Protocolos para Telefonia IP

Sérgio Yoshioka

Trabalho Final de Mestrado Profissional

Instituto de Computação
Universidade Estadual de Campinas

Protocolos para Telefonia IP

Sérgio Yoshioka

Julho de 2003

Banca Examinadora:

- Prof. Dr. Nelson Luis Saldanha da Fonseca (Orientador)
  Instituto de Computação - UNICAMP
- Prof. Dr. Edmundo Roberto Mauro Madeira
  Instituto de Computação - UNICAMP
- Prof. Dr. Omar Carvalho Branquinho
  Universidade São Francisco - USF
- Prof. Dr. Paulo Lício de Geus (Suplente)
  Instituto de Computação - UNICAMP

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Yoshioka, Sérgio

Y83p Protocolos para telefonia IP / Sérgio Yoshioka -- Campinas, [S.P. :s.n.], 2003.

Orientador: Nelson Luis Saldanha da Fonseca

Trabalho final (mestrado profissional) - Universidade Estadual de Campinas, Instituto de Computação.

1. Redes de computação – Protocolos. 2. Telecomunicações. 3. Comutação de pacotes (Transmissão de dados). 4. TCP/IP (Protocolos de rede de computação). 5. Sistemas multimídias. I. Fonseca, Nelson Luis Saldanha da. II. Universidade Estadual de Campinas. Instituto de Computação. III. Título.

Protocolos para Telefonia IP

Este exemplar corresponde à redação final do Trabalho Final devidamente corrigida e defendida por Sérgio Yoshioka e aprovada pela Banca Examinadora.

Campinas, 28 de Julho de 2003.

Prof. Dr. Nelson Luis Saldanha da Fonseca
Instituto de Computação UNICAMP
(Orientador)

Trabalho Final apresentado ao Instituto de Computação, UNICAMP, como requisito parcial para a obtenção do título de Mestre em Computação na área de Engenharia da Computação.

TERMO DE APROVAÇÃO

Tese defendida e aprovada em 28 de julho de 2003, pela Banca Examinadora composta pelos Professores Doutores:

Prof. Dr. Omar Branquinho
Universidade de São Francisco

Prof. Dr. Edmundo R. M. Madeira
IC - UNICAMP

Prof. Dr. Nelson Luis Saldanha da Fonseca
IC - UNICAMP

Resumo

A telefonia IP, também chamada de VoIP (*Voice over IP*), pode ser definida como qualquer aplicação telefônica usada em uma rede de comutação de pacotes de dados que utiliza o protocolo *Internet Protocol* (IP). Engloba novas aplicações que exploram a integração da comunicação de voz, imagens e de dados simultaneamente. Protocolos vêm sendo propostos para telefonia IP. No entanto, um grande desafio a ser transposto por estes protocolos é a garantia de qualidade de voz similar à da telefonia comutada por circuitos. Este trabalho apresenta os protocolos H.323, SIP, MGCP e Megaco/H.248 para telefonia IP, faz uma comparação destes protocolos e aborda fatores que afetam a Qualidade de Serviço (QoS) de telefonia IP.

Abstract

IP telephony can be defined as any telephonic application over the Internet Protocol and is one of the new applications that explore the integration of voice, image and data communication. Protocols have been proposed for IP telefony. However, one of the challenges in the IP telephony is to assure that the voice quality has similar quality of the one in circuit-switched telephony. This work presents the protocols H.323, SIP, MGCP and Megaco/H.248 for IP telephony and compare them. It also describes the issues which impact the Quality of Service (QoS) in IP telephony.

Dedicatória

Dedico este trabalho aos meus pais Yoshioka Kazuyo e Setsú Yoshioka pelo apoio e incentivo em todos os momentos de minha vida.

In Memoriam: Ao "anjinho" que Deus chamou tão inesperadamente e precocemente, deixando imensas saudades para seus pais.

Agradecimentos

A Deus por tudo que tem feito por mim.

À minha querida companheira Cíntia pelo apoio irrestrito, perseverança, otimismo, carinho, amor e compreensão, principalmente nos momentos mais desafiadores.

Aos meus filhos Thiago e Guilherme que proporcionaram muitas alegrias que serviram de motivação para superar tudo.

Ao meu orientador, Prof. Dr. Nelson Luis Saldanha da Fonseca, pela atenção, paciência, compreensão, sensibilidade e incentivo que foram fundamentais para a efetiva conclusão do mestrado diante das dificuldades pessoais e do período de convalescença.

Ao meu irmão Eduardo Yoshioka, pela presteza em ajudar-me no que fosse preciso, muitas vezes abdicando de seus afazeres.

Aos amigos e colegas que estiveram presentes oferecendo apoio e incentivo para mim e minha família. Em especial ao Anderson Luiz Barbosa, Marlene Callas, Prof. Dr. Tabajara Dias Andrade e Tatiana Patrasso Coracini.

Ao Luciano Roberto Rampazzo, amigo de mais de duas décadas, pela solidariedade e bondade.

Aos amigos Carlos Eduardo Pereira e Valéria Bernadete Seckler Pereira pela presença e apoio em vários momentos importantes de minha vida.

Ao Prof. Dr. Joinvile Batista Júnior que compartilhando seus conhecimentos no início de minha carreira profissional, foi um dos motivadores para esta caminhada.

Aos demais docentes, funcionários e colegas de turma do Instituto de Computação pela amizade e companheirismo demonstrados.

Gostaria de registrar um agradecimento especial ao Prof. Dr. João Luiz Pinto e Silva (FCM-UNICAMP) pela sensibilidade e competência demonstrados em um momento de grande provação para minha família.

In Memoriam: A Profª. Dra Kazue Panetta (FCM-UNICAMP) que trouxe ao mundo meus dois filhos, pelos conselhos, incentivo, dedicação e exemplo de profissionalismo.

Conteúdo

Índice de Figuras

Índice de Tabelas

1 Introdução

A telefonia IP, também chamada de VoIP (*Voice over IP*), pode ser definida como qualquer aplicação telefônica usada em uma rede de comutação de pacotes de dados, que utiliza o protocolo *Internet Protocol* (IP) [COLLINS] [DEFVOIP] [THALHAMMER]. A telefonia IP engloba novas aplicações que exploram a integração da comunicação de voz, imagens e de dados simultaneamente. Estas aplicações englobam computadores (Figura 1.a), computadores com telefone (Figura 1.b), telefone com telefone (Figura 1.c) e podem existir tanto em rede IP privativa, Internet pública ou intranet.

Algumas referências à telefonia IP enfocam a realização de chamadas de longa distância usando Internet. A idéia de se fazer chamadas de longa distância grátis sobre a Internet pública é chamada de VON (*Voice on the Net*) [MOCKINGBIRD] [VONCOM]. VON, portanto, é um aplicação específica de telefonia IP, com organizações, como *a Voice On the Net Coalition* [VONORG], atuando na disseminação e defesa de interesses de empresas que atuam neste segmento.

As chamadas VON inicialmente eram de baixa qualidade com retardos substanciais, e eram rotuladas de chamadas grátis na Internet [RINDE], e tinham um custo inexpressivo quando comparados com a rede pública de telefonia. A qualidade da voz era muito inferior a rede telefônica pública, com atrasos superiores a três segundos e mesmo assim era atrativo para grupos de usuários que trocavam a qualidade da voz por um preço nulo. Essas primeiras aplicações utilizavam PCs que introduziam retardos devido a natureza *half-duplex* das placas de som e eram preparadas para executar sons a partir de CD-ROMs. Os processadores 486 Intel®, lentos para tratar voz, bem como o sistema operacional Microsoft® Windows 3.1, predominante na época, não era um autêntico sistema multitarefa, inserindo retardos na emulação de multitarefas. Um outro fator de inserção de retardo eram os modems utilizados da época.

Além disso, a natureza "*best effort*" dos serviços Internet introduz retardos variáveis e mesmo "buracos" na transmissão de voz que resultam em uma perceptível baixa qualidade de voz em relação a rede de telefonia pública. Assim sendo, as técnicas de telefonia IP devem buscar o transporte do tráfego de voz com qualidade.

O mercado de telefonia IP concentra-se em dois tipos de aplicações chaves. O primeiro tipo consiste de redes privadas corporativas que buscam aproveitar as "*intranets*" existentes, inserindo serviços de voz e fax com tecnologia de telefonia IP, economizando com pagamentos as operadoras telefônicas e com gerenciamento de uma única rede, ao invés do gerenciamento da rede de dados e da rede de voz.

O segundo tipo de aplicação de telefonia IP consiste na utilização de dispositivos projetados para permitir o transporte de voz entre de redes de dados e redes de telefonia convencional.

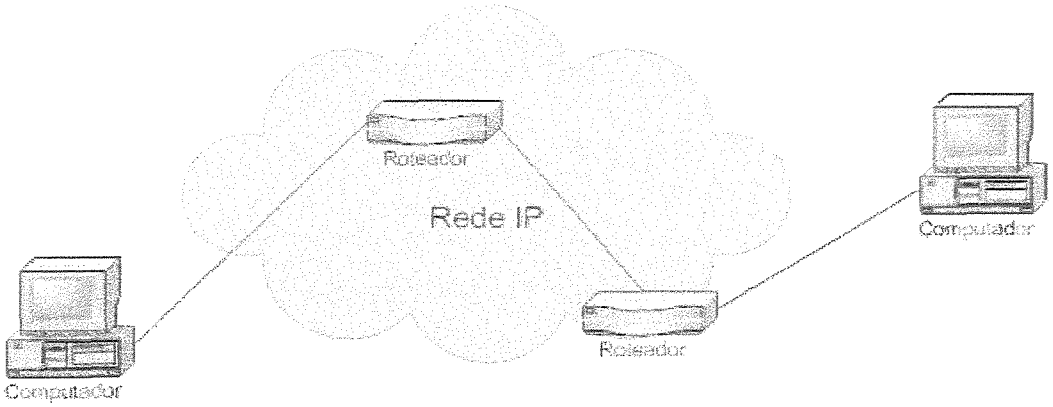

Figura 1.a Telefonia IP - Computador a Computador

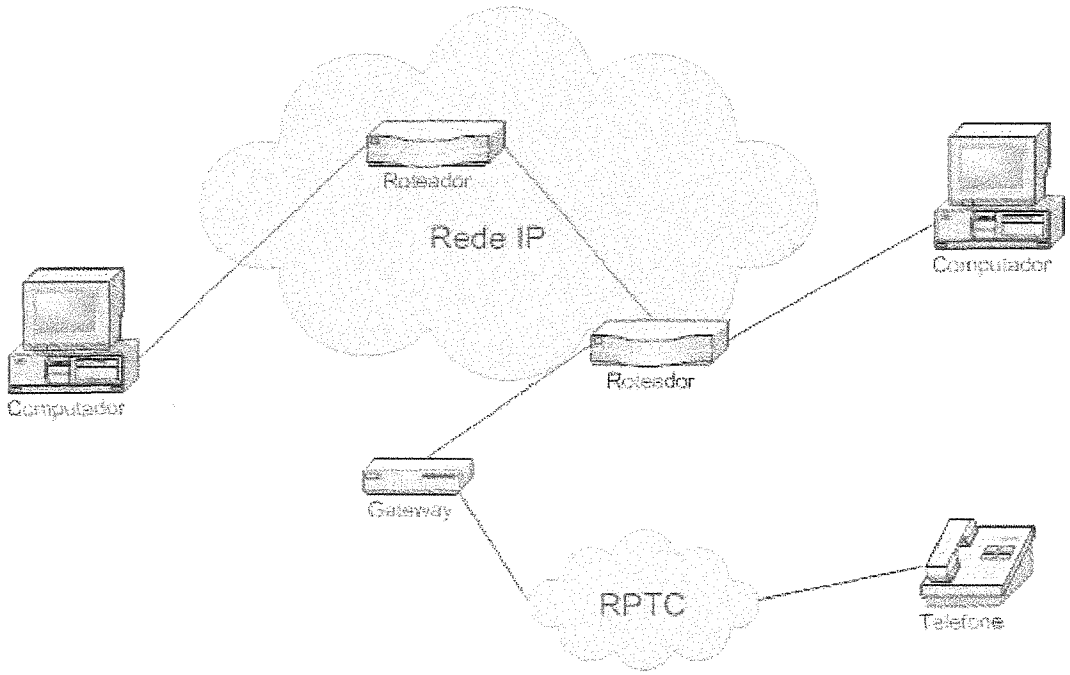

Figura 1.b Telefonia IP - Computador a Telefone

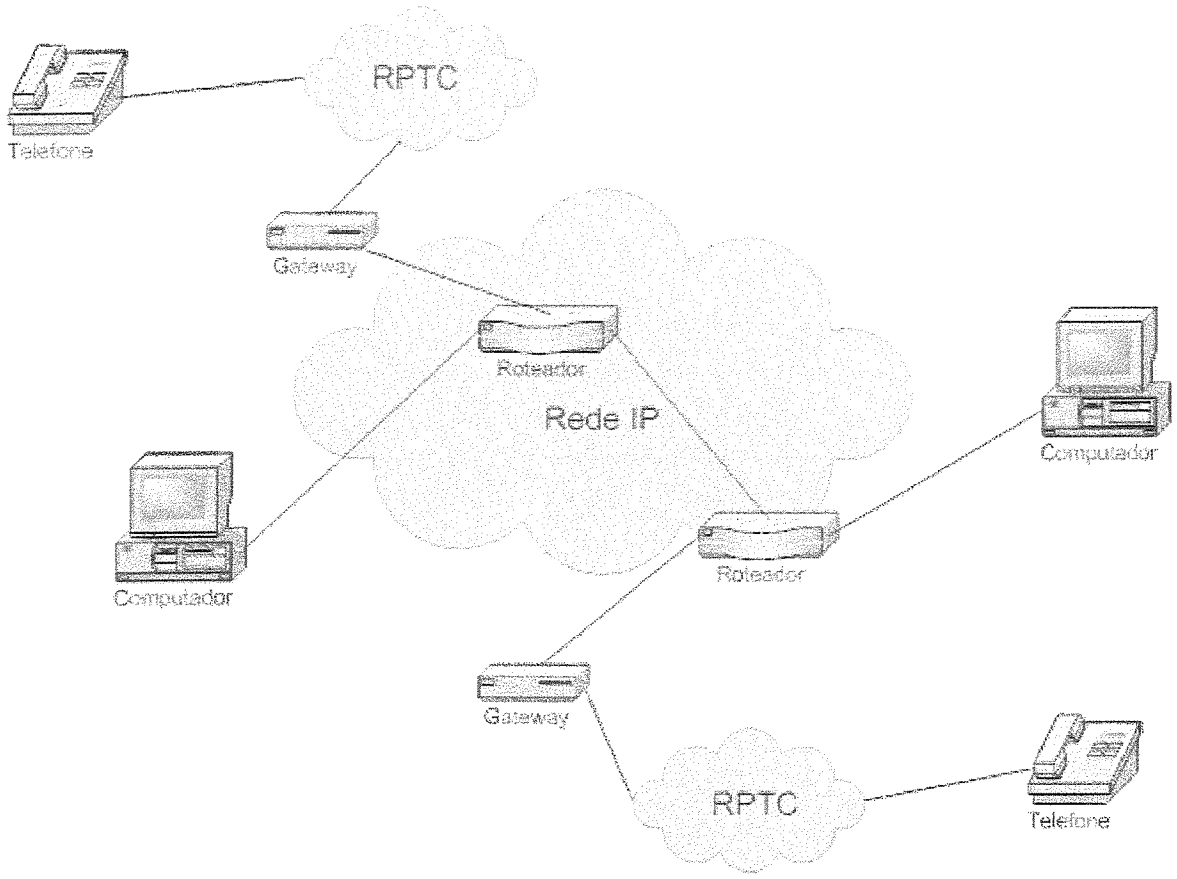

Figura 1.c Telefonia IP - Diferentes Cenários

Em breve estarão operando as redes de próxima geração, também conhecidas como NGN (*Next Generation Networks*), que são redes de comunicação baseadas em interfaces abertas e com capacidade para transmitir voz, dados, imagens, som e vídeo simultaneamente em uma estrutura comum. Também são chamadas de redes multisserviços. A principal diferença entre as redes de próxima geração e as redes convencionais das operadoras telefônicas de comutação por circuitos está na estrutura de transmissão por pacotes adotada nessas redes que utiliza o *Internet Protocol* (IP). A principal mudança realizada na estrutura das operadoras, para oferecerem esses novos serviços, refere-se à transmissão de voz. Para que possam trafegar nas novas redes, os sinais de voz são convertidos em pacotes, que se misturam aos pacotes de dados durante o transporte.

Para interoperar e integrar a rede de telefonia IP com a rede pública telefônica comutada (RPTC), baseada em comutação por circuitos são usados *gateways*, que são equipamentos que convertem a sinalização e o transporte da voz entre os dois tipos de redes.

Na telefonia convencional de comutação por circuitos a arquitetura é centralizada, ou seja, os telefones são controlados por comutadores centralizados para simplificar o gerenciamento dada a falta de recursos dos telefones. Uma vantagem adicional da

tecnologia da telefonia IP é permitir a adoção tanto de uma arquitetura centralizada como de uma distribuída, dependendo dos protocolos utilizados, permitindo a adoção de gerenciamento simplificado com mais recursos para os pontos terminais (*endpoints*).

A arquitetura centralizada na telefonia IP permite o gerenciamento, provisionamento e controle de chamadas de modo centralizado, simplificando o fluxo de mensagens de chamadas. Esta arquitetura opera de modo semelhante aos sistemas da telefonia convencional, o que torna mais fácil o entendimento desta nova tecnologia para os profissionais do sistema telefônico convencional.

As arquiteturas distribuídas permitem que a inteligência da rede seja distribuída entre os dispositivos de controle de chamadas e os pontos terminais. Por inteligência da rede entendemos o roteamento das chamadas, tarifação, resolução de nomes e endereçamento, provisionamento, serviços suplementares, gerenciamento, entre outros [PACKETVOICE].

No sistema telefônico convencional além da rede de transporte de voz e sinalização de chamadas, são geralmente utilizadas redes IPs para a gerência da rede telefônica, provisionamento de dados, coleta de dados de tarifação, etc.

Com a telefonia IP é possível o uso da mesma rede IP para essas funcionalidades possibilitando a otimização do uso da infra-estrutura.

Como vantagens adicionais da telefonia IP pode-se citar:

- Custos reduzidos de ligações de longa distância;
- Melhor ocupação de banda na rede IP;
- Criação de novas classes de serviços combinando o uso de características de voz em tempo real com o de processamento de dados nas redes, tais como *telecommuting*, *call centers* baseados em *web*, telemedicina, *instant messenger*, etc [Schulzrinne1];
- Uso mais eficiente do grande número de redes IP existentes;
- Interoperabilidade com a rede pública de telefonia comutada (RPTC) através de *gateways* de mídia e de sinalização;
- Integração com aplicações e recursos existentes nas redes de dados, provendo maior variedade de serviços.

No entanto, existem alguns desafios para telefonia IP, tais como atingir uma qualidade de voz similar a da telefonia convencional, bem como garantir que a qualidade de voz mantenha-se estável durante a chamada, como ocorre na telefonia convencional. Outro desafio é manter uma disponibilidade similar da rede telefônica convencional, superior a 99,999%, de modo a não gerar insatisfação com os usuários [COLLINS] [DOUSKALIS].

Do ponto de vista social e econômico, é preciso prover mecanismos para que a telefonia IP não se torne uma opção de tecnologia para uma elite [GORALSKY].

Além disso, a telefonia IP deve preservar os serviços já existentes na telefonia convencional para os usuários.

O compromisso com a Qualidade de Serviço (QoS - *Quality of Service*) deve enfocar parâmetros relacionados com o transporte no protocolo IP tais como: retardo, perda de pacotes, *jitter*[1], bem como a convivência com o tráfego de dados, mecanismos de supressão de silêncio e de cancelamento de eco que influenciam a qualidade da voz, um dos desafios da telefonia IP, como veremos ao longo desta monografia.

As redes de telefonia móvel de terceira geração, como a *UMTS (Universal Mobile Telecommunications System)*, permitem a transmissão de dados a altas taxas de transmissão em redes IPs, já prevendo classes de serviço para aplicações sensíveis ao atraso, como a telefonia IP. Desta maneira, a transmissão de voz nestas tecnologias, também deverá ser feita através da comutação de pacotes, utilizando protocolos de telefonia IP [HERSENT].

Esta monografia está dividida da seguinte forma: na segunda seção são apresentadas as características dos protocolos de telefonia IP MGCP, Megaco/H.248, H.323 e SIP. São feitas também comparações entre protocolos. Na terceira seção são apresentados parâmetros de Qualidade de Serviço e fatores que afetam a qualidade de voz para telefonia IP. Finalmente, na quarta seção são apresentadas as conclusões sobre este trabalho e seus possíveis desdobramentos.

2 Protocolos de Telefonia IP

Nesta seção, serão apresentados os protocolos SIP, H.323, MGCP e Megaco/H.248 para telefonia IP. Uma comparação entre estes protocolos também será apresentada.

2.1 Protocolo SIP (Session Initiation Protocol)

O protocolo *Session Initiation Protocol* (SIP) foi especificada pela IETF (*Internet Engineering Task Force*) [IETF] no grupo de trabalho MMUSIC (*Multi Party Multimedia Session Control*). A primeira versão (1.0) foi submetida em 1997 como *Internet Draft* [SIPCHARTER][JOHNSTON]. Mudanças significativas foram realizadas no protocolo, resultando em outra submissão como *Internet Draft* versão 2.0. Em março de 1999 foi publicada como RFC 2543 [RFC2543] e em setembro de 1999 foi estabelecido o grupo de trabalho SIP. Em 2002 foi submetido um novo *Internet Draft* [RFC2543BIS], corrigindo algumas falhas da RFC 2543, conhecida como "RFC 2543bis". Esse *Internet Draft* tornou-se em Junho de 2002 a RFC 3261[2] "*Session Initiation Protocol*" [RFC3261] e tornou obsoleta a RFC 2543.

O SIP é um protocolo que incorpora características de outros protocolos usados na Internet como HTTP *(Hiper Text Transport Protocol)*, SMTP *(Simple Mail Transport Protocol)* e DNS *(Domain Name System)* [SIPCHARTER] [JOHNSTON] [SCHULZRINNE2]. O SIP utiliza esquema de codificação textual, com uso de cabeçalhos do SMTP. Utiliza o modelo cliente-servidor e as URLs (*Uniform Resource Locators*) do protocolo http.

---

[1] Na subseção 3.2 Parâmetros de Qualidade de Serviço serão detalhados esses parâmetros.

[2] A RFC 3261 corrige erros e detalha melhor cenários da RFC 2543. De acordo com [RFC3261] algumas mudanças podem trazer problemas de interoperabilidade. Este trabalho foi baseado na [RFC2543BIS].

SIP foi concebido pelo IETF para ser um protocolo de sinalização, permitindo modificar e terminar sessões de comunicação interativa entre dois ou mais participantes. Essas sessões podem incluir voz, vídeo, *chat*, mensagens instantâneas, jogos interativos e realidade virtual.

O SIP utiliza outros protocolos como o *Session Description Protocol* (SDP) para negociações de codificadores[3] de voz, o *Domain Name System* (DNS) para localização de nomes, *Uniform Resource Locators* (URL) [RFC1738] para endereçamento e o *Telephony Routing Over IP* (TRIP) para roteamento de chamadas.

Os serviços suportados pelo SIP incluem:

- Localização de usuários - determina a localização do usuário para chamada;
- Estabelecimento de chamada: sinaliza toque de chamada e o estabelecimento de chamada;
- Disponibilidade do usuário - determina a disponibilidade da parte chamada para estabelecer a comunicação;
- Capacidade do usuário - determina o meio de comunicação e seus parâmetros de configuração. O SIP usa o protocolo SDP para negociação de parâmetros;
- Tratamento de chamada: transferência, características e terminação de chamadas.

Embora o IETF tenha progredido na criação de extensões permitindo a integração e interfuncionamento com a RTPC, a grande motivação do protocolo SIP é criar um ambiente que suporta modelos de comunicação de próxima geração em rede IP [IEC].

A seguir serão apresentados o endereçamento SIP, os servidores e clientes SIP, diagramas de chamadas SIP e as mensagens SIP.

2.1.1 Endereçamento

O protocolo SIP adota para endereçamento um identificador com formato similar ao do telnet ou email podendo ser "usuário@domínio", "usuário@host", "usuário@IP" ou "númerodotelefone*@gateway*", este último indicando um número de telefone da rede pública acessível via um determinado *gateway*.

O SIP usa esses endereços como parte da URLs SIP. Como exemplos podemos citar: sip://sergio@unicamp.br, sip://5501999940000@gateway1 e sip://sergio@10.10.10.1.

Estes endereços podem ser colocados em uma página *web* como *link* para fazer uma chamada SIP [WANG] [SCHULZRINNE2].

---

[3] Um codificador de voz digitaliza a voz analógica utilizando técnicas de compressão e amostragem. Quanto maior a compressão, maior será o custo computacional para o processamento. Além disso, a perda de pacotes ou mesmo atraso em codificadores que compactam muito (G.729 por exemplo), tem um impacto na clareza muito mais acentuado que um codificador que compacta menos (por exemplo G.711).

2.1.2 Mensagens SIP

O protocolo SIP usa seis tipos de mensagens, chamados de métodos, entre o agente usuário e servidor:

- *INVITE* - convite para estabelecer conexão entre dois agentes usuários;
- *BYE* - para terminar uma conexão entre dois pontos terminais;
- *ACK* - para reconhecer as respostas finais dadas em requisições de *INVITE*;
- *OPTIONS* - para obter as informações de capacidade e disponibilidade do usuário e servidor;
- *REGISTER* - para informar a localização do usuário para o servidor SIP de registro;
- *CANCEL* - para finalizar um pedido enquanto o servidor não tiver enviado uma resposta final.

Existem quatro tipos de cabeçalhos presentes nas mensagens SIPs: *general*, *request*, *response* e *entity*. O SIP também possui classes de respostas de mensagens que retornam informações das solicitações feitas, tais como: atendimento do lado chamado (mensagem "200"), alarmando lado chamado (mensagem "180"), etc. Maiores detalhes estão disponíveis no apêndice.

O SIP utiliza o protocolo SDP para descrever uma chamada, especificando tipo de codificador de voz, nome da sessão e atributos. O SDP é definido pela RFC 2327 [RFC2327] produzido pelo grupo de trabalho da IETF MMUSIC.

O SDP é um protocolo com formato textual criado inicialmente para descrever sessões de *multicast* para a rede de comunicação *multicast* da Internet (MBONE) sendo a primeira aplicação do SDP foi o SAP (*Session Announcement Protocol*) usado para enviar e receber anúncios das sessões MBONE.

O SDP contém as seguintes informações sobre sessões:

- Endereço IP (IP v4 ou *hostname*);
- Número da porta (TCP ou UDP usada para transporte);
- Tipo de mídia (vídeo, áudio, interativo, etc);
- Codificador de mídia adotado (GSM, PCM-lei A, G.711, G.729, MPEG II, etc);
- Nome da sessão e sua finalidade;
- Informações para contato (email, telefone);
- Banda Passante;
- Tempo de início e fim de sessão;
- Zona;
- Conexão;
- Atributo.

Uma mensagem SDP é composta por um conjunto de linhas, sendo cada linha um campo, cujos nomes são abreviados por uma letra minúscula, imediatamente seguido do(s) valor(es). Caso exista mais de um valor, estes devem estar separados exatamente por um

espaço em branco. Os campos são seqüencialmente ordenados para facilitar a análise dos dados, sendo alguns campos obrigatórios. A descrição dos campos do SDP está no apêndice.

2.1.3 Servidores e Clientes SIP

Um sistema SIP pode consistir de agentes usuários SIP e servidores SIP. Os participantes (agentes usuários) de uma chamada SIP podem tanto gerar como responder requisições, atuando como cliente quando geram requisições e como servidor quando respondem as requisições, ou seja, os agentes usuários tem uma parte cliente e outra servidor.

Uma chamada SIP pode ser feita diretamente entre os usuários, sem necessidade de servidores, como ilustra a Figura 2.

A arquitetura SIP permite distribuir seus serviços entre diversos servidores que são descritos a seguir, com suas possíveis atuações.

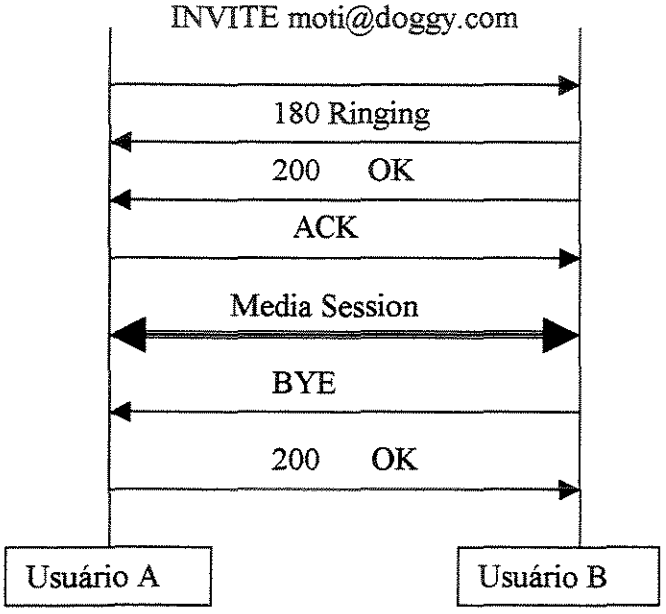

Figura 2 Troca de sinalização entre chamada simples SIP

2.1.3.1 Servidores SIP

Servidores SIP são aplicações que aceitam requisições SIP e respondem, interagindo e fazendo requisições para os agentes usuários, intermediando os processos de busca e negociação entre os agentes usuários. Os tipos de servidores SIP são:

- Servidor *proxy*

Um servidor *proxy* executa o processo de sinalização no lugar dos clientes (agentes usuários), encaminhando as requisições para um servidor de próximo salto (*next hop*

server), que pode ser um outro *proxy* ou o destino final (agente usuário servidor). Veja exemplo na Figura 3.

Para fazer o encaminhamento usa um servidor de localização, que contém informação sobre o próximo salto ou o novo endereço do cliente com o qual se deseja conectar, fazendo então o mapeamento do endereço antigo para o novo. Este mapeamento é útil, por exemplo, na situação em que o usuário tenha mudado temporariamente ou permanentemente de localização para que os demais usuários possam acessar automaticamente a nova localização.

Um servidor *proxy* pode operar no modo "sem estado" ou "com estado". O servidor *proxy* "sem estado", não armazena nenhuma informação de requisições ou respostas que tenha enviado ou recebido. Não retransmite mensagens e não usa relógios de temporização. Já o servidor "com estado" armazena as requisições e respostas recebidas no passado e usa estas informações para futuras requisições e respostas. Ao encaminhar uma mensagem, o servidor ativa um relógio de temporização. Caso o intervalo de temporização termine sem que o servidor receba alguma mensagem de confirmação, a mensagem é retransmitida.

- Servidor de redirecionamento

Um servidor de redirecionamento usa o serviço de localização. No entanto, diferentemente do servidor *proxy*, a informação da localização atual somente é devolvida ao lado chamador, que a partir da(s) informaçã(ões) deve iniciar a sinalização com o lado chamado diretamente, não envolvendo o servidor de redirecionamento na negociação. O servidor de redirecionamento é útil para obter a localização atual do usuário que se moveu temporariamente ou permanentemente, informando os endereços alternativos do usuário, bem como ajudar no balanceamento de carga, informando um servidor alternativo para um usuário. A Figura 4 ilustra uma situação em que ocorreu uma mudança temporária de localização de um usuário, e o servidor de redirecionamento informa a localização atual desse usuário.

- Servidor de registro

Um usuário SIP pode ter seu endereço IP alterado devido a várias razões, como no caso de fornecimento de endereços dinâmicos pelo provedor para um usuário móvel ou devido a mudança de localização física. A função do servidor de registro aceitar pedidos "REGISTER" é manter atualizado o cadastro de localização dos usuários SIP.

A Figura 5 ilustra o armazenamento do novo endereço IP do usuário A associado ao endereço de URL SIP. É feito um cadastramento do novo endereço IP do usuário A no servidor de registro, permitindo que outros usuários que desejem contactar esse usuário possam estabelecer contato através de um serviço de localização que utiliza os dados armazenados no servidor de registro. O servidor de registro torna disponíveis suas informações para outros servidores SIP (*proxy*, redirecionamento) dentro do mesmo domínio administrativo.

Esta funcionalidade geralmente é combinada com outras como de *proxy* ou servidor de redirecionamento, mas trata-se de um processo lógico distinto.

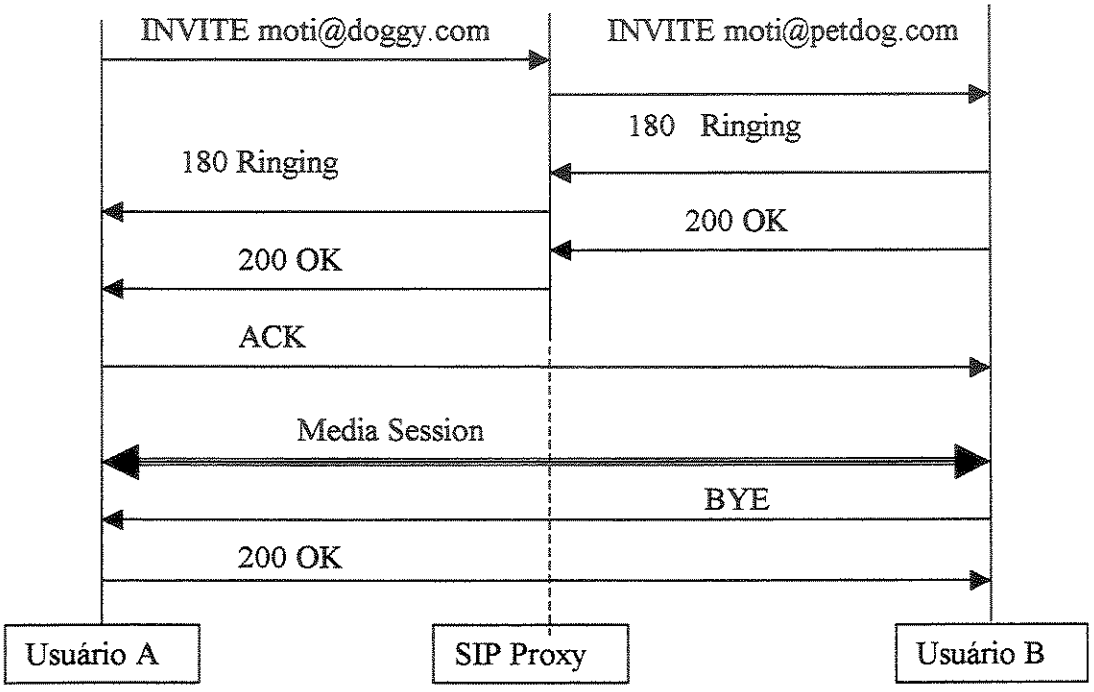

Figura 3 Sinalização entre chamada com SIP Proxy

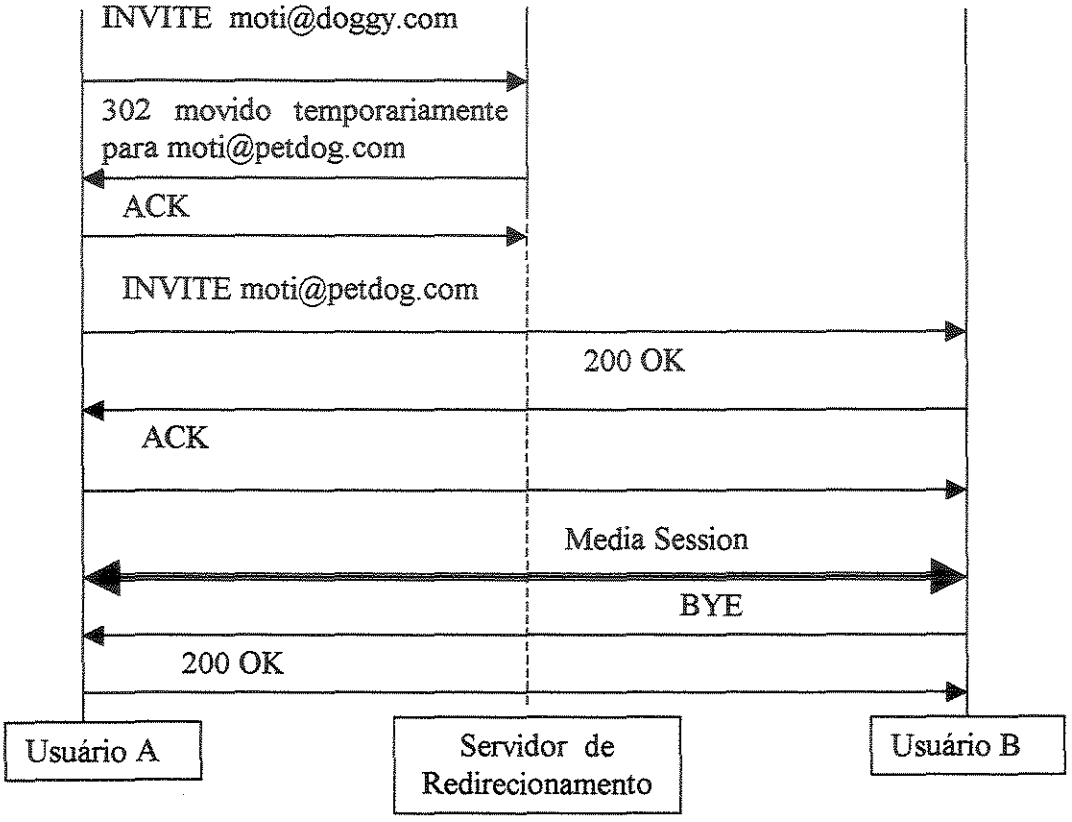

Figura 4 Sinalização de chamada com servidor de redirecionamento

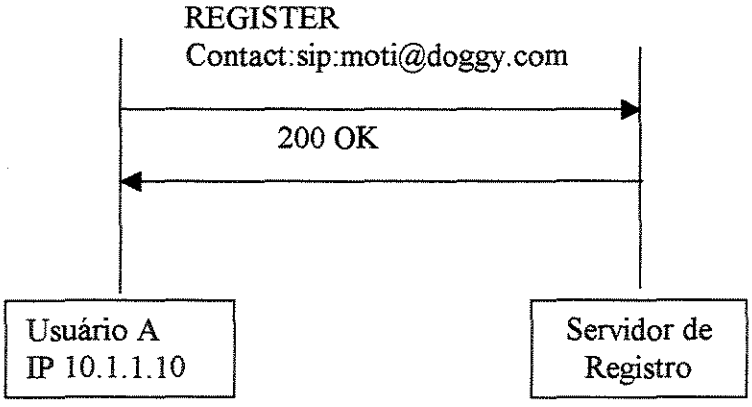

Figura 5 Registro de usuário no servidor de registro

- SIP *Gateway*

É um servidor que faz a interoperabilidade entre uma rede SIP e outra rede que usa outro protocolo de sinalização, podendo interoperar com a rede pública de telefonia comutada (RPTC) e com outros protocolos tais como o protocolo H.323.

A Figura 6 mostra um exemplo de funcionamento do *gateway* SIP/RPTC.

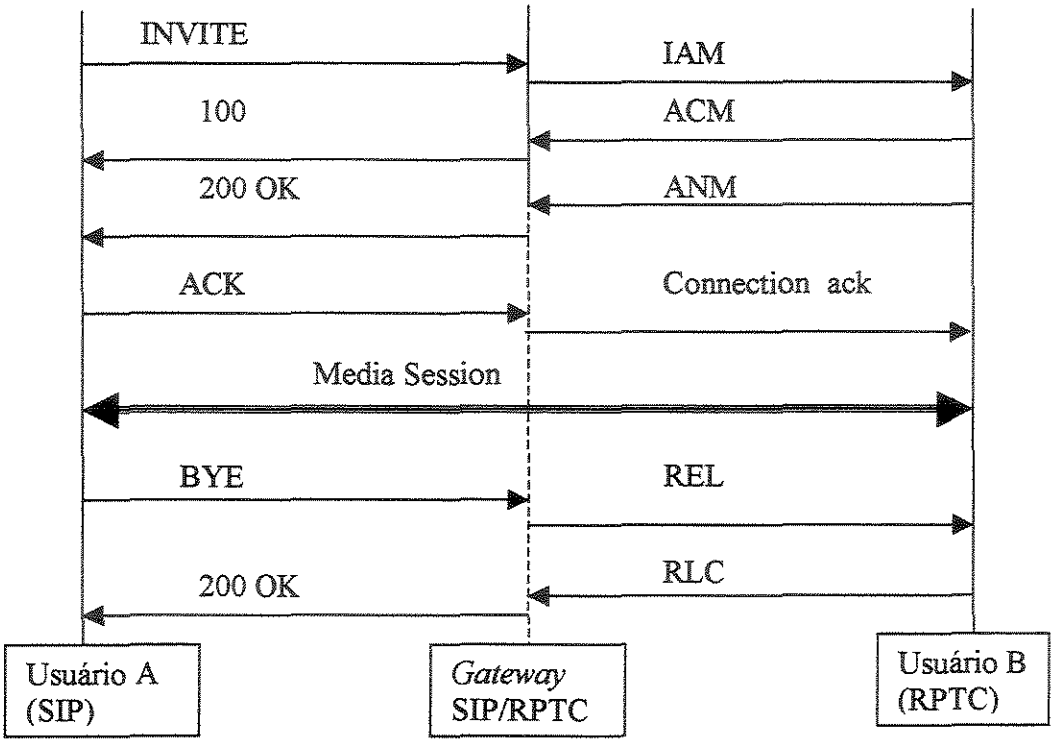

Figura 6 Uso de *Gateway* SIP/RPTC para chamada entre SIP e RPTC

Não existe distinção entre um servidor *proxy*, servidor de redirecionamento, agente usuário servidor, exceto que o agente usuário servidor pode aceitar ou rejeitar requisições enquanto o servidor *proxy* e o servidor de redirecionamento não pode [SCHULZRINNE4].

2.2 Protocolo H.323

Os primeiros sistemas de telefonia IP usavam sinalização proprietária. Dois usuários podiam se comunicar somente se ambos usassem o mesmo sistema proprietário, existindo, portando um problema de interoperabilidade entre sistemas de diferentes vendedores, impedindo uma adoção mais ampla da telefonia IP [ERICSSON]. Em resposta ao problema de interoperabilidade surgiu a recomendação H.323. Esta recomendação é uma especificação "guarda-chuva" publicada pelo ITU [ITU].

A primeira versão do H.323 surgiu em 1996 com o título de "*Visual Telephone Systems and Equipment for LANs with no Quality of Service*", que era orientado a comunicações em redes locais. Em 1998, foi gerada a segunda revisão da recomendação com o título *de "Packet-Based Multimedia Communications Systems*", sendo que esta versão recebeu mais suporte que seu predecessor, principalmente por operadores de rede e vendedores com mais experiência na telefonia tradicional. Esta versão é amplamente implementada em soluções de telefonia IP e tornou-se um padrão.

A terceira versão trata da comunicação de fax sobre a rede entre outros. A recomendação H.323 está na sua quarta revisão[4] (liberada em 17 de novembro de 2000), sendo sua característica principal o oferecimento de QoS no nível de transporte através do uso do protocolo RSVP (*Resource Reservation Protocol*) [RFC2205]. Além disso, foram definidos o formato URL H.323 que é "h323:usuário@host" e o mecanismo para possibilitar balanceamento de carga de *gatekeepers*.

Empresas como Cisco® [CISCO], Genuity® [GENUITY], iBasis® [IBASIS], Itxc® [ITXC], Lucent® [LUCENT], Microsoft® [MICROSOFT], PictureTel® [PICTURETEL], Polycom® [POLYCOM], Radvision® [RADVISION], Siemens® [SIEMENS], Sonus Networks® [SONUS], Tanberg® [TANBERG], VocalTec® [VOCALTEC] adotaram o H.323 [PACKETIZER].

Um ambiente H.323 é composto dos seguintes elementos:

- *Gateway* - Permitem a interconexão com outros dispositivos em ambientes de redes heterogêneos, servindo de pontes e mapeando protocolos de controle de chamada (Q.931, H.225.0, etc), protocolos de controle (H.242, H.245, etc), métodos de codificação (G.711,G.729, etc), métodos de serialização (empacotamento RTP, etc). Realizam o estabelecimento e o término da chamada entre outras funções;

- MCU (*Multipoint Control Unit*) - Permitem sessões com múltiplos participantes, conferências multimídias entre terminais. Coordenam a alocação de capacidade para os participantes. Um MCU possui um controlador multiponto (MC - *Multipoint Controller*) que tem a função de controlar a conferência e a negociação (H.245) entre terminais e os recursos alocados. Possui também um processador multiponto (MP - *Multipoint Processor*) que tem a função de manipular os fluxos de mídia, fazendo o processamento das mídias. Os MCs e os MPs podem estar implementados em qualquer componente H.323;

- Terminal - Iniciam e finalizam chamadas H.323 ou participam de conferências multipontos. Terminal, *gateway* e MCU são referenciados coletivamente como pontos terminais. Podem ser desde um simples telefone H.323 até uma avançada estação de trabalho;

- *Gatekeeper* - Por questões administrativas, trechos de uma rede IP são agrupadas em zonas (Figura 7), que são grupos lógicos de dispositivos. As zonas podem conter parte de uma topologia descentralizada conectada por roteadores e abranger uma ampla área geográfica. Um *gatekeeper* centraliza, administra e monitora todas as chamadas H.323 dentro de uma zona provendo dois serviços principais: resolução de endereços e admissão de chamadas. O *gatekeeper* provê facilidades de encaminhamento de chamadas, bem como serviços suplementares (status de chamada, contabilidade de chamadas, etc). Suas funções incluem:

[4] Existe o *Draft revised Recommendation H.323 V5 (for Consent)* de maio de 2003 disponível em [H323V5] para uso interno aos membros do ITU-T.

a) Tradução de endereços - Permite o uso de esquemas proprietários de endereçamento local (chamados de *alias*), tais como mnemônicos, *nicknames* (apelidos), endereços de e-mail. Traduz estes para endereços IPs.

b) Controle de admissão - Controla a configuração de chamadas de telefonia IP entre terminais e *gateways* que estão sob sua responsabilidade e os que estão fora da sua zona. Acessos podem ser liberados ou negados baseados em autenticação, endereços origem e destino, hora do dia ou qualquer outra variável conhecida pelo *gatekeeper*, executando um papel de segurança.

c) Gerenciamento de banda - Requisita que os terminais ou *gateways* H.323 modifiquem parâmetros de comunicação das chamadas de modo a gerenciar a banda que pode estar sendo compartilhada por sessões múltiplas, promovendo um uso mais eficiente e coordenado da banda passante.

d) Gerenciamento de zona - Coordena funções em dispositivos sobre sua guarda, como por exemplo em uma zona que requer que no máximo 25 chamadas sejam permitidas em um enlace de pouca banda para evitar degradação de qualidade.

e) Sinalização de Chamada - Atua como "*proxy*" de sinalização de chamada para os terminais ou mesmo *gateways* que representa, tendo a responsabilidade do suporte do protocolo de controle de chamada. Pode servir simplesmente como ponto de contato inicial para as chamadas. Após admitir uma chamada proposta, os dois *gateways* ou terminais são conectados para trocarem sinalização diretamente.

Utilizando *gatekeeper* são possíveis dois modelos diferentes de chamadas no H.323. No primeiro modelo os dois pontos terminais comunicam-se diretamente (modelo de chamada direta). No segundo modelo, o *gatekeeper* tem o controle da chamada (modelo de chamada roteado pelo *gatekeeper*), permitindo atuar como um controlador multiponto, registrar as chamadas e fornecer serviços de valor agregado [TOGA]. O *gatekeeper* não é um elemento obrigatório em uma chamada H.323. No caso de ausência deste, é preciso prover outro mecanismo de resolução e transporte de endereços.

- *Proxy* - Atuam em nome de um elemento H.323 para contatar outro elemento da arquitetura.

As mensagens trocadas entre entidades H.323 são especificadas pelas recomendações ITU H.225.0 e H.245. O H.225.0 é um protocolo composto por dois módulos, sendo uma parte variante da recomendação Q.931 da ITU-T, usada para estabelecer e encerrar conexões entre pontos terminais H.323. Este tipo de sinalização é conhecido como sinalização de chamada ou sinalização Q.931. O outro módulo H.225.0 é conhecido como sinalização RAS (*Registration, Admission and Status*), que é usada entre pontos terminais e *gatekeepers* habilitando um *gatekeeper* a gerenciar os pontos terminais em sua zona. O protocolo H.245 é um protocolo de controle de mídia que será detalhado mais adiante.

A sinalização de chamada passa por cinco fases [GORALSKY]:

- Estabelecimento de chamada - Nesta fase, o ponto terminal chamador notifica o ponto terminal chamado da intenção de abrir um canal de áudio (e possivelmente vídeo ou outra mídia). A fase de inicialização define também uma mensagem com o propósito de informar o chamador que o ponto terminal chamado foi alertado de uma chamada. A seqüência exata de sinalização de chamada varia dependendo da configuração de rede, em particular da presença e localização de um ou mais *gatekeepers* no relacionamento de sinalização. Em todos os casos, entretanto, o ponto terminal chamador inicializa a conexão com uma mensagem de inicialização. O ponto terminal chamado responde com uma mensagem *connect* contendo o endereço IP do canal de controle H.245 com a finalidade de configurar o canal de mídia com mensagens H.245;

- Comunicação inicial e troca de capacidades - Após completar com sucesso a fase de estabelecimento de chamada, ambos pontos terminais prosseguem para o estabelecimento do canal de controle H.245 através da troca de informações relacionadas a capacidade de cada um dos pontos terminais na chamada. A capacidade refere-se aos tipos de canais de mídia suportados. Por exemplo, todos os *gateways* H.323 devem suportar canais de áudio, mas muitos não suportam canais de vídeo ou *white-boarding*[5] definidos no H.323;

- Estabelecimento de comunicação audiovisual - Neste ponto, os pontos terminais são livres para estabelecer os canais lógicos que irão transportar o fluxo de informação da chamada. Para informação de áudio, cada ponto terminal de conversação abre seu próprio canal unidirecional. Não há requisitos de que o mesmo codificador ou a mesma taxa de transmissão sejam usados em ambas direções.

- Serviços de chamada - Nesta fase, são realizadas alterações dos parâmetros da chamada negociada durante as três fases anteriores. Podem incluir ajustes na banda requerida pela chamada, a adição ou retirada de participantes durante uma conferência, ou a troca do status ou mensagens de "*keepalive*" entre os *gateways* e/ou terminais;

- Terminação de chamada - O dispositivo que deseja terminar uma chamada H.323 necessita simplesmente descontinuar a transmissão de fluxo de informação (primeiro vídeo, depois dados e então áudio, se elementos além de áudio estiverem presentes) e então enviar uma troca de mensagem de terminação de chamada similar ao estabelecimento de chamada usada no início da chamada. Assim como no estabelecimento de chamada, o procedimento de terminação de chamada varia dependendo do papel desempenhado pelo *gatekeeper* na chamada. Quando o *gatekeeper* está presente, ele deve ser notificado da terminação da chamada e assim ajustar a tabela de banda disponível. As mensagens de RAS's e as de sinalização de chamada estão descritas no apêndice.

[5] É uma funcionalidade que permite a escrita ou desenho sobre imagens compartilhadas entre os participantes de uma chamada.

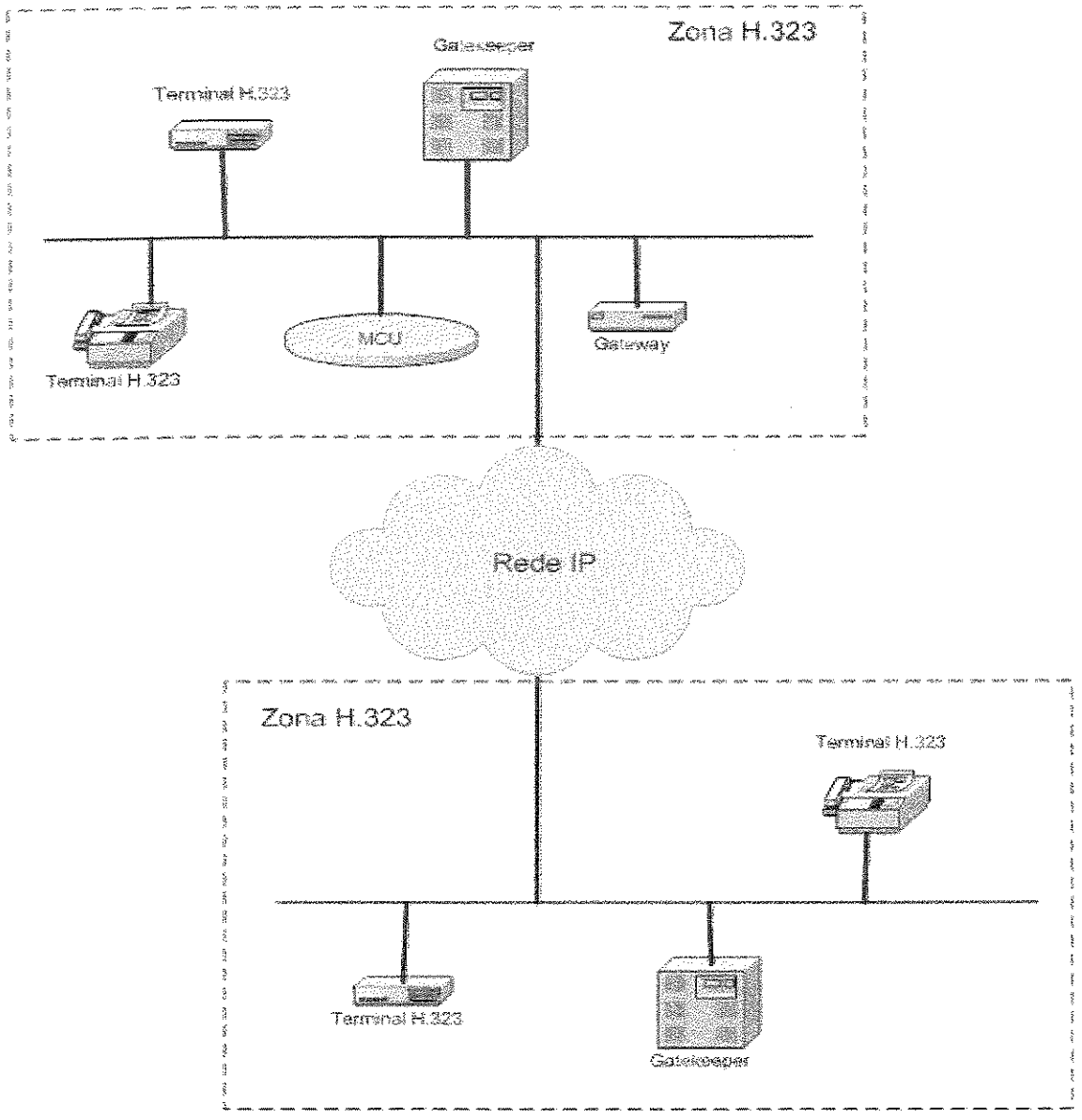

Figura 7 Zonas H.323

2.2.1 O protocolo H.245

O H.245 é o protocolo de controle de mídia que o H.323 usa após o estabelecimento da chamada. É usado para negociar e estabelecer os canais de mídia transportados pelos protocolos RTP e RTPC [RFC1889] [RFC1890]. O protocolo H.245 forma uma base comum para controle de mídia e de conferência para um número de sistemas de comunicação multimídia do ITU-T, sendo que este possui mensagens e procedimentos outros não utilizados no H.323, bem como algumas extensões exclusivas para o H.323. As funcionalidades oferecidas pelo protocolo H.245, que são usadas no H.323, podem ser classificadas em quatro categorias, das quais as três primeiras são mandatórias para operação H.323:

- Determinação mestre-escravo - Em qualquer conferência um ponto terminal tem que assumir a função de mestre e um outro de escravo. A determinação de quem é o mestre envolve duas informações de cada entidade. A primeira informação é o valor do tipo de terminal e o segundo é um número randômico gerado entre um e 16.777.125. Um mestre é criado após comparar os valores de tipo de terminal, que indica a capacidade de tratamento de mídia (áudio, vídeo, dados). O ponto terminal que tem o maior valor de tipo de terminal, ou seja, maior capacidade de tratamento de mídia, é automaticamente o mestre. Caso os valores de tipo de terminal sejam iguais, então é feita a determinação mestre-escravo pelo número randômico gerado associado ao terminal;

- Troca de capacidade - Habilita os pontos terminais a compartilhar informações relativas a capacidade de transmissão e recepção. É usado pelos elementos H.323 para negociar o conjunto comum de capacidades operacionais. O conjunto de capacidade descreve todos os aspectos de operação entre os elementos de comunicação: tipo de mídia, número de canais simultâneos, *bit rate* máximo, e outras opções. Este processo pode ocorrer a qualquer momento durante uma chamada, permitindo a renegociação de características de operação (utilização de banda ou mudança de carga de processamento);

- Controle de canal de mídia - Após informações de capacidades terem sido trocadas, os pontos terminais podem abrir e fechar canais lógicos de mídia. Canais lógicos são identificadores usados no H.245 para identificar unidirecionalmente um fluxo de mídia. O controle de fluxo, vazão e mudanças de modos de operação da mesma maneira que outras mensagens sempre referenciam um canal lógico. O transmissor de mídia é limitado a abrir canais lógicos no seu conjunto de capacidades de recepção. Qualquer fluxo de áudio é um canal unidirecional. Isto significa que cada transmissor necessita abrir um canal para o(s) receptor(es) permitindo implicitamente o uso de codificadores de forma assimétrica e diferentes tipos de fluxos de mídia em cada direção;

- Controle de conferência - Fornece aos pontos terminais ciência em conferências múltiplas. Determina o conjunto de capacidades adequadas para uma conferência. Estabelece o modelo entre todos os pontos terminais. O controle de conferência também provê funções administrativas tais como controle de assentos.

O H.323 utiliza o protocolo H.245 para sinalização de canal lógico para controle de mídia e a funcionalidade de sinalização de chamada do protocolo H.225.0 sobre a camada TCP. Sobre a camada UDP é utilizada a funcionalidade de sinalização do terminal H.323 com o *gatekeeper* (RAS). Também sobre a camada UDP estão os protocolos RTP e RTCP, que serão descritos na seção 3.1, para transporte de áudio digitalizado por um dos codificadores de voz disponíveis. A Figura 8 ilustra a pilha de protocolos do H.323 para telefonia IP.

<table>
<tr><td colspan="2">Áudio
Codificadores</td><td colspan="3">Controle</td></tr>
<tr><td colspan="2">G.711
G.722
G.723
G.728
G.729</td><td rowspan="2">H.225.0
Sinalização
Terminal
para
Gatekeeper
(RAS)</td><td rowspan="2">H.225.0

Sinalização
de
Chamada</td><td rowspan="2">H.245

Sinalização
de Canal
Lógico</td></tr>
<tr><td>RTP</td><td>RTCP</td></tr>
<tr><td colspan="3">UDP
transporte não confiável</td><td colspan="2">TCP
transporte confiável</td></tr>
</table>

Figura 8 Pilha de protocolos H.323 para telefonia IP

2.3 Protocolo MGCP (Media Gateway Control Protocol)

O *Media Gateway Control Protocol* (MGCP) é um protocolo para controlar *gateways* de telefonia a partir de elementos de controle de chamadas externos, chamados de controladores de *gateway* de mídia ou agentes de chamada. É um protocolo "sem estado", ou seja, não armazena nenhum histórico das transações prévias entre *gateways* de mídia, também denominados *gateway* de voz, e o controlador de *gateway* de mídia

O protocolo é especificado na RFC 3435[6] [RFC3435] entitulada "*Media Gateway Control Protocol (MGCP) Version 1.0*" de Janeiro de 2003, que substitui a RFC 2705 [2705]. É baseado no SGCP (*Simple Gateway Control Protocol*) versão 1.1 como extensão do projeto NCS (*Network-based Call Signalling Protocol Standard*) da CableLabs e no IPDC (*Internet Protocol Device Control*) versão 1.0.

Um *gateway* de mídia de telefonia é um elemento de rede que fornece a conversão entre sinais de áudio transportados nos circuitos telefônicos em pacotes de rede de dados e vice-versa.

[6] Este trabalho foi feito baseando-se na RFC2705. A RFC3435 faz algumas correções, esclarecimentos e novos detalhamentos tais como permitir IPv6 nos pontos de terminação e acréscimo de novos códigos de retorno.

Como exemplos de *gateways* pode-se citar:

- *Trunking gateways*: interfaceiam entre a rede de telefonia e a rede de voz sobre IP;
- *Voice over ATM gateways*: operam da mesma maneira que os *gateways* de voz sobre IP só que para ATM;
- *Residential gateways*: interfaceiam com os conectores analógicos tradicionais RJ11 para redes de voz sobre IP (aparelhos xDSL, *cable modems*, etc) para assinantes residenciais. A Figura 9 exemplifica uma chamada MGCP entre dois *gateways* residenciais;
- *Access gateways*: operam com os conectores analógicos tradicionais RJ11 ou interface digital PBX para redes de voz sobre IP. São *gateways* de pequena escala;
- *Business gateways*: interfaceiam com os tradicionais PBX digitais ou uma interface "*soft* PBX" integrando com a rede de voz sobre IP.

O protocolo MGCP tem um modelo de conexão no qual os elementos básicos são os pontos terminais e as conexões. Os pontos terminais são origem ou destinos de dados e podem ser virtuais ou fisicos.

Exemplos de pontos terminais fisicos:

- Uma interface em um *gateway* que termina um tronco conectado a uma Rede Pública de Telefonia Comutada (RPTC). Esses tipos de *gateways* são chamados *trunk gateways*;
- Uma interface de *gateway* que termina em uma linha de conexão analógica de um telefone residencial é chamado de *residential gateway*.

Um exemplo de ponto terminal virtual é uma fonte de áudio em um servidor de conteúdo de áudio. A criação de pontos terminais fisicos requerem instalação de hardware, enquanto a criação de pontos terminais virtuais pode ser feita por software. As conexões podem ser ponto-a-ponto ou multiponto. Uma conexão ponto-a-ponto é aquela associação entre dois pontos terminais para a transmissão de dados entre eles. Uma conexão multiponto é aquela estabelecida entre um ponto terminal com uma sessão ponto-a-ponto, tendo, portanto, mais de dois participantes. Conexões podem ser estabelecidas em diversos tipos de rede:

- Transmissão de pacotes de áudio usando RTP e UDP em uma rede TCP/IP;
- Transmissão de pacotes de áudio usando AAL2 ou outra camada de adaptação sobre redes ATM;
- Transmissão de pacotes sobre uma conexão interna, por exemplo, um *backplane* TDM ou uma interconexão de um barramento interno de um *gateway*.

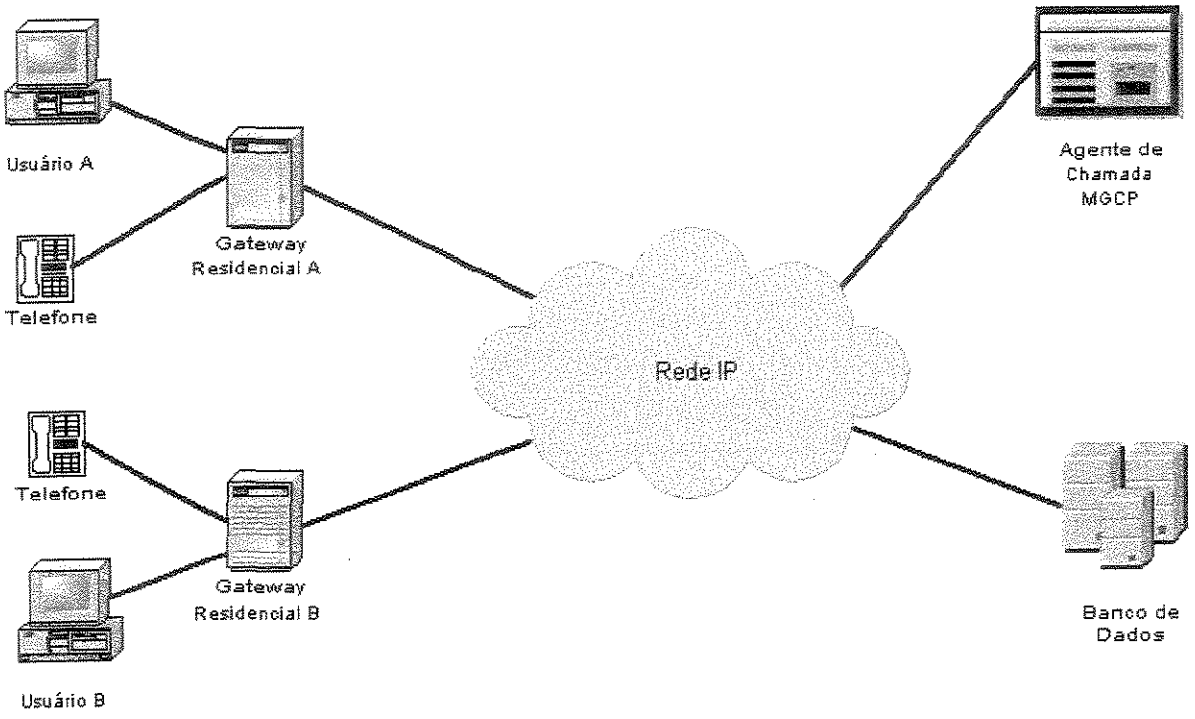

Figura 9 Chamada MGCP entre dois RGWs

Para conexões ponto-a-ponto os pontos terminais podem estar no mesmo *gateway* ou em *gateways* distintos.

As comunicações entre agentes de chamada não são realizadas com o protocolo MGCP [COLLINS]. Quando dois pontos de terminação estão localizados em *gateways* de mídia gerenciados por diferentes agentes de chamadas, os agentes de chamadas trocam informações entre si utilizando um protocolo de sinalização, como por exemplo o SIP, para sincronização da criação de conexão entre os pontos de terminação.

Em [VOVIDA] existe uma biblioteca com código fonte aberto para a pilha de protocolo MGCP versão 1.0 de Outubro de 1999, que pode ser usado tanto para o agente de chamada (*Media Gateway Controller*) ou para aplicação do *gateway* de mídia que precisa enviar e receber mensagens sobre a rede.

A seguir são descritos a arquitetura e os comandos de MGCP.

2.3.1 Arquitetura

O MGCP assume a arquitetura de controle de chamada, na qual a inteligência deste controle está fora dos *gateways* e são controlados por elementos externos, chamados de agentes de chamada ou controladores de *gateway* de mídia (MGC - *Media Gateway Controller*). É um protocolo do tipo mestre/escravo, onde os *gateways* de mídia devem executar os comandos enviados pelos agentes de chamada. A sincronização entre os agentes de chamada não é realizada pelo MGCP, devendo os agentes de chamada se sincronizarem de modo a enviar comandos coerentes para os *gateways* subordinados.

2.3.2 Comandos MGCP

O protocolo MGCP executa suas funções em seqüências de comandos. O controlador de *gateway* de mídia é responsável pelo envio de comandos MGCP para os pontos terminais e pelo recebimento dos reconhecimentos (ACK) para cada comando. Os comandos e as respostas são em formato texto. O MGCP possui oito tipos de comandos que contém um verbo que indica a ação a ser executada com parâmetros adicionais:

- *CreateConnection* (CRCX) - Mensagem do agente de chamada para o *gateway* de mídia usada para criar a conexão entre dois pontos terminais;

- *ModifyConnection* (MDCX) - Mensagem do agente de chamada para o *gateway* de mídia usada para modificar características de uma conexão em curso;

- *DeleteConnection* (DLCX) - Mensagem do agente de chamada para o *gateway* de mídia ou vice-versa. É usada para remover conexões, sendo que múltiplas sessões podem ser apagadas simultaneamente usando estruturas hierárquicas avançadas de nomes e ou caracteres como o "*" (coringa). Em encerramentos de conexões o *gateway* de mídia envia para o agente de chamada parâmetros cujos valores indicam a qualidade da conexão que são:

  a) *Packet Sent* (PS): Total de pacotes (RTP) enviados;
  b) *Octects Sent* (OS): Total de octetos (número de *payloads*) enviados;
  c) *Packets Received* (PR): Total de pacotes (RTP) recebidos;
  d) *Octets Received* (OR): Total de octetos recebidos;
  e) *Packets Lost* (PL): Total de pacotes perdidos. São indicados por "buracos" na seqüência de pacotes;
  f) *Jitter* (JI): Um inteiro expressando a média dos *jitters*;
  g) *Latency* (LA): Um inteiro representando o atraso médio em milisegundos.

- *NotificationRequest* (RQNT) - Mensagem do agente de chamada para o *gateway* de mídia usada para solicitar ao *gateway* a notificação de determinados eventos em um ponto terminal;

- *Notify* (NTFY) - Mensagem do agente de chamada para o *gateway* de mídia usada para notificação de eventos;

- *AuditEndPoint* (AUEP) - Mensagem do agente de chamada para o *gateway* de mídia usada para verificar o status de um determinado ponto terminal;

- *AuditConnextion* (AUCX) - Mensagem do agente de chamada para o *gateway* de mídia que permite o agente de chamada verificar parâmetros associados a uma conexão;

- *ReStartInProgress* (RSIP) - Mensagem do *gateway* de mídia para o agente de chamada que sinaliza que um ponto terminal ou grupo de pontos terminais entrou ou saiu de serviço. Possui três opções:

  a) *Graceful* - sem nenhuma conexão perdida;
  b) *Forced* - conexão(ões) perdida(s);
  c) *Restart* - o *gateway* reiniciará em breve.

Todos os comandos e respostas MGCP tem um cabeçalho, contendo parâmetros que estão descritos no apêndice. Os comandos do MGCP exigem um reconhecimento, sendo que este retorna um código com o status do comando. Os códigos de resultados são gerados pelo *gateway* quando está sendo removida uma conexão a fim de informar o agente de chamada sobre o motivo do encerramento da conexão, ou para ser usado no comando *RestatInProgress* para informar o *gateway* do motivo da reinicialização *(restart)*.

A relação de código de mensagem de resposta e sua descrição, bem como as mensagens dos códigos de resultado estão no apêndice.

2.4 Protocolo Megaco/H.248

Protocolo H.248, também conhecido como protocolo Megaco, é um padrão criado para permitir o agente de chamada controlar *gateways* de mídia, representando a união de esforços entre o ITU (ITU-T Recomendação H.248) e o IETF (*Megaco Protocol Version* 1.0 - RFC3015 [RFC3015][7]). O Megaco/H.248 atende os requisitos para protocolo de controle de *gateway* de mídia como especificado na RFC 2805 "*Media Gateway Control Protocol Architecture and Requirements*" [RFC2805]. Esse esforço cooperativo visa a definição de um protocolo de sinalização comum para as redes de voz sobre IP de próxima geração [HERSENT].

O Megaco/H.248 oferece a possibilidade tanto de sinalização binária quanto textual e recomenda que os agentes de chamada, também denominados *softswitches*, implementem ambos tipos [DOUSKALIS1]. A versão textual é escrita usando *Augmented Backus-Naur Form* (ABNF), da RFC 2234 [RFC2234], enquanto a versão binária é escrita usando *Abstract Syntax Notation One* (ASN.1), descrito no ITU-T Rec X.680, 1997.

---

[7] Em Junho de 2003 foi disponibilizada a RFC 3525 entitulada "*Gateway Control Protocol Version 1* " [RFC3525] contendo algumas modificações e esclarecimentos sobre o texto da RFC 3015 que tornou-se obsoleto. Este trabalho é baseado na RFC 3015.

O Megaco/H.248 pode ser usado sobre o protocolo de transporte TCP ou sobre o UDP. A versão binária possui porta *default* 2945 e a versão textual tem porta *default* 2944.

Há vários pontos em comum entre MGCP e o Megaco/H.248, tais como: ambos operam em modo mestre-escravo, modo de requisição e resposta, e na codificação de eventos e sinais [DOUSKALIS1].

A seguir serão descritos a arquitetura e os comandos do Megaco/H.248.

2.4.1 Arquitetura

O protocolo Megaco/H.248 é considerado um protocolo complementar ao H.323 e ao SIP, uma vez que um agente de chamada controla os *gateways* de mídia utilizando Megaco/H.248, podendo comunicar-se entre si via H.323 ou SIP.

É necessário definir algumas das terminologias usadas em Megaco/H.248.

Terminação é uma entidade lógica dentro de um *gateway* de mídia que é capaz de originar e receber fluxos multimídia, de modo similar aos pontos terminais do MGCP. O contexto é considerado como a associação lógica entre as terminações. Por exemplo, todas as terminações que estão participando de uma conferência constituem um contexto simples.

O contexto é uma abstração de nível mais alto que as conexões no MGCP.

Comandos entre o agente de chamada e o *gateway* de mídia são agrupados em transações que recebem um identificador único de transação (*TransactionID*). As transações consistem de uma ou mais ações, que por sua vez consistem de uma série de comandos que são limitados a um contexto, sendo que tipicamente cada ação especifica um contexto, representado por identificador único de contexto (*ContextID*).

As transações garantem o processamento ordenado dos comandos, ou seja, são executados seqüencialmente. Na primeira falha de um comando em uma transação, os demais comandos da transação não são executados. A ordem de execução das transações não é garantida, pois podem ser executadas em qualquer ordem inclusive simultaneamente.

Uma transação é composta por:

- *TransactionRequest* - Solicitação de transação contendo uma ou mais ações, cada qual especificando o contexto alvo e um ou mais comandos por contexto. Ele é invocado pelo emissor, sendo que para cada requisição existe um *TransactionRequest*. Cada transação tem um identificador para correlação com a resposta do *TransactionReply* ou *TransactionPending* do receptor;

- *TransactionReply* - Resposta de solicitação de transação que é invocada pelo receptor. Há somente uma invocação de resposta por transação. Uma resposta contém uma ou

mais ações. Cada qual especificando o contexto alvo e uma ou mais respostas por contexto. O identificador de transação deve ser o mesmo usado no correspondente *TransactionRequest*. Cada parâmetro de resposta representa um valor de retorno ou uma descrição de erro;

- *TransactionPending* - Indica que uma transação está sendo processada, mas ainda não terminou. É usado para prevenir que o emissor presuma que um *TransactionRequest* foi perdido enquanto na realidade ele demanda mais tempo para completar que o intervalo normal da transação.

Múltiplas transações podem ser concatenadas dentro de uma mesma mensagem. As transações dentro de uma mesma mensagem são tratadas independentemente não havendo ordem implícita de execução.

A Figura 10 ilustra a terminologia adotada [RFC3015].

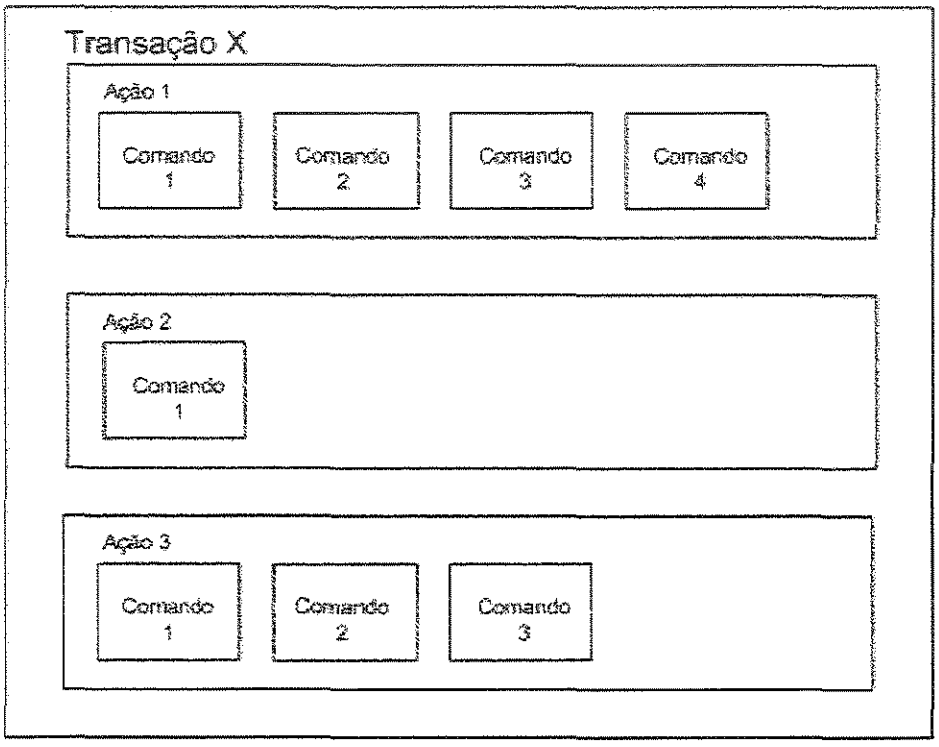

Figura 10 Terminologia Megaco/H.248

Quando um *gateway* de mídia relata um erro para um agente de chamada, isto é feito através de um descritor de erro. Um descritor de erro consiste de um código de erro e opcionalmente um texto associado. Os códigos de erro são apresentados no apêndice sobre o Megaco/H.248.

Na subseção seguinte serão apresentados os comandos do Megaco/H.248.

2.4.2 Comandos Megaco/H.248

O Megaco/H.248 define oito comandos para controlar e manipular contextos e terminações. Os comandos são:

- *Add* - Adiciona uma terminação para um contexto existente ou novo. Atua de maneira similar ao comando *CreateConnection* no MGCP;

- *Modify* - Modifica propriedades e eventos de uma terminação. Este comando é similar ao comando *ModifyConnection* no MGCP;

- *Subtract* - Remove a terminação de um contexto. Atua de maneira similar ao comando *DeleteConnection* do MGCP. A terminação então retorna a estatística (podem ser quantidade de pacotes enviados, pacotes recebidos, *jitter*, etc) de sua participação no contexto. O comando *Subtract* usado na última terminação remove o contexto;

- *Move* - Move a terminação referenciada para um outro contexto. Atua de maneira similar ao comando *ModifyConnection* do MGCP no qual um ponto de terminação pode ser movimentado para outra conexão;

- *AuditValue* - Retorna o status atual de propriedades, eventos, sinais e estatística de uma ou mais terminações referenciadas;

- *AuditCapabilities* - Retorna todos os possíveis valores para propriedades de eventos e sinais associados com uma ou mais terminações, diferentemente do comando *AuditValue* que retorna os valores em uso. O uso conjunto do comando *AuditValue* com o comando *AuditCapabilities* obtém as mesmas informações do comando *AuditEndPoint* do MGCP;

- *Notify* - Informa o agente de chamada da ocorrência de eventos solicitados no *gateway* de mídia. Tem a mesma função que o comando de *Notify* do MGCP;

- *ServiceChange* - O *gateway* de mídia notifica a um agente de chamada que a terminação ou grupo de terminação estão fora de serviço ou estão retornando para "em serviço". O agente de chamada pode sinalizar ao *gateway* de mídia que um outro agente de chamada estará com o controle da sinalização, enviando o comando *ServiceChange* para o *gateway* de mídia. Similar ao comando *ReStartInProgress* do MGCP, quando enviado pelo *gateway* de mídia;

- *Reply* - É a resposta enviada pelo receptor de mensagem Megaco/H.248. A resposta pode ser final ou provisória. Respostas provisórias indicam que a mensagem foi recebida, está sintaticamente correta, e está sendo processada. Uma resposta mais atual ao comando será provida assim que for conhecida.

O protocolo Megaco/H.248 define um número de descritores que estão disponíveis para uso com comandos e respostas. Estes descritores formam os parâmetros de um

comando e/ou resposta e fornecem informações adicionais para qualificar um dado comando ou resposta.

Um determinado descritor pode ser opcional, obrigatório ou proibido, dependendo do comando ou resposta. Os parâmetros de um descritor podem ser [COLLINS] [RFC3015]:

- *Under specified*: envolve o uso de "*any*" ou o caracter "$", habilitando o receptor do comando para selecionar qualquer valor que ele possa suportar;
- *Over specified*: o emissor do comando fornece uma lista de parâmetros que podem ser aceitos ordenados por preferência. O receptor do comando seleciona uma das escolhas oferecidas para uso, e a resposta do comando indicará a escolha feita.;
- *Fully specified*: o parâmetro é assinalado de maneira explícita de maneira que o receptor do comando deva usar esse parâmetro.

Em geral o formato texto de um descritor é:

NomeDoDescritor=<Identificador>{param=valor, param=valor...}

A relação de descritores está no Apêndice.

Para descrever as características dos tipos de terminações (por exemplo: terminação conectada a um tronco digital e terminação conectada a uma linha analógica), o Megaco/H.248 incorpora o conceito de "*packages*", que são grupos de propriedades, sinais, eventos, procedimentos e estatísticas. Uma determinada terminação implementa uma lista de "*packages*" deste modo descrevendo suas características. Em [RFC3015] é feito uma orientação para a especificação de novos "*packages*" e que podem ser registrados no IANA (*Internet Assigned Numbers Authority*) [IANA] por razões de interoperabilidade.

2.5 Uma comparação entre protocolos de telefonia IP

Nesta seção é feita a comparação entre os protocolos MGCP e Megaco/H.248 que são protocolos de controle de *gateways* de mídia. A comparação entre MGCP e Megaco/H.248 enfoca entre outros itens a arquitetura, os comandos, o tipo de codificação usada, os tipos de respostas e a terminologia. A outra comparação realizada é entre os protocolos SIP e H.323, que são protocolos de sinalização de chamada, sendo complementares ao MGCP e Megaco/H.248 [WANG].

2.5.1 Comparação entre os protocolos MGCP e Megaco/H.248

Na arquitetura *softswitch*, na qual ocorre a separação das funções de conversão e transporte de mídia (*gateways* de mídia) das funções de controle e sinalização de chamadas (agentes de chamada), tanto o Megaco/H.248 como o MGCP são protocolos de interfaceamento entre agentes de chamadas também denominados *Media Gateway Controllers* (MGC's) e os *gateways* de mídia que fazem a conversão de mídia.

Ambos os protocolos, trabalham na arquitetura de modelo centralizado, onde a inteligência da rede ficam com os agentes de chamadas.

O protocolo Megaco/H.248 é derivado do MGCP, e possui arquitetura e comandos similares ao MGCP, sendo resultado do esforço colaborativo entre as organizações de padronização IETF e ITU.

Estudos sobre o MGCP tem sido conduzidos pela PacketCable™ [PACKETCABLE] e o Softswitch Consortium™ [SOFTSWITCH]. Não há nenhum envolvimento na especificação de nenhum organismo internacional de padronização, diferentemente do Megaco/H.248.

Apesar da precedência do MGCP, o Megaco/H.248 tende a ser amplamente adotado pelas indústrias como padrão definido pela ITU e IETF.

O Megaco/H.248 oferece uma série de evoluções em relação ao MGCP [RADVISION] tais como:

- Suporta serviços multimídia e conferência multiponto aprimorados;
- Sintaxe melhorada para processamento mais eficiente da semântica das mensagens;
- Opções de transporte UDP e TCP;
- Permite codificação textual ou binária;
- Formalização do processo para extensão para incremento de funcionalidades;
- Definição expandida de *packages*.

A principal diferença entre as duas implementações é que com Megaco/H.248 os comandos aplicam-se as terminações relativas a um contexto, ao invés de conexões individuais, no caso do MGCP.

Conexões são feitas com duas ou mais terminações em um contexto comum. Este conceito de contexto facilita o suporte para multimídia e chamadas em conferência. O contexto pode ser visto como uma ponte para suportar múltiplos fluxos de mídia para serviços multimídia.

Tanto no Megaco/H.248 como no MGCP o mecanismo primário para extensão é através de *packages*, sendo que existem regras para definição de novos pacotes para permitir a expansão de funcionalidade. Os *packages* Megaco/H.248 são mais abrangentes, definem propriedades e estatísticas além das informações de evento e sinal que podem ocorrer nas terminações.

Ambos protocolos usam o SDP, que é textual, para descrever formalmente parâmetros. Protocolos baseados em texto simplificam a pilha de protocolo e parte da implementação, da depuração, etc, retirando dependências de códigos específicos de máquinas (exemplo: notação *big* ou *little endian*).

Ambos protocolos não foram projetados para suportar multimídia da mesma maneira que os protocolos H.323 e SIP e não tem precedência de erros nos códigos de

erros, sendo que somente um único código de erro é retornado por transação, fazendo com que em casos de múltiplas condições de erro, somente uma possa ser relatada, levando a necessidade de usar outros mecanismos para melhor caracterizar o problema.

Na Tabela 1 compara-se resumidamente o MGCP e o Megaco/H.248.

	MGCP	**Megaco/H.248**
Origem	IETF	IETF/ITU-T
Versão atual[8]	RFC3435 (01/2003)	RFC3525 (06/2003)
Arquitetura	Centralizada	Centralizada
Pontos de terminação	*Gateway* de mídia	*Gateway* de mídia
Controle de chamada	Agente de Chamada	Agente de chamada
Transporte de *fax-relay*	T.38[9] [ITUT38]	T.38
Terminologia	Pontos terminais, Conexões	Terminações, Contexto
Provedor de serviços suplementares	Agente de chamada	Agente de chamada
Transação	Um Comando	N Ações Cada Ação = N Comandos
Protocolo de descrição de chamada	SDP	SDP
Software livre	[VOVIDA]	Não
Transporte de voz	RTP/RTCP	RTP/RTCP
Transporte de sinalização	UDP	TCP ou UDP
Tipo de resposta	Um	Dois (*TransactionReply* e *TransactionPending*)
Suporte a multimídia	Sim	Sim
Codificação	Texto (BNF)	Texto (ABNF) e Formato Binário (ASN.1)

Tabela 1 Comparação entre MGCP e Megaco/H.248

2.5.2 Comparação entre os protocolos SIP e H.323

O protocolo H.323 foi inicialmente concebido para ser usado em redes locais e não em redes de longa distância como o protocolo SIP [WANG].

Nas versões mais recentes foi introduzido o conceito de zona, que é uma coleção de todos os terminais, *gateways* e MCUs gerenciados por um *gatekeeper*. Foram também definidos procedimentos para localização de usuários entre zonas.

Para um grande número de domínios e para processos de localização complexos, o H.323 apresenta ainda problemas de escalabilidade como, por exemplo, a adequada

[8] Este trabalho foi baseado na RFC 3015 do Megaco/H.248 e na RFC 2705 para o MGCP.
[9] Recomendação T.38: Permite a transmissão de fax em tempo real através de *gateways* sobre uma rede IP. A recomendação [ITUT37] também trata de transmissão de fax "*store-and-forward*" em Internet.

detecção de laços de *loop*. Por outro lado, o SIP foi concebido para WAN, sendo que a detecção de *loop*[10] é implementada. O mecanismo de endereçamento e de localização de usuários foi projetado para uso na Internet, uma das grandes vantagens do SIP sobre o H.323 [WANG], sendo que o tamanho da rede não é um limitante [BEIJAR].

A arquitetura de ambos os protocolos é distribuída, ou seja, a inteligência da rede é distribuída entre os pontos de terminação e os dispositivos de controle de chamada. Também é possível criar redes SIP de maneira centralizadas utilizando *back-to-back user agents* (B2BUAs) [B2BUA] e redes H.323 centralizadas utilizando o modelo de chamada roteado pelo *gatekeeper* [PACKETVOICE].

Nas versões iniciais do H.323 o tempo mínimo para estabelecimento de chamada era alto e questionado. Atualmente tempo mínimo de fazer a configuração de chamada é o mesmo para ambos 1,5 *round trips* [H323XSIP1].

No H.323 é possível o balanceamento de carga com o *gatekeeper* e tratamento de falhas em elementos da rede enquanto o SIP não oferece essas facilidades [H323XSIP1].

A depuração do SIP é simples uma vez que a sinalização é baseada em textos como no MGCP, Megaco/H.248 e HTML. Nenhum esforço ou tempo adicional é necessário para atualizar a depuração. Já a depuração do H.323 exige ferramentas especializadas que necessitam ser adaptadas quando existem mudanças em algum item [H323XSIP]. Por outro lado, no SIP as mensagens são maiores, por serem textuais, ocupando mais banda [H323XSIP1].

Na questão de tarifação, ambos tem mecanismos para registrar as chamadas realizadas. No entanto, no SIP as chamadas devem necessariamente passar através do *proxy*, enquanto que no H.323 o ponto terminal informa o início e o fim da chamada para o *gatekeeper* através do protocolo RAS, sem necessidade de passar através do *gatekeeper* [H323XSIP1].

No protocolo H.323 cada codificador usado tem que ser previamente registrado e padronizado antes que possam ser usado pelas aplicações H.323. Atualmente somente codificadores desenvolvidos pelo ITU são registrados. No SIP os codificadores suportados por um ponto terminal são listados usando *Session Description Protocol* (SDP) durante a fase de estabelecimento de conexão. Os codificadores são estabelecidos por *strings*, que não limitam os codificadores para um intervalo de valores de códigos pré-definidos [BEIJAR].

Para definição de serviços o protocolo H.323 utiliza uma abordagem clara e bem definida, orientada a objetos, onde os serviços suplementares tem definido sua própria máquina de estados, independente da máquina de estados da chamada base. Aproveita a experiência do ITU na área de telecomunicações, reaproveitando a definição de serviços suplementares já realizados, podendo ter ciclos de desenvolvimento de produtos menores.

---

[10] Na [RFC3621] a detecção de "*loop*" foi corrigida e melhor detalhada, sendo agora opcional. É mandatório o uso da de um contador "*max-forward*" para um melhor resultado na detecção de "*loops*".

O SIP fornece recomendações de implementações muito básicas. Um serviço suplementar é composto por uma ou mais transações, não sujeitas a padronização do protocolo, ou seja, não é padronizado explicitamente e a semântica fica a cargo da implementação, podendo gerar problemas de interoperabilidade, funcionalidade e interação entre serviços suplementares [GLASSMAN].

A motivação principal do protocolo SIP é criar um ambiente que suporte redes de comunicação de próxima geração utilizando aplicações Internet e a própria Internet, tanto que utiliza outros protocolos da IETF, tais como SDP, URL e DNS, para definir outros aspectos de telefonia IP e multimídia. Suas características estão mais associadas ao modelo de comunicação da Internet que as do protocolo H.323. Em contrapartida, as extensões do SIP para compatibilizar com os serviços do sistema telefônico convencional não estão tão bem definidas como do H.323 [PACKETVOICE].

Embora inicialmente o protocolo H.323 somente funcionasse no modelo *stateful* com uso de *gatekeeper*, na versão mais atual é possível trabalhar também no modelo *stateless* [TOGA]. No SIP as transações funcionam em ambos modelos [SCHULZRINNE3]. No modelo *stateful* todas as informações do estado da chamada devem ser mantidas enquanto a chamada estiver ativa. No modelo *stateless* um servidor recebe a solicitação de chamada, executa operações, encaminha a chamada e descarta as informações.

No protocolo SIP, existe um campo *Priority* no cabeçalho *Request* que prioriza algumas linhas telefônicas. Alguns países fazem exigência legal para priorização de linhas telefônicas. Os valores possíveis para esse campo são: não urgente, normal, urgente, emergência. O protocolo H.323 não tem esse diferencial [HERSENT].

Em [H323XSIP] é recomendado o uso do SIP, mesmo atualmente existando mais implantações de H.323, especialmente em conferências realizadas através de PCs [WANG], devido a sua menor complexidade, fácil interoperabilidade, sua facilidade para criação de novos serviços e para implementação[WEILER] [SCHULZRINNE2].

Para [WANG] o SIP é mais adequado que o H.323 para o uso conjunto com *softswitches*.

Segundo [GLASSMAN], ambos protocolos devem coexistir em diferentes ambientes, com diferentes implementações, gerando uma grande necessidade de interoperabilidade entre eles no futuro.

Concluindo, ambos protocolos estão evoluindo como pode-se constatar em [SIPRFCS] [H323DOCS]. Na evolução[11] estão surgindo novas oportunidades[12] de uso, melhorias e correções de funcionalidades.

Segue a Tabela 2 ilustrando uma comparação entre os protocolos SIP e H.323:

---

[11] Em 12/2002 foi apresentada a RFC 3428 que trata de mensagem instantânea utilizando SIP.

[12] SIP foi escolhido pela *The 3rd Generation Partnership Project* (3GPP) [3GPP] como protocolo de sinalização para redes de sistemas móveis de 3ª geração. A RFC 3455 [RFC3455] é resultado desta escolha

	H323	SIP
Origem	ITU-T	IETF
Versão atual	Versão 4 (11/2002)	RFC3261 (06/2002)
Mensagens	Formato binário	Formato textual
Codificação de mensagens	ASN.1 e SDL	ABNF[13]
Tarifação	Sim.	Sim. Deve usar chamadas com *proxy*
Priorização de linhas telefônicas	Não	Sim
Suporte a multimídia	Sim	Sim
Mecanismo de QoS	Sim	Não
Tratamento de falha na rede	Sim	Não
Protocolo de descrição de chamada	H.245 e H.225.0	SDP
Detecção de *loop*	Sim	Sim
Transporte de voz	RTP/RTCP	RTP/RTCP
Provedor de serviços suplementares	Pontos de terminação e controle de chamada	Pontos de terminação e controle de chamada
Transporte de sinalização	TCP	TCP/UDP
Controle de chamada	*Gatekeeper*	Servidor *proxy* e de redirecionamento
Endereçamento	Flexível aceitando URL´s, dígitos E.164 entre outros	Somente URL´s
Arquitetura	Distribuída ou centralizada	Distribuída ou centralizada
Software livre	[OPENH323]	[VOVIDA] e [LINFONE]
Autenticação/Criptografia	H.325	S/MIME, SSL
Escalabilidade	LAN	WAN
Transporte de *fax-relay*	T.38	T.38
Pontos de terminação	*Gateway*, terminal	Agente usuário

Tabela 2 Comparação entre H.323 e SIP

3 Qualidade de Serviço em Telefonia IP

Qualidade de Serviço (QoS) pode ser definido como "*O efeito coletivo da execução do serviço, que determina o grau de satisfação do usuário do serviço*"[LEPPÄNEN]. Pode-se também definir QoS como *"a habilidade das redes de garantir e manter certo nível de desempenho para cada aplicação de acordo com as necessidades especificadas para cada usuário"* [DOUSKALIS].

O conceito de QoS é geralmente associado aos parâmetros relacionados a qualidade do sinal de voz (*jitter*, retardo de pacotes, banda disponível, perda de pacotes), no entanto,

[13] Inserido na [RFC3621]

outros aspectos fazem parte de seu escopo como segurança (privacidade, integridade, autenticidade, não repúdio), disponibilidade/confiabilidade da rede e perda de informações devido a falhas na rede [DOUSKALIS].

O QoS para telefonia IP visa oferecer mecanismos para obter principalmente a qualidade de voz em tempo real. Para isso é importante conhecermos os fatores que afetam a qualidade de serviço, como é feito o transporte da voz em rede de dados, mecanismo de aferição de qualidade de voz e mecanismos de qualidade de serviço.

Como alguns mecanismos para QoS citamos *Multi-Protocol Label Switching* (MPLS) [RFC2702], *Resource Reservation Protocol* (RSVP) [RFC2205], controle de enfileiramento, priorização e congestionamento de pacotes.

Detalhes e outros mecanismos de QoS podem ser encontrados em [QOSSBRC], [QOSCISCO], [CONGCISCO] e [MAGALHAESECARDOZO].

Esta seção está dividida da seguinte maneira: na Subseção 3.1 são apresentados os parâmetros de Qualidade de Serviço; na Subseção, na Subseção 3.2 é abordado o protocolo RTP/RTPC usado para transporte de voz sobre IP, que procura atenuar os efeitos de *jitter* e provê parâmetros da qualidade de transmissão; na Subseção 3.3 é abordada a qualidade de voz para telefonia.

3.1 Parâmetros de Qualidade de Serviço

A qualidade de voz da rede telefônica tem um caráter subjetivo, dependendo de vários parâmetros, englobando a questão da fidelidade da reprodução de uma fala e sua inteligibilidade [DOUSKALIS]. O retardo tem um papel fundamental na qualidade da voz.

O atraso fim-a-fim, (Figura 11) definido pela diferença de tempo entre o momento do envio do primeiro *bit* de um pacote de um terminal emissor e o momento em que o terminal receptor recebe este *bit*, depende da topologia (roteadores, *firewall*, *proxies*, etc), do desempenho dos equipamentos, o empacotamento de informações, filas de entrada e de saída de pacotes, da carga da rede (uso da rede), etc. O atraso tem uma influência muito grande em aplicações de tempo real como a telefonia IP. Os atrasos devem ser de no máximo 150 ms para serem consideradas ótimas. Atrasos da ordem de 250 ms já aumentam em muito a possibilidade dos usuários terem que esperar o "término da fala" para começar a falar. A telefonia convencional tipicamente não produz 150 ms de atraso fim-a-fim, o que é imperceptível ao ser humano. As ligações internacionais, em especial, quando usados satélites chegam a ter 1 segundo de atraso que é inaceitável.

O ITU-T define com relação a atraso de voz os seguintes intervalos:

- de 0 até 150 ms: ótimo;
- de 150 até 300 ms: bom;
- de 300 até 450 ms: ruim;
- acima de 450 ms: inaceitável.

O grande desafio da telefonia IP é justamente garantir uma qualidade de voz similar da rede telefônica pública convencional provavelmente compartilhando e concorrendo com outras aplicações IP em tempo real. Existem obstáculos a serem superados no ambiente de rede que influenciam a qualidade de voz em telefonia IP.

A perda de pacotes (Figura 12) devido ao congestionamento da rede, obriga os roteadores a descartar pacotes, influenciam a qualidade da voz. Perdas periódicas de pacotes da ordem de 5% a 10% podem afetar significativamente a qualidade de voz. Perdas ocasionais de pacotes devido a "rajadas" podem tornar a conversação difícil [LEPPÄNEN].

O *Jitter* (Figura 13) é a variação do intervalo entre chegadas de pacotes introduzidos pelo comportamento variável do atraso de pacotes na rede.

Pacotes podem ser recebidos fora de ordem (Figura 14), obrigando a aplicação a ordená-los ou descartá-los. Um exemplo prático pode ser citado, quando existem mais de uma rota para o destino, e os pacotes de voz acabam sendo encaminhados por rotas distintas fazendo com que os pacotes cheguem desordenados.

A largura da banda disponível é outro parâmetro muito importante. Quanto mais banda disponível, melhor o desempenho, especialmente para o tráfego de pacotes de dados, conhecidos como aplicações "*bandwidth-bound*", sensíveis a banda disponível. Já as aplicações de voz são conhecidas como aplicações "*delay-bound*", sensíveis à atrasos [GORALSKY]. Quanto maior a banda disponível, menor deverá ser o atraso na rede.

A disponibilidade e confiabilidade da rede é importante para a telefonia IP que deve manter a robustez existente na telefonia convencional. Atualmente é esperado uma disponibilidade da rede entre 99,995% a 99,999%, o que significa a indisponibilidade menor que vinte e seis minutos e vinte e oito segundos por ano [ARKIN] [DOUSKALIS] [GORALSKY] [SCHULZRINNE1].

Segurança é outro tópico importante para telefonia IP [ARKIN] [GORALSKY] [THALHAMMER]. Eventuais ataques de *phrackers*[14], podem acabar comprometendo QoS, tornando a rede indisponível (*denial of service*) entre outras conseqüências.

Para a telefonia IP deve-se garantir a integridade, privacidade, não-repúdio e autenticidade das chamadas visando evitar fraudes. Para tal, mecanismos de autenticação e criptografia são importantes.

[14] *phrackers*: São os *hackers* especializados em quebrar e burlar os sistemas de segurança telefônicos com os mais diferentes objetivos.

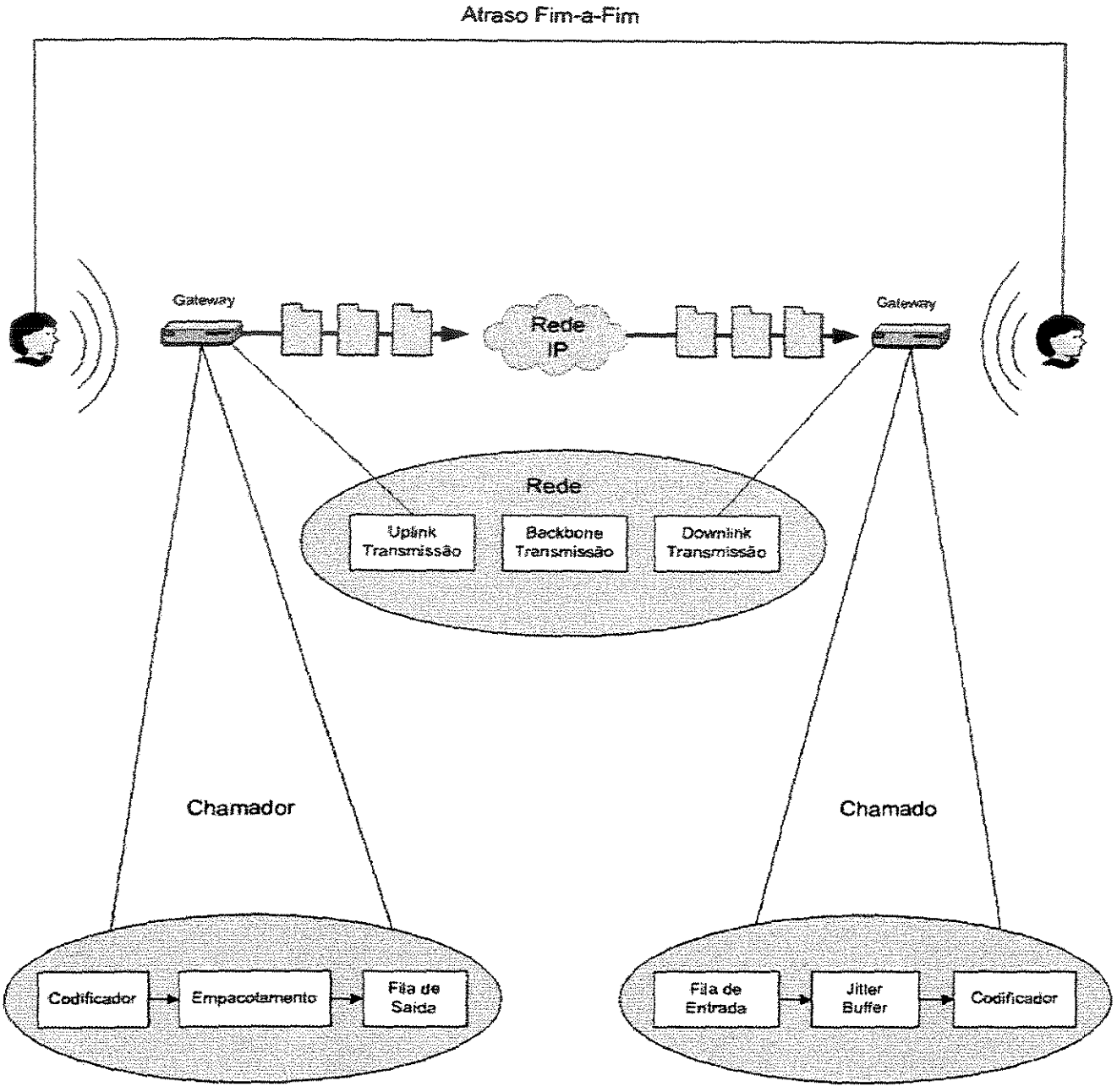

Figura 11 Atraso de voz fim-a-fim

Conceitos de segurança de redes podem ser encontrados em [STALLINGS]. Em [ARKIN], [BEIJAR], [TELCORDIA] e [THALHAMMER] são apresentados aspectos gerais de segurança para telefonia IP. Em [THERNELIUS] é feita uma análise sobre *firewalls*, NAT (*Network Address Translation*) [RFC1631] e o protocolo SIP. Em [GAMM] são apresentados aspectos de segurança para NGN. Em [FWH323] é feita uma breve análise sobre *firewalls* com o protocolo H.323. Na [RFC3329] é especificado um mecanismo de segurança entre o agente usuário e a próxima entidade SIP. Na [RFC3303] é descrita a integração de dispositivos de segurança para telefonia IP com *firewalls*.

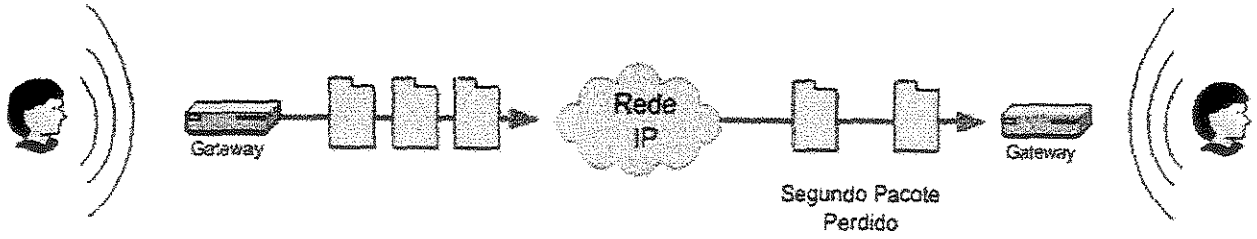

Figura 12 Perda de pacote transmitido

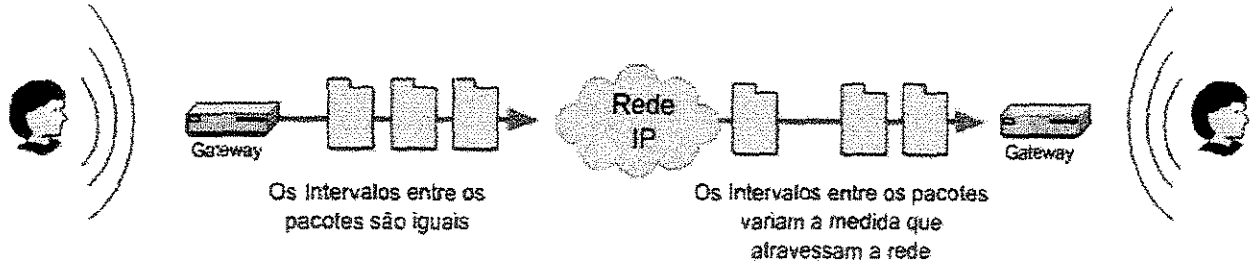

Figura 13 Ocorrência de *Jitter*

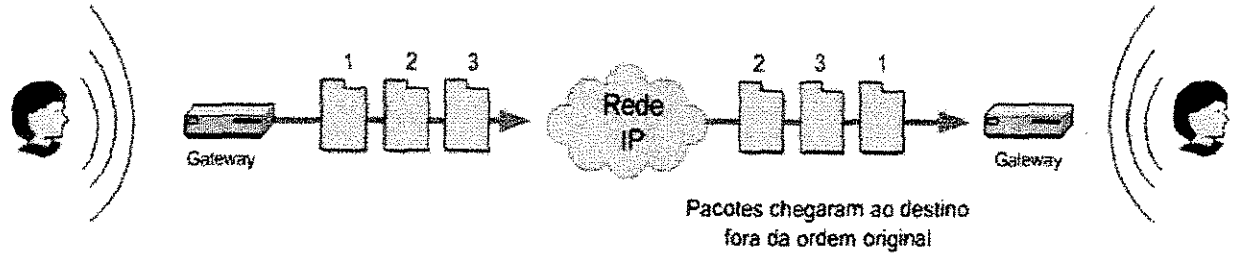

Figura 14 Recepção de pacotes fora de ordem

3.2 Transporte de Voz Sobre IP

O protocolo IP oferece serviços de rede "*best effort*". Isto significa que o protocolo no máximo, se compromete a despachar pacotes. Neste modelo, se os pacotes forem descartados, o protocolo IP não recupera esses pacotes. O protocolo *Transmission Control Protocol* (TCP) que é o protocolo de transporte na Internet, oferece serviço de entrega garantida. O TCP fornece este serviço, introduzindo atrasos na entrega, que não se constitui em problema para aplicações típicas de dados, tais como *e-mail*, *web browsing*, transferência de arquivos, etc. No entanto, para aplicações de voz e outras de tempo real, que são sensíveis aos atrasos, o uso do protocolo TCP pode tornar facilmente essas aplicações não factíveis. Assim sendo para o transporte de voz é usado o outro protocolo de transporte da pilha TCP/IP, o protocolo *User Datagrama Protocol* (UDP), que não é orientado a conexão.

Devido a natureza de entrega não confiável dos serviços providos pelo protocolo UDP, são necessários mecanismos para garantir que os pacotes sejam entregues em tempo

voz similar ao da telefonia convencional, de comutação por circuitos. Para tal, é usado o protocolo RTP (*Real-Time Transport Protocol*) [RFC1889] [RFC1890].

O RTP é um protocolo de transporte de tempo real que visa oferecer um serviço de entrega fim-a-fim para aplicações que transmitem dados em tempo real, tais como áudio e vídeo. Associado ao RTP existe outro protocolo RTCP (*Real-Time Control Protocol*), que recolhe periodicamente as informações dos participantes da sessão e provê entre outras informações para a aplicação:

- parâmetros de qualidade da transmissão de uma sessão RTP: *jitter*, perda média de pacotes, número total de pacotes transmitidos, etc;
- a identidade dos participantes: nomes, *e-mails*, organização, número telefônico, etc;
- sincronismo intermídia: necessário para sincronizar diferentes mídias como áudio e vídeo, caso suas origens sejam de diferentes servidores.

As principais funções providas pelo RTP são:

- Tipo de *payload*: o *payload* de cada pacote RTP é a informação em tempo-real contida em cada pacote. O seu formato é livre, e deve ser definido pela aplicação ou pelo perfil do RTP em uso. Para evitar a análise do conteúdo do *payload*, o cabeçalho de cada pacote RTP contém um número que indica o tipo de *payload* de cada pacote, que essencialmente são codificadores para digitalização de áudio e vídeo. A interpretação do número do tipo do *payload* é especificada na RFC 1890;

- *TimeStamp*: é um campo de 32 bits que indica o instante em que a primeira amostra de *payload* foi gerada. O instante da amostragem deve ser derivada de um relógio que incrementa monotonicamente e linearmente o tempo, de modo que as aplicações possam tratar os pacotes de uma maneira sincronizada, possibilitando o cálculo do jitter. A freqüência do relógio é dependente do formato do *payload* do dado. Por exemplo, a freqüência para esquema típico de codificação de voz é 8000Hz (cada 0,125ms). O incremento do *timestamp* dependerá do número de amostras contidas em um pacote. Por exemplo, se um pacote contém 10 amostras de voz e um *timestamp* de um, então o próximo pacote deve possuir *timestamp* de valor 11. Dado que cada amostra ocorre a cada 0,125ms, então a diferença de 10 no *timestamp* indica uma diferença de 1,25ms. O valor inicial do *timestamp* do primeiro pacote é um número escolhido aleatoriamente [COLLINS];

- Número de seqüência: é um campo de 16 bits que é incrementado de um em cada pacote de dados RTP enviado, e pode ser usado pelo receptor para detectar a perda de pacotes e chegada de pacotes fora de seqüência. Uma aplicação de áudio pode usar o número de seqüência e o *timestamp* para gerenciar um *buffer* de recepção. Uma aplicação pode determinar que irá armazenar 100 ms de fala no *buffer* antes de iniciar sua reprodução. Cada vez que um pacote RTP chega, é colocado na posição apropriada, dependendo do número de seqüência. Se um pacote não chegar a tempo e ainda estiver faltando no momento da reprodução, a aplicação poderá copiar o último quadro do pacote que acabou de ser reproduzido e repeti-lo até chegar a vez do próximo pacote

recebido, ou usar algum esquema de interpolação definido pelo codificador de áudio que estiver sendo usado.

O RTP e o RTCP permitem aos receptores compensar o *jitter* de rede, por meio de controle de *buffer* e sequenciamento, e obter mais informações da rede para que medidas corretivas possam ser tomadas pela camada superior da aplicação. Ambos protocolos não tem influência sobre o comportamento da rede IP e nem controlam a Qualidade de Serviço (QoS - *Quality of Service*) [COLLINS]. O RTP e o RTCP são geralmente utilizados com o protocolo UDP, embora também possam ser usados com o protocolo TCP, em diferentes portas, sendo assinalada uma porta par para o RTP, e a porta de número imediatamente superior (ímpar) é assinalada para o RTCP. Ambos somente podem usar portas do intervalo de 1025 a 65535, sendo as portas 5004 e 5005 alocadas como portas *default* no caso das portas não serem explicitamente alocadas. Não é obrigatório o uso do RTCP junto ao RTP.

Os protocolos MGCP, Megaco/H.248, SIP e H.323 usam o RTP/RTCP para transporte de voz.

3.3 Qualidade da Voz

Alguns outros fatores devem ser considerados em telefonia IP que afetam a qualidade da voz, como o codificador de voz, o cancelamento de eco (híbrido e acústico), a supressão de silêncio[15], ou seja o não envio de pacotes quando da ausência de fala, a geração de ruído de conforto[16], ou seja a inserção de ruídos de conforto quando ocorre a opção de supressão de silêncio.

A qualidade de voz pode ser mensurada de modo a obtermos valores de referência. O *Percentual Speech Quality Measurement* (PSQM) é uma das técnicas[17] para mensurar a qualidade de voz, sendo definida pela recomendação P.861 da ITU-T [ITUP861]. Trata-se de uma medição objetiva da qualidade da fala. Ela foi desenvolvida originalmente para testar codificadores e acabou tendo grande aceitação como padrão *de facto* para testar sistemas de telefonia IP [CHOWDHURY]. A idéia básica do modelo PSQM é medir os sinais processados, executar uma análise objetiva entre a versão original e a processada, e após isso oferecer uma opinião da qualidade das funções de processamento que ocorreram em cima do sinal original.

O ITU-T também define métodos de teste subjetivo na recomendação P.800 [ITUP800] como o *Mean Opinion Score* (MOS), que se utiliza de técnicas estatísticas para quantificar as respostas subjetivas de um grupo de usuários. O MOS é usado para determinar a qualidade de fala geral, solicitando que os ouvintes classifiquem a amostra de voz dando as seguintes notas:

---

[15] Com a supressão de silêncio pode ser reduzido de 40% a 50% o requisito de banda, uma vez que a conversação humana tem um modelo de comportamento *half-duplex* [DOUSKALIS].

[16] O ruído de conforto é uma função complementar a função de supressão de silêncio. Visa oferecer ao ouvinte "sons" durante os períodos em que a supressão de silêncio não está enviando pacotes de voz.

[17] Outro método muito difundido e idêntico ao PSQM é o PAMS (*Perceptual Analysis Measurement System*) da *British Telecom*. Também existe *E-model* da recomendação ITU G-107.

- 1 (ruim): ininteligível, o usuário não entende a mensagem decodificada;
- 2 (fraca): o sinal possui interrupções devido a sua degradação, obrigando ao usuário a fazer um esforço considerável para entender trechos da conversação;
- 3 (regular): o usuário sente-se incomodado com as degradações, mas não há interrupções, conseguindo entender a mensagem com esforço moderado;
- 4 (boa): a voz é agradável de se ouvir. Percebe degradações mínimas, mas não se incomoda com elas, nenhum esforço apreciável é necessário;
- 5 (ótima): o usuário não percebe diferença com o trecho original, não percebendo nenhum degradação e não sendo necessário nenhum esforço para entender a fala.

O resultado aritmético da avaliação de um coleção de MOS é denominada de *Mean Conversation-Opinion Score* (MOS_C).

A Figura 15 ilustra o funcionamento do PSQM:

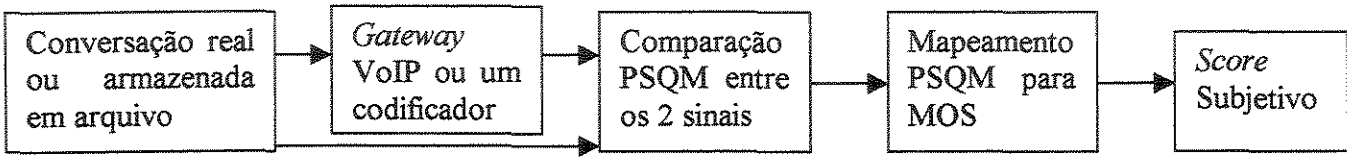

Figura 15 Exemplo do funcionamento PSQM

Uma consideração importante sobre o MOS é que não é um valor absoluto, sendo dependente do contexto em que foi coletado, ou seja dos parâmetros usados, tais como codificador, supressão de eco, detecção de silêncio, etc.

Supondo uma avaliação da qualidade de voz fim-a-fim IP, é preciso também considerar o impacto da carga da rede, do tipo de tráfego de interferência, da configuração da rede e dos equipamentos, do desempenho acústico e de áudio dos equipamentos terminais, de políticas de QoS adotadas, da existência de NAT e *firewalls* [DOUSKALIS1].

4 Conclusões

A telefonia IP apresenta uma série de vantagens como melhor aproveitamento de banda de rede, integração e evolução de aplicações existentes, criação de novos serviços e interconexão com a telefonia comutada por circuitos. É necessário, no entanto, que os serviços atualmente existentes atendam os requisitos mínimos de QoS. Assim sendo a evolução tecnológica não implicará em perda da qualidade (em especial de voz) e sim no acréscimo de funcionalidades às redes IP, tornando-as mais atraentes esta nova tecnologia para os usuários finais. Mecanismos para QoS devem ser adotados para obter uma qualidade de voz adequada para o tráfego de telefonia IP.

As soluções de telefonia IP são interessantes para as operadoras e corporações que podem reduzir custos utilizando-se de *backbones* já instalados, ou aumentar a receita provendo novos serviços e utilizando-se de novas aplicações emergentes.

O mercado corporativo é o nicho no qual as soluções de telefonia sobre IP estão sendo mais implantadas, permitindo o uso da rede de dados para o transporte de voz. O protocolo SIP bem como o H.323 são interessantes para o uso em ambientes corporativos, substituindo PBXs, integrando com *backbones* corporativos nos quais o controle do uso de banda e de serviços é plausível. O protocolo H.323 é mais usado em conferências com PC's enquanto que o SIP tende a ser adotado pelos provedores de redes de dados interessados na telefonia IP [WANG] [GLASSMAN].

No entanto, ambos protocolos ainda não são disseminados para uso em assinantes comuns (usuários domésticos) em especial pela necessidade de aparelhos telefônicos especiais (telefones IP's e *softphones*), cujos custos são maiores que os dos telefones comuns [SCHULZRINNE1]. Além disso, o modelo tarifário existente não incentiva a migração do usuário doméstico para esta nova tecnologia, pois atualmente terá que pagar uma tarifa (ainda) maior para uso da rede de dados em sua casa para utilizar o serviço de telefonia, além do investimento nos aparelhos telefônicos. Uma alternativa, no caso do Brasil, para a adoção e disseminação desta tecnologia, visando entre outros itens a inclusão digital, é a utilização de recursos do FUST (Fundo de Universalização dos Serviços de Telecomunicações) para implantação de soluções de telefonia IP em conjunto com outros serviços como Internet, em entidades públicas como bibliotecas, escolas, hospitais, centros de saúde e comunidades carentes.

Existe uma disputa de mercado entre os protocolos SIP (IETF) e H.323 (ITU-T), evidente em algumas comparações existentes [COMPSIPH323]. No entanto, ambas soluções continuam evoluindo. Essa disputa, além dos aspectos técnicos, tem um grande aspecto comercial envolvendo corporações que atuam no setor, sejam como fabricantes ou usuários das tecnologias. O fato do SIP ter sido escolhido pela 3GPP [3GPP], pode indicar uma vantagem comercial para o SIP sobre o H.323. No entanto, acreditamos que a solução poderia ser um esforço colaborativo mútuo similar ao Megaco/H.248

A tendência natural é que haja uma migração do MGCP para o Megaco/H.248, que é uma evolução do MGCP para controle de *gateways* de mídia, e é resultado do esforço

conjunto do ITU-T e do IETF. A solução de uso de protocolos controladores de *gateways* de mídia é muito importante para permitir o acesso da planta atual da rede telefônica para as redes com protocolo IP, neste momento de transição, integrando tecnologias, fazendo uma evolução incremental e preservando investimentos já realizados.

A tecnologia de telefonia IP ainda apresenta algumas questões práticas que precisam ser melhor detalhadas e tratadas tais como escuta judicial autorizada (como implantar, como tratar quando a chamada e seus dados forem criptografados), aderência a modelos de tarifação neste novo paradigma de comunicação. A tarifação atualmente é orientada pelo degrau tarifário[18] [ANATEL] no caso de ligações "não locais" e multi-medição (Karlsson-Acrescido[19]) [ANATEL] no caso de ligações locais e regionais (dependendo do horário com medição simples).

Também a questão da segurança precisa ser melhor aprofundada, pois alguns mecanismos de segurança (IPSec [RFC2401], *firewalls* e *Network Address Translation* (NAT) [RFC1631]) podem ser adequados para transações de dados comerciais tolerantes a atrasos, mas podem impactar no desempenho e funcionamento de redes de telefonia IP e na integração com protocolos de telefonia IP (H323, SIP, Megaco/H.248 e MGCP) [DOUSKALIS1] [SCHULZRINNE1]. No entanto, prover mecanismos que evitem fraudes e indisponibilização de serviços em telefonia IP são mandatórios.

Outra questão que necessita atenção é a interligação entre os *backbones* de telefonia IP, que estão surgindo entre as diversas operadoras no mundo, de modo que interconectem entre si e com a Internet, não sendo simplesmente soluções de *backbones* proprietários [THERNELIUS].

Prevê-se que a tecnologia de telefonia IP, deva ter sua expansão nos próximos anos provendo integração com aplicações *web*, *video on demand*, *e-learning* e outras de tempo real nas *Next Generation Networks* e nas redes de telefonia móveis como UMTS.

Como evolução deste trabalho podemos citar o aprofundamento do tema de segurança em telefonia IP. Pelas pesquisas realizadas, esse assunto ainda está em desenvolvimento e ainda demanda estudos mais detalhados, tais como, mecanismos de segurança para os protocolos de telefonia IP, integração e impacto destes mecanismos em QoS.

Como referências adicionais ao trabalho citamos: [SCHULZRINNE], [SIP], [SIPCENTER], [PACKETIZER], [COMMWEB], [PROTOCOLS] e [TECHGUIDE].

---

[18] Intervalos de distâncias geodésicas, entre as localidades e centros de área de tarifação, para os quais são determinados níveis tarifários específicos.

[19] Método de tarifação por multimedição em que é aplicado aleatoriamente e registrado um pulso de tarifação quando da recepção do sinal de atendimento; os pulsos de tarifação subsequentes são enviados periodicamente ao contador associado ao terminal do assinante chamador em uma cadência predeterminada, durante o período de conversação.

5 Referências Bibliográficas

1. [3GPP] http://www.3gpp.org consultado em 20/06/2003
2. [ANATEL] http://www.anatel.gov.br/ajuda/glossario consultado em 13/06/2003
3. [ARKIN] Ofir Arkin, "Why E.T. Can't Phone Home? Security Risk Factors with IP Telephony based Networks", Novembro de 2002
4. [B2BUA] http://www.ietf.org/internet-drafts/draft-pierce-ieprep-assured-service-arch-01.txt, consultado em 23/06/2003
5. [BEIJAR] N. Beijar, "Signalling Protocols for Internet Telephony - Architectures based on H.323 and SIP", 1998
6. [CISCO] http://www.cisco.com
7. [CISCOSAFE] http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safip_wp.htm
8. [CHOWDHURY] D. D. Chowdhury, "Projetos Avançados de redes IP - Roteamento, Qualidade de Serviço e Voz sobre IP", editora Campus, 2002
9. [COLLINS] D. Collins, "Carrier Grade Voice Over IP", editora Mc-Graw-Hill, 2001
10. [COMPSIPH323]http://www.packetizer.com/iptel/h323_vs_sip/complist.html consultado em 21/06/2003
11. [COMMWEB] http://www.commweb.com
12. [CONGCISCO] CISCO SYSTEMS, "Congestion Avoidance Overview", http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/qcprt3/qcdconav.pdf consultado em 31/04/2003
13. [DEFVOIP] Microsoft Corporation, *"Internet Protocol (IP) Telephony MarketTrends"*, http://www.microsoft.com/windows/Embedded/devices/voip/voipindtrends.asp consultado em 28/07/2003
14. [DOUSKALIS] B. Douskalis, "IP Telephony - The Integration of Robust VoIP Services", editora Prentice Hall, 2000
15. [DOUSKALIS1] B. Douskalis, "Putting VoIP to Work Softswitch Network Design and Testing", editora Prentice Hall, 2002
16. [ERICSSON] http://www.ericsson.com/ipservices/literature/pdf/whitepaper.pdf
17. [FWH323] Polykon Networks, *Technical white paper addressing issues with H.323, Security & Firewalls*, "Creating Building Blocks For Voice & Video Over IP", 2002
18. [GAMM] B. Gamm, B.Howard e Olivier Paridaens, "Security features required in a NGN", Alcatel *Telecommunication Review 2nd Quarter* 2001
19. [GENUITY] http://www.genuity.com consultado em 14/06/2003
20. [GLASMANN] J. Glasmann, W. Kellerer e H. Müller, "Service Architectures in H.323 and SIP – A Comparison", 2002
21. [H323DOCS] http://www.packetizer.com/iptel/h323/doc_status.html consultado em 20/06/2003
22. [H323V5] http://www.packetizer.com/iptel/h323 consultado em 20/06/2003
23. [H323XSIP] *Nortel Networks*, "A Comparison of H.323v4 and SIP", Tóquio, Japão, 5 de Janeiro de 2000 - http://www1.cs.columbia.edu/sip/drafts/sip_h323v4.doc
24. [H323XSIP1] http://www.packetizer.com/iptel/h323_vs_sip consultado em 19/06/2003

25. [HERSENT] O. Hersent, D. Guide e J.P. Petit, "Telefonia IP Comunicação Multimídia Baseada em Pacotes", editora Addison-Wesley, 2002
26. [IANA] http://www.iana.org/
27. [IBASIS] http://www.ibasis.net consultado em 13/06/2003
28. [IEC] http://www.iec.org consultado em 13/06/2003
29. [IETF] http://www.ietf.org consultado em 13/11/2001
30. [ITU] http://www.itu.int consultado em 13/06/2003
31. [ITUP800] ITU-T *Recommendation* P.800 "Methods for subjective determination of transmission quality"
32. [ITUP861] ITU-T *Recommendation* P.861 "Objective quality measurement of telephone-band (300-3400 Hz) speech codecs"
33. [ITUT37] ITU-T *Recommendation* T.37 "Procedures for the transfer of facsimile data via store-and-forward on the Internet"
34. [ITUT38] ITU-T *Recommendation* T.38 "Procedures for real-time Group 3 facsimile communication over IP networks"
35. [ITXC] http://www.itxc.com consultado em 13/06/2003
36. [JOHNSTON] A.B. Johnston, "SIP Understanding the Session Initialized Protocol", editora Artech House, 2001
37. [LEPPÄNEN] Leppänen Marko, "Voice over IP", *Helsinki University Technology - Department of Computer Science*, 2001
38. [LINFONE] http://www.linphone.org consultado em 13/06/2003
39. [LUCENT] http://www.lucent.com consultado em 13/06/2003
40. [MAGALHAESECARDOZO] Mauricio Magalhães e Eleri Cardozo, apostila "*Qualidade de Serviço na Internet*", DCA-FEEC-UNICAMP, 1999
41. [MICROSOFT] http://www.microsoft.com consultado em 13/06/2003
42. [MOCKINGBIRD] *MockingBird Networks*, "An introduction to IP Telephony", 1999
43. [OPENH323] http://www.openh323.org consultado em 10/01/2002
44. [PACKETCABLE] http://www.packetcable.com consultado em 13/10/2001
45. [PACKETIZER] http://www.packetizer.com/iptel/h323 consultado em 10/11/2001
46. [PACKETVOICE] *Cisco Systems*, "*Understanding Packet Voice Protocols*" - *Web ProForum Tutorials*, www.iec.org, consultado em 14/04/2003
47. [PICTURETEL] http://www.picturetel.com consultado em 13/06/2003
48. [POLYCOM] http://www.polycom.com consultado em 13/06/2003
49. [PROTOCOLS] http://www.protocols.com consultado em 14/01/2002
50. [QOSCISCO] *Cisco Systems*, "Quality of Service for Voice over IP", http://www.cisco.com/en/US/tech/tk652/tk698/technologies_white_paper09186a00800d6b73.shtml#24245 consultado em 30/04/2003
51. [QOSSBRC] C. A. Kamienski e D. Sadok, minicurso "Qualidade de Serviço na Internet", SBRC 2000, Belo Horizonte, 23 a 26 de maior de 2000.
52. [RADVISION] http://www.radvision.com consultado em 15/12/2001
53. [RAKESH] A. Rakesh, "Voice over IP: Protocols and Standards" 2/7/2000
54. [RFC1631] http://www.ietf.org/rfc/rfc1631.txt
55. [RFC1633] http://www.ietf.org/rfc/rfc1633.txt
56. [RFC1738] http://www.ietf.org/rfc/rfc1738.txt
57. [RFC1889] http://www.ietf.org/rfc/rfc1889.txt
58. [RFC1890] http://www.ietf.org/rfc/rfc1890.txt
59. [RFC1918] http://www.ietf.org/rfc/rfc1918.txt
60. [RFC2205] http://www.ietf.org/rfc/rfc2205.txt

61. [RFC2234] http://www.ietf.org/rfc/rfc2234.txt
62. [RFC2327] http://www.ietf.org/rfc/rfc2327.txt consultado em 03/01/2002
63. [RFC2401] http://www.ietf.org/rfc/rfc2401.txt
64. [RFC2543] http://www.ietf.org/rfc/rfc2543.txt consultado em 03/01/2002
65. [RFC2543BIS] http://www.ietf.org/internet-drafts/draft-ietf-sip-rfc2543bis-09.txt consultado em 10/01/2002
66. [RFC2702] http://www.ietf.org/rfc/rfc2702.txt
67. [RFC2705] http://www.ietf.org/rfc/rfc2705.txt consultado em 10/12/2001
68. [RFC2805] http://www.ietf.orf/rfc2805.txt consultado em 10/01/2002
69. [RFC3015] http://www.ietf.org/rfc/rfc3015.txt consultado em 10/01/2002
70. [RFC3031] http://www.ietf.org/rfc/rfc3031.txt consultado em 12/06/2003
71. [RFC3261] http://www.ietf.org/rfc/rfc3261.txt consultado em 20/06/2003
72. [RFC3303] http://www.ietf.org/rfc/rfc3303.txt consultado em 12/06/2003
73. [RFC3329] http://www.ietf.org/rfc/rfc3329.txt consultado em 12/06/2003
74. [RFC3435] http://www.ietf.org/rfc/rfc3435.txt consultado em 12/06/2003
75. [RFC3455] http://www.ietf.org/rfc/rfc3455.txt consultado em 21/06/2003
76. [RFC3525] http://www.ietf.org/rfc3525.txt consultado em 20/06/2003
77. [RINDE] J.Rinde, "Telephony in 2005" – *Computer Networks* 31 (1999) páginas 157-168
78. [SCHULZRINNE] http://www.cs.columbia.edu/~hgs/papers/ consultado em 20/04/2001
79. [SCHULZRINNE1] H. Schulzrinne, apresentação, "SIP Services and Applications", Washington, D.C, 20/04/2001
80. [SCHULZRINNE2] H. Schulzrinne e J.Rosenberg, "Signaling for Internet Telephony", 02/02/1998
81. [SCHULZRINNE3] H. Schulzrinne e J. Rosenberg, "A Comparison of SIP and H.323 for Internet Telephony", obtido na data de 30/04/2003 do endereço http://www.cs.columbia.edu/~hgs/papers/Schu9807_Comparison.pdf
82. [SCHULZRINNE4] H. Schulzrinne e J. Rosenberg, "Internet Telephony: architecture and protocols - an IETF perspective" – *Computer Networks* 31 (1999) páginas 237-255
83. [SIEMENS] http://www.siemens.com consultado em 13/06/2003
84. [SIP] http://www.cs.columbia.edu/sip
85. [SIPCENTER] http://www.sipcenter.com
86. [SIPCHARTER] http://ww.ietf.org/html.charters/sip-charter.html
87. [SIPRFCS] http://www.packetizer.com/iptel/sip consultado em 22/06/2003
88. [SIPFORUM] http://www.sipforum.org
89. [SIPH323] http://www.sipcenter.com/files/Service_Architecures_SIP-H323.pdf consultado em 14/08/2001
90. [SOFTSWITCH] http://www.softswitch.org consultado em 13/10/2001
91. [SONUS] http://www.sonusnet.com consultado em 13/06/2003
92. [STALLINGS] William Stallings, "Cryptography and Network Security: Principles and Practice", editora Prentice Hall; *3rd edition* (2002).
93. [SYS-SECURITY] http://www.sys-security.com/html/projects/VoIP.html consultado em 13/06/2003
94. [TELCORDIA] Telcordia Tecnologies, "Next Generation Networks: Voice Over Packet Industry Summit Security Challenges and Strategy", 2001
95. [TANDEBERG] http://www.tandberg.net consultado em 13/06/2003

96. [THERNELIUS] F.Thernelius, master's thesis, "SIP, NAT and Firewalls", Maio de 2000, *Department of Teleinformatics at the Royal Institute of Technology in Stockholm*
97. [THALHAMMER] Johann Thalhammer, *Master Thesis* "Security in VoIP-Telephony Systems", *Institute for Applied Information Processing and Comuunications Graz University of Technology - Austria*, 2002
98. [TOGA] J.Toga e J.Ott, "ITU-T Standardization activities for interactive multimedia communications on packet-based networks:H.323 and related recommendations" - *Computer Networks* 31 (1999) páginas 205-223
99. [VOCALTEC] http://www.vocaltec.com consultado em 13/06/2003
100. [VONCOM] http://www.von.com consultado em 30/05/2003
101. [VONORG] http://www.von.org consultado em 30/05/2003
102. [VOVIDA] http://www.vovida.org consultado em 10/12/2001
103. [TECHGUIDE] http://www.techguide.com/comm/sec_html/voiceip.shtml
104. [WANG] Ligang Wang, *Master Thesis Concordia University*, Canadá, "Modelling and Verification of Interworking Between SIP and H.323", 2002
105. [WEILER] Lars Weiler, apresentação "Voice over IP", 2002

Apêndice 1

Cabeçalhos SIP

Formato Compactado

Alguns cabeçalhos SIP têm um formato compactado, no qual o nome do cabeçalho é denotado por um único caracter minúsculo.

Formato Compactado	Cabeçalho
c	*Content type*
e	*Content encoding*
F	*From*
I	*Call ID*
L	*Content lenght*
M	*Contact (moved)*
S	*Subject*
T	*To*
V	*Via*

Cabeçalho *General*

Incluem todos os cabeçalhos requeridos pelas mensagens SIP, podendo estar presentes tanto para requisições como para respostas.

Cabeçalho	Descrição
Call-ID	Identifica unicamente a chamada entre dois agentes usuários. Obrigatório em todas as requisições e respostas SIP.
Contact	Identifica o recurso solicitado ou o solicitante do recurso, dependendo se presente em mensagem de requisição ou de resposta
Cseq	Contém um número decimal que é incrementado a cada requisição, e é usado pelo agente usuário servidor para identificar requisições fora de seqüência, diferenciar requisições novas de antigas (cSeq diferentes) ou retransmissão (mesmo cSeq).
Date	Usada para transportar a data em que requisições ou respostas foram enviadas. Suporta somente o time *zone* GMT
Encryption	É usado para especificar a parte da mensagem SIP que está criptografada.
From	Indica a origem da requisição, podendo detalhar por chamada
Organization	Indica a organização que o originador de chamado pertence.
Retry-After	Indica quando um serviço ou recurso pode estar disponível novamente. Pode ser uma data ou uma especificação de tempo em segundos a aguardar
Subject	Indica o título da sessão
Supported	Lista uma ou mais opções implementadas por um agente usuário ou servidor. Usualmente colocada em respostas para requisições *OPTIONS*
Timestamp	Usado pelo agente usuário cliente para marcar o momento exato de uma requisição que foi gerada.
To	Obrigatório em toda mensagem SIP, indica o destino da requisição.
User Agent	Usado para passar informações sobre o agente usuário originador da requisição. Pode ser informação do fabricante, versão de software ou comentários.
Via	Usado para registrar a rota SIP tomada e é usada para rotear a resposta de volta

Cabeçalhos *Request*

São adicionados pelo agente usuário cliente para modificar ou prover informação suplementar sobre a requisição.

Cabeçalho	Descrição
Accept	Indica o formato de mensagem aceito. O *default* é *application*/sdp
Accept-Contact	Especifica quais URLs a requisição pode ser encaminhada. É usado para oferecer controle parcial do originador de chamada no modo com que os servidores *proxy* processam as chamadas
Accept-Encoding	Usado para especificar o tipo aceito de codificação que o corpo da mensagem. O *default* é *text/plain*.
Accept-Language	Usado para especificar as preferências de idioma
Authorization	Usado para fornecer as credenciais de um agente usuário em uma requisição ao servidor.
Hide	Usado pelos agentes usuários ou *proxy* para solicitar que o *next hop proxy* criptografe o cabeçalho via para esconder a informação de roteamento.
In-Reply-To	Indica qual *Call-ID* que a requisição está respondendo ou referencia
Max-Forwards	Indica o número máximo de saltos que uma requisição SIP pode fazer
Priority	Usado para setar a urgência da requisição (não urgente, normal, urgente, emergência)
Proxy-Authorization	Usado para levar as credenciais do agente usuário em uma requisição para o servidor *proxy*.
Proxy-Require	Usado para listar *features* e extensões que o agente usuário requisita para um *proxy* suportar para processar a requisição.
Record_Route	Usado para forçar roteamento através de um *proxy* para todas as requisições subsequentes em uma sessão com dois agentes usuários.
Reject-Contact	Especifica quais URL´s a requisição não pode usar como *proxy*
Request-Disposition	Usado para requisitar *proxy* ou servidor de redirecionamento
Require	Usado para especificar características e extensões que um agente usuário cliente requisita para um agente usuário servidor para processar a requisição
Response-Key	Usado pelo cliente para solicitar que as respostas da requisição sejam criptografadas com a chave pública contida neste campo
Route	Usado para forçar o roteamento para uma requisição através de um caminho específico. O caminho é extraído do campo *Record-Route* e/ou *Contact* recebido na requisição anterior dentro da mesma chamada.
RAck	Usado para responder a uma requisição PRACK para uma reconhecimento confiável de uma resposta que contém cabeçalho Rseq
Session-Expires	Usado para colocar um limite de validade da sessão. Válido somente se o cabeçalho "Supported: timer" estiver presente na requisição/resposta presente/anterior
Responde Headers	Usados para fornecer mais informações do que o código e a mensagem de resposta pelo agente usuário servidor ou servidor SIP

Cabeçalhos *Response*

São adicionados pelos servidores SIP ou agentes usuários servidores para fornecer mais informações além do código e texto da resposta.

Cabeçalho	Descrição
Proxy-Authenticate	Indica que agente usuário cliente deva formular a credencial no cabeçalho *Proxy-Authorization* na requisição subsequente para autorizar e validar o uso do *proxy*. Usado na mensagem "407 Proxy Authentication Required"
Server	Informações sobre o agente usuário servidor que está gerando as respostas.
Unsupported	Usado para indicar *features* que não são suportadas pelo servidor feitas em uma requisição anterior.

Warning	Usado para fornecer informações mais específicas do que o código de mensagem. O cabeçalho contém um código de três dígitos de *waning*, qual servidor inseriu o cabeçalho e o texto de *warning* entre aspas duplas.
WWW-Authenticate	Indica que agente usuário cliente deva informar a credencial para o agente usuário ou servidor de registro para autenticação. Usado na mensagem "401 Unauthorized"
RSeq	Usado para respostas de *INVITEs* que requerem transporte confiável

Cabeçalhos *Entity*

Fornecem informações adicionais do corpo da mensagem ou do recurso solicitado.

Cabeçalho	Descrição
Allow	Indica os métodos suportados pelo *proxy* ou agente usuário servidor enviando as respostas.
Content-Encoding	Indica que a lista de esquema de codificação está aplicada para o corpo da mensagem.
Content-Disposition	Usado para descrever a função do corpo da *mensagem (session, icon, alert, render)*
Content-Length	Indica o número de caracteres do corpo da mensagem. O valor 0 indica que não há corpo de mensagem
Content-Type	Usado para especificar o tipo de formato do corpo da mensagem. Se não estiver presente o *default* é *application*/sdp
Expires	Indica o intervalo de tempo no qual a requisição ou conteúdo de mensagem é válido. Pode conter uma data SIP ou o intervalo em segundos em que é válido.
MIME-Version	Indica a versão do *Multipurpose Internet Mail Extension Protocol* usado para construir o corpo da mensagem. SIP não é considerado MIME-*compliant* pois não usa a especificação MIME, usando o padrão SIP.

Classes de Respostas de Mensagens SIP

Um servidor SIP responde com uma ou mais respostas de mensagens SIP, sendo que a maioria das respostas finaliza a transação SIP [HERSENT] [JOHNSTON] [RAKESH].

Classe	Descrição	Ação
1xx	Informativo: Status de chamada antes de seu completamento	Se for a primeira informação o cliente deveria reiniciar novamente a temporização para retransmissão
100	Tentando	
180	Chamando	
181	Chamada sendo retransmitida	
182	Chamada colocada na fila	
183	Sessão em Progresso	
2xx	Sucesso: Requisição foi feita com sucesso	Se for uma mensagem de INVITE, a mensagem ACK deve ser retornada. Caso contrário deve parar a solicitação de requisições
200	OK	
3xx	Redirecionamento: Servidor retornou possíveis resultados.	O cliente deve tentar novamente as requisições em outro servidor
300	Múltiplas escolhas	
301	Movido permanentemente	
302	Movido temporariamente	
305	Usar *Proxy*	
380	Serviço alternativo	
4xx	Erro no Cliente: a requisição falhou devido a um erro no cliente. Pode ser sintaxe inválida ou incapacidade do servidor atender.	O cliente deveria tentar novamente a requisição, reformulando-a de acordo com a resposta.

400	Pedido inválido	
401	Não autorizado	
402	Necessário pagamento	
403	Proibido	
404	Não encontrado	
405	Método não permitido	
406	Não aceitável	
407	Necessária autenticação do *proxy*	
408	Tempo para pedido esgotado	
409	Conflito	
410	Não mais presente	
411	Necessário fornecer comprimento	
413	Corpo da mensagem de pedido muito grande	
414	URI do pedido muito grande	
415	Tipo de mídia não suportado	
420	Extensão inválida	
480	Temporariamente indisponível	
481	Transação ou *leg* de chamada não existente	
482	Laço de *loop* detectado	
483	Excesso de segmentos (saltos)	
484	Endereço incompleto	
485	Ambíguo	
486	Ocupado localmente	
487	Requisição cancelada	
488	Não aceitável localmente	
5xx	Falha no Servidor: a requisição falhou devido a falha no servidor	As requisições devem ser feitas em outro servidor
500	Erro interno do servidor	
501	Não implementado	
502	*Gateway* inválido	
503	Serviço não disponível	
504	Tempo esgotado no *gateway*	
505	Versão de SIP não suportada	
6xx	Falha Global: a requisição falhou	A requisição não deveria ser tentada novamente
600	Ocupado em todos os lugares	
603	Declínio	
604	Não existe em lugar nenhum	
606	Não aceitável	

Apêndice 2

H.323

Tabela de Mensagens RAS [COLLINS]

Mensagem	Função
GatekeeperRequest(GRQ)	Usado por um ponto terminal quando tentando descobrir seu *gatekeeper*
GatekeeperConfirm(GCF)	Usado pelo *gatekeeper* para indicar que será o gatekeeper de um determinado ponto terminal
GatekeeperReject(GRJ)	Usado pelo *gatekeeper* para indicar que não será o gatekeeper de um determinado ponto terminal
RegistrationRequest(RRQ)	Usado pelo ponto terminal para registro com um *gatekeeper*
RegistrationConfirm(RCF)	Resposta positiva do *gatekeeper* para o ponto terminal, indicando sucesso no registro.
RegistrationReject(RRJ)	Resposta negativa de um RegistrationRequest
UnregistrationRequest(URQ)	Usado tanto por um *gatekeeper* quanto um ponto terminal para cancelar um registro existente
UnregistrationConfirm(UCF)	Usado tanto por um *gatekeeper* quanto um ponto terminal para confirmar o cancelamento de um registro
UnregistrationReject(URJ	Resposta negativa de um UnregistrationRequest
AdmissionRequest(ARQ)	Enviado por um ponto terminal para um *gatekeeper* para solicitar permissão para participar de uma chamada
AdmissionConfirm(ACF)	Usado pelo *gatekeeper* para autorizar o ponto terminal a participar de uma chamada
AdmissionReject(ARJ)	Usado pelo *gatekeeper* para negar permissão para um ponto terminal participar de uma chamada
BandwidthRequest(BRQ)	Enviado por um *gatekeeper* ou ponto terminal para requisitar mudança na alocação de comprimento de banda
BandwithConfirm(BCF)	Resposta positiva de uma solicitação *BandwidthRequest*
BandwidthReject(BRJ)	Usado pelo ponto terminal ou *gatekeeper* para negar a mudança de comprimento de banda; usado somente por um ponto terminal se o novo comprimento de banda não pode ser suportado
InfoRequest(IRQ)	Enviado pelo *gatekeeper* para um ponto terminal requerendo informação de status
InfoRequestResponse(IRR)	Enviado de um ponto terminal para um *gatekeeper* para fornecer informação de status; pode ser enviado por demanda ou de forma autonoma
InfoRequestAck(IACK)	Enviado pelo *gatekeeper* como confirmação de uma solicitação IRR
InfoRequestNak(INAK)	Enviado pelo *gatekeeper* em resposta a uma solicitação IRR em uma situação de erro, tal como de um ponto terminal não registrado
DisangageRequest(DRQ)	Enviado por um ponto terminal ou *gatekeeper* para solicitar término de conexão de uma chamada em um ponto terminal
DisangageConfirm(DCF)	Resposta positiva de um DRQ
DisangageReject(DRJ)	Resposta negativa de um DRQ; por exemplo de um ponto terminal não registrado
LocationRequest(LRQ)	Enviado para um *gatekeeper* para solicitar a tradução de um *alias* para endereço de rede
LocationConfirm(LCF)	Resposta de um LRQ com o endereço solicitado
LocationReject(LRJ)	Resposta de um LRQ quando a tradução não foi bem sucedida
Non-StandardMessage(NSM)	Mensagem especifica de fabricante
UnknownMessageResponse(XRS)	Resposta a uma mensagem não reconhecida
RequestInProgress(RIP)	Enviado por um ponto terminal ou *gatekeeper* como uma resposta temporária se uma solicitação está tomando muito tempo para ser processada

ResourceAvailableIndicate(RAI)	Enviado pelo *gateway* para um *gatekeeper* a fim de informar o *gatekeeper* da capacidade atual do *gateway*
ResourceAvailableConfirm(RAC)	Enviado por um *gatekeeper* como reconhecimento de um RAI

Tabela de Mensagens de Sinalização de Chamada (H.225.0) [COLLINS]

Mensagem	Função	Comentário
Alerting	Enviado pelo ponto terminal chamado para indicar que o usuário chamado está sendo alertado	Deve ser suportado
Call Proceeding	Uma resposta temporária opcional enviada pelo ponto terminal chamado ou *gatekeeper* antes do envio da mensagem de *Connect*	Deveria ser enviado se o ponto terminal chamado usa um *gatekeeper*
Connect	Uma indicação de que o usuário chamado aceitou a chamada	Deve ser suportado
Progress	Mensagem opcional enviado pelo ponto terminal chamado antes da mensagem de *Connect*	Pode ser usado pelo *gateway* chamado no caso de *internetworking* com RPTC
Setup	Mensagem inicial usada para começar o estabelecimento de uma chamada	Deve ser suportado
Setup Acknowledge	Resposta opcional para mensagem de *Setup*	Pode ser encaminhado de um *gateway* no caso de *internetworking* com RPTC
Release Complete	Usado para terminar uma chamada	A mensagem Q.931 *release* não é usada
User Information	Mensagem opcional que é usada para enviar informações adicionais de estabelecimento de chamada	Pode ser usada em sinalização *overlap*
Notify	Mensagem opcional que é usada para fornecer informação para apresentação para o usuário	Pode ser usado pelo ponto terminal chamado ou chamador
Status	Enviado em resposta a uma mensagem de Status *Inquiry* ou em resposta a uma mensagem desconhecida	Mensagem opcional
Status Inquiry	Mensagem enviada para interrogar o lado remoto sobre o status atual da chamada	Pode ser enviado em conjunto com procedimentos de status do RAS
Facility (Q.932)	Usado para redirecionar uma chamada ou invocar um serviço suplementar	Pode ser enviado por qualquer lado a qualquer momento; é útil para transportar informações quando nenhuma outra mensagem poderia ser enviada

Apêndice 3

MGCP

Parâmetros de Comandos MGCP [DOUSKALIS]

Nome do Parâmetro	Código	Valor do Parâmetro
CallID	C	*String* Hexadecimal com pelo menos 32 caracteres. O valor é enviado pelo agente de chamada para o ponto terminal do *gateway* de mídia e identifica a chamada, que pode envolver uma ou mais conexões locais
ConnectionID	I	Este valor é selecionado pelo ponto terminal do *gateway* de mídia como resultado de um comando CRCX
NotifiedEntity	N	Um identificador no formato RFC821 (por exemplo: MGC@sv.qualquerrede.com:5625 ou sv@[10.1.1.4]. Se o endereço IP real é usado, ele deve vir entre colchetes. A entidade especificada é assumida como quem receberá todas as notificações para os eventos requisitados. Se o parâmetro é omitido, o ponto terminal enviará os eventos ocorridos para a última entidade que enviou um comando válido.
RequestIdentifier	X	Este parâmetro é selecionado pelo agente de chamada e enviado para o *gateway* de mídia sempre que uma notificação de evento é requisitada. O *gateway* de mídia responde com o mesmo valor de parâmetro quando o evento requisitado é observado e NTFY é enviado para o agente de chamada.
LocalConnectionOptions	L	Esta estrutura caracteriza o método de codificação para o fluxo de mídia, período de empacotamento, banda a ser usada, tipo de serviço e o uso de cancelamento de eco. É enviada pelo agente de chamada para o ponto terminal, geralmente em um comando CRCX.
ConnectionMode	M	Define a o canal de comunicação como *full duplex, half duplex* (somente envio ou recebimento), *loopback*, inativo, *check* contínuo ou dados. Enviado pelo agente de chamada para o ponto terminal.
RequestedEvents	R	O MGC envia um ou mais códigos para o evento procurado pelo *gateway* de mídia ponto terminal através deste parâmetro. Eventos incluem, "no gancho", "fora do gancho", dígitos teclados, etc. Os eventos podem ser requisitados para serem enviados imediatamente, separados para posterior transmissão ou acumulados.
SignalRequest	S	Este parâmetro é enviado pelo agente de chamada para o ponto terminal do *gateway* de mídia para requisitar a execução de um sinal como por exemplo o tom de discar.
DigitMap	D	O mapa de dígito é enviado pelo agente de chamada para o ponto terminal do *gateway* de mídia para facilitar a coleta da *string* de dígitos válidos de acordo com um plano de numeração. Uma análise de dígito preliminar pode ser feita antes da *string* ser passada para análise posterior. *Strings* que não casam com o plano atual de encaminhamento não são transmitidas para o *gateway* de mídia.
ObservedEvents	O	É enviado pelo *gateway* de mídia para o agente de chamada quando um ou mais eventos requisitados foram observados pelo ponto terminal.
ConnectionParameters	P	São estatísticas gerais sobre o desempenho da conexão. São enviados pelo ponto terminal quando a conexão é deletada
SpecifiedEndPointID	Z	Um identificador no formato RFC821, como por exemplo: EndPoint@sv.qualquerrede.com:5625, [10.1.1.4]
RequestedInfo	F	É código RC (*RemoteConnectionDescriptor*) ou LC (*LocalConnectionDescriptor*).
QuarantineHandling	Q	Eventos requisitados podem ocorrer imediatamente após um evento prévio detectado tenha causado um NTFY e antes do ACK ser recebido pelo agente

		de chamada. Isto é conhecido como "estado de notificação". A palavra chave "*process*" requisita que os eventos observados neste intervalo sejam armazenados enquanto a palavra chave "*discard*" solicita que eles sejam descartados pelo ponto terminal.
DetectedEvents	T	Lista os eventos requisitados que são o mínimo que devem ser detectados pelo ponto terminal do *gateway* de mídia enquanto no "estado de notificação". É enviado pelo agente de chamada para o ponto terminal
EventStates	ES	Lista de estados de pontos terminais que podem ser auditados e devem ser retornados para o agente de chamada em resposta para um comando *AuditEndpoint*. Por exemplo: ES:hu—*the phone is off-hook*
RestartMethod	RM	Métodos suportados são "*graceful*", "*forced*", "*restart*" ou "*disconnected*". É enviado pelo *gateway* de mídia para indicar que um ponto terminal está sendo colocado fora de serviço ou retornando em serviço.
RestartDelay	RD	Enviado pelo *gateway* de mídia quando *RestartInProgress* é enviado por um ponto terminal. Especifica o número de Segundos após o qual o ponto terminal executará o *RestartMethod*, exceto para "*forced*", no qual é imediato. Se não presente o *delay* é 0.
Capabilities	A	As capacidades do ponto terminal podem ser requisitadas pelo agente de chamada através de um comando *AuditEndpoint*. Capacidades são o algoritmo de compressão (lista de codificadores suportados), período de empacotamento (intervalo), banda (intervalo), cancelamento de eco, supressão de silêncio, modos de conexão, o tipo de serviço, e o pacote de evento. Um pacote de evento é um aglomerado de sinais e eventos suportados por um específico tipo de ponto terminal, por exemplo telefone analógico.

Associação de Comandos e Parâmetros MGCP [DOUSKALIS]

A tabela abaixo mostra a associação entre linhas de parâmetros e os comandos MGCP. "M" indica mandatório, "O" indica opcional e "-" indica não permitido.

Nome do Parâmetro	**CRCX**	**MDCX**	**DLCX**	**RQNT**	**NTFY**	**AUEP**	**AUEX**	**RSIP**
CallID	M	M	O	-	-	-	-	-
ConnectionID	-	M	O	-	-	-	M	-
NotifiedEntity	O	O	O	O	O	-	-	-
RequestIdentifier	O	O	O	M	M	-	-	-
LocalConnectionOptions	M	O	-	-	-	-	-	-
ConnectionMode	M	O	-	-	-	-	-	-
RequestedEvents	O	O	O	O	-	-	-	-
SignalRequest	O	O	O	O	-	-	-	-
DigitMap	O	O	O	O	-	-	-	-
ObservedEvents	-	-	-	-	M	-	-	-
ConnectionParameters	-	-	O	-	-	-	-	-
SpecifiedEndPointID	-	-	-	-	-	-	-	-
RequestedInfo	-	-	-	-	-	O	O	-
QuarantineHandling	O	O	O	O	-	-	-	-
DetectedEvents	O	O	O	O	-	-	-	-
EventStates	-	-	-	-	-	-	-	-
RestartMethod	-	-	-	-	-	-	-	M
RestartDelay	-	-	-	-	-	-	-	O
Capabilities	-	-	-	-	-	-	-	-

Tabela de códigos de mensagens de erro MGCP

Código	Descrição
100	*The transaction is currently being executed. An actual completion message will follow on later*
200	*The requested transaction was executed normally.*
250	*The connection was deleted.*
400	*The transaction could not be executed, due to a transient error.*
401	*The phone is already off hook*
402	*The phone is already on hook*
403	*The transaction could not be executed, because the endpoint does not have sufficient resources at this time*
404	*Insufficient bandwidth at this time*
500	*The transaction could not be executed, because the endpoint is unknown.*
501	*The transaction could not be executed, because the endpoint is not ready*
502	*The transaction could not be executed, because the endpoint does not have sufficient resources*
510	*The transaction could not be executed, because a protocol error was detected.*
511	*The transaction could not be executed, because the command contained an unrecognized extension.*
512	*The transaction could not be executed, because the gateway is not equipped to detect one of the requested events.*
513	*The transaction could not be executed, because the gateway is*
	Not equipped to generate one of the requested signals.
514	*The transaction could not be executed, because the gateway cannot send the specified announcement.*
515	*The transaction refers to an incorrect connection-id (may have been already deleted)*
516	*The transaction refers to an unknown call-id.*
517	*Unsupported or invalid mode.*
518	*Unsupported or unknown package.*
519	*Endpoint does not have a digit map.*
520	*The transaction could not be executed, because the endpoint is "restarting".*
521	*Endpoint redirected to another Call Agent.*
522	*No such event or signal.*
523	*Unknown action or illegal combination of actions*
524	*Internal inconsistency in LocalConnectionOptions*
525	*Unknown extension in LocalConnectionOptions*
526	*Insufficient bandwidth*
527	*Missing RemoteConnectionDescriptor*
528	*Incompatible protocol version*
529	*Internal hardware failure*
530	*CAS signaling protocol error.*
531	*Failure of a grouping of trunks (e.g. facility failure).*

Tabela de mensagens de resultados de códigos

Código	Descrição
000	*Endpoint state is nominal. (This code is used only in response to audit requests.)*
900	*Endpoint malfunctioning*
901	*Endpoint taken out of service*
902	*Loss of lower layer connectivity (e.g., downstream sync)*

Apêndice 4

Megaco/H.248

Códigos de Erro de Comandos Megaco/H.248

Código Erro	Texto
400	*Bad Request*
401	*Protocol Error*
402	*Unauthorized*
403	*Syntax Error in Transaction*
406	*Version Not Supported*
410	*Incorrect identifier*
411	*The transaction refers to an unknown ContextId*
412	*No ContextIDs available*
421	*Unknown action or illegal combination of actions*
422	*Syntax Error in Action*
430	*Unknown TerminationID*
431	*No TerminationID matched a wildcard*
432	*Out of TerminationIDs or No TerminationID available*
433	*TerminationID is already in a Context*
440	*Unsupported or unknown Package*
441	*Missing RemoteDescriptor*
442	*Syntax Error in Command*
443	*Unsupported or Unknown Command*
444	*Unsupported or Unknown Descriptor*
445	*Unsupported or Unknown Property*
446	*Unsupported or Unknown Parameter*
447	*Descriptor not legal in this command*
448	*Descriptor appears twice in a command*
450	*No such property in this package*
451	*No such event in this package*
452	*No such signal in this package*
453	*No such statistic in this package*
454	*No such parameter value in this package*
455	*Parameter illegal in this Descriptor*
456	*Parameter or Property appears twice in this Descriptor*
471	*Implied Add for Multiplex failure*
500	*Internal Gateway Error*
501	*Not Implemented*
502	*Not ready.*
503	*Service Unavailable*
504	*Command Received from unauthorized entity*
505	*Command Received before Restart Response*
510	*Insufficient resources*
512	*Media Gateway unequipped to detect requested Event*
513	*Media Gateway unequipped to generate requested Signals*
514	*Media Gateway cannot send the specified announcement*
515	*Unsupported Media Type*
517	*Unsupported or invalid mode*
518	*Event buffer full*
519	*Out of space to store digit map*

520	*Media Gateway does not have a digit map*
521	*Termination is "ServiceChangeing"*
526	*Insufficient bandwidth*
529	*Internal hardware failure*
530	*Temporary Network failure*
531	*Permanent Network failure*
581	*Does Not Exist*

Descritores Megaco/H.248 [DOUSKALIS1]

Descritor	Finalidade
Modem	Tipo e propriedade de modem
Mux	Tipo e propriedade de multiplexadores multimídia
Media	Descrição da mídia
TerminationState	Propriedades de terminação não associado o fluxo de mídia
Stream	Lista de descritores de mídia (tipos, modo, etc) para um fluxo. Podem ser *Local, Remote* ou *LocalControl*
Local, Remote	Contém propriedade de mídia que o *gateway* de mídia recebe e envia para o ponto terminal remoto respectivo
LocalControl	Propriedades para auxiliar o *gateway* de mídia e o *softswitch* na sinalização de comunicação. Também contém a propriedade modo, o qual pode ser inicializado para ser enviado somente, recebido somente, local *loopback* ou inativo
Events	Envia os eventos para serem detectados pelo *gateway* de mídia e especifica como manipular a notificação do *softswitch*
EventBuffer	Descreve como manipular os eventos quando bufferização for permitido
Signais	Lista de sinais a serem aplicados para a terminação
Audit	Lista de itens desejados como uma resposta de um comando *audit*
Packages	Os tipos de pacotes suportados para a terminação; usado em comando *audit*
DigitMap	Padrões de dígitos aceitáveis discados na terminação, que são reportados como simples evento quando o casamento ocorre. Isto não significa que um número válido foi discado, ele simplesmente indica que a forma em que os dígitos foram discados formam uma seqüência válida de acordo com o mapa carregado. Por exemplo, se uma central telefônica deseja somente aceitar 10 dígitos, um mapa de dígitos que suporta 10 dígitos pode ser carregado no *gateway* de mídia. Os dígitos serão armazenados até que os 10 dígitos tenham sido detectados e um simples evento será reportado para o *softswitch* para a análise
ServiceChange	Mudanças de serviço afetam terminações, grupos de terminação (por exemplo facilidades) e *gateways* inteiros. Mudanças podem ser *power-up* ou *power-down*.
ObservedEvents	Usado em *Notify* ou *AuditValue*, é usado de modo similar ao mesmo descritor do MGCP
Statistics	Usado em *Subtract* ou *Audit*. Retorna as estatísticas mantidas na terminação

Apêndice 5

SDP

Descrição de Campos [JOHNSTON]

Campo	Descrição	Obrigatório
v=	Versão do protocolo	Sim
o=	Proprietário/criador da sessão	Sim
s=	Nome da sessão	Sim
i=	Informação sobre a sessão	Não
u=	Uniform Resource *Identifier*	Não
e=	Endereço de email	Não
p=	Número de telefone	Não
c=	Informação de conexão	Sim
b=	Informação sobre largura de banda	Não
t=	Tempo que a sessão está ativa	Sim
r=	Intervalo de repetição	Não
z=	Ajustes de time *zone*	Não
k=	Chave de criptografia	Não
a=	Linhas de atributo de sessão	Não
m=	Informação da mídia	Sim
a=	Descrição da mídia	Não

- Versão do protocolo - Contém a versão do SDP. Por causa da versão atual ser 0 sempre será v=0.

- Proprietário/criador da sessão - Contém informações sobre o originador da chamada, sendo usado para identificar unicamente a sessão.

Formato: o=<nome do usuário> <id da sessão> <versão> <tipo de rede> <tipo do endereço> <endereço>

Onde:

<nome do usuário> : *login* do originador ou o host

<id sessão> : Número usado para garantir unicidade. Pode ser um número gerado aleatoriamente ou timestamp do *Network Time Protocol* (NTP)

<versão> : Número que é incrementado para cada mudança de sessão. Recomenda-se o uso do *timestamp* do NTP

<tipo de rede> : É sempre IN para Internet

<tipo do endereço> : Pode ser IP4 para IPv4 ou IP6 para IPv6

<endereço> : Pode ser usada a forma decimal ou *fully qualified host name*

Exemplo: o= yoshioka 3450983822 3450983234 IN IP4 192.168.0.1

- Nome da sessão - Contém o nome da sessão que pode conter qualquer caracter.

Formato: s=<nome da sessão>

Onde:
<nome da sessão> : Um ou mais caracteres

Exemplo: s=Voz sobre IP com SIP

- Informação sobre a sessão - Contém informação sobre a sessão. É um campo opcional.

Formato: i=<descrição da sessão>

Onde:
<descrição da sessão> : Um ou mais caracteres

Exemplo: i=Sessao de teste de SIP

- *Uniform Resource Identifier* - Contém o *Uniform Resource Identifier* com mais informações sobre a sessão. É um campo opcional.

Formato: u=<URI>

Onde:
<URI> : *Uniforme Resource Identifier*

Exemplo: u=http://www.ic.unicamp.br/sdp.ps

- Endereço de *e-mail* - Contém identificação de endereço de *e-mail.* É um campo opcional.

Formato: e=<*e-mail*> "(" <texto livre> ")" ou e=<texto livre> "<" <*e-mail*> ">"

Onde:
<*e-mail*> : endereço de *e-mail*
<texto livre> : zero ou mais caracteres

Exemplos: e=871067@ic.unicamp.br (Sergio Yoshioka)
e=871067@ic.unicamp.br

- Número de telefone - Contém identificação de número de telefone. É um campo opcional.

Formato: p=<número do telefone> "(" <texto livre> ")" ou
e=<texto livre> "<" <número do telefone> ">"

Onde:
<número do telefone>: número do telefone
<texto livre> : zero ou mais caracteres

Exemplos: p=+55-19-9778-1577 (Sergio Yoshioka)
p=Sergio Yoshioka <+55-19-9778-1577>

- Informação de conexão - Contém identificação da conexão. É opcional se for especificado no nível de mídia.

Formato: c=<tipo de rede> <tipo de endereço> <endereço de conexão>

Onde:

<tipo de rede>	: é definido como IN para Internet
<tipo de endereço>	: é definido como IP4 para endereços IPv4
<endereço de conexão>	: é o endereço IP que enviará os pacotes da mídia

Para sessões *multicast*, TTL (*Time to Live*) deve ser informado após o <endereço de conexão> separando essa informação por "/".

Exemplos: c=IN IP4 224.2.17.12/255
c=IN IP4 192.9.200.1

- Informação sobre largura de banda - Contém informação sobre largura de banda requerida. É um campo opcional.

Formato: b=<modificador>:<valor de banda>

Onde:

<modificador>	: pode ser CT (*Conference Total*) usado para sessões *multicast*, especificando o montante total de banda que pode ser usado por todos os participantes da sessão, ou AS (*Application Specific*) usado para especificar a banda especifica para uma aplicação.
<valor de banda>	: é especificado em kilobytes por segundo

Exemplos: b=CT:120
b=AS:256

- Tempo que a sessão está ativa - Contém informação sobre o tempo de início e de parada da sessão usando *timestamps* NTP.

Formato: t=<tempo de início> <tempo de parada>

Onde:

<tempo de início>	: indica o início da sessão
<tempo de parada>	: indica o final da sessão. Esse parâmetro com valor zero, em uma sessão agendada, indica que a sessão terá tempo indefinido. Caso o parâmetro <tempo de início> também tenha valor zero, indica que a sessão é permanente.

Exemplos: t=2873397496 2873404696
t=2873397496 0

- Intervalo de repetição - Contém informação sobre o intervalo de repetição da sessão, podendo ser especificados na notação NTP ou em dias (d), horas (h), minutos (m). A repetição ocorre até atingir o tempo de parada descrita no campo anterior. É um campo opcional.

Formato: r=<intervalo de repetição> <duração ativa> <lista de *offsets* a partir do tempo de início>

Onde:
<intervalo de repetição> : indica o intervalo para repetição
<duração ativa> : indica o tempo que deve ficar ativo
<lista de *offsets* a partir do tempo de início>: indica a lista de *offsets* para ativar a sessão a partir do tempo de início.

Exemplo: r=7d 1h 0 24h
Indica que a repetição será feita semanalmente, por uma hora, começando a partir do <tempo de início> variando inicialmente 0 e depois 25 horas até atingir o tempo de parada.

- Ajustes de *time zone* - Contém informação sobre o intervalo de repetição da sessão, podendo ser especificados na notação NTP ou em dias (d), horas (h), minutos (m). A repetição ocorre até atingir o tempo de parada descrita no campo anterior. É um campo opcional.

Formato: r=<intervalo de repetição> <duração ativa> <lista de *offsets* a partir do tempo de início>

Onde:
<intervalo de repetição> : indica o intervalo para repetição
<duração ativa> : indica o tempo que deve ficar ativo
<lista de *offsets* a partir do tempo de início>: indica a lista de *offsets* para ativar a sessão a partir do tempo de início.

Exemplo: r=7d 1h 0 24h
Indica que a repetição será feita semanalmente, por uma hora, começando a partir do <tempo de início> variando inicialmente 0 e depois 25 horas até atingir o tempo de parada.

- Chave de criptografia - Contém informação sobre a chave de criptografia a ser usada. É um campo opcional.

Formato: k=<método> ou k=<método>:<chave de criptografia>

Onde:
<método> : indica o método a ser usado que pode ser: *clear, base64, uri* ou *prompt*.
<chave de criptografia> : indica a chave de criptografia. Caso a opção de método escolhida tenha sido *prompt* esse parâmetro não será enviado.

Exemplo: k=*prompt*

- Atributo da sessão - Contém informação sobre os atributos da sessão. Pode ser usado para ampliar informações do SDP, fornecendo maiores informações da mídia. Pode ser um ou mais campos de atributo para cada *payload* de mídia, listado no campo de mídia. É opcional.

Formato: a=<atributo> ou a=<atributo>:<valor>

Onde:
<atributo> : indica o atributo da mídia
<valor> : indica o valor associado ao atributo

Exemplos: a=recvonly
a=rtpmap:0 PCMU/8000

- Informação da mídia - Contém informação sobre o tipo de mídia da sessão. É um parâmetro obrigatório.

Formato: m=<mídia> <porta> <transporte> <lista de formatos>

Onde:
<mídia> : indica o tipo de mídia. Pode *ser audio, video, application, data ou control.*
<porta> : indica o número da porta a ser usada
<transporte> : indica o tipo de protocolo de transporte a ser usado: RTP/AVP (*Real-time Transport Protocol / Audio Video Profiles*) ou udp.
<lista de formatos> : contém mais informações sobre a mídia. Usualmente os tipos de *payload* da mídia. Mais de um tipo de *payload* pode ser usado indicando múltiplos codificadores que podem ser aceitos.

Exemplo: M=*audio* 49180 RTP/AVP 0 3
Indica que a mídia é áudio, pode ser recebida na porta 49180, o protocolo de transporte é o RTP/AVP, e os formatos que podem ser usados são o PCM-μ *law* G711 (valor 0) e o GSM (valor 3).

- Descrição da mídia - Contém informações mais específicas sobre atributos da mídia após o campo informação de mídia (m). Seguem os campos opcionais de atributos da mídia que tem a mesma sintaxe apresentada para o nível de sessão:

i= Título da mídia.
c= Informação sobre a conexão. É opcional se incluída no nível de sessão.
b= Informação sobre largura de banda.
k= Informação sobre chave de criptografia
a= Atributos da mídia.