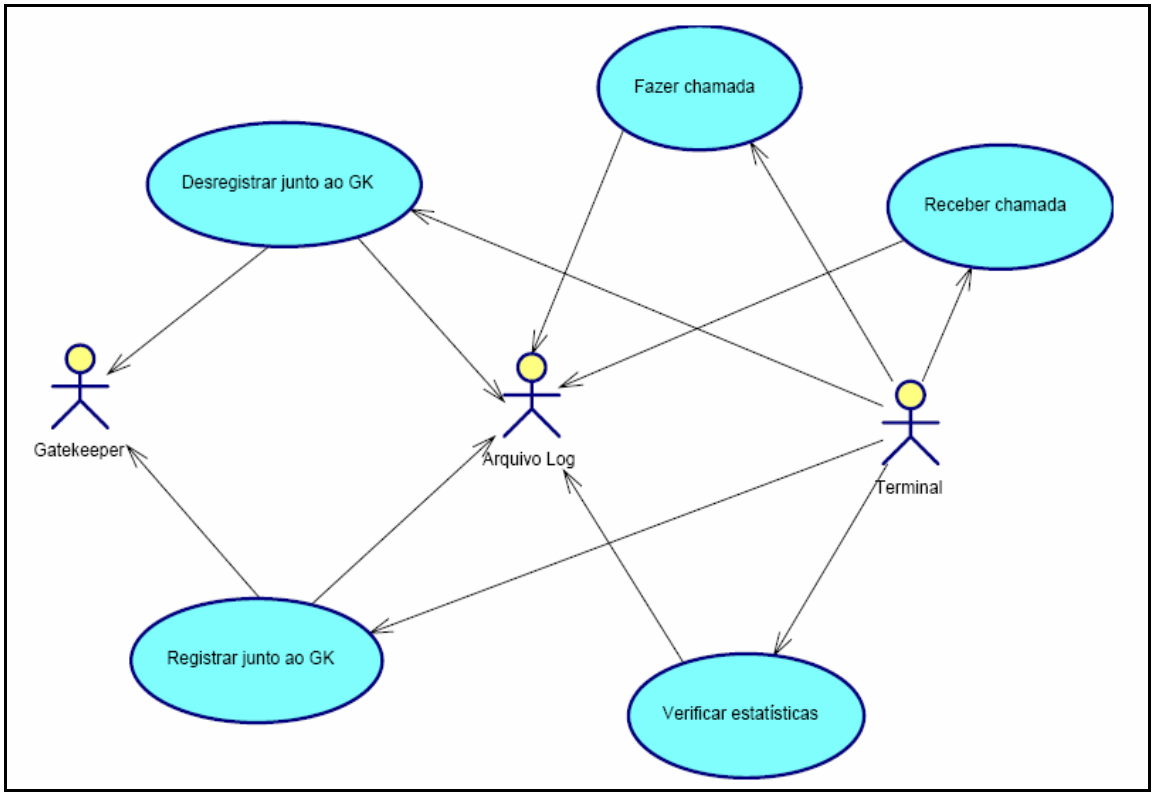


Figura 6: Diagrama de Casos e Uso

4.2.2. Diagramas de Seqüências

Nos itens seguintes é descrita a operação de cada caso de uso. Nessas descrições são empregados os termos “Terminal chamador” e “Terminal chamado”, que, em

conformidade com o diagrama de casos de uso da Figura 6, são equivalentes ao ator "Terminal". O que distingue os terminais é o papel desempenhado por cada um numa chamada: o "Terminal chamador" inicia a chamada enquanto o "Terminal chamado" recebe uma chamada de forma passiva.

4.2.2.1 Fazer Chamada

Descrição: O usuário é capaz de efetuar uma chamada para qualquer terminal H.323 (ou "*gateway*"), utilizando para tanto o endereço IP do terminal destino ou seu *alias*.

Procedimento 1 – Usuário não registrado junto a um *Gatekeeper*:

- O usuário especifica o endereço IP do destino chamado;
- A ferramenta realiza a chamada;
- A ferramenta troca a lista de *codecs* suportados, selecionando o "melhor *codec*" comum (O "melhor *codec*" é o que possui a melhor qualidade por banda consumida);
- Os canais lógicos são abertos;
- A operação é registrada no arquivo de *log*;
- A comunicação é estabelecida.

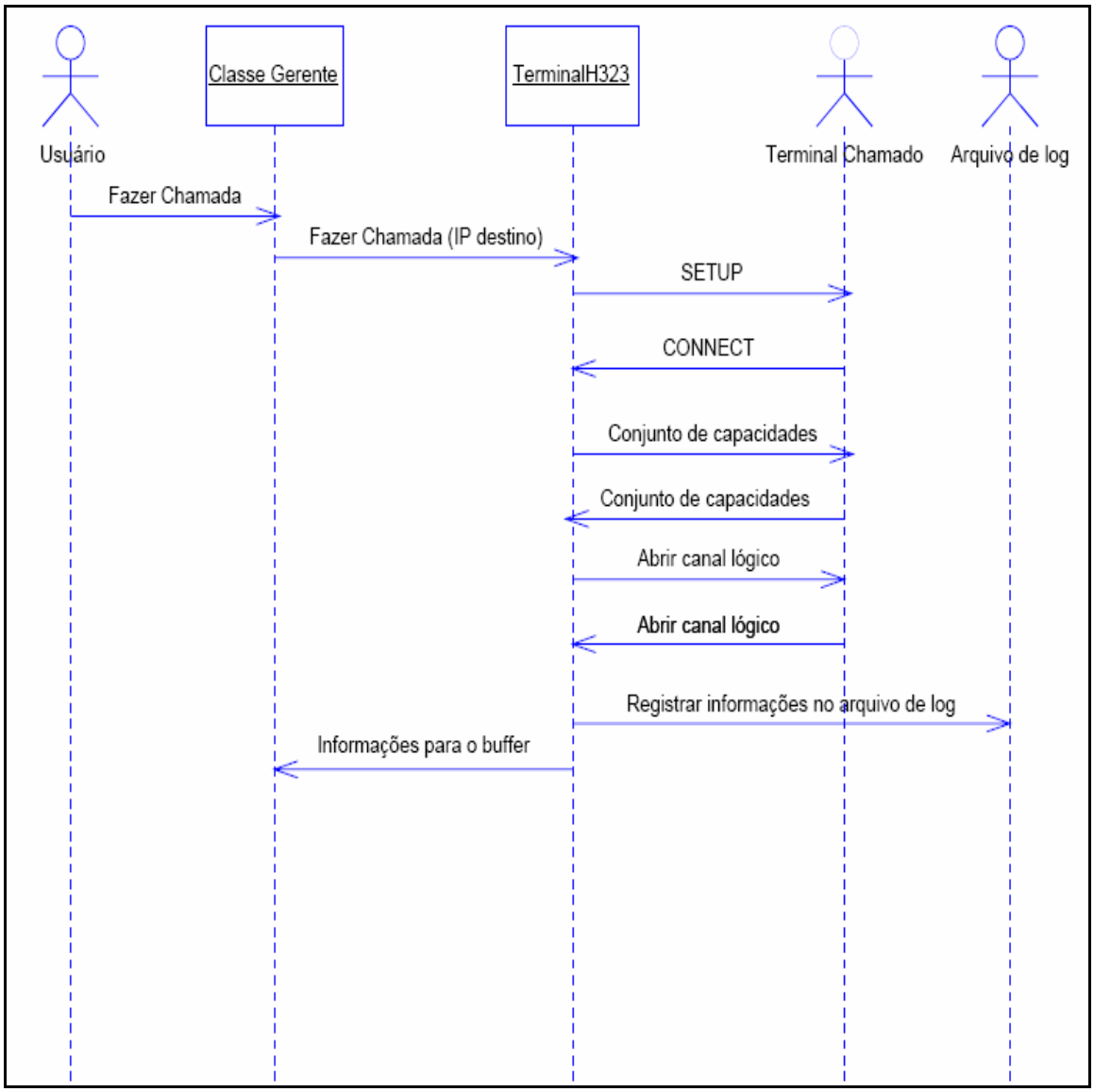


Figura 7: Chamada sem registro junto ao GK

Procedimento 2 – Usuário registrado junto a um *Gatekeeper*:

- O usuário especifica o alias do terminal destino;
- A ferramenta comunica-se com o *Gatekeeper*, informando o alias do terminal destino;

- A ferramenta recebe o endereço IP do terminal H.323 através de uma mensagem de retorno do GK;
- A ferramenta realiza a chamada;
- A ferramenta troca a lista de *codecs* suportados, selecionando o "melhor *codec*" comum;
- A comunicação é estabelecida;
- Os canais lógicos são abertos;
- A operação é registrada no arquivo de *log*;
- A comunicação é estabelecida.

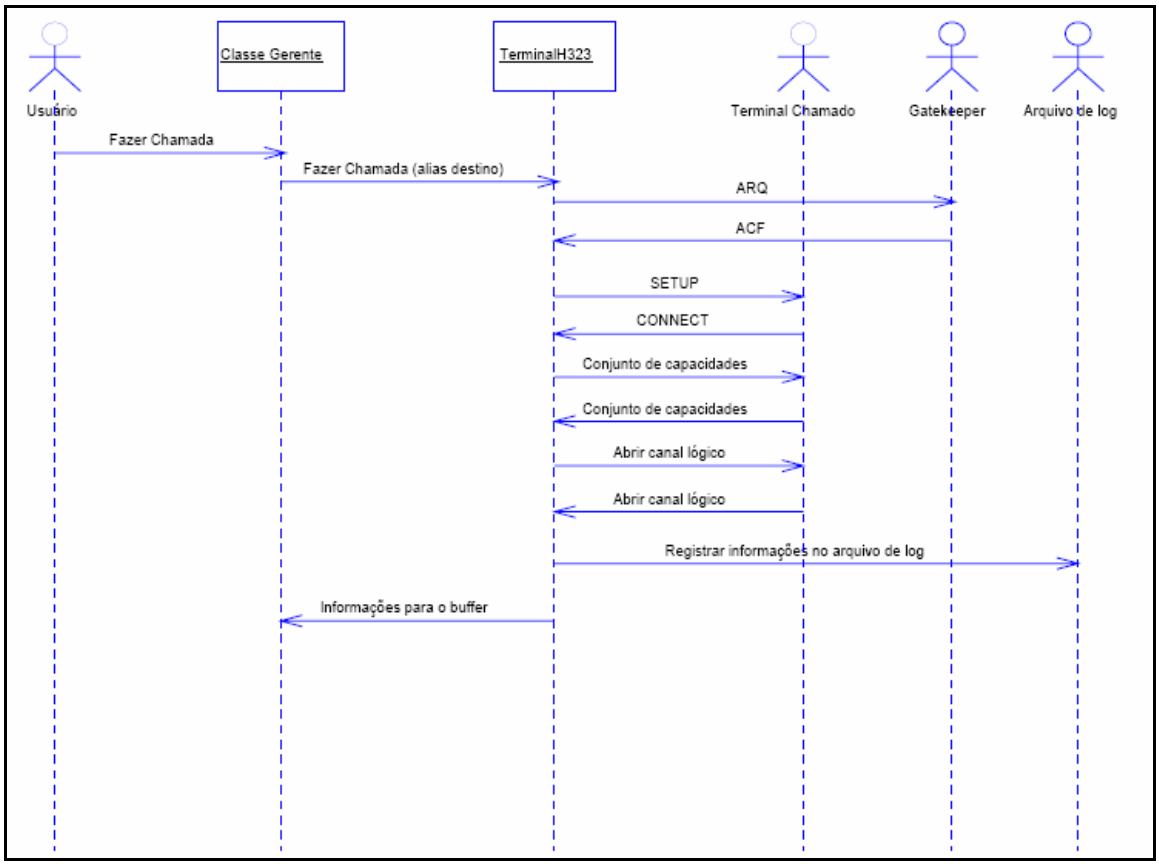


Figura 8: Chamada com registro junto ao GK

4.2.2.2. Receber Chamada

Descrição: O usuário é capaz de receber chamadas de qualquer terminal H.323.

Procedimento:

- O usuário inicia a ferramenta;
- A ferramenta “ouve” chamadas na porta TCP 1720;
- Ao receber uma chamada H.323, a comunicação é estabelecida;
- Os canais lógicos são estabelecidos;
- A operação é registrada no arquivo de log.

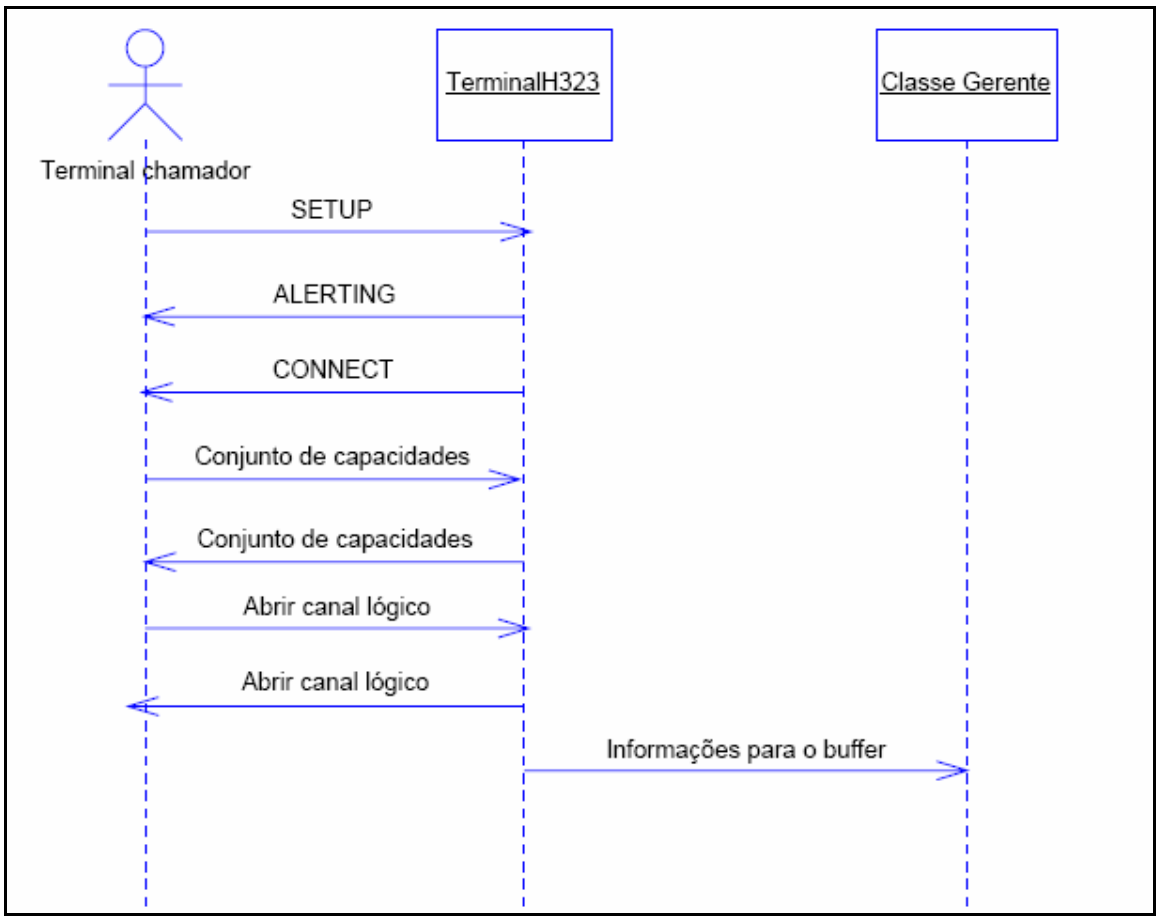


Figura 9: Receber chamada

4.2.2.3. Registrar junto ao GK

Descrição: O usuário pode registrar-se junto ao *Gatekeeper*, informando no registro o *alias* a ser utilizado pelo primeiro. Para realizar o registro, pode-se utilizar o endereço IP do *Gatekeeper* ou descobrimento de GK através de mensagens *multicast*.

Procedimento 1 – Utilizando o IP do *Gatekeeper*

- O usuário especifica o endereço IP do GK;
- O usuário fornece um *alias* para registro junto ao GK;
- O terminal H.323 envia uma mensagem de registro ao *Gatekeeper* especificado pelo endereço;
- O terminal H.323 recebe uma mensagem de confirmação;
- O terminal H.323 está registrado;
- A operação é registrada no arquivo de log.

Procedimento 2 – Utilizando mensagens *multicast*

- O usuário fornece um *alias* para registro junto ao GK;
- O terminal H.323 envia uma mensagem *multicast* de registro junto ao GK;
- O terminal H.323 recebe uma mensagem de confirmação de algum *Gatekeeper*;
- O terminal H.323 está registrado;
- A operação é registrada no arquivo de log.

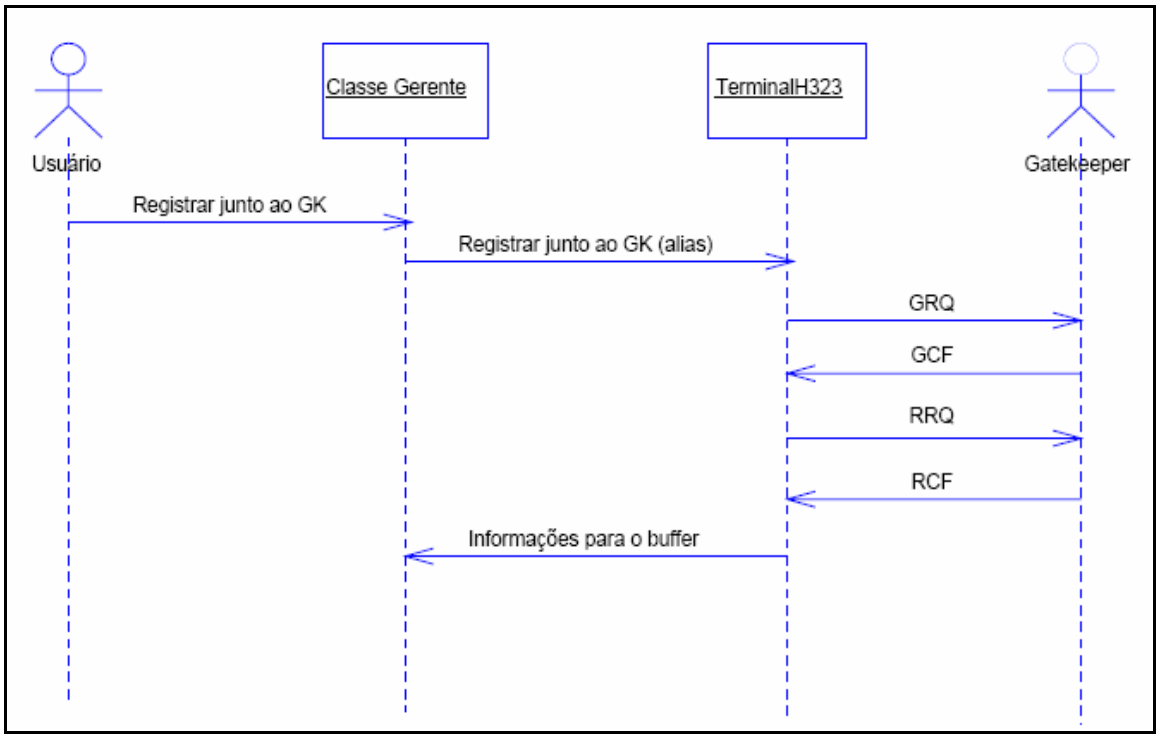


Figura 10: Registro junto ao GK

4.2.2.4. Desregistrar junto ao GK

Descrição: O usuário pode desregistrar-se junto ao *Gatekeeper*. Para realizar o desregistro, pode-se utilizar o endereço IP do *Gatekeeper* ou mensagens *multicast* de desregistro.

Procedimento 1 – Utilizando o IP do *Gatekeeper*

- O usuário especifica o endereço IP do GK;
- O terminal H.323 envia uma mensagem de desregistro ao GK no endereço especificado;

- O terminal H.323 recebe uma mensagem de confirmação;
- O terminal H.323 está desregistrado;
- A operação é registrada no arquivo de log.

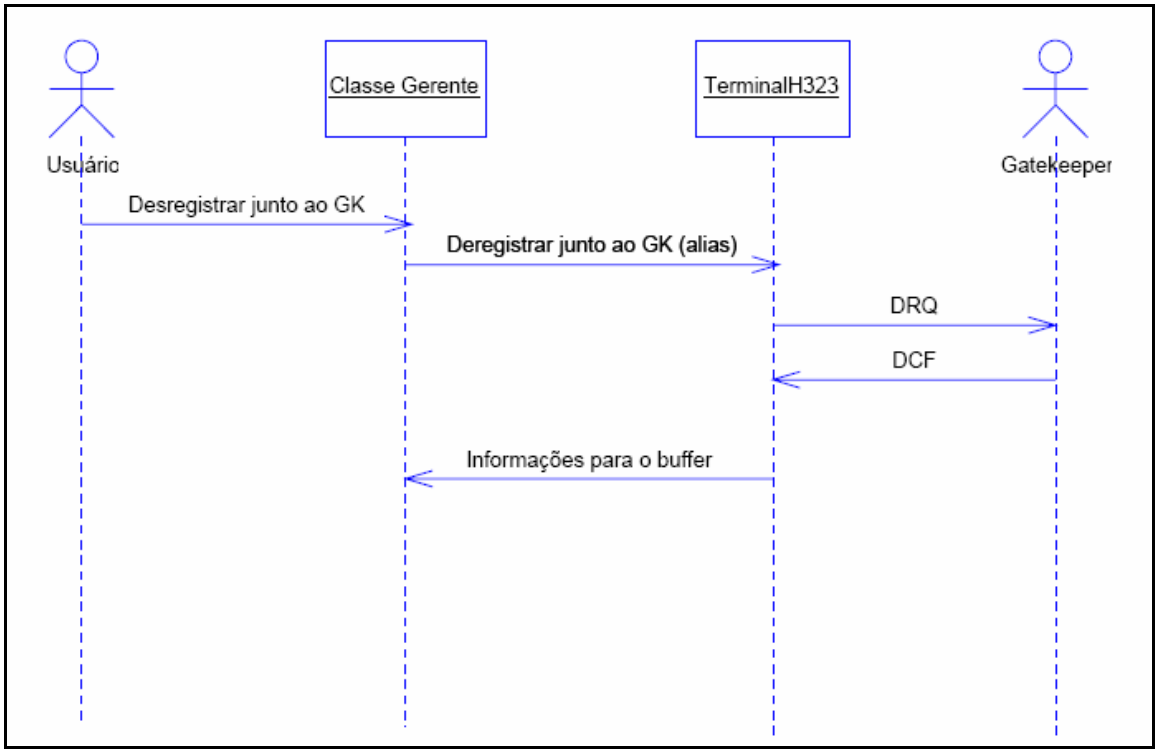


Figura 11: Desregistro junto ao GK

Procedimento 2 – Utilizando mensagens multicast

- O terminal H.323 envia uma mensagem *multicast* de desregistro junto ao GK;
- O terminal H.323 recebe uma mensagem de confirmação;
- O terminal H.323 está desregistrado;
- A operação é registrada no arquivo de log.

4.2.2.5. Verificar estatísticas

Descrição: O usuário pode verificar as estatísticas e dados operacionais da comunicação atual. Se o terminal não estiver participando de uma chamada H.323, nenhum dado é exibido nessa verificação.

Procedimento:

- O usuário solicita verificação das estatísticas da comunicação atual;
- Os dados estatísticos são apresentados pela ferramenta.

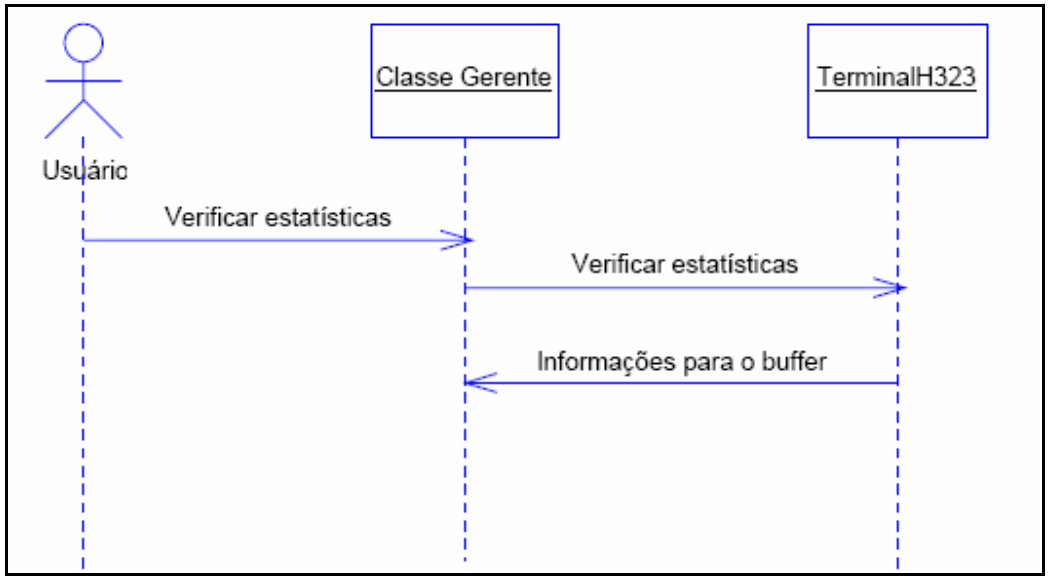


Figura 12: Verificar estatísticas

4.3 Metodologia de Implementação

Como o objetivo desse projeto é desenvolver uma aplicação que sirva tanto como uma ferramenta de áudio, quanto como um suporte ao aprendizado do padrão H.323, as tecnologias empregadas nesse desenvolvimento devem atender a ambos os requisitos.

Todo o código fonte foi escrito em C++, uma vez que tanto as bibliotecas operacionais PWLib e OpenH323, são escritas nessa linguagem de programação. Com o intuito de prover uma maior reusabilidade e organização do código, arquivos de cabeçalho (.h) foram criados para cada implementação correspondente (arquivos .cxx).

O coração da ferramenta foi implementado através dos recursos contidos nas bibliotecas PWlib e OpenH323lib, sobretudo nessa última. De fato, a biblioteca PWLib é utilizada apenas como uma interface comum para comunicação com o Sistema Operacional. Como essa biblioteca é utilizada por praticamente todas as aplicações que utilizam as bibliotecas do OpenH323, esse procedimento foi aqui também adotado.

No que se refere à biblioteca OpenH323, todas as operações da pilha H.323 são implementadas por ela.

Durante o desenvolvimento da aplicação, as bibliotecas e a aplicação foram compiladas, de forma que o programa executável gerado utilizasse essas bibliotecas de forma dinâmica, na máquina local, sem incluí-las em seu código objeto. Ao final da implementação, as bibliotecas e a aplicação foram compiladas de forma que o executável gerado possuísse todas as funções necessárias no seu código objeto. Dessa forma, esse programa seria capaz de ser executado em qualquer outra máquina com compatibilidade de Sistema Operacional, sem a necessidade prévia de compilação das bibliotecas PWLib e OpenH323.

Para executar a aplicação, considerando que essa era compilada de forma compartilhada (*shared*) com as bibliotecas previamente citadas, a variável de ambiente "LD_LIBRARY_PATH" precisou ser adicionada através do seguinte comando.

```
"export LD_LIBRARY_PATH=($PWLIBDIR)/lib:($OPENH323DIR)/lib"
```

A fim de reduzir esforços desnecessários concernentes ao objetivo desse projeto, o código fonte foi compilado apenas no ambiente Unix. Como o código faz uso das bibliotecas PWLib, ele é totalmente portável para o ambiente Windows®, caso isso seja necessário. Deve ficar claro que, nesse caso, a compilação nessa plataforma deveria ser efetuada.

4.4 Ferramentas auxiliares de implementação

Para realizar o desenvolvimento do projeto, algumas ferramentas auxiliares foram empregadas. As seções 4.4.1 e 4.4.2 descrevem as principais características dessas ferramentas.

4.4.1 Projeto OpenH323

O projeto OpenH.323 tem como objetivo criar uma implementação da pilha de protocolos ITU H323 que seja completa, interoperável e de código aberto. Qualquer implementação, comercial ou não, está livre de qualquer pagamento por utilização dessa implementação. Esse projeto teve início em setembro de 1998 pela Equivalence Pty Ltd, uma companhia privada australiana.

Foi muito conveniente o uso dos recursos disponibilizados pelo projeto OpenhH323 no desenvolvimento da ferramenta, uma vez que as implementações

comerciais da pilha H.323 são caras, tanto para obtenção da licença de uso quanto para a distribuição do código gerado.

Esse projeto é atualmente coordenado pela Quicknet Technologies, porém continua aberto a qualquer um que esteja interessado em seu uso. Encoraja-se a publicação de todo uso comercial ou privado do código do OpenH323, sob a licença MPL (Mozilla Public License).

O projeto OpenH323 também está apto a realizar contratos para consultoria em desenvolvimento de aplicações H.323. Sucessos recentes de tais parcerias incluem projetos para companhias como a Agilent, Nortel, Lucent e Net2Phone, só para citar alguns exemplos.

De maneira geral, as bibliotecas do OpenH323 estão baseadas na versão 4 do padrão ITU H.323. Entretanto, deve-se ter em mente que algumas características dessa versão podem estar fora da implementação corrente, ou mesmo novos recursos de versões posteriores podem estar presentes na página oficial do projeto (OpenhH323, 2005).

4.4.2 Bibliotecas PWLib e OpenH323lib

A biblioteca PWLib (PWLib, 2005) é uma biblioteca multiplataforma, que pode ser usada para escrever aplicações que serão compiladas e executadas em Sistemas Operacionais Windows, Linux e algumas outras variantes do Unix. Ela foi desenvolvida pela Equivalence, sendo também de caráter *open source*.

Já a biblioteca OpenH323lib (OpenH323lib, 2005), através de suas inúmeras classes, implementa as funcionalidades necessárias ao desenvolvimento de terminais H.323, MCU, *Gatekeeper* e *gateways*.

As documentações dessas bibliotecas são grandes o suficiente para não serem incluídas aqui, entretanto, durante o desenvolvimento do *Gatekeeper*, foram consultadas inúmeras vezes, e devido a necessidade, constituem a maior parte da arquitetura da ferramenta.

4.5 Ambiente de Testes

O aplicativo de comunicação selecionada para auxiliar os testes do projeto, foi o Gnomemeeting, pois sua interface é amigável, de fácil manuseio e apresentou bom desempenho, comparado a outros aplicativos testados, como o OhPhone e o OpenPhone (OPENH323, 2005).

No início de sua operação, o aplicativo "escuta" os pedidos de comunicação na porta pré-estabelecida (TCP 1720), assim, qualquer terminal H.323, em especial o elemento *Gatekeeper*, pode iniciar uma comunicação ao abrir uma chamada com a ferramenta na porta citada. A arquitetura da rede utilizada para testes pode ser encontrada na Figura 13.

O *Gnomemeeting* é capaz de realizar registro e desregistro junto a um *Gatekeeper*, tanto diretamente, através de um endereço IP, quanto por "*descobrimento multicast*", onde uma consulta é feita através da rede à procura de *Gatekeeper*s. Caso essa última opção seja a escolhida, a consulta ao GK deve ser feita sem o fornecimento de um endereço, mas

apenas através do *alias* desejado para registro. A chamada pode ser efetuada desta mesma forma, através do endereço IP destino ou a utilização do *alias* destino.

O comportamento utilizado para resposta a um pedido de chamada é aceitar automaticamente ou não esse pedido (essa característica é configurável pela definição do padrão H.323).

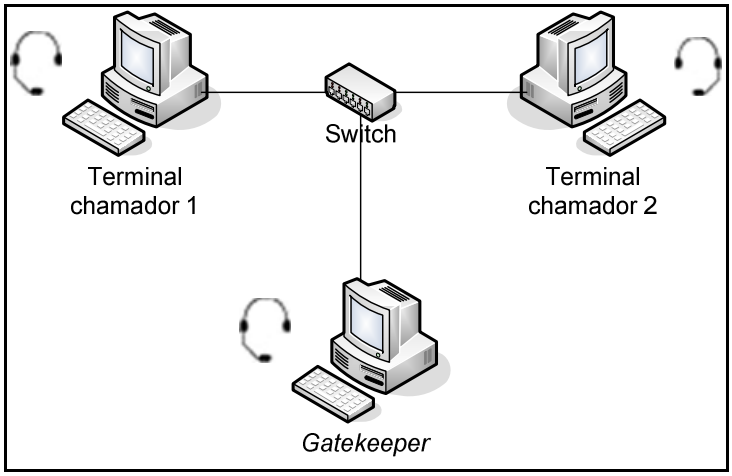


Figura 13: Ambiente de testes da ferramenta.

Na realização dos testes, verificaram-se alguns cenários de operação. Tais cenários, presentes na especificação do padrão, visam apresentar as trocas básicas de mensagens entre as entidades H.323.

Vale ressaltar que todas as trocas de mensagens já foram mencionadas e explicitadas em capítulos anteriores.

O aplicativo *Gnomemeeting*, na Figura 14, mostra em seu Histórico Geral a conexão e interação feita com o *Gatekeeper* desenvolvido.

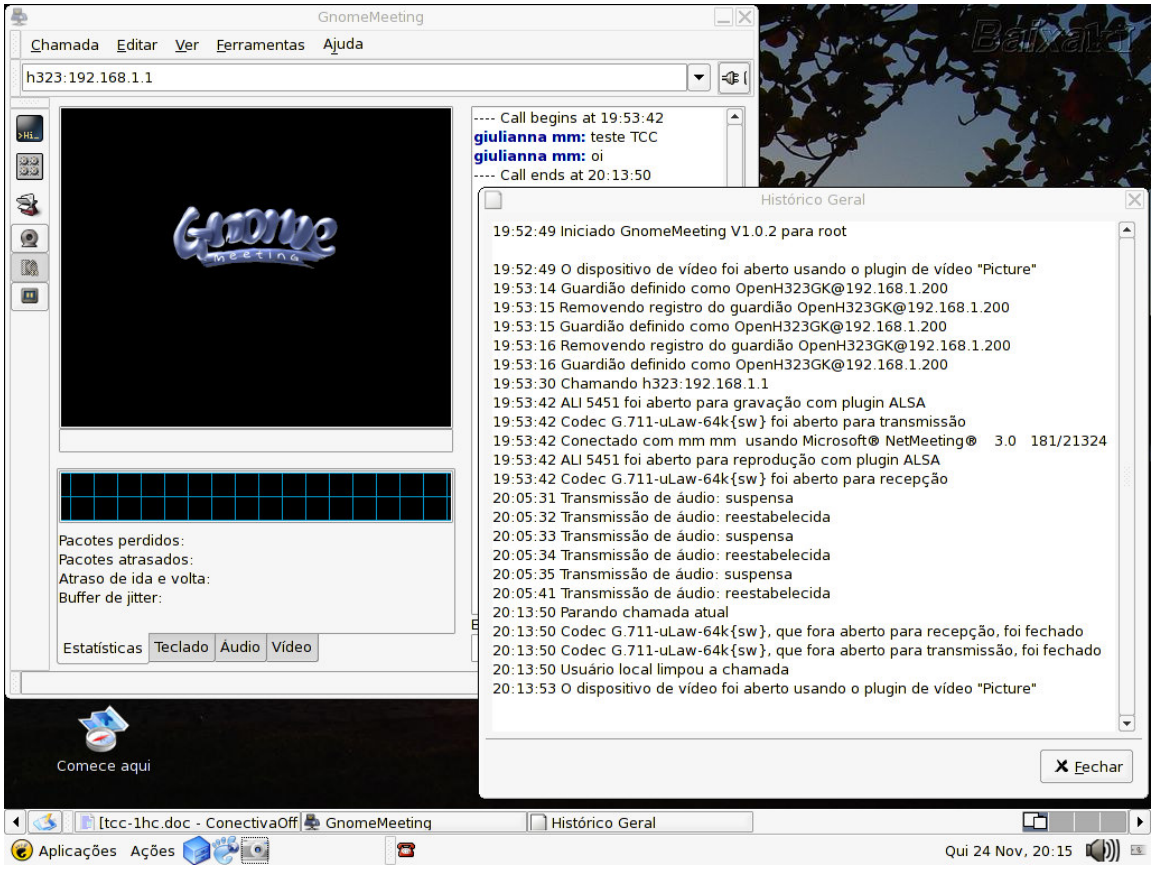


Figura 14: Histórico Geral do Gnomemeeting após a conexão com o Gatekeeper

O *Gnomemeeting* atribui o nome de Gardião ao *Gatekeeper* devido ao grande controle da ligação que o mesmo efetua. Para melhor visualização, segue abaixo onde indica a conexão efetuada.

```
19:52:49 Iniciado GnomeMeeting V1.0.2 para root
19:52:49 O dispositivo de vídeo foi aberto usando o plugin de
vídeo "Picture"
19:53:14 Guardião definido como OpenH323GK@192.168.1.200
19:53:15 Removendo registro do guardião
OpenH323GK@192.168.1.200
19:53:15 Guardião definido como OpenH323GK@192.168.1.200
19:53:16 Removendo registro do guardião
OpenH323GK@192.168.1.200
19:53:16 Guardião definido como OpenH323GK@192.168.1.200
19:53:30 Chamando h323:192.168.1.1
```

CONCLUSÃO E PERSPECTIVAS

Em relação ao padrão H.323, nem todos os possíveis ambientes de testes foram utilizados, tendo em vista que o objetivo da ferramenta é apresentar de forma clara a troca de mensagens básicas numa comunicação seguindo as especificações desse padrão e analisar os registros feitos pelo *Gatekeeper.*

Com a fase de testes completada, fica clara a adequação da ferramenta aos objetivos propostos, podendo ser ela utilizada como ferramenta VoIP englobando os aspectos básicos do H.323.

Considerando a arquitetura de comunicação multimídia obtida, o *Gatekeeper* desenvolvido e testado, cumpriu com seus objetivos, podendo assim ser incorporado inclusive em provedores de telefonia IP para efetuar registros e controle de usuários.

Em relação ao desenvolvimento da ferramenta, algo a respeito das bibliotecas de código aberto deve ser mencionado. De fato, nem todos os recursos das bibliotecas PWLib e OpenH323 foram utilizados. Isso se deve ao fato de que essas bibliotecas possuem uma completude muito grande em relação aos objetivos definidos no escopo da ferramenta, principalmente se tratando da biblioteca OpenH323. Com essa última, características avançadas do padrão H.323 são possíveis de ser implementadas, características mesmo incomuns na maioria das aplicações comerciais, como aprofundar a utilização dessa biblioteca para atribuir valores as chamadas destinadas a rede STFC, fazendo o tratamento dos controles de utilização do sistema.

REFERÊNCIAS BIBLIOGRÁFICAS

(CLAUDE, 2002)	Claude, Falbriad; Protocolos e Aplicações para Rede de Computadores, Ed. Érica; Janeiro 2002
(COMER, 1998)	COMER, Douglas E. Interligação em Rede com TCP/IP. Ed. Campus. Rio de Janeiro, 1998.
(CTI USP, 2005)	Coordenadoria de Tecnologia da Informação – USP. Disponível em: www.usp.br/cci/downloads/VoIP-CTI-20-05-2005.ppt
(DAMIEN SANDRAS, 2005)	Disponível em: www.gnomemeeting.org
(GVT, 2005)	Disponível em: http://www.gvt.com.br/home/index.jsp
(HERSENT, 2002)	HERSENT, Oliver. Telefonia IP. Ed. Addison Wesley. São Paulo, 2002.
(ITU, 2005)	(ITU, 2005) - Página oficial do ITU. Disponível em: http://www.itu.org.
(McCABE, 1998)	MCCabe, James D.; Practical Computer Network Analysis and Desing; Morgan Kaufmann Series in Networking, 1998.
(Net2Phone, 2005)	Net2phone. Disponível em: www.net2phone.com
(Nikotel, 2005)	Nikotel. Disponível em: www.nikotel.com
(OPENH323, 2005).	Página oficial do projeto - OpenH323. Disponível em: http://www.openh323.org
(OpenH323lib, 2005),	Página oficial do projeto - OpenH323. Disponível em: http://www.openh323.org
(PACKETIZER, 2005)	Página com referências para documentações de padrões de comunicação multimídia. Disponível em: http://www.packetizer.org
(PENNO, 1999)	Minicurso Voz sobre IP e Voz sobre Frame Relay, SBRC, Maio 1999

(PRYCKER, 2005) Página com referências para documentações de padrões de comunicação multimídia. Disponível em: http://www.packetizer.org

(PWLib, 2005) Página oficial do projeto - OpenH323. Disponível em: http://www.openh323.org

(RNP, 2005) Página da Rede Nacional de Ensino e Pesquisa (RNP) sobre videoconferência. Disponível em: http://www.rnp.br/videoconferencia

(SILVA, 2000) Silva, A., Qualidade De Serviço Em Voip, Rnp Newsgeneration, Volume 4, Número 3, Maio 2000.

(SkypeIn, 2005) SkypeIn. Disponível em: www.skype.com/products/skypein

(SkypeOut, 2005) Skype. Disponível em: (www.skype.com/products/skypeout), acesso em: 19/11/2005.

(TANENBAUM, 2003) TANENBAUM, Andrew S. Redes de Computadores. Ed Elsevier. Rio de Janeiro, 2003.

(YAMADA, 2001) Yamada, Hideaki; Higuchi, Norio; Voice Quality Evaluation of IP-Based Voice Stream Multiplexing Schemes, KDDI R&D Laboratories Inc.; Japan, 2001.