PROJETO DE REDES
www.projetoderedes.com.br

INSTITUTO DE TECNOLOGIA DA AMAZÔNIA

RONALDO NUNES PEREIRA

VOZ SOBRE IP

UMA PROPOSTA DE IMPLANTAÇÃO

Manaus

2004

RONALDO NUNES PEREIRA

VOZ SOBRE IP

UMA PROPOSTA DE IMPLANTAÇÃO

Monografia em Redes de Computadores
Para a obtenção do título de Bacharel em Eng.ª de Computação
Instituto de Tecnologia da Amazônia – UTAM
Departamento de Computação

Orientador: Prof. MSc. Antônio Cauper Filho

Manaus

2004

INSTITUTO DE TECNOLOGIA DA AMAZÔNIA

RONALDO NUNES PEREIRA

VOZ SOBRE IP

UMA PROPOSTA DE IMPLANTAÇÃO

Monografia em Redes de Computadores
Para a obtenção do título de Bacharel em Eng.ª de Computação
Instituto de Tecnologia da Amazônia – UTAM
Departamento de Computação

Aprovada por:

.....
Prof. Orientador Antônio Cauper Filho, MSc. (UTAM)

.....
Prof. Ednaldo Coelho Pereira, MSc. (UTAM)

.....
Prof. Rodrigo Choji de Freitas, Esp. (UTAM)

Aprovada em..... / ..... / 2005

Manaus

2004

DEDICATÓRIA

Aos meus pais, Omar e Ivaneide por todas as suas angústias e preocupações que passaram por minha causa, pelo amor, carinho e proteção que me deram, dedico-lhes esta conquista com toda a minha gratidão.

AGRADECIMENTOS

Agradeço a imprescindível ajuda de meu orientador, Prof. Cauper, pela paciência com que sempre me acolheu.

Agradeço à coordenadora da disciplina, Prof.ª Ângela por ter me ajudado sempre que precisei.

Agradeço a minha esposa Denise pela contribuição, amor e paciência em todos os meus anos de curso.

Agradeço aos meus filhos, Raffael e Rodrigo, pois sempre que fraquejava apenas um afago dessas pequenas criaturas me tornavam forte novamente.

Agradeço ao meu chefe na SEMEF, Denis pelas várias ausências, atrasos e saídas antes da hora que ele permitiu.

Agradeço a meus amigos e colegas pelo apoio e estímulo, em especial a minha grande amiga Karen Monteiro que tornou esta monografia possível.

Na natureza não existem prêmios, nem castigos, apenas conseqüências.

Carlos Castanheda.

O valor das coisas não está no tempo em que elas duram, mas na intensidade com que acontecem. Por isso existem momentos inesquecíveis, coisas inexplicáveis e pessoas incomparáveis.

Fernando Pessoa

Não existe nada completamente errado no mundo, mesmo um relógio parado consegue estar certo duas vezes ao dia.

Paulo Coelho

O homem é um sucesso se pula da cama de manhã e vai dormir a noite, e nesse meio tempo faz o que gosta.

Bob Dylan

Um passo a frente e você não está mais no mesmo lugar.

Anônimo

RESUMO

Esta monografia apresenta as principais vantagens da implantação de uma rede de voz sobre IP (VoIP – Voice over IP) em uma rede corporativa, tais como: a diminuição de custos com ligações telefônicas locais, interurbanas e até mesmo internacionais. Tal implantação, em alguns casos, é bastante simples e torna-se muito mais vantajosa caso a empresa já possua uma rede de dados. O uso de um protocolo padrão já bastante conhecido e utilizado no mundo todo como o IP só faz aumentar a confiança em utilizá-lo também para a transmissão de voz. Como as conversações telefônicas têm características de tempo-real faz-se necessário utilizar uma série de subsídios extras para garantir a qualidade do serviço das ligações, ou seja, uma política de qualidade (QoS – Quality of Service) bastante apurada. Voz sobre IP pode ser uma alternativa bastante viável e confiável não apenas para empresas que necessitam reduzir seus custos com ligações telefônicas, mas também para aquelas que precisam modernizar sua telefonia, gerenciando melhor sua infra-estrutura telefônica, acrescentando milhares de ramais (um ramal por funcionário, por exemplo), podendo estabelecer cotas de conversação entre outras possibilidades. A modernísima tecnologia VoIP demanda um alto custo, sendo este um forte ponto negativo, com essa desvantagem essa tecnologia ainda fica fora da realidade da maioria das pequenas empresas, tendo com isso uma limitação em seu universo de uso, ficando restrita a apenas as médias e grandes empresas.

Palavras-chave:
VoIP – Voz sobre IP – Redes de Computadores – Telefonia IP

ABSTRACT

This monograph presents the main advantages of the implantation of a net of Voice over IP (VoIP – Voice over IP) in a corporate net, such as: the decrease of costs with phone calls local, intercity and even international. Such implantation, in some cases, it is quite simple and it becomes much more advantageous case the company already possesses a net of data. The use of a standard protocol already plenty known and used in the whole world as IP only makes to also increase the trust in using it for the transmission of the voice. As the phone conversations have characteristics of time-real is done necessary to use a series of extra subsidies to guarantee the quality of the service of the connections, in other words, a quality politics (QoS - Quality of Service) quite select. Voice over IP can be a quite viable and reliable alternative not just for companies that need to reduce their costs with phone calls, but also for those that need modernize your telephony, managing your phone infrastructure better, increasing thousands of extensions (an extension for employee, for example), could establish conversation quotas among other possibilities. The modern technology VoIP demands a high cost, being this a fort negative point, with that disadvantage that technology is still out of the reality of most of the small companies, tends with that a limitation in your use universe, being just restricted the averages and great companies.

Word-key:
VoIP - Voice over IP – Net of Computers – Telephony IP.

LISTA DE ILUSTRAÇÕES

Figura 01: Sistemas de processamento em lote..... 16
Figura 02: Sistema de time-sharing..... 17
Figura 03: Compartilhamento de recursos..... 18
Figura 04: Hub e Switch..... 22
Figura 05: Modelo OSI em camadas e protocolos..... 25
Figura 06: Comparação entre os modelos OSI e TCP/IP..... 27
Figura 07: Relacionamento entre os protocolos IP, TCP e UDP..... 28
Figura 08: Forma geral de um Ipv6..... 31
Figura 09: Ligação telefônica IP sem PSTU e ISDN..... 33
Figura 10: Ligação telefônica IP com rede ISDN presente..... 33
Figura 11: Eco do locutor..... 35
Figura 12: Eco do ouvinte..... 35
Figura 13: Headset..... 37
Figura 14: Telefone viva-voz..... 38
Figura 15: handset..... 39
Figura 16: Cancelador de eco elétrico num cenário VoIP – PSTN..... 40
Figura 17: Cenário com a presença de eco elétrico e eco acústico..... 41
Figura 18: Telefonia Analógica..... 44
Figura 19: Chamada de voz do terminal A para o terminal B..... 49
Figura 20: Encontrando um gatekeeper..... 54
Figura 21: Completando a chamada..... 56
Figura 22: Fechando os canais de comunicação..... 58
Figura 23: Telefone IP..... 59
Figura 24: Cenário atual da rede computacional da SEMEF..... 63
Figura 25: Sistema atual de telefonia da SEMEF..... 64
Figura 26: Vocoder IEN 6000..... 66
Figura 27: PABX BXS / 20..... 68
Figura 28: Sistema VoIP da SEMEF..... 70

LISTA DE ABREVIATURAS E SIGLAS

AEC	Acoustic Echo Canceller – Cancelador de Eco Acústico.
ARQ	Admission Request – Pedido de Admissão.
ATM	Assynchronous Transfer Mode – Modo de Transferência Assíncrono: Moderno modelo de rede de altíssima velocidade.
BRQ	Bandwidth Request – Pedido de Largura de Banda.
CAC	Centro de Atendimento ao Contribuinte.
dB	Decibéis – Unidade de medida de som.
DCF	Disengage Confirm – Confirmação de Divórcio.
DNS	Domain Name Service – Serviço de Nomes de Domínio: protocolo prestador de serviços de nomes de domínio.
DoS	Denied of Service – Negação de Serviço.
DRQ	Disengage Request – Pedido de Divórcio.
DTMF	Digital Tone Multi Frequency – Multi Freqüência de Tom Digital.
EEC	Electric Echo Canceller – Cancelador de Eco Elétrico.
FTP	File Transmission Protocol – Protocolo Transmissor de Dados.
Gbps	Gigabits por segundo: Taxa de transmissão numa rede.
GFC	Gatekeeper Confirm – Confirmação de Gatekeeper.
GRQ	Gatekeeper Request – Requisição Multicast.
HTTP	Hyper Text Transfer Protocol – Protocolo de Transferência de Hiper Texto.
IEEE	Institute of Electrical and Eletronics Engineers – Instituto de Engenheiros Elétricos e Eletrônicos.
IETF	Internet Engineering Task Force – Força Tarefa para a Engenharia da Internet.
IMTC	International Multimedia Teleconferencing Consortium - Consórcio Internacional de Multimídia e Teleconferência.
IP	Internet Protocol – Protocolo de Internet: conjunto de normas e regras adotadas para permitir que diferentes equipamentos mantenham comunicação.
IPX	Internet Protocol eXtended – Protocolo compatível com redes Novel Netware.
IRC	Internet Relay Chat – Conversa Reservada pela Internet.
IRR	Information Request – Pedido de Informação.
ISDN	Integrated Service Digital Network – Rede Digital com Serviços Integrados: Modernas redes computacionais que integram numa mesma banda; vídeo, áudio e texto.

ISO	Internacional Standardization Organization – Organização Internacional de Padronização: Entidade internacional formada por cientistas, empresas, professores, estudantes, etc. visando à padronização internacional dos componentes de rede.
ITMC	International Multimedia Teleconferencing Consortium – Consórcio Internacional de Multimídia e Teleconferência.
ITU	International Telecommunication Union – União Internacional de Telecomunicações.
LAN	Local Area Network – Rede de Área Local.
LDAP	Lightweight Directora Access Protocol – Protocolo Leve para Acesso ao Diretório.
MAN	Metropolitan Área Network – Rede de Área Metropolitana.
Mbps	Mega bits por segundo: Taxa de transmissão numa rede.
MC	Multipoint Controller – Controlador Multiponto.
MCU	Multipoint Control Unit – Unidade de Controle Multiponto.
MP	Módulo Processador – Cada um dos componentes de uma rede.
ms	Milisegundos – Unidade de medida de tempo.
NNTP	Network News Transfer Protocol – Protocolo de Transferência para novas redes.
OSI	Open System Interconnection – Sistema Aberto de Interconexão: Modelo de conexão de redes criado pela ISO.
PABX	Private Automatic Branch Exchange – Alteração de Filial Automática e Particular: Equipamento que realiza o chaveamento de uma rede de telefonia.
PC	Personal Computer – Computador pessoal.
PMM	Prefeitura Municipal de Manaus.
PSTN	Public Switched Telephone Network – Rede de Telefonia Alternada Pública: Rede de telefonia tradicional e analógica.
QoS	Quality of Service – Qualidade de Serviço: é a política adotada para usufruir o máximo de qualidade de um produto ou serviço.
RAS	Registration, Admission and Status – Estado de Admissão e Registro.
RR	Receiver Reports – Receptor de Relatórios.
RRQ	Registration Request – Pedido de Registro.
RSVP	Resource reSerVation Protocol - Protocolo de Reserva de Recursos.
RTCP	Real-Time Control Protocol – Protocolo de Controle de Tempo Real.
RTP	Real -Time Transport Protocol – Protocolo de Transporte em Tempo Real.
SEMEF	Secretaria Municipal de Economia e Finanças.
SIPP	Simple Internet Protocol Plus – Protocolo Internet Simplificado e Melhorado.
SMTP	Simple Mail Transfer Protocol – Protocolo de Transferência Simples de E-mail.
SPX	Superior Protocol eXtended – Protocolo compatível com Novell Netware.

SR	Send Report – Envio de Relatórios.
Tbps	Terabits por segundo: Taxa de transmissão numa rede.
TDM	Time Division Multiplexing – Multiplexando a Divisão de Tempo.
TELNET	Terminal Virtual Network – Terminal Virtual de Redes: Protocolo simulador de terminal.
TCP	Transmission Control Protocol – Protocolo de controle de transmissão.
TTL	Time To Live – Tempo Para Viver.
UDP	User Datagram Protocol – Protocolo de Datagrama de Usuário: protocolo sem conexão não confiável para aplicações que não necessitam nem de controle de fluxo, nem da manutenção da seqüência das mensagens enviadas.
URQ	Unregistration Request – Pedido de Retirada.
VAT	Vídeo Audio Tool – Ferramenta Audio Visual.
VoIP	Voice over IP – Voz sobre IP: Moderna tecnologia de rede que promove a convergência das redes de telefonia e computadores.
WAN	Wide Area Network – Rede de Área Longa
www	World Wide Web – Teia de Alcance Mundial: Serviço mais notório e famoso da Internet.

SUMÁRIO

INTRODUÇÃO..... 14

1 UMA BREVE HISTÓRIA DAS REDES DE COMPUTADORES..... 16
1.1 Redes de Computadores..... 18
1.2 Concentradores de Rede..... 20
1.3 Arquitetura de Redes..... 23
1.3.1 Modelo de Referência OSI..... 23
1.3.2 Arquitetura TCP/IP..... 25
1.3.2.1 Camada Inter-redes..... 26
1.3.2.2 Camada de Transporte..... 27
1.3.2.3 Camada de Aplicação..... 28
1.3.2.4 Camada Host/Rede..... 29
1.4 Protocolo IP..... 30

2 PROBLEMAS COM A VOZ..... 32
2.1 Conexão de referência..... 32
2.2 Eco em uma rede telefônica..... 34
2.2.1 Eco de locutor - Eco de ouvinte..... 34
2.2.2 Eco híbrido..... 35
2.2.3 Eco Acústico..... 36
2.2.4 Como limitar o eco..... 39
2.2.4.1 Supressores de eco..... 39
2.2.4.2 Canceladores de eco..... 40

3 PADRÃO VoIP - H.323..... 42
3.1 Uma breve história..... 42
3.2 Do RTP ao H.323..... 43
3.3 Transportando voz sobre uma rede de pacotes..... 44
3.4 Por que RTP / RTCP?..... 45
3.5 H.323 propriamente dito..... 47
3.5.1 Chamada de voz do terminal A para o terminal B..... 47
3.5.1.1 Primeira fase: inicializando a chamada..... 48
3.5.1.2 Segunda fase: estabelecendo o canal de controle. 49
3.5.1.3 Terceira fase: início da chamada..... 50
3.5.1.4 Quarta fase: diálogo..... 50
3.5.2 Chamando um telefone comum a partir da Internet..... 51
3.5.2.1 Primeira fase: onde está o gatekeeper?..... 53

3.5.2.2 Segunda fase: permitindo nova chamada..... 54
3.5.2.3 Terceira fase: sinalização da chamada..... 55
3.5.2.4 Fase de término..... 57

4 PROJETO DE IMPLANTAÇÃO NA SEMEF..... 59
4.1 Equipamentos utilizados na solução de voz sobre IP..... 59
4.1.2 Telefone IP..... 59
4.2 Qualidade do serviço – QoS..... 60
4.2.1 Considerações para qualidade..... 60
4.2.1.1 Jitter..... 60
4.2.1.2 Latência..... 60
4.2.1.3 Largura de banda..... 61
4.2.1.4 Perda de pacotes..... 61
4.2.1.5 Segurança..... 62
4.2.1.6 Confiabilidade..... 62
4.3 Cenário atual da rede SEMEF..... 63
4.4 Cenário proposto para a rede da SEMEF..... 65
4.4.1 Situação 1: Chamada VoIP de um terminal para outro entre os prédios..... 68
4.4.2 Situação 2: Chamada de um ramal IP de um prédio para outro ou para o mesmo prédio..... 68
4.4.3 Situação 3: Chamada de um ramal IP para uma estação de trabalho e vice-versa..... 69
4.4.4 Situação 4: Chamando um telefone externo a partir de um ramal IP ou estação de trabalho..... 69

CONCLUSÃO..... 71

REFERÊNCIAS BIBLIOGRÁFICAS..... 72

INTRODUÇÃO

O homem sempre teve a necessidade de se comunicar, e com o passar dos séculos veio a necessidade de se comunicar a grandes distâncias. Formas de comunicação através de sinais de fumaça ou pombos correio foram as maneiras encontradas por nossos ancestrais para tentar aproximar as comunidades distantes. O telégrafo, o rádio, a tv e os computadores são exemplos do esforço humano em desenvolver novas tecnologias tendo como principal objetivo a comunicação. Dentro da informática, à área de rede desponta como a principal ramificação desta ciência não importa qual seja a sua área de atuação; banco de dados, desenvolvimento etc. Você sempre precisará de uma rede atuando por trás, como uma fundamental ferramenta para auxiliar em seus projetos e mesmo divulgar seus resultados. Uma das mais modernas, interessante e complexa representante do cenário das novas tecnologias de rede é a VoIP (*Voice over IP*). Com o vertiginoso desenvolvimento das tecnologias para sistemas de informação, vimos à instalação das redes de telefonia em escala mundial, acarretando alguns problemas colaterais em empresas de todos os tipos e tamanhos, o mais doloroso deles é o custo das ligações internacionais, interurbanas ou até mesmo aquelas milhares ligações locais que fazemos em nossos locais de trabalho todos os dias. Organizações com centenas de escritórios dispersos por uma extensa área geográfica podem, através do apertar de um botão, analisar o status atual de suas filiais mais remotas, porém não conseguem gerenciar

sua estrutura telefônica, sofrendo desperdícios consideráveis ao final de seu ano fiscal. Este é o primeiro cenário de utilização da tecnologia VoIP, utilizar a já existente rede de computadores das grandes corporações para diminuir os custos de telefonia e gerenciar essa conturbada área dentro das empresas. A Secretaria Municipal de Economia e Finanças (SEMEF), como quase todas grandes corporações possui os mesmos problemas de telefonia, visando diminuir os custos com a conta telefônica e um melhor gerenciamento de sua infra-estrutura de telefonia, esta monografia apresenta uma proposta de implantação de um sistema VoIP na SEMEF. No primeiro capítulo tem-se uma breve abordagem na história das redes de computadores, seus conceitos e definições, modelo OSI, arquitetura TCP/IP com ênfase no protocolo IP. No segundo capítulo mostra-se dois antigos problemas dos engenheiros de telefonia que junto com a tecnologia VoIP entraram para o vocabulário dos profissionais de informática – Eco e Atraso – Suas definições, os tipos de conexões nas quais incidem e também formas de amenizá-los ou excluí-los da proposta de implantação. No capítulo 3 faz-se uma abordagem ao padrão VoIP utilizado na proposta o H.323, ou seja, é a teoria que irá fornecer embasamento a parte prática do projeto: os protocolos utilizados, definição e caracterização do gatekeeper que será o principal componente (em software) a ser utilizado. O capítulo 4 mostra a proposta de implantação: os equipamentos que serão necessários; os que a instituição já possui e os que serão necessários ser comprados. As principais considerações sobre a qualidade do Sistema VoIP-SEMEF, parâmetros de comparação e propostas de melhorias. No capítulo encontra-se também gráficos com as estruturas de dados e telefonia atuais da instituição e um gráfico demonstrando a convergência entre as duas redes. Tem-se também, as quatro situações iniciais de utilização da tecnologia VoIP na SEMEF.

1 UMA BREVE HISTÓRIA DAS REDES DE COMPUTADORES

Na década de 1950, computadores eram máquinas grandes e complexas, operadas por pessoas altamente especializadas. Usuários enfileiravam-se para submeter suas leitoras de cartões ou fitas magnéticas que eram processados em lote (como na figura 01).

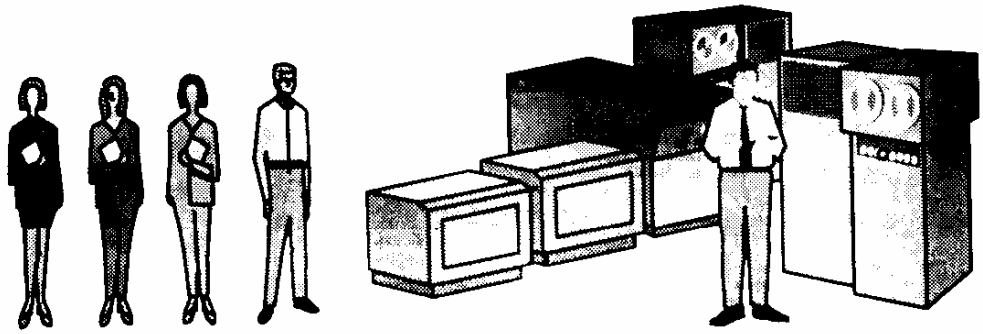

Figura 01: Sistemas de processamento em lote.

Não havia nenhuma forma de interação direta entre usuários e máquina. Avanços na década de 1960 possibilitaram o desenvolvimento dos primeiros terminais interativos, permitindo aos usuários acesso ao computador central através de linhas de comunicação. Usuários passavam a ter então um mecanismo que possibilitava a interação direta com o computador, ao mesmo tempo em que avanços nas técnicas de processamento davam origem a sistemas de tempo compartilhado (time-sharing), permitindo que várias tarefas dos diferentes usuários ocupassem simultaneamente o computador central, através de uma espécie de revezamento no tempo de ocupação do processador.

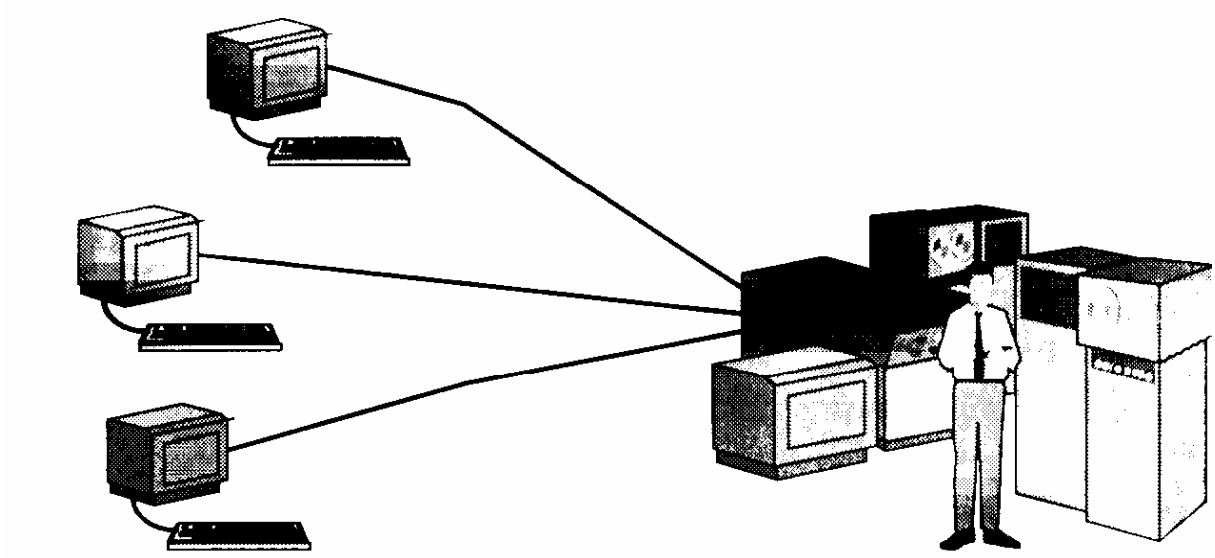

Figura 02: Sistema de time-sharing.

Mudanças na caracterização dos sistemas de computação ocorreram durante a década de 1970: de um sistema único centralizado e de grande porte, disponível para todos os usuários de uma determinada organização, partia-se em direção à distribuição do poder computacional. O desenvolvimento de minis e microcomputadores de bom desempenho, com requisitos menos rígidos de temperatura e umidade, permitiu a instalação de considerável poder computacional em várias localizações de uma organização, ao invés da anterior concentração deste poder em uma determinada área. Embora o custo de hardware de processamento estivesse caindo, o preço dos equipamentos eletromecânicos continuava alto. Mesmo no caso de dados que podiam ser associados a um único sistema de pequeno porte, a economia de escala exigia que grande parte dos dados estivessem associados a um sistema de grande capacidade centralizado. Assim a interconexão entre os vários sistemas para o uso compartilhado de dispositivos periféricos tornou-se importante. A capacidade de troca de informações também foi uma razão importante para a interconexão. Usuários individuais de sistemas de computação não trabalham isolados e necessitam de alguns dos benefícios oferecidos por um sistema centralizado. Entre

esses a capacidade de troca de mensagens entre os diversos usuários e a facilidade de acesso a dados e programas de várias fontes quando da preparação de um documento. Ambientes de trabalho cooperativos se tornaram uma realidade tanto nas empresas como nas universidades, exigindo a interconexão dos equipamentos nessas organizações. Para tais problemas de performance os pesquisadores criaram novas arquiteturas que propunham a distribuição e o paralelismo como forma de melhorar desempenho, confiabilidade e modularidade dos sistemas computacionais [SOARES 1995].

Figura 03: Compartilhamento de recursos.

1.1 REDES DE COMPUTADORES

Uma Rede de Computadores é formada por um conjunto de módulos processadores (MPs) capazes de trocar informações e compartilhar recursos, interligados por um sistema de comunicação.

O sistema de comunicação vai se constituir de um arranjo topológico interligando os vários módulos processadores através de enlaces físicos (*meios de transmissão*) e de um conjunto de regras com o fim de organizar a comunicação (*protocolos*). Quanto ao seu tamanho as Redes de Computadores possui três grandes classificações:

Redes Locais (*Local Area Networks – LANs*) surgiram dos ambientes de institutos de pesquisa e universidades. Com as mudanças no enfoque de sistemas de computação que ocorreram durante a década de 1970, o poder computacional foi distribuído. O desenvolvimento de minis e micro computadores de bom desempenho permitiu a instalação de considerável poder computacional em várias unidades de uma organização ao invés da anterior concentração em uma determinada área. Redes locais surgiram, assim, para viabilizar a troca e o compartilhamento de informações e dispositivos periféricos (recursos de hardware e software), preservando a independência das várias estações de processamento, e permitindo a integração em ambientes de trabalho corporativo.

Redes Metropolitanas (*Metropolitans Area Network – MANs*) quando a distância de ligação entre os vários módulos procesadores começa a atingir distâncias metropolitanas, chamamos esses sistemas não mais de redes locais, mas de Redes Metropolitanas. A definição do termo “rede metropolitana” surgiu com o aparecimento do padrão IEEE 802.6 (*Institute of Electrical and Eletronics Engineers*). Uma rede metropolitana apresenta carcterísticas semelhantes as das redes locais, sendo que as MANs, em geral, cobrem distâncias maiores que as LANs.

Redes Geograficamente Distribuídas (*Wide Area Networks – WANs*) surgiram da necessidade de se compartilhar recursos especializados por uma maior comunidade de usuários geograficamente dispersos. Por terem um custo de

comunicação bastante elevado (circuitos para satélites e enlaces de microondas), tais redes são em geral públicas, isto é, o sistema de comunicação, chamado sub-rede de comunicação, é mantido, gerenciado e de propriedade de grandes operadoras (públicas ou privadas), e seu acesso é público [SOARES 1995]. No quadro abaixo temos a classificação das redes quanto a sua distância:

Distância do interprocessador	**Processadores localizados no (a) mesmo (a)**	**Exemplo**
0,1 m	Placa de circuitos	Máquina de fluxo de dados.
1 m	Sistema	Multicomputador
10 m	Sala	Rede Local
100 m	Prédio	
1 km	Campus	
10 km	Cidade	Rede Metropolitana
100 km	País	Rede geograficamente distribuída
1.000 km	Continente	
10.000 km	Planeta	Internet

Fonte: [TANENBAUM 1997].

1.2 CONCENTRADORES DE REDE

A topologia de uma rede irá determinar, em parte, o método de acesso utilizado. Métodos de acesso são necessários para regular o acesso a meios físicos compartilhados. Assim, costuma-se associar os métodos de acesso às topologias

utilizadas. A instalação física das redes tem sofrido uma forte tendência na direção da utilização de hubs, o que, *fisicamente,* corresponde à implantação de uma topologia em estrela. Essa tendência é explicada, basicamente, pela crescente necessidade de melhorar o gerenciamento e a manutenção nessas instalações. O maior problema da topologia em estrela, como mencionado, é a sua baixa confiabilidade dada à presença de um elemento central no qual as falhas provocam a parada central do sistema. Porém, os avanços da eletrônica já permitem, hoje, que se construam equipamentos de alta confiabilidade, viabilizando esse tipo de topologia.

A utilização de hubs, no entanto, não exige, necessariamente, que as interfaces das estações com a rede a percebam como uma topologia em estrela. Do ponto de vista da interface das estações com a rede, o funcionamento se dá como em uma barra ou em um anel, com os seus respectivos métodos de acesso. Note, porém, que a implementação física, interna nos hubs, pode ser qualquer uma desde que essa interface seja preservada.

Pelo que apresentou-se, podemos diferenciar dois tipos de topologias: uma *topologia lógica,* que é aquela observada sob o ponto de vista das interfaces das estações com a rede (que inclui o método de acesso), e uma *topologia física,* que diz respeito ao layout físico utilizado na instalação da rede.

A demanda por maiores taxas de transmissão e melhor utilização dos meios físicos, aliados à evolução contínua da microeletrônica, começou a alterar a construção desses equipamentos concentradores. A partir do momento em que as estações estão ligadas a um elemento central, no qual a implementação interna é desconhecida, mas a interface é coerente com as estações, é possível pensar que esses elementos podem implementar arquiteturas que não utilizam apenas um meio

compartilhado, mas sim possibilitam a troca de mensagens entre várias estações simultaneamente. Desta forma, estações podem obter para si taxas efetivas de transmissão bem maiores do que as observadas anteriormente. Esse tipo de elemento central é denominado (assim como na topologia em estrela) switch.

Seguir essa tendência utilizando-se dos métodos de acesso para meios compartilhados impõe limitações muito grandes às taxas de transmissão que se pode atingir, muito embora tenha sido uma necessidade de mercado manter as interfaces anteriormente padronizadas. Mas a evolução natural, como não poderia deixar de ser, veio com a criação de novas interfaces de acesso que permitiram que taxas de transmissão bem maiores fossem utilizadas. Redes ATM baseiam-se na presença de switches de grande capacidade de comutação que permitem taxas de transmissão que podem chegar à ordem de Gbps.

Assim, a topologia em estrela, tanto física quanto logicamente, retoma seu lugar no mundo das redes de computadores [SOARES 1995].

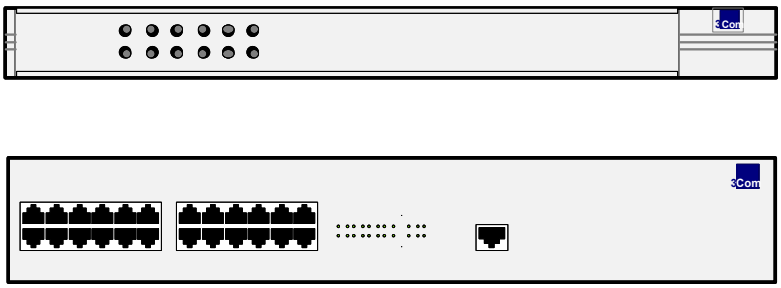

Figura 04: Hub e Switch.

1.3 ARQUITETURAS DE REDES

1.3.1 Modelo de referência OSI

Da experiência obtida no projeto de redes, vários princípios surgiram, possibilitando que novos projetos fossem desenvolvidos de uma forma mais estruturada que os anteriores. Dentre esses princípios se destaca a idéia de estruturar a rede como um conjunto de *camadas hierárquicas,* cada uma sendo construída utilizando as funções e serviços oferecidos pelas camadas inferiores.

Cada camada (ou nível) deve ser pensada como um programa ou processo, implementado por hardware ou software, que se comunica com o processo correspondente em outra máquina remota. As regras que governam a conversação de um nível N qualquer são chamadas de *protocolo* de nível N. A Figura 05 mostra um exemplo de uma estrutura com sete camadas.

Na verdade, dados transferidos em uma comunicação de um nível específico não são enviados diretamente (horizontalmente) ao processo do mesmo nível em outra estação, mas "descem", verticalmente, através de cada nível adjacente da máquina transmissora até o nível 1 (que é o nível físico onde na realidade há a única comunicação horizontal entre máquinas), para depois “subir”, verticalmente, através de cada nível adjacente da máquina receptora até o nível de destino. Os limites entre cada nível adjacente são chamados de *interfaces.*

A *arquitetura da rede é* formada por níveis, interfaces e protocolos. Cada nível oferece um conjunto de serviços ao nível superior, usando funções realizadas no próprio nível e serviços disponíveis nos níveis inferiores. Como já mencionamos, um protocolo de nível N é um conjunto de regras e formatos (semântica e sintaxe), através dos quais informações ou dados do nível N são trocados entre as entidades

do nível N, localizadas em sistemas distintos, com o intuito de realizar as funções que implementam os serviços do nível N. Um ou mais protocolos podem ser definidos em um nível.

O projeto de protocolos em níveis é a maneira mais eficiente de se estruturar uma rede. Uma vez definida claramente a interface entre os diversos níveis, uma alteração na implementação de um nível pode ser realizada sem causar impacto na estrutura global.

O número, o nome, o conjunto de funções e serviços, e o protocolo de cada camada varia de uma arquitetura de rede para outra. Inicialmente, cada fabricante desenvolveu sua própria arquitetura de modo que seus computadores pudessem trocar informações entre si. Essas arquiteturas são denominadas proprietárias porque são controladas por uma única entidade: o fabricante. Rapidamente, os usuários perceberam que as arquiteturas de redes proprietárias não eram uma boa solução, pois seu objetivo era permitir intercâmbio de informações entre computadores de um mesmo fabricante enquanto que o parque instalado na maioria das organizações era equipamentos de diferentes fornecedores.

Para permitir o intercâmbio de informações entre computadores de fabricantes distintos tornou-se necessário definir uma arquitetura única, e para garantir que nenhum fabricante levasse vantagem em relação aos outros a arquitetura teria que ser aberta e pública. Foi com esse objetivo que a International Organization for Standardization (*ISO*) definiu o modelo denominado *Model for Open System Interconnection* (*OSI*) [ISO 84, ISO 92], que propõe uma estrutura com sete níveis como referência para a arquitetura dos protocolos de redes de computadores.

Embora o modelo OSI da ISO possa ser usado tanto em redes de longa distância quanto em redes locais, ele foi, em princípio, pensado para o uso em redes

de longa distância. A coexistência de redes heterogêneas (locais, metropolitanas e de longa distância) fez com que se tornasse necessário definir uma arquitetura voltada para a interconexão dessas redes. Uma arquitetura importante no contexto de interconexão de redes heterogêneas é a Arquitetura Internet.

Figura 05: Modelo OSI em camadas e protocolos.

1.3.2 Arquitetura TCP/IP

Quando foram criadas as redes de rádio e satélite, começaram a surgir problemas com os protocolos então existentes, o que forçou a criação de uma nova arquitetura de referência. Seu objetivo era conectar várias redes ao mesmo tempo. Essa arquitetura veio a ficar conhecida como arquitetura **TCP/IP** (*Transmission Control Protocol / Internet Protocol*)**,** graças a seus dois principais protocolos. Esse modelo foi definido pela primeira vez por Cerf e Kahn, 1974. Uma nova perspectiva foi oferecida em Leiner et al., 1985. A filosofia de projeto na qual se baseia o modelo é discutida em Clark, 1988.

Diante da preocupação do Pentágono de que seus preciosos hosts, roteadores e gateways de inter-rede fossem destruídos de uma hora para outra,

definiu-se também que a rede fosse capaz, de sobreviver à perda de hardwares da sub-rede, impedindo que as conversas que estivessem sendo travadas fossem interrompidas. Em outras palavras, o Pentágono queria que as conexões permanecessem intactas enquanto as máquinas de origem e de destino estivessem funcionando, mesmo que algumas máquinas ou linhas de transmissão intermediárias deixassem de operar repentinamente. Por essa razão, era preciso criar uma arquitetura flexível, capaz de se adaptar a aplicações com necessidades divergentes, como por exemplo a transferência de arquivos e a transmissão de dados de voz em tempo real.

1.3.2.1 Camada Inter-redes

Todas essas necessidades levaram à escolha de uma rede de comutação de pacotes baseada em uma camada de ligação inter-rede. Essa camada, chamada de camada inter-redes, integra toda a arquitetura. Sua tarefa é permitir que os hosts injetem pacotes em qualquer rede e garantir que eles sejam transmitidos independentemente do destino (que pode ser outra rede). E possível, inclusive, que esses pacotes cheguem em outra ordem diferente daquela em que foram enviados, obrigando as camadas superiores a reorganizá-los, caso a entrega tenha de respeitar algum tipo de ordem. Observe que, nesse caso, a expressão "inter-rede" é usada no sentido genérico, muito embora essa camada esteja presente na Internet.

A analogia usada nesse caso diz respeito ao sistema de correio. Uma pessoa pode soltar uma seqüência de cartas internacionais em uma caixa de correio em um país e, com um pouco de sorte, a maioria delas será entregue no endereço correto no país de destino. Provavelmente as cartas atravessarão um ou mais gateways internacionais, mas esse processo é transparente para os usuários. Por

essa razão, cada país (ou seja, cada rede) tem seus próprios selos, tamanhos de envelope preferidos e regras de entrega escondidas dos usuários.

A camada inter-redes define um formato de pacote oficial e um protocolo chamado de IP (*Internet Protocol*). A tarefa da camada inter-redes é entregar pacotes IP onde eles são necessários. O roteamento é uma questão de grande importância nessa camada, assim como evitar congestionamentos. Por essas razões, é razoável dizer que a função da camada inter-redes TCP/IP é muito parecida com a da camada de rede OSI. A Figura 06 mostra a correspondência entre elas.

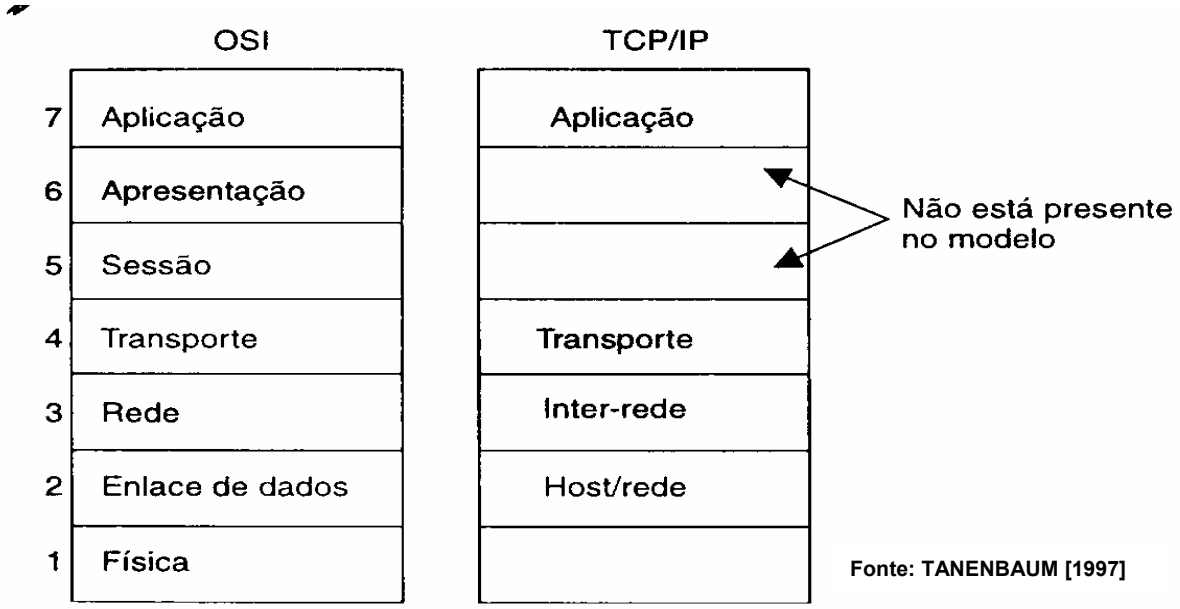

Figura 06: Comparação entre os modelos OSI e TCP/IP.

1.3.2.2 Camada de Transporte

No modelo TCP/IP, a camada localizada acima da camada inter-redes é chamada de **camada de transporte**. A finalidade dessa camada é permitir que as entidades par (peer entity) dos hosts de origem e de destino mantenham uma conversação, exatamente como acontece na camada de transporte OSI. Dois protocolos fim a fim foram definidos aqui. O primeiro deles, o TCP **(***Transmission*

Control Protocol)**,** é um protocolo orientado à conexão confiável que permite a entrega sem erros de um fluxo de bytes originado de uma determinada máquina em qualquer computador da inter-rede. Esse protocolo fragmenta o fluxo de bytes de entrada em mensagens e passa cada uma delas para a camada inter-redes. No destino, o protocolo TCP remonta as mensagens recebidas no fluxo de saída. O TCP cuida também do controle de fluxo, impedindo que um transmissor rápido sobrecarregue um receptor lento com um volume de mensagens muito grande.

O segundo protocolo dessa camada, o **UDP** (*User Datagram Protocol*)**,** é um protocolo sem conexão não confiável para aplicações que não necessitam nem de controle de fluxo, nem da manutenção da seqüência das mensagens enviadas. Ele é amplamente usado em aplicações em que a entrega imediata é mais importante do que a entrega precisa, como a transmissão de dados de voz ou de vídeo. A relação entre o IP, o TCP e o UDP é mostrada na Figura 07. Desde que o modelo foi desenvolvido, o IP foi implementado em muitas outras redes.

<table>
<tr><td rowspan="3">PROTOCOLOS</td><td>TELNET</td><td>FTP</td><td>SMTP</td><td>DNS</td><td>APLICAÇÃO</td></tr>
<tr><td colspan="2">TCP</td><td colspan="2">UDP</td><td>TRANSPORTE</td></tr>
<tr><td colspan="4">IP</td><td>REDE</td></tr>
</table>

Nomes no Modelo OSI

Figura 07: Relacionamento entre os protocolos IP, TCP e UDP.

1.3.2.3 Camada de Aplicação

O modelo TCP/IP não tem as camadas de sessão e de apresentação. Como não foi percebida qualquer necessidade, elas não foram incluídas. A experiência com o modelo OSI provou a seguinte tese: elas são pouco usadas na maioria das

aplicações. Acima da camada de transporte, está a **camada de aplicação.** Ela contém os protocolos de alto nível. Dentre eles estão o protocolo de terminal virtual (TELNET), o protocolo de transferência de arquivos (FTP) e o protocolo de correio eletrônico (SMTP). O protocolo do terminal virtual permite que um usuário de um computador estabeleça login em uma máquina remota e trabalhe nela. O protocolo de transferência de arquivos permite mover dados com eficiência de uma máquina para outra. Originalmente, o correio eletrônico era um tipo de transferência de arquivos; no entanto, posteriormente um protocolo especializado foi desenvolvido para essa função. Muitos outros protocolos foram incluídos com o decorrer dos anos, como o DNS (*Domain Name Service*), que mapeia os nomes de host para seus respectivos endereços de rede, o NNTP (*Network News Transfer Protcol*), o protocolo usado para mover novos artigos, e o HTTP (*Hyper Text Transfer Protocol*) , o protocolo usado para buscar páginas na WWW (*World Wide Web*), entre outros.

1.3.2.4 Camada Host/Rede

Abaixo da camada inter-redes, encontra-se um grande vácuo. A arquitetura TCP/IP não especifica coisa alguma, exceto pelo fato de que o host tem de se conectar com a rede utilizando um protocolo, para que seja possível enviar pacotes IP. Esse protocolo não é definido e varia de host para host e de rede para rede. Os livros e a documentação que tratam do modelo TCP/IP raramente descrevem esse protocolo [TANENBAUM 1997].

1.4 O PROTOCOLO IP

O protocolo IP (*Internet Protocol*) foi projetado visando conseguir transportar dados entre os mais diferentes tipos de redes. Sua tarefa é fornecer a melhor forma de transportar pacotes de dados da origem para o destino, independente das redes onde ambos estejam. Cada pacote é transmitido, e se for necessário, pode ser dividido em pedaços menores no meio do caminho. Isso se deve ao fato de uma rede não conseguir transportar o pacote com o tamanho original. Outra característica do IP é que se trata de um protocolo não orientado à conexão (Os pacotes podem ser enviados de uma origem para um destino a partir de diferentes caminhos), e também não é responsável por verificar se um pacote que foi enviado chegou ou não ao seu destino, ficando esta função a cargo do protocolo de transporte, caso necessário. O protocolo IP, apesar de possuir uma grande escalabilidade, sofreu algumas mudanças e foi evoluindo de acordo com o tempo. Tendo com isso várias versões, entre as quais a versão 4 (IPv4) e a versão 6 (IPv6). Durante um bom tempo os recursos do IPv4 foram utilizados de forma satisfatória. Porém com a explosão da Internet na década de 90, e o inúmero crescimento de equipamentos que deveriam se conectar a Internet, surgiu um problema. O número de endereços IP logo estaria esgotado, não suportando a demanda. Pois a versão 4 do protocolo IP suporta somente 2^{32} endereços. Com esse problema em vista a IETF (*Internet Engineering Task Force*) começou a trabalhar em uma nova versão do IP, já na década de 90. Os principais objetivos, entre outros, da nova versão do IP eram:

- Possuir um número quase inesgotável de endereços IP.
- Reduzir o esforço necessário para o roteamento dos pacotes IP, melhorando assim o *throughput*.
- Diminuir o tamanho das tabelas de roteamento.

• Oferecer uma segurança maior em relação ao IPv4.

• Aumentar a importância da informação sobre o tipo de serviço, principalmente para os serviços de tempo real.

• Possibilitar a evolução do protocolo.

• Possibilitar a compatibilidade entre a nova versão e o IPv4.

A nova versão do protocolo IP chama-se SIPP (*Simple Internet Protocol Plus*), mais conhecida como IPv6. Tal versão utiliza todos os bons recursos do IPv4, não utilizando ou melhorando os recursos ruins. Além de criar outros recursos quando necessário. Um pacote Ipv6 possui um cabeçalho fixo (obrigatório), zero ou mais cabeçalhos de extensão e os dados. Como se pode verificar na Figura 08.

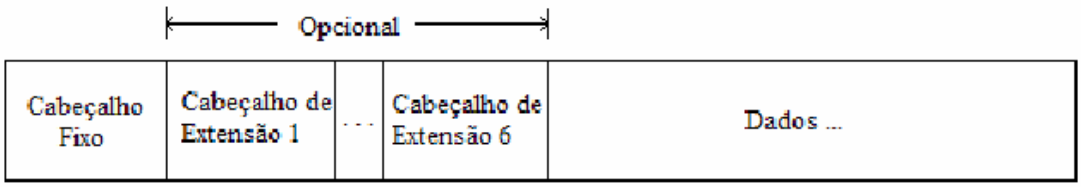

Figura 08: Forma geral de um IPv6.

2 PROBLEMAS COM A VOZ

Os problemas - eco e atraso - são bem conhecidos pelos planejadores de redes telefônicas desde os primórdios da telefonia, e as redes telefônicas atuais foram projetadas para manter esses efeitos imperceptíveis para a maioria dos clientes. Ao transportar voz sobre IP, toma-se muito mais difícil controlar o eco e o atraso. Como veremos, isso exigirá tecnologia de ponta e otimização de todos os componentes para tomar o serviço aceitável para todos os clientes.

2.1 CONEXÃO DE REFERÊNCIA

O nosso primeiro cenário é este representado na figura 09, uma chamada telefônica de um telefone IP para uma rede de computadores IP (ou vice-versa) sem o envolvimento de terminais PSTN (*Public Switched Telephone Network*) ou ISDN (*Integrated Service Digital Network*), ou seja, uma ligação IP pura. Neste caso o grande problema a enfrentar é o atraso. Quando a ligação partir do telefone IP ela irá para o vocoder (*gateway de telefonia*), o vocoder verificará para qual tipo de equipamento vai a chamada, no nosso caso não será necessária nenhuma codificação ou decodificação de sinais. O atraso do tipo jitter (variação de tempo entre as chegadas dos pacotes do endereço de origem) se dá devido a congestionamentos na rede, uma forma de contornar o problema será a implementação de buffers de jitter (implementações em software que visam adaptar a chamada conforme o status da rede no momento da chamada).

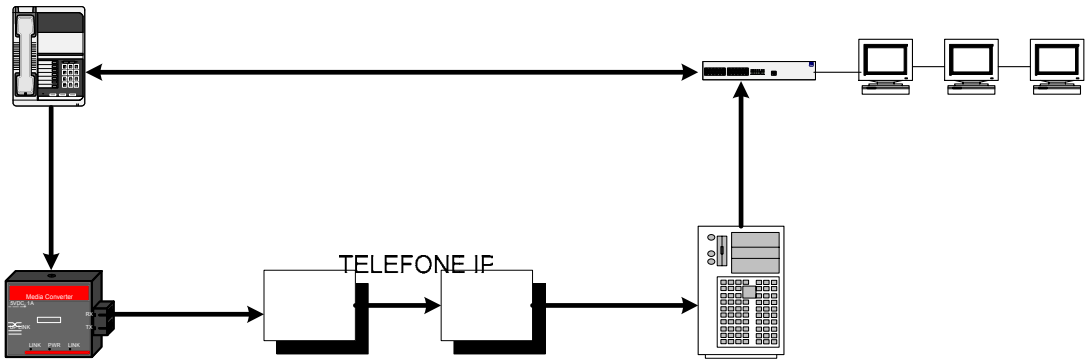

Figura 09: Ligação telefônica IP sem PSTU e ISDN.

Um outro cenário para uma ligação IP é o da figura 10 abaixo, porém mais complexo. Neste caso se quer estabelecer uma chamada entre um telefone IP e um telefone convencional (comutado por uma central digital) que está dentro da empresa. Quando a chamada partir do telefone IP, o vocoder se encarregará do buffer de jitter, o protocolo de transporte utilizado entre o telefone IP e o vocoder é o UDP, assim como entre os dois vocoders, mesmo que a chamada seja para um telefone no mesmo prédio ela será enviada para um gateway e assim chegar ao telefone convencional.

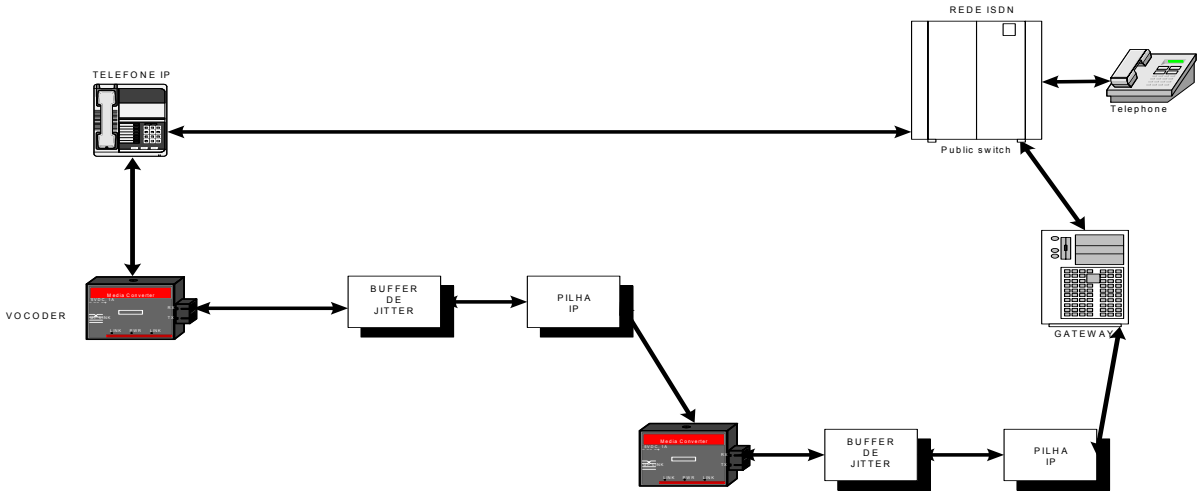

Figura 10: Ligação telefônica IP com rede ISDN presente.

A situação acima representada é bastante complexa, pois trabalhamos com uma rede ISDN por meio de um gateway. Quando o gateway faz interface com uma rede não IP, a interface do usuário para a rede se dá, na maioria dos casos, usando apenas implementações em software. O modelo inclui as fontes mais significativas de degradação da qualidade de voz:

- a rede IP introduz perda de pacotes e *jitter;*
- os buffers de *jïtter* (JB) influenciam o atraso de fim a fim e a perda de quadros;
- as interfaces acústicas introduzem eco acústico;
- as interfaces analógicas introduzem eco elétrico em híbridos.

É descrito aqui os principais fatores de influência sobre a percepção da qualidade de voz pelo usuário final. A maioria desses fatores são comuns tanto à telefonia de comutação de circuitos quanto à telefonia IP. No entanto, a telefonia IP possui algumas características únicas, como atrasos longos, *jïtter* e perda de pacotes, portanto, requer uma nova estrutura para avaliar a qualidade de voz.

2.2 ECO EM UMA REDE TELEFÔNICA

2.2.1 Eco de locutor - Eco de ouvinte

O eco mais importante é o do locutor - ele é a percepção que o locutor tem da sua própria voz, porém atrasada. Esse eco pode ser causado por um eco elétrico (híbrido) ou eco acústico ocorrido no lado do ouvinte. Se o eco do locutor for refletido duas vezes, ele também poderá afetar o ouvinte. Nesse caso, o ouvinte escuta a voz do locutor duas vezes - um sinal alto primeiro e depois um sinal atenuado e muito atrasado. Este é o eco de ouvinte (veja as Figuras 11 e 12).

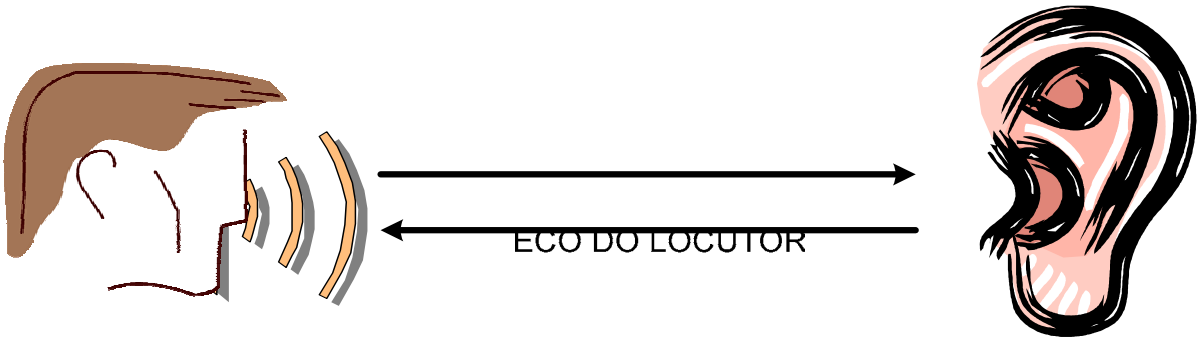

Figura 11: Eco do locutor.

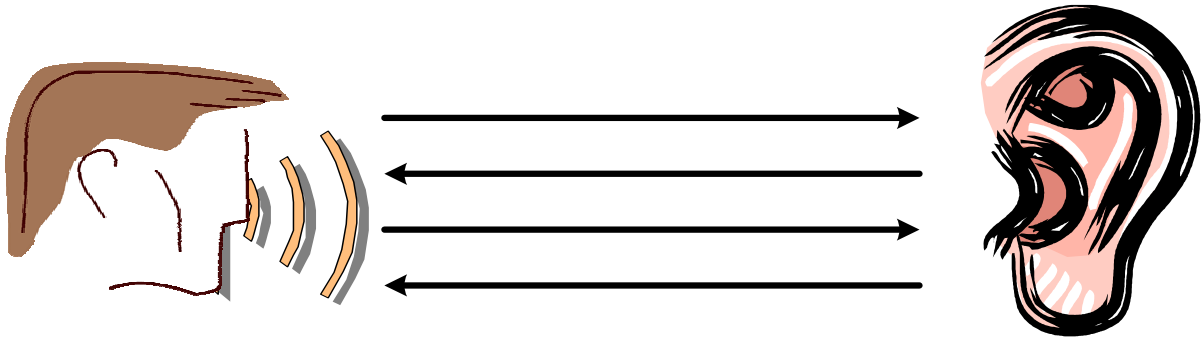

Figura 12: Eco do ouvinte.

2.2.2 Eco híbrido

Para usar menos fios, o sistema telefônico foi projetado para usar apenas dois fios. Devido a capacitâncias parasitas na linha, a maior parte dos sinais do microfone dissipava-se no alto-falante do locutor (que então tendia a falar mais baixo) e quase nada alcançava o ouvinte. Assim, o projeto final teve que corresponder à impedância característica da linha. Agora o sinal do microfone é dividido igualmente entre dois pares de fios e o locutor dificilmente ouve a si mesmo no seu próprio alto-falante (um pequeno desequilíbrio é mantido para que ele não

tenha a impressão de que está falando no vazio). Dependendo de quando um determinado equipamento foi instalado, alguns telefones mais antigos também são equipados com uma impedância real de 600Ω. Esses valores foram aceitos como um bom valor médio para uma linha típica. A impedância real de uma determinada linha varia de acordo com o seu comprimento (geralmente, de O a 9 km), de maneira que sempre haverá algum descasamento.

2.2.3 Eco Acústico

Aqui chamamos de "telefone amplificado" ao telefone com amplificador e alto-falante sem cancelamento de eco acústico, e de "telefone viva-voz" um telefone amplificado com cancelamento de eco acústico.

O eco acústico é simplesmente à parte do sinal acústico, realimentada do alto-falante de um dispositivo para o microfone desse mesmo dispositivo. Geralmente o eco acústico é um sinal parasita de 10 a 15 dB (*decibéis*) abaixo do sinal acústico da pessoa que realmente fala ao microfone. Da mesma maneira que o eco híbrido, esse nível de eco acústico não será notado se o atraso de ida e volta estiver abaixo de 20 ms. Acima de 40 ms a pessoa do outro lado da linha tem a impressão de estar conversando em uma cisterna e as coisas pioram acima dos 40 ms de atraso de ida e volta.

Uma maneira fácil de suprimir o eco acústico é usar um *headset,* mas com dispositivos apropriados é possível reduzir a potência do eco parasita à cerca de 45 dB abaixo do sinal o locutor, mesmo no caso de um telefone viva-voz.

Figura 13: Headset.

A recomendação G.167 do ITU (*International Telecommunication Union*) fornece alguns valores para o caminho típico de eco para usar durante testes:

• Para sistemas de teleconferência, o tempo de reverberação (tempo após o qual a energia de impulso de som cai abaixo de 60 dB da potência original) médio calculado sobre a largura de banda de transmissão geralmente será de 400 ms. O tempo de reverberação na oitava mais baixa não ultrapassará duas vezes essa média; enquanto o tempo de reverberação na oitava mais alta não será inferior à metade deste valor. O volume da sala de testes típica será da ordem de 90 m^3;

• Para telefones viva-voz e videofones, o tempo médio de reverberação, calculado sobre a largura de faixa de transmissão, geralmente será de 500 ms; o tempo de reverberação na oitava mais baixa não ultrapassará duas vezes essa média; enquanto o tempo de reverberação na oitava mais alta não poderá ser inferior à metade desse valor. O volume da sala de testes típica será da ordem de 50 m^3;

• Para telefones móveis uma câmara, simulando o interior de um carro, pode ser usada. O tempo de reverberação médio típico será de 60 ms. O volume da sala de testes será de 2,5 m^3.

Figura 14: Telefone viva-voz.

Os canceladores de eco geralmente não funcionam com eco acústico tão bem quanto num eco elétrico porque o trajeto do eco acústico varia muito mais, o que toma mais difícil captar dinamicamente o eco sintetizado ao eco real. Especificamente, o desempenho de canceladores de eco compatíveis com a Recomendação G.165 do ITU podem não ser suficientes. Uma recomendação mais nova, a G.168, está disponível e já implementada por algumas empresas. Essa recomendação contém acréscimos importantes, tais como a capacidade de parar o cancelamento de eco ao detectar o tom de inversão de fase dos modens de alta velocidade.

Valores típicos para a atenuação de eco acústico nos dispositivos atuais são:

• telefones amplificados (80% do mercado na França): 10 a 15 dB;

• telefones viva-voz: 35 a 40 dB;

• telefone com *handset* de boa qualidade: 35 a 40 dB.

Figura 15: handset.

2.2.4 Como limitar o eco

Dois tipos de dispositivos são comumente usados para limitar o eco, são eles: os canceladores de eco e os supressores de eco.

2.2.4.1 Supressores de eco

Os supressores de eco foram desenvolvidos na década de 1970. A idéia consiste em introduzir uma grande perda no caminho de envio quando a parte distante está falando. Essa técnica é amplamente utilizada nos telefones viva-voz mais simples, mas tende a atropelar a fala do locutor quando a parte distante fala ao mesmo tempo.

2.2.4.2 Canceladores de eco

Cancelador de eco é muito mais complexo que um supressor de eco, pois ele realmente constrói uma estimativa de eco para removê-la do sinal que chega.

No caso de voz em tempo real em uma rede de comutação de pacotes como VoIP, o eco elétrico deve ser cancelado caso o gateway IP venha a estabelecer uma chamada entre um terminal PSTN de dois fios e um PC ou estação de trabalho multimídia. Uma das mais importantes funções do gateway de telefonia IP é o cancelamento do eco elétrico gerado pela transformação de quatro fios para dois fios. Se o usuário de PC possuir um *headset* (que contém um microfone próximo à boca do locutor), não haverá eco acústico, portanto, não existirá a necessidade de um cancelador de eco acústico *(Acoustic Echo Canceller* - AEC) na placa de som do PC. Como mostrado na figura 16, é necessário ter um EEC (*Electric Echo Canceller*) no gateway e um AEC no ambiente do PC se o usuário do PC tiver um microfone e alto-falantes em uma situação de viva-voz. Se não houver nenhum EEC o eco elétrico perturbará o lado do PC e, caso não exista nenhum AEC, o eco acústico perturbará o lado da PSTN.

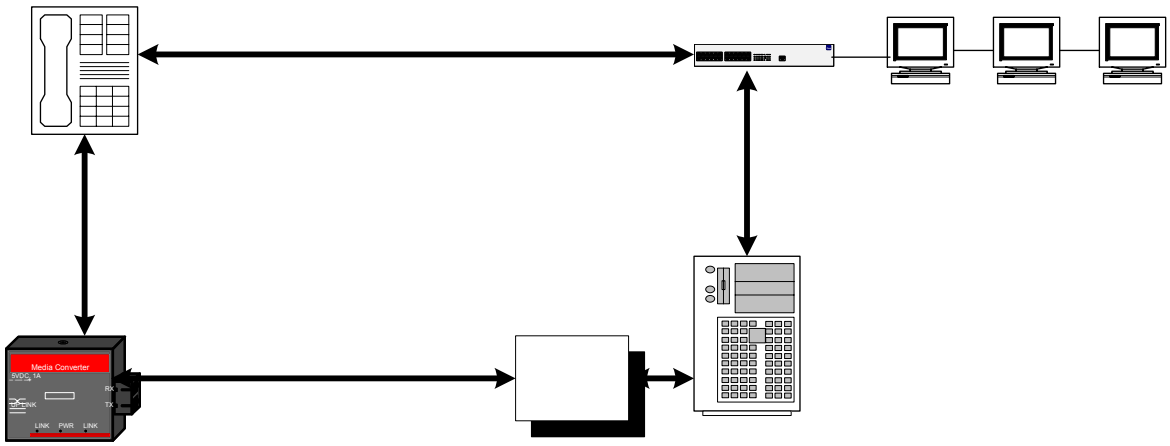

Figura 16: Cancelador de eco elétrico num cenário VoIP – PSTN.

Em uma rede IP o atraso geralmente é alto e imprevisível. Para uma rede comutada, como uma PSTN ou uma ISDN, este geralmente não é o caso; mas em países muito grandes, como os Estados Unidos (o caminho da costa leste à costa oeste também é longo para uma chamada telefônica), o atraso de transmissão é tão alto que um EEC faz-se necessário até mesmo para as chamadas terrestres (usando *links* de fibra ótica). Tal fato foi um dos principais impulsionadores do novo esquema de codificação de baixo atraso a 16 kbit/s do ITU (o futuro G.728 pretendia substituir o G.726 de 32 kbit/s). Isso evita a necessidade de atualizar a base instalada de EECs nos Estados Unidos.

Mesmo quando se usa esquemas de codificação de baixo atraso para sistemas de telefonia celular digital, VoIP, voz em *frame relay* ou mesmo voz em ATM, a utilização de EECs é realmente obrigatória e isso causa impacto sobre o custo do sistema como um todo. Contudo, uma codificação de voz com um baixo atraso algorítmico e de processamento relaxará os requisitos para o desempenho do EEC (rejeição de eco). Para enfrentar o eco acústico, um AEC deve ser instalado no terminal viva-voz seja qual for à rede e o *link* de transmissão usados [HERSENT 2002].

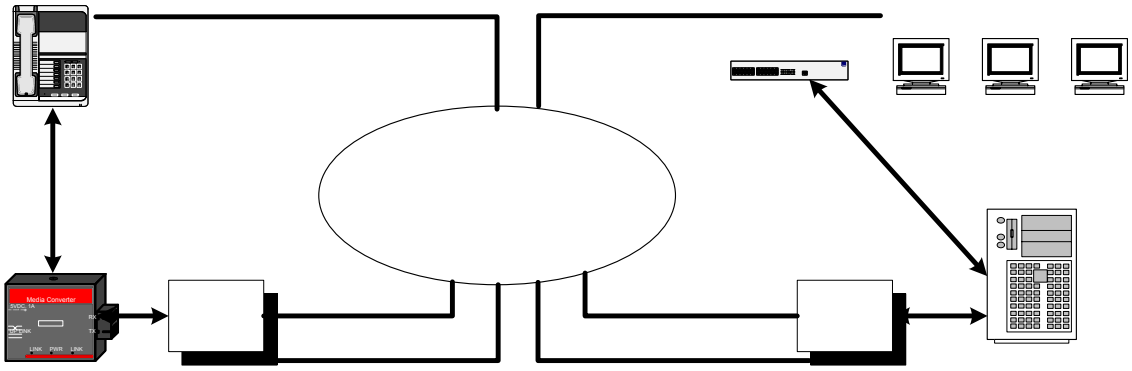

Figura 17: Cenário com a presença de eco elétrico e eco acústico.

3 PADRÃO VOIP – H.323

3.1 UMA BREVE HISTÓRIA

O H.323v1 teve poucas ambições. Observando o crescente sucesso das redes locais (LANs) com base em IP, IPX e Apple Talk em todos os tipos de companhias, o Grupo de Estudos 16 do ITU-T decidiu criar o H.323, “sistemas e equipamentos de telefone visual para redes locais que fornecem uma qualidade de serviço não garantida”, um padrão exclusivo para LANs para conferências audiovisuais. Originalmente, a responsabilidade pelas comunicações multimídia foi alceada para o Grupo de Estudos 15. O grupo de estudos já tinha adquirido grande experiência durante o desenvolvimento do H.320, “conferências multimídia para redes com base em ISDN”. Esse antecedente teve algumas conseqüências boas para o H.323, como boa interoperabilidade com o H.320 e algumas conseqüências ruins, como uma estrutura pesada desnecessária.

O H.323 não atraiu maior interesse do mercado até que a VocalTec e a Cisco fundaram o fórum *Voice over IP* (VoIP) para estabelecer padrões para produtos VoIP. Nessa época o enfoque no fórum VoIP estava voltado para a especificação de pontos finais de comunicação utilizando protocolos de sinalização com base no UDP. Quando grandes empresas de software e hardware perceberam o potencial da telefonia pela Internet, elas forçaram o fórum VoIP a se tornar parte do IMTC *(International Multimedia Teleconferencing Consortium) e,* graças à sua fatia de mercado e força, mudaram o enfoque do grupo de atividades VoIP de maneira a sintonizar o H.323 com as especificações da telefonia pela Internet. Com algumas mudanças menores, o H.323 parecia ser bastante adequado para o mais popular de todos os ambientes WAN: a Internet.

3.2 DO RTP AO H.323

O RTP / RTCP *(Real-Time Transport Protocol / Real-Time Control Protocol),* foi o conjunto de protocolos usado nas primeiras ferramentas para conferências disponíveis na Internet: o VAT *(Visual Audio Tool)* usou o RTP versão 0. Desde então, o RTP evoluiu até a versão 2. O RTP é um protocolo que possibilita o transporte de dados em tempo real (ou, mais precisamente, isócrono) sobre o IP. Esse protocolo permite um certo nível de tolerância para *o jitter* e a perda de pacotes. O ITU-T H.225.0 faz um trabalho de detalhamento (na verdade, a especificação inteira do RTP / RTCP está anexada a ele) para aplicações de videoconferências H.323.

O H.323 é uma especificação guarda-chuva que descreve de maneira completa a arquitetura e a operação de um sistema de videoconferências sobre uma rede de pacotes. O H.323 não é específico para o IP: há seções no uso do H.323 sobre IPX ou ATM *(Asichronous Transfer Mode).* A estrutura do H.323 é completa e inclui a especificação de:

- terminais de videoconferência;
- gateways entre uma rede H.323 e outras redes de voz e vídeo (H.320/ RTPC etc.);
- *gatekeepers,* que são a parte inteligente da rede H.323, realizando o registro de terminais, admissão de chamadas e muito mais;
- blocos funcionais MCU *(Multipoint Control Unit),* MC *(Multipoint Controller)* e MP *(Multipoint Processor)* usados para conferências com diversos participantes.

3.3 TRANSPORTANDO VOZ SOBRE UMA REDE DE PACOTES

O sistema telefônico mais comum nos dias de hoje ainda é o analógico. A telefonia analógica usa a modulação de sinais elétricos ao longo de um cabo para transportar voz (veja a figura 18).

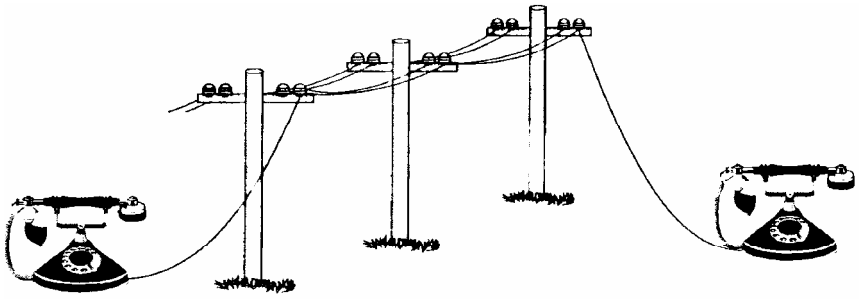

Figura 18: Telefonia Analógica.

Apesar de ser uma tecnologia muito antiga, a transmissão analógica tem muitas vantagens: ela é simples e mantém o atraso fim a fim na transmissão de voz muito baixo, uma (vez que o sinal se propaga ao longo do cabo quase na velocidade da luz. Também é barata quando há relativamente poucos usuários falando ao mesmo tempo, e quando eles não estão muito distantes entre si. Mas a tecnologia analógica mais básica requer um par de cabos por conversação ativa, o que se toma rapidamente impraticável e caro. Uma primeira melhoria da tecnologia analógica básica foi multiplexar várias conversações no mesmo cabo, usando uma freqüência de transporte separada para cada sinal. Mas mesmo com essa técnica, a telefonia analógica tem muitas desvantagens:

- a menos que se usem mesas de comutação manuais, as chaves analógicas exigem uma grande quantidade de mecanismos eletromecânicos que são caros para comprar e manter;

• ruído parasítico é adicionado em todos os estágios da transmissão porque não há como dizer o que é sinal e o que é ruído, de maneira que o sinal não pode ser limpo.

Por todas essas razões, muitos países atualmente usam uma rede telefônica digital. Na maioria das vezes, a linha do assinante permanece analógica, mas o sinal analógico é convertido em um fluxo de dados digitais na primeira central local. Normalmente, esse sinal tem uma taxa de comunicação de 64 kbits/s (uma amostra de 8 bits a cada 125 μs).

Agora vários canais de voz podem ser multiplexados ao longo da mesma linha de transmissão usando uma tecnologia chamada multiplexação por divisão no tempo *(Time Division Multiplexing* - TDM).

3.4 POR QUE RTP / RTCP?

Voz e vídeo sobre IP possuem um grande inimigo o *jitter* (variação de tempo entre chegadas de pacotes do endereço de origem).

O RTP *(Real-Time Transport Protocol* - Protocolo de Transporte em Tempo Real) foi projetado para permitir que os receptores compensem o *jitter* e a perda de seqüência dos pacotes introduzidos pelas redes IP. O RTP pode ser usado para qualquer fluxo de dados em tempo real, como voz e vídeo. O RTP define um modo de formatar pacotes IP que carregam dados isócronos e inclui:

• informação sobre o tipo de dado transportado;

• números de seqüência.

Um outro protocolo, o RTCP *(Real-Time Control Protocol* - Protocolo de Controle em Tempo Real), geralmente é usado com o RTP para permitir o transporte de algum retorno sobre a qualidade da transmissão (a quantidade *de jitter,* a perda

média de pacotes etc.) e também pode transportar algumas informações a respeito da identidade dos participantes.

O RTP e o RTCP não têm qualquer influência sobre o comportamento da rede IP; eles de maneira alguma controlam a qualidade de serviço. A rede pode perder, inserir atraso ou perder a seqüência de um pacote RTP da mesma maneira que qualquer outro pacote IP. O RTP não deve ser confundido com protocolos como o RSVP *(Resource reSerVation Protocol* -Protocolo de Reserva de Recursos). O RTP e o RTCP simplesmente permitem aos receptores compensar o *jitter* da rede, por meio do controle de buffer e seqüenciamento apropriados, e ter mais informações a respeito da rede de maneira que medidas corretivas apropriadas possam ser adotadas (redundância).

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

O UDP é um protocolo de transporte não orientado a conexão, portanto não confiável sob o ponto de vista de diversos aspectos, porém é ideal para serviços e aplicações em tempo real como o VoIP. O TCP é outro protocolo de transporte, confiável e orientado a conexão, indicado para certos cenários em VoIP, como por exemplo uma chamado entre duas estações de trabalho.

3.5 H.323 PROPRIAMENTE DITO

O H.323 não inventou a videoconferência em IP. Pesquisadores e estudantes fizeram isso por anos usando RTP / RTCP. No entanto, o RTP / RTCP possui apenas capacidades de sinalização muito básicas, como vimos anteriormente.

O H.323 define principalmente a sinalização necessária para estabelecer chamadas e conferências, para escolher codecs (*codificadores e decodificadores*) etc. O núcleo do RTP / RTCP ainda é usado para transportar fluxos isócronos e obter retorno sobre a qualidade da rede, mas aspectos mais peculiares do RTP, como distribuição de alias de e-mail, geralmente não são usados pelo H.323.

O H.323 lida com um problema complexo e, conseqüentemente, ele próprio é bastante complexo. O conjunto de documentos que um engenheiro de H.323 precisa como referência (Q.931, H.323, H.225, H.245, H.235, H.332), toma um certo tempo para ser lido.

3.5.1 Chamada de voz do terminal A para o terminal B

Para este primeiro e fácil exemplo consideremos que dois usuários conectados a dois terminais IP distintos gostariam de estabelecer uma chamada de voz. Do ponto de vista de uma rede de comutação de circuitos, os usuários teriam a mesma experiência que teriam se estivessem usando dois terminais analógicos conectados às suas respectivas centrais, desejando ter uma conversação. Outros aspectos relacionados à chamada, tais como segurança, tarifação e gerenciamento, não são considerados aqui.

O estabelecimento de uma chamada H.323 fim a fim requer duas conexões TCP entre os dois terminais IP, uma para o estabelecimento da chamada e outra

para o controle da chamada e a troca de informações sobre capacidades. A conexão TCP inicial é feita do terminal chamador para uma porta conhecida no terminal chamado e a conexão transporta as mensagens de estabelecimento da chamada, definidas no H.225.0. Mensagens de controle da chamada usam uma segunda conexão TCP. Após o recebimento da chamada, o terminal chamado espera por uma conexão TCP em uma porta dinâmica; o terminal chamado comunica o número dessa porta na mensagem de aceitação de chamada. O terminal chamador então estabelece a segunda conexão TCP com aquela porta.

3.5.1.1 Primeira fase: inicializando a chamada

O H.323 utiliza as seguintes mensagens de sinalização para controle de chamada na interface usuário-rede: setup, alerting, connect e release complete.

Na figura 19, é aberta sessão no terminal A, deseja fazer uma ligação para o terminal B, conhecendo o endereço IP de B (10.2.3.4). O terminal A envia ao terminal B uma mensagem setup na porta conhecida do canal de sinalização de chamadas (porta 1720, definido pelo H.225.0) usando uma conexão TCP.

- uma capacidade de transporte, um campo complexo que pode indicar, entre outras coisas, se a chamada terá apenas áudio ou áudio e vídeo. Gateways ISDN podem colocar nesse campo alguns elementos copiados da mensagem setup ISDN;

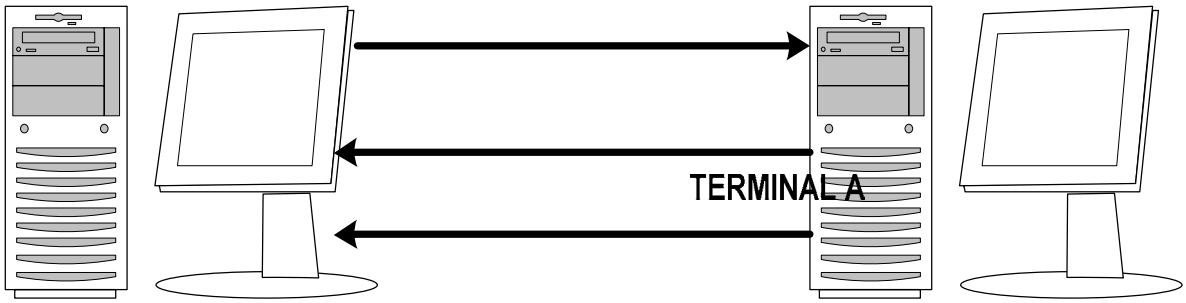

Figura 19: Chamada de voz do terminal A para o terminal B.

As mensagens de alerting e connect devem ser enviadas pelo terminal de B imediatamente após o recebimento de uma mensagem setup. Uma delas deve ser recebida pelo terminal A antes que o temporizador de setup expire (em geral, após quatro segundos). Após alerting ter sido enviada, o usuário tem até três minutos para aceitar ou recusar a chamada.

Tower PC

3.5.1.2 Segunda fase: estabelecendo o canal de controle

O controle da chamada e as mensagens de troca de capacidades são enviados na segunda conexão TCP, que o terminal chamador estabelece com uma porta dinâmica no terminal chamado.

A primeira mensagem enviada através do canal de controle é a TerminalCapabilitySet, que transporta um número de seqüência, os terminais enviam essa mensagem um para o outro e acusam o seu recebimento com uma mensagem TerminalCapabilitySetAck.

3.5.1.3 Terceira fase: início da chamada

Agora o terminal A e o terminal B precisam abrir canais de mídia para voz e possivelmente para vídeo e dados. Para abrir um canal de voz até B, A envia uma mensagem H.245 OpenLogicalChannel que contém o número que será dado ao canal lógico, além de outros parâmetros como o tipo dos dados que serão transportados. No caso de som ou vídeo (que serão transportados sobre o RTP), a mensagem OpenLogicalChannel menciona também o endereço UDP e a porta para a qual B deve enviar os RR *(Receiver Reports)* RTCP, o tipo do *payload* (informação em tempo real contida em cada pacote) RTP e a capacidade de parar de enviar dados durante períodos de silêncio.

B envia uma mensagem OpenLogicalChannelAck referente a esse canal lógico tão logo ele esteja pronto para receber dados de A. Essa mensagem contém o número da porta UDP para a qual A deve enviar os dados RTP e a porta UDP para a qual A deve enviar os dados RTCP. Enquanto isso, B também pode ter aberto um canal lógico com A seguindo o mesmo procedimento.

3.5.1.4 Quarta fase: diálogo

Agora o terminal A e o terminal B podem conversar e ver um ao outro, caso eles também tenham aberto canais lógicos para vídeo. Os dados da mídia são enviados em pacotes RTP. Os pacotes RTCP SR (*Sender Report*) enviados por A são usados para permitir que B sincronize múltiplos fluxos RTP e também podem ser usados por B para estimar a taxa esperada de dados RTP e para medir a distância ao transmissor. Os pacotes RTCP RR (*Receiver Report*) enviados por B permitem que A meça a qualidade de serviço da rede entre A e B: as mensagens RTCP contêm a fração de pacotes que foram perdidos desde o último RR, a perda

cumulativa de pacotes, o *jitter* entre chegadas e o mais alto número de seqüência recebido. Os terminais H.323 devem responder ao aumento da perda de pacotes reduzindo a taxa de envio dos mesmos.

Observe que o H.323 manda usar apenas um par de portas RTP / RTCP para cada sessão. Podem haver três sessões principais entre os terminais H.323: a sessão de áudio, a sessão de vídeo e a sessão de dados, mas nada no padrão impede que um terminal abra mais sessões. Para cada sessão deve haver apenas uma porta RTCP usada, isto é, se houver simultaneamente um fluxo RTP de A para B e de B para A, o transmissor RTCP e os RRs para ambos os fluxos vão usar a mesma porta UDP.

3.5.2 Chamando um telefone comum a partir da Internet

No caso simples descrito anteriormente, o terminal A ligou para o terminal B diretamente em seu endereço IP corrente 10.2.3.4. Essa situação é conveniente para mostrar os aspectos básicos do H.323, mas é improvável de acontecer na realidade. O endereço IP na grande maioria dos casos é dinâmico, ou seja, não serve para uma sessão de chamada fora de uma rede local.

O próximo exemplo é mais complicado. O terminal A deseja ligar para o terminal B (que agora é um telefone comum), esse exemplo mostrará a necessidade de uma nova entidade H.323, chamada *gatekeeper.*

O *gatekeeper é o* componente mais complexo da estrutura do H.323. Ele foi introduzido no H.323v1, mas naquela ocasião a maioria não entendeu realmente o quanto ele seria útil. No melhor caso, o *gatekeeper* foi considerado uma espécie de diretório que mapeava nomes amigáveis em endereços IP e algumas empresas tiveram “idéias melhores” de como fazer isso. Ainda hoje alguns softwares e

hardwares “padrão H.323” que não usam o *gatekeeper,* mas sim mecanismos proprietários que vão desde servidores IRC *(Internet Relay Chat)* até servidores LDAP *(Lightweight Directora Access Protocol)* para encontrar o endereço de transporte de um outro telefone IP.

O H.323v2 esclareceu o papel do *gatekeeper e* hoje em dia é amplamente aceito o fato de que o *gatekeeper é o* lugar certo para todos os serviços com base em rede, isto é, aqueles que precisam ser executados independentemente do terminal ou de quando o terminal é desligado. Esses serviços incluem registro (a capacidade de saber que alguém está no sistema e pode ser contactado em um terminal em particular), admissão (verificação do direito de acessar recursos) e status (monitoramento da disponibilidade de recursos da rede relacionados a telefones como gateways e terminais). Encontrar o endereço de transporte a ser usado para alcançar um determinado alias naturalmente também é parte do papel do *gatekeeper,* uma vez que esse endereço de transporte pode depender do status da parte chamada (se a pessoa não estiver no sistema, por exemplo, a chamada deve ser redirecionada para uma secretária eletrônica ou para um telefone comum por meio de um gateway), da identidade do terminal chamador (nem todos estão autorizados a ligar para o terminal A) ou do status de um recurso em particular (se todas as portas em um gateway estiverem ocupadas, pode ser necessário instruir o terminal chamador a usar um outro gateway).

Dessa forma, nesta seção consideramos que o terminal chamador tem acesso a um *gatekeeper* e mostramos algumas de suas características em ação. O terminal e o *gatekeeper* usam um protocolo específico para fins de registro, admissão e status, que logicamente ganhou o nome de RAS *(Registration, Admission and Status).*

3.5.2.1 Primeira fase: onde está o gatekeeper?

Em configurações simples, o endereço IP do *gatekeeper* pode ser configurado manualmente no terminal IP. No entanto, o H.323 desenvolveu um mecanismo para encontrar dinamicamente um *gatekeeper* (GK) na rede. Isso tem muitas vantagens, como no caso de uma pessoa que tem um laptop e circula por vários escritórios.

Para encontrar um *gatekeeper,* um terminal H.323 deve enviar uma requisição multicast de *gatekeeper* (GRQ), o terminal pode especificar se ele deseja contactar um *gatekeeper* em particular. O terminal menciona também seus aliases, permitindo assim que um *gatekeeper* responda apenas a grupos específicos de terminais.

Essa mensagem deve ser enviada inicialmente com um TTL *(Time To Live)* muito baixo, com o objetivo de atingir primeiro os *gatekeepers* na rede local e depois usar a técnica de busca em anel crescente *(expanding ring search).* Essa mensagem GRQ diz ao *gatekeeper* em que endereço e porta o terminal espera receber a resposta, que tipo de terminal é e quais são os aliases do terminal (como visto na figura 20).

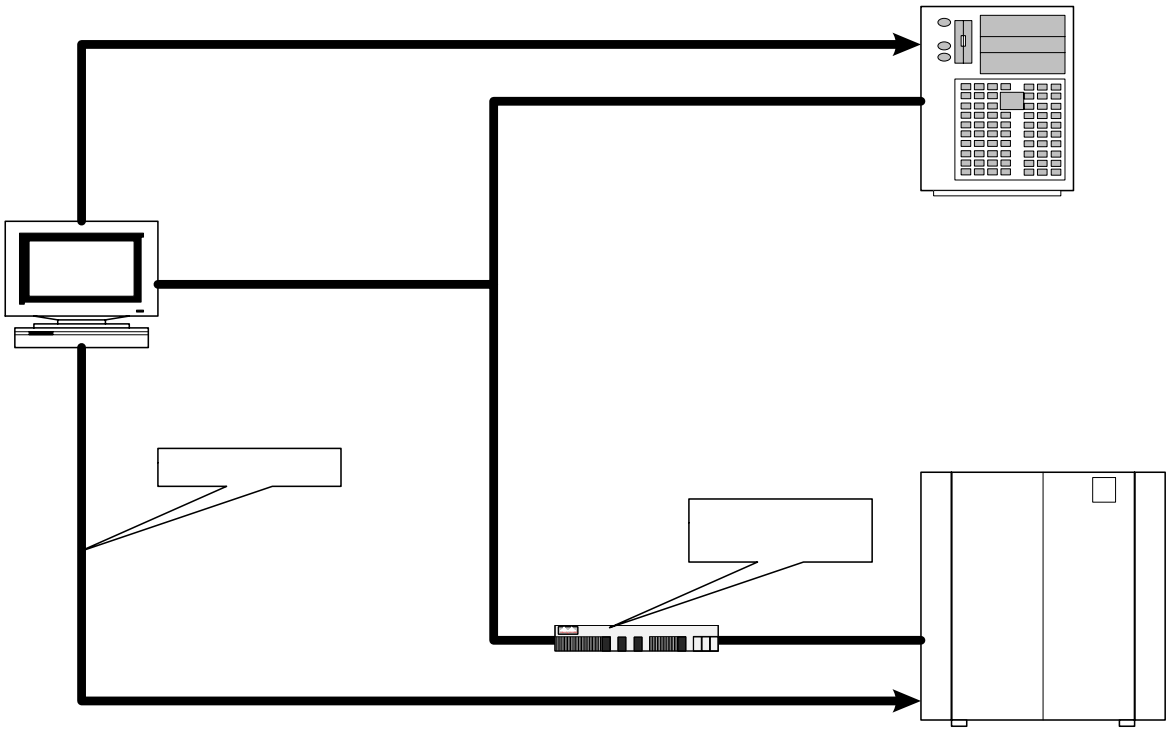

Figura 20: Encontrando um gatekeeper.

3.5.2.2 Segunda fase: permitindo nova chamada

Agora que o terminal A encontrou um *gatekeeper* e está registrado, ainda precisa pedir permissão ao *gatekeeper* para cada chamada que ele quiser fazer. Nesse caso, ele deseja alcançar sua avó no número 0xx11 6543312. Seu terminal enviará primeiro uma mensagem ARQ *(Admission Request)* ao seu *gatekeeper.* Essa mensagem RAS (*Registration and Admission Status*) inclui:

• um número seqüencial;

• o identificador do terminal conforme designado pelo *gatekeeper;*

• o tipo da chamada (fim a fim);

• o modelo de chamada que o terminal deseja utilizar (direto ou roteado por *gatekeeper);*

• uma estimativa da largura de banda bidirecional que será usada por essa chamada para áudio e vídeo. Isso inclui o áudio e o vídeo que serão enviados a partir da parte chamada.

Se decidir aceitar a chamada, o *gatekeeper* responderá com uma mensagem “Admission Confirm" (ACF) que especifica:

• o modelo de chamada em uso;

• o endereço de transporte e a porta a serem usados para a sinalização da chamada. Esse endereço pode ser o próprio endereço IP do terminal chamado (ou o endereço IP de um gateway, no caso de se estar chamando um número de telefone comum).

• a largura de banda permitida para a chamada;

3.5.2.3 Terceira fase: sinalização da chamada

A mensagem “Admission Confirm” forneceu ao terminal A, a informação de que ele precisava para completar a chamada (Figura 21). Agora o terminal pode enviar uma mensagem Setup para o endereço de sinalização de chamada e a porta especificados pelo *gatekeeper*, no nosso caso um gateway para a rede telefônica.

Antes de prosseguir o gateway pode perguntar ao *gatekeeper* se ele está autorizado a efetuar a chamada usando uma seqüência ARQ / ACF. O ARQ mencionará tanto o alias da ponta que está chamando e o endereço de sinalização de chamada quanto o alias da ponta chamada e o endereço de sinalização de chamada. O gateway sabe, a partir do elemento de informação de número da parte chamada da mensagem Setup, qual o número de telefone ele deve chamar.

O gateway enviará uma mensagem H.225 Alerting para o terminal chamador, tão logo ele tenha recebido uma indicação da rede telefônica, que o telefone analógico esteja tocando, e enviará a mensagem Connect tão logo ele seja tirado do gancho. Se o gateway estiver conectado por meio de uma linha ISDN, esses eventos serão sinalizados pela rede telefônica usando mensagens similares às Q.931 Alerting e Connect. Caso seja uma linha analógica, o gateway precisa detectar as condições correspondentes a campainha (conforme figura 21).

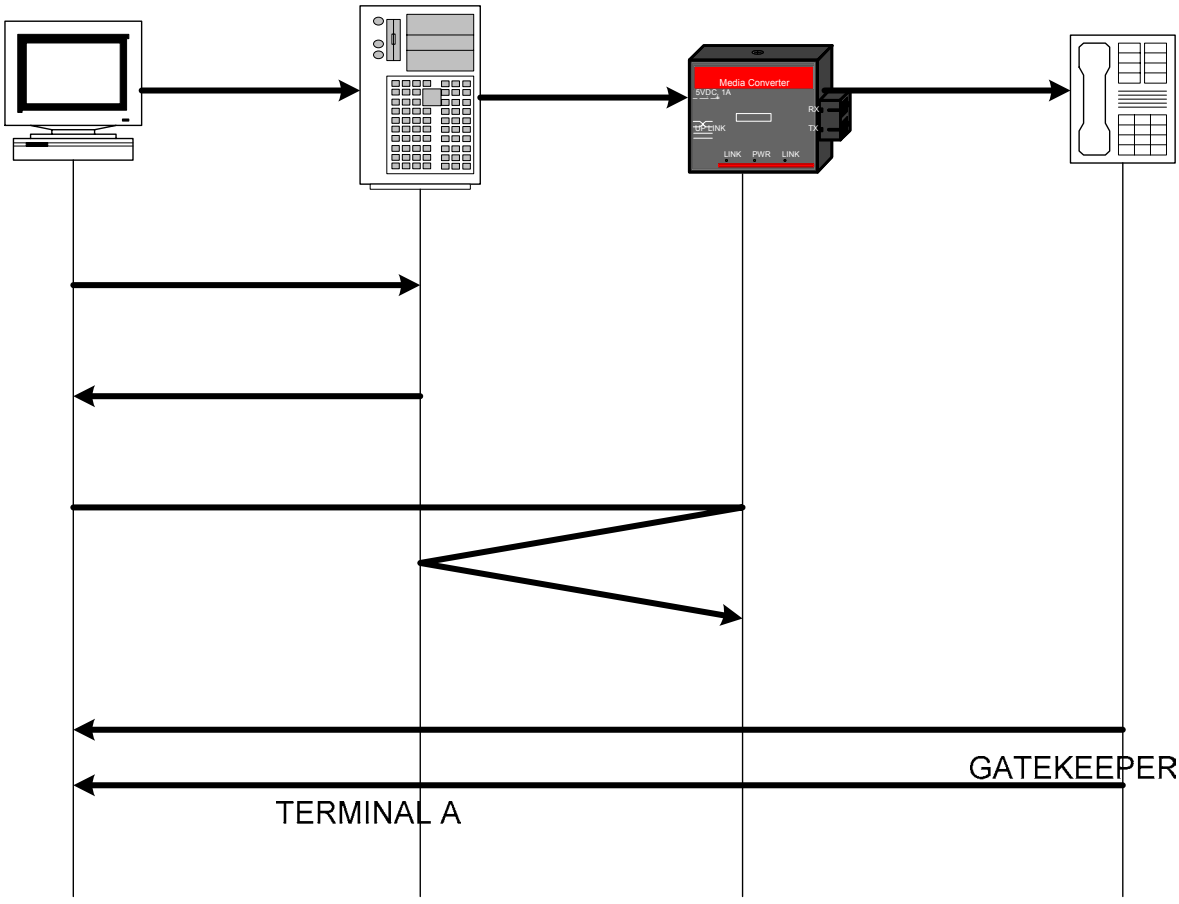

Figura 21: Completando a chamada.

3.5.2.4 Fase de término

Quem for cortar a ligação (por exemplo: o gateway) precisa primeiro fechar seus canais lógicos usando a mensagem H.245 CloseLogicalChannel, o gateway envia então uma mensagem H.245 EndSessionCommand para o terminal A e espera até receber a mesma mensagem do terminal A. O gateway então fecha o canal H.245, em seguida o terminal e o gateway devem enviar uma mensagem DRQ *(Disengage Request)* ao *gatekeeper* (dessa forma, o *gatekeeper* fica sabendo que a largura de banda foi liberada). *O gatekeeper* responde a cada um com uma mensagem “Disengage Confirm” (DCF).

Se durante a comunicação o *gatekeeper* quiser cancelar a ligação, ele também poderá enviar uma mensagem DRQ a uma das pontas. Nesse momento, a ponta deve enviar uma mensagem H.245 EndSessionCommand à outra ponta, esperar até receber um EndSessionCommand, fechar o canal Q.931 com um ReleaseComplete e enviar uma mensagem DCF ao *gatekeeper.*

Para impedir que um terminal queira fechar uma conexão com um gateway sem enviar um EndSessionCommand / ReleaseComplete ao gateway, quando um *gatekeeper* receber uma mensagem DRQ do terminal, primeiro ele vai esperar até que tenha recebido uma mensagem DRQ do gateway antes de responder com uma mensagem DCF. Se o *gatekeeper* receber uma mensagem DRQ do gateway (como no nosso exemplo), ele vai esperar até que tenha recebido uma mensagem DRQ do terminal antes de enviar uma mensagem DCF ao gateway. Se o *gatekeeper* não receber uma mensagem DRQ do terminal dentro de alguns segundos, ele pedirá ao terminal para desconectar enviando uma mensagem DRQ. Espera-se que o terminal desconecte e envie uma mensagem DCF de volta, mas caso ele não faça isso dentro de alguns segundos (o PC pode ter travado), o *gatekeeper* enviará uma

mensagem DCF ao gateway assim mesmo. Esse procedimento evita fraudes e operações indesejadas devido a terminais instáveis ou que não estejam em conformidade com os padrões, conforme a figura 22 [HERSENT 2002].

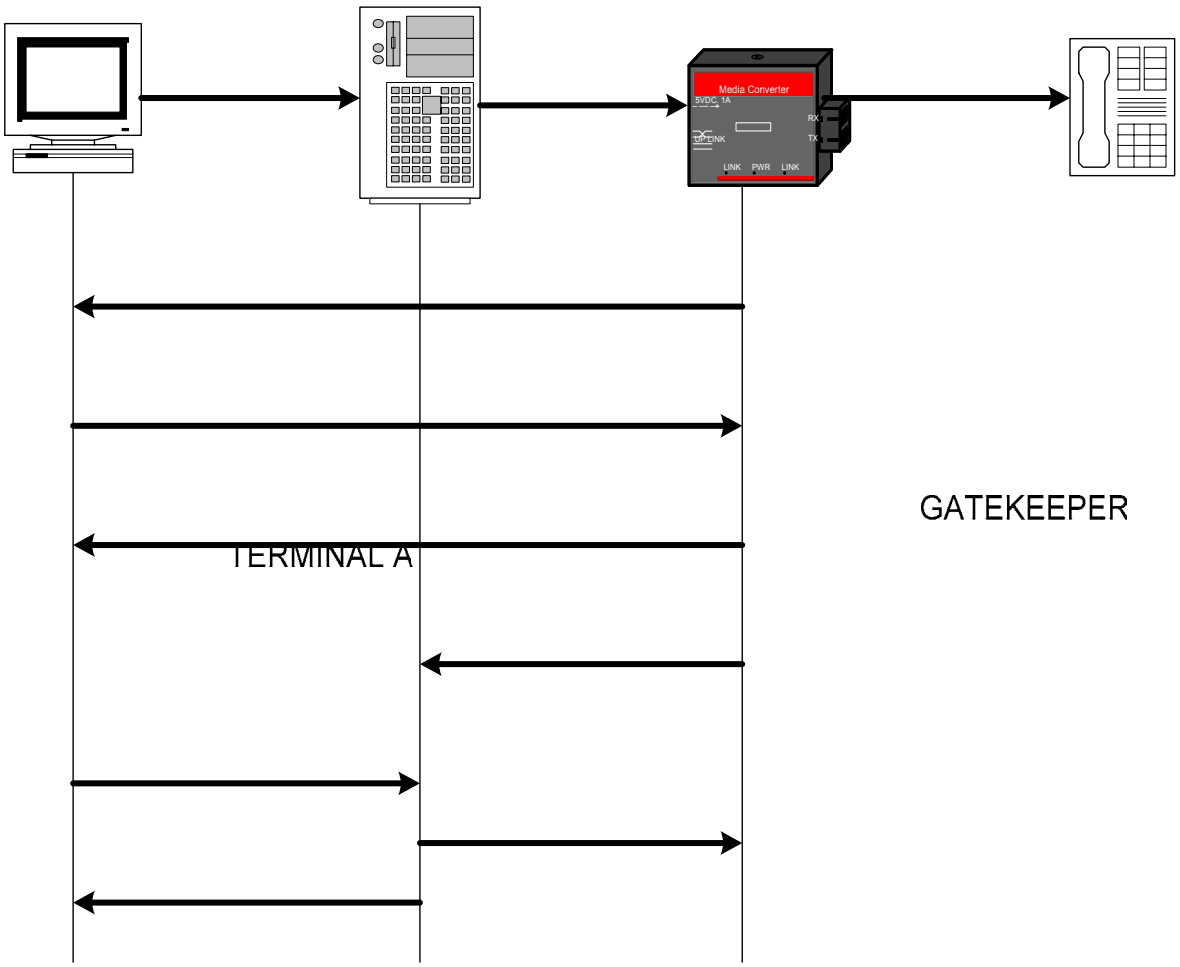

Figura 22: Fechando os canais de comunicação.

4 PROJETO DE IMPLANTAÇÃO NA SEMEF

4.1 EQUIPAMENTOS UTILIZADOS NA SOLUÇÃO DE VOZ SOBRE IP

Existem alguns equipamentos que podem ou devem ser utilizados para implantar uma solução de Voz sobre IP em uma rede corporativa. Dar-se-á uma breve introdução sobre alguns desses equipamentos nos itens a seguir.

4.1.2 Telefone IP

Telefones IP são terminais que possuem, além das características e funcionalidades dos telefones normais, várias funções que podem aumentar a produtividade de uma corporação. Algumas destas funções e características podem ser:

- Suporte a serviços na Internet.
- Suporte a características de qualidade de serviço.
- Menus de fácil navegação.
- Lista de histórico de chamadas.
- Diretórios.
- Fácil atualização.

Figura 23: Telefone IP.

4.2 QUALIDADE DO SERVIÇO - QoS

Qualidade de serviço pode ser considerada uma exigência básica, porém irá depender de quanto o usuário deseja investir na mesma. Alguns fatores que podem ser observados para que se determine o nível de qualidade do serviço de voz são: fidelidade da voz, disponibilidade da rede, disponibilidade de funções do telefone e escalabilidade.

4.2.1 Considerações para qualidade

De acordo com [CHRISTESEN 2001] existem algumas questões que podem ser levadas em consideração para que haja uma certa qualidade de serviço. Tais questões estão diretamente relacionadas com os itens citados abaixo.

4.2.1.1 Jitter

Jitter é uma variação de tempo entre chegadas de pacotes do endereço de origem. Caso houvesse uma taxa de transmissão constante com intervalo de 20 ms entre a transmissão de um pacote e outro tais pacotes deveriam chegar ao destino com intervalo de 20 ms. Porém como cada pacote pode trafegar na rede por diferentes rotas e diferentes meios esse tempo de chegada pode variar. Fato este que diminuiria a qualidade do serviço. *Buffers* podem ser utilizados neste caso com a finalidade de amenizar (e não eliminar totalmente) o problema da variação de tempo de chegada dos pacotes ao destino.

4.2.1.2 Latência

Latência é o intervalo de tempo em que um pacote sai de sua origem e chega ao seu destino. Em termos de telefonia, latência é o tempo em que uma pessoa

fala algo e chega ao ouvido do receptor. Uma grande latência não significa necessariamente que ocorrerá uma degradação da voz, porém o que pode ocorrer é uma perda de sincronização. Para que se obtenha uma boa qualidade em chamadas telefônicas a latência deve possuir um valor menos que 150 ms. Para que isso ocorra devem ser tomadas algumas providências para que o tempo de empacotamento, transmissão e transporte dos dados diminuam.

4.2.1.3 Largura de banda

Largura de banda é um fator essencial para que se tenha uma qualidade de serviço em conversações telefônicas. A largura de banda para a transmissão de voz depende de vários fatores e pode ser calculada facilmente de acordo com informações de amostragem e quantização da voz, algoritmos de compressão e etc. Porém em redes corporativas além da transmissão de voz a rede é usada para muitas outras finalidades. E como a transmissão de voz em uma conversação telefônica deve ocorrer em tempo real, tais dados devem possuir uma prioridade em relação a outros eventuais. É claro que a decisão de uma largura de banda maior ou menor deve ser tomada de acordo com as necessidades e prioridades da empresa. Porém vale ressaltar que uma banda muito estreita para a transmissão de voz deve influenciar negativamente na qualidade do serviço.

4.2.1.4 Perda de pacotes

A perda de pacotes é outro fator crítico que implica diretamente na qualidade de serviço. Existem vários fatores que podem levar à perda de um pacote IP. Podemos citar entre eles o estouro de *buffer* em roteadores e *switchs*. Em que os pacotes que chegarem e encontrarem o *buffer* cheio serão então descartados. Pacotes per-

didos em aplicações que utilizam o protocolo UDP e RTP não podem ser retransmitidos e mesmo que pudessem não seria nada interessante. Pois duas mensagens enviadas em seqüência poderiam chegar em ordem inversa, o que não é tolerável em aplicações de tempo-real. Porém como a perda de pacotes pode ser inevitável, tolera-se uma pequena perda. Penso que caso a perda seja menor que 5% do total de pacotes a qualidade não é significativamente afetada. No caso de aplicações em tempo-real é melhor perder uma pequena porcentagem dos pacotes do que atrasar a transmissão como um todo com a utilização de longos *buffers*.

4.2.1.5 Segurança

Segurança é um fator que sempre deve ser considerado em redes corporativas, seja em aplicações de tempo-real ou não. Para manter a qualidade de serviço o acesso à rede deve ser permitido somente a pessoas autorizadas. Deve-se também evitar ataques *denial-ofservice* (Ataques de negação de serviço. O serviço é requisitado por vários usuários ao mesmo tempo e o provedor do serviço não consegue atender a demanda e pode vir a ficar “fora do ar” - DoS) colocando endereços IPs não válidos para os equipamentos de voz. Como a rede utiliza o protocolo IP existem métodos de tornar as informações mais confiáveis e menos suscetíveis a ataques através da utilização de criptografia que já é suportada nativamente pela versão 6 do IP (IPv6).

4.2.1.6 Confiabilidade

Algumas providências devem ser tomadas em relação à confiabilidade da rede como um todo. Uma solução para aumentar a confiabilidade seria usar equipa-

mentos e *links* redundantes. Isso deixaria a rede menos suscetível a falhas e aumentaria assim a qualidade do serviço.

4.3 CENÁRIO ATUAL DA REDE SEMEF

A Prefeitura Municipal de Manaus é uma instituição pública de grande porte e uma de suas secretarias à SEMEF (*Secretaria Municipal de Economia e Finanças*) é uma pequena amostra do poderio de gastos de uma companhia de grande porte, os gastos com a telefonia da SEMEF são bastante elevados e esta instituição está no grupo daquelas que precisam urgentemente de um projeto em VoIP.

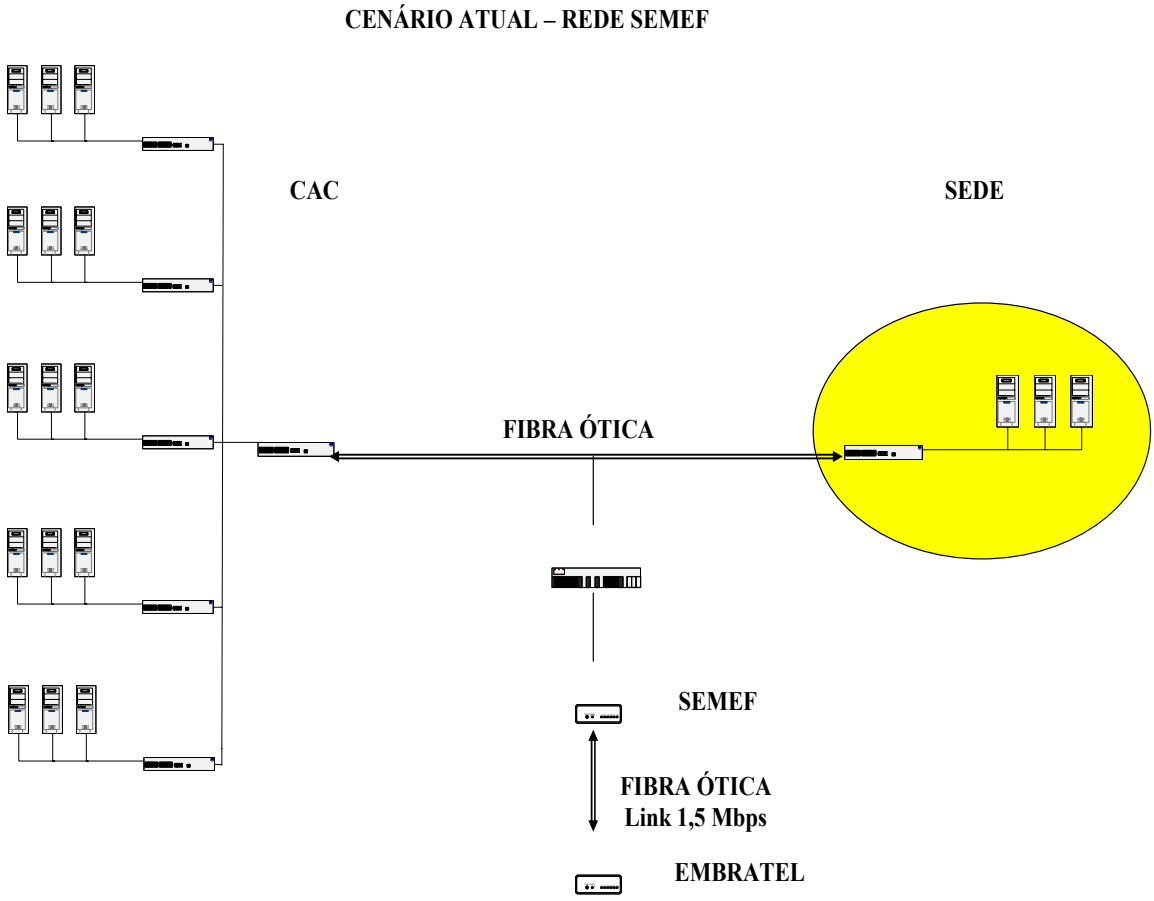

Figura 24: Cenário atual da rede computacional da SEMEF.

Estações de
Trabalhc

Switch 3com
4º Andar

A Figura 24 demonstra a topologia geral da rede computacional da Secretaria Municipal de Economia e Finanças – SEMEF da Prefeitura Municipal de Manaus, que é centralizada no bairro da Compensa interligada com uma LAN no centro de Manaus. A parte delimitada em cinza é um resumo da rede da sede que é maior que a do CAC (Centro de Atendimento ao Contribuinte) que fica localizado no centro. O CAC é conectado via fibra ótica com a SEDE de onde parte um link de 1,5Mbps com a EMBRATEL. Este link custa aos cofres públicos a quantia de R$ 5.500,00 / mês.

A figura abaixo indica como é o sistema de telefonia atual da SEMEF, verificamos que é totalmente independente da rede de computadores.

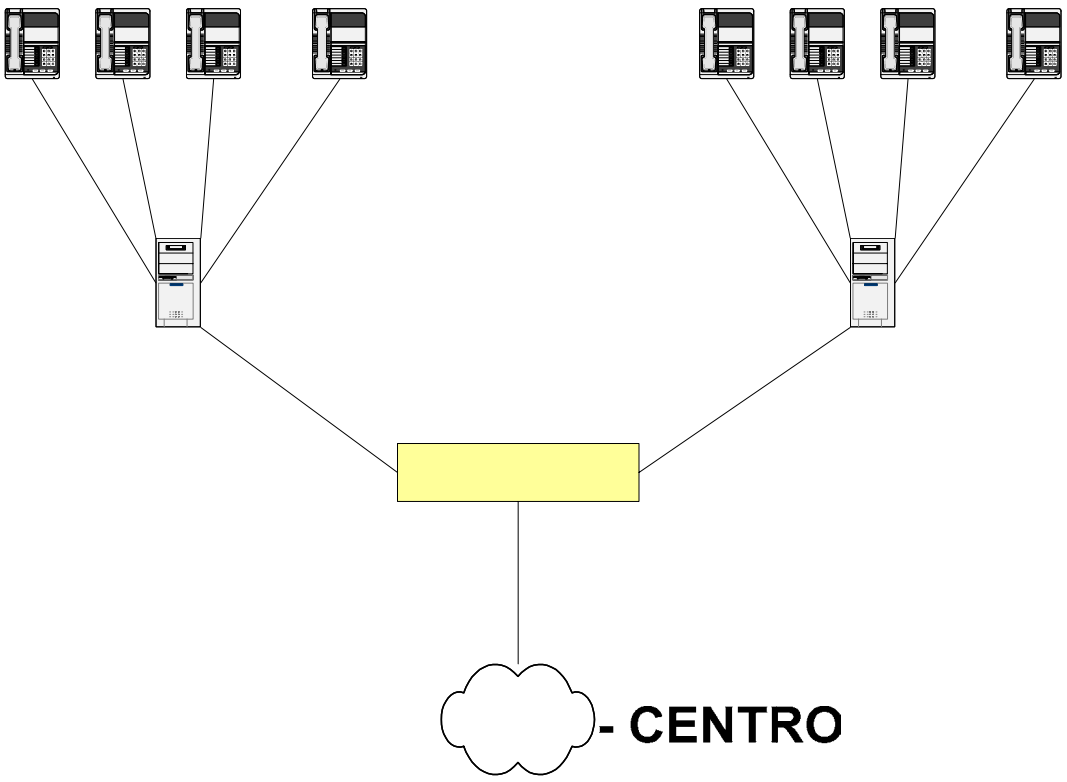

Figura 25: Sistema atual de telefonia da SEMEF.

Telefones do térreo, 1º, 2º, 3º e 4º andar

A transmissão da voz é feita de maneira totalmente independente da transmissão de dados, cuja rede utiliza os protocolos TCP/IP. Quando uma chamada telefônica era requisitada o PABX verificava se era uma chamada interna ou externa, caso seja interna ele direcionava a ligação para o ramal de destino, caso contrário envia a chamada para um multiplexador que por sua vez a envia para a rede de telefonia pública (*Telemar*). A partir da central da Telemar a chamada será encaminhada para a central de destino. Tal estrutura funcionava perfeitamente, porém tinha o inconveniente de ser uma solução de alto custo, devido a grande quantidade de ligações telefônicas realizadas diariamente entre os cerca de 1.200 funcionários da SEMEF em ambos os prédios.

4.4 CENÁRIO PROPOSTO PARA A REDE DA SEMEF

Para a implantação do projeto VoIP – SEMEF, necessitamos de dois equipamentos codificador de voz (*vocoders*), não teremos gastos com software pois usaremos o Microsoft Messenger, cerca de 120 telefones do modelo IP (uma para cada sala da SEMEF), isso se faz necessário para possuirmos uma redundância no sistema, necessitamos também de uma duplicação da largura de banda da SEMEF, pois cada telefone consumirá 64Kbps a mais, isso acarretará um aumento 1.024 Kbps no tráfego da rede.

Abaixo temos uma planilha com o total do investimento proposto:

EQUIPAMENTO	QUANTIDADE	PREÇO UNITÁRIO	PREÇO TOTAL
Vocoder	2	R$ 26.000,00	R$ 52.000,00
Telefone IP	120	R$ 184,86	R$ 22.183,20
Aumento na largura da banda	-	-	R$ 15.000,00 / mês
TOTAL	-	-	R$ 89.183,20

Fonte: preços coletados na Internet em Novembro de 2004 / Valor da largura da banda coletado junto a EMBRATEL em junho de 2004.

Vocoder é o codificador de voz que fica responsável por transformar o sinal analógico da voz, proveniente do PABX, em um sinal digital e empacotá-lo para que possa trafegar na rede IP. O modelo IEN 6000 possui portas ethernet 10Mbps BNC e UTP, que neste caso estão ligadas ao PABX e ao switch, respectivamente.

Figura 26: Vocoder IEN 6000.

O equipamento que funciona como **multiplexador e terminador ótico** é responsável por pegar várias ligações telefônicas de vários canais de entrada e transmitir por apenas um canal de saída, que utiliza fibra ótica para a transmissão do sinal telefônico. Neste caso o multiplexador recebe as chamadas do PABX e envia para a rede de telefonia pública (Telemar).

Com a inclusão do codificador de voz será possível unir a rede de voz com a rede de dados. Fato este que possibilita então que a voz seja enviada como dados comuns na rede da SEMEF.

A SEMEF manteve intacto quase todos os seus equipamentos já existentes e adicionou os somente dois codificadores de voz em sua estrutura. Todos os equipamentos utilizados estão listados abaixo:

- 120 Telefones IP
- 2 PABX (já existentes)
- 2 VOCODER (IEN 6000 - Hypercom)
- Switchs Gigabits (já existentes)
- Roteadores CISCO SYSTEMS (já existentes)

O **PABX** é uma central telefônica interna responsável por todo o gerenciamento das ligações telefônicas. Ele é responsável por enviar a ligação para o codificador de voz, caso seja necessário. O modelo BXS / 20, mostrado na figura abaixo possui, entre outras, as seguintes características:

- Plataforma multitarefa que permite, entre outros, os seguintes serviços: PABX, Correio de voz, Correio de fax, etc.
- Usa o sistema operacional Windows 2000.
- Possibilidade de interligação com qualquer central PABX.
- Portas E1 para interligar com a operadora de telecomunicações.

Figura 27: PABX BXS / 20.

4.4.1 Situação 1: Chamada VoIP de um terminal para outro entre os prédios

Quando um funcionário quiser fazer uma chamada de voz do CAC (centro) utilizando a sua estação de trabalho para uma outra estação de trabalho situada na SEDE (compensa) ou vice-versa. Esta é a situação mais simples no VoIP, é a primeira forma de comunicação não tarifada pois está usando a infra-estrutura da rede.

4.4.2 Situação 2: Chamada de um ramal IP de um prédio para outro ou para o mesmo prédio

Quando um funcionário de qualquer um dos prédios quiser fazer uma chamada via ramal IP, sua chamada será roteada do vocoder mais próximo até o vocoder do outro prédio. Está chamada também não será tarifada pela companhia telefônica.

4.4.3 Situação 3: Chamada de um ramal IP para uma estação de trabalho e vice-versa

Quando um funcionário quiser fazer uma chamada do seu ramal IP para uma estação de trabalho, sua chamada será encaminhada até o PABX mais próximo que por sua vez procurará o seu vocoder correspondente que roteará a chamada para o vocoder de outro prédio. Este vocoder encaminhará a chamada para o servidor gateway e este para a estação. Caso a chamada partir da estação de trabalho, será o servidor gateway (ao invés do PABX) que encaminhará a mensagem para vocoder.

4.4.4 Situação 4: Chamando um telefone externo a partir de um ramal IP ou estação de trabalho

Caso a chamada parta de um ramal IP, ela irá procurar o PABX, caso parta de uma estação irá para o servidor gateway, em ambos os casos a chamada será roteada pelo vocoder mais próximo e irá para o gateway da telemar. Esta situação será tarifada pois utiliza a companhia telefônica, entretanto, haverá um gerenciamento de todas chamadas (algo impossível na estrutura atual), o administrador de rede que atualmente gerencia apenas a rede de dados, possuirá relatórios detalhados e em tempo real de todas as chamadas telefônicas que parte da SEMEF para fora, quais são os ramais mais utilizados, quais os números externos mais acionados, quanto tempo dura uma chamada, quais são os funcionários “mais assíduos” ao telefone, etc. Dessa forma poderá ser estabelecida uma política de telefonia na instituição.

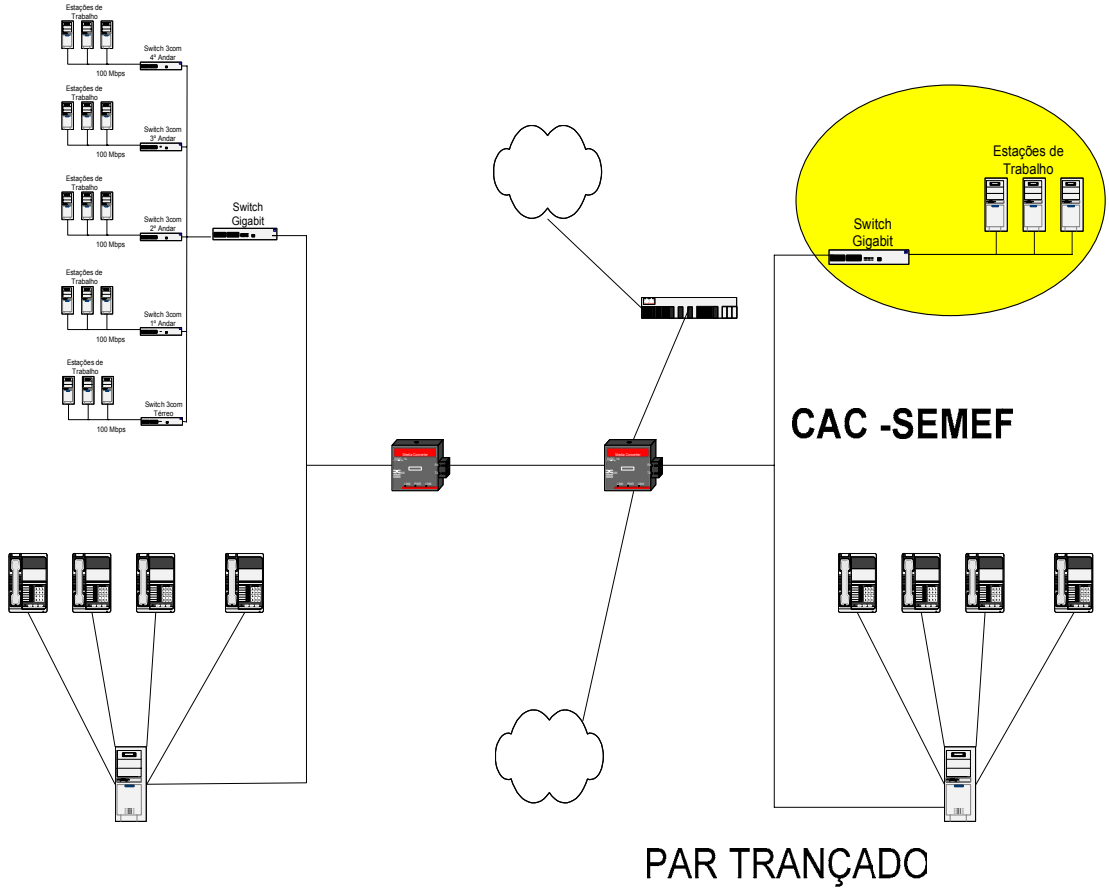

Figura 26: Sistema VoIP da SEMEF.

Telefones do térreo, 1º, 2º,
3º e 4º andar
(900 ramais em 8 linhas)

CABO COAXIAL

PABX

CONCLUSÃO

Nesta monografia observa-se que a tecnologia de voz sobre IP, em alguns casos, é uma alternativa bastante viável para corporações que desejam diminuir custos com ligações telefônicas. Como a estrutura da rede IP é bastante simples e utilizada no mundo todo, isso ajuda muito a perceber as vantagens que voz sobre IP pode proporcionar para as empresas. Como, por exemplo, utilizar uma rede IP já existente para incluir também o serviço de voz. No caso da SEMEF a implantação de voz sobre IP trará somente benefícios, com previsão para uma diminuição em seus gastos com ligações telefônicas e mantendo a qualidade do serviço satisfatoriamente. No caso SEMEF, a implantação de VoIP será bastante simples, devido ao acréscimo de somente dois vocoders e telefones IP por uma questão de redundância, o retorno financeiro dos investimentos será imediato (previsão). A tecnologia VoIP não causará o fim da utilização da telefonia convencional em ambientes corporativos, mas certamente será responsável por uma fatia considerável em ligações de longa distância. Pois vem se mostrando, em alguns casos, uma alternativa técnica e financeiramente viável.

REFERÊNCIAS BIBLIOGRÁFICAS

TANENBAUM, Andrew S. ***Redes de Computadores***. 4. ed. Campus. Rio de Janeiro: 1997.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER Sérgio. ***Redes de Computadores***. 6. ed. Campus. Rio de Janeiro: 1995.

FURASTÉ, Pedro Augusto. ***Normas Técnicas para o Trabalho Científico***. 13. ed.Dáctilo Plus. Porto Alegre: 2004.

HERSENT, Oliver; GUIDE, David; PETIT, Jean Pierre. ***Telefonia IP – Comunicação multimídia baseada em pacotes***. 1. ed. Makron Books. Rio de Janeiro: 2002.