João Carlos Peixoto de Almeida da Costa

Implementação e Gerência de uma Arquitetura de Voz sobre IP

Orientador:
Prof. Paulo Henrique de Aguiar Rodrigues, Ph.D.

Universidade Federal do Rio de Janeiro - UFRJ
Instituto de Matemática - IM
Núcleo de Computação Eletrônica – NCE

Rio de Janeiro, Setembro de 2003

Implementação e Gerência de uma Arquitetura de Voz sobre IP

João Carlos Peixoto de Almeida da Costa

DISSERTAÇÃO SUBMETIDA AO CORPO DOCENTE DO INSTITUTO DE MATEMÁTICA/NÚCLEO DE COMPUTAÇÃO ELETRÔNICA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM INFORMÁTICA.

Aprovada por:

_____
Prof. Paulo Henrique de Aguiar Rodrigues, Ph.D.

_____
Prof[a]. Luci Pirmez, D.Sc.

_____
Prof. José Ferreira de Rezende, Dr.

RIO DE JANEIRO, RJ - Brasil
Setembro de 2003

Ficha Catalográfica

Peixoto, João Carlos de Almeida da Costa.

Implementação e Gerência de uma Arquitetura de Voz sobre IP / João Carlos Peixoto de Almeida da Costa. - Rio de Janeiro, 2003

xii, 167 f.: il.

Dissertação (Mestrado em Informática) – Universidade Federal do Rio de Janeiro - UFRJ, Instituto de Matemática - IM/NCE, 2003.

Orientador: Paulo Henrique de Aguiar Rodrigues

1. VOIP 2. SNMP 3. Gerenciamento de Redes

I. Rodrigues, Paulo Henrique de Aguiar (Orient.) II. Universidade Federal do Rio de Janeiro. Instituto de Matemática. III. Título.

À Nataly

MINHA COMPANHEIRA DE ESTRADA NO APRENDIZADO DO AMAR,
PELO CONVÍVIO ESTIMULANTE E CUMPLICIDADE

E AOS MEUS PAIS,

POR TODO O ESFORÇO E DEDICAÇÃO SEMPRE DISPENSADOS NA
MINHA FORMAÇÃO

Agradecimentos

AGRADECEMOS A TODOS AQUELES QUE DE ALGUMA FORMA, CONTRIBUIRAM NA EXECUÇÃO DESTA PESQUISA, E EM PARTICULAR:

Ao Prof. Júlio Salek, pelo incentivo, apoio e por acreditar que este trabalho seria possível (***in memorium)*** .

Ao Prof. Paulo Aguiar pela orientação, estímulo na execução do trabalho, leitura crítica dos manuscritos e valiosas sugestões que tanto enriqueceram nossa pesquisa.

Aos professores dos Cursos de pós-graduação em Informática da Universidade Federal do Rio de Janeiro que muito contribuíram para nossa formação profissional.

Ao amigo Fabio David, pelo apoio e atenção sempre constantes durante todo o processo de elaboração da tese.

Aos colegas do Laboratório VOIP IP, pela oportunidade de convivência profissional e cooperação.

Ao Núcleo de Computação Eletrônica pelas condições de trabalho fornecidas e suporte que asseguraram o bom andamento de nosso estudo.

Resumo da Tese apresentada ao IM/NCE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

Implementação e Gerência de uma Arquitetura de Voz sobre IP

João Carlos Peixoto de Almeida da Costa

Setembro/2003

Orientador: Paulo Henrique de Aguiar Rodrigues

Programa: Informática

O uso da tecnologia de voz sobre IP (VOIP) está em franca expansão. A integração das redes de voz e dados traz inúmeras vantagens, incluindo redução nos custos e a facilidade na comunicação entre os usuários. Este trabalho explora a implementação de uma rede VOIP, incluindo a seleção do protocolo a ser adotado, dos dispositivos necessários à sua implementação, dos detalhes de configuração e requisitos de gerência.

O gerenciamento de uma rede VOIP é importante para garantir a qualidade de voz nas chamadas e a disponibilidade do serviço. Para que se possa utilizar o protocolo *Simple Network Management Protocol* (SNMP) para atender este objetivo, é necessário saber como se constituem as bases de informações gerenciais (MIBs) implementadas nos equipamentos e serviços monitorados. MIBs definidas através de órgãos de padronização, como o ITU-T e IETF, e outras especificadas pelos fabricantes, para atender as necessidades de gerenciamento de redes VOIP, são revistas ao longo deste trabalho.

O protocolo *Remote Access Dial In User Service* (RADIUS) também é avaliado como uma fonte de informações para organizar um histórico das chamadas realizadas.

Um sistema integrado de gerenciamento VOIP está sendo proposto para o uso destas informações no controle da configuração do serviço, na identificação de falhas, na análise da performance e na contabilização das chamadas realizadas.

Abstract of Thesis presented to IM/NCE/UFRJ as a partial fulfilment of the requirements for the degree of Master of Science (M.Sc.)

Implementation and Management of a Voice over IP Architecture

João Carlos Peixoto de Almeida da Costa

September/2003

Advisor: Paulo Henrique de Aguiar Rodrigues

Department: Informatics

Voice over IP technology is becoming a reality in our days. Several advantages come from the integration of voice and packet networks, including cost reduction and improved communication between users. In this work we focus on the implementation of a VOIP network, defining the architecture, configuration details and management requirements.

The VOIP network management is important to ensure the service availability and voice call quality monitoring. The use of Simple Network Management Protocol (SNMP) to achieve this goal requires full knowledge of the management information base (MIB) implemented on the monitored services and devices. We review and analyze MIBs defined by standardization bodies, as ITU-T and IETF, and also MIBs provided by VOIP vendors.

We also explore using Remote Access Dial In User Service (RADIUS) as a tool to collect call history.

We propose a VOIP management system that integrates different SNMP collected data and Radius information to implement service configuration control, failures detection, performance analysis and call accounting.

LISTA DE SIGLAS E ABREVIATURAS

AAL	*ATM Adaptation Layer*
AF	*Assured Forwarding*
ANI	*Automatic Number Identification*
ATM	*Asynchronous Transfer Mode*
CBR	*Constant Bit Rate*
CDR	*Call Detail Record*
CODEC	*Coder/Decoder*
DNIS	*Dialed Number Identification Service*
DSCP	*Differentiated Service Code Point*
DTMF	*Dual Tone Multi Frequency*
EF	*Expedited Forwarding*
IETF	*Internet Engineering Task Force*
ICMP	*Internet Control Message Protocol*
ICPIF	*Calculated Planning Impairment Factor*
LLQ	*Low Latency Queue*
MC	*Multipoint Controller*
MCU	*Multipoint Control Unit*
MIB	*Management Information Base*
MOS	*Mean Opinion Scores*
MP	*Multipoint Processor*
MTBF	*Mean Time Between Failures*
MTTR	*Mean Time to Repair*
NAS	*Network Access Server*
PBX	*Private Branch Exchange*
QoS	*Quality of Service*
RADIUS	*Remote Authentication Dial In User Service*
RAQMON	*Real-time Application Quality of Service Monitoring*
RAS	*Registration, Admission and Status*
RFC	*Request For Comments*
RMON	*Remote Monitoring*
RNP	Rede Nacional de Pesquisa
RDS	*RAQMON Data Source*
RDSI	*Rede Digital de serviços Integrados*
RRC	*RAQMON Report Collector*
RTP	*Real Time Protocol*
RTCP	*Real Time Control Protocol*
SIP	*Session Initiation Protocol*
SMI	*Structure of Management Information*
SNMP	*Simple Network Management Protocol*
TDM	*Time Division Multiplexing*
VSA	*Vendor Specific Attribute*
VOIP	*Voice over IP*

SUMÁRIO

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Telefonia e dados são aplicações indispensáveis a qualquer empresa ou organização moderna. As redes de telefonia e as redes de dados sempre foram caracterizadas como redes distintas, utilizando infra-estruturas totalmente independentes. Ao utilizar os dois serviços, é necessária a contratação de canais de comunicação específicos e de prover estruturas internas diferentes, o que representa uma duplicação do custo e dos esforços para manter a funcionalidade de ambas. A convergência para uma única infra-estrutura capaz de suportar os dois serviços pode representar uma economia razoável de recursos. A rede IP, com a inclusão de mecanismos para garantir a qualidade de serviço aos diferentes tipos de tráfego em circulação pela rede, torna-se do ponto de vista econômico e tecnológico, uma alternativa viável e interessante para suporte a esta convergência. Duas modalidades de serviço podem ser consideradas no uso da tecnologia VOIP (Voz sobre IP): o serviço puramente VOIP, onde há a substituição total do PBX (*Private Branch Exchange*) por aplicações que implementam os serviços tradicionais de telefonia, acrescidos opcionalmente por serviços adicionais, como a integração com o serviço de correio eletrônico e a WEB; e a segunda modalidade, onde são utilizados equipamentos para interligar e adaptar a rede de telefonia tradicional à rede IP, os chamados *gateways* de voz. Essa segunda modalidade permite que usuários dos dois mundos se comuniquem ou que a rede IP possa ser utilizada para interligar PBXs distantes. No primeiro caso, a economia está associada à redução na infra-estrutura de telefonia necessária, onde normalmente o custo com aquisição de PBXs e com os serviços de manutenção destes equipamentos são bastante elevados. No segundo caso, a economia está associada à diminuição nos gastos com a telefonia pública, principalmente nas ligações de longa distância.

Analisando, por exemplo, o perfil da conta telefônica da UFRJ pode ser verificado um custo elevado com telefonia celular e um valor baixo associado às ligações de longa distância. O uso de tecnologia VOIP ainda não permite uma redução

com os custos de telefonia celular, visto que a transmissão de dados pelos celulares ainda apresenta um custo muito elevado. Desta forma, o uso de VOIP não permitirá reduzir de forma significativa os custos associados à telefonia. Entretanto, muitas ligações telefônicas deixam de ser realizadas porque a maioria dos telefones não permite a realização de ligações de longa distância, o que dificulta, por exemplo, o contato de um pesquisador ou da administração da universidade com o MEC, com o CNPq ou com outras universidades. Neste caso, o grande benefício no uso da tecnologia será o fato de permitir a implantação de uma rede VOIP que interligue universidades, centros de pesquisa, ministérios e órgãos associados, integrada com a rede de telefonia convencional dessas instituições. Desta forma, poderão ser estabelecidas chamadas VOIP entre qualquer máquina conectada à rede IP dessas instituições. A interligação com a telefonia convencional permitirá também realizar chamadas diretas entre quaisquer ramais dessas instituições sem gastos envolvidos, além de permitir chamadas entre os ramais e as máquinas IP. A comunicação entre as pessoas dessas instituições, que antes era limitada, passa a ser possível, possibilitando uma melhor comunicação sem que haja aumento nos custos com telefonia. O setor de bolsas do CNPq poderá, por exemplo, ter um número VOIP que estará ao dispor para o contato de qualquer pesquisador das instituições participantes.

A universidade utiliza atualmente uma rede de telefonia composta de várias centrais telefônicas (PBXs – *Private Branch Exchange*) conectadas. Entretanto, não consegue atender a todos os usuários, seja porque não possui infra-estrutura física que permita disponibilizar um ramal ou porque não possui mais ramais disponíveis em centrais telefônicas específicas. Como a rede de dados atende grande parte da universidade, será viável estender a "telefonia" até locais onde não exista atualmente. Desta forma, será possível usar a tecnologia VOIP para estabelecer chamadas entre terminais VOIP nestes locais, com outros terminais ou telefones convencionais.

Outro benefício no uso da tecnologia VOIP é tornar transparente a localização do usuário. Este passa a receber uma identificação que permite contactá-lo independente da sua localização física ou da máquina que esteja utilizando, basta que indique a sua localização atual em registros mantidos em servidores VOIP, que serão utilizados para localizá-lo quando de uma nova chamada.

A integração com outras aplicações IP permitirá o desenvolvimento de novos serviços, como um sistema unificado de mensagens integrando telefonia, correio eletrônico e fax, ou então, *call centers* com aplicações integradas ao serviço VOIP que facilitem a comunicação com o usuário atendido, entre outras.

1.1 Histórico

Na década de 70, pesquisadores universitários já familiarizados com a transmissão de texto e dados na *Arpanet*, decidiram tentar a transmissão de voz na rede de dados já existente ([1], [2], [3], [4] e [5]). Alguns destes experimentos demonstraram que conferências de voz eram possíveis utilizando a tecnologia de comutação de pacotes, entretanto, não foram produzidas ferramentas que pudessem ser amplamente utilizadas.

No final dos anos 80 e início dos 90, o crescente poder de processamento das estações de trabalho permitiu realizar conferências de voz entre usuários conectados à Internet. Vários experimentos realizados na *Dartnet* (*Defense Advanced Research Technology Network*) envolvendo o uso de *multicast* geraram ferramentas que permitiam a conferência de voz [6]. Entretanto, o uso destas ferramentas era limitado, visto que poucas pessoas na Internet tinham acesso a estações de trabalho UNIX e estas aplicações, além de instáveis, eram difíceis de utilizar. Adicionalmente, a limitada largura de banda nos enlaces que formavam a estrutura central (*backbone*) da Internet na época, tornava muito difícil a obtenção de uma qualidade de som aceitável. Apesar de não requerer uma largura de banda muito grande, a qualidade do áudio nas aplicações de voz depende bastante de redes não congestionadas, sendo susceptíveis a vários fatores, a saber, atrasos (*delay*), variações no atraso (*jitter*) e perdas de pacotes.

Avanços na infra-estrutura de redes, na codificação da voz e no poder de processamento dos equipamentos permitiram a proliferação da tecnologia de VOIP a partir do ano de 1995. Este ano foi marcado pelo lançamento de um grande número de produtos comerciais para aplicações VOIP. Em especial, a empresa israelense *Vocaltec* lançou o *Internet Phone,* o primeiro produto comercial largamente utilizado para este fim [7]. Este foi o primeiro produto que demonstrou que a Internet poderia ser utilizada para prover chamadas de voz em tempo real com uma boa qualidade de áudio, não

sendo muito diferente da obtida nas chamadas realizadas através do sistema de telefonia tradicional.

Estes produtos se caracterizavam por prover a comunicação entre dois computadores, não sendo possível a comunicação de um computador com a telefonia tradicional. Houve a necessidade então de "*gateways* de voz", computadores que fizessem a ponte entre a rede de telefonia e a Internet, convertendo o sinal de voz analógico do telefone em pacotes IP que trafegam na Internet. No final de 1995 e início de 1996, um grupo de pessoas formou uma associação chamada "*Free World Dialup*", que trabalhou em um projeto de desenvolvimento de um software que permitia que usuários na Internet ligassem para telefones tradicionais que, apesar de restrito em funcionalidades, demonstrou que a Internet não era limitada aos computadores conectados [8]. Ainda em 1995, outra empresa (IDT – *International Discount Telecommunications*) anunciou um serviço que permitia a realização de chamadas a partir de um computador na Internet para telefones comuns nas principais cidades dos EUA cobrando 10 cents o minuto [9]. Este serviço permitia, por exemplo, que uma pessoa no Japão ligasse para um telefone nos EUA a preços módicos, alterando significativamente a política de preços adotada até o momento para os serviços de telecomunicações.

Nesta época ainda não existiam soluções para o uso das redes IP para a interligação de PBXs. Entretanto, uma outra tecnologia estava sendo utilizada em projetos de pesquisa para este fim, a tecnologia ATM (*Asynchronous Transfer Mode*). A recomendação ITU-T I.363.1 especifica a camada de adaptação AAL-1 (*ATM Adaptation Layer*) [10], onde são definidos serviços que permitem o desenvolvimento de aplicações que tenham como requisitos a transferência de dados a uma taxa constante de bits (CBR – *Constant Bit Rate*) e o suporte ao sincronismo entre origem e destino. A definição desta camada permitiu o desenvolvimento de aplicações para a emulação de circuitos TDM (*Time Division Multiplexing*), que permitiram implementar o serviço de voz sobre ATM (VoATM – *Voice over ATM*). Vários projetos foram realizados na época utilizando estas aplicações, tais como os experimentos desenvolvidos no Laboratório VOIP do NCE/UFRJ, Brasil [11] e na rede de pesquisa da Austrália (AARnet – *Australian Academic and Research Network*) [12]. Nestes experimentos, os

PBXs (*Private Branch Exchange*) eram interligados utilizando PVCs (*Permanent Virtual Circuit*) que emulavam circuitos TDM E1 (N x 64Kbps). Uma limitação ao uso do serviço de VoATM era o requisito de que as localidades deveriam estar necessariamente interligadas através de redes ATM, o que restringia o uso do serviço.

Ao surgirem os primeiros *gateways* de voz IP, a Internet tornava-se o meio ideal para a implementação do serviço de telefonia, em função de sua abrangência e facilidade de conexão. Estes equipamentos tornaram possível implementar o conceito de telefonia IP, onde PBXs em localidades distintas eram conectados utilizando a rede IP como meio de transporte. Esta aplicação tornou possível a conectividade telefônica entre localidades remotas sem a necessidade de utilizar a rede de telefonia pública. Um *gateway* converte o sinal proveniente do PBX em pacotes IP, estes são transmitidos pela Internet até o *gateway* remoto, onde são convertidos novamente para a rede de telefonia e então transmitidos para o telefone remoto. Outra aplicação possível é a utilização dos *gateways* diretamente conectados à telefonia pública, possibilitando ligações de longa distância sem a utilização do serviço das operadoras de telefonia pública de longa distância. O uso do serviço de telefonia sobre IP traz vantagens:

- convergência das redes de dados e telefonia para uma estrutura única;
- redução nos custos de operação, já que será utilizada a mesma equipe para cuidar dos dois serviços;
- quando uma instituição ou empresa se conecta a várias localidades remotas, não há a necessidade de linhas independentes para telefonia e para dados;
- independência do custo em relação à distância.

A padronização nos protocolos de sinalização (Recomendações ITU-T H.323 [13] e IETF SIP – *Session Initiation Protocol* [14]) e de transporte de mídia (RTP – *Real-Time Transport Protocol* [15]) na rede IP e a crescente oferta de *gateways* de voz comerciais, associados às vantagens do serviço de telefonia IP, incentivaram a criação de uma série de projetos para a implantação deste serviço a partir do final da década de 90. Na área acadêmica, destacam-se os trabalhos realizados nas redes nacionais de pesquisa da Austrália [16], da Alemanha [17] e da República Tcheca[18], as quais

utilizam o protocolo H.323 para fins de sinalização, com previsão de uso do protocolo SIP.

No projeto australiano, a tecnologia VOIP é implementada sobre a rede de dados da rede de pesquisa australiana (AARNet). As universidades e instituições de pesquisa que participam do projeto realizam todas as ligações para a telefonia pública através da AARNet, sejam locais ou de longa distância. Em novembro de 1999 eram realizadas em média 3300 chamadas telefônicas diárias envolvendo telefones e aparelhos de fax, com uma duração média de 237 segundos. O custo das chamadas era 70% a 90% inferior ao cobrado pelas operadoras de telefonia para o mesmo tipo de serviço. Atualmente, são utilizados cerca de 62 *gateways* de voz, sendo uma das maiores redes de telefonia IP em operação.

O projeto VOIP na rede nacional de pesquisa da Alemanha (G-Win) começou em 2000 com o objetivo de testar a qualidade necessária para a transmissão de voz e o teste de interoperabilidade dos diferentes dispositivos VOIP. No final do ano de 2002, cerca de 20 universidades e centros de pesquisa participavam do projeto.

O grupo de telefonia IP da rede da República Tcheca (CESNET - *Czech Education and Scientific NETwork*) iniciou suas atividades em 1999 com o objetivo de interligar os PBXs de diversas universidades e conectar esta estrutura à rede de telefonia pública. Atualmente, envolve 12 instituições conectadas através de 10 *gateways* de voz. O objetivo do projeto é testar as tecnologias existentes para transmissão de voz em redes de dados (VOIP), o desenvolvimento de novas ferramentas e componentes visando o uso da tecnologia e o teste de interoperabilidade dos produtos de diferentes vendedores.

No Brasil, o grupo de trabalho VOIP (GT-VOIP) da Rede Nacional de Pesquisa (RNP) [19] desenvolve experimentos associados a VOIP e telefonia IP, sendo responsável pela implementação de um serviço experimental de telefonia no *backbone* RNP2, permitindo às organizações usuárias utilizar suas redes para estabelecer comunicação de voz a partir de seus PBXs, telefones IP e/ou estações de trabalho. No projeto-piloto a ser implementado até outubro de 2003, está previsto o uso de *gateways* PSTN/H.323, que possibilitarão a interconexão de PBXs com a Internet e o uso

transparente da telefonia IP para o usuário final, e a implantação de *gatekeepers* que facilitarão a utilização da telefonia IP diretamente de estações de trabalho.

1.2 Objetivos e revisão bibliográfica

Este trabalho faz parte do projeto de pesquisa do GT-VOIP da RNP onde está sendo desenvolvido um projeto-piloto de alcance nacional, que servirá como base para a implantação do serviço VOIP no *backbone* da RNP, o qual envolverá inicialmente 14 instituições conectadas ao *backbone* da RNP.

Está previsto o uso de *gateways* de voz para permitir a integração da telefonia tradicional das instituições envolvidas, provida por PBXs tradicionais, à rede IP. Equipamentos adicionais serão utilizados para permitir a localização dos usuários e a admissão das chamadas (*gatekeepers)* e para realizar o gerenciamento do serviço. Com o projeto implantado, será possível ligar a partir de um ramal interno da rede de telefonia destas instituições ou de um computador configurado como um cliente VOIP para ramais de qualquer uma das instituições participantes, sem que seja utilizada a infra-estrutura de telefonia pública. Desta forma, será possível uma economia de recursos na comunicação telefônica entre as instituições. Adicionalmente, o projeto permitirá que usuários que normalmente não podem realizar ligações interurbanas possam ligar para ramais de qualquer uma das instituições, melhorando a comunicação. A integração com o serviço VOIP da Internet2 permitirá também a comunicação direta com ramais das instituições internacionais que participam do projeto [20].

Além de fomentar a implantação do serviço VOIP e de seu uso efetivo para facilitar a comunicação entre as instituições, o projeto também tem o objetivo de disseminar o uso da tecnologia no país, promovendo a formação técnica de recursos humanos na área através de cursos.

A expectativa em relação ao serviço é que tenha uma qualidade comparável ao da telefonia tradicional, caracterizada pela confiabilidade e pela alta disponibilidade. Confiabilidade identifica o quão um serviço pode se manter operacional até que ocorram falhas, a qual pode ser medida pelo tempo médio entre falhas (MTBF – *Mean Time Between Failures)* e pelo tempo médio para reparo das falhas (MTTR – *Mean*

Time To Repair). Neste sentido, um serviço confiável está associado diretamente a um MTBF elevado e a um MTTR baixo. Disponibilidade pode ser definida como a proporção de tempo em que o serviço está disponível para uso.

A disponibilidade anunciada pelos fabricantes de equipamentos de telecomunicações é tradicionalmente de cinco 9's (99,999%), o que significa um tempo de paralisação de somente 5 minutos e 15 segundos por ano [21]. Em termos do serviço de telefonia, este índice de disponibilidade está associado diretamente ao serviço local envolvendo os PBXs e as centrais de comutação da concessionária. Quando o serviço envolve chamadas de longa distância, este índice pode ser menor. No Brasil, a Agência Nacional de Telecomunicações (Anatel) define uma meta para as concessionárias de ter uma disponibilidade de 98% [22], sendo que as mesmas obtiveram um índice de 99,87% em 2002[23].

No contexto de VOIP, disponibilidade pode ser definida como a probabilidade de uma chamada ser estabelecida com sucesso na primeira tentativa em que é realizada, não considerando fatores como telefone ocupado ou as chamadas não atendidas. Considerando que as chamadas realizadas com sucesso ocorrem enquanto o serviço está operacional, a disponibilidade do serviço pode ser calculada como proposto por Jiang e Schulzrinne[23]:

$$\text{Disponibilidade} = \frac{\text{\# de chamadas realizadas com sucesso}}{\text{\# de chamadas realizadas (1a. Tentativa)}}$$

Objetivando a medição da disponibilidade de um serviço VOIP operando na Internet, Jiang e Schulzrinne obtiveram um índice de 98% em testes envolvendo medições ativas, longe dos cinco 9's da telefonia tradicional, mas aceitável se comparada à da telefonia celular, normalmente entre 97% e 99% [24][1] .

A disponibilidade do serviço VOIP envolve o uso de rotas alternativas na rede IP, além da avaliação do hardware e software utilizados nos equipamentos que provêm o serviço VOIP. Em relação ao software, deve ser levado em consideração não só o tempo empregado na atualização do sistema operacional utilizado nos equipamentos envolvidos, mas também a necessidade de avaliar o funcionamento de todas as

[1] http://www.oftel.gov.uk/publications/research/2001/call_survey/results.htm#national

funcionalidades utilizadas, para que se garanta que continuam operando corretamente. Este procedimento deve ser sempre realizado, visto que não há como garantir que as modificações realizadas pelo fabricante não afetem o funcionamento das funcionalidades disponíveis nas versões anteriores dos softwares utilizados nestes equipamentos.

Outro fator importante a considerar na implantação do serviço VOIP está associado à qualidade da voz. A comutação por circuito adotada na telefonia garante uma largura de banda constante e sem variações depois que uma chamada é estabelecida, o que permite receber a voz com uma qualidade muito boa. A transmissão de voz na Internet possui características peculiares a este ambiente que devem ser consideradas. A Internet é caracterizada como um serviço de entrega de melhor esforço (*best effort*), não havendo garantias de qualidade de serviço. Esta forma de operar atende as necessidades da maior parte das aplicações em rede, entretanto, o serviço de voz sobre IP é caracterizado como uma aplicação em tempo real, exigindo padrões mínimos de desempenho, sendo sensível a alguns fatores: perda de pacotes, atrasos na entrega dos pacotes (*delay)* e variação no atraso (*jitter*) [25].

A Internet é caracterizada por apresentar canais de comunicação que apresentam taxas altas de utilização, obrigando o enfileiramento dos pacotes nas interfaces dos equipamentos de rede. Normalmente, todos os pacotes são tratados com uma política FIFO (*First In/First Out*), sem que haja um tratamento diferenciado por tipo de serviço. O congestionamento nos canais pode provocar o estouro das filas, o que leva ao descarte de pacotes. Os protocolos de transporte ou a própria aplicação cuidam para que os pacotes perdidos sejam retransmitidos. No caso da voz, a retransmissão não tem sentido, já que é uma aplicação em tempo real sensível a atrasos.

Outra conseqüência do enfileiramento é a variação no tempo de chegada dos pacotes ao destino (*jitter*), tirando-os da cadência de tempo com que foram transmitidos. *Buffers (Dejitter Buffers* ou *playout buffer)* são utilizados no receptor para compensar esta variação, permitindo a reprodução da voz com a mesma marcação de tempo com que foram transmitidos. Entretanto, um tamanho muito grande deste buffer, que permitisse grandes variações na chegada dos pacotes, provocaria um atraso na reprodução, o que afetaria a interatividade nas chamadas. Desta forma, este *buffer* só

aceita os pacotes recebidos dentro de um tempo máximo definido, os que chegarem depois serão descartados.

A perda de pacotes pode ocorrer ainda em função de falhas nos equipamentos, ou devido a erros na rede. A perda de pacotes pode ser esporádica ou pode ocorrer em rajadas, às quais as aplicações VOIP são mais sensíveis. A perda de pacotes pode ser mascarada com a utilização de vários mecanismos de *Packet loss concealment* (PLC) [26] e [27]: repetição dos últimos pacotes, interpolação a partir dos pacotes anteriores e posteriores ou predição dos pacotes perdidos. Outra opção é o envio de informações redundantes que permitam recompor as informações perdidas, *Forward Error Correction* (FEC) [28].

O atraso afeta a interatividade de uma conversa, havendo um tempo máximo aceitável para a chegada dos pacotes no destino. A recomendação ITU-T G.114 [29] define os parâmetros aceitáveis de atraso na transmissão fim-a-fim de voz: 0 a 150ms é um valor aceitável para a maioria das aplicações; 150 a 400 ms é um valor aceitável, mas deve-se estar atento ao impacto do tempo de transmissão na qualidade da aplicação; e acima de 400ms como inaceitável para a maioria das aplicações. Os atrasos ocorrem em função de alguns fatores: processamento nos *Codecs* (*coder/decoder*), montagem dos pacotes de voz que serão transmitidos, enfileiramento nas interfaces, serialização, transmissão no meio físico, latência nos equipamentos de rede e pela ação do *playout buffer* no receptor.

Os valores aceitáveis para atender o serviço VOIP podem ser resumidos em:

- a perda de pacotes dever ser no máximo de 1%;
- o atraso entre origem e destino (*one-way latency)* não deve ultrapassar 150-200 ms;
- o jitter médio não deve ser superior a 30 ms.

Uma arquitetura de serviços diferenciados [30], associada a uma política de filas que garanta um tratamento priorizado para o serviço VOIP, torna-se necessária para que a largura de banda necessária, os atrasos, o *jitter* e a perda de pacotes possam ser minimizados. O uso de filas de baixa latência (*Low Latency Queue*) especificamente para o serviço VOIP é indicado para atender este objetivo. A RFC 2598 [31]

recomenda a associação de serviços como o VOIP a um tratamento *Express Forwarding* (EF), para que na transmissão fim-a-fim possa ser garantida a largura de banda necessária, pequena perda de pacotes, pequena latência e pequeno *jitter.* Entretanto, para que este mecanismo seja efetivo, todos os equipamentos de rede envolvidos na comunicação fim-a-fim devem oferecer o mesmo tipo de tratamento, principalmente os conectados a canais congestionados. Ao utilizar o serviço VOIP através da Internet não existe esta garantia, já que nem todas as redes utilizam esta política, estando o tráfego associado, sujeito a alterações que podem influenciar a qualidade das chamadas. Estudos realizados ([32], [33] e [34]) apresentam avaliações da qualidade de serviço no uso de VOIP na Internet.

O gerenciamento de redes VOIP envolve a monitoração dos equipamentos e das condições da rede para garantir a disponibilidade do serviço e a qualidade da voz, compatíveis com as da telefonia tradicional.

O protocolo *Simple Network Management Protocol* (SNMP)[35] é padrão na gerência de redes IP. Apesar das deficiências existentes em versões anteriores do protocolo, a versão 3 apresenta características que garantem a performance e a segurança na troca de mensagens entre a estação de gerência e os dispositivos que serão gerenciados.

No uso de SNMP, devem ser avaliadas as informações de gerenciamento disponíveis na MIB (*Management Information Base*) do equipamento gerenciado, assim como os alarmes ou notificações que podem ser emitidas para identificação de problemas.

A qualidade da voz pode ser obtida através da avaliação subjetiva das chamadas utilizando o método para o cálculo do *Mean Opinion Score* (MOS), como recomendado pelo ITU-T [36]. Um grupo de pessoas avalia a qualidade da voz nas chamadas realizadas através do sistema em teste, MOS é a média obtida das notas atribuídas pelo grupo, a qual varia de 1 (péssimo) a 5 (ótimo). Cole e RosenBluth [37] descrevem um método para monitorar a qualidade da voz através da Internet baseado no *E-Model*, um modelo analítico para estimar a qualidade da voz definido na recomendação ITU-T G.107 [38]. Com base no número de pacotes perdidos, no atraso medido e no *Codec*

utilizado, é empregado o *E-Model* para calcular o fator-R como estimativa da qualidade de voz. Este fator varia em uma escala de 0 100, mas pode ser comparado ao MOS, como apresentado na Figura 1-1. Os valores necessários ao cálculo do fator-R podem ser deduzidos através de monitoração passiva ou não intrusiva, que os obtém da observação dos fluxos associados às chamadas em curso; ou através de monitoração ativa ou intrusiva, onde são avaliadas as condições associadas ao tráfego injetado na rede especificamente para os testes.

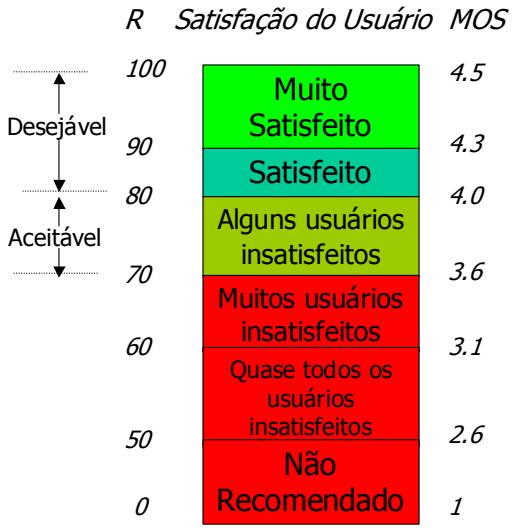


Figura 1-1 – Comparação de valores do fator R com MOS

A contabilização dos recursos consumidos em cada chamada pode ser obtida através de SNMP. Entretanto, para que esta coleta pudesse ser efetuada haveria a necessidade de monitorar constantemente os agentes, para identificar as chamadas ativas e as que terminaram, e coletar as informações pertinentes. O protocolo *Remote Authentication Dial In User Service* (RADIUS)[39] originalmente utilizado para autenticar usuários que faziam acesso aos provedores Internet através de acesso discado, foi estendido e adaptado para uso com serviço VOIP para prover informações sobre os recursos consumidos nas chamadas [40].

A avaliação das chamadas realizadas, além de ser utilizada para fins estatísticos e de contabilização das chamadas, poderá ser usada para a identificação de problemas. A definição de uma estratégia que permita recolher informações sobre as chamadas realizadas e a correlação das causas que forçaram o término ou que tenham impedido o estabelecimento das chamadas, também poderá auxiliar na identificação de problemas.

Neste aspecto, serão analisadas neste trabalho, informações que podem ser obtidas através dos protocolos SNMP e *Radius*.

O primeiro objetivo deste trabalho é apresentar uma proposta que indique as configurações a utilizar e a solução de alguns problemas que podem ser encontrados para a implantação de uma rede VOIP. Esta proposta será utilizada no projeto-piloto VOIP a ser implantado pela RNP.

Após a operacionalização do serviço, há a necessidade de implantar uma ferramenta para o gerenciamento dos equipamentos e do serviço VOIP que será oferecido, com especial atenção à qualidade das chamadas realizadas. A identificação de problemas nas chamadas em curso pode disparar mecanismos que permitirão melhorar a qualidade do serviço ou pode ser utilizada para mapear problemas na rede que possam estar afetando as chamadas. Novas chamadas VOIP podem ser recusadas caso a rede não garanta a qualidade das chamadas.

Ferramentas orientadas ao gerenciamento do serviço VOIP são normalmente fornecidas por empresas como a Cisco[2], que além do alto custo envolvido, apresentam soluções fechadas que não permitem adaptações a necessidades específicas. Não foram encontradas ferramentas de código aberto que pudessem ser adaptadas às necessidades do projeto que será implementado.

O segundo objetivo deste trabalho é especificar uma metodologia que defina o que deve ser gerenciado e de onde podem ser obtidas as informações necessárias, que servirá de base para o desenvolvimento de uma ferramenta de código aberto e disponível a outras instituições, que possibilite a gerência de uma rede VOIP.

Uma dificuldade no uso do protocolo SNMP é encontrar de forma centralizada um detalhamento das informações de gerenciamento que estão disponíveis nas MIBs dos equipamentos monitorados, assim como as notificações que podem ser ativadas nestes agentes para a sinalização de problemas. A identificação das variáveis, como se relacionam e das notificações que podem ser geradas por cada equipamento facilita a definição da estratégia a adotar no gerenciamento dos dispositivos com o uso do SNMP.

---

[2] http://www.cisco.com/en/US/products/sw/cscowork/index.html

O terceiro objetivo deste trabalho é identificar estas MIBs, com a finalidade de gerenciar os equipamentos utilizados no projeto e o serviço VOIP, servindo de base para a ferramenta proposta. Ao longo do trabalho foi feito um levantamento das fontes de onde podem ser coletadas as informações de gerenciamento específicas para o serviço VOIP, visto não que não existe na literatura uma fonte que reúna e discuta como obtê-las. Serão detalhadas MIBs especificadas pelo IETF, pelo ITU-T e pelos fabricantes.

Este trabalho visa estudar aspectos associados ao gerenciamento do serviço VOIP, buscando a implantação deste serviço na RNP de forma escalável, considerando a participação de um número crescente de instituições. Experiências relatadas na montagem dos projetos-piloto da República Tcheca[3][41], da Alemanha[4][17] e da Austrália[5] [42] e [43] serão utilizadas como base para este trabalho.

1.3 Organização da tese

O trabalho está dividido em 6 capítulos. No capítulo 2, são apresentados os cenários possíveis na implementação de voz sobre IP, com uma descrição dos padrões em sinalização VOIP padronizados, em especial a recomendação ITU-T H.323.

O capítulo 3 é dedicado ao detalhamento do projeto-piloto que será implementado, com uma descrição dos componentes utilizados, plano de numeração, características das portas de voz, sinalização adotada para interligar os *gateways* de voz aos PBXs, os problemas existentes e como serão contabilizadas as chamadas.

No capítulo 4, são avaliados os mecanismos que podem ser utilizados no gerenciamento dos equipamentos e das chamadas VOIP. As MIBs definidas pelo ITU-T, pelo IETF e pelos fabricantes são avaliadas para identificar as informações que podem auxiliar o gerenciamento de redes VOIP. As informações disponibilizadas através do Radius também são apresentadas, incluindo as informações específicas definidas pelos fabricantes.

[3] http://www.ces.net/project/iptelephony/
[4] http://bsd.rrze.uni-erlangen.de/~fd/voip_en.html
[5] http://www.aarnet.edu.au/rd/voip/index.html

O capítulo 5 apresenta uma descrição de um sistema integrado para gerenciamento de redes VOIP, em especial do que será utilizado na gerência do projeto-piloto. São apresentadas as fontes de informações que serão empregadas no gerenciamento de configuração, contabilidade de recursos consumidos, de falhas e de performance associadas ao serviço. As notificações enviadas para alertar situações anormais específicas também são discutidas.

O capítulo 6 apresenta as conclusões e oferece sugestões de estudos futuros com o objetivo de dar continuidade a este trabalho.

Capítulo 2

Implementação de Voz sobre IP (VOIP)

O uso da tecnologia VOIP oferece uma série de cenários para os usuários do serviço, como pode ser visto na Figura 2-1.

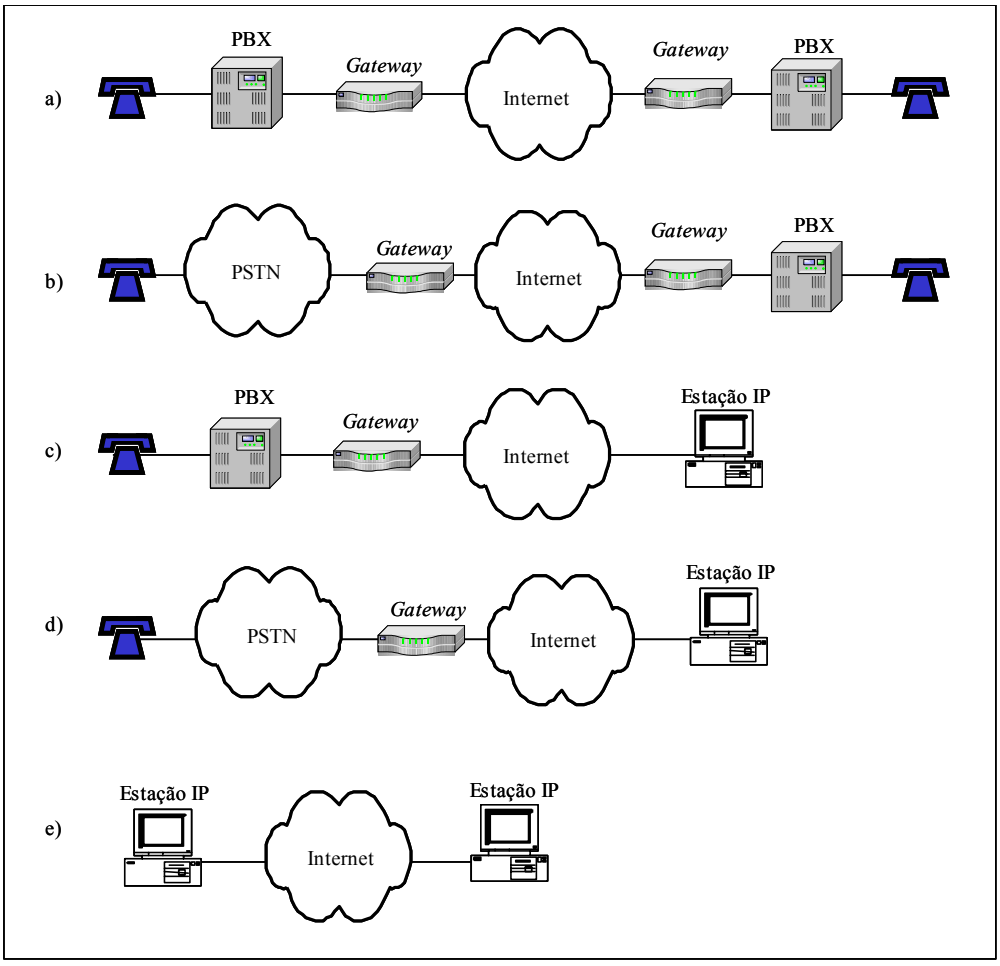


Figura 2-1 – Cenários possíveis no uso do serviço VOIP

No cenário (a), uma chamada é realizada da partir de um ramal para um outro em uma localidade remota interligada através da Internet. Este cenário reduz a zero o custo com telefonia em chamadas realizadas entre localidades que utilizem apenas acesso Internet. O uso de VOIP não implica em mudanças na conectividade da rede com a Internet. Entretanto, aplicações VOIP requerem uma largura de banda relativamente

pequena, porém constante, variando entre 20 e 100 Mbps [6] dependendo da compressão de voz utilizada. Neste caso, é recomendado que as conexões com a Internet tenham banda suficiente e que operem com QoS para garantir as necessidades requeridas para manter a qualidade da voz, considerando o número de ligações previsto nestes enlaces. Visto que a Internet em geral não oferece garantia para voz, a qualidade da ligação fim-a-fim vai depender dos diversos *backbones* Internet trafegados, bem como das boas condições de latência e perda nos pontos de troca de tráfego entre as redes. Exceto numa rede corporativa, o serviço VOIP ainda não consegue a garantia fim-a-fim necessária. No cenário (b), a chamada é realizada da rede pública de telefonia para um ramal de uma localidade remota. Neste cenário há uma redução no custo com ligações de longa distância. Nos dois cenários seguintes (c) e (d), uma ligação é realizada de um ramal telefônico, ou da telefonia pública, para uma estação com uma aplicação VOIP residente. Este ambiente amplia o número de usuários com acesso ao serviço de telefonia, pois permite estender o serviço de telefonia até localidades onde não existam telefones disponíveis, mas haja uma estrutura de rede de dados funcionando. No último cenário (e), é apresentado um ambiente onde as chamadas podem ser realizadas entre estações que têm uma aplicação VOIP residente. Em todos os cenários, também é possível iniciar as chamadas no sentido oposto.

Com exceção do último cenário, em todos os outros há a necessidade de se utilizar um *gateway*, responsável pela adaptação da sinalização e da voz da telefonia tradicional, para a sinalização e fluxos de mídia utilizados em redes VOIP. Na conexão com a rede de telefonia podem ser utilizados ramais analógicos ou troncos digitais. No primeiro caso, o sinal de voz recebido é analógico, enquanto que no segundo, já se encontra convertido para o formato digital (PCM 64Kbps). Na adaptação para VOIP, o *gateway* será responsável pelas funções descritas a seguir.

A sinalização de linha é utilizada para indicar o início, o atendimento e o término das chamadas. A sinalização recebida do PBX deve ser repassada ao destino da chamada através da sinalização de chamadas do VOIP. O destino pode ser um terminal VOIP ou um *gateway* conectado a um PBX remoto e, neste caso, a sinalização VOIP é convertida de volta para a empregada na rede de telefonia. Além da sinalização de linha

[6] Inclui os cabeçalhos RTP, UDP e IP.

é utilizada uma sinalização acústica para indicar ao usuário o estado de operação do sistema telefônico, onde é informado através de sinais específicos na linha o tom de sinal de discar (*dial tone*), a indicação de uma nova chamada (*ring tone*), a indicação de que o usuário remoto está sendo sinalizado de uma nova chamada (*ring back tone*) e linha ocupada (*busy tone*), entre outros. Esta sinalização é transmitida no canal de áudio, sendo codificado e transmitido junto com a voz.

Um plano de numeração definido no *gateway* será utilizado para identificar o destino da chamada. Este destino pode ser um *gateway* remoto, uma estação VOIP ou o próprio PBX ao qual o *gateway* está conectado. Na rede VOIP, estes dígitos codificados em *Dual Tone Multi Frequency* (DTMF) podem ser repassados para o destino, sendo prevista a sua transmissão no mesmo canal que a voz ou através da sinalização. A última opção é a mais indicada por não sofrer distorções, a que o canal de áudio está sujeito no processo de codificação e decodificação da voz.

O *gateway* deve receber a voz da rede de telefonia e codificá-la para a transmissão através da rede IP. O objetivo é tentar obter a maior compressão possível no sinal a ser transmitido, devendo-se levar em consideração que esta compressão provoca um atraso na transmissão, e que a codificação e a conseqüente decodificação no destino, envolvem um processamento complexo. Vários algoritmos podem ser utilizados para este fim, onde o objetivo é prover a melhor qualidade da voz, utilizando a menor taxa de transmissão, o menor atraso e a menor complexidade de implementação possível. Os *Codecs* (Codificador/Decodificador) são os responsáveis em codificar e decodificar os sinais utilizando um algoritmo específico. Nas chamadas VOIP é possível utilizar várias opções de *Codec,* os dois dispositivos envolvidos negociam qual deve ser utilizado. Na Tabela 2-1 são apresentadas as características de alguns *Codecs* utilizados, os valores associados ao processamento e a qualidade de voz foram obtidos de artigos de Cox e Peter [44] e de Perkins *et al.* [45]. A taxa de transmissão mostrada na tabela se refere apenas à taxa do *Codec,* não levando em consideração os cabeçalhos dos protocolos dos níveis inferiores.

Tabela 2-1 – Características de Codecs utilizados em dispositivos VOIP

Codec	Taxa de transmissão (kbps)	Tamanho do quadro (mseg)	Processamento (MIPS)	Qualidade da VOZ (MOS)
G.711 (PCM)	64	0.125	> 0.5	4.10
G.726 (ADPCM)	16/24/32/40	0.125	2	3.85
G.728 (LD-CELP)	16	0.625		3.85
G.729 (CS-ACELP)	8	10	20	3.92
G.729A (CS-ACELP)	8	10	10.5	3.7
G.723.1 (MP-MLQ)	6.3	30	14.6	3.9
G.723.1 (ACELP)	5.3	30	16	3.65

2.1 Sinalização

Na rede VOIP, assim que o usuário disca um número de telefone, ou faz uso de um *alias* (nome associado a um número), é necessária uma sinalização que determine inicialmente o estado do dispositivo remoto chamado (*called party*), indicando se o mesmo está ocupado ou disponível. Caso esteja disponível, a sinalização será responsável por estabelecer a chamada. Quando um dos usuários desliga, a sinalização será utilizada para terminar a chamada e liberar os recursos alocados.

Três padrões são utilizados na sinalização em redes VOIP: a recomendação H.323 do ITU-T (*International Telecommunication Union – Telecom standardization*) [13], o protocolo SIP (*Session Initiation Protocol*) do IETF (*Internet Engineering Task Force*) [14] e a recomendação H.248 do ITU-T [46].

A recomendação H.323 compreende um conjunto de protocolos utilizados para a realização de conferências multimídia utilizando vídeo, voz e dados em rede de pacotes, onde não há garantia em relação à qualidade do serviço (QoS). A primeira especificação do H.323 foi aprovada em 1996, mas os primeiros *drafts* da série H.32x foram

aprovados no início dos anos 90. A segunda versão, aprovada em janeiro de 1998, além da correção de problemas associados à primeira especificação, trouxe novas funcionalidades que permitiram o uso do H.323 em redes WAN (*Fast Start e H.245 Tunneling).* Podemos ainda destacar o suporte à segurança, à QoS (*Quality of Service*) e à disponibilidade (*alternate gatekeepers*). Novas versões de H.323 têm sido aprovadas desde então, agregando novas funcionalidades. A versão 3 foi aprovada em maio de 1999, a versão 4 em novembro de 2000 e a versão 5 em julho de 2003.

Os equipamentos utilizados em redes H.323 incluem terminais, gateways, *Multipoint Control Units* (MCU) e *gatekeepers*, como descrito no tópico 2.2. Os três primeiros são chamados *endpoints* H.323 pois podem iniciar e receber chamadas H.323.

A recomendação H.323 define um conjunto de protocolos que são utilizados para fins de sinalização das chamadas (H.225) e controle dos canais de mídia (H.245), como descrito no tópico 2.3. O tráfego associado à mídia é transportado utilizando o protocolo *Real-Time Protocol* (RTP).

O protocolo SIP foi desenvolvido inicialmente dentro do grupo de trabalho MMUSIC (*Multiparty Multimedia Session Control*) do IETF. Posteriormente, um grupo de trabalho específico em SIP acabou sendo criado. SIP é um protocolo de aplicação baseado em texto, que utiliza o modelo "requisição-resposta", similar ao HTTP, para iniciar sessões de comunicação interativa entre usuários. Na Figura 2-2, pode ser visto um exemplo da sinalização estabelecida entre dois terminais SIP. Tais sessões incluem vídeo, voz, *chat*, mensagens instantâneas, jogos interativos e realidade virtual. A descrição das características da sessão, tais como os *Codecs* utilizados e endereços associados aos fluxos de mídia, é realizada pelo protocolo SDP (*Session Description Protocol*).

O protocolo SIP é especificado na RFC 2543, que passou ao estado de padrão proposto (*proposed standard)* em março de 1999. O protocolo SIP segue uma arquitetura cliente/servidor. Os dois terminais envolvidos são chamados de *user agent*s (UA), responsáveis em originar ou terminar requisições SIP, atuando como clientes ou servidores SIP, respectivamente. Opcionalmente, além dos agentes podem ser utilizados servidores procuradores (*proxy servers*), atuando como intermediários no

encaminhamento de mensagens SIP e dos fluxos de mídias entre dois agentes. Esses têm funções adicionais associadas a autenticação e autorização de uso do serviço, que são essenciais quando é necessária a contabilização das chamadas. O uso de *proxies* facilita a implementação da segurança da rede. Outros componentes podem ser utilizados para facilitar o encaminhamento de chamadas (*redirect server*) e a localização de usuários (*registrar server*).

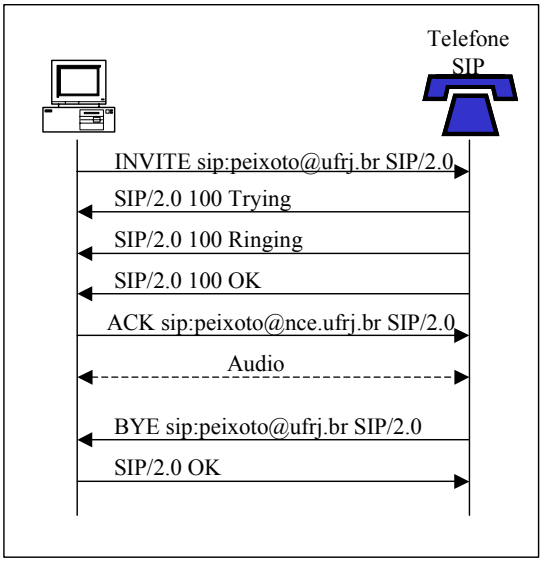


Figura 2-2 – Sinalização entre dois terminais SIP

O protocolo MGCP (*Media Gateway Control Protocol*) foi proposto pelo grupo de trabalho *Megaco* (*Media Gateway Control*) do IETF, objetivando uma integração da arquitetura SS#7, adotada em redes de sinalização na telefonia tradicional, com redes IP, Frame Relay e ATM. Em uma evolução do MGCP, o trabalho cooperativo de grupos do ITU-T e do IETF resultou na recomendação H.248, definida também como protocolo Megaco (IETF), através da RFC3015 [47].

Media Gateways (MG) convertem a mídia entre os vários tipos de rede a que podem estar conectados. Enquanto no H.323 o *gateway* participa ativamente da sinalização, no MGCP esta função é dissociada do *gateway* e passa a ser realizada pelo MGC (*Media Gateway Controller*), também chamado de *softswitch*. Este equipamento pode controlar vários MGs. O principal objetivo do MGCP era a decomposição da arquitetura H.323 para que, de forma semelhante às redes SS#7, haja uma rede de pacotes empregada exclusivamente para o transporte da sinalização, a qual será utilizada

para controlar os comutadores por onde trafega a voz. O H.248 é um protocolo "*master*/*slave*", onde o MGC tem um controle total sobre os elementos da rede e o MG apenas executa os comandos recebidos, como apresentado na Figura 2-3. Ele contrasta com o H.323 e com o SIP, protocolos "*peer-to-peer*", onde os clientes podem estabelecer sessões diretamente com outros clientes.

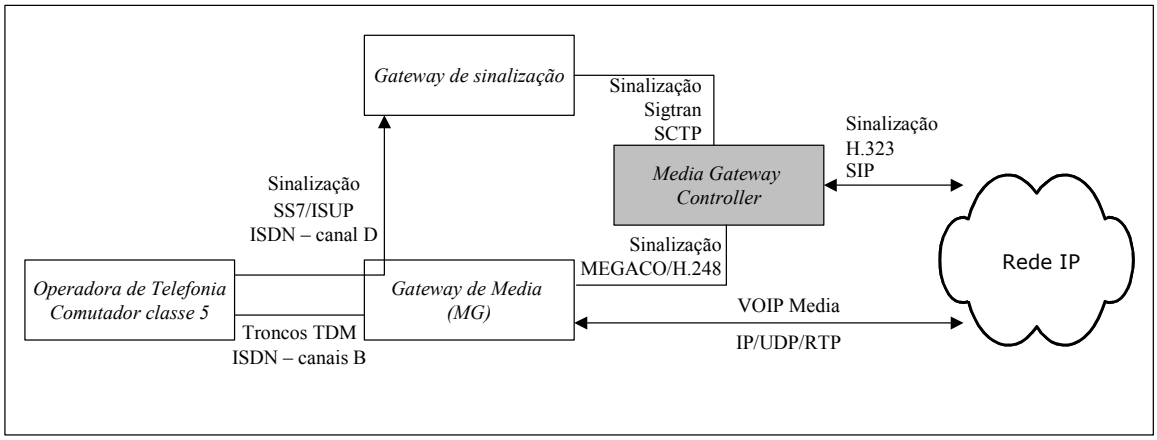


Figura 2-3 – Arquitetura H.248/Megaco

O protocolo H.248 é considerado complementar ao H.323 e ao SIP. Nele um MGC irá controlar um MG usando H.248, mas irá se comunicar com outros utilizando H.323 ou SIP. A comunicação entre MGCs não é definida no H.248/*Megaco*. Na Figura 2-3 pode ser vista a arquitetura do Megaco. Além dos MGs e dos MGCs, é utilizado um *gateway* que a tem responsabilidade de terminar a sinalização proveniente da rede de telefonia e transportá-la para o MGC através do protocolo SigTran (*Signaling Translation*).

Estes três protocolos têm similaridades, uma vez que têm o objetivo comum de prover uma comunicação VOIP. Eles diferem somente na localização da "inteligência", ou seja, onde é realizado o processamento [3]: no H.323, a inteligência é distribuída por todos os elementos que compõem a rede (terminais, *gateways, gatekeepers* e *MCUs*); no SIP, a inteligência fica restrita aos dispositivos terminais (*endpoints*) das chamadas; e no H.248, a inteligência fica na rede (MGCs), não sendo feito qualquer processamento nos *gateways* (MGs).

O protocolo H.248/Megaco é indicado para redes com grandes quantidades de *gateways,* operando com grandes quantidades de portas, e onde haja a necessidade de integração com redes SS#7. Em redes de menor porte e onde haja a necessidade de comuniação *peer-to-peer*, os protocolos H.323 e SIP são os indicados. O protocolo SIP, por ter sido definido pela comunidade IP, apresenta características que o adaptam facilmente para novas aplicações na Internet. O H.323, por ter sido desenvolvido pela comunidade de telecomunicações, tem uma melhor interação com a telefonia tradicional. O H.323 foi definido com o objetivo de prover um sistema unificado que permitisse comunicação multimídia envolvendo voz, vídeo e dados. A arquitetura é bem definida em relação aos componentes e à sinalização. O H.323 apresenta também procedimentos definidos para um melhor gerenciamento do serviço e recuperação em caso de falhas. O SIP especifica um protocolo de sinalização aberto. Conseqüentemente, as implementações podem variar, não sendo totalmente compatíveis.

Na prática, um grande número de redes VOIP utiliza o protocolo H.323 devido à grande disponibilidade de produtos H.323 no mercado, ao maior número e estabilidade de implementações, ao foco na integração com a rede de telefonia e às facilidades associadas ao gerenciamento do serviço e das chamadas. Entretanto, vem sendo ampliado o número de produtos e aplicações que utilizam o SIP.

Este trabalho tem por objetivo a discussão de mecanismos associados à gerência de redes VOIP que utilizam o protocolo H.323.

2.2 Arquitetura H.323

A recomendação H.323 define uma arquitetura para estabelecer uma comunicação multimídia em redes de pacotes que não tenham suporte a qualidade de serviço (QoS). O H.323 é um documento base que faz referência a um conjunto de protocolos e formatos de mensagens definidos em outros documentos, e explica como os vários protocolos interagem com os vários elementos que compõem a arquitetura. Na Tabela 2-2 são apresentadas as recomendações do ITU-T definidas para dar suporte a sinalização H.323.

Tabela 2-2 – Recomendações ITU-T que dão suporte à sinalização H.323

Recomendação ITU	Título
H.225.0	Call Signaling Protocols and Media Stream Packetization for Packet-Based Multimedia Communication Systems
H.235	Security and Encryption for H-Series Multimedia Terminals
H.245	Control Protocol for Multimedia Communication
H.350.x	Directory Services Architecture for Multimedia Conferencing
H.450.x	Supplemental Services for H.323
H.460.x	Guidelines for the Use of the Generic Extensible Framework
Série T.120	Data Protocols for Multimedia Conferencing

Além das funções de sinalização, a arquitetura H.323 incorpora vários formatos associados à mídia transmitida em fluxos específicos, como apresentado na Tabela 2-3. Em redes VOIP, os fluxos associados à transmissão do áudio são encaminhados utilizando-se o protocolo RTP.

Tabela 2-3 – Formatos de mídia reconhecidos na arquitetura H.323

Mídia	Formatos
Áudio	G.711, G.722, G.723.1, G.728, G.729, GSM, ISO/IEC 11172-3
Vídeo	H.261, H.262, H.263
Dados	Série de recomendações T.120

A arquitetura H.323 especifica quatro componentes básicos: terminais, *gatekeepers* (GK), *gateways* (GW) e *multipoint control units* (MCU).

2.2.1 Terminais H.323

O terminal H.323 equivale a um telefone incrementado com uma série de funcionalidades, que embute obrigatoriamente recursos para a transmissão de áudio e, opcionalmente, pode incluir recursos para a transmissão de vídeo e o compartilhamento de dados. Os terminais são configurados com uma interface de rede e são operados diretamente pelo usuário.

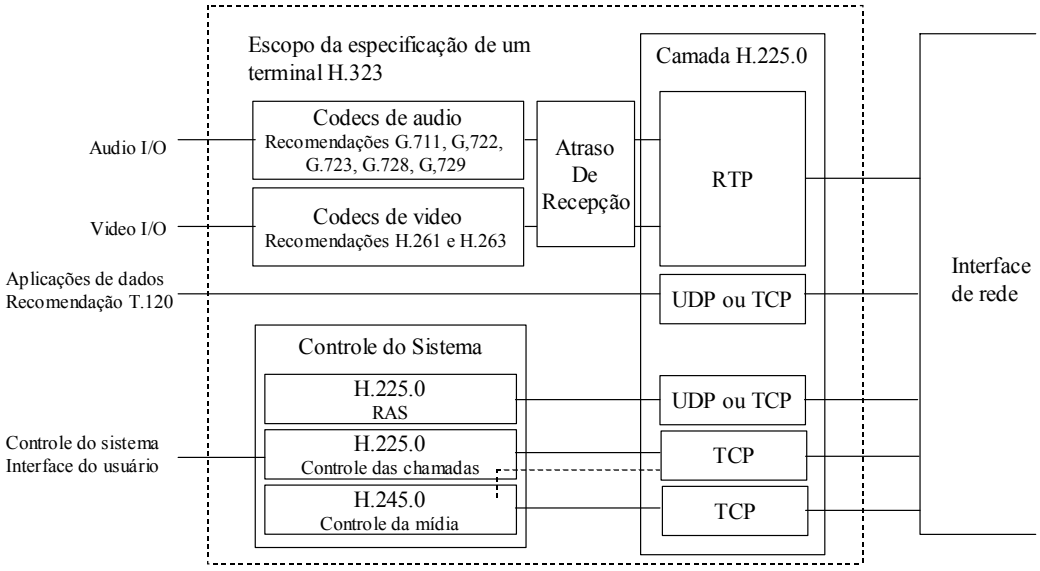


Figura 2-4 – Elementos funcionais do terminal H.323

A Figura 2-4 apresenta os elementos funcionais de um terminal H.323. A camada H.225.0 formata os fluxos de vídeo, áudio, dados e de controle em mensagens que são transmitidas através da interface de rede, e recuperam os fluxos de mensagens recebidas da rede. Esta camada é responsável pelo enquadramento, pelo sequenciamento de mensagens e pela detecção de erros na transmissão e recepção de fluxos de mídia e de controle. Em redes VOIP, estas funções são realizadas pelos protocolos IP/UDP/RTP para a transmissão do áudio e pelos protocolos IP/TCP na transmissão dos fluxos de controle.

Todos os terminais H.323 precisam implementar o protocolo H.225, que define um conjunto de mensagens para a sinalização das chamadas (Q.931) e para a comunicação com o *gatekeeper* (RAS). A sinalização é utilizada para o estabelecimento (*setup*), término (*teardown*) e controle das chamadas. Outro componente necessário é o protocolo H.245, utilizado na sinalização dos canais de mídia, onde são negociadas as capacidades suportadas pelos dois dispositivos H.323 e iniciados os canais lógicos por onde serão transmitidos os fluxos de mídia (Figura 2-5).

O terminal H.323 deve dar suporte ainda aos protocolos RTP e RTCP utilizados para a transmissão da mídia e para o monitoramento da qualidade da chamada, respectivamente.

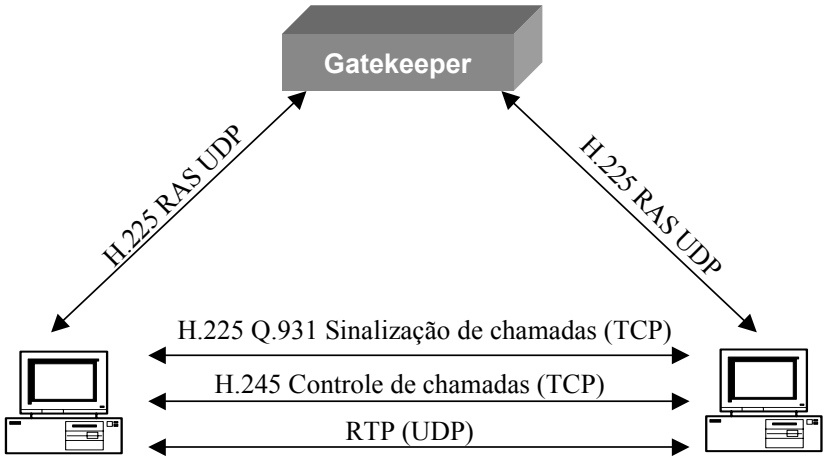


Figura 2-5 – Sinalização e fluxos de mídia H.323 com uso de gatekeeper

Os fluxos RTP podem ser unidirecionais ou bidirecionadas, depende como for negociado na sinalização. De qualquer forma, sempre existem dois canais de mídia, um para cada sentido da conversação. Em cada sentido há uma conexão RTCP associada, através da qual a estação receptora do fluxo de mídia reporta diversas informações associadas à QoS do fluxo RTP recebido. Analisando essas informações é possível avaliar a perda de pacotes, o atraso e o *jitter* associado a cada um dos fluxos. Como as condições da rede podem ser diferentes nos dois sentidos, pode haver problemas em um sentido e no sentido contrário não existir qualquer alteração. A avaliação da qualidade das chamadas pode ser realizada analisando estas informações.

2.2.2 *Multipoint Control Units* (MCU)

O *Multipoint Control Unit* (MCU) dá o suporte necessário a conferências envolvendo mais de dois dispositivos em redes H.323. O MCU consiste de um *Multipoint Controller* (MC) e de zero ou mais *Multipoint Processors* (MP). O MC manipula a negociação H.245 com todos os dispositivos que vão participar de uma conferência, identificando as capacidades de áudio e vídeo comuns a todos, determinando assim o modo de comunicação a ser adotado (SCM – *Selected Communications Mode*). O protocolo H.245 é utilizado ainda para verificar se os dispositivos envolvidos suportam comunicação *multicast*. Cada conferência estabelecida é associada somente a um MC. Cada dispositivo H.323 estabelece uma sessão bidirecional com o MC.

O MP é responsável por converter a mídia para diferentes formatos, por exemplo, de G.711 para G.723.1, ou por combinar o áudio proveniente de várias fontes, transmitindo o fluxo combinado para todos os dispositivos.

As conferências H.323 podem ser descentralizadas ou centralizadas. As descentralizadas dependem do suporte à transmissão *multicast* nos dispositivos envolvidos, já que os fluxos de mídia para os dispositivos associados à conferência serão transmitidos utilizando-se este tipo de endereçamento. Nas conferências centralizadas, todos os fluxos de mídia são transmitidos para o MCU que, por sua vez, os retransmite para todos os dispositivos que participam da conferência. Neste caso, a transmissão pode ser realizada utilizando-se endereçamento *unicast* ou *multicast*, ou ambos.

2.2.3 Gateways

A principal função do *gateway* é prover a interconexão entre redes que não utilizam o protocolo H.323, tais como redes RDSI (Rede Digital de Serviços Integrados) que utilizam o protocolo H.320 para a realização de conferências multimídia e a rede de telefonia tradicional.

O *gateway* realiza funções como a tradução da sinalização utilizada para o estabelecimento e término de chamadas e a conversão do formato da mídia de uma rede para a outra.

O *gateway* é tratado na rede H.323 como mais um dispositivo H.323, implementando os protocolos para a sinalização de chamadas (H.225), sinalização de canais de mídia (H.245) e transmissão da mídia (RTP/RTCP) em chamadas realizadas com outros *gateways,* terminais ou MCUs.

Em redes VOIP, os *gateways* são configurados com portas de voz para conexão a PBXs e comutadores de telefonia. Várias alternativas de conexão são possíveis, variando conforme o tipo de porta disponível no PBX e no *gateway*. O capítulo 3 explora as várias alternativas de conexão, permitindo a realização de chamadas da rede de telefonia, inclusive da telefonia pública, para terminais H.323 na rede IP, ou vice-

versa. O uso de dois ou mais *gateways* permite a realização de chamadas entre ramais de PBXs diferentes, utilizando-se a rede IP como transporte, em substituição à rede de telefonia pública.

O *gateway* deve ter informações suficientes do plano de numeração em uso na rede VOIP, para que possa encaminhar as chamadas com base no número E.164[7] discado pelo usuário que iniciou a chamada. As chamadas recebidas são encaminhadas de acordo com o número E.164 recebido através da sinalização de chamada (*Setup* H.225), no caso do VOIP, ou do endereço E.164 discado, no caso da telefonia. As chamadas podem ser destinadas a telefones tradicionais ou a dispositivos H.323; o *gateway* deve saber como encaminhá-las. A arquitetura H.323 pressupõe a existência de um *gatekeeper*, elemento que auxilia na localização do destino.

2.2.4 Gatekeepers

O *gatekeeper* (GK) é o principal elemento na arquitetura H.323, onde regula que dispositivos podem iniciar ou receber chamadas. Uma das principais diferenças do H.323 em relação ao protocolo SIP, é que no SIP não existe um dispositivo definido explicitamente para o controle de acesso aos recursos da rede.

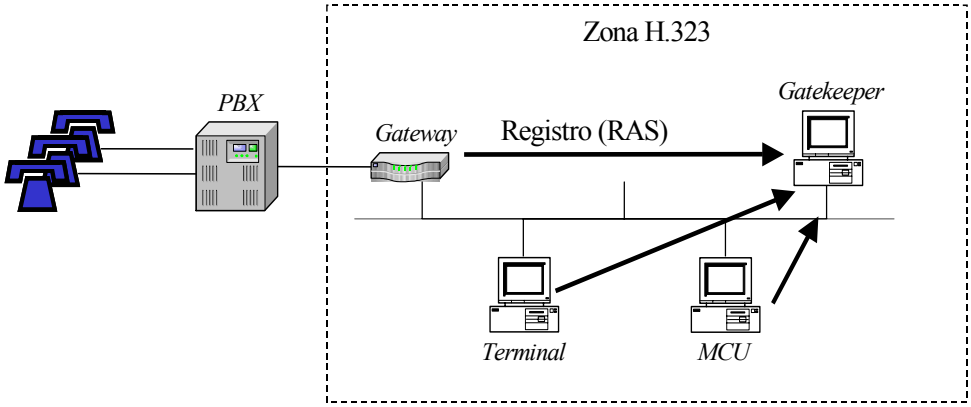


Figura 2-6 – Zona H.323

A arquitetura H.323 utiliza o conceito de "zona", que compreende um GK e todos os dispositivos H.323 que este controla, como visto na Figura 2-6. Os dispositivos H.323 utilizam o protocolo RAS (*Registration, Admission and Status*) para se registrar

[7] O padrão ITU-T E.164 define a numeração empregada em redes públicas de telefonia

no GK, através da mensagem RRQ (*Registration Request*). Recebem como resposta uma mensagem positiva, com um RCF (*Registration Confirm*), ou não, com um RRJ (*Registration Reject*).

O GK deve prover a todos os dispositivos registrados os serviços de controle de admissão (*admission control*), tradução de endereços (*address translation*) e controle de largura de banda (*bandwidth control*).

Qualquer chamada realizada a partir de terminais e *gateways* deve ser autorizada pelo GK. Antes de iniciar qualquer chamada, o dispositivo H.323 utiliza o protocolo RAS para solicitar autorização ao GK para realizar a chamada. São usadas para este fim, as mensagens ARQ (*Admission Request*), ACF (*Admission Confirm*) e ARJ (*Admission Reject*). Os critérios que devem ser utilizados pelo GK para autorizar uma chamada não são especificados no H.323, ficando a critério da implementação. Pode ser utilizado, por exemplo, um sistema pré-pago, em que as chamadas só são autorizadas se o usuário ainda tiver crédito disponível. Restrições para determinadas faixas de telefones também podem ser adotadas como, por exemplo, permitir ligações para celulares somente a usuários específicos.

As conexões entre dispositivos H.323 são realizadas com base no endereço de rede e no identificador TSAP (*Transport Service Access Point*). Em redes IP, o endereço de rede é um endereço IP e o identificador TSAP é um número de porta TCP ou UDP. O uso de apelidos (*aliases*) facilita a identificação de dispositivos H.323 para os usuários do serviço. Estes podem ser identificadores H.323 (H.323-ID), representados por uma seqüência qualquer de caracteres, ou endereços E.164, numeração adotada na telefonia. No momento em que solicita o registro no GK, o dispositivo informa os apelidos e o endereço que o identificam. Ao iniciar uma chamada, o terminal envia no pedido de admissão, o apelido do terminal que está sendo chamado. Com base nas informações que dispõe, o GK traduz o apelido para um endereço IP e número de porta TCP, que serão utilizados para alcançar o terminal destino. A partir desta informação, pode ser iniciada a sinalização H.225 para estabelecer a chamada. Os *gateways* registram no GK, informações sobre os prefixos associados ao PBX em que estão conectados, de forma que todas as chamadas direcionadas a ramais utilizando o prefixo registrado sejam direcionadas ao *gateway*.

O *gatekeeper* deve estar preparado para controlar a banda alocada a uma chamada. Por exemplo, havendo uma mudança do *Codec* utilizado, pode haver uma mudança na banda necessária para os fluxos de mídia. O pedido de mudança deve ser solicitado ao GK através do protocolo RAS. Havendo limitação na largura de banda alocada ao serviço VOIP, o pedido pode ser aceito, ou não. São utilizadas para este fim, as mensagens BRQ (*bandwidth request)*, BCF *(bandwidth confirm)* e BRJ (*bandwidth reject*).

Opcionalmente, o *gatekeeper* pode realizar o gerenciamento da largura de banda alocada ao serviço, onde novas chamadas somente serão admitidas se existir banda disponível. Caso não haja, as chamadas serão rejeitadas ou direcionadas para *gatekeepers* alternativos. Desta forma, é possível implementar o serviço VOIP sem causar prejuízos às outras aplicações na rede. O uso de *gatekeepers* alternativos pode ocorrer também no caso de sobrecarga provocada por um número muito grande de chamadas. Esta facilidade garante o uso do serviço H.323 em redes de grande porte.

O *gatekeeper* pode manter uma lista das chamadas ativas, de forma que possam ser identificados os terminais ocupados e para prover informações necessárias ao gerenciamento da largura de banda.

A sinalização de chamadas (H.225), o controle de canais associados à mídia (H.245) e os próprios canais de mídia (RTP/RTCP) são normalmente estabelecidos diretamente entre o dispositivo que realiza a chamada e o que é chamado, após receber a confirmação do pedido de admissão do *gatekeeper*. Este modo de operação é chamado de *Direct Call Signaling*. Alternativamente, o *gatekeeper* pode intermediar a sinalização entre os dispositivos envolvidos, quando opera no modo *gatekeeper routed call signaling*. Neste modo, a sinalização H.225 passa a ser estabelecida entre o dispositivo que inicia a chamada e o *gatekeeper*, que a repassa ao dispositivo chamado, ou ao *gatekeeper* onde dispositivo chamado está registrado. Este procedimento facilita a implementação de mecanismos de segurança na rede, já que apenas o gatekeeper precisará ter visibilidade direta da Internet.

O *gatekeeper* é um dispositivo que tem controle sobre as chamadas realizadas ou recebidas pelos dispositivos na “zona” sob sua responsabilidade, sendo uma importante

fonte de informações que podem ser utilizadas para fins de contabilização de chamadas e bilhetagem. Apesar de dois dispositivos poderem estabelecer chamadas entre si sem o uso de *gatekeepers*, esta opção deve ser evitada para não afetar o gerenciamento do serviço, principalmente ao se usar *gateways*.

A política de segurança normalmente adotada nas redes corporativas acaba gerando problemas para o uso do protocolo H.323. As máquinas internas normalmente não são alcançáveis a partir da Internet, o estabelecimento de uma conexão TCP só ocorre quando iniciada a partir das máquinas internas. Outro problema está associado aos canais de mídia, que utilizam portas TCP diferentes a cada chamada realizada. A solução para facilitar o uso de H.323 através da Internet e a configuração dos *firewalls,* é o emprego do *gatekeeper* como *proxy* para o tráfego RTP. Com esta configuração, todo o tráfego de mídia da rede interna para a Internet, e vice-versa, é realizado através do *gatekeeper*. Na realidade, o *gatekeeper* estabelece duas chamadas, uma com a máquina interna e outra com a externa, intermediando todo o tráfego entre as duas e realizando as adaptações necessárias na sinalização. Desta forma, o *firewall* é configurado para permitir o tráfego associado à mídia, das máquinas internas somente com o gatekeeper e deste para qualquer máquina na Internet.

Quando o destino da chamada é um dispositivo em outra "zona", o *gatekeeper* remoto deve ser localizado para que possam ser obtidas informações sobre este dispositivo. Dois métodos podem ser utilizados com este objetivo: para apelidos tipo H323 ID, deve ser utilizado o serviço DNS, e para endereços E.164, mensagens RAS (LRQ – *Location request*).

O uso de DNS para a localização do gatekeeper remoto, requer que o H323 ID associado ao destino esteja no formato *usuário@domínio*. Nas informações associadas ao domínio no serviço DNS, deve haver um registro dos tipos SRV ou TXT, indicando o endereço IP do *gatekeeper* associado ao domínio.

Ao utilizar endereços E.164 como apelido, devem ser definidos os prefixos que são atendidos por cada "zona". No caso de *gateways* conectados à rede de telefonia, estes devem indicar no registro os prefixos associados ao telefones atendidos por esta conexão. Desta forma, as chamadas destinadas a estes telefones serão encaminhadas

para o *gateway*. Na comunicação entre zonas, os *gatekeepers* devem ter uma configuração estática dos prefixos atendidos por cada *gatekeeper* conhecido. Desta forma, ao receber um pedido de admissão, o prefixo é extraído do apelido do destino. A partir do prefixo é identificado o endereço do *gatekeeper* remoto, para onde é enviada uma mensagem RAS (LRQ – *Location Request*), como apresentado na Figura 2-7.

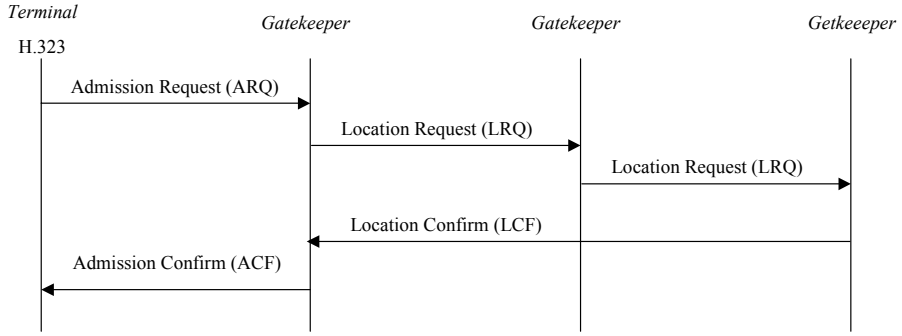


Figura 2-7 – Sinalização RAS: uso de LRQs

Ao receber a mensagem LRQ é verificado se o destino está registrado. Em caso afirmativo, e não havendo restrições, será enviada uma confirmação de localização (LCF – *Location Confirm*), indicando os parâmetros necessários ao estabelecimento do canal de sinalização de chamadas. Caso contrário, é enviada uma mensagem LRJ (*Location Reject).* Mensagens LRQ recebidas por um *gatekeeper* podem ser reenviadas a outros *gatekeepers.* Neste caso, só o *gatekeeper* onde estiver registrado o destino, ou que não tenha como encaminhar a LRQ para outro *gatekeeper*, retorna as mensagens LCF ou LRJ, respectivamente.

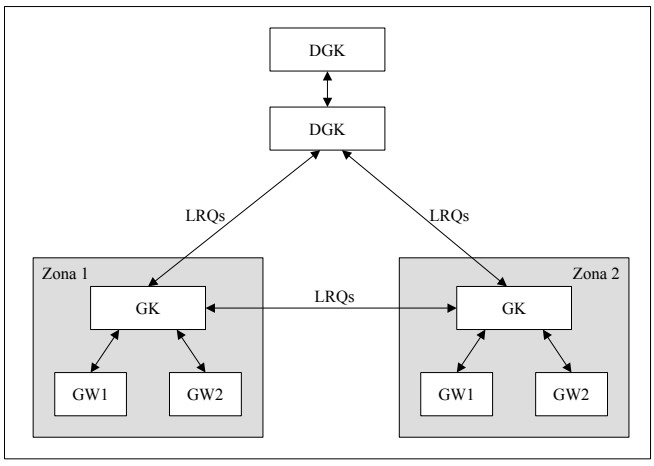


Figura 2-8 – Uso de Directory Gatekeeper

Gatekeepers específicos para a função de encaminhamento de mensagens LRQ, os *Directory Gatekeepers* (DGK), podem ser utilizados para estruturar redes H.323 com um grande número de "zonas". Na Figura 2-8, é apresentado um esquema de uma rede utilizando DGKs.

Detalhes da sinalização H.323 podem ser encontrados no anexo 1.

Capítulo 3

Detalhamento da Arquitetura Adotada no Projeto-Piloto VOIP da Rede Nacional de Pesquisa

Redes de telefonia de quatorze instituições de P&D de diferentes regiões do Brasil serão interligadas utilizando-se a Internet, em paralelo à rede de telefonia pública (PSTN – *Public Switched Telephone Network*). A sinalização VOIP seguirá a recomendação H.323, com previsão de utilização futura do protocolo SIP. Depois de implantado o projeto, será possível a realização de chamadas entre telefones e terminais H.323 de qualquer instituição participante.

A arquitetura básica implementada nas instituições será composta de um *gateway* de voz, de um *gatekeeper* e de uma estação de gerenciamento do serviço, conforme apresentado na Figura 3-1. A estação irá operar como servidor e utilizar o protocolo *Radius* para a coleta de informações de contabilização das chamadas realizadas através do *gatekeeeper* e do *gateway*. Outras funções associadas ao gerenciamento do serviço VOIP na instituição também serão implementadas neste servidor. Opcionalmente, as instituições podem utilizar um equipamento que permitirá a conexão direta de um pequeno número de telefones analógicos à rede, operando como um *gateway* de pequena capacidade. No projeto serão utilizados para este fim, equipamentos Cisco ATA188 configurados com duas portas de voz analógicas e uma interface *ethernet*.

A RNP será responsável pelo gerenciamento da operação do serviço VOIP. Uma estação de gerenciamento irá monitorar a operação dos equipamentos utilizados em cada instituição empregando o protocolo SNMP. Nessa estrutura será mantido um *gatekeeper* para instituições que não tenham capacidade momentânea de operar tal dispositivo e o DGK. Um servidor *Radius* de reserva irá atender as instituições cujos servidores principais apresentem algum problema.

Cada instituição utilizará um *gateway* H.323 conectando a sua estrutura atual de telefonia à rede IP. A conectividade com a rede de telefonia será efetuada através dos

PBXs das instituições. Duas alternativas de conexão são possíveis, uma utilizando ramais analógicos e a outra usando troncos digitais. A opção adequada depende da configuração do *gateway* e do PBX em cada instituição. O *gateway* será responsável por encaminhar as chamadas para os ramais internos ou para telefones públicos, com base em prefixos que serão adotados no plano de numeração do piloto.

Utilizando a descrição acima, são possíveis três cenários nas instituições participantes, como apresentado na Figura 3-1.

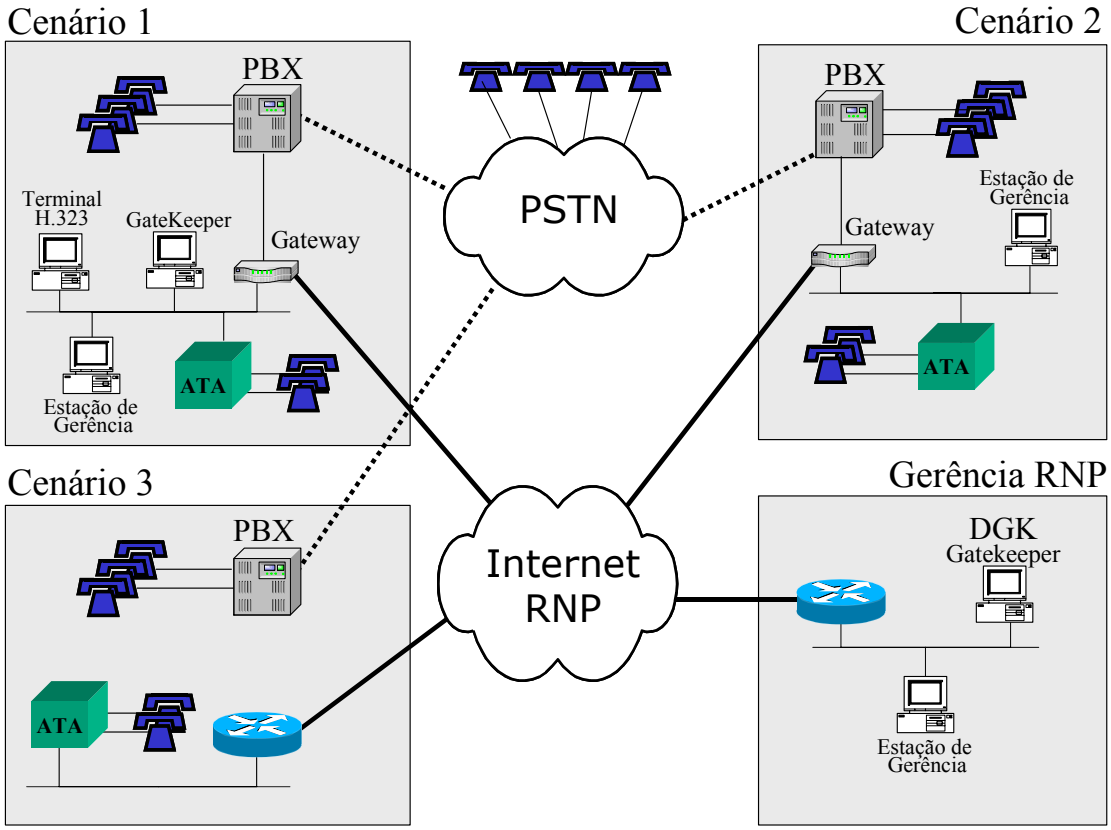


Figura 3-1 – Cenários possíveis no projeto-piloto RNP

Cenário 1 – ambiente completo, composto de PBX, *gateway, gatekeeper* e estação de gerência. Opcionalmente podem ser utilizados um ou mais ATAs para o uso de telefones analógicos.

Cenário 2 – ambiente composto de PBX, gateway e Radius, sem gatekeeper. Opcionalmente podem ser utilizados um ou mais ATAs para o uso de telefones analógicos.

Cenário 3 – Este é o cenário mais simples, configurado somente com Cisco ATA. Não haverá conexão direta entre a rede IP e a rede de telefonia. Os telefones conectados ao ATA poderão realizar e receber chamadas de outras instituições utilizando VOIP. O ATA deverá estar registrado, todavia, em algum *gatekeeper*.

3.1 Plano de Numeração

Nesta primeira fase do projeto, o encaminhamento de chamadas entre instituições está baseado em números de telefone, seguindo a recomendação ITU-T E.164 [48].

Com a escalabilidade do serviço VOIP será investigado futuramente um esquema baseado em DNS, onde o plano de numeração permitirá que usuários sejam mapeados em domínios e a procura de usuários passa a ser dirigida ao DNS. O *gatekeeper* estará registrado no DNS da instituição e responderá pelas requisições de localização de usuários locais. Neste novo ambiente, a figura do DGK não existiria, reduzindo o trabalho de configuração e gerência associado ao serviço VOIP.

A numeração telefônica adotada no Brasil inclui o Código Nacional (CN), composto de dois dígitos, acrescido do número do assinante, que pode ter 7 ou 8 dígitos dependendo da região. O Código Nacional é o código utilizado nas ligações nacionais de longa distância (DDD), sendo administrado pela Agência Nacional de Telecomunicações (ANATEL). O número do assinante é administrado pelas concessionárias de telefonia pública local, e depende da central telefônica local onde o assinante está conectado. O código de central é a parte do número de assinante que identifica a central local, sendo composto de três dígitos, no caso da numeração a 7 dígitos, ou de 4 dígitos, no caso da numeração a 8 dígitos.

Objetivando o mínimo possível de mudanças no PBX das instituições participantes, os números de assinante já alocados à telefonia de cada instituição serão mantidos na rede VOIP. Os *gatekeepers* serão configurados para encaminhar todas as chamadas direcionadas a essas instituições para os *gateways*, e estes para os PBXs. Os *gatekeepers* e *gateways* irão encaminhar as chamadas com base em um prefixo, composto do código nacional e do identificador da central. Entretanto, várias

instituições na mesma região podem ser atendidas pela mesma central. Por exemplo, duas instituições podem compartilhar o mesmo identificador de central (2598). Neste caso, serão utilizados mais dígitos do código do assinante para identificar a instituição. Por exemplo, o prefixo (25984) estará associado a uma instituição, e o (25983) será atribuído à outra.

Tabela 3-1 – Prefixos alocados às instituições participantes do projeto-piloto

Instituição	Prefixos adotados	
	Telefonia	Terminais H.323
CNPq	(61) 3489	0 (61) 3489
IME	(21) 2546	0 (21) 2546
INPA	(92) 64334	0 (92) 64334
MEC	(61) 410	0 (61) 410
RNP-Brasília	(61) 321 (61) 322 (61) 323	0 (61) 321 0 (61) 322 0 (61) 323
RNP-Campinas	(19) 378733	0 (19) 378733
RNP-RJ	(21) 320596	0 (21) 320596
UFAM	(92) 64746	0 (92) 64746
UFF	*[8]	*
UFC	(85) 288	0 (85) 288
UFPE	*	*
UFRJ	(21) 2598 (21) 2562 (21) 3873	0 (21) 2598[9] 0 (21) 2562 0 (21) 3873
UFSC	(48) 33163 (48) 33164	0 (48) 33163 0 (48) 33164
USP	(11) 3091	0 (11) 3091

As instituições terão também uma faixa de números reservados para atender à identificação de terminais H.323 na rede IP da instituição. Por simplicidade e para evitar administração de conflitos, estes números receberão o mesmo prefixo associado à instituição, acrescidos do dígito 0 (zero) no início do número. Desta forma, uma instituição terá pelo menos dois prefixos associados, um para os terminais H.323 e outro para os ramais telefônicos, como apresentado na Tabela 3-1. O uso do Código Nacional para chamadas envolvendo dispositivos da mesma instituição é opcional.

[8] Não definidos até o momento
[9] Nem todos os números associados a estes prefixos pertencem à UFRJ. Na implementação do projeto será utilizado mais um dígito para os prefixos utilizados

Na Tabela 3-1 são apresentados os prefixos adotados pelas instituições participantes do projeto-piloto. Exemplo de números utilizados na UFRJ:

Ramal virtual: 0 21 2598 4201, onde:

0 → identifica um ramal virtual, ou seja, é um identificador associado a um terminal H.323 (o terminal deve estar registrado no *gatekeeper* da instituição) ;
21 → identifica uma instituição que funciona na cidade do Rio de Janeiro (Código Nacional);
2598 → identifica a instituição, no caso a UFRJ (Código da Central);
4201 → número de ramal interno.

Ramal telefônico normal: 21 2598 3354, onde:

21 → identifica uma instituição que funciona na cidade do Rio de Janeiro (Código Nacional);
2598 → identifica a instituição, no caso a UFRJ (Código da Central);
3354 → número de ramal interno.

Cada instituição terá inicialmente uma "zona" H.323 controlada pelo seu *gatekeeper*. Um DGK gerenciado pela RNP será empregado para interligar logicamente os *gatekeepers* das instituições. Este DGK já faz *peering* com o DGK utilizado pelo WG VOIP[10] da Internet2, o que já possibilita a realização de chamadas com instituições de diversas partes do mundo registradas neste DGK [20]. Ligações internacionais realizadas a partir de qualquer instituição, devem ser precedidas do prefixo 00, acrescido do código do país, código nacional de destino e número do assinante. O *gatekeeper* das instituições deve ser configurado para remover o prefixo 00 ao receber as chamadas, encaminhado-as ao DGK, que as repassará ao DGK da Internet2. O *gatekeeper* das instituições também será configurado para incluir o código de país (55) nas chamadas direcionadas a outras instituições. O DGK deve ser configurado para tratar as chamadas precedidas do código 55 para um dos *gatekeepers* do projeto-piloto,

[10] Grupo de trabalho VOIP da Internet2

conforme o plano de numeração definido no DGK. Chamadas provenientes da Internet2 são direcionadas ao DGK com o prefixo 55. Ao receber chamadas com o prefixo 55, o *gatekeeper* da instituição deve removê-lo.

Restrições aos terminais H.323 que podem ter acesso ao projeto serão implementadas no *gatekeeper,* o qual só admitirá chamadas provenientes de terminais H.323 autorizados. A autorização é baseada atualmente no endereço IP ou em endereço de subrede. O uso de um apelido H.323 associado a uma senha e utilizando o protocolo H.235 para autenticação é opcional.

Os *gatekeepers* serão configurados inicialmente para uso das opções "*fast start*" e "H.245 *tunneling*", facilitando a implementação de mecanismos de segurança nas redes das instituições, associados ao serviço VOIP. Com este objetivo, o *gatekeeper* irá operar também como *proxy* dos fluxos RTP e RTCP. No tratamento de QoS no backbone da RNP, apenas os fluxos originados dos IPs do *gatekeeper* e do *gateway* serão atendidos prioritariamente.

Os *gatekeepers* serão elementos essenciais à operação da rede VOIP, onde qualquer falha nestes dispositivos afetará o funcionamento da rede VOIP de toda a instituição. Os *gateways* e terminais H.323 devem prever a configuração de *gatekeepers* alternativos, que devem ser utilizados caso os principais não estejam acessíveis. No projeto-piloto, os *gateways* e *gatekeepers* já prevêem este tipo de configuração, os terminais não. Enquanto não são desenvolvidos mecanismos nos terminais que permitam esta facilidade, uma solução seria o uso de duas máquinas configuradas como *gatekeeper* e respondendo pelo mesmo IP através do uso do mecanismo de *Virtual Router Redundancy Protocol* (VRRP) [49]. No uso desse protocolo, duas ou mais máquinas respondem por um endereço IP virtual, uma como *master* e as outras como *backup*. Caso a *master* deixe de responder, uma das *backups* responde pelo IP virtual. Desta forma, o serviço poderia ser mantido, mesmo que haja algum problema com o *gatekeeper* principal. Esta solução não terá efeito se a máquina estiver respondendo e o serviço não estiver operacional. Neste caso, deve ser adotado um programa monitor na própria estação para tentar ativar o serviço e para emitir alertas para o administrador da rede. Como o *gatekeeper* utilizado não tem suporte a SNMP não haveria formas de ativá-lo remotamente utilizando este protocolo. De qualquer forma, o serviço pode ser

monitorado utilizando a porta TCP/7000, através da qual poderá ser verificada a situação operacional do serviço.

3.2 Encaminhamento de Chamadas

Ligações provenientes de telefones convencionais serão encaminhadas através do PBX para as portas de voz dos *gateways* através do uso de um número chave do plano de numeração da instituição. Dessa forma, o usuário estará explicitamente optando por usar o serviço VOIP. Este modo de operação do serviço elimina a necessidade de qualquer reprogramação de rota no PBX.

O comportamento normal do *gateway* será oferecer um segundo tom de linha, quando deve ser discado um novo número que será interpretado pelo plano de discagem do *gateway*. O *gateway* estará configurado para utilizar o *gatekeeper* para localização do destino da chamada. Um pedido de admissão é enviado utilizando sinalização RAS. Ao receber a mensagem ARQ do *gateway,* o *gatekeeper* verifica se o destino é algum terminal H.323 da instituição. Se for, e o terminal estiver registrado, o mesmo será sinalizado da nova chamada utilizando a sinalização H.225 Q.931. Caso não esteja registrado, será enviada para o *gateway* uma mensagem RAS com o motivo "*Called party not registered"*. Sendo destinada a outra instituição, o *gatekeeper* reescreve o número chamado com o prefixo 55, indicativo de chamadas nacionais. Nas chamadas nacionais e internacionais será enviada uma mensagem LRQ para o DGK, que deverá identificar o destino com base no prefixo do número chamado. Caso seja precedido do prefixo internacional 00, o número será reescrito, retirando o prefixo 00, e uma mensagem LRQ será encaminhada para o DGK da Internet2. Caso seja destinado a uma instituição do projeto, uma mensagem LRQ será encaminhada ao respectivo *gatekeeper.* Se o destino for um terminal registrado ou um telefone convencional, uma mensagem LCF é enviada ao *gatekepeer* original, que utilizará a sinalização H.225 Q.931 para estabelecer a chamada. Caso contrário, será enviado um LRJ com o motivo "*Called party not registered*".

Objetivando facilitar a implementação do projeto e orientar os usuários no uso do serviço, recomendamos o uso do recurso *Interactive Voice Response (IVR)* se disponível no *gateway*. O IVR permite que seja emitida uma mensagem de voz

previamente gravada instruindo o usuário a utilizar o sistema. Os dígitos discados pelo usuário serão capturados pelo IVR e serão interpretados pelo plano de discagem. Uma possibilidade no uso do IVR é a análise do usuário, onde é solicitada uma identificação que será empregada para verificar se o mesmo é autorizado a utilizar o sistema. Nesta verificação pode ser utilizado um mecanismo semelhante ao serviço de telefone pré-pago, onde o crédito do usuário seria verificado. Havendo crédito, a chamada seria autorizada e iria ocorrer enquanto o usuário tiver crédito. O IVR nos *gateways Cisco* é implementado com a linguagem *Tool Command Language* (TCL).

Nas chamadas provenientes de um terminal H.323 é feito um pedido de admissão ao *gatekeeper* utilizando a mensagem ARQ. O tratamento será igual ao das provenientes do *gateway.*

3.3 Conexão com os PBXs

Os *gateways* podem ser conectados ao PBX através de portas de voz analógicas ou digitais. As portas de voz analógicas podem ser de três tipos: *Foreign Exchange Station* (FXS), *Foreign Exchange Office* (FXO) e *Ear&Mount* (E&M). As interfaces digitais estarão conectadas a trocos E1 (2Mbps) ou T1 (1.544Mbps), onde pode estar sendo empregada sinalização associada a canal (CAS) ou sinalização em canal comum (CCS).

A sinalização de linha é a responsável pela alocação da linha telefônica no estabelecimento da chamada e para liberá-la quando a chamada terminar. Interfaces analógicas podem utilizar três tipos de sinalização de linha: *loopstart, groundstart* e *Ear&Mount.*

A sinalização de linha mais comum e mais simples em telefonia é a *loopstart*, onde dois fios são utilizados para interligar o telefone ao PBX, como apresentado nas Figura 3-2 e Figura 3-3. O PBX fornece a alimentação da linha (-48Vdc) e o aterramento para formar o *loop* local. Este circuito é fechado no momento em que o usuário retira o fone do gancho, condição OFF-HOOK. Quando o circuito é fechado, passa a circular uma corrente elétrica que é detectada pelo PBX. Este, estando pronto para receber a sinalização dos números do telefone chamado, fornece um tom de linha disponível (*Dial Tone*).

Ao terminar a chamada, o usuário coloca o fone no gancho abrindo o *loop*, liberando a linha para novas chamadas.

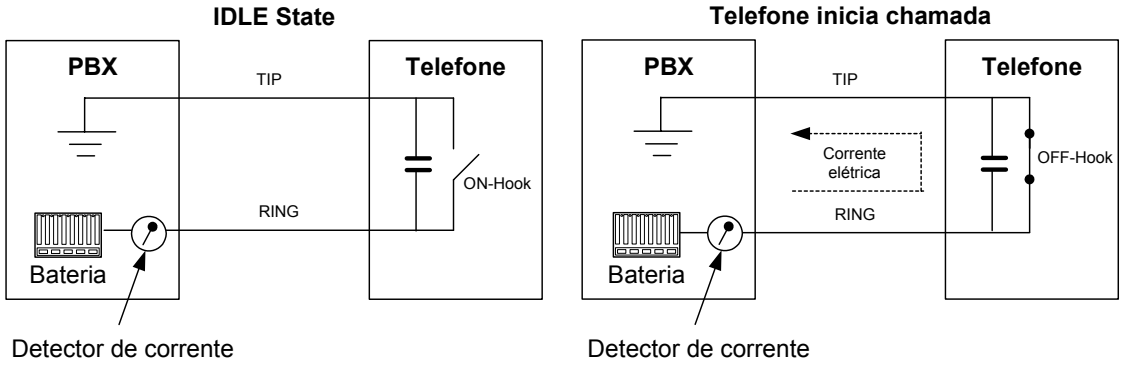


Figura 3-2 – Sinalização *Loop-start*: chamadas iniciadas pelo telefone

Nas chamadas provenientes do PBX, um sinal de chamada (*ring tone*) é transmitido no pino *RING,* sinalizando o usuário de uma nova chamada. Ao retirar o fone do gancho, o circuito é fechado.

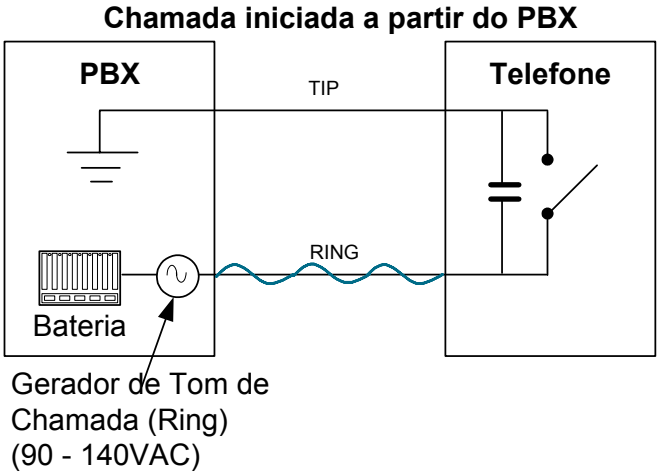


Figura 3-3 – Sinalização *Loop-start*: chamada iniciada pelo PBX

Nos *gateways* de voz, portas de voz do tipo FXS são utilizadas para implementar o mesmo comportamento que o ramal analógico do *gateway*, ou seja, fornecem a alimentação da linha. Nestas portas podem ser ligados telefones analógicos, de onde podem ser estabelecidas chamadas através da rede VOIP.

A porta FXO implementa a mesma funcionalidade do telefone e deve ser ligada a um ramal analógico do PBX. Nas chamadas iniciadas pelo *gateway,* o *loop* é fechado na porta FXO, sendo identificado pelo PBX. Nas chamadas provenientes do PBX, a porta FXO identifica o tom de chamada e fecha o *loop.* Quando as chamadas são terminadas pelo *gateway,* o *loop* é aberto e a linha é liberada para novas chamadas. Existe um problema quando a chamada é terminada pelo lado do PBX, já que este não tem um mecanismo que sinalize o término da chamada, não liberando a linha para novas chamadas. Algumas soluções de sinalização são adotadas para solucionar este problema: *power denial, battery reversal, groundstart e supervisory tone disconnect (STD)*. As três primeiras dependem de mudanças na configuração do PBX e do *gateway*, enquanto que a última depende somente de mudanças no *gateway.*

Na solução de *power-denial,* o PBX remove a alimentação da linha *RING,* por um período mínimo de 350ms, após o término da chamada. Na solução *battery-reversal,* a polaridade das linhas é invertida quando termina a chamada, ou seja, a alimentação de –48Vdc passa a ser efetuada através do pino TIP e o aterramento pelo RING. Na sinalização *groundstart,* o uso de chaves que abrem o *loop* permite sinalizar o término da chamada, como pode ser visto na Figura 3-4.

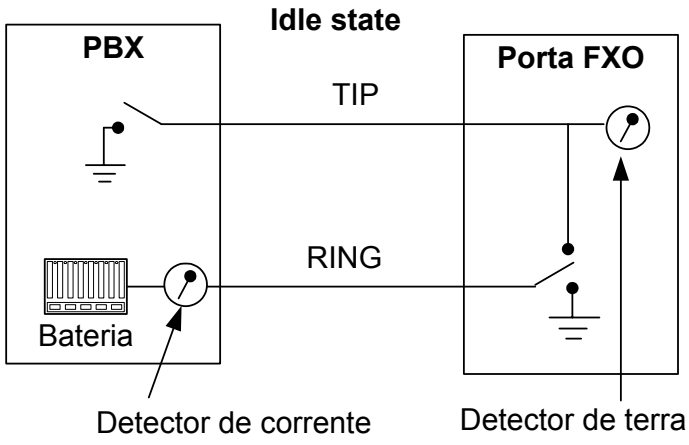


Figura 3-4 – Sinalização *ground-start*

A última alternativa de desconexão é a identificação do tom de desconexão provido pelo PBX quando termina a chamada, normalmente um tom de ocupado (*busy tone*). Na telefonia convencional, ao receber esta sinalização, o usuário coloca o fone no

gancho. No caso do *gateway,* este deve ser configurado para reconhecer o tom de desconexão, abrindo o *loop*. Como o tom da sinalização pode variar conforme o país, a porta do PBX e a do *gateway* devem fazer uso da mesma configuração de tons.

O objetivo no projeto-piloto é realizar o mínimo de configurações no PBX, visto que normalmente envolvem um custo elevado para a instituição. Dessa forma, a solução adotada nas portas de voz FXO com sinalização *loop-start* é o uso da desconexão por tom, que exige somente a configuração do *gateway,* adequado-o ao PBX. As maiores dificuldades encontradas em laboratório para esta configuração foram a compatibilização do padrão de tons do *gateway* com o empregado no PBX*,* e o uso de sistemas operacionais no *gateway* onde este mecanismo funcione corretamente.

Em portas E&M, são utilizadas linhas distintas para a sinalização, independentes das de voz, como apresentado na Figura 3-5. Esta sinalização é normalmente utilizada na interligação de PBX (*tie-line*), onde, dependendo da configuração adotada, 2 ou 4 fios (RING e TIP / RING1 e TIP1) são utilizados para a transmissão da voz, e os pinos E e M são utilizados na sinalização entre PBXs. Como depende de portas específicas no PBX e no *gateway*, não estão sendo adotadas no projeto-piloto. Este tipo de sinalização também pode ser empregado em troncos digitais, neste caso só será necessária a configuração do PBX e do *gateway* para que interoperem.

Figura 3-5 – Conexão entre PBXs com troncos E&M

As portas de voz analógicas permitem somente uma ligação por vez, o que limita o número de chamadas realizadas através do *gateway.* Objetivando um número maior de chamadas simultâneas, podem ser adotados troncos digitais, por onde trafegam até 30

canais de voz. No Brasil, os circuitos E1 são padrão em facilidades digitais de PBXs. Em troncos E1 trafegam *frames* que compreendem 32 canais digitais DS0 (64Kbps), sendo o canal 1 reservado para enquadramento e alarmes, e o canal 16 utilizado na sinalização dos canais.

A sinalização em canais digitais pode ser associada ao canal (*Channel Associated Signaling* – CAS) ou em canal comum (*Common Channel Signaling* - CCS) . No uso de CAS, toda a sinalização associada às chamadas é transmitida no mesmo canal que a voz (*in-band*), enquanto que no CCS é transmitida em um canal separado (*out-band)*, sendo previsto o seu uso no projeto-piloto. A sinalização CAS E1-R2 é a adotada no Brasil para a conexão de PBXs e a central telefônica da concessionária. *Integrated Services Digital Network* (ISDN) e SS#7 são exemplos de sinalização CCS.

O uso de sinalização digital no PBX requer interfaces específicas nos PBXs e nos *gateways*, além de requerer uma configuração compatível nos dois dispositivos.

No projeto-piloto serão empregadas duas configurações iniciais de *gateway*, dependendo do volume de chamadas previsto para a instituição: na primeira são utilizadas quatro portas analógicas FXO, enquanto na segunda uma porta digital E1.

O número de chamadas de voz simultâneas em uma interface digital depende do número de *Digital Signal Processors* (DSP) instalados. O DSP é o responsável pela conversão da voz analógica em pacotes que serão transmitidos na rede IP. A quantidade de chamadas suportadas por DSP depende da complexidade do *Codec* utilizado. *Codecs* são classificados em duas categorias: média (G.711, G.726, G.729A e G.729AB) e alta complexidade (G.728, G.723, G.729 e G,.729B). Os DSPs utilizados nos *gateways* Cisco utilizados no projeto-piloto suportam 4 chamadas simultâneas utilizando *Codecs* de média complexidade ou duas com os de alta.

3.4 Contabilização das Chamadas

Informações sobre as chamadas, tais como tempo de duração, terminais e *gateways* envolvidos, tráfego transmitido e recebido (bytes e pacotes), e causa da desconexão são fornecidas pelo *gateway* através de registros CDR (*Call Detail Record*),

transmitidos utilizando o protocolo Radius (*Remote Authentication Dial In User Service*).

Os CDRs são direcionados a servidores Radius, onde é possível gerar diversos relatórios sobre o uso do serviço. Entre os relatórios possíveis podem ser destacados os relatórios diários de uso do serviço (distribuição horária das chamadas, motivos de desconexão, estatísticas de erros ao longo do dia – número de pacotes perdidos, número de pacotes adiantados, número de pacotes atrasados, nível de atraso na rede, e outros) e perfil das chamadas (tempo de uso, pacotes/bytes transmitidos e recebidos, motivos de desconexão, qualidade da voz, e outros). As estatísticas de erro serão utilizadas também para a identificação de possíveis problemas na rede.

O *Radius* utiliza o protocolo UDP no transporte de mensagens para o servidor, não havendo retransmissão no caso de falhas na rede ou no servidor. Neste caso, as informações são perdidas, afetando a contabilização das informações. Em face da importância dos dados exportados nos CDRs, torna-se necessário o uso de mecanismos que impeçam a perda dos mesmos. Um servidor secundário será utilizado na RNP para receber os CDRs, caso não haja confirmação de que estes foram gravados no servidor primário. A consolidação das informações provenientes dos CDR deve prever também a análise de CDRs que porventura estejam armazenados no servidor secundário. Em uma segunda fase do projeto, quando o número de chamadas de uma instituição for elevado, é recomendado o uso de um servidor secundário na própria instituição. Desta forma, informações importantes para fins de contabilização não correm o risco de serem perdidas. Além disso, deixará de ser gerado tráfego no backbone associado a CDRs (*Call Detail Records)* no caso de problemas no servidor primário, que poderá ser elevado se o número de chamadas for alto.

O uso do banco de dados MySQL permite que seja implementado um mecanismo de replicação de informações entre os servidores de banco de dados, visando a diminuição na probabilidade de perda de dados.

3.5 Plataformas de Hardware/Software Adotadas no Projeto-Piloto

No projeto-piloto serão adotados *gateways* Cisco modelo 2600, adquiridos pela RNP. Inicialmente serão utilizados três equipamentos com duas portas digitais E1 e quatro configurados com quatro portas FXO. Estes equipamentos também podem operar como *gatekeepers*, o que será instalado na RNP será configurado como o DGK do projeto-piloto.

Os softwares utilizados na implementação do projeto-piloto foram escolhidos com a premissa de que sejam de código aberto e que possam ser implantados em diferentes sistemas operacionais, principalmente Linux, FreeBSD e Microsoft Windows 2000.

Diversas implementações de *gatekeepers* estão disponíveis: *OpenGK*, *OpenGatekeeper*, *OpenGatekeeper* H.323 *Proxy* e *GnuGk*. Uma comparação detalhada das várias opções pode ser encontrada em [50]. Dentre estes, o *GnuGk* foi escolhido, por ser o projeto que apresenta a maior quantidade de funcionalidades, como suporte a autenticação de usuários integrada com *Radius*, LDAP e banco de dados SQL, reescrita de endereços E.164, encaminhamento de LRQs permitindo que atue como DGK e opere como proxy H.323. O número de chamadas concurrentes permitido também é elevado. A documentação do projeto apresenta a possibilidade de 10 mil registros e milhares de chamadas concurrentes quando configurado para operar no modo *routed signaling*.

Terminais H.323 podem utilizar o *OpenPhone*[11], software desenvolvido pela Equivalence Psy. Ltd. Opcionalmente, pode ser utilizado o aplicativo *Netmeeting*, da Microsoft. Este apresenta várias limitações, sendo a principal a falta de suporte a H.235, que implementa mecanismos de autenticação e transmissão segura de chamadas H.323.

O servidor *Radius* será implementado com o uso do software *FreeRadius*, visto que permite a replicação de servidores e tem interface com bancos de dados *MySQL*, *Oracle, PostgreSQL e Sybase*. Será utilizado o banco *MySQL* para o armazenamento das informações, realizado pelo próprio servidor *Radius*, para que possam ser gerados os relatórios estatísticos.

[11] http://www.openh323.org

3.6 Protótipo do Cenário Proposto

Uma implementação reduzida do cenário proposto foi implementada para atender os participantes do 4º. Workshop da Rede Nacional de Pesquisa (WRNP) e do 21º. Simpósio Brasileiro de Redes de Computadores (SBRC) [51] .

A idéia do experimento foi possibilitar que os usuários congressistas do WRNP/SBRC pudessem realizar e receber ligações vindas tanto da Internet como da telefonia convencional, através dos PBXs da UFRJ e do hotel do evento. Deste modo foi montado um ambiente no hotel onde o evento estava sendo realizado, e outro na Universidade Federal do Rio de Janeiro, conforme apresentado na Figura 3-6.

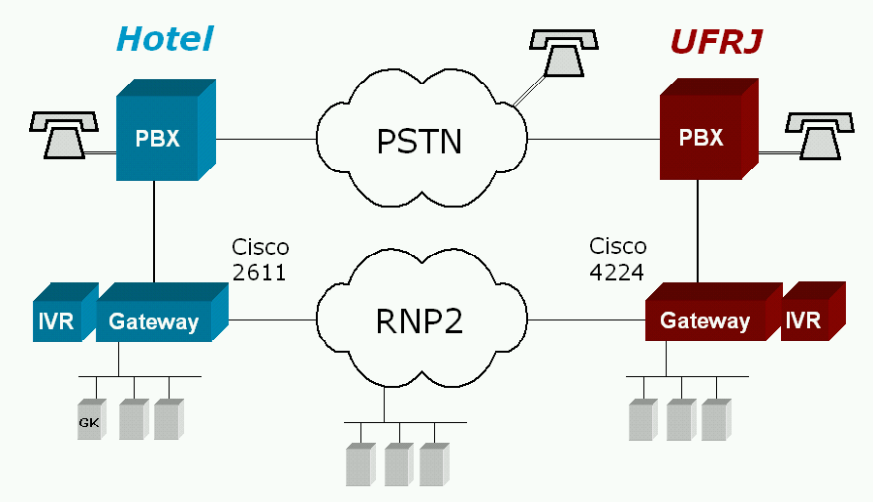


Figura 3-6 – Cenário utilizado no WRNP

A estrutura montada permitiu analisar vários aspectos associados à implantação e monitoração do serviço. Em especial, foi de forma prática confirmada a necessidade de implementação de QoS no *backbone* da RNP, de forma que se possa garantir a qualidade da voz. A coleta de informações através do protocolo *Radius* permitiu avaliar a quantidade de chamadas e o perfil do tráfego de voz, além de gerar uma base de dados com informações que permitiram avaliar as causas do término das chamadas. A avaliação das que terminaram de forma anormal foram utilizadas para determinar as possíveis causas, onde foi verificado que a maioria estava associada ao fato de não haver uma garantia de QoS no *backbone* da RNP. Maiores informações sobre o projeto-piloto podem ser obtidas no relatório técnico P.4.1 do GT-VOIP RNP [52].

Capítulo 4

Gerenciamento VOIP

A implementação de redes VOIP introduz uma série de desafios no gerenciamento de uma rede, visto que há a necessidade de garantir que o serviço apresente uma qualidade que justifique o seu uso. O serviço de telefonia está associado a uma qualidade mínima, a qual deve ser o objetivo com a migração do serviço para a rede IP. Problemas transientes, como perda de pacotes ou atrasos provocados por congestionamentos, podem ser admissíveis em serviços tradicionais de redes IP, mas normalmente não são aceitáveis para o tráfego de voz. Neste sentido, alguns pontos devem ser avaliados: supervisionar a operação dos equipamentos envolvidos, garantir a disponibilidade do serviço, manter a qualidade de voz nas chamadas e dispor de mecanismos que permitam contabilizar, tarifar e realizar auditorias das chamadas realizadas.

O Plano Geral de Metas de Qualidade (PGMQ) [22] e [53], estabelecido pela Agência Nacional de Telecomunicações (ANATEL), define métricas associadas ao serviço de telefonia fixa, que devem ser garantidas pelas concessionárias do serviço, dentre elas podem ser destacadas:[12]

- em 98% dos casos, o usuário deve ter a garantia da obtenção do sinal de discar em menos de 3 segundos (média alcançada em 2002: 99,87%);
- 65% das chamadas locais e de longa distância realizadas, devem ser completadas (média obtida em 2002: 69,19% para chamadas locais e 67,69% para chamadas nacionais);
- os casos de ligações locais e de longa distância não realizadas em função de congestionamento da rede não devem exceder a 5% das realizadas (média obtida em 2002: 1,44% para chamadas locais e 2,59% para chamadas de longa distância);

[12] As métricas apresentadas são relativas aos períodos de maior movimento: 9:00 às 11:00hs, 14:00 às 16:00hs e 20:00 às 22:00hs

- as chamadas deverão ser realizadas com boa qualidade de transmissão, em níveis adequados e sem ruídos ou interferências, com baixa incidência de queda de ligações ;
- as prestadoras do serviço deverão dispor de sistemas de supervisão para atuar preventivamente na detecção de defeitos;

A análise dessas métricas e dos valores obtidos denota as características de alta disponibilidade do serviço de telefonia tradicional. A tendência do usuário com o serviço VOIP é a aceitação de um serviço com uma menor qualidade, face às outras vantagens que pode apresentar, como o fator custo. Esta comparação é idêntica à da telefonia celular, onde a menor qualidade da voz é justificável em função da mobilidade. Entretanto, do ponto de vista do provedor do serviço, é importante garantir no VOIP uma qualidade semelhante à de telefonia, ou seja, possibilidade de discagem imediata e a qualquer momento, que a grande maioria das chamadas seja completada na primeira tentativa em que é realizada e que haja uma boa qualidade na voz.

A monitoração do sistema para que falhas que possam ocorrer sejam identificadas e corrigidas rapidamente é importante para manter a disponibilidade do sistema.

Uma chamada com boa qualidade de voz é aquela em que os participantes podem se comunicar sem dificuldade, não havendo no canal de voz, ruídos ou perturbações que possam distraí-los ou incomodá-los. A comutação por circuito garante ao serviço de telefonia uma largura de banda fixa e garantida ao longo de todo o circuito, durante toda a chamada. Problemas de qualidade podem ocorrer, mas com uma incidência muito baixa e normalmente provocada por defeitos ou instalações fora do padrão. Em redes comutadas por pacotes, os recursos são compartilhados e problemas como atrasos ou perdas de pacotes decorrentes de filas cheias e canais de comunicação saturados, podem ocorrer. Esses problemas podem afetar a qualidade das chamadas, com a perda de partes da conversa ou com uma demora na reprodução remota do que foi transmitido, afetando a interatividade. Há, portanto, a necessidade de monitorar as condições da rede e a qualidade das chamadas que estão sendo realizadas.

4.1 Áreas Funcionais da Gerência de Redes

Na definição da estrutura de gerenciamento de sistemas abertos, a recomendação ITU-T X.700 [54] define os requisitos básicos que devem ser providos por esta estrutura, os quais são categorizados em:

- gerenciamento de falhas
- gerenciamento de contabilidade
- gerenciamento de configuração
- gerenciamento de performance
- gerenciamento de segurança

4.1.1 Gerenciamento de Falhas

Gerenciamento de falhas engloba a detecção, localização e correção das condições anormais que afetam o funcionamento da rede. Envolve a monitoração constante de seus componentes, através da requisição periódica de informações que permitam verificar a situação operacional destes elementos e através do tratamento de notificações (alarmes) enviadas pelos mesmos, na ocorrência de alguma anormalidade que afete a operação dos serviços oferecidos.

Os elementos de rede devem implementar uma base de informações gerenciais para que possam ser gerenciados. Esta base mantém informações que refletem a operação de seus componentes, as quais são consultadas para verificar o seu funcionamento.

Agentes podem ser implementados na rede para monitorar o seu funcionamento e dos serviços oferecidos, que ao verificarem situações anormais na sua operação notificam a gerência da rede. Estes agentes podem ser embutidos nos vários elementos que compõem a rede ou podem operar de forma autônoma. Uma avaliação deve ser realizada nos alarmes recebidos, classificando-os e priorizando o tratamento em função do impacto causado. Mecanismos para a correlação de alarmes devem ser utilizados para que a causa de falhas possa ser identificada, preferencialmente numa ação pró-ativa, onde a identificação e correção de falhas ocorre antes que o usuário do serviço perceba.

Um histórico dos eventos ocorridos que estejam associados a falhas deve ser mantido em arquivos *log,* para que possam ser examinados.

4.1.2 Gerenciamento de Configuração

Gerenciamento de configuração provê as funções para identificar os elementos da rede e de exercer controle sobre os mesmos, garantindo sua operação. Engloba mecanismos para monitorar, alterar e manter a configuração da rede e de seus componentes.

Projetos e alterações na topologia da rede estão incluídos neste tópico.

4.1.3 Gerenciamento de Contabilidade

Habilita a medida do consumo dos recursos da rede, de forma que possam ser tarifados. Cotas no uso dos recursos podem ser estabelecidas, criando limites no uso dos serviços oferecidos.

4.1.4 Gerenciamento de Desempenho

Gerenciamento de desempenho provê funções para relatar o comportamento e a eficiência da rede e de seus componentes. Com este objetivo devem ser coletados e analisados dados estatísticos que possam auxiliar na medição da qualidade do serviço que está sendo prestado.

A área de desempenho interage com a de falhas, através de indicativos de problemas provenientes da análise das estatísticas coletadas, e com a de configuração, de forma que alterações possam ser realizadas decorrentes das conclusões derivadas da análise das informações coletadas.

Na avaliação da qualidade é importante definir as métricas que reflitam a performance da rede e de seus componentes e a metodologia de coleta e os valores limítrofes para a classificação da qualidade.

4.1.5 Gerenciamento de Segurança

Provê um conjunto de funções que permite assegurar a segurança da rede e de seus componentes. Engloba a segurança no acesso aos recursos, alarmes associados a violações da segurança e à segurança dos dados.

4.1.6 Gerenciamento de Redes VOIP

O gerenciamento de uma rede VOIP deve prover os recursos necessários para manter a funcionalidade do serviço com uma qualidade adequada, atendendo às áreas funcionais previstas no gerenciamento de redes.

4.2 Gerenciamento de Redes IP

O protocolo SNMP foi selecionado pelo IETF como a arquitetura a ser utilizada na gerência de redes baseadas nos protocolos TCP/IP, tendo como principal característica a simplicidade de implementação. Esta característica tornou-o o padrão de fato na gerência de redes TCP/IP.

A primeira versão formulada em 1988, foi publicada oficialmente em 1990 através de três RFCs que definiram a estrutura das informações de gerenciamento (SMI), a base de informações gerenciais (MIB) e o protocolo para comunicação entre o gerente e agentes (SNMP).

A arquitetura de gerenciamento SNMP é baseada no modelo clássico de gerenciamento de redes, composto de gerente, agente e objetos gerenciados. Vários nós da rede, os agentes, serão gerenciados por uma estação de gerenciamento, o gerente. A estação de gerenciamento é a interface entre o administrador da rede e o sistema de gerenciamento, permitindo que a rede seja monitorada e controlada, como apresentado na Figura 4-1.

Nos agentes, as informações relativas aos recursos gerenciados são mantidas em uma base de informações que independe da arquitetura de hardware e software do agente, a *Management Information Base* (MIB). As informações disponibilizadas nesta base são obtidas através de instrumentação do agente, a qual não é definida na arquitetura.

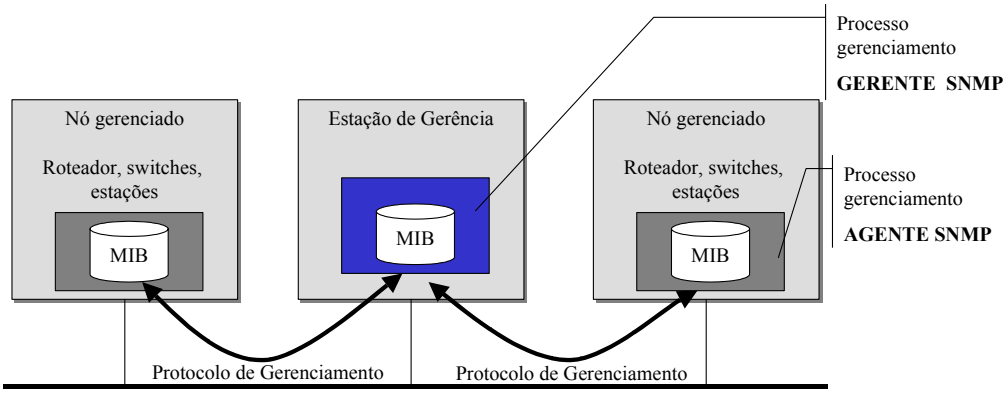


Figura 4-1 – Modelo do gerenciamento SNMP

A estrutura das informações na MIB é definida utilizando a linguagem formal *Abstract Syntax Notation 1 (ASN.1)*. A *Structured Management Information version 2* (SMIv2) estabelece os tipos básicos de dados ASN.1 que podem ser utilizados para a inclusão de objetos nessa estrutura e as regras para escrever e revisar os módulos que descrevem os objetos que compõem a MIB.

O protocolo SNMP é utilizado pelo módulo gerente para a coleta das informações disponíveis na MIB dos agentes. O protocolo SNMP utiliza o mecanismo de requisição/resposta (*polling*), onde através de operações periódicas são recolhidas as informações necessárias à monitoração dos agentes, ou alteradas as condições de operação desses nós, como apresentado na Figura 4-2. Por exemplo, o estado operacional, o tráfego de pacotes e o número de erros associados às portas de voz do *gateway* podem ser monitorados periodicamente. Em outro exemplo, uma porta de voz pode ser desabilitada por intervenção do administrador da rede ou por ter sido identificado um número excessivo de erros pela estação de gerência.

As operações definidas no SNMPv1 (*getrequest* e *getnextrequest)* obtêm somente uma resposta para cada informação solicitada do agente. O número de agentes gerenciados, a quantidade de informações requisitada e a periodicidade de coleta podem então ser responsáveis por um grande tráfego de rede associado a gerenciamento. A partir da versão 2 do SNMP foi definida uma nova operação (*getBulkRequest*) que permitiu a coleta de um número maior de informações por requisição, reduzindo o tráfego gerado e melhorando a performance do protocolo.

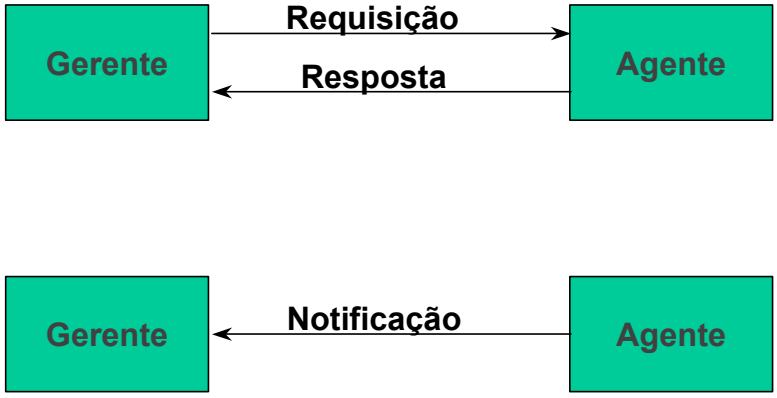


Figura 4-2 – Modelo de comunicação SNMP

Além do mecanismo de *polling*, os agentes podem notificar o gerente de condições anormais na operação do agente utilizando a operação *trap*. No protocolo não está prevista uma mensagem de confirmação do recebimento do *trap* por parte do gerente. Como o protocolo SNMP utiliza UDP (*User Datagram Protocol*) para o transporte de mensagens, não existe a garantia de que o gerente irá receber a notificação, o que é uma deficiência do SNMP. Outra notificação prevista a partir da versão 2 é a *inform* que, ao contrário das notificações do tipo *trap,* aguarda uma confirmação de que foi recebida no destino. Caso não receba, deve ser retransmitida.

Módulos MIB descrevem e definem os objetos que os agentes disponibilizam, cujos valores associados serão lidos ou alterados através do protocolo de gerenciamento. As notificações que podem ser enviadas pelos agentes também são definidas nos módulos MIB. Em cada módulo é especificado um conjunto de objetos relacionados a recursos específicos do nó gerenciado. Um módulo pode conter, por exemplo, objetos que descrevem o estado operacional, o tipo e a quantidade de bytes recebidos e

transmitidos por cada uma das interfaces do agente gerenciado. A especificação dos módulos, e dos objetos que descrevem, pode ser realizada de duas formas: no âmbito do IETF e outros órgãos de padronização ou pelos fabricantes dos equipamentos que serão gerenciados. Nos dois casos, documentos públicos descrevem a estrutura dos módulos utilizando a linguagem definida na SMIv2. Os equipamentos de rede gerenciáveis incorporam um agente SNMP em seu sistema operacional que implementa os módulos pertinentes aos seus componentes e à sua operação, incluindo os padronizados e os desenvolvidos pelo fabricante. A descrição desses módulos deve ser compilada na estação de gerência, para que esta conheça os objetos disponíveis nos agentes que gerencia.

A troca de mensagens SNMPv1 entre gerente e agentes utilizava um mecanismo de segurança baseado em *community*, uma "senha" definida no agente que deveria ser utilizada em todas as mensagens SNMP enviadas a esse agente. Este mecanismo é vulnerável, visto que a informação da *community* utilizada é enviada nas mensagens em texto claro, que pode se facilmente obtida analisando os pacotes SNMP capturados da rede. Esta deficiência limitava o uso do SNMP somente para fins de monitoração dos agentes, não era recomendado para controlá-los.

A simplicidade do SNMP, que o ajudou a ocupar o campo de gerenciamento das grandes redes, é a principal responsável pelas suas limitações associadas à eficiência, segurança, flexibilidade e na distribuição da sua administração. Estas deficiências limitaram o uso do SNMPv1 à monitoração dos recursos, não sendo indicada a sua utilização para fins de controle dos agentes monitorados. A segunda versão do SNMP, conhecida como SNMPv2 [56] e lançada em 1993, objetivou a correção das deficiências da versão original. Entretanto, divergências associadas ao mecanismo de segurança que deveria ser adotado impediram sua evolução como padrão Internet. Objetivando a definição de uma arquitetura que representasse uma evolução do SNMP, onde todas as deficiências das versões anteriores pudessem ser corrigidas, o IETF definiu uma nova versão em janeiro de 1998, o SNMPv3 [57].

Um conjunto de RFCs descreve o esquema de gerenciamento SNMP [58]:

- a arquitetura de gerenciamento, através da RFC 3411;
- mecanismos para descrever os objetos e eventos para fins de gerenciamento, através das RFCs 2578, 2579 e 2580 ;
- formato das mensagens para a troca de informações de gerenciamento, através das RFCs 3412, 3414 e 3417;
- operações utilizadas no acesso às informações de gerenciamento e o formato das PDUs associadas, através das RFC 3416;
- um conjunto de aplicações fundamentais à tarefa de gerenciamento, descrito na RFC 3413;
- mecanismo de controle de acesso, através da RFC 3415.

As características do protocolo SNMP permitem utilizá-lo na monitoração periódica dos valores associados aos objetos gerenciados. Entretanto, o SNMP não é adequado para a monitoração em tempo real de fluxos de mídia associados às chamadas, onde possam ser coletadas continuamente informações sobre perda de pacotes, atrasos ou *jitter.* Além da demora da atualização das informações na MIB, haveria um excesso de tráfego associado às requisições e respostas SNMP.

O uso de *Remote Network Monitoring (*RMON)[59] , uma extensão ao SNMP onde monitores de rede coletam informações sobre o tráfego nos segmentos onde estão instalados, permitindo gerar estatísticas, coletar pacotes ou emitir alarmes associados às condições da rede, seria uma opção para monitorar o tráfego em tempo real. Entretanto, as características dos protocolos VOIP, onde os fluxos são associados a endereços de portas TCP/UDP diferentes para cada chamada, dificultam a configuração do RMON para efetuar a monitoração destes fluxos, já que não haveria uma "inteligência" para identificar os fluxos associados a VOIP que trafegam pela rede.

Extensões no esquema do RMON permitiram criar mecanismos que possibilitam a monitoração de qualquer variável numérica na MIB do agente, com a geração de alarmes, caso ultrapasse limites definidos. Este mecanismo criou uma facilidade para gerar alarmes associados ao comportamento de variáveis importantes no gerenciamento

de equipamentos e serviços, antes restritos a alarmes fixos definidos pelo fabricante ou através de RFCs .

O grupo de trabalho RMONMIB do IETF, com intuito de criar mecanismos que permitam monitorar aplicações em tempo real como o VOIP, definiu uma nova extensão ao RMON. A RAQMON (*Real-time Application Quality of Service Monitoring*)[60] é a proposição de um esquema que permite obter informações provenientes de aplicações de tempo real. O objetivo é ter agentes simples RDS (*RAQMON Data Source*) coletando informações de QoS diretamente de aplicações e utilizando o protocolo RTCP ou o SNMP para transferir estas informações em intervalos de tempo bem curtos para agentes externos (RRC - *RAQMON Report Collector*), que fazem o processamento das informações recebidas, avaliam os resultados para identificar possíveis problemas e os disponibilizam em MIBs. O objetivo é ter agentes RDS sem complexidade de implementação, de forma que possam ser utilizados em telefones IP, terminais e outros dispositivos associados a aplicações em tempo real.

4.2.1 Arquitetura Básica SNMPv3

O SNMPv3 foi definido com o intuito de ser utilizado em redes de vários tamanhos e complexidade. Diferente das outras versões, o SNMPv3 utiliza uma arquitetura modular, onde os subsistemas existentes podem ser substituídos, ou novos podem ser adicionados. O princípio básico é ter um protocolo que independa da definição das informações de gerenciamento, de forma que o protocolo possa ser atualizado sem que a estrutura das informações precise ser alterada.

O SNMPv3 utiliza um mecanismo de segurança baseado em usuário (USM – *User-based Security Model*) que garante a privacidade, integridade e autenticidade nas mensagens trocadas entre gerente e agentes. O conjunto de objetos que um usuário pode visualizar na MIB de um agente é limitado com base no *View-based Access Control Model* (VACM). A melhoria na segurança permite que o SNMPv3 possa ser utilizado para fins de controle dos agentes, o que não era indicado nas outras versões. Desta forma, variáveis MIB com acesso de escrita podem ser alteradas utilizando a operação *setrequest*.

As características de segurança associadas ao SNMPv3 permitem o seu uso na gerência de redes VOIP. Apesar das melhorias relacionadas à performance na operação do SNMPv3, deve haver uma atenção especial na gerência de uma quantidade muito grande de equipamentos. A avaliação dos equipamentos que são gerenciados, os objetos a monitorar e a freqüência das consultas deve ser criteriosa para manter o tráfego de gerenciamento dentro de limites aceitáveis.

4.3 Avaliação de Management Information Base (MIB)

O uso do SNMP na gerência da rede envolve a avaliação dos módulos disponíveis na MIB dos equipamentos que serão gerenciados. O objetivo é levantar os objetos e as notificações disponíveis para a gerência do serviço VOIP. MIBs definidas pelo ITU-T , pelo IETF e por alguns fabricantes de equipamentos permitem um acompanhamento do funcionamento do serviço e dos equipamentos. Apesar das MIBs estarem definidas, a implementação nos equipamentos depende do fabricante.

4.3.1 Recomendação ITU-T H.341

A recomendação ITU-T H.341 [60], publicada em 1999 junto com a versão 3 do H.323, definiu um conjunto de MIBs para o gerenciamento de sistemas multimídia baseados nos protocolos H.323 e H.320. Estas MIBs têm por objetivo padronizar as informações de gerenciamento disponíveis em sistemas de conferência multimídia, apresentando objetos que podem ser utilizados para fins de gerenciamento de falhas, performance e configuração. Apesar da importância das informações que oferecem, estas MIBs ainda não são implementadas pela maioria dos dispositivos H.323. Nenhum dos equipamentos e softwares avaliados dispunha destas MIBs.

O uso da MIB H.341 é opcional, entretanto se for implementada em um dispositivo, deve ser dado o suporte a todos os módulos pertinentes, conforme a Tabela 4-1. Os módulos mandatórios devem ser implementados nos dispositivos referenciados. Funções como o suporte a conferência H.323, nem sempre são implementadas nos dispositivos H.323. Neste caso, os módulos MIB correspondentes só devem ser implementados se a função estiver ativada no dispositivo.

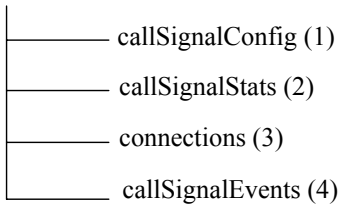
Tabela 4-1– Aplicabilidade de módulos MIB H.341 por tipo de dispositivo H.323

	Terminal	*Gatekeeper*	MCU	*Gateway*
Mandatório	Callsignalling H.245 Terminal RTP	RAS Gatekeeper	Callsignalling H.245 MC RTP	Callsignalling Gateway RTP
Mandatório se o módulo estiver instalado	RAS MC[13] MP[14]	Callsignalling H.245 MC MP RTP	RAS MP	RAS MC MP

MIB H225CallSignalling

Conjunto de objetos que apresenta uma série de informações sobre a sinalização H.225 e sobre as chamadas que estão sendo realizadas pelo dispositivo H.323. Estas informações são organizadas em quatro grupos funcionais:

ccitt(0).null(0).h(8).h341(341).mib(1).mmH323Root(1).h225CallSignalling(1).



O grupo *callSignallConfig* detalha parâmetros que influenciam no comportamento do protocolo H.225. Os objetos apresentam o número máximo de conexões permitidas (*callSignalMaxConfig*), o número disponível de conexões (*callSignalAvailableConections)* e os tempos máximos de espera para o retorno de mensagens de sinalização do dispositivo remoto (*callSignalConfigT301 e callSignalConfigT303*). Objetos que indiquem a porta TCP configurada para receber a sinalização das chamadas (*setup)* não são previstos.

[13] MC (*Multipoint Controller)*
[14] *MP(Multipoint Processor)*

O *callSignalStats* é útil para definir estatísticas das chamadas estabelecidas pelo dispositivo. Apresenta o número de chamadas realizadas e recebidas pelo dispositivo, o número de mensagens de sinalização H225 enviadas e recebidas classificadas por tipo (*setup*, *call proceeding, alerting, setupack, progress, release complete, statusmsg, statusinquiry, facility e notify),* o tempo médio por chamada e o número de conexões ativas.

O grupo *ConnectionEntry* apresenta informações pertinentes às conexões ativas mantidas com outros dispositivos H.323. Em redes IP, para cada chamada são apresentados o endereço IP e o número da porta TCP utilizados na sinalização H.225 e H.245 nos dispositivos envolvidos, identificadores H.225 do dispositivo remoto (H323-ID e E.164), hora de início, os tipos de dispositivo envolvidos na chamada (terminais, MC, MP, *gateway* e *gatekeeper*) e o estado da chamada.

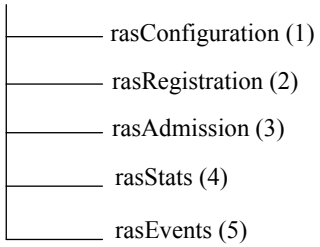
O grupo *callSignalEvents* é utilizado para definir as notificações associadas à sinalização de chamadas. Na recomendação está prevista a notificação *callReleaseComplete*, enviada ao final de uma chamada H.225, onde indica o motivo do término da chamada:

34 - *noBandwidth; no circuit/channel available*
47 - *gatekeeperResources; resource unavailable*
3 - *unreachableDestination; no route to destination*
16 - *destinationReject; destination did not accept this call*
88 - *invalidRevision; incompatible destination*
111- *noPermission; Interworking unspecified*
38 - *unreachableGatekeeper; network out of order*
42 - *gatewayResources; switching equipment congestion*
28 - *badFormaTAddress; invalid number format*
41 - *adaptiveBusy; Temporary Failure*
17 - *inConference; user busy*
31 - *undefined.*

MIB RAS

A MIB RAS apresenta informações relativas à sinalização RAS, sendo organizada em 5 grupos funcionais:

ccitt(0).null(0).h(8).h341(341).mib(1).mmH323Root(1).ras(2).



No grupo *rasConfiguration* são definidas variáveis que descrevem como o dispositivo H.323 opera e em que *gatekeeper* irá tentar se registrar. Nos caso de *gatekeepers,* apresenta informações sobre a própria configuração. Indica o *gatekeeperId,* a porta UDP utilizada no procedimento de *getkeepeerdiscovery*, o tempo de espera pelo retorno de mensagens e o número de retransmissões de mensagens.

O grupo *rasRegistration* apresenta informações sobre os dispositivos registrados no *gatekeeper,* incluindo endereços IP, portas para sinalização de chamadas e apelidos. Quando disponível em dispositivos H.323*,* apresenta somente uma linha com as informações RAS do dispositivo, indicando também o *gatekeeper* onde está registrado.

O grupo *rasAdmission* identifica as chamadas permitidas pelo *gatekeeper*. Em redes IP, indica o endereço IP e as portas TCP utilizadas para a sinalização de chamada do dispositivo que inicia a chamada e do chamado, a indicação de quem iniciou a chamada e o tempo de admissão. Os identificadores da chamada (*ConferenceID, Call Reference Value e Call identifier*) são apresentados, os quais permitem reunir todas as informações sobre a chamada nos *gateways*, *gatekeepers,* terminais envolvidos e mensagens de sinalização associadas à chamada. Caso esteja sendo limitada a largura de banda, é apresentada a banda máxima permitida para a chamada. No *gatekeeper*, apresenta todas as chamadas admitidas em curso, enquanto que no dispositivo é limitada às admissões requisitadas pelo mesmo.

O grupo rasStats apresenta contadores que permitem diagnosticar problemas em pedidos de registro e de admissões no *gatekeeper* e estatísticas das mensagens RAS enviadas e recebidas.

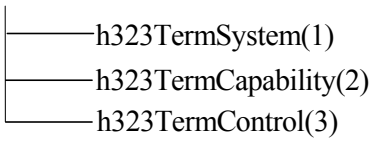
O único evento previsto associado à sinalização RAS é o *admissionReject*. Caso seja habilitado no dispositivo, notificações são enviadas para a estação de gerenciamento quando um pedido de admissão é rejeitado, indicando o motivo:

1 - calledPartyNotRegistered
2 - invalidPermission
3 - requestDenied
4 - undefinedReason
5 - callerNotRegistered
6 - routeCallToGatekeeper
7 - invalidEndpointIdentifier
8 - resourceUnavailable
9 - securityDenial
10 - qosControlNotSupported
11 – incompleteAddress

MIB Terminal

Reúne objetos que apresentam características de terminais H.323, organizados em três grupos:

ccitt(0).null(0).h(8).h341(341).mib(1).mmH323Root(1).h323Terminal(3)



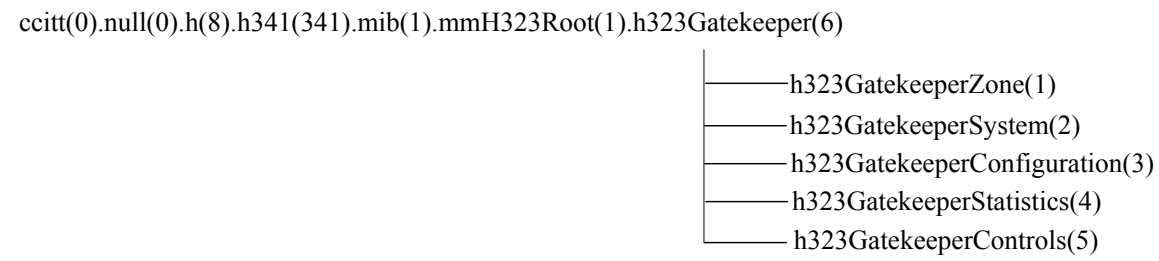
O grupo *h323TermSystem* apresenta uma descrição do dispositivo, indicando versões de hardware e software, fabricante, código do país de origem e localização do terminal.

O grupo *h323TermCapability* apresenta as características operacionais do terminal associados aos algoritmos de áudio e vídeo utilizados.

Os objetos do grupo *h323TermControl* permitem controlar remotamente o dispositivo (*restart, shutdown* e *restart statistics)*

MIB Gatekeeper

Apresenta informações relativas ao *gatekeeper* divididas em 5 grupos:



Os grupos *h323GatekeeperSystem* e *h323GatekeeperConfiguration* apresentam variáveis sobre versões de hardware e software, localização e fabricante do dispositivo e se está habilitado o envio de notificações associadas ao grupo.

Os objetos do grupo *h323GatekeeperZone* apresentam informações relacionadas às "zonas" local e remotas a que o *gatekeeper* está associado, incluindo nome da "zona", endereço IP do *gatekeeper*, largura de banda máxima que pode ser alocada para todas as chamadas na "zona", largura de banda alocada às chamadas ativas e o número de admissões ARQs aceitas e rejeitadas na "zona" local.

O grupo *h323GatekeeperStatistics* apresenta um contador indicando a quantidade de erros no GK e os objetos definindo o erro mais recente, que podem ser utilizados na verificação de problemas associados ao *gatekeeper.* Os erros incluídos neste grupo são somente os relativos ao dispositivo, não incluem erros associados às chamadas.

A variável disponível no grupo *h323GatekeeperControl* pode receber comandos remotos para controle do *gatekeeper* (*Restart, shutdown* e *reset statistics*).

As notificações previstas neste grupo são enviadas nas mudanças no estado operacional do *gatekeeper* (*h323GatekeeperStart* e *h323GatekeeperGoingDown*) ou na ocorrência de um erro. No caso de erros é indicada a severidade (*critical, minor, major* e *warning)* e a provável causa:

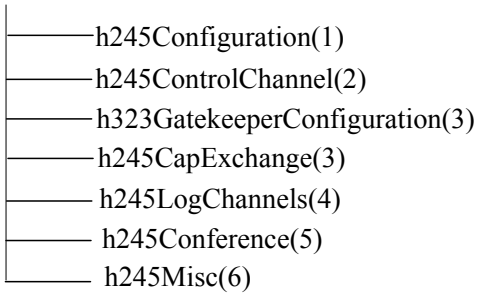
qoSDegraded(2)
lossOfConn(3)
commProtocolError(4)

alarmSignal(5)
performanceDegraded(6)
callEstablishmentError(16)
alarmOnIncomingConn (17)
alarmOnOutgoingConn(18)
lossOfIncomingConn (19)
lossOfOutgoingConn (20)
componentFailure(30)
processingError (31)
congestion(32)
powerProblem(33)

MIB H.245

Apresenta informações relativas ao protocolo de sinalização de mídia H.245, sendo dividido em 8 grupos:

ccitt(0).null(0).h(8).h341(341).mib(1).mmH245Root(3).h245(1)



O grupo *h245Configuration* permite o gerenciamento remoto de vários contadores que definem os tempos limite no recebimento de mensagens do dispositivo remoto (*TerminalCapabilitySetAck, TerminalCapabilitySetReject, OpenLogicalChannelAck, OpenLogicalChannelReject, CloseLogicalChannelAck, RoundTripDelayResponse, Master Slave Determination, RequestModeAck e RequestModeReject*), conforme especificação na recomendação H.245.

O grupo *h245ControlChannel* inclui objetos que descrevem o número máximo permitido de canais H.245, o número de canais ativos, o número de túneis H.245 ativos e um conjunto de contadores associados ao número de mensagens enviadas, recebidas ou com falha em relação ao estabelecimento do canal de controle e à negociação de *master/slave.* Indica também, informações sobre o estado do canal de controle H.245

em todas as chamadas estabelecidas, se *master* ou *slave*, e qual o tipo de dispositivo remoto.

O grupo *h245CapExchange* apresenta uma série de contadores associados às mensagens de negociação de capacidades enviadas, recebidas e as que apresentaram erros. Apresenta ainda uma tabela contendo as várias capacidades associadas a cada dispositivo com que o agente mantém uma chamada ativa, as quais foram enviadas e recebidas durante a negociação *terminal exchange capability*.

O grupo *h245LogChannelsChannel* contém descritores de todas os canais lógicos estabelecidos ou sendo estabelecidos pelo dispositivo. Inclui contadores descrevendo as mensagens de abertura de canais lógicos enviadas, recebidas e que apresentaram algum tipo de erro.

Contadores no grupo *h245conference* descrevem estatísticas relacionadas a conferências H.323.

Tabelas do grupo *h245Misc* descrevem os resultados de mensagens *RoundTripDelayRequest* e *MaintenanceLoopRequest* enviadas conforme a recomendação ITU-T H.245.

MIB Gateway H.323

Esta MIB descreve objetos associados a um *gateway* H.323, que pode estar interligado a redes H.320 ou a redes de telefonia tradicional (PSTN). É dividida em 8 grupos:

ccitt(0).null(0).h(8).h341(341).mib(1).mmH323GatewayRoot(4).h323Gw(1)

- h323GwSystem(1)
- h323GwConfiguration(2)
- h323GwCapabilities(3)
- h323GwConnections(4)
- h323GwCalls(5)
- h323GwStatistics(6)
- h323GwControls(7)
- h323GwNotifications (8)

O grupo *h323GwSystem* descreve o sistema, incluindo fabricante, versões de hardware e software.

O grupo *h323GwConfiguration* apresenta um objeto para habilitar ou não, o envio de notificações associadas a este grupo. Outros objetos descrevem os apelidos (H.323 *alias*) atuando como prefixos de telefone nas portas conectadas a PBXs. Uma limitação desse grupo é que este só permite um prefixo por porta, o que o torna muito restritivo. Inclui ainda a relação dos *gatekeepers* onde está registrado, além do endereço IP e o número de porta onde espera receber as mensagens de sinalização de chamadas. Em gateways conectados à PSTN, indica também o número de portas de voz disponíveis.

Uma tabela no grupo *h323GwCapabilities* identifica os *Codecs* (áudio/vídeo/dados) suportados nas interfaces de rede do *gateway* H.323. A deficiência desta MIB é permitir a identificação de somente um *Codec* para transmissão e de um para recepção, por interface. Não é possível identificar se a interface suporta mais de um *Codec.*

Objetos do grupo *h323GwConnections* descrevem os dispositivos H.323 conectados ao *gateway*. Inclui a descrição de erros ocorridos na conexão, a identificação dos canais de sinalização H.225 e H.245 e dos fluxos RTP utilizados. Em conexões com a PSTN identifica a porta de voz utilizada.

O grupo *h323GwCalls* descreve as chamadas entre dois dispositivos através do *gateway*, basicamente identificando a hora da conexão e a ocorrência de algum erro.

Uma tabela no grupo *h323GwStatistics* descreve o número total de chamadas já estabelecidas, o número de chamadas ativas, o número possível de novas chamadas em função dos recursos disponíveis, o número médio de chamadas simultâneas e o tempo médio por chamada para cada interface do *gateway*. As estatísticas H.323 incluem o número de pacotes recebidos, transmitidos e perdidos, e o número de chamadas H.323 ativas por interface do gateway. Um objeto também indica o número de chamadas ativas mantidas com a PSTN.

O grupo *h323GwControl* permite o recebimento de comandos remotos para controle do equipamento (*restart*, *shutdown* e *reset statistics*).

As notificações que podem ser enviadas pelo *gateway* indicam mudanças no estado operacional do equipamento (*h323GwStart* e *h323GoingDown*) e erros (*h323GwError*) que ocorram, indicando a severidade (*Critical, Minor, Major e Warning)* e as prováveis causas:

qoSDegraded(2)
lossOfConn(3)
commProtocolError(4)
alarmSignal(5)
performanceDegraded(6)
callEstablishmentError(16)
alarmOnIncomingConn (17)
alarmOnOutgoingConn(18)
lossOfIncomingConn (19)
lossOfOutgoingConn (20)
componentFailure(30)
processingError (31)
congestion(32)
powerProblem(33)

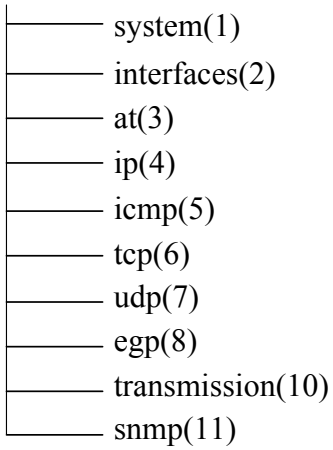
4.3.2 MIBs IETF

Os vários grupos de trabalho do IETF definem uma série de MIBs específicas para o gerenciamento de equipamentos, protocolos, serviços e aplicações. Na gerência do serviço VOIP é importante identificar dentre as MIBs padronizadas, as que apresentam objetos úteis a este objetivo. De qualquer forma, elas só podem ser utilizadas se forem implementadas no equipamento gerenciado.

MIB-II

A MIB-II [62] inclui os objetos básicos que qualquer agente SNMP deve implementar. O uso destes objetos permite adotar soluções comuns a todos os equipamentos que implementam SNMP.

iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1)



O grupo *system* apresenta as características do equipamento, incluindo o hardware e o sistema operacional utilizado, localização, responsável e a indicação do tempo em que o equipamento está operacional. A identificação do fabricante e do modelo do equipamento será utilizada para definir como este é gerenciado.

Uma tabela do grupo *interfaces* apresenta as características, estado operacional, informações estatísticas de tráfego e erros associadas a todas as interfaces do equipamento, incluindo as portas de voz e interfaces virtuais.

O estado operacional das interfaces físicas pode ser monitorado através da variável *ifOperStatus* (Up=1, Down=2, Testing=3, Dormant=5). O objeto *ifAdminStatus* permite habilitar ou desativar interfaces físicas e virtuais.

Os *gateways* Cisco utilizados no projeto-piloto fazem o mapeamento das portas de voz FXS, FXO, E&M e troncos digitais em entradas da tabela de interfaces. Os *dial peers*[15] utilizados para definir o plano de numeração do *gateway* também são representados através de uma interface virtual. Desta forma, é possível identificar todas as portas de voz e *dial-peers* definidos no *gateway*. Em relação às portas de voz é possível verificar se elas estão habilitadas ou não, através do objeto *ifAdminStatus*, e se estão em uso com o objeto *ifOperStatus*. Em relação aos *dial-peers*, é possível verificar se estão ativos ou não através do objeto *ifAdminStatus.*

[15] Dial peer é a entidade lógica responsável por iniciar e receber chamadas. Em cada chamada realizada ou recebida pelo *gateway* haverá um *dial peer* correspondente, selecionado normalmente em função do número destino da chamada

Tabela 4-2 – Valores de *IfType, ifOperStatus e ifAdminStatus* por tipo de interface

<table>
<tr><th colspan="2">Tipo de interface</th><th>ifType</th><th>ifOperStatus</th><th>ifAdminStatus</th></tr>
<tr><td>Portas de Voz</td><td>DS0-group</td><td>81</td><td rowspan="4">Em uso (1)
Dormant – em espera (5)</td><td rowspan="8">Ativado (1)
Desativado (2)</td></tr>
<tr><td></td><td>E&M</td><td>100</td></tr>
<tr><td></td><td>FXO</td><td>101</td></tr>
<tr><td></td><td>FXS</td><td>102</td></tr>
<tr><td></td><td>DS1</td><td>18</td><td rowspan="4">Ativado (1)
Desativado (2)
Testing (3)</td></tr>
<tr><td></td><td>ISDN</td><td>63</td></tr>
<tr><td>Dial-peers</td><td>POTS</td><td>103</td></tr>
<tr><td></td><td>VOIP</td><td>104</td></tr>
</table>

O objeto *ifIndex* é utilizado como índice em outros grupos associados às interfaces. Um problema comum em equipamentos modulares é a mudança do índice associado a uma interface com a inserção ou remoção de módulos. Mecanismos para manter a numeração, mesmo que haja a instalação de novos módulos, devem ser observados na configuração dos equipamentos.

Informações relativas a tráfego (*ifInOctets, ifOutOctets, ifInUcastPkts e ifOutUcastPkts)* e erros (*ifInErrors, ifOutErrors e ifInDiscards)* só estão disponíveis em interfaces físicas.

A MIB *if-Mib* definida através da RFC2863 [63] estende os objetos definidos no grupo *interfaces.* Entretanto, não apresenta extensões que auxiliem a gerência associada ao serviço VOIP.

As notificações *linkup* e *linkdown* previstas no grupo *interfaces* permitem indicar mudanças no estado operacional de interfaces físicas.

No grupo *IP*, a tabela *ipAddrTable* apresenta a configuração IP associada às interfaces do equipamento. A tabela *ipRouteTable* descreve a tabela de roteamento ativa no dispositivo.

Os outros grupos da MIB-II não apresentam informações relevantes para o gerenciamento VOIP. Entretanto, módulos podem ser agregados ao grupo *transmission* específicos para cada tipo de interface.

RFC 1406 – Gerenciamento de troncos E1

Uma extensão no grupo *transmission* definida na RFC 1406 [64] define uma MIB importante no gerenciamento de troncos E1, sendo obrigatória em todo o equipamento que implementa uma interface E1.

As quatro tabelas iniciais apresentam informações sobre a ponta local (*Near End*) do tronco E1, enquanto que as seguintes são relativas à ponta remota (*Far End*). A implementação do grupo de tabelas relativas à ponta remota é opcional.

A tabela *dsx1ConfigTable* apresenta as configurações associadas ao canal E1, as quais podem ser alteradas remotamente com o uso de SNMP. Inclui o tipo (E1, E1-CRC, E1-MF e E1-MF-CRC) onde é possível verificar se está sendo utilizada CRC e multiquadro (MF), o código de linha (HDB3, AMI e B8ZS), o modo de operação (T1 *robbed bit signaling,* E1 CAS e E1 CCS), a fonte do clock (*looptiming, localtiming e throughtiming*) e o estado da linha:

dsx1RcvFarEndLOF	Far end LOF (a.k.a., Yellow Alarm)
dsx1XmtFarEndLOF	Near end sending LOF Indication
dsx1RcvAIS	Far end sending AIS
dsx1XmtAIS	Near end sending AIS
dsx1LossOfFrame	Near end LOF (a.k.a., Red Alarm)
dsx1LossOfSignal	Near end Loss Of Signal
dsx1LoopbackState	Near end is looped
dsx1T16AIS	E1 TS16 AIS
dsx1RcvFarEndLOMF	Far End Sending TS16 LOMF
dsx1XmtFarEndLOMF	Near End Sending TS16 LOMF
dsx1RcvTestCode	Near End detects a test code
dsx1OtherFailure	Any line status not defined here

A tabela *dsx1CurrentTable* apresenta uma série de estatísticas relativas aos últimos 15 minutos de operação do tronco (*errors seconds (ES), severely errors seconds (SES), severely errors framing seconds (SEFS), unavailable seconds (UAS), controlled slip seconds (CSS), path coding violations (PCV), line errored seconds (LES), bursty errored seconds (BES), degraded minutes (DM) e line code violations (LCV)*), importantes na identificação e correção de falhas no tronco.

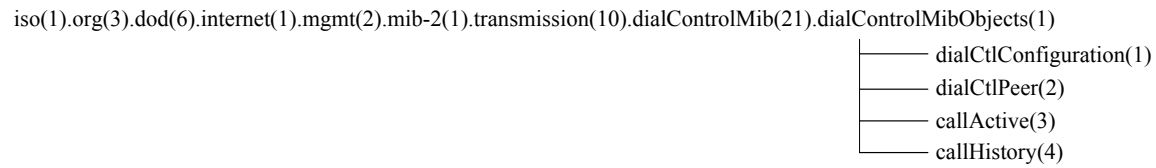
A tabela *dsx1IntervalTable* apresenta as mesmas estatísticas só que relativo ao último período de 24 horas em intervalos de 15 minutos. A tabela *dxs1TotalTable* apresenta estatísticas sobre o número total para cada tipo de erro no período de 24 horas anteriores.

As tabelas do grupo *FarEnd* apresentam as mesmas estatísticas que as tabelas locais e nos mesmos intervalos de amostragem. Entretanto, não são apresentadas variáveis relativas a erros do tipo PVC e LCV.

RFC 2128 – Dial Control MIB

Esta MIB foi desenvolvida para a coleta de informações que permitam monitorar conexões sob demanda realizadas ou recebidas através das várias interfaces físicas. Em cada conexão haverá um par externo para quem estará sendo estabelecida ou de quem estará sendo recebida uma chamada. Na MIB são incluídas as informações necessárias para definir como devem ser estabelecidas as novas conexões, e como identificar quem está estabelecendo uma conexão para o agente que está sendo monitorado. Informações relativas às conexões ativas e um histórico das que já foram realizadas também são mantidas nesta MIB.

A MIB é estruturada em 4 grupos:



Objetos no grupo *dialCtlConfiguration* definem que conexões serão aceitas e se as notificações relativas a esta MIB são enviadas ou não.

No grupo *dialCtlPeer* são mantidas duas tabelas, uma relativa à configuração dos *dial-peers* para onde são estabelecidas ou de onde são recebidas chamadas, e a segunda tabela mantêm estatísticas relativas aos *dial-peers* configurados. Cada *dial-peer* deve ter uma entrada correspondente na tabela de interfaces. Os *gateways* Cisco apresentam um *dial-peer* definido para cada destino estabelecido no plano de discagem do dispositivo, cada um associado a uma interface virtual no grupo *interfaces*. As chamadas recebidas também são associadas a um *dial-peer*, de acordo com o identificador E.164 do dispositivo que iniciou a chamada.

Informações de configuração incluem a interface associada ao *dial-peer* (VOIP, FXO, FXS, E&M, ISDN ou E1), o índice na tabela de interfaces (*ifindex*), o número do telefone do destino de acordo com o plano de discagem, o número de telefone que pode originar chamadas para este *dial-peer,* se está habilitado a receber ou a iniciar chamadas, o tempo de desconexão por inatividade e o tempo máximo da chamada.

As estatísticas incluem o tempo total de duração das chamadas realizadas e o número total de unidades de cobrança associadas ao uso; o número de chamadas realizadas e recebidas com sucesso, das que falharam e das que foram recusadas; o motivo da desconexão da última chamada; e a hora (*sysUpTime*) em que foi recebida a última chamada. Estas estatísticas são úteis para identificar problemas associados a *dial-peers* e a interfaces de voz, e para estabelecer gráficos do número de chamadas realizadas ou que apresentaram algum tipo de problema.

O grupo *callActive* apresenta informações sobre as chamadas ativas indicando a hora de início do estabelecimento da chamada (*Setup Time*) , o número do chamador, o número chamado, a interface, a hora de conexão (*Connection time*), o estado da chamada (*unknown, connecting, connected* ou *active*), o tipo de origem (*originate* ou *answer)* e o tráfego associado à chamada.

Chamadas realizadas através do *gateway* são divididas em dois segmentos (*call legs*), um associado ao *dial-peer* por onde a chamada foi recebida e o outro associado ao *dial-peer* iniciado pelo *gateway* para que a chamada seja completada, como apresentado na Figura 4-3. O primeiro é do tipo *answer*, já que foi iniciada por uma chamada externa. O segundo é do tipo *originate,* já que origina uma conexão a partir do

gateway para o destino da chamada. O tráfego é indicado pela quantidade de bytes e de pacotes recebidos e enviados por cada *call leg*. Na tabela não é definido um objeto que permita associar os dois *call legs*.

A tabela não dispõe de objetos que permitam associar a chamada com as mensagens de sinalização geradas e nem de informações sobre endereços de rede dos dispositivos envolvidos.

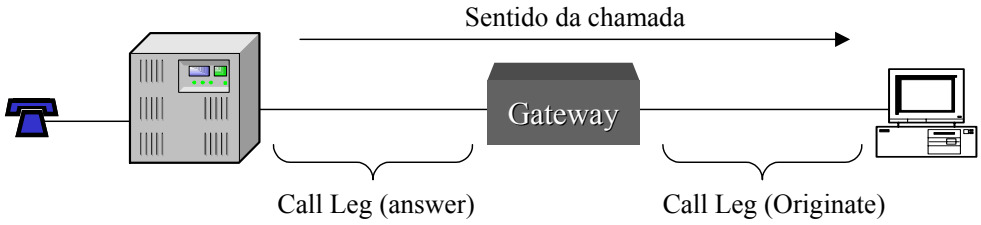


Figura 4-3 – Estrutura de call legs no uso de gateway

O grupo *callHistory* pode manter um histórico das chamadas realizadas. Parâmetros do grupo definem a quantidade máxima de entradas que o agente pode manter e o tempo mínimo que elas devem permanecer armazenadas. São mantidos no histórico, a indicação do *dial-peer* utilizado, a hora de conexão e desconexão, o motivo do término da chamada, o tipo de chamada (*answer* ou *originate*) e o tráfego de rede associado.

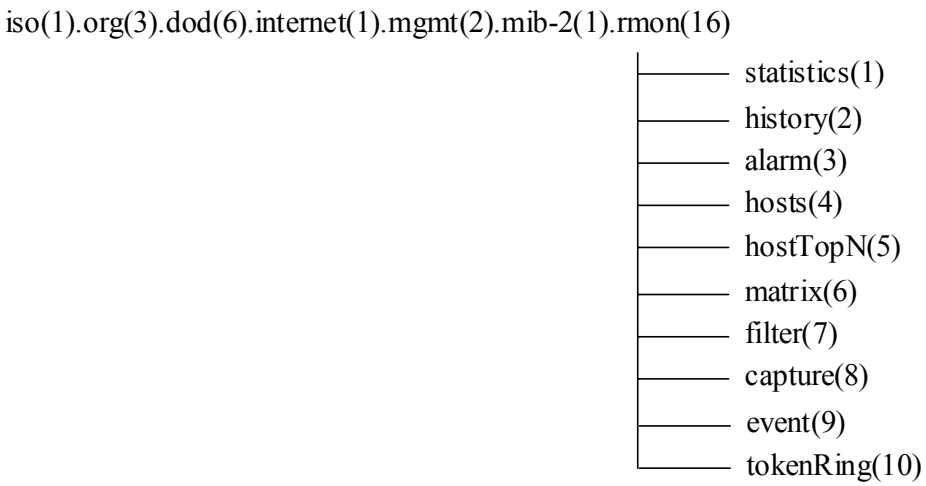
Os objetos *setuptime, connectime* e *disconnecttime* contêm o valor do objeto sysuptime na hora do evento a que relacionam. O cálculo da hora tem que considerar a diferença entre o valor dessas variáveis e o do *sysuptime* na hora da coleta.

Nesta MIB são previstas notificações que podem ser enviadas no início ou no término das chamadas, onde são indicadas as horas de início do estabelecimento (*setup*), do atendimento (*connect*) e do término da chamada (*disconnect*), o tipo de chamada e o motivo do término da chamada.

RFC 2819 – Remote Monitoring MIB

As operações do protocolo SNMP são limitadas aos mecanismos de *polling*, onde variáveis da MIB são consultadas ou alteradas, e ao envio de notificações. A composição das MIBs e as notificações previstas devem ser explicitamente definidas na

implementação do agente SNMP. A proposição original do SNMP era limitada à monitoração do equipamento, não sendo previstos mecanismos que possibilitassem a monitoração das condições dos segmentos de rede. A proposta de uma estrutura de monitoração remota (RMON – *Remote Monitoring*) representou a definição de uma extensão importante para o SNMP, onde monitores de rede (*Probes*) operam em modo "promíscuo", capturando o tráfego do segmento onde estão instalados e possibilitando a emissão de estatísticas, a definição de alarmes que permitam monitorar condições relativas ao comportamento do tráfego analisado, emissão de eventos em função dos alarmes configurados, captura de pacotes ou parte deles em função de filtros pré-definidos, geração de matriz de tráfego e de relatórios de tráfego associados aos equipamentos da rede monitorada [65]. Duas versões de RMON foram definidas, uma baseada na análise das informações embutidas no cabeçalho do quadro MAC (RMON1) e a segunda, nas contidas nos cabeçalhos do pacote de rede (camada 3) e do segmento (camada 4) (RMON2). A seguir são apresentados os grupos RMON1:



A *probe* RMON pode ser configurada remotamente com o uso de SNMP, onde são comandadas as operações que a mesma deve realizar. A MIB RMON mantém uma tabela por grupo, onde são criadas entradas relativas a cada requisição realizada. Uma segunda tabela em cada grupo é utilizada para armazenar as estatísticas e os valores associados a cada requisição efetuada.

No ambiente VOIP, o RMON não se mostrou adequado, visto que não possui mecanismos que permitam a monitoração de fluxos específicos, como necessário para a monitoração das chamadas. Entretanto, o mecanismo de alarmes pode ser estendido para que variáveis numéricas da MIB sejam monitoradas e comparadas a limites (*thresholds*) definidos, sendo possível especificar limites superiores e/ou inferiores. Entradas podem ser criadas no grupo eventos para que seja emitida uma notificação SNMP, caso os limites sejam ultrapassados. A fim de evitar a emissão contínua de eventos em casos de oscilação da variável monitorada é empregado o mecanismo de histerese, como apresentado na Figura 4-4 .

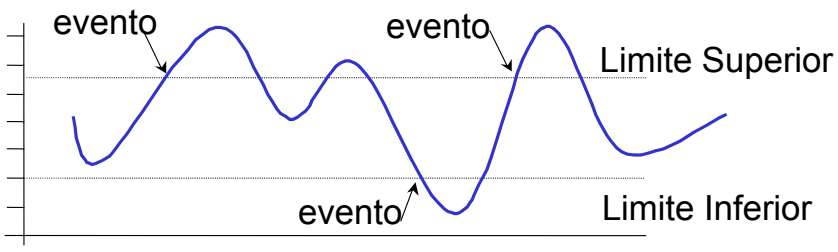


Figura 4-4 – Mecanismo de histerese associado a eventos RMON

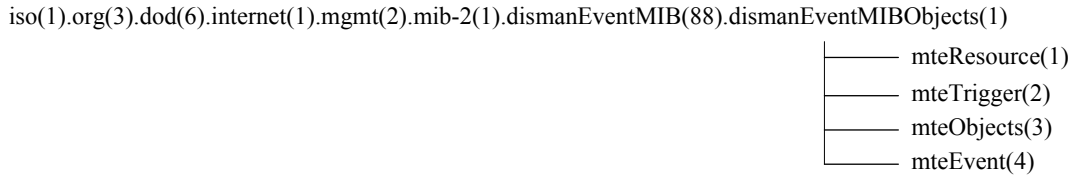
Os grupos *alarm* e *event* podem ser implementados em qualquer dispositivo SNMP, mesmo que os outros grupos não o estejam. Desta forma, variáveis associadas a tráfego e às condições de chamadas VOIP podem ser monitoradas, gerando uma notificação SNMP quando ultrapassados os limites definidos.

RFC 2981 – Event MIB

O envio de notificações indicando alguma falha ou indício de que algo não está funcionamento corretamente é importante para o gerenciamento de uma rede. A concepção original do SNMP previa somente as notificações já pré-definidas na MIB, não havia a possibilidade de criar novas sob demanda. A MIB *Event* definida na RFC 2981 utilizou conceitos da MIB RMON para mudar essa concepção, criando a possibilidade de que variáveis da MIB sejam monitoradas, e que ao ultrapassarem limites pré-definidos ou assumam determinados valores, possam gerar uma notificação ou alterar o conteúdo de outras variáveis [66]. Esta MIB difere da MIB RMON na possibilidade de haver testes e dos diferentes tipos de variáveis que podem ser testadas.

No RMON somente variáveis numéricas poderiam ser avaliadas. A MIB depende do uso de SNMPv3, sendo composta de 4 grupos:

Na tabela *mteTrigger* são definidos os objetos que são monitorados e como, relacionando-os ao disparo de um evento. São previstos três tipos de operação com os objetos:



- *existence* - gera um evento se o objeto existir, se não existir ou se foi alterado
- teste booleano - verifica se o objeto é igual, diferente, maior ou menor que um valor determinado
- *threshold* - gera um evento se o objeto ficar acima de um limite superior (*Rising),* abaixo de um limite inferior *(Falling)* ou em qualquer uma das duas situações.

A tabela *mteObjects* define os objetos que devem ser adicionados à notificação quando esta é enviada. A seleção dos objetos deriva do tipo de evento e no tipo de teste que foi realizado.

A tabela *mteEvent* define a ação que é tomada quando um evento ocorre. Pode ser enviada a notificação, ser atribuido um valor a uma variável da MIB ou ambos.

RFC 2982 - Distributed Management Expression MIB

A *expression MIB* permite a criação de novos objetos na MIB a partir da definição de uma expressão complexa, onde podem ser referenciados outros objetos [67]. O uso em conjunto com a MIB *Event* permite uma mudança na filosofia da gerência SNMP, antes focada no mecanismo de "*polling*", para uma gerência baseada em eventos. Desta forma, pode ser reduzido o tráfego associado a SNMP, além de permitir uma reação mais rápida a falhas que possam ocorrer na rede.

O uso desta MIB permite criar expressões do tipo:

Percentual de pacotes perdidos = (lostpackets / (receivedPkts + lostPackets))

Um evento poderia ser configurado para gerar uma notificação, caso o percentual de perdas associado a um fluxo RTP ultrapasse 1% dos pacotes recebidos.

RFC 2959 – RTP MIB

As informações de gerenciamento relativas ao protocolo RTP são apresentadas na MIB RTP [67], sendo organizada em 6 grupos:

iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).rtpMIB(87).rtpMIBObjects(1)

- rtpSessionInverseTable(2)
- rtpSessionTable(3)
- rtpSenderInverseTable(4)
- rtpSenderTable(5)
- rtpRcvrInverseTable(6)
- rtpRcvrTable(7)

Na tabela *rtpSessionTable* são apresentadas informações sobre as sessões RTP ativas, identificando a hora em que foram iniciadas, o protocolo de transporte utilizado, o endereço IP e o número da porta associado ao RTP e ao RTCP no dispositivo local e no remoto.

A tabela *rtpSenderTable* descreve os emissores dos fluxos RTP , incluindo o identificador *Synchronization Source (SSRC),* o endereço IP e número de porta do emissor, o número de pacotes, bytes e *sender reports (SR)* transmitidos, a hora do último SR recebido e o *payload type* do último pacote RTP recebido.

A tabela *rtpRcvrTable* lista informações sobre os receptores dos fluxos RTP. Variáveis desta tabela indicam o SSRC do emissor e do receptor, o endereço IP e a porta do receptor, o *round trip time* (RTT), o número de pacotes perdidos, o *jitter,* o número de pacotes RTCP *receiver report (RR)* recebidos e o número de pacotes e bytes recebidos no fluxo RTP. As entradas são associadas ao par *Sender/Receiver* dos fluxos RTP.

As tabelas inversas são utilizadas para relacionar as sessões com o emissor e receptores dos fluxos RTP.

A MIB RTP pode ser implantada nos dispositivos emissores ou receptores do fluxo RTP, ou em estações que monitorem os fluxos RTP estabelecidos na rede.

4.3.3 MIBs privadas

MIBs desenvolvidas por fabricantes dos equipamentos utilizados em redes VOIP podem atender a necessidades não previstas nas MIBs definidas através do IETF. Como a implementação destas MIBs depende do fabricante e do modelo de equipamento, uma solução de gerenciamento baseada nos objetos disponíveis nestas MIBs fica restrita a redes que utilizem estes dispositivos. Nos equipamentos utilizados no projeto-piloto foi possível identificar uma série de MIBs que permitem a configuração e monitoração dos vários componentes de um *gateway* de voz. A descrição das MIBs analisadas pode ser encontrada em http://www.cisco.com/cgi-bin/Support/Mibbrowser/mibinfo.pl?tab=4.

Cisco-Voice-If-MIB

Esta MIB apresenta informações comuns a todas as interfaces de voz do *gateway*, digitais ou analógicas, sendo composta da tabela *cvIfCfgTable.*

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).cisco(9).ciscoMgmt(9).ciscoVoiceInterfaceMIB(64).
cvIfObjects(1).cvIfCfgObjects(1).

Esta tabela permite a configuração e a monitoração dos parâmetros: ruído de fundo, controle do recurso *music on hold* (MOH), ganho inserido no sinal de entrada, atenuação na transmissão do sinal, cancelamento de eco, tipo de conexão (*trunk, plar* e *normal*), padrão de tons adotado e o tempo máximo entre dígitos (*Inter digit timeout*).

O tipo de conexão define o comportamento da porta de voz ao receber a sinalização de uma nova chamada pela rede de telefonia. Quando configurada em modo *normal*, o usuário recebe um segundo tom de discagem, quando deve digitar o número do destino para que a chamada possa ser estabelecida. O *gateway* estabelece um novo *call leg* com base no número digitado. No modo *Private Line Automatic Ringdown* (PLAR), ao receber a sinalização de uma nova chamada na porta de voz, o *gateway* estabelece um novo *call leg* com base em um número previamente definido na configuração da porta. Este número pode ser definido através da variável *cvIfCfgConnectionNumber*. No modo *trunk*, é definido um *call leg* permanente entre a porta de voz e o destino, sendo que o destino também é definido através desta variável. Este modo é utilizado normalmente na conexão de PBXs.

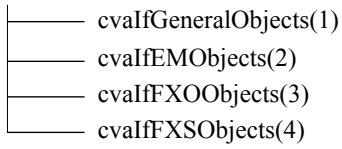
O padrão de tons adotado na sinalização para o usuário (*dial tone, ring tone, busy tone)* é definido conforme o país, havendo um código específico para cada um. Esta configuração deve ser compatível com a configuração do PBX. O mecanismo FXO *supervisory disconnect* só funciona quando este parâmetro é configurado corretamente.

As portas de voz são associadas à tabela *interfaces* da MIB-II através da variável *ifIndex.*

Cisco-Voice-Analog-If-MIB

Esta MIB apresenta variáveis de gerenciamento específicas de portas de voz analógicas do tipo *Foreign Exchange Station (FXS), Foreign Exchange Office (FXO) e Ear&Mount (E&M)*, sendo dividida em 4 grupos:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).cisco(9).ciscoMgmt(9).ciscoVoiceAnalogIfMIB(62).
cvaIfObjects(1)



O grupo *cvaIfGeneralObjects* indica a impedância nas portas de voz, se estas têm *Digital signal Processor* (DSP) embutido e a quantidade de erros de sinalização associados a cada uma das portas analógicas.

Os três grupos restantes são específicos por tipo porta, apresentando uma entrada para cada tipo suportado. No caso das portas FXO pode ser configurado ou monitorado o tipo de sinalização (*loopstart* ou *groundstart*), o número de toques antes do atendimento, a supervisão de desconexão, o tipo de discagem (*pulse* ou *DTMF)* e a temporização (*DigitDuration, InterDigitDuration, PulseRate* e *PulseInterdigitDuration*) associados às portas. Permite ainda monitorar o estado da porta (*onhook* ou *offhook*) e se está sendo recebida a sinalização de uma nova chamada (*Ring*).

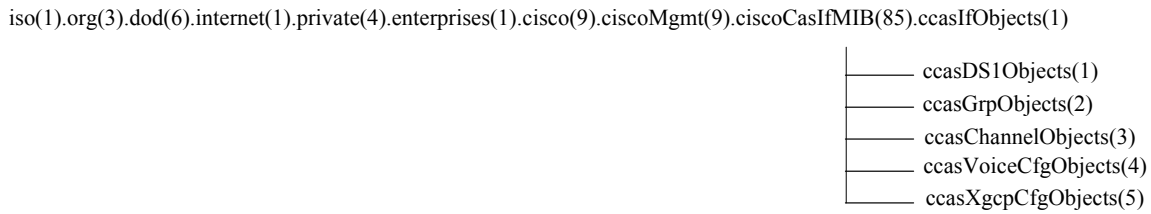
A tabela de portas FXS apresenta objetos que permitem visualizar e alterar a sinalização adotada (*loopstart* ou *groundstart),* a freqüência do sinal indicando novas chamadas e a temporização associada. Permite ainda monitorar se a porta está recebendo a sinalização de uma nova chamada.

A tabela *cvalIfEMObjects* apresenta objetos associados ao tipo utilizado, à sinalização, operação e o tipo de discagem adotados em portas E&M.

Esta MIB junto com Cisco-VOICE-IF-MIB permite a gerência das portas de voz analógicas associada à área de falhas e configuração.

Cisco-CAS-IF-MIB

Esta MIB estende a MIB definida na RFC 1406 para o gerenciamento de troncos E1/T1 que utilizam sinalização CAS (*Call Associated Signal)*. Neste tipo de tronco, os canais DS0 (64Kbps) são agrupados em grupos (CAS-group), aos quais é atribuída uma sinalização comum, por exemplo, *loopstart*, *groundstart*, E&M e E1-R2. O canal 16 do tronco E1 é utilizado para o transporte da sinalização associada ao canal, para cada canal DS0 são associados 4 bits para fins de sinalização (bits ABCD). Os canais DS0 selecionados devem ter correspondência com os do tronco proveniente do PBX. No caso de troncos E1 podem ser selecionados até 30 canais DS0 para formar um grupo. A MIB é composta de 5 grupos:



O grupo *ccasDS1Objects* contém um objeto que descreve os canais DS0 alocados em cada tronco DS1. No caso de troncos E1 são alocados 4 octetos para este fim, onde cada bit corresponde a um dos canais DS0 alocado. Um bit configurado com o valor 1 indica que o canal está associado ao grupo CAS.

O grupo *ccasGrpObjects* apresenta a configuração de cada grupo CAS definido no *gateway,* onde são indicados os canais DS0 alocados e o tipo de sinalização utilizado. Tabelas no grupo são dedicadas às características de cada tipo de sinalização, onde são apresentados objetos detalhando a configuração associada ao tipo de sinalização utilizado.

O grupo *ccasChannelObjects* é composto de uma tabela que permite a configuração do recurso *busyout* associado a cada canal DS0 utilizado no *gateway.*

Quando esta opção está ativada, o PBX recusa chamadas provenientes do PBX através do respectivo canal. Uma segunda tabela permite monitorar os canais indicando o estado dos bits ABCD recebidos e transmitidos na sinalização do canal, a situação do mecanismo de *busyout* e a indicação do uso do canal (*speech, data, vídeo, fax* ou *modem*).

A tabela *ccasVoiceCfgEntry* apresenta a configuração específica de voz para cada canal DS0 utilizado, indicando ganho, atenuação, cancelamento de eco, ruído de fundo, o nível de MOH, padrão de tons e o tipo de conexão utilizada (*plar, trunk* ou *comum).*

A associação das informações aos troncos é realizada através da variável *ifIndex* do grupo *interfaces*. Os objetos desta MIB são basicamente para fins de configuração não havendo objetos que permitam gerenciar falhas associadas aos troncos.

Cisco-Class-Based-QOS-MIB

Nesta MIB estão disponíveis objetos que permitem obter a configuração e estatísticas associadas à configuração QoS de equipamentos Cisco, divididos em 21 tabelas:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).cisco(9).ciscoMgmt(9).ciscoCBQosMIB(166)

Os objetos QoS configurados nestes equipamentos associados à configuração QoS, passíveis de serem monitorados, incluem: *matchStatements*, *classMap*, *FeatureAction*, *PolicyMap* e *ServicePolicy*.

MatchStatements apresentam as condições utilizadas para a classificação dos pacotes IP. Inclui classificação baseada em endereço IP, IP DSCP, intervalo de portas UDP, protocolo, interface e COS (*class of service*)

ClassMap estão associados a classes de tráfego criados no equipamento para onde são direcionados os pacotes conforme a classificação realizada pelas condições definidas em *matchStatement.* Cada classe pode ser associada a um ou mais critérios de classificação.

Feature Actions estão associados à definição das ações possíveis de serem aplicadas no tráfego que está sendo classificado. Inclui *traffic-shapping*, associação a filas específicas (LLQ) , uso de RED (*Random Early Packet Discard*) e a marcação de pacotes (DSCP, IP Precedence, MPLS Exp, L2 COS).

PolicyMap está associado à configuração que associa as ações possíveis em cada uma das classes definidas.

Service Policy está associado à configuração da política de QoS que é utilizada nas interfaces dos equipamentos.

O interesse nesta MIB está na avaliação dos descartes de pacotes ocorridos em cada classe de serviço especificada no equipamento. Na configuração de QoS relacionado aos canais de mídia VOIP deve ser definida uma classe associada a uma fila LLQ (*Low Latency Queue*), para a qual devem ser direcionados os pacotes associados a este tráfego. Esta fila deve ter uma largura de banda garantida nas interfaces de saída do equipamento. Os pacotes classificados podem ser marcados com DSCP 46 (0x101110), indicativo de tráfego EF (*Expedited Forwarding*). A classificação dos pacotes que chegam e que devem ser direcionados a esta classe, pode ser feita com base no endereço IP ou no valor do campo IP DSCP. Recomendações do fabricante indicam que o tráfego associado à sinalização das chamadas deve ser marcado com DSCP af31 (0x011010). A avaliação das estatísticas associadas à classe criada permitirá verificar o tráfego gerado (*cbQosCMPostPolicyBitRate*) e o tráfego descartado (*cbQosCMDropBitRate*), ambos medidos em bits por segundo. A avaliação de que há tráfego descartado pode gerar um tráfego excessivo associado à classe ou que a largura de banda reservada não está adequada ao tráfego associado à classe.

Não existem notificações definidas nesta MIB.

Cisco-DSP-MGMT-MIB

O *Digital Signal Processor* (DSP) são os responsáveis pelo processamento na conversão do sinal de voz em pacotes. No *gateway*, um DSP pode tratar várias chamadas simultâneas, o número depende da capacidade do DSP e da complexidade do *Codec* utilizado. *Codecs* são classificados em duas categorias: média (G.711, G.726, G.729A e G.729AB) e alta complexidade (G.728, G.723, G.729 e G.729B). Os DSPs

utilizados atualmente em *gateways* Cisco suportam 4 chamadas utilizando *Codecs* de média complexidade ou duas chamadas de alta. A monitoração dos recursos disponíveis no DSP a sua operação constituem uma necessidade importante na gerência de *gateways* de voz.

A MIB Cisco-DSP-MGMT é composta do grupo *cdspMgmtObjects* que contém duas tabelas: *cdspCardStatusTable* e *cdspStatusTable*. A primeira apresenta uma entrada para cada cartão DSP instalado no *gateway,* indicando o seu estado operacional e o consumo de recursos. A segunda apresenta informações sobre cada um dos DSPs.

Notificações podem ser enviadas se um cartão DSP for reinicializado devido a problemas.

Cisco-Dial-Control-MIB

A MIB *Dial-Control-MIB,* definida através da RFC 2128, utiliza índices para a tabela associada ao histórico das chamadas (*callActiveSetupTime e callActiveIndex*) que dificultam o acesso por algumas ferramentas de gerência, já que o primeiro índice referencia um tempo relativo. Com o objetivo de facilitar o acesso às informações disponíveis sobre as chamadas já finalizadas foi criada uma nova tabela que utiliza um índice mais objetivo (*cCallHistoryIndex*), facilitando o acesso. Este índice indica a ordem de entrada da chamada nesta tabela.

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).cisco(9).ciscoExperiment(10).ciscoDialControlMib(25).
ciscoDialControlMibObjects(1)
└——— cCallHistory(1)

As informações são as mesmas que as da MIB *Dial-Control-MIB,* inclusive o fato de não possuir uma forma de associar os dois *call legs* de uma chamada.

Nos experimentos, foi possível identificar uma variável não documentada na MIB (*cCallHistoryEntry.20*), que apresenta o mesmo comportamento que o VSA *Release-Source* (Tabela 5-6), permitindo identificar por qual dos dois *call legs* associados à chamada foi iniciada a desconexão. Desta forma, é possível utilizar o motivo de desconexão associado a este *call leg* para identificar a causa da desconexão da chamada.

Cisco-Voice-Dial-Control-MIB

Esta MIB complementa as informações apresentadas na MIB Dial-Control-MIB para descrever os *dial-peers* e os *call legs* associados às chamadas. A MIB é dividida em 4 grupos:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).cisco(9).ciscoMgmt(9).ciscoVoiceDialControlMIB(63)
.cvdcMIBObjects(1)

- cvGeneralConfiguration(1)
- cvPeer(2)
- cvGatewayCallActive(3)
- cvGatewayCallHistory(4)

O grupo *cvGeneralConfiguration* apresenta um objeto que é utilizado para controlar o envio de notificações associadas à qualidade da voz das chamadas. Quando habilitada, uma notificação é enviada quando termina uma chamada e é verificado que apresentou problemas associados à qualidade da voz. O parâmetro ICPIF[16], calculado conforme a recomendação ITU-T G.113 [72], é utilizado para avaliar a qualidade das chamadas em função de interferências que estas recebem na transmissão. No cálculo deste parâmetro são utilizadas parcelas, cujos valores dependem do *Codec* utilizado, da perda de pacotes e do atraso medido no fluxo RTP recebido. Chamadas que terminam com um ICPIF superior a um valor pré-definido, 20 por padrão, disparam o envio da notificação *cvGeneralPoorQoVNotification*.

Tabela 4-3 – Qualidade de voz associada a valores de ICPIF

Valores do fator ICPIF	Qualidade da voz
0 a 5	Muito boa
6 a 10	Boa
11 a 20	Adequada
21 a 30	Regular
31 a 45	Ruim
46 a 55	Péssima

[16] ICPIF (*Calculated Planning Impairment Factor)* é calculado com base nos fatores da transmissão que interferem na qualidade da chamada. Os fatores considerados pelo fabricante podem ser obtidos em http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00800946f8.shtml

O grupo *cvPeer* permite gerenciar a configuração dos *dial-peers*, entidade com a qual são estabelecidas as chamadas iniciadas ou recebidas pelo *gateway.*

Cada chamada tratada pelo *gateway* envolve dois *call legs*, cada um associado a um *dial-peer*. Objetos distribuídos em 4 tabelas representam as características específicas de cada tipo de *dial-peer* que pode ser estabelecido*: Voice,* VoFR e VOIP.

Os grupos *cvGatewayCallActive* e *cvGatewayCallHistory* apresentam informações complementares sobre as chamadas ativas e das que já terminaram. A MIB *Dial Control MIB* descrita na RFC 2128 apresenta os grupos *callActive* e *callHistory* que permitem obter informações sobre as chamadas ativas e um histórico das que já foram realizadas. Entretanto, apresenta alguns problemas que dificultam a avaliação de uma chamada. Nas duas tabelas, as informações são específicas para cada *call leg*, não existem variáveis que relacionem os dois *call legs* associados a cada chamada realizada através do *gateway*. As tabelas também não têm variáveis que permitam uma associação com os fluxos de sinalização H.323.

Nesta MIB, duas tabelas são associadas às chamadas ativas e duas às que já terminaram. Das duas utilizadas em cada grupo, uma é relativa a *call legs* tipo POTS, ou seja, de telefonia, e outra aos do tipo VOIP. Desta forma, características específicas de cada tipo de *call leg* podem ser descritas na MIB. As duas tabelas do grupo *cvGatewayCallActive* são uma extensão à tabela de chamadas ativas definidas na MIB *Dial-Control-MIB*. O índice utilizado é o mesmo *(callActivesetupTime e callActiveIndex)*. Desta forma, para cada chamada realizada através do *gateway*, existe um *call leg* tipo POTS representado através de entradas na tabela *callActiveTable* da *Dial-Control-MIB* e na tabela *cvCallHistoryTable* desta MIB, as duas relacionadas através do mesmo índice; e um *call leg* tipo VOIP representado na *Dial-Control-MIB* e na tabela *cvVoIPCallActiveTable.* As informações dos dois *call legs* podem ser relacionadas através do objeto *callActiveConnectionId*, disponível nas duas tabelas da MIB Cisco. Este objeto também permite relacionar os *call legs* com os CDRs gerados pelo *Radius.*

Informações disponíveis na tabela *cvVoIPCallActiveTable* permitem identificar o endereço IP e a porta TCP utilizada pelo dispositivo remoto, a indicação se está sendo

utilizada alguma política de QoS, VAD, o *Codec*, informações sobre os mecanismo de compensação de *jitter* e de pacotes perdidos *(CvVoIPCallActiveGapFillWithSilence, cvVoIPCallActiveGapFillWithPrediction, cvVoIPCallActiveGapFillWithInterpolation* e *cvVoIPCallActiveGapFillWithRedundancy)*, além de informações que permitem analisar como se comportam os fluxos de mídia RTP associados à chamada, importantes para fins de monitoração da qualidade das chamadas (*cvVoIPCallActiveLostPackets, cvVoIPCallActiveEarlyPackets, cvVoIPCallActiveLatePackets e cvVoIPCallActiveReceiveDelay*).

Quatro objetos não documentados na MIB (*cvVoIPCallActiveEntry.24, cvVoIPCallActiveEntry.25, cvVoIPCallActiveEntry.27 e cvVoIPCallActiveEntry.28*) identificaram o endereço IP e a porta TCP utilizados na comunicação entre o *gatekeeper* operando como *proxy* RTP e o terminal H.323. Estas informações são importantes, pois permitem identificar todos os dispositivos envolvidos mesmo com o uso de *proxy*.

O grupo *cvGatewayCallHistory* representa uma extensão à Cisco-Dial-Control-MIB, mantendo informações sobre chamadas já terminadas. As duas se relacionam com o uso do mesmo índice para as duas tabelas (*cvCallHistoryIndex*). Em função dos problemas associados aos índices utilizados na *Dial-Control-MIB*, a Cisco não utiliza a tabela *callHistory* em seu *gateways*. Neste grupo são mantidas informações importantes sobre as chamadas já finalizadas, principalmente em relação aos *call legs* tipo VOIP. Além das mesmas informações disponíveis na tabela de chamadas ativas, é possível obter informações sobre o ICPIF associado à chamada, o que define como foi a qualidade média da chamada. A associação dos *call legs* e dos CDRs *Radius* gerados para uma chamada podem ser relacionados através do objeto *callHistoryConnectionId.*

Dois objetos da *Cisco-Call-History-MIB* (*ciscoCallHistoryTableMaxLength* e *ciscoCallHistoryRetainTimer)* definem o número máximo de entradas e o tempo mínimo em minutos que as mesmas devem ser mantidas no histórico de chamadas.

CISCO-RTTMON-MIB

A monitoração ativa permite uma verificação das condições da rede mesmo na ausência de tráfego "real". Desta forma, é grande a possibilidade de identificar

problemas antes que sejam percebidos pelos usuários. Como o serviço VOIP é susceptível à perda de pacotes, a atrasos na entrega dos pacotes e ao *jitter*, é importante que estas métricas sejam avaliadas. Os *gateways* desenvolvidos pela Cisco implementam o agentes SAA (*Service Assurance Agent*) que permitem a monitoração ativa da rede, onde vários fatores podem ser avaliados. No caso do VOIP, é possível enviar uma rajada de pacotes UDP entre *gateways* para que sejam obtidas informações de variação no atraso (*jitter*), perda de pacotes e tempo médio de retorno dos pacotes (RTT). Versões mais recentes de sistema operacional permitem medir *one-way delay*, considerando que o agente SAA e o *responder* estejam sincronizados com uso de NTP. A transmissão é realizada utilizando pacotes com mesmas características que os associados aos fluxos RTP, garantindo o mesmo tratamento dispensado a estes ao longo da rede. Além da monitoração dos resultados através de uma MIB específica, é possível disparar eventos que notifiquem problemas relativos à monitoração que está sendo realizada.

Uma preocupação no uso desta facilidade é o consumo de recursos dos equipamentos envolvidos. O manual do usuário do serviço [69] descreve o cálculo do consumo de CPU e memória em função do número de operações realizadas. Limites podem ser estabelecidos para que a performance do equipamento não seja afetada.

4.4 Contabilização e Tarifação de Redes VOIP

O uso do serviço de telefonia tradicional é tarifado com base no tempo de utilização. O modelo utilizado para a contabilização dos recursos utilizados e a respectiva tarifação é baseado na coleta dos registros de detalhamento das chamadas, os *Call Detail Records* (CDRs), gerados pelos equipamentos envolvidos e que descrevem informações relativas a cada chamada realizada.

A arquitetura utilizada em redes VOIP para a contabilização de recursos envolve a interação entre os dispositivos da rede, servidores de contabilização, e servidores de tarifação. Os dispositivos de rede coletam os dados relativos ao consumo de recursos associados a cada uma das chamadas. Estas informações são transferidas para um servidor, via um protocolo específico, para que possam ser processadas. Este processamento envolve a consolidação de todas as informações recebidas associadas a

cada chamada, com a eliminação de informações duplicadas. As informações podem então ser repassadas às aplicações responsáveis pela tarifação dos recursos consumidos.

Informações coletadas dos CDRs podem ser utilizadas também na identificação de problemas no funcionamento da rede. Dados como o número de chamadas não completadas ou as que terminam de forma anormal podem ser utilizados para este fim.

Os protocolos utilizados atualmente para fins de transferência das informações de contabilização em redes IP são o *Simple Network Management Protocol* (SNMP) e o *Remote Authentication Dial In User Service* (Radius) . Os dois apresentam métodos diferentes para a transferência. O primeiro utiliza o método de "*polling*", onde variáveis MIB contendo um histórico das chamadas são consultadas através de requisições SNMP. O segundo opera com a orientação a eventos, onde o dispositivo de rede envia os CDRs durante a realização e ao término de uma chamada.

Informações sobre as chamadas realizadas através do sistema VOIP são importantes para o:

- gerenciamento de falhas - avaliar chamadas não completadas ou que terminaram por falha. A correlação das causas das desconexões a outros fatores pode auxiliar na identificação de problemas na rede;
- gerenciamento de contabilidade - contabilizar o número de chamadas realizadas, identificando os usuários envolvidos e os recursos consumidos.
- gerenciamento de performance - avaliação do tráfego associado ao serviço, que pode ser utilizado para a definição da largura de banda a ser reservada para o serviço VOIP, garantindo a qualidade necessária. Uma avaliação da qualidade da voz associada a cada chamada também pode ser avaliada para a identificação de problemas na rede e para a geração de estatísticas associadas ao serviço.
- gerenciamento de configuração - identificação da necessidade de investimentos na aquisição de novos equipamentos ou componentes, tais como, novas portas de voz. Investimentos na infra-estrutura de rede ou da telefonia para dar suporte ao serviço também podem ser identificados.

4.4.1 Remote Authentication Dial In User Service (Radius)

O protocolo *Remote Authentication Dial In User Service* foi desenvolvido inicialmente para uso dos provedores de acesso Internet na autenticação de usuários e autorização no uso dos serviços oferecidos. O protocolo é utilizado para o transporte de informações entre um servidor central *Radius*, onde são mantidos os perfis dos usuários cadastrados, e o equipamento a que o usuário se conecta, o *Network Access Server* (NAS). Através de mensagens *access-request*, o NAS solicita a validação dos usuários que se conectam. O servidor *Radius* valida o usuário baseado no nome do usuário e na senha fornecida e, caso seja aceito, uma mensagem *access-accept* é enviada ao NAS com informações sobre a configuração e os serviços que o usuário está autorizado a utilizar.

A aplicação *Radius* usa o modelo cliente/servidor, utilizando o protocolo UDP no transporte das mensagens entre os dispositivos e o servidor. Um exemplo simplificado do processo de autenticação *Radius* é apresentado na Figura 4-5.

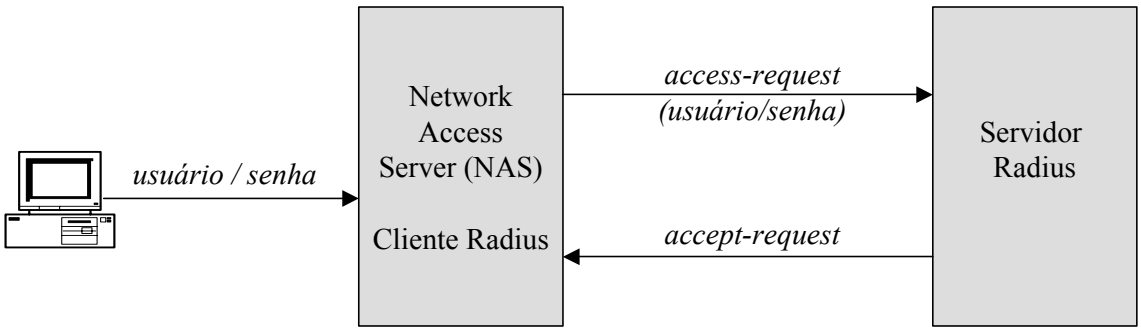


Figura 4-5 – Esquema simplificado de autenticação de usuário com Radius

Extensões foram implementadas no protocolo *Radius* para que informações com a contabilização dos recursos consumidos nas sessões estabelecidas sejam enviadas pelo NAS ao servidor *Radius*, que irá armazená-las para que sejam processadas e analisadas. Registros indicando detalhes das chamadas, os CDR (*Call Detail Records*), são repassados ao servidor *Radius* através de mensagens *accounting-request*. O servidor *Radius* confirma o recebimento e o correto armazenamento das informações com a mensagem *accounting-response*. O servidor Radius não envia nenhuma mensagem, se houver algum problema com o CDR ou no armazenamento das informações. Caso o

NAS não receba a mensagem de confirmação, é prevista a retransmissão da requisição e, havendo a persistência do problema, a mensagem é enviada para servidores *Radius* alternativos. O mecanismo de tratamento de retransmissão não está definido na RFC, o que pode levar a diferentes implementações. Em todas as soluções avaliadas nos experimentos foi possível configurar nos dispositivos, *gatekeepers* e *gateways,* vários servidores alternativos e o número de retransmissões para cada servidor. Entretanto, o CDR é perdido se todos os servidores apresentam problema, o que prejudica a tarifação e as estatísticas. Outros mecanismos para obter estas informações devem ser previstos para que as informações sobre as chamadas realizadas não sejam perdidas, como descrito no capítulo 5.4.

No envio de informações de contabilidade, três diferentes mensagens são utilizadas, como especificado em [70]: *start*, enviada no início da sessão; *interim*, opcionalmente enviada em intervalos de tempo pré-definidos ao longo da sessão, como sugerido em [71]; e *stop*, enviada ao final da sessão, informando a duração, o tráfego gerado e a causa da desconexão. Na Figura 4-6 é apresentado um esquema simplificado dos procedimentos adotados pelo Radius.

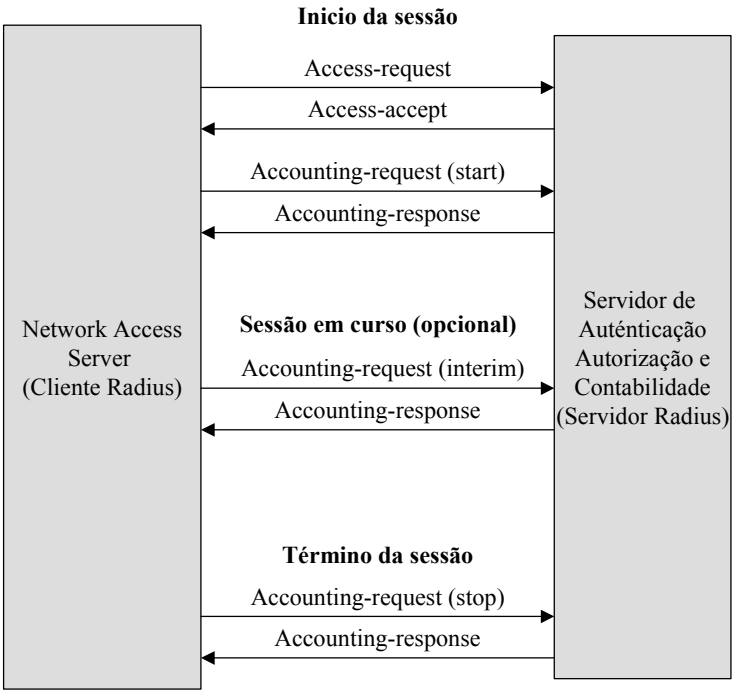


Figura 4-6 – Esquema simplificado do protocolo Radius

4.4.2 Atributos *Radius* para Fins de Contabilização

Mensagens *radius* incluem seqüências de atributos, onde cada um é representado pela tupla tipo, tamanho e valor, como apresentado na Figura 4-7.

Tipo (8 bits)	Tamanho (8 bits)	Valor (tamanho variável)

Figura 4-7 – Formato dos atributos *Radius*

O campo tipo é de 8 bits, limitando em 256 o número possível de atributos, sendo que a faixa de 192 a 255 já é reservada para fins experimentais ou para aplicações privadas. Esta característica acaba limitando o uso do *Radius*. Os atributos na faixa de 40 a 59 são utilizados especificamente para fins de contabilidade [70]. Na Tabela 4-4, são apresentados os atributos *radius* úteis na contabilização dos recursos utilizados em redes VOIP.

Tabela 4-4 – Atributos *Radius* importantes para contabilização (IETF, RFC 2866)

Tipo	Definição	Definição
1	User-Name	
4	NAS-IP-Address	Endereço IP do servidor NAS
30	Called-station-Id	Número do destino da chamada
31	Calling-station-Id	Número que originou a chamada
40	Acct-Status-Type	Define o tipo de mensagem. Os principais tipos para fins de contabilização são: *Start, stop e interim-update.*
41	Acct-Delay-Time	Indica quanto tempo o cliente está tentando enviar as informações. Normalmente 0 seg, variando somente nas retransmissões.
42	Acct-Input-Octets	
43	Acc-Output-Octets	
44	Acct-Session-Id	Valor que identifica uma sessão, permitindo associar os registros *start*, *interim-update* e *stop* da mesma sessão.
46	Acct-Session-Time	Indica o tempo da sessão, só é enviado em mensagens *stop*
47	Acct-Input-Packets	
48	Acct-Output-Packets	
49	Acct-Terminate-Cause	Apresenta a causa do término da sessão, só é enviado em mensagens *stop*
61	NAS-Port-Type	Indica a porta do dispositivo onde foi iniciada a sessão.

O atributo tipo 26 é reservado para uso específico dos fabricantes, permitindo que os mesmos criem atributos próprios sem requerer aprovação no IETF. Neste caso, o campo reservado ao valor do atributo 26 deve ser substituído pela tupla tipo/tamanho/valor do atributo definido pelo fabricante, o VSA (*Vendor Specific Attribute*), precedida de um campo identificando o fabricante. Uma única mensagem *Radius* pode conter vários atributos e VSAs encadeados. Dicionários de VSAs são definidos pelos fabricantes para que possam ser identificados no servidor *Radius*.

As RFCs definindo o uso do protocolo *Radius* não especificam atributos contendo informações mais detalhadas para a avaliação de chamadas VOIP. Com objetivo de manter um conjunto maior de informações sobre as chamadas realizadas, os fabricantes adotam VSAs específicos para o serviço VOIP, com destaque para os criados pelo fabricante Cisco, listadas no anexo 2.

4.4.3 Aplicação Radius em VOIP: Autenticação e Autorização

O uso mais comum do *Radius* integrado ao serviço VOIP, para fins de autenticação e autorização, é o de serviço de pré-pago, onde o usuário recebe uma identificação (*PIN Code*), uma senha e um crédito. Ao utilizar o serviço, uma aplicação (IVR - *Interactive Voice Response*) interage com o usuário solicitando o código de identificação do usuário e a senha. Um pedido de autenticação do usuário é enviado ao servidor *radius* que retorna o crédito do usuário. De posse dessa informação, o *gateway* ou o *gatekeeper* podem controlar o tempo da chamada, desconectando-a caso o crédito expire. Ao final da chamada, o crédito é atualizado na base de dados mantida no servidor *radius.*

Nos *gateways* utilizados nos experimentos (Cisco), os VSAs *h323-credit-amount* e *h323-credit-time* são utilizados para implementar a aplicação de pré-pago. A linguagem TCL (*Tool Command Language*) incorporada ao *gateway* permite a definição de roteiros responsáveis pela coleta de informações do usuário, geração de requisições *radius* e tratamento da resposta. Uma necessidade não prevista pelo fabricante é a classificação dos usuários, de forma a restringir o uso de serviços específicos a determinadas classes de usuários. No uso do serviço VOIP no projeto-

piloto, verificou-se ser útil esta classificação, definindo quem poderia realizar ligações para a telefonia pública, nacionais de longa distância e internacionais. Utilizando os recursos disponíveis, a solução indicada neste caso, é empregar o VSA Cisco *H323-ivr-in* para que o servidor radius informe em que categoria o usuário se encaixa. O servidor *Radius,* ao receber uma requisição de acesso, seleciona o usuário com base no código (Pin code) indicado no atributo IETF *User-name.* A categoria associada ao usuário (valores sugeridos: 0 – sem restrições, 1 - uso restrito a VOIP, 2 – uso restrito a VOIP e telefonia pública local e 3 – uso restrito a VOIP e telefonia pública nacional) é repassada na resposta, no formato *H323-ivr-in=categoria:3*. Caso a categoria seja diferente de zero, o VSA *H323-return_code* deve ser preenchido pelo servidor *Radius* com um valor que indique a necessidade do roteiro TCL verificar o número discado com a categoria associada, definindo se a chamada e permitida ou não (valor sugerido: *H323-return-code* = 60). Esta solução é viável também no *gatekeeper*, onde é utilizado o software de código aberto GNUGK. A versão 2.0 já incorpora funções que suportam VSAs Cisco, mas haveria necessidade de adaptá-las para o tratamento do atributo específico. A única diferença em relação à solução no *gateway* é a seleção do usuário, que neste caso seria feita com base no apelido H.323.

4.4.4 Aplicação Radius em VOIP: Contabilização de Recursos

O uso normal do servidor *Radius* é receber informações associadas à contabilidade de uma chamada VOIP proveniente de um *gatekeeper* H.323. A cada chamada pode ser gerado um CDR no início da chamada, opcional, e outro no final. O atributo IETF *Acct-Session-Id* é utilizado para associar os dois. Em chamadas envolvendo *gateways*, são criadas duas sessões para fins de contabilização dos recursos, uma para cada segmento da chamada, o *call leg.* Em cada chamada haverá um *call leg* do tipo telefonia, associado à ligação do *gateway* com o PBX, e uma VOIP, na sessão entre o *gateway* e o dispositivo VOIP remoto. Em chamadas envolvendo o *gateway* e um terminal H.323, por exemplo, são enviados 4 CDRs para o servidor Radius. Dois no início da chamada (*Acct-session-type = start*) e dois no final (*Acct-session-type=stop*), correspondentes a duas sessões distintas, uma de telefonia e outra VOIP, como apresentado na Figura 4-8.

No exemplo apresentado, podem ser notadas duas sessões distintas, cada uma associada a um *call leg* e identificada pelo atributo *Acct-Session-Id*. O VSA *h323-conf-id* permite associar todos registros relacionados à mesma chamada. O VSA *h323-call-type* identifica se a sessão está associada à telefonia ou a VOIP. Outro VSA importante é o *h323-call-origin*, onde pode ser deduzido se o *call leg* foi criado a partir do *gateway* (*origin = originate*), ou se foi criado por um dispositivo externo (*origin = answer*). No exemplo pode ser notado que a chamada foi iniciada a partir do PBX, a qual levou o *gateway* a estabelecer uma chamada com o terminal H.323.

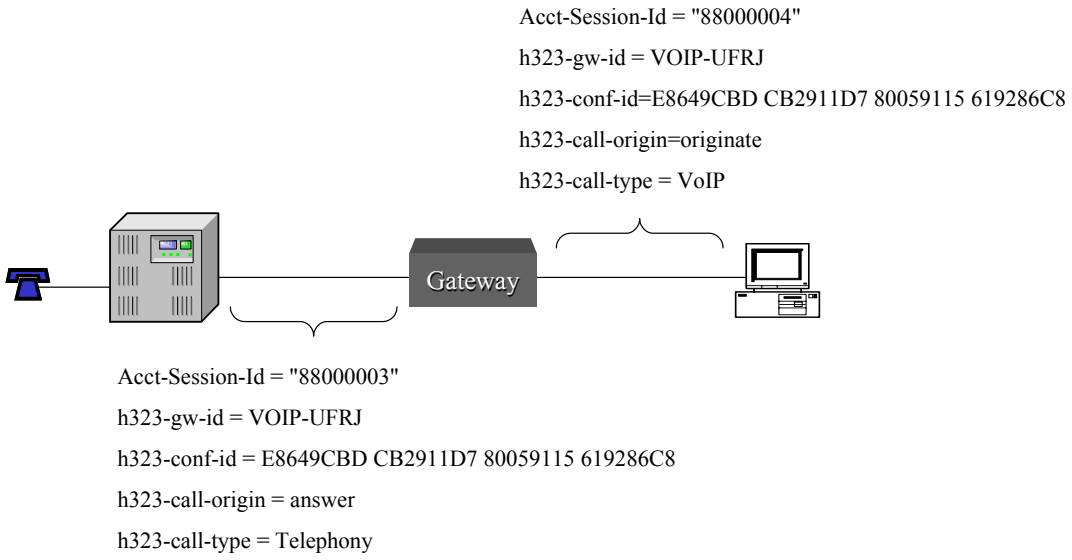


Figura 4-8 – Exemplos de CDR gerados em chamadas VOIP

Chamadas estabelecidas envolvendo mais de um *gateway* geram dois CDRs em cada *gateway,* como apresentado na Figura 4-9. No exemplo são gerados 4 CDRs do tipo *start* e 4 do tipo *stop*, todos apresentando o VSA *h323-conf-id* igual, o que permite correlacioná-los. Analisando o VSA *H323-Call-Origin* é possível identificar a ordem de criação de cada um dos segmentos.

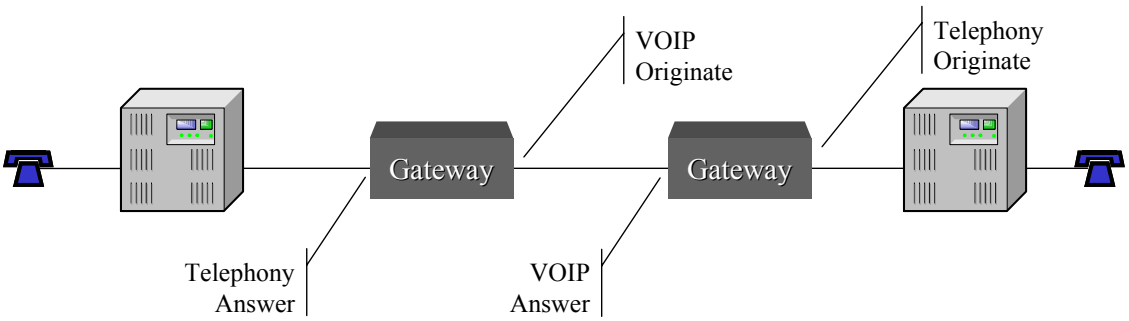


Figura 4-9 – Tipos de call leg associados a chamadas VOIP

Na mesma figura podem ser verificadas duas sessões associadas à rede VOIP, uma em cada *gateway*. Apesar de estarem contabilizando informações duplicadas sobre a mesma chamada, vários VSAs apresentam informações diferentes para cada sentido da comunicação. Atributos representando atrasos, pacotes perdidos, pacotes atrasados ou adiantados e a qualidade da chamada são associados a canais lógicos diferentes, um para cada sentido, e podem ser utilizados para identificar problemas que afetem a qualidade da chamada. Estes recursos foram utilizados no experimento realizado entre um *gateway* instalado na cidade Natal e outro no Rio de Janeiro, interligados através do *backbone* da Rede Nacional de Pesquisa (RNP), durante a realização do Simpósio Brasileiro de Redes de 2003 [51]. Em várias chamadas realizadas foram percebidos problemas na qualidade somente em um dos sentidos, tais como, voz picotada ou com falhas. Na análise dos CDRs foi possível identificar problemas associados a atrasos elevados e perdas de pacotes no sentido Natal-Rio de Janeiro, que correlacionadas à análise dos circuitos de comunicação pode associar os problemas à saturação destes canais, já que não havia uma configuração de QoS que garantisse um tratamento diferenciado ao tráfego de voz.

Em *call legs* tipo VOIP, os VSAs *early-packets, late-packets, lost-packets e receive-delay* são utilizados para avaliar parâmetros como *jitter*, atrasos e perda de pacotes RTP, que influenciam diretamente a qualidade da chamada. O VSA *h323-voice-quality* apresenta um valor já compilado de *impairment/calculated planning impairment factor* (ICPIF) para avaliação da qualidade da voz, de acordo com a recomendação ITU-T G.113 [72]. Fatores como perda de pacotes e atrasos influenciam este fator. Quanto maior, pior a qualidade da voz na chamada, como apresentado na Tabela 4-3. A avaliação destes VSAs pode auxiliar na identificação de problemas na rede afetando a qualidade das ligações VOIP realizadas.

Capítulo 5

Proposta de um Sistema Integrado de Gerência VOIP

Um sistema de gerenciamento VOIP deve exercer diversas atividades de forma integrada, envolvendo as cinco áreas funcionais de gerenciamento para prover: controle sobre a configuração dos equipamentos, monitorar a operação dos dispositivos envolvidos, tratar as notificações recebidas, manter a qualidade das chamadas e contabilizar os recursos consumidos por cada chamada.

Considerando a avaliação das MIBs disponíveis para o gerenciamento da estrutura VOIP e dos protocolos disponíveis (SNMP, ICMP, Syslog, *Radius* e Telnet/SSH) é proposta uma estrutura para o gerenciamento dos dispositivos a ser utilizada no projeto-piloto VOIP da RNP. Esta estrutura é composta de uma hierarquia em dois níveis. No primeiro nível são utilizadas estações para o gerenciamento do serviço em cada instalação, as quais ficam subordinadas a uma estação central que está localizada no centro de operações da RNP.

5.1 Estrutura Proposta de Gerenciamento

A proposição é que cada instituição possua a sua estação de gerenciamento, a partir da qual pode gerenciar a estrutura montada para atender o serviço VOIP, como apresentado na Figura 5-1. O objetivo é que uma estação servirá para efetuar todas as tarefas necessárias à gerência do serviço, incluindo a base do sistema de gerenciamento, o banco de dados e o serviço de contabilização de chamadas.

A base do sistema de gerenciamento inclui suporte necessário ao gerenciamento dos equipamentos utilizando os protocolos ICMP e SNMP. O requisito básico é que o usuário deve ter acesso ao sistema utilizando uma interface WEB para monitorar e controlar os recursos gerenciados. Desta forma, o acesso poderá ser feito a partir de outras máquinas na Internet. Restrições de acesso devem ser consideradas em função da importância das informações disponibilizadas, garantindo assim a sua privacidade.

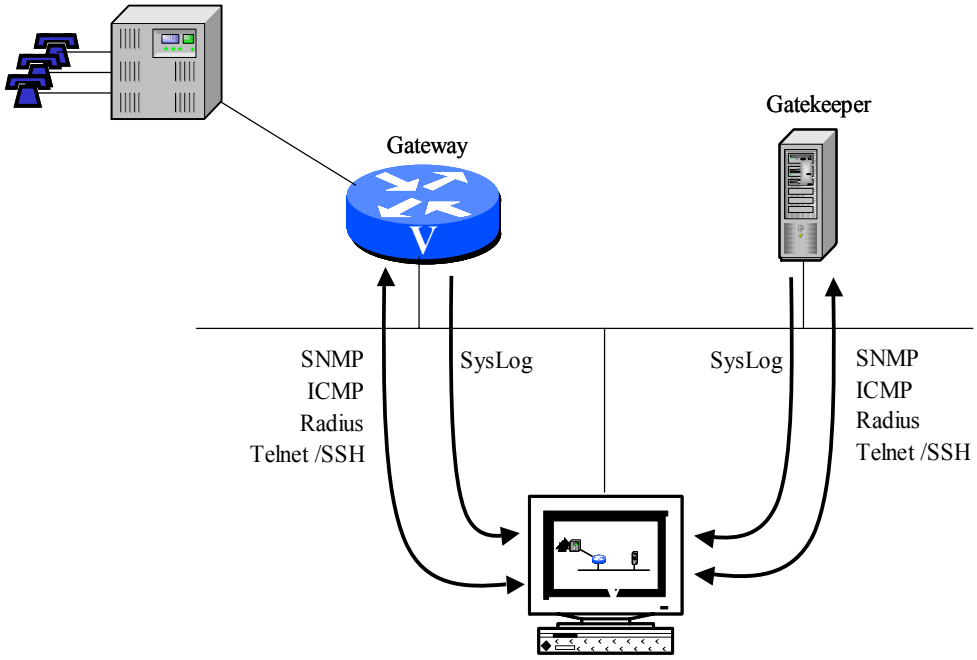


Figura 5-1 – Esquema de gerenciamento VOIP nas instituições

Informações relativas à configuração e operação dos equipamentos, de notificações recebidas e de arquivos de *log* devem ser filtradas e armazenadas em banco de dados.

Os CDRs recebidos através do protocolo *Radius* devem ser tratados e filtrados para evitar a duplicação de dados e então, as informações relativas a cada chamada devem ser armazenadas em banco de dados para a geração de estatísticas e para fins de tarifação.

As informações disponíveis são relativas somente à instituição. O sistema deve prever o uso do protocolo ICMP para que seja monitorada a alcançabilidade dos dispositivos de outras instituições.

Uma estação de gerenciamento centralizada na RNP é utilizada no gerenciamento dos *gateways* e *gatekeepers* de todas as instituições que participam do projeto-piloto, como apresentado na Figura 5-2. Esta estação deve estar habilitada ao uso dos protocolos SNMP, ICMP e Telnet/SSH para o controle e coleta das informações necessárias ao gerenciamento de toda a estrutura.

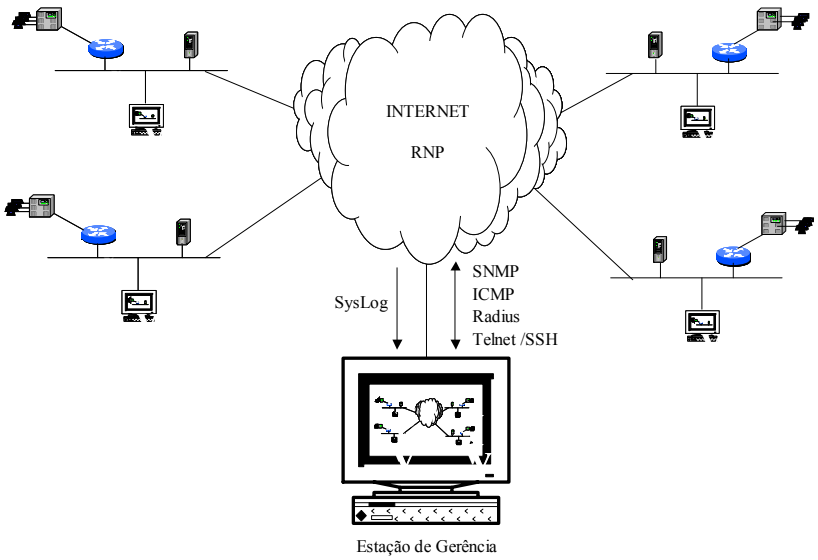


Figura 5-2 – Esquema de gerenciamento proposto para a RNP

A estação de gerenciamento central utilizará o SNMP para controlar e coletar as informações necessárias ao gerenciamento de toda a estrutura. Notificações SNMP (*informs e traps*) serão recebidas da gerência de cada instituição. Qualquer notificação deve ser filtrada inicialmente pela estação da instituição, evitando que a transmissão das mensagens SNMP possa gerar tráfego desnecessário no *backbone* da RNP.

Esta estação pode funcionar como um servidor reserva para os CDRs emitidos pelos dispositivos, caso o servidor principal da instituição apresente algum problema. Um esquema de replicação do banco deve ser utilizado para que estas informações possam ser gravadas posteriormente no servidor principal da instituição. O servidor de cada instituição deve ter acesso aos CDRs gerados por seus dispositivos armazenados no servidor da RNP para a consolidação das informações relativas às chamadas realizadas pela instituição. Neste sentido, é utilizado o mecanismo de servidores *master*/*slave* do MySQL para realizar a transferência dos CDRs gravados no servidor da RNP (*master*) para o das instituições (*slaves*), quando estes estiverem operacionais. Nas instituições onde o volume de chamadas for elevado é incentivado o uso de um servidor *Radius* secundário na própria instituição.

5.2 Gerenciamento de Configuração

O sistema deverá cadastrar as informações relativas a cada instituição em três níveis: instituição, equipamentos e componentes.

As instituições serão cadastradas manualmente utilizando opções do sistema. Inclui as informações: nome e endereço da instituição; dados do responsável pelo projeto, responsável técnico e equipe técnica (nome, telefone e email); prefixos dos telefones virtuais; e descrição dos *PBXs* utilizados (fabricante, modelo, números de ramais atendidos, plano de numeração e tipo de interfaces disponíveis para conexão aos *gateways*). As informações sobre a instituição, prefixos, responsáveis e equipe técnica devem estar disponíveis a todas instituições.

Relacionada a cada instituição serão cadastradas as informações relativas aos dispositivos (*gateway e gatekeeper)* que implementam o serviço VOIP nas instituições: endereçamento IP, prefixos atendidos, identificadores H.323 e informações de segurança de acesso (*communities*, usuários e senhas). Estas informações são configuradas manualmente no sistema.

Utilizando os dados configurados, deve ser utilizado o protocolo SNMP para obter as informações relativas à configuração dos equipamentos: fabricante, modelo, sistema operacional, portas de voz e *dial-peers*.

A Tabela 5-1 apresenta a lista de objetos que devem ser coletados da MIB para descrever os *gateways.*

O *gatekeeper* GNUGK não tem suporte a SNMP, a fim de gerenciar sua operação deve ser implementado um agente SNMP neste dispositivo.

Tabela 5-1 – Lista de objetos MIB com informações sobre o *gateway H.323*

Objetivo	MIB	Objeto
Fabricante/Modelo	MIB-II	*system.sysObjectID*
Sistema Operacional	MIB-II	*system.sysDescr*
Hostname	MIB-II	*system.sysName*
Fabricante/Hardware /Software	ITU H.341 *Gateway* H.323	Grupos *h323GwSystem* e *h323GwCapabilities*
	ITU H.341 *Gatekeeper* H.323	Grupos *h323GatekeeperSystem* e *h323GatekeeperConfiguration*
Descrição dos *dial-peers*	*cisco-voice-Dial-control-MIB*	Coletar informações do grupo *cvPeer*

Informações relativas às portas de voz que são utilizadas na conexão com o PBX podem ser obtidas da MIB utilizando os objetos descritos na Tabela 5-2. O fabricante Cisco desenvolveu uma série de MIBs privadas que permitem um maior controle sobre a configuração das portas. A MIB definida pelo ITU-T para a gerência do *gateway* foi indicada na tabela, apesar dos equipamentos analisados não suportarem tal MIB.

Tabela 5-2 – Lista de objetos MIB que descrevem características das portas de voz

Objetivo	MIB	Objeto
Portas de Voz		Selecionar informações de interfaces com *ifType* = 18, 81, 100, 101 e 102
Índice (será utilizado como referência no acesso a outras tabelas)	MIB-II	*interfaces.ifTable.ifTableEntry.ifIndex*
Tipo	MIB-II	*interfaces.ifTable.ifTableEntry.ifType*
Descrição	MIB-II	*interfaces.ifTable.ifTableEntry.ifDescr*
Características de portas de voz (*ifType*=100, 101 ou 102)	*Cisco-Voice-If-MIB*	Coletar informações da tabela *cvIfCfgObjects*
Características de portas de voz E&M (*ifType*=100)	*Cisco-Voice-Analog-If-MIB*	Coletar informações da tabela *cvaIfEMObjects*
Características de portas de voz FXO (*ifType*=101)	*Cisco-Voice-Analog-If-MIB*	Coletar informações da tabela *cvaIfFXOObjects*
Características de portas de voz FXS (*ifType*=102)	*Cisco-Voice-Analog-If-MIB*	Coletar informações da tabela *cvaIfFXSObjects*
Características de interfaces E1 (ifType=18)	RFC1406	Coletar objetos da tabela *dsx1Configtable*.
Características de interfaces virtuais associadas a grupos de canais DS0 (*ifType*=81)	*Cisco-CAS-IF-MIB*	Coletar objetos do grupo *ccasGrpObjects*
Características de canais DS0 em troncos E1 com sinalização CAS	*Cisco-CAS-IF-MIB*	Coletar objetos dos grupos *ccasChannelObjects* e *ccasVoiceCfgObjects*

Os *dial-peers* descrevem interfaces virtuais que são utilizadas para iniciar chamadas e recebê-las quando direcionadas ao *gateway*. Os *call legs* definem o plano de numeração do *gateway*, indicando para onde devem ser estabelecidas todas as chamadas realizadas a partir do *gateway*. A Tabela 5-3 descreve os vários objetos definidos em MIBs que permitem controlar e monitorar a configuração de *call legs* em *gateways* H.323. Os *Codecs* utilizados nas chamadas H.323 são associados ao *call leg*.

Tabela 5-3 – Objetos que descrevem *call legs* em gateways de voz

Objetivo	MIB	Objeto
Dial-peers		Na tabela interfaces será criada uma interface virtual para cada *dial-peer* configurado no *gateway* (*ifType*=103 e 104)
Descrição de prefixos associados às portas de voz	ITU H.341 *Gateway H.323*	Grupo *H323GwConfiguration*
Codecs associados às interfaces de rede	ITU H.341 *Gateway H.323*	*H323GwCapabilities*
Índice (será utilizado como referência no acesso a outras tabelas)	MIB-II	*interfaces.ifTable.ifTableEntry.ifIndex*
Tipo (103=POTS, 104=VOIP)	MIB-II	*interfaces.ifTable.ifTableEntry.ifType*
Descrição	MIB-II	*interfaces.ifTable.ifTableEntry.ifDescr*
Descrição dos *dial-peers* e interfaces associadas	RFC2128	Coletar informações dos grupos *dialCtlConfiguration* e *dialCTLPeer*
Descrição dos *dial-peers*	Cisco-voice-Dial-control-MIB	Coletar informações do grupo *cvPeer*

Redes H.323 são organizadas em "zonas", cada uma controlada por um *gatekeeper* onde terminais e *gateways* H.323 ficam registrados. A informação sobre os equipamentos registrados no *gatekeeper* é importante para fins de gerenciamento. O *gatekeeper* utilizado não tem suporte a SNMP. Entretanto, as informações podem ser obtidas através da console do *gatekeeper* conectando à porta TCP/7000 do servidor onde o mesmo está operando. O uso do comando "rv" permite obter as informações relativas a todos os registros. Na Figura 5-3 pode ser vista a saída do comando, onde podem ser vistos dois dispositivos registrados, um *gateway* e um terminal. Em cada linha associada ao registro podem ser vistas várias informações sobre os dispositivos: endereço IP, porta TCP associada à sinalização de chamadas, os vários apelidos associados (*dialedDigits* no caso de endereços E.164 e h323_ID, no caso de identificadores H.323) e o tipo de dispositivo. No caso dos *gateways*, são indicados ainda os prefixos associados à rede de telefonia a que o mesmo está conectado, indicando que todas as chamadas destinadas a telefones com este prefixo devem ser direcionadas ao *gateway* indicado. Estas informações devem ser tratadas com roteiros *Perl* para serem apresentados na console de gerenciamento. Se o *gatekeeper* estiver implementado em equipamentos Cisco, pode ser utilizada a MIB *Cisco-gatekeeper-MIB* (grupo *cgkZone*) para coletar informações sobre a "zona" local e às remotas. O grupo *h323GatekeeperZone* da MIB ITU-T *gatekeeper* também permite obter informações sobre os dispositivos registrados no *gatekeeer.*

```
rv
AllRegistrations
RCF|146.164.247.202:1720|03001:dialedDigits=3001:dialedDigits=02125983001:di
aledDigits=2125983001:dialedDigits=025983001:dialedDigits=UFRJ-
VOIP:h323_ID|gateway|8038_endp
Mon, 25 Aug 2003 02:09:34 -0300 C(0/15/21)  <2>
Prefixes: 213873,212598,212562

RCF|200.141.82.206:1720|peixoto:h323_ID=025983399:dialedDigits=03399:dialed
Digits|terminal|8062_endp
Mon, 25 Aug 2003 02:09:44 -0300 C(0/1/1)  <2>
Number of Endpoints: 2
```

Figura 5-3 – Obtendo informações sobre dispositivos registrados

O gerenciamento de configuração também envolve o controle dos equipamentos, permitindo que remotamente sejam ativadas ou desativadas portas de voz, ou que se reinicialize o equipamento. A fim de realizar este controle é necessário ter acesso de escrita à MIB do equipamento. A Tabela 5-4 descreve os objetos que permitem este controle.

Tabela 5-4 – Objetos que permitem o controle remoto de dispositivos H.323

Objetivo	MIB	Objeto
Restart / Shutdown / Reset Statistics	ITU H.341 *Gateway H.323*	Grupo *H323GwControls*
	ITU H.341 Terminal *H.323*	Grupo *H323TermControl*
	ITU H.341 *Gatekeeper H.323*	Grupo *H323GateKeeperControls*
Ativar/Desativar portas de voz e *dial-peers*	MIB-II	Objeto *interfaces.iftable.ifEntry.ifAdminStatus*
Reload	OLD-CISCO-TS-MIB	TsMsgSend (1.3.6.1.4.1.9.2.9.9.0 = 2)

Outro ponto importante no gerenciamento de configuração é manter uma cópia da configuração dos equipamentos utilizados. Em equipamentos Cisco, a cópia da configuração para um servidor TFTP pode ser realizada utilizando a MIB *Cisco-Config-Copy-MIB*, como apresentado na Figura 5-4.

```
# Deve ser criada uma entrada na MIB Cisco-Config-Copy-MIB
# relativa à copia que será realizada. Todas as entradas relativas à
# mesma operação são associadas através de um número escolhido
# aleatoriamente. As variáveis abaixo devem ser atribuídas utilizando
# o comando setrequest do SNMP
# Prefixo:
cisco.ciscoMgmt.ciscoConfigCopyMIB.ciscoConfigCopyMIBObjects.
ccCopy.ccCopyTable.ccCopyEntry

# Definir o protocolo utilizado para efetuar a cópia (TFTP=1)
ccCopyProtocol.<random number> integer 1

# Definir os arquivos de origem e destino (arquivo de rede = 1, startup-config=3,
# running-config=4)
ccCopySourceFileType.<Random number> integer 3
ccCopyDestFileType.<Random number> integer 1

# Definir o endereço IP e o nome do arquivo a ser utilizado
# quando for utilizado um arquivo na rede (TFTP)
ccCopyServerAddress.<Random number> ipaddress "<server ip address>"
ccCopyFileName. <Random number> octetstring "<file name>"
# Criando e ativando a ação definida (createandgo=4)
ccCopyEntryRowStatus.<Random number> integer 4

#  O acompanhamento da operação de cópia pode ser realizado através da variável
#  ccCopyState.<random number>
#  Os valores possíveis são waiting(1), running(2), # successful(3)  e failed(4)

# Ao terminar a cópia, a linha da tabela que foi criada deve
# ser removida. A variável que indica o estado da linha deve
# ser configurada com o valor destroy(6).
ccCopyEntryRowStatus.<Random Number> integer 6
```

Figura 5-4 – Cópia de arquivos de configuração utilizando SNMP

No anexo 3 podem ser visualizadas algumas telas que são utilizadas pelo sistema de gerenciamento para fins de gerenciamento de configuração.

5.3 Gerenciamento de Contabilidade

Em redes VOIP utilizando a arquitetura H.323, a principal forma de contabilizar as chamadas é através dos CDRs recebidos através do protocolo *Radius* provenientes de *gatekeepers* e de *gateways*. As informações sobre as chamadas já realizadas também podem ser obtidas de MIBs específicas SNMP ou através da console do *gatekeeper* (porta TCP/7000), como apresentado na Figura 5-5.

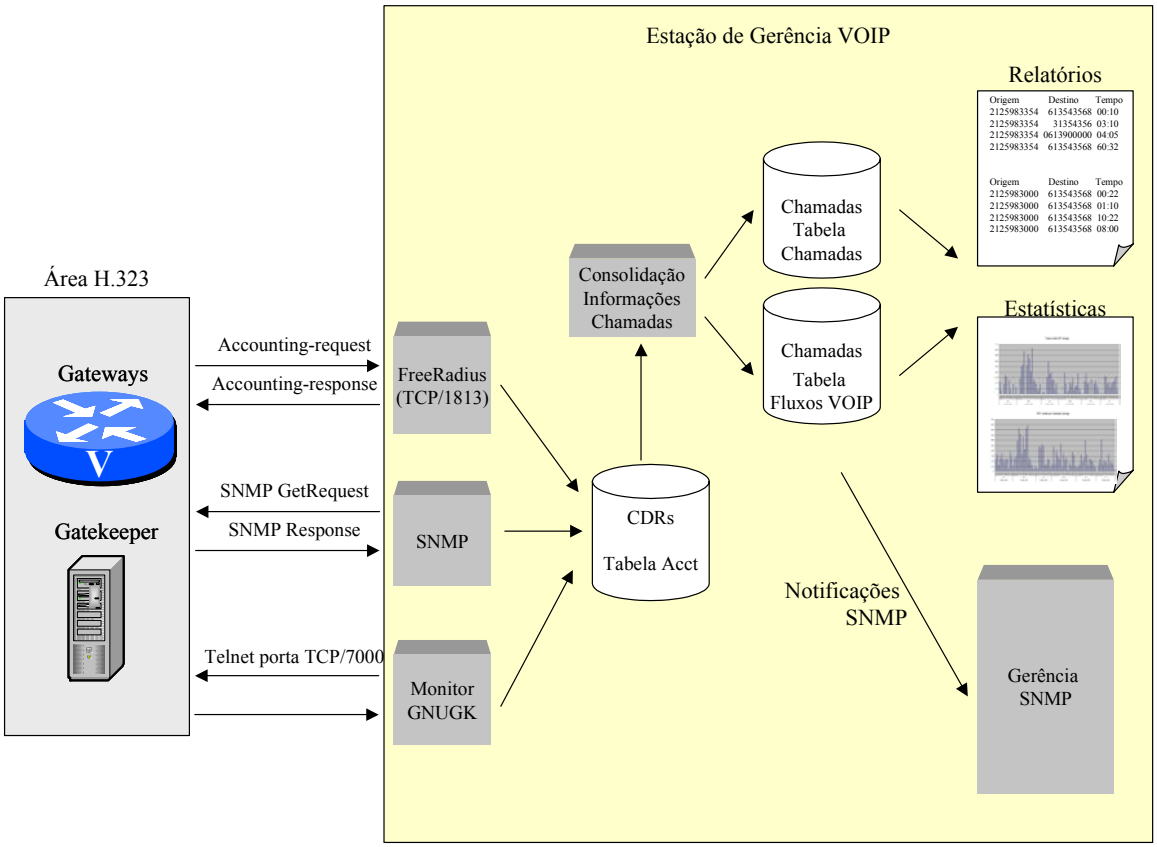


Figura 5-5 – Esquema do gerenciamento de contabilidade

Uma preocupação em relação ao tratamento das informações relativas à contabilidade de recursos com origens diferentes, deve ser a de manter os horários sincronizados em todos os dispositivos envolvidos. Com este objetivo, os *gateways, gatekeepers* e servidores *Radius* devem utilizar o protocolo *Network Time Protocol* (NTP) para sincronizar seus relógios, preferencialmente utilizando o mesmo servidor NTP.

Os CDRs podem ser recebidos do *gatekeeper* e do *gateway*, a seguir é detalhado o procedimento para o tratamento das informações provenientes de cada dispositivo.

Nas ligações entre dois terminais H.323 dentro da mesma "zona" é gerado pelo *gatekeeper* um CDR no início da chamada e outro ao final. Na Figura 5-6 são apresentados dois CDRs associados à mesma chamada, gerados pelo *gatekeeper* utilizado no projeto-piloto. Na configuração do *gatekeeper* foi definido que seriam utilizados no CDR, VSAs com o mesmo formato que os definidos pelo fabricante Cisco (opção do GnuGK).

```
Tue Aug 12 17:32:35 2003
    Acct-Status-Type = Start
    NAS-IP-Address = 146.164.247.196
    NAS-Identifier = "UFRJGK"
    NAS-Port-Type = Virtual
    Service-Type = Login-User
    Acct-Session-Id = "acb50002"
    User-Name = "peixoto"
    Calling-Station-Id = "025983399"
    Called-Station-Id = "025983300"
    h323-gw-id = "h323-gw-id=UFRJGK"
    h323-conf-id = "h323-conf-id=3FBD83C3 E8ED1810 87AC0053 45000000"
    h323-call-origin = "h323-call-origin=proxy"
    h323-call-type = "h323-call-type=VoIP"
    h323-remote-address = "h323-remote-address=146.164.247.207"
    Acct-Delay-Time = 0
    Client-IP-Address = 127.0.0.1
    Acct-Unique-Session-Id = "df37cafae85365a8"
    Timestamp = 1060720355
Tue Aug 12 17:51:59 2003
    Acct-Status-Type = Stop
    NAS-IP-Address = 146.164.247.196
    NAS-Identifier = "UFRJGK"
    NAS-Port-Type = Virtual
    Service-Type = Login-User
    Acct-Session-Id = "acb50002"
    User-Name = "peixoto"
    Acct-Session-Time = 1159
    Calling-Station-Id = "025983399"
    Called-Station-Id = "025983300"
    h323-gw-id = "h323-gw-id=UFRJGK"
    h323-conf-id = "h323-conf-id=3FBD83C3 E8ED1810 87AC0053 45000000"
    h323-call-origin = "h323-call-origin=proxy"
    h323-call-type = "h323-call-type=VoIP"
    h323-setup-time = "h323-setup-time=17:32:35.169 BRT Tue Aug 12 2003"
    h323-connect-time = "h323-connect-time=17:32:39.863 BRT Tue Aug 12 2003"
    h323-disconnect-time = "h323-disconnect-time=17:51:59.380 BRT Tue Aug 12
2003"
    h323-disconnect-cause = "h323-disconnect-cause=10"
    h323-remote-address = "h323-remote-address=146.164.247.207"
    Acct-Delay-Time = 0
    Client-IP-Address = 127.0.0.1
    Acct-Unique-Session-Id = "df37cafae85365a8"
    Timestamp = 1060721519
```

Figura 5-6 – CDRs emitidos em chamadas realizadas entre terminais H.323

Os vários CDRs gerados associados à mesma chamada podem ser identificados pelo atributo *Acct-Session-Id* ou pelo VSA *h323-conf-Id.* No exemplo apresentado, foram identificados dois CDRs, um indicando o início da chamada (*Acct-Status-Type = "Start"*), e o segundo o término (*Acct-Status-Type = "Stop"*). Vários motivos podem impedir a emissão do CDR no término da chamada, tendo como conseqüência a perda das informações corretas sobre a chamada. Um mecanismo previsto no *Radius* para manter uma monitoração constante das chamadas ativas, minimizando o efeito da perda de informações, é o uso de CDRs intermediários, mas não é implementado na versão atual do *GnuGK*. Um mecanismo para evitar a perda de informações neste caso é gerar uma cópia dos CDRs no arquivo de *log* gerado pelo aplicativo. Análises periódicas nestes arquivos podem ser empregadas para localizar as informações perdidas. No GnuGK, os CDRs também são apresentados na console do aplicativo (porta TCP/7000). Com este propósito, pode ser utilizado um roteiro *Perl* fornecido no pacote do GnuGK para capturar estas informações, apresentado no anexo 4. Registros duplicados devem ser descartados, o uso do atributo *Acct-Session-Id* ou do *h323-conf-id* associados ao atributo *Acct-Status-Type* pode ser utilizado como chave única para evitar a duplicidade.

Ao receber os CDRs, o servidor *Radius* deve armazená-los no banco de dados SQL. O esquema da tabela criada no banco de dados MySQL para fins de contabilização é apresentado no anexo 5. Uma tabela específica deve ser criada para armazenar o resumo das informações das chamadas realizadas, que é utilizada para fins de tarifação e estatística. Nessa tabela devem ser criados campos para armazenamento dos atributos *User-Name, h323-remote-address, Called-Station-Id, Calling-Station-Id* e *Acct-Session-Time,* que identificam o usuário local, o endereço IP e identificador do terminal chamado, o identificador do terminal chamador e o tempo da chamada em segundos, respectivamente. Um campo deve ser criado para identificar se a ligação é local, nacional de longa distância ou internacional, o qual deve ser definido a partir dos identificadores dos terminais origem e destino da chamada.

O motivo da desconexão (*h323-disconnect-cause)* também deve ser mantido para fins estatísticos e para a identificação de possíveis problemas na rede. As causas de desconexão de chamadas H.323 derivam da recomendação ITU-T Q.931, conforme apresentado na Tabela 5-5.

Apesar de configurado para gerar VSAs Cisco, o GnuGK não gera informações sobre tráfego, nem sobre a qualidade da voz associada à chamada.

Tabela 5-5 – Causas de desconexão Q.931 associadas a chamadas H.323

Disconnect Cause (decimal / hex)	Disconnect Text
3 (0x3)	No route to destination
16 (0x10)	Normal call clearing
17 (0x11)	User busy
18 (0x12)	No user response
20 (0x14)	Subscriber absent
21 (0x15)	Call rejected
27 (0x1B)	Destination out of order (Mensagem de sinalização não pode ser enviada para o dispositivo remoto)
28 (0x1C)	Invalid number
31 (0x1F)	Normal, unspecified
34 (0x22)	No circuit
47 (0x2F)	No resource (Erro na alocação de recursos internos – sem memória para alocar no *gateway*, por exemplo)
49 (0x31)	QoS unavailable (QoS requisitada não está disponível)
63 (0x3F)	Service or option not available, or unspecified
102 (0x66)	Recovery on timer expiry (Mensagens H.323 *alerting* ou *connect* não foram recebidas no tempo máximo definido)

Ligações envolvendo um ou mais *gateways* geram uma quantidade maior de CDRs, dois para cada *call leg.* Os *gateways* devem ser configurados para o envio de VSAs que forneçam um maior número de informações sobre cada chamada. Nos equipamentos do projeto-piloto, *gateways Cisco,* foi adotada a configuração apresentada na Figura 5-7.

O procedimento inicial para a análise é a seleção de todos os CDRS relativos a uma única chamada, reunindo todos os que apresentam o mesmo *h323-conf-id.* CDRs repetidos devem ser descartados, a chave *h323-conf-id + Acct-Session-ID + Acct-Status-Type* pode ser utilizada para identificar CDRs duplicados. Um número muito elevado de CDRs repetidos denota um problema no servidor *Radius* ou na transmissão da mensagem *accounting-response* para o *gateway*. As informações obtidas dos CDRs devem ser utilizadas para gerar um registro na tabela de chamadas realizadas, onde são resumidas as informações dos *call legs* recebidos de cada chamada.

```
! Cria o grupo de servidores Radius que irão receber os CDRs
aaa group server radius RNP-ACCOUNTING
server 146.164.247.196 auth-port=1812 acct-port=1813
server 146.164.247.209 auth-port=1812 acct-port=1813
! Define envio de CDRs de “start” e “stop” para servidores do grupo
! Ativa o processo de autenticação, autorização e contabilidade (AAA)
aaa new-model
aaa accounting connection h323 start-stop group RNP-ACCOUNTING
! Ativa contabilidade VOIP
gw-accounting aaa
! Habilita o envio de todos os VSAs VOIP
acct-template callhistory-detail
! Configura chave secreta que será utilizada na troca de mensagens
! com os servidores radius (key=”RNP”)
radius-server 146.164.247.196 auth-port=1812 acct-port=1813 key RNP
radius-server 146.164.247.209 auth-port=1812 acct-port=1813 key RNP
```

Figura 5-7 – Configuração de contabilidade Radius em gateways Cisco

Nos CDRs recebidos no início da chamada (*Acct-Status-Type = ”Start”*) deve ser identificada a origem (*User-name e Calling-Station-Id*) e o destino da chamada (*Called-Station-Id*).

Em chamadas realizadas de um terminal H.323 para um telefone convencional, o atributo *User-name* contém o número de telefone que iniciou a chamada. Nestes casos, o nome do usuário deve ser obtido do CDR recebido do gatekeeper. Nas chamadas provenientes da rede de telefonia através de portas FXO, o número do telefone que

origina a chamada, o nome do usuário e o número do telefone chamado não são indicados no CDR. Neste caso, deve ser associado um identificador à porta de voz do *gateway*17, o qual é informado nos atributos *Calling-Station-Id* e *User-Name* do CDR. O número do telefone chamado deve ser obtido do *call leg* VOIP. Quando a rede de telefonia estiver conectada através de troncos E1, as portas do gateway devem ser configuradas para que sejam coletados os identificadores *Automatic Number Identification (ANI)* e *Dialed Number Identification Service* (DNIS) na sinalização com a rede de telefonia, os quais correspondem ao número do telefone que originou a chamada e ao do número chamado, respectivamente. Utilizando os dois números deve ser identificado se a chamada é local, nacional de longa distância ou internacional.

O endereço IP (*NAS-IP-Address*) e a identificação da porta de voz utilizada no gateway (*Cisco-NAS-Port*) devem ser armazenados também no registro da chamada.

Um campo deve ser criado na tabela para identificar se a chamada foi iniciada através da rede de telefonia ou da rede VOIP. Para isto, deve ser selecionado o CDR com o VSA *h323-call-origin = "answer"*, onde o VSA *h323-call-type* é utilizado para identificar o tipo. Havendo CDRs relativos à mesma chamada no servidor *Radius*, provenientes dos dois gateways diferentes, o parâmetro *h323-setup-time* deve ser utilizado para identificar o gateway em que foi originada a chamada. Este procedimento só funciona adequadamente se os relógios dos equipamentos envolvidos estão sincronizados.

Ao término da chamada são recebidos os CDRs (*Acct-Status-Type = "Stop"*), dos quais devem ser descartados os repetidos. Informações sobre tráfego gerado na rede IP devem ser armazenados numa tabela específica do banco de dados, onde são armazenados os parâmetros (*Acct-Input-Octets*, *Acct-Output-Octets*, *Acct-Input-Packets*, *Acct-Output-Packets*), obtidos do *call leg* VOIP. Como o servidor *Radius* pode estar recebendo informações provenientes de vários gateways é importante manter registros distintos, cada um associado a um *gateway.* A comparação dos pacotes enviados em um sentido com os recebidos no sentido oposto, serve para identificar os pacotes perdidos

[17] Comando de configuração de porta de voz : station id E.164

em um dos canais lógicos, o que pode sinalizar problemas associados a congestionamento ou a falhas.

O tempo de duração da chamada (*Acct-session-time*) deve ser armazenado para fins de tarifação e estatísticas. Deve ser considerado o valor associado ao último *call leg* estabelecido para a chamada (*h323-call-origin= "originate"*). Chamadas não atendidas pelo usuário apresentam este tempo com o valor zero. Em chamadas destinadas à telefonia tradicional deve haver o cuidado de configurar as portas de voz com suporte à sinalização de linha que identifica o atendimento pelo usuário chamado (*answer supervision*), caso contrário o tempo associado à sinalização da chamada (*ring*) é considerado como tempo de sessão.

Tabela 5-6 – Origem da desconexão de chamadas

Release source	Origem da desconexão
1	Telefone que originou a chamada
2	Dispositivo VOIP que originou a chamada
3	Telefone que recebeu a chamada
4	Dispositivo VOIP que recebeu a chamada
5	*Gateway* (interno) – *Call leg Telephony*
6	*Gateway* (interno) – *Call leg VOIP* (Exemplo: Canal lógico liberado por troca do *CODEC*)
7	Aplicação interna do *gateway* (Exemplo: Roteiro TCL – IVR)
8	Liberação interna
9	Comando de console
10	Servidor *Radius* Externo
11	SNMP
12	Agente de controle externo

O motivo da desconexão (*release-source, h323-disconnect-cause* e *h323-disconnect-text)* também deve ser mantido para fins estatísticos e para a identificação de possíveis problemas na rede. As causas de desconexão de chamadas H.323 derivam da recomendação ITU-T Q.931, conforme apresentado na Tabela 5-5. As informações de desconexão devem ser obtidas do *call leg* onde foi iniciada a desconexão. A Tabela 5-6

deve ser utilizada na identificação da origem da desconexão com base no VSA *release-source.*

Quando as portas de voz FXO estão configuradas para realizar a desconexão baseada em tons, as chamadas terminadas na telefonia são finalizadas após o recebimento do tom específico, normalmente o tom de ocupado (*busy tone*). Nestes casos, o motivo de desconexão indicado é o código 0x11 "*User busy*". Esta situação é diferenciada das chamadas não completadas porque o destino estava ocupado, analisando o tempo da chamada. Chamadas não completadas têm uma duração de zero segundos.

A avaliação do motivo de desconexão pode auxiliar na verificação de problemas associados a equipamentos (*gateways* e *gatekeepers*), componentes (portas de voz, troncos E1, canais DS0 e ramais de PBX), configuração ou à própria rede (configuração de QoS, canais saturados, e falhas nos equipamentos ou circuitos de comunicação).

Informações sobre a qualidade das chamadas (*h323-voice-quality*, *round-trip-delay, early-packets, late-packets e lost-packets*) devem ser armazenadas em tabela especifica do banco de dados. Estes atributos são associados ao fluxo RTP que chega ao *gateway*. Na análise destes parâmetros podem ser identificadas chamadas que apresentaram algum problema que afetou a qualidade. O VSA *h323-voice-quality* varia de 0 a 55 (ver Tabela 4-3), quanto maior o valor deste parâmetro, pior a qualidade da chamada. O *gateway* pode ser configurado para a emissão de notificações *(traps)* quando uma chamada termina com este parâmetro com valores superiores a 20, valor que pode ser alterado. A avaliação dos vários indicativos é útil para identificar possíveis problemas de conexão entre dispositivos específicos, advindos de defeitos ou de não estar sendo utilizado um mecanismo que garanta a QoS necessária ao serviço VOIP.

Informações sobre as ligações em curso e as já realizadas também podem ser obtidas através do protocolo SNMP. Nas MIBs ITU-T, os grupos *connectionEntry* da MIB *H225CallSignalling, rasAdmission* da MIB *RAS e h323calls* da MIB *Gateway H.323* listam informações importantes sobre as chamadas ativas. Entretanto, nenhuma destas MIBs está implementada nos *gateway* e *gatekeepers.*

A MIB *Dial Control MIB* descrita na RFC 2128 apresenta os grupos *callActive* e *callHistory* que permitem obter informações sobre as chamadas ativas e um histórico das que já foram realizadas. Entretanto, apresenta alguns problemas que dificultam a avaliação de uma chamada. Nas duas tabelas, as informações são específicas para cada *call leg*, não existem variáveis que relacionem os dois *call legs* associados a cada chamada realizada através do *gateway*. As tabelas também não têm variáveis que permitam uma associação com os fluxos de sinalização H.323. A cada chamada realizada através do *gateway* são criadas duas entradas na tabela, uma para cada *call leg.* Um deles estará associado ao dispositivo que iniciou a chamada (*callOrigin="Answer")*, onde pode ser coletado o H323-ID *(callActivePeerAddress)*, o *dial-peer (callPeerIfIndex* → indice para a tabela *interfaces)*, a hora da conexão *(callActiveConnectTime)* e o tráfego (*callActiveTransmitPackets, callActiveTransmitBytes, callActiveReceivePackets e callActiveReceiveBytes*) associados à conexão mantida com o dispositivo que originou a chamada. O segundo *call leg* apresenta as mesmas informações associadas à conexão estabelecida com o destinatário da chamada. A tabela *callHistory* apresenta os mesmos objetos acrescidos da hora da desconexão e do motivo para o término da chamada.

Nos *gateways* Cisco, a MIB privada *Cisco-Voice-Dial-Control-MIB* apresenta informações complementares à *Dial-Control-MIB* para cada chamada ativa. A tabela *callHistory* da *Dial-Control-MIB* não é implementada em função de problemas associados aos índices utilizados. O histórico das chamadas é mantido nas MIBS *Cisco-Dial-Control-MIB* e *Cisco-Voice-Dial-Control-MIB*. Nas tabelas Cisco são apresentados objetos que permitem um melhor controle sobre a qualidade das chamadas.

As variáveis *ciscoCallHistoryTableMaxLength* e *ciscoCallHistoryRetainTimer* da MIB *Cisco-Call-History-MIB* permitem definir o número máximo de entradas e o tempo mínimo que cada entrada será mantida no histórico, respectivamente. Estes valores devem ser selecionados de forma a facilitar a coleta de informações das tabelas, já que um grande número de entradas pode gerar um tráfego excessivo na rede. Entretanto, um número pequeno de entradas mantidas por pouco tempo pode ter como conseqüência a perda de dados associados às tabelas. Como o SNMP é utilizado como uma reserva às informações providas pelo *Radius*, é sugerido um tempo mínimo de 24

horas, durante o qual poderá ser utilizado na consolidação das informações dos *Radius.* Desta forma, as informações que não forem obtidas via *Radius*, podem ser obtidas através do SNMP.

Exemplos das informações disponíveis em uma chamada ativa e no histórico da chamada após o seu término são apresentados nos anexos 6 e 7, respectivamente.

A consolidação das informações que serão recebidas através do protocolo Radius é realizada por um roteiro *Perl*, ativado a cada 30 minutos nas estações de gerência de cada instituição. Este roteiro deve reunir todos os CDRs associados a uma chamada, dos quais são eliminados os duplicados. A partir das informações recebidas, é gerado um registro para cada chamada terminada no período posterior ao último acionamento do roteiro. As chamadas em que foi recebida a indicação do início, mas que ainda não tenha sido recebido o CDR de término, devem ser verificadas. Inicialmente deve ser consultado o dispositivo que gerou o CDR de "start", verificando se a chamada ainda continua ativa. Como o protocolo Radius não permite fazer este tipo de consulta, a verificação pode ser realizada através de SNMP ou, no caso do GnuGK, através do console. Caso seja verificado que a chamada já foi finalizada, o servidor secundário, localizado na RNP, deve ser consultado para a existência de algum CDR relativo à chamada. O banco SQL da RNP deve permitir o acesso a partir dos servidores Radius para que estas consultas possam ser realizadas. Existindo, as informações são consolidadas. Caso não as tenha, deve ser utilizado o protocolo SNMP para consulta às MIBs já descritas para obter as informações necessárias. Os dispositivos devem ser configurados para manter estas informações por um período mínimo de 24 horas, para que não sejam perdidas informações que prejudiquem a estatística e a tarifação. De qualquer forma, se o equipamento for desligado, as informações são perdidas. No caso do GnuGK, as informações devem ser obtidas do arquivo de log. Na possibilidade de não haver o fechamento da chamada, um campo no registro deve indicar que a chamada terminou mas não foram obtidas informações do término da chamada. O uso de CDRs intermediários pode ser interessante para manter informações mais constantes das chamadas, mas pode haver um tráfego grande na rede em função desta opção.

Nas informações consolidadas, deve ser feita uma análise da qualidade de voz nas chamadas realizadas, a qual só será possível quando o CDR recebido apresentar os

VSAs necessários. Deverá ser preparada uma matriz apresentando a qualidade de voz nas chamadas realizadas com as outras instituições nas últimas 24 horas. Caso o percentual de chamadas realizadas com qualidade baixa (ICPIF > 20) seja superior a 10% do total de chamadas realizadas com uma determinada instituição, deve ser enviado um alarme para a estação de gerência da instituição e outro para a estação central da RNP para que seja verificada a rota entre as duas instituições. Este percentual e o valor do ICPIF podem ser ajustados para condições mais ou menos críticas, a critério da gerência da rede. Este procedimento só deve ser adotado se o número de chamadas realizadas for superior a cinco, número também ajustável.

O mesmo tipo de avaliação deve ser realizado utilizando as chamadas que terminaram de forma anormal. Outra matriz deve ser montada, indicando o número destas chamadas para cada uma das instituições do projeto, associada a uma tabela com os motivos da desconexão. Caso o número de chamadas terminadas com os motivos *no route to destination, no resource, destination out of order* ou *recovery on timer expiry* exceda 10% do total realizado entre as duas instituições, alarmes devem ser enviados para a estação de gerência da instituição e outro para a da RNP. Uma avaliação das chamadas que terminaram com o motivo *user busy* também deve ser realizada, que pode auxiliar a identificar problemas associados a portas de voz ou troncos do PBX, ou pode indicar a necessidade de aumentar a quantidade de conexões com o PBX.

O processo de consolidação e análise da qualidade e do motivo de desconexão pode ocorrer antes de ser completado o período definido, se for identificado um número alto de chamadas com problemas de qualidade ou de desconexões anormais.

Semanalmente deve ser feita uma cópia de segurança do banco SQL, e os registros com os CDRs podem ser removidos do banco.

Uma cópia das informações consolidadas deve ser enviada para a estação de gerência da RNP diariamente para que possam ser gerados relatórios estatísticos, que poderão ser utilizados para identificar problemas. Relatório contendo o número total de chamadas realizadas por hora do dia deve ficar disponível para acesso via WEB, a média da duração da chamadas deve ser apresentada. Outro relatório deve apresentar a qualidade das chamadas, indicando o número de chamadas realizadas por hora, por

faixa de qualidade (Tabela 4-3). Um quadro com os motivos de desconexão das chamadas por hora também deve ser disponibilizado.

Uma matriz apresentando as chamadas realizadas e associando a qualidade e o motivo de desconexão das chamadas para cada par de instituições, por hora do dia, também deve estar disponível.

5.4 Gerenciamento de Falhas

O gerenciamento das falhas é um dos mais críticos dentro do serviço, onde tem a função de monitorar os equipamentos envolvidos e a rede para garantir que o serviço possa ser provido com a qualidade necessária. Caso não seja possível garantir essa qualidade, deve apresentar mecanismos que não permitam a admissão de novas chamadas.

A estratégia a ser adotada envolve a monitoração de variáveis críticas nos equipamentos envolvidos utilizando o SNMP, e alertando a estação de gerência se for verificado algum problema. Uma área na tela do sistema será reservada para a apresentação das mensagens de alerta, as quais devem ter uma cor de fundo que indique o quão críticos são os problemas indicados. Como pode haver uma quantidade muito grande de mensagens, deve ser dada a opção para seleção com base na gravidade da falha, endereço IP, data/hora e tipo de mensagem. Uma opção deve ser utilizada para que seja confirmada a leitura da mensagem, mensagens críticas não lidas devem ser comunicadas através de email a uma lista pré-definida de administradores (configurável). Opções do sistema devem permitir que se habilite o envio de mensagens a usuários específicos, através de email, *instant message* ou mensagens de celular, conforme o nível de criticidade da falha.

As mensagens de alerta e notificações devem ser enviadas para a estação de gerenciamento da instituição, a qual deve apresentá-las na janela de gerenciamento. Uma configuração específica para cada instituição deve indicar que situações devem ser alertadas à estação de gerenciamento principal, localizada na RNP. A comunicação entre as estações deve ser feita com notificações SNMP do tipo *inform.*

A verificação de que os *gateways* e *gatekeepers* estejam operacionais é importante para manter o serviço disponível para as instituições. A monitoração dos *gateways* deve ser realizada empregando o protocolo SNMP para realizar coletas periódicas das variáveis MIB-II *SysUpTime, ifAdminStatus* e *ifOperStatus* para as interfaces de rede e portas de voz utilizadas. A primeira verificação a ser realizada é se há uma resposta à requisição, indicando que o equipamento está alcançável. O passo seguinte é utilizar a variável *sysUpTime* para verificar quando foi realizada a última inicialização do equipamento. Um valor inferior à coleta anterior indica que o mesmo foi reinicializado, o que deve ser indicado na estação de gerência. Estes equipamentos costumam apresentar longos períodos sem que precisem ser reinicializados, uma constância na inicialização dos mesmos pode ser uma indicação de problemas, o que também deve ser alarmado na estação de gerência. Os dispositivos monitorados devem ser programados para o envio dos *traps* genéricos *coldstart e warmstart,* enviados quando o equipamento é reinicializado. Nas mensagens recebidas com a notificação pode ser obtida a causa da inicialização, a qual deve ser apresentada na estação de gerência.

A informação sobre o estado operacional das interfaces e porta de voz é útil para verificar se estão operacionais ou não. Nas interfaces operacionais (*ifAdminStatus=UP)*, o estado operacional deve estar na situação *UP* ou *dormant*. Caso contrário, deve ser indicado uma situação anormal das interfaces. Os equipamentos também devem ser configurados para o envio dos *traps* genéricos *linkdown* e *linkup*, os quais indicam problemas nas interfaces.

No caso de troncos E1, a MIB definida na RFC 1406, a análise da variável *dsx1LineStatus* permite verificar problemas associados ao canal. A análise das estatísticas disponíveis na tabela *dsx1CurrentTable* também permite verificar a existência de falhas. Notificações associadas aos DSPs são identificadas através de notificações definidas na MIB Cisco-DSP-MGMT-MIB.

As notificações definidas na MIB ITU-T *Gateway H.323* (*h323GwStart, h323GoingDown e h323Goingdown)* permitem monitorar mudanças no estado operacional do *gateway,* assim como identificar falhas associadas a este dispositivo.

Notificações correspondentes também são definidas na MIB *Gatekeeper*. Entretanto, as MIBS ITU-T não estão disponíveis nos equipamentos testados.

O *gatekeeper* utilizado no projeto não implementa um agente SNMP que permita a sua monitoração. O uso do pacote Net-SNMP[18] permite que um agente seja implementado na estação onde o serviço está operando, de forma que possam ser monitorados recursos deste equipamento. O uso da MIB *Host-Resources,* definida na RFC 1514, permite monitorar a carga no uso de CPU e os processos ativos, incluindo os recursos consumidos por cada. Alternativamente, o uso do console do GnuGK (porta TCP/7000) pode ser utilizado para verificar se o serviço está operacional.

A avaliação do consumo de recurso no *gateway* pode ser feita através da MIB Cisco-Process-MIB, onde é possível avaliar o consumo de CPU dos últimos cinco segundos, do último minuto e dos últimos cinco minutos. Uma avaliação destas variáveis pode identificar problemas no *gateway* que devem alertados através da estação de gerência.

Um ponto vital para que o serviço VOIP seja utilizado é a garantia que parâmetros como perda de pacotes, atraso e *jitter* estejam dentro de limites aceitáveis. A MIB IETF definida na RFC 2959 apresenta informações relativas ao protocolo RTP que podem ser utilizadas para avaliar cada fluxo RTP estabelecido. A tabela *rtpRcvrTable* apresenta variáveis (*rtpRcvrRTT, rtpRcvrJitter* e *rtpRcvrLostPackets*) que indicam as condições relativas a cada um dos fluxos. Entretanto, a operação normal do SNMP não permite uma monitoração constante destas informações, já que o mecanismo de *polling* não pode ser utilizado com uma constância que permita acompanhar cada um dos fluxos em tempo real, seja pela latência imposta na geração das mensagens de requisição e resposta, seja pelo tempo de atualização das variáveis na MIB do sistema monitorado. O problema mais sério ao uso desta MIB é o fato de que em nenhum dos equipamentos testados a mesma foi implementada, o que impede a monitoração dos fluxos RTP.

Uma alternativa em *gateways* Cisco é o uso da tabela de chamadas ativas disponível na MIB *Cisco-Voice-Dial-MIB* (*cvVoIPCallActiveTable)* para este fim. Entretanto, o uso desta MIB apresenta o mesmo problema em relação ao uso do

[18] Disponível na Internet em http://www.net-snmp.org/ (Acesso em: Ago 2003)

mecanismo de *polling* do SNMP. As MIBs *Event* e *Expression*, definidas nas RFCs 2981 e 2982, respectivamente, podem ser utilizadas para solucionar este problema. A MIB *Event* adapta mecanismos previstos no RMON para que sejam emitidos alarmes em função do comportamento de variáveis da MIB. Desta forma, seria possível monitar as variáveis descritas para que os alarmes fossem emitidos quando necessário. A MIB *Expression* pode ser utilizada para criar novas variáveis em função de outras existentes na MIB. É útil, por exemplo, para calcular a percentagem de pacotes perdidos como uma função dos pacotes perdidos em relação aos pacotes recebidos. A monitoração desta nova variável pode levar à emissão de um alarme caso esta percentagem seja superior a um valor limite pré-definido dos pacotes recebidos. Uma alternativa é o uso de alarmes RMON.

O uso de *probes* que sejam inseridos na rede para capturar informações sobre os fluxos RTP utilizando monitoração passiva, também é uma alternativa para monitorar a qualidade associada a cada um das chamadas. Um dos trabalhos sendo desenvolvido no Laboratório VOIP do NCE/UFRJ envolve o desenvolvimento de uma ferramenta para a captura destes fluxos e uma avaliação da qualidade. A implementação de um agente SNMP que implemente a MIB RTP e outras necessárias à avaliação da qualidade das chamadas é necessária para que estas informações possam ser avaliadas utilizando SNMP. A implementação de notificações SNMP associadas à qualidade das chamadas também devem ser implementadas para permitir uma reação mais rápida a problemas que possam estar ocorrendo na rede.

O objeto ICPIF disponível na tabela *cvVoIPCallHistoryTable* da MIB *Cisco-Voice-Dial-Control-MIB* também pode ser utilizada para avaliar a qualidade das chamadas que já terminaram, o que pode auxiliar na identificação de problemas associados a conexões específicas. Quando habilitada, a notificação *cvdcPoorQoVNotification* é enviada quando uma chamada terminada com a avaliação de que a qualidade medida ao longo de toda a chamada não atendeu à esperada. Esta notificação é enviada, por padrão, quando o fator ICPIF calculado for superior ou igual 20, o que pode alterado para ajustar à expectativa de qualidade na chamadas VOIP realizadas através do *gateway*.

Ao adotar uma política de QoS no *backbone* da RNP seria importante que pudesse ser avaliado se há descarte associado ao tráfego VOIP nos roteadores por onde este passa. Como não existem notificações específicas que permitam identificar esta condição, é utilizado o mecanismo de alarmes e eventos definido no RMON. Na tabela *Alarm* da RMON MIB é possível criar entradas que permitem definir alarmes a partir da avaliação de qualquer variável numérica na MIB. O alarme está associado à definição de valores de limite inferior e superior, aos quais a variável selecionada é comparada. A tabela *Event* desta MIB permite criar associados aos alarmes criados, que permitem definir a emissão de uma notificação SNMP (*Trap*), caso a variável monitorada no alarme associado ultrapasse os limites definidos. A MIB *Cisco-Class-Based-QOS-MIB* dispõe de uma instância do objeto *cbQosCMDropBitRate* para cada classe de serviço criadas nos roteadores que adotam políticas de QoS. A monitoração deste objeto pode disparar uma notificação, caso seja verificado qualquer tráfego descartado na classe associada à mídia VOIP. Estas notificações devem ser direcionadas à gerência do serviço VOIP na RNP, onde mecanismos de avaliação definidos na estação de gerência vão avaliar as notificações recebidas. A correlação destas notificações associadas a QoS com outras condições monitoradas pode auxiliar a identificação de problemas no backbone que afetem a QoS associada ao serviço VOIP. Uma opção ao emprego de RMON é o uso da MIB Event.

A monitoração ativa da rede de forma a identificar problemas mesmo não quando não há chamadas ativas deve ser considerada para que possa haver uma reação pró-ativa na resolução de problemas. Ferramentas já desenvolvidas permitem realizar este tipo de avaliação, como apresentado em [69]. Estas ferramentas devem ser associadas a agentes SNMP que permitam a emissão de notificações ao serem verificadas condições anormais nos testes realizados. O fabricante Cisco desenvolveu um agente para os *gateways* (SAA – *Service Assurance Agent*), que podem ser configurados para emitir fluxos com as mesmas características que os de pacotes RTP, inclusive em relação à marcação de serviços diferenciados DSCP. Um agente remoto (*SAA responder*) é configurado para ecoar os pacotes recebidos. A avaliação da quantidade de pacotes perdidos, atrasados e adiantados, do *round trip time*(RTT), de *one-way delay* e do *jitter* permite determinar a situação da rede entre os dois pontos nas mesmas condições em que opera o serviço VOIP. A configuração dos agentes

envolvidos pode ser realizada através de comandos específicos nos agentes ou realizada remotamente através de SNMP, onde são configuradas todas as opções associadas. A MIB *Cisco-RTTMON-MIB* é utilizada para este fim, onde também podem ser observados os contadores contendo os resultados instantâneos de todos os testes ativos. A notificação *rttMonThresholdNotification* pode ser utilizada para indicar situações anormais que possam afetar a qualidade das chamadas. Como cada teste ativado consome recursos do *gateway*, o fabricante implementa mecanismos que limitam os recursos utilizados. Além dos testes associados especificamente a VOIP, são possíveis testes envolvendo coleta de RTT e *Jitter Hop-by-HOP* com uso de ICMP, medições de RTT, medições de *jitter* e medições de tempos com a simulação de solicitações http ou DNS entre dois agentes SAA. A rede VOIP implementada na Austrália utiliza um mecanismo semelhante para mapear a situação de QoS na rota para cada instituição participante.

A avaliação do motivo da desconexão das chamadas também é outra fonte para a identificação de problemas. Esta informação pode ser obtida dos CDRs gerados pelo *Radius* ou através das MIBs *Dial-Control-MIB* e *Cisco-Dial-Control-MIB*. Os dados obtidos podem auxiliar a identificar problemas associados a portas de voz, troncos digitais, ramais do PBX ou conexões com dispositivos remotos específicos.

Falhas que indiquem problemas na rede que impeçam a realização de chamadas com uma qualidade mínima podem disparar uma mudança de configuração dos *gateways*, desabilitando as portas de voz analógicas através do objeto *ifAdminStatus* (*interfaces)* ou, no caso de canais digitais, configurando a condição *busyout* (MIBs Cisco-CAS-IF-MIB ou Cisco-POP-MGMT-MIB). Ao perceber que um canal está na condição *busyout,* o PBX utilizar uma rota alternativa para estabelecer a chamada. Não existindo uma, é retornado um tom para o usuário indicando que a chamada não pode ser completada.

Programas monitores na estação de gerência da instituição devem analisar todas as notificações recebidas, para que seja tomada alguma ação. No caso de *traps* associados à qualidade das chamadas, este programa deve avaliar se houveram chamadas com problema de qualidade nos 30 minutos anteriores. Para que esta avaliação possa ser efetuada, deve ser realizada inicalmente a consolidação das

informações recebidas através do protocolo *Radius*. O procedimento normal é realizar esta consolidação a cada 30 minutos. Havendo mais chamadas com problema no período avaliado deve ser enviada uma notificação SNMP (*inform)* para a estação de gerência da RNP indicando o problema e as instituições envolvidas, além de gerar um alarme para a estação local.

Ao receber notificações de problemas associados à qualidade de chamadas provenientes das instituições, um programa monitor na estação de gerência da RNP deve avaliar a ocorrência de outras notificações nos 60 minutos anteriores. Problemas correlacionados devem ser levantados. Caso seja implementada nos roteadores do backbone, a monitoração de descarte associado às filas LLQ, deve ser verificado se não há ocorrência de notificações associadas a roteadores na rota da instituição afetada. Estas informações devem ser repassadas à console da estação de gerência para que seja verificado o problema, indicando todas as notificações correlacionadas. Havendo um número elevado de chamadas afetadas, pode ser utilizada monitoração ativa com uso do agente SAA, para verificar problemas associados a QoS no backbone. Havendo alguma notificação associada a QoS, a monitoração deve ser feita entre a RNP e o roteador onde o problema foi reportado. Caso não haja notificações deste tipo, o teste deve ser feito inicialmente entre a RNP e o *gateway* da instituição que reportou o problema. Nos dois casos, deve ser disparado um teste entre os *gateways* das instituições onde foi identificado o problema de perda de qualidade nas chamadas. Os resultados dos testes devem ser reportados para a estação de gerência.

5.5 Gerenciamento de Performance

Várias métricas podem ser utilizadas para caracterizar o uso do serviço VOIP:

- número de chamadas realizadas/recebidas;
- número de chamadas não completadas;
- duração média das chamadas;
- distribuição das chamadas ao longo do dia;
- definição das horas de maior utilização;
- classificação das chamadas por qualidade de voz, utilizando o valor de ICPIF;

- distribuição da qualidade das chamadas por hora ou por horas do dia;
- número de chamadas terminadas de forma anormal, classificando-as pelo motivo da desconexão (*cause code);*
- número de chamadas não completadas, classificando-as pelo motivo (*cause code*).

Nas MIB ITU-T *H225CallSignalling, RAS, Gatekeeper e Gateway* são definidas tabelas estatísticas onde é possível identificar o número de chamadas estabelecidas e recebidas pelo dispositivo, número de mensagens de sinalização enviadas e recebidas e tempo médio das chamadas.

As informações obtidas dos CDRs *Radius* são a principal fonte de informações estatísticas relativas às chamadas. O grupo *callHistory* da *Dial-Control-MIB,* não implementada em equipamentos Cisco*,* apresenta as mesmas informações disponíveis através de SNMP. As variáveis *callHistoryTableMaxLength* e *callHistoryRetainTimer* definem o número máximo de entradas e o tempo mínimo que cada entrada pode ser mantida nesta tabela, respectivamente. Na *Dial-Control-MIB* estão disponíveis informações importantes sobre a quantidade de chamadas estabelecidas com sucesso e as que falharam, além do número de chamadas que foram aceitas e as recusadas para cada *dial peer* definido no *gateway*.

As MIBs *Cisco-Dial-Control-MIB* e *Cisco-Voice-Dial-Control-MIB* apresentam informações das chamadas já terminadas. Na primeira, podem ser coletados dados relativos ao tráfego gerado e recebido pelas chamadas e sobre o motivo da desconexão. A segunda apresenta informações sobre a qualidade das chamadas realizadas (ICPIF, *lost packets, early packets, late packets e round trip delay).*

Estatísticas associadas ao gatekeeper devem ser obtidas dos arquivos de log gerados pelo GnuGK, onde podem ser registradas todas as mensagens de sinalização RAS associadas ao dispositivo. Os registros podem ser enviados periodicamente para a estação de gerenciamento para que possam ser consolidados. Desta forma, é possível gerar dados que permitam uma análise das mensagens geradas e recebidas, onde podem ser avaliadas requisições aceitas e rejeitadas, das quais é possível extrair os motivos da rejeição. É possível ainda, obter o número de terminais que se registraram no gatekeeper

e os que tiveram pedido de registro recusado, com os motivos. A coleta destas informações também pode ser realizada através do console do GnuGK, com uma adaptação do roteiro Perl apresentado no anexo 3.

A análise das informações estatísticas coletadas pode ser utilizada para definir a necessidade de novos recursos como equipamentos, canais de comunicação, portas de voz, troncos de voz ou ramais no PBX.

5.6 Implementação da Plataforma de Gerência

Ferramentas serão desenvolvidas no Laboratório VOIP do NCE/UFRJ seguindo a metodologia apresentada, para que possa ser realizado o gerenciamento da estrutura que irá compor o projeto-piloto do GT-VOIP da RNP.

Os softwares adotados no desenvolvimento do sistema de gerenciamento devem ser de código aberto de forma que possam ser adaptados às necessidades do projeto.

O sistema operacional *Linux* está sendo adotado como base para o desenvolvimento, haja vista, a sua disponibilidade, o suporte de uma grande comunidade de desenvolvedores, a performance e o suporte a todos os outros pacotes que são utilizados no projeto. A maior dificuldade ao desenvolvimento do ambiente de gerência será manter as mesmas condições e ambiente em todas as estações de gerência que serão utilizadas no projeto. Neste sentido, será definido uso da versão mais recente do sistema operacional *Linux Red Hat*[19] em todas estações. O requisito mínimo de *hardware* será uma estação com processador Pentium 400MHz, 192MB de memória RAM e 80GB de disco rígido.

O sistema será desenvolvido utilizando como base o projeto Net-SNMP[20], que oferece o suporte necessário ao desenvolvimento de aplicações de gerenciamento utilizando o protocolo SNMP. A versão atual suporta o SNMPv3, requisito para garantir a segurança no uso do SNMP. Como o pacote GnuGK, adotado como *gatekeeeper* do piloto, não oferece suporte SNMP, será utilizado o agente extensível do Net-SNMP que permitirá o gerenciamento do serviço.

[19] Red Hat Linux 9
[20] Disponível na Internet em http://www.net-snmp.org/ (Acesso em: Ago 2003)

O pacote *Freeradius*[21] foi escolhido para implementar o servidor *Radius*, visto que apresenta um suporte de um grupo grande de desenvolvedores, tem a capacidade de replicação de informações e tem integração com bancos de dados MySQL e com LDAP. Nos testes realizados foi utilizada a versão 0.9.0.

O banco de dados utilizado será o *MySQL*, em função da compatibilidade com todas as aplicações utilizadas no projeto, pela robustez e pelo suporte em diversos sistemas operacionais.

Os programa utilizados serão desenvolvidos utilizando a linguagem de programação *Perl* com suporte a banco de dados MySQL e SNMP. Está previsto também, o uso da linguagem C++.

Estatísticas e gráficos serão implementados utilizando os módulos *statistics* e *gdgraphs* em *Perl* com o uso dos softwares MRTG (Multi e RRDTool (Round Robin Database Tool)[22].

[21] Disponível na Internet em http://www.freeradius.org/ (Acesso em: ago 2003)
[22] Disponível na Internet em http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/ (Acesso em: ago 2003)

Capítulo 6

Conclusões

Neste trabalho foram discutidos detalhes de como implementar o serviço VOIP para atender várias instituições interconectadas através da Internet, todas elas conectadas à Rede Nacional de Pesquisa (RNP).

No capítulo 2, foram apresentados cenários possíveis em ambientes VOIP, com uma descricão dos padrões de sinalização, em especial a arquitetura H.323.

A arquitetura adotada no projeto-piloto VOIP foi apresentada no capítulo 3, com detalhamento dos equipamentos utilizados, do plano de numeração, dos cuidados na conexão com o PBX e do mecanismo de coleta dos registros das chamadas para fins de contabilização.

No capítulo 4, foi avaliada a arquitetura SNMP em relação às necessidades do gerenciamento em redes VOIP, onde devemos ter mecanismos para garantir os requisitos de alta disponibilidade, confiabilidade e qualidade da voz, característicos das redes de telefonia tradicionais. Na análise realizada, foi verificada que a versão atual do SNMP apresenta características de segurança e performance que permitem seu uso pleno no gerenciamento do serviço VOIP. Versões anteriores apresentavam deficiências neste sentido que limitavam o uso do SNMP.

Neste capítulo, também foram avaliadas as bases de informações gerenciais (MIBs) especificadas pelo IETF, ITU-T e fabricantes de equipamentos para identificar aquelas que apresentam informações específicas para o gerenciamento de equipamentos e serviços VOIP.

O ITU-T especifica um conjunto de MIBs padronizadas para a gerência dos protocolos e dispositivos definidos na recomendação H.323. Foi avaliado um conjunto amplo de informações para a gerência de redes VOIP baseadas nessa recomendação. No entanto, ainda não estão disponíveis na grande maioria das implementações.

O IETF, por sua vez, não define MIBs direcionadas ao gerenciamento dos protocolos que compõem o H.323. Entretanto, especifica módulos MIB para a gerência

de configuração, de detecção de falhas e de análise de performance dos equipamentos utilizados, como *gateways e gatekeepers*, e seus componentes. Em especial para o serviço VOIP, são importantes as informações relativas às interfaces de rede, portas de voz e troncos digitais DS1. Um conjunto mínimo de dados sobre as conexões associadas às chamadas ativas, e um histórico das chamadas já realizadas, é definido na *dial-control-mib*. Porém, a organização destas MIB não permite um uso eficiente para fins de contabilização das chamadas VOIP. Uma MIB específica para a monitoração dos protocolos RTP e RTCP também é definida no IETF, o que permite monitorar a qualidade dos fluxos de mídia associados às chamadas VOIP, mas esta até o momento não está implementada nos equipamentos testados.

Como as MIBs definidas pelo IETF não são direcionadas à gerência específica de redes baseadas na recomendação H.323, e como as MIBs ITU-T não são normalmente implementadas, a gerência do serviço só é efetiva com MIBs privadas específicas. Nos equipamentos do fabricante Cisco foi possível identificar um conjunto de MIBs privadas, orientadas ao gerenciamento das chamadas realizadas através do serviço VOIP. Dados importantes para a contabilização das chamadas realizadas estão disponíveis nessas MIBs, além de informações que permitem identificar problemas que afetam a qualidade da voz.

Adicionalmente, no capítulo 4 foi analisado o serviço Radius com a finalidade de verificar seu uso na coleta dos registros das chamadas. Os atributos padrão obtidos através do serviço Radius permitem a coleta de informações úteis na contabilização de chamadas. Foram identificados atributos específicos definidos pelo fabricante que permitem obter uma maior quantidade de informações associadas às chamadas, inclusive a indicação de problemas que afetam a QoS associada aos canais de mídia VOIP. O uso do protocolo UDP pelo Radius não garante a entrega das mensagens, devendo ser utilizados mecanismos adicionais para evitar a perda de dados necessários às estatísticas e tarifação das chamadas.

As características de operação do protocolo SNMP não permitem seu uso na monitoração passiva da qualidade de voz associada às chamadas ativas em tempo real. Entretanto, foram identificadas extensões na MIB RMON e na MIB *Event* que

permitem a monitoração de variáveis associadas à QoS nas chamadas, e a emissão de alarmes caso seja identificada a queda na qualidade das mesmas.

No capítulo 5, foi especificado um sistema integrado para gerenciamento de redes VOIP com o uso do SNMP, das MIBs descritas no capítulo 4 e do serviço Radius.

Como trabalho futuro, seria interessante a realização de análise semelhante associada ao uso dos protocolos IETF SIP e ITU-T H.248/MEGACO.

Ferramentas de monitoração passiva, em desenvolvimento no Laboratório VOIP, são necessárias para o acompanhamento da qualidade de voz associada às chamadas ativas. A integração de MIBs específicas a estas ferramentas deve ser promovida, para que o protocolo SNMP possa ser melhor utilizado para esse fim.

A avaliação do *gateway* de código aberto *Asterisk*[23] será de grande valia para estudos associados à integração com a telefonia tradicional e de *gateways* H.323/SIP/MGCP.

A avaliação do comportamento das variáveis disponíveis nas MIBs associadas ao serviço VOIP pode auxiliar na definição dos valores limite que serão utilizados na ativação de alarmes. O desenvolvimento de sistemas especialistas que usem lógica difusa pode ser útil no tratamento e na correlação de alarmes, na identificação da causa de falhas ou de quedas na qualidade das chamadas e na gerência pró-ativa do funcionamento do serviço VOIP. Estudos neste sentido devem ser encaminhados para que se possa garantir uma alta disponibilidade para o serviço VOIP.

Outro trabalho futuro interessante seria a implementação das MIBs ITU-T H.341 nos *gatekeepers* e terminais H.323 de código aberto que facilitaria a gerência desses dispositivos.

Finalmente, o grupo de trabalho RMONMIB do IETF publicou recentemente um conjunto de *drafts* com uma proposta para a monitoração da QoS associada a aplicações de tempo real. Implementação da proposta d*o framework Real-Time Application Quality of Service Monitoring (RAQMON)* associada ao uso do protocolo SNMP pode facilitar a monitoração passiva das chamadas em curso e deve ser perseguida como objetivo futuro *[60]*.

[23] Disponível na Internet em http://www.asterisk.org

Referências Bibliográficas

[1] COHEN D. Specifications for the Network Voice Protocol (NVP).IETF RFC 741, nov. 1977.

[2] MAGILL D. T. Adaptive speech compression for packet communication systems. *Conference record of the IEEE National Telecommunications Conference*, pp. 29D-1 - 29D-5, 1973.

[3] COHEN D. *Specifications for the Network Voice Protocol* ISI/RR-75-39, USC/Information Sciences Institute, mar. 1976.

[4] COHEN D. Issues in Transnet Packetized Voice Communication *Proceedings of the Fifth Data Communications Symposium Snowbird*, pp. 6-10/13, Utah, set. 1977.

[5] COHEN D. A Protocol for Packet Switching Voice Communication *Proceedings of Computer Network Protocols Symposium*, Liege, Belgium, fev. 1978.

[6] SCHULZRINNE H. *Voice communication across the Internet: A network voice terminal.*Technical Report TR 92-50, Dept. of Computer Science, University of Massachusetts, Amherst, Massachusetts, jul. 1992.

[7] VOCALTEC Communications Ltd. *Internet Phone*. Disponível na Internet em: http:/ /www.vocaltec.com. Acesso em: ago. 2003.

[8] PULVER J. *About Free World Dialup - History and Reflections.* Disponível na Internet em: http://www.pulver.com/fwd/about.html, Acesso em: ago. 2003

[9] IDT Corporation. *IDT Announces Major Breakthrough That Will Allow Worldwide PC-TO-Telephone Calls Over The Internet.* Disponível na Internet em: http://www.idt.net/corporate/press/releases/58.asp. Acesso em: ago. 2003

[10] ITU-T Rec. I.363.1. *Protocol layer requirements B-ISDN ATM: Adaptation Layer specification: Type 1 AAL.* ago. 1996.

[11] MARCONDES, C. A. C.; COSTA, J. C. P. A. *Relatório de Pesquisa em Telefonia sobre ATM e Interoperabilidade entre Circuitos Emulados E1 em Equipamentos Fore e 3Com.* Relatório Técnico do NCE/UFRJ, Universidade Federal do Rio de Janeiro. Rio de Janeiro, Fev. 2000. Disponível na Internet em: http://www.voip.nce.ufrj.br/index_papers_2000_pt.htm. Acesso em: ago. 2003

[12] AUSTRALIAN ACADEMIC AND RESEARCH NETWORK. *History of VoIP project.* Disponível na Internet em: http://www.aarnet.edu.au/rd/voip/implementation/history.html Acesso em: jul. 2003

[13] ITU-T Rec. H.323. *Visual Telephone Systems and Equipment for Local Area Networks Which Provide a Non-Guaranteed Quality of Service.* mai. 1996.

[14] HANDLEY. M.; SCHULZRINNE H.; SCHOOLER E.; ROSENBERG J. *SIP: Session Initiation Protocol.* IETF RFC 2543, mar. 1999.

[15] SCHULZRINNE H.; CASNER. S.; FREDERICK. R.; JACOBSON B. *RTP: A transport protocol for real-time applications.* IETF RFC 1889, jan. 1996.

[16] AUSTRALIAN ACADEMIC AND RESEARCH NETWORK. *VOIP Project.* Disponível na Internet em: URL: http://www.aarnet.edu.au/rd/voip/index.html Acesso em: ago. 2003

[17] DRESSLER F. Advantages of VoIP in the German research network. *Proceedings of 5th IEEE International Conference on High Speed Networks and Multimedia Communications (IEEE HSNMC 2002),* pp. 56-60, Jeju Islands, Korea, Jul. 2002 URL: http://bsd.rrze.uni-erlangen.de/~fd/publications/hsnmc02.pdf. Acesso em: ago. 2003

[18] CESNET. *Voice services in the CESNET2 network*. Disponível na Internet em: URL: http://www.ces.net/project/iptelephony/. Acesso em: ago. 2003

[19] REDE NACIONAL DE PESQUISA. *Grupos de trabalho 2002-2003*. Disponível na Internet em: http://www.rnp.br/pd/gts2002-2003/gt-voip.html. Acesso em: ago. 2003.

[20] INTERNET2. *H.323 VOIP Testebed Gatekeeper Zones&Prefixes* Disponível na Internet em: http://voip.internet2.edu/h323/docs/gk02.html, Acesso em: jul. 2003.

[21] AUDIN G. Reality check on five-nines. *Business Communications Review*, pp. 22–27, mai. 2002.

[22] ANATEL Resolução no. 30. *Plano Geral de Metas de Qualidade para o Serviço Telefônico Fixo Comutado.* jun. 1998. Disponível na Internet em: http://www.anatel.gov.br/biblioteca/planos/planos.asp, Acesso: ago. 2003

[23] JIANG W.; SCHULZRINNE H. Assessment of VoIP Service Availability in the Current Internet. *PAM2003 The Passive and Active Measurement Workshop*, La Jolla, California, abr. 2003.

[24] AGÊNCIA NACIONAL DE TELECOMUNIÇAÇÕES *SGIQ : Gerenciamento de Indicadores de Qualidade*. Disponível na Internet em: http://sistemas.anatel.gov.br/sgiq/Relatorios_ASP/RelConsolidacao.asp. Acesso em ago. 2003.

[25] TOWSLEY D. Providing Quality of Service in Packet Switched Networks. *Performance Evaluation of Computer and Communication Systems*, pp. 560-586, Springer-Verlag, jul. 1993.

[26] HARDMAN V.; SASSE A.; HANDLEY M.; WATSON A. Reliable Audio for Use over the Internet, *Proceedings of INET'95*, jun. 1995.

[27] SANNECK H. Concealment of lost speech packets using adaptive packetization, *Proceedings IEEE Multimedia Systems 1998.* Austin, Texas, june 1998.

[28] BOUTREMANS C.; BOUDEC J. *Adaptive Joint Playout Buffer and FEC Adjustement for Internet Telephony.* EPFL-I&C-ICA, Disponível na Internet em: http://icwww.epfl.ch/publications/, Tech. Rep. IC, 2002.

[29] ITU-T Rec. G.114. *General Characteristics of International Telephone Connections and International Telephone Circuits: One-Way Transmission Time.* fev. 1996.

[30] BLAKE S.; BLACK D.; CARLSON M.; DAVIES E.; WANG Z.; WEISS W. *An Architecture for Differentiated Services.* IETF RFC 2475, dez. 1988

[31] JACOBSON V.; NICHOLS K.; PODURI K. *An Expedited Forwarding PHB* IETF RFC 2598, jun. 1999.

[32] KOSTAS T. J.; BORELLA M. S.; SIDHU I.; SCHUSTER G. M. Real-time voice over packet-switched networks. *IEEE Network*, pages 18–27, fev. 1998.

[33] BORELLA M.; SWIDER D.; ULUDAG S. Internet Packet Loss: Measurement and Implications for End-to-End QoS. *International Conference on Parallel Processing Workshops*, pp. 3-12, Minnesota, ago. 1998.

[34] MARKOPOULOU A.; TOBAGI F.; KARAM M. Assessment of voip quality over Internet backbones. *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, New York, New York, jun. 2002.

[35] HARRINGTON D.; PRESUHN R.; WIJNEN B. *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.* IETF RFC 3411, dez. 2002

[36] ITU-T Rec. P.800e. *Methods for subjective determination of transmission quality.* ago. 1996.

[37] COLE, R.G.; ROSENBLUTH, J. H. Voice over IP Performance Monitoring. *ACM SIGCOMM Computer Communication Review.* V. 31, n.2 pp. 9-24, Nova York, EUA, Abr. 2001.

[38] ITU-T rec. G.107 *The E-Model, a computational model for use in transmission planning.* mai. 2000

[39] RIGNEY C.; RUBENS A.; SIMPSON W.; WILLENS S. *Remote Authentication Dial In User Service (RADIUS).* IETF RFC 2138, abr. 1997

[40] RIGNEY C. *RADIUS Accounting.* IETF RFC 2139, abr. 1997

[41] UBIK S. *Using and Administering IPTA - The IP Telephony Accounting System.* CESNET Technical Report, Nov. 2002 URL: http://staff.cesnet.cz/~ubik/publications/2002/ipta.pdf. Acesso em: ago. 2003

[42] TURNER G. *Network design for Voice over IP in AARNet*. Documento disponível na Internet em URL:// http://www.aarnet.edu.au/rd/voip/qos/configuration.pdf. Acesso em: ago. 2003.

[43] KINGHAM S. *Specification for the Billing of Telephone Call Charges Over AARNet.* Disponível na Internet em: http://old.www.aarnet.edu.au/rd/voip/reportingbilling/billingsystemspec6.pdf, Acesso em: ago. 2003

[44] COX R. V.; PETER K. Low Bit-Rate Coders for Multimedia Communication. *IEEE Communications Magazine,* pp. 34-41, dez. 1996

[45] PERKINS M. E.; EVANS K.; PASCAL D.; THORPE L. A. Characterizing the Subjective Performance of the ITU-T 8kb/s Speech Coding Algorithm- ITU-T G.729. *IEEE Communications Magazine*, pp. 74-81, set. 1997.

[46] ITU-T Rec. H.248. *Gateway Contol Protocol,* jun. 2000

[47] CUERVO F.; GREENE N.; RAYHAN A. et al. *Megaco Protocol Version 1.0.* IETF RFC 3015, nov. 2000

[48] ITU-T E.164. *The international public telecommunication numbering plan* mai. 97

[49] KNIGHT S.; WEAVER D.; WHIPPLE D.; HINDEN R.; MITZEL D.; HUNT P.; HIGGINSON P.; SHAND M.; LINDEM A. *Virtual Router Redundancy Protocol.* IETF RFC 2338, abr. 1998

[50] MARCONDES, C.A.C. *Implantação e Desenvolvimento de Serviços para Ambiente Heterogêneo de Telefonia IP*. Orientador: Paulo Henrique Aguiar. Rio de Janeiro: UFRJ/CCMN Programa de Pós-Graduação IM/NCE, Abr. 2002. 107p. Dissertação (Mestrado em Ciência da Computação) Disponível na Internet em http://www.voip.nce.ufrj.br/publication/2002/tese_cesar_2002.pdf. Acesso em: ago. 2003.

[51] REDE NACIONAL DE PESQUISA, *Documento de Avaliação do Ambiente Experimental de VOIP durante o 4o. WRNP e 21o. SBRC: Descrição, Resultados, Problemas*, Relatório Técnico P.4.1., jun. 2003. Disponível na Internet na http://www.voip.nce.ufrj.br/publication/reports/gt-voip-p41.pdf. Acesso em: ago. 2003

[52] REDE NACIONAL DE PESQUISA. *Projeto-Piloto VOIP: requisitos de produção - arquitetura, requisitos de hardware/software, protocolos, estrutura de gerência e descrição de testes,* Relatório Técnico P.5.1., jun. 2003. Disponível na Internet em: http://www.voip.nce.ufrj.br/publication/reports/gt-voip-p51.pdf. Acesso em: ago. 2003

[53] AGÊNCIA NACIONAL DE TELECOMUNIÇAÇÕES *Controle de contratos do STFC*. Disponível na Internet em: http://sistemas.anatel.gov.br/Sgcc/Relatorios/PgmqConsolidado.asp. Acesso em ago. 2003.

[54] ITU-T Rec. X.700. *Management framework for Open Systems Interconnection (OSI) for CCITT applications* , nov. 1992

[55] CLARK A. *Proposal for Passive QoS Monitoring Methodology for Voice over IP*, ETSI TIPHON 19, Temporary Document 98. Disponível na Internet em: http://www.telchemy.com/references/stdcontribs/19td098.pdf. Acesso em: ago. 2003

[56] CASE J.; McCLOGHRIE K.; ROSE M.; WALDBUSSER S. *Introduction to version 2 of the Internet-standard Network Management Framework.* IETF RFC 1441, abr. 1993

[57] HARRINGTON D.; PRESUHN R.; WIJNEN B. *An Architecture for Describing SNMP Management Frameworks*. IETF RFC 2271 jan. 1998

[58] CASE J.; MUNDY R.; PARTIN D.; STEWART B. *Introduction and Applicability Statements for Internet-Standard Management Framework.* IETF RFC 3410, dez. 2002

[59] WALDBUSSER, S. *Remote Network Monitoring Management Information Base*, IETF RFC 2819, mai. 2000

[60] SIDDIQUI A.; GOLOVINSKY E. *Real-time Application Quality of Service Monitoring (RAQMON) Framework.* IETF DRAFT draft-ietf-rmonmib-raqmon-framework-02.txt, Jun. 2003 (Trabalho em progresso)

[61] ITU-T Rec. H.341. *Multimedia management information base.* mai. 1999

[62] McCLOGHRIE K. *SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2.* IETF RFC 2013, nov. 1996

[63] McCLOGHRIE K.; KASTENHOLZ F. *The Interfaces Group MIB*. IETF RFC 2863, jun. 2000

[64] BAKER F.; WATT J. *Definitions of Managed Objects for the DS1 and E1 Interface Types.* IETF RFC 1406, jan. 1993.

[65] WALDBUSSER S. *Remote Network Monitoring Management Information Base* IETF RFC 2819, mai. 2000

[66] KAVASSERI R. *Event MIB*. IETF RFC 2981, oct. 2000

[67] KAVASSERI R. *Distributed Management Expression MIB* IETF RFC 1982, oct. 2000

[68] BAUGHER M., STRAHM B., SUCONICK I., *Real-Time Transport Protocol Management Information Base* IETF RFC 2959, oct 2000

[69] CISCO SYSTEMS. *Cisco Service Assurance Agent User Guide*. Disponível na Internet em http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/saaug_ai.htm. Arquivo consultado em ago. 2003.

[70] RIGNEY C. *RADIUS Accounting* IETF RFC 2866, jun. 2002

[71] RIGNEY C.; WILLATS W.; CALHOUN P. *RADIUS Extensions.* IETF RFC 2869, jun. 2002

[72] ITU-T Rec. G.113. *Transmission impairments due to speech processing.* fev. 2002

Anexos

Anexo 1

Sinalização H.323

A comunicação entre dois dispositivos H.323 envolve uma série de fluxos associados à comunicação com o *gatekeeper*, à sinalização das chamadas e ao controle e transporte da mídia. Os protocolos definidos para estas funções para uso com aplicações de áudio são apresentadas na Figura 1-1.

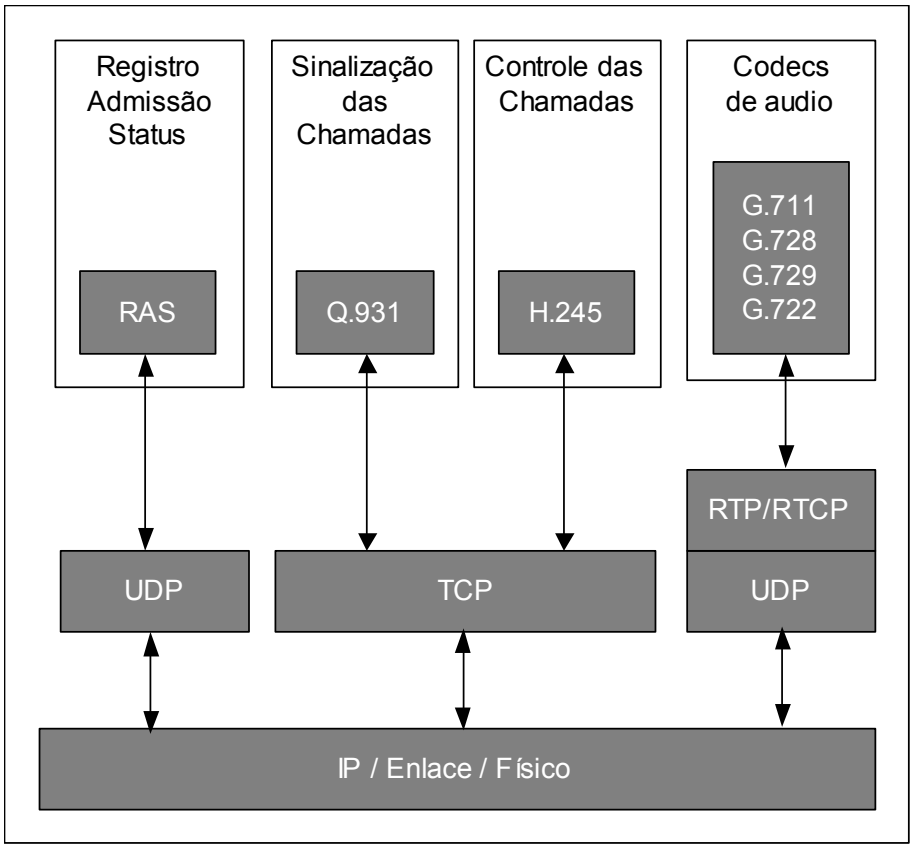


Figura 1-1 – Pilha de protocolos H.323 para uso em aplicações VOIP

A cada fluxo serão associados um endereço de rede e um TSAP específico. Em redes IP, são utilizados o endereço IP e os números de portas TCP e UDP, respectivamente. Cada um dos fluxos envolvidos em uma chamada está associado a uma conexão independente, utilizando protocolos de transporte e portas diferentes. Os endereços associados à maioria dos fluxos são determinados dinamicamente e são

repassados para o seu par através da sinalização. Na Tabela 1-1 é apresentado um resumo de como estes identificadores são determinados .

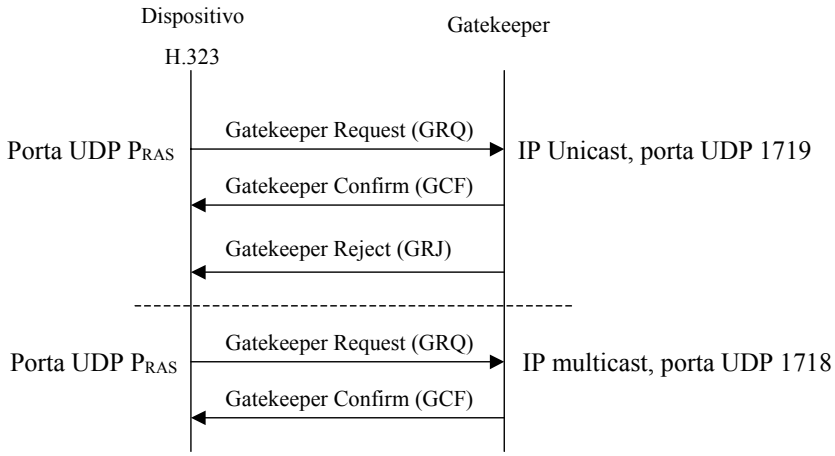
Tabela 1-1 – Endereços de rede e TSAPs associados sinalização e fluxos de mídia

Objetivo	Método de obter o endereço de rede	Método de obter o TSAP
Localização do gatekeeper	• Definido estaticamente • Requisições DNS (TXT / SRV) • *Multicast* gatekeeper.mcast.net = 224.0.1.41	• UDP porta 1719 • UDP porta 1718
Comunicação com gatekeeper (RAS)	• *Multicast* gatekeeper.mcast.net 224.0.1.41 • Definido estaticamente • Requisições DNS (TXT / SRV)	• UDP porta 1719
Sinalização H.225.0	• Traduzido do apelido H.323 (alias) pelo *gatekeeper*	• TCP porta 1720 • Traduzido do apelido H.323 (*alias*) pelo *gatekeeper*
Sinalização H.245	• Segue a mesma rota que a sinalização H.225	• Porta TCP dinâmica aprendida da sinalização H.225
RTP/RTCP	• Especificado no estabelecimento do canal lógico na sinalização H.245	• Portas UDP aprendidas da sinalização H.245

Sinalização RAS

RAS (*Registration, Admission and Status*) é o protocolo de sinalização utilizado na comunicação entre dispositivos H.323 e o *gatekeeper*. O canal RAS é estabelecido antes de qualquer outro canal de sinalização, sendo totalmente independente dos utilizados para a sinalização de chamadas e para o controle da mídia.

O endereço IP do *gatekeeper* que é utilizado por um dispositivo H.323 pode ser especificado estaticamente. Neste caso, uma mensagem RAS (GRP - *Gatekeeper Request*) é enviada ao *gatekeeper*, que aceita, ou não, este pedido. Opcionalmente, o endereço IP do *gatekeeper* pode ser anunciado através do serviço DNS, onde pode estar associado a registros do tipo SRV (*service location record*) ou do tipo TXT. Em consultas ao servidor DNS é retornado o endereço IP do *gatekeeper*. Esta facilidade permite um rápido ajuste dos dispositivos em face a alguma mudança nos endereços IP associados aos *gatekeepers*, já que bastaria ajustar a configuração no servidor DNS. Quando o endereço do *gatekeeper* é configurado estaticamente, há a necessidade de reconfigurar todos os clientes. Outra possibilidade de identificar o gatekeeper a ser utilizado é o envio de mensagens GRP associadas ao endereço *multicast* 224.0.1.41 (gatekeeper.mcast.net). Havendo um disponível, é enviada uma mensagem GCF. Na resposta, pode ser enviada uma lista de *gatekeepers* alternativos, que podem ser utilizados em caso de falha no principal, mantendo o funcionamento da rede. Na Figura 1-2 pode ser visto o procedimento de descoberta de *gatekeepers* por um dispositivo H.323.



P_{RAS} – Porta UDP associada à sinalização RAS (Estabelecida dinamicamente)

Figura 1-2 – Sinalização RAS: descoberta de *gatekeepers*

Confirmado o *gatekeeper*, deve ser realizado o registro do dispositivo através da mensagem RRQ (*Registration Request*). É retornada uma resposta afirmativa (RCF - *Registration Confirm*) ou negativa (RRJ - *Registration Reject*), conforme apresentado na Figura 1-3. O aceite do registro fica a critério da implementação de *gatekeeper*. O *gatekeeper* mantém um registro do dispositivo, contendo o endereço IP e a porta TCP

do canal associado à sinalização de chamadas (H.225), o tipo de dispositivo (terminal, *gateway* ou MCU), dados sobre o produto (modelo, versão e fabricante), os apelidos associados (*aliases*) e informações associadas a segurança H.323 (H.235). No caso de *gateways*, são mantidas informações sobre os prefixos E.164 atendidos, indicando que chamadas destinadas a números que utilizem este prefixo poderão ser encaminhados através da conexão com a rede de telefonia.

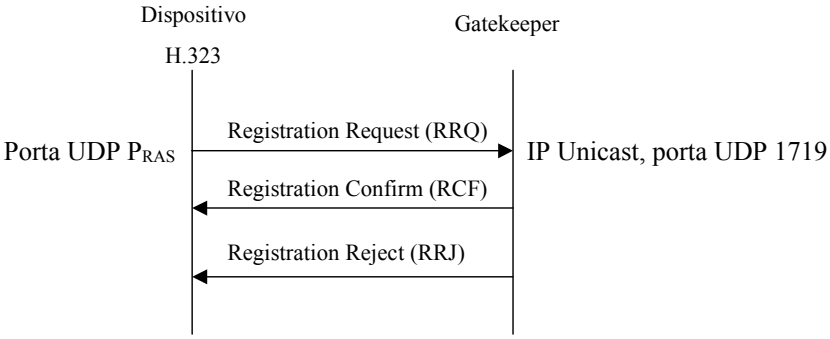


Figura 1-3 – RAS: registro no *gatekeeper*

Após a confirmação do registro, o dispositivo registrado pode então realizar uma chamada. Ao iniciá-la, deve enviar um pedido de admissão utilizando a mensagem ARQ (*Admission Request*). Nesse pedido é informado o apelido (*alias*) do dispositivo para onde será realizada a chamada, o qual pode ser uma seqüência de caracteres (H.323 ID), ou um número telefônico seguindo a recomendação E.164. O *gatekeeper* verifica se o dispositivo destino está registrado. Caso esteja e não hajam restrições, é enviada uma mensagem ACF (*Admission Confirm*), indicando o endereço IP e a porta TCP a serem utilizadas para se iniciar a sinalização da chamada. Esse endereço e porta podem estar associados ao dispositivo destino, no caso de sinalização direta, ou ao *gatekeeper*, se a sinalização tiver que ser encaminhada através do *gatekeeper* (*routed signaling*).

Quando o destino da chamada é um dispositivo em outra "zona", o *gatekeeper* remoto deve ser localizado para que possam ser obtidas informações sobre este dispositivo. Dois métodos podem ser utilizados com este objetivo: para apelidos tipo H323 ID, deve ser utilizado o serviço DNS, e para endereços E.164, mensagens RAS (LRQ – *Location request*).

O uso de DNS para a localização do *gatekeeper* remoto, requer que o H323 ID associado ao destino esteja no formato *usuário@domínio*. Nas informações associadas

ao domínio no serviço DNS, deve haver um registro dos tipos SRV ou TXT, indicando o endereço IP do *gatekeeper* associado ao domínio.

Ao utilizar endereços E.164 como apelido, devem ser definidos os prefixos que são atendidos por cada "zona". No caso de *gateways* conectados à rede de telefonia, estes devem indicar no registro os prefixos associados ao telefones atendidos por esta conexão. Desta forma, as chamadas destinadas a estes telefones serão encaminhadas para o *gateway*. Na comunicação entre zonas, os *gatekeepers* devem ter uma configuração estática dos prefixos atendidos por cada *gatekeeper* conhecido. Desta forma, ao receber um pedido de admissão, o prefixo é extraído do apelido do destino. A partir do prefixo é identificado o endereço do *gatekeeper* remoto, para onde é enviada uma mensagem RAS (LRQ – *Location Request*), como apresentado na Figura 1-4.

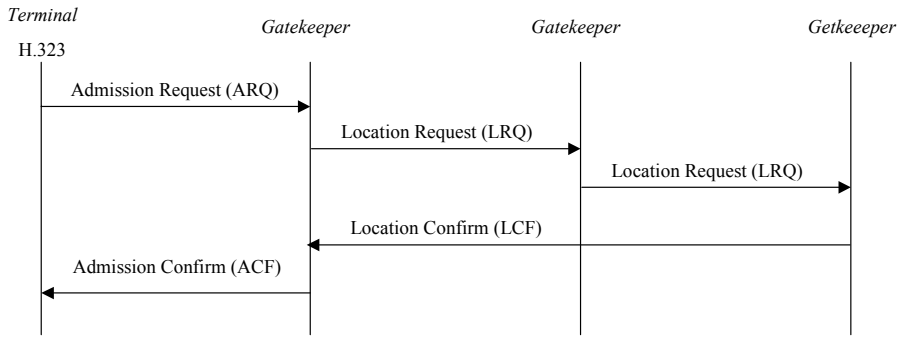


Figura 1-4 – Sinalização RAS: uso de LRQs

Ao receber a mensagem LRQ é verificado se o destino está registrado. Em caso afirmativo, e não havendo restrições, será enviada uma confirmação de localização (LCF – *Location Confirm*), indicando os parâmetros necessários ao estabelecimento do canal de sinalização de chamadas. Caso contrário, é enviada uma mensagem LRJ (*Location Reject).* Mensagens LRQ recebidas por um *gatekeeper* podem ser reenviadas a outros *gatekeepers.* Neste caso, só o *gatekeeper* onde estiver registrado o destino, ou que não tenha como encaminhar a LRQ para outro *gatekeeper*, retorna as mensagens LCF ou LRJ, respectivamente.

Gatekeepers específicos para a função de encaminhamento de mensagens LRQ, os *Directory Gatekeepers* (DGK), podem ser utilizados para estruturar redes H.323 com um grande número de "zonas". Na Figura 1-5, é apresentado um esquema de uma rede utilizando DGKs.

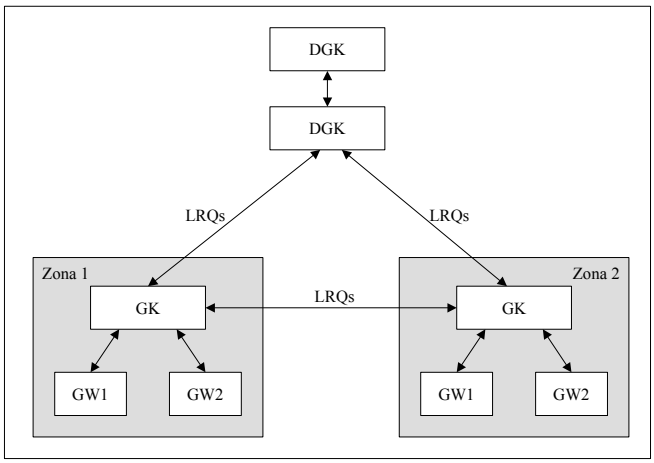


Figura 1-5 – Uso de Directory Gatekeeper

O IETF, através do grupo de trabalho IPTEL (IP *Telephony*), busca soluções para questões associadas à atribuição de nomes e roteamento em protocolos VOIP. O protocolo TRIP (*Telephony Routing over IP*) definido na RFC 3219, objetiva uma troca de informações entre domínios, "zonas" no caso do H.323, de forma a montar tabelas dinâmicas de "roteamento" que definam como alcançar os *gateways* de voz com base em prefixos E.164. Este protocolo apresenta um funcionamento semelhante ao BGP (*Border Gateway Protocol*) e é independente do protocolo de sinalização em uso, seja SIP ou H.323.

Identificado o endereço IP e o número da porta TCP associados ao canal de sinalização, uma conexão TCP é estabelecida com o dispositivo destino, por onde é realizada a sinalização da chamada utilizando o protocolo H.225.0. A mensagem H.225.0 *SETUP* é enviada neste canal para o dispositivo remoto, indicando a solicitação para estabelecer uma chamada H.323. Ao receber esta mensagem e não havendo restrições, o dispositivo remoto indica que recebeu o pedido de estabelecimento da conexão enviando a mensagem H.225 *CALL PROCEEDING*, e envia um pedido de admissão ao gatekeeper em que está registrado, usando a mensagem ARQ. Aprovada a

admissão, o usuário remoto é avisado da chamada. Ao indicar a chegada de uma nova chamada ao usuário remoto, normalmente através do toque do telefone, a mensagem H.225 *ALERTING* é enviada para o dispositivo que iniciou a chamada. Quando a chamada é atendida no dispositivo remoto, este envia a mensagem H.225.0 *CONNECT,* confirmando o estabelecimento da conexão. Na Figura 1-6, pode ser observada toda a sinalização RAS até o estabelecimento da chamada.

Na seqüência, é estabelecido um canal para sinalização de controle da mídia H.245, que entre outras atribuições, tem a função de estabelecer os canais RTP por onde vão trafegar os fluxos de mídia. O endereço IP e o número das portas UDP associadas a esses canais são indicados ao dispositivo remoto através do canal de controle de mídia.

Ao término da chamada, a mensagem RAS DRQ (*Disengage Request*) é enviada pelo dispositivo que inicia a desconexão para o *gatekeeper.* O *gatekeeper* confirma a desconexão com a mensagem DCF (*Disengage Confirm*). O mesmo procedimento ocorre com o outro dispositivo. A desconexão também pode ser iniciada a partir do *gatekeeper* que, neste caso, é o responsável em enviar a mensagem DRQ ao dispositivo.

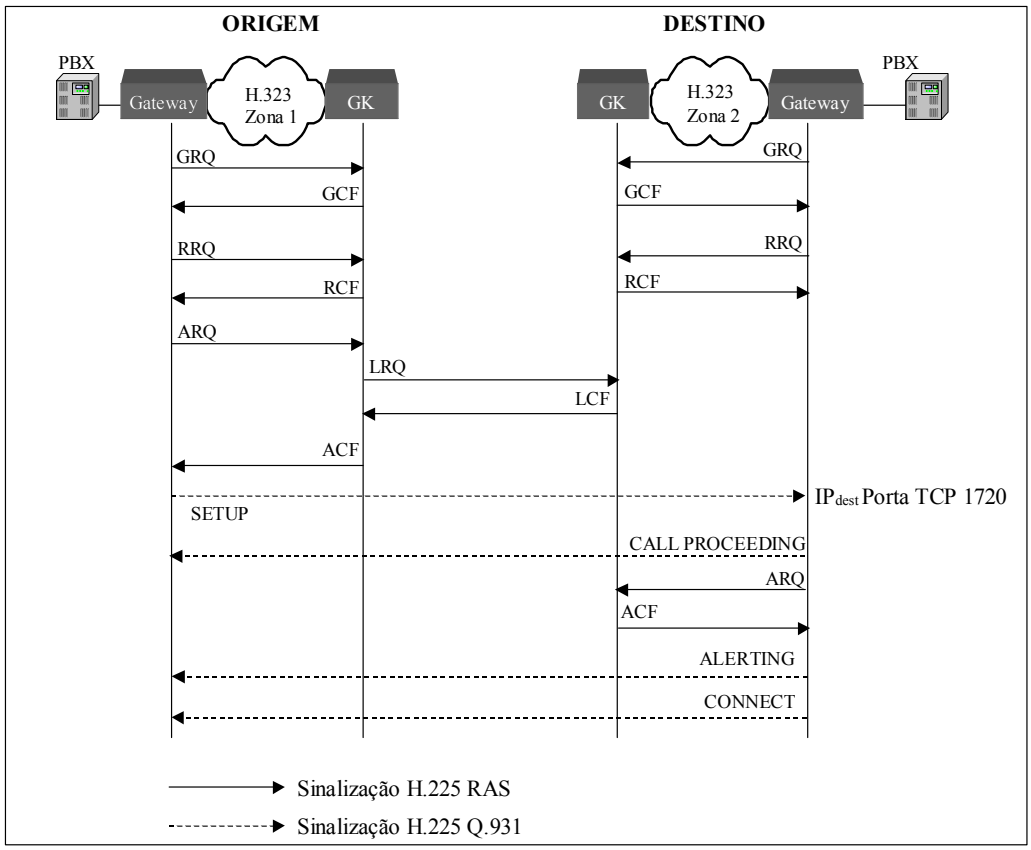


Figura 1-6 – Sinalização H.225

Sinalização H.225.0

O objetivo da sinalização H.225 é estabelecer, manter e terminar chamadas H.323. Mensagens associadas a serviços suplementares H.450.x também trafegam na sinalização H.225.0.

Os dispositivos aguardam normalmente um pedido de estabelecimento de novas chamadas através da porta TCP 1720. Entretanto, outras portas podem ser utilizadas. Os identificadores utilizados devem ser informados ao *gatekeeper* no momento do registro.

Serviços suplementares permitem que serviços tradicionais da telefonia sejam implementados em redes H.323. Isso inclui transferência de chamadas, chamada em espera, uso de MOH (*Music on Hold*) e indicação de chamadas em espera.

A sintaxe das mensagens que são usadas na sinalização das chamadas deriva das recomendações ITU-T Q.931 e Q.932 (serviços suplementares), utilizadas na

sinalização de conexões em redes ISDN (*Integrated Services Digital Network*). Na Tabela 1-2 são apresentadas as mensagens Q.931 empregadas na sinalização H.225.0.

Tabela 1-2 – Mensagens H.225.0 Q.931/Q.932

Mensagem	Descrição
ALERTING	Aviso de que o usuário remoto está sendo alertado que existe uma chamada nova
CALL PROCEEDING	Informações para estabelecimento da chamada foram recebidas; informações adicionais não serão mais recebidas
CONNECT	O usuário remoto aceitou a chamada, ou seja, atendeu o telefone.
USER INFORMATION	Permite a troca de informações diversas entre os dispositivos.
PROGRESS	Enviado pelo *gateway* para indicar que uma chamada que será realizada através do PBX está sendo providenciada
RELEASE COMPLETE	Término da chamada
SETUP	Início de nova chamada
STATUS	Resposta ao comando STATUS INQUIRY
STATUS INQUIRY	Utilizado para solicitar informações sobre o estado de uma chamada
FACILITY (Q.932)	Requisita serviços suplementares (H.450.x). Provê, por exemplo, informações para onde uma chamada deve ser redirecionada. Pode ser utilizada também para o estabelecimento de canais de sinalização H.245.

Quando não são utilizados *gatekeepers,* a sinalização H.225.0 é estabelecida diretamente entre os dispositivos envolvidos na chamada, como pode ser visto na Figura 1-7.

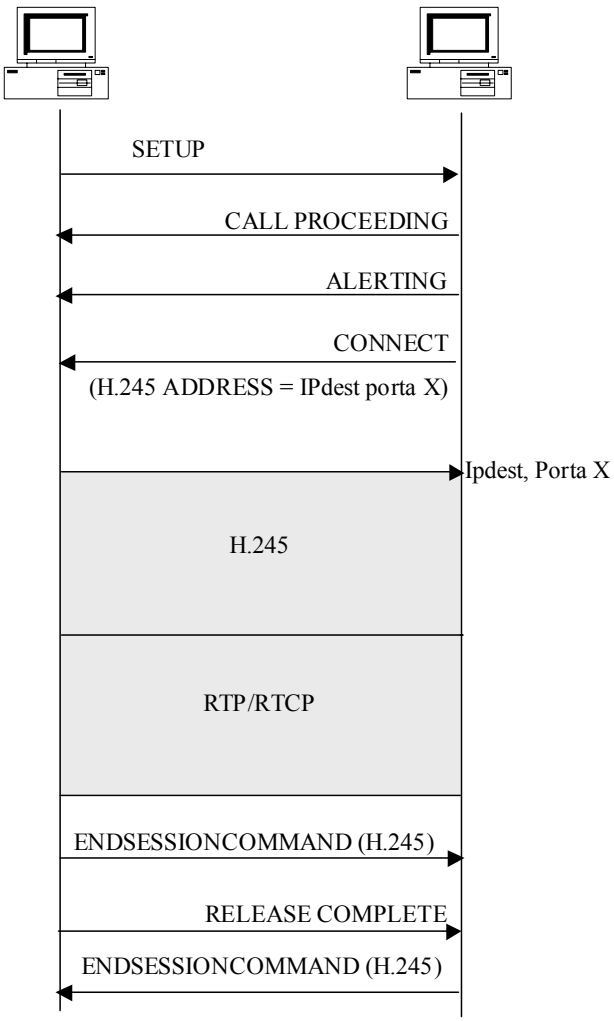


Figura 1-7 – Sinalização H.225 entre dois terminais H.323

Havendo um *gatekeeper*, podem ser aplicados dois modos de operação: *directed call signaling* e *gatekeeper routed call signaling*. No primeiro, a sinalização de chamada Q.931 é estabelecida diretamente entre os dispositivos. Uma conexão TCP é utilizada entre os dispositivos para o canal de sinalização, como pode ser visto na Figura 1-7. Na segunda opção, a sinalização é encaminhada através de um ou mais *gatekeepers,* havendo uma conexão TCP independente em cada segmento da sinalização, como pode ser visto na Figura 1-8.

A decisão sobre o tipo a ser utilizado é do *gatekeeper* e a escolha é informada ao dispositivo durante a admissão de uma chamada. A principal razão associada ao uso da intermediação do *gatekeeper* está associada à questão segurança. O gatekeeper pode operar como um procurador (*proxy*) para acesso aos dispositivos H.323 em redes protegidas por *firewalls* e, para isto, a sinalização H.245 deve ser tunelada através do H.225 e a mídia devem ser encaminhada através do *gatekeeper.*

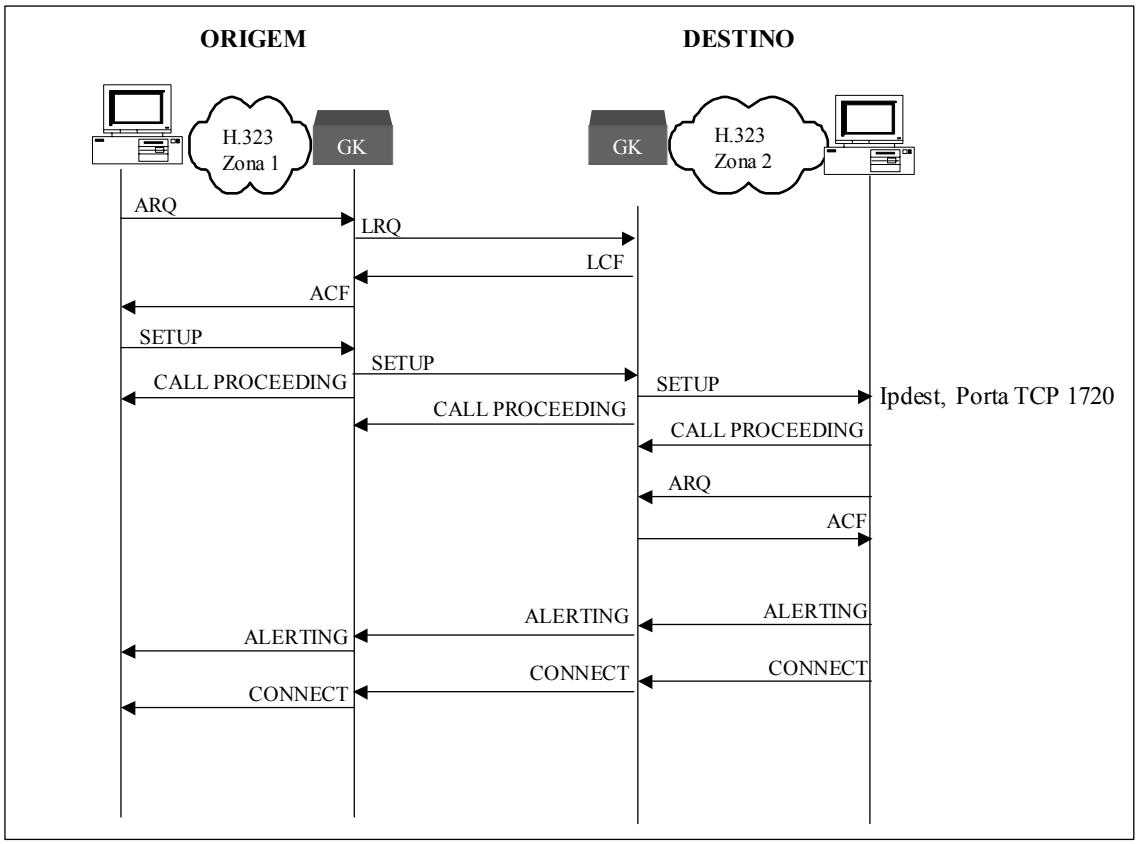


Figura 1-8 – Gatekeeper routed call signaling

Sinalização H.245.0

O canal de controle de mídia é estabelecido dinamicamente sobre uma conexão TCP, conforme as informações indicadas na mensagem CONNECT da sinalização H.225. Este canal é responsável pela troca de informações sobre as capacidades suportadas por cada dispositivo, pela determinação do dispositivo que controla o canal de sinalização em uma relação mestre/escravo (*master*/*slave*) e pelo estabelecimento dos canais lógicos por onde será transmitida a mídia.

Antes que possa ser estabelecido qualquer canal de mídia, é necessário que seja negociado o conjunto de capacidades comuns aos dispositivos, tais como, formatos de mídia (*Codecs*), suporte a RSVP, parâmetros de RSVP suportados e outras funcionalidades (*DTMF relay* e *Hook-flash*). Mensagens *TerminalCapabilitySet* são utilizadas para este fim.

A recomendação H.323 define que todas as implementações devem suportar o formato de mídia ITU-T G.711, nas variações *a-law* e *u-law*. Opcionalmente, podem suportar outros formatos, como G.722, G.723.1, G.728 e G.729.

Os dispositivos envolvidos em uma chamada elegem um como sendo o *master*, que tem a função de controlar o estabelecimento do canal de mídia e de resolver conflitos que possam ocorrer na negociação de capacidades. Mensagens *MasterSlaveDetermination* são aplicadas para esta finalidade.

A terceira fase do H.245 está associada à abertura dos canais lógicos, quando são estabelecidas as sessões RTP e RTCP para a transmissão dos fluxos de mídia. Cada direção terá uma conexão independente. Mensagens *OpenLogicalChannel* são empregadas para indicar os números das portas UDP que serão usadas nas sessões RTP e RTCP, o formato da mídia (*Codec)* e as informações sobre o uso de RSVP.

O H.323 original foi previsto somente para ambientes LAN, onde não havia grandes atrasos na comunicação entre dispositivos. Isto explica o grande número de fluxos necessários para estabelecer uma chamada, o que é um problema crítico quando o RTT é elevado. A chamada para ser estabelecida tem que passar pela sinalização H.225, e pela H.245, e então são estabelecidos os fluxos de mídia. Considerando, por exemplo, uma situação onde o *Round Trip Time* (RTT) varia em torno de 200ms, uma chamada pode demorar mais de 600ms para ser estabelecida. Objetivando uma redução no tempo de estabelecimento de uma chamada, a versão 2 do H.323 introduziu um novo modelo para a negociação e criação dos canais lógicos. As mensagens *openLogicalChannel* passam a ser transmitidas na mensagem SETUP do H.225. A confirmação a esta mensagem (*openLogicalChannelAck*) é transmitida na mensagem *CONNECT* enviada pelo dispositivo remoto. Este procedimento permite que ao terminar a sinalização H.225, os dois dispositivos já possam iniciar a transmissão dos fluxos de mídia. Este

procedimento recebe a denominação de "*fast start*". Esta opção é padrão no uso das versões mais atuais do H.323, mas pode ser recusada na sinalização da chamada se um dos dispositivos não aceitar esta facilidade. Na versão 2 também foi definido o envio de mensagens H.245 embutidas nas mensagens Q.931, diminuindo o número de conexões TCP necessárias. O uso da opção "H.245 *tunneling*" em conjunto com o modo "*gatekeeper routed calls signaling*" facilita a implementação de políticas de segurança em redes onde o serviço VOIP é utilizado.

A partir da versão 4 do H.323 é permitido que o canal de sinalização H.245 seja estabelecido em paralelo ao "*fast start*", diminuindo o tempo para o término de toda a sinalização associada ao estabelecimento de uma chamada H.323

Anexo 2

Tabela de *Vendor Specific Attributes* (VSA) Radius Cisco

VSA	Descrição
call-origin-endpt	Identifica o gateway ou gatekeeper originador da chamada VOIP. Contém o endereço IP do gateway originador ou o InterZone ClearToken (IZCT) da zona do gatekeeper originador da chamada.
call-origin-endpt-type	Indica o tipo de informação no campo call-origin-endpt.
charge-number	O atributo CHN é gerado pelo cliente RADIUS do gateway e, quando disponível, é enviado para o servidor RADIUS nas mensagens de início e fim de contabilidade
charged-units	O número de unidades de cobrança associadas a essa conexão. Para chamadas entrando, ou quando a informação de cobrança não é fornecida pelo switch, o valor desse objeto será igual a zero.
Cisco-NAS-port	Identificação da porta de entrada no NAS ou gateway. A sintaxe do Cisco-NAS-port é: *signalling type controller: timeslot group/control channel: bearer channel* O atributo Cisco-NAS-port tem a mesma função do atibuto 5 do RADIUS, mas usa strings do IOS Cisco associadas às portas físicas.
codec-bytes	Especifica o tamanho do *payload* do pacote de voz.
coder-type-rate	Define o Codec utilizado Especifica a taxa de transmissão de compressão de voz/fax para o segmento associado à chamada.
disconnect-text	Texto ASCII descrevendo a razão do término da chamada.
early-packets	O número de pacotes de voz recebidos que chegaram adiantados demais para serem armazenador no buffer de jitter durante a chamada.
gapfill-with-silence	Duração do sinal de voz substituído por silêncio, em razão de não ter recebido em tempo (ou perdido) o sinal

VSA	Descrição
	de voz do gateway dessa chamada. Em milisegundos.
gapfill-with-prediction	Duração do sinal de voz substituído por sinal sintetizado a partir de parâmetros ou amostras de dados anteriores no tempo, por não ter recebido em tempo (ou perdido) o sinal de voz do gateway dessa chamada. Um exemplo são as estratégias de *frame-erasure* e *frame-concelament* nos algoritmos de compressão do G.729 e G.723.1.
gapfill-with-interpolation	Duração do sinal de voz inserido a partir de sinal sintetizado a partir de amostras de dados anteriores e posteriores no tempo, por não ter recebido em tempo (ou perdido) os dados de voz do gateway dessa chamada.
gapfill-with-redundancy	Duração do sinal de voz tocado com sinal sintetizado a partir de parâmetros de redundância disponíveis, por não haver recebido em tempo (ou perdido) os dados de voz do gateway dessa chamada.
gw-final-xlated-cdn	O número chamado traduzido antes de ser enviado pelo gateway.
gw-rxd-cdn	O número chamado como é recebido pelo gateway na mensagem de sinalização, antes que qualquer regra de tradução seja aplicada.
gw-final-xlated-cgn	O número que originou a chamada já traduzido antes de ser enviado pelo gateway.
gw-rxd-cgn	O número que originou a chamada, como é recebido pelo gateway na mensagem de sinalização antes que qualquer regra de tradução seja aplicada.
h323-billing-model	Tipo de serviço de bilhetagem adotado para uma chamada específica.
h323-call-origin	Comportamento do gateway em relação à conexão que está ativa para esse segmento. Valores possíveis: originate, answer.
h323-call-type	Tipo ou família de protocolos usada nesse segmento da chamada (VOIP ou POTS).
h323-conf-id	Identificador de chamada único, gerado pelo gateway. Usado para identificar os eventos distintos bilhetáveis

VSA	Descrição
	(chamadas) dentro de uma única sessão. Na API de controle de chamadas do IOS Cisco (CCAPI), esse valor é chamado de GUID (globally unique identifier). O h323-conf-id é diferente do h323-incomind-conf-id. Por exemplo, em chamadas “long pound” (chamadas nas quais você utiliza a tecla # para fazer uma nova chamada) com uma aplicação pré-paga, um novo valor h323-conf-id é gerado para cada nova chamada.
h323-connect-time	Hora da conexão no formato NTP (Network Time Protocol): hora, minutos, segundos, microsegundos, zona horária, dia da semana, mês, dia do mês e ano.
h323-credit-amount	Quantidade de crédito (em moeda corrente) que a conta contém.
h323-credit-time	Número de segundos autorizados para a chamada.
h323-currency	Moeda corrente usada com h323-credit-amount.
h323-disconnect-cause	Código Q.931 que indica a causa da desconexão
h323-disconnect-time	Hora de desconexão no formato NTP: hora, minutos, segundos, microsegundos, zona horária, dia da semana, mês, dia do mês, ano.
h323-gw-id	Nome DNS ou nome local do gateway de voz que está enviando o VSA.
h323-incoming-conf-id	Um número único para identificar uma sessão de voz em um gateway, onde a sessão é terminada quando quem iniciou a chamada coloca o telefone no gancho. O valor h323-incoming-conf-id é usado para: • Acoplar os segmentos de entrada e saída para uma sessão em um gateway particular • Match the outbound and inbound call legs for a session on a particular gateway • Coletar e casar todos os registros para múltiplas chamadas pedidas (dentro dos limites de uma sessão) no gateway
h323-ivr-in	AVpairs definidos pelo usuário enviados do servidor RADIUS para o gateway de voz. Você pode ler e utilizar o valor do gateway via um script TCL IVR customizado.

VSA	Descrição
h323-ivr-out	AVpairs definidos pelo usuário enviados do gateway de voz para o servidor RADUS. O valor pode ser definido (escrito) através de um script TCL IVR customizado.
h323-preferred-lang	Linguagem a ser usada para tocar o prompt de áudio especificado pelo h323-prompt-id.
h323-prompt-id	Índice de um array que seleciona arquivos de prompt usados em um gateway.
h323-redirect-ip-address	Endereço IP para uma chamada alternativa ou redirecionada.
h323-redirect-number	Número telefônico para o qual a chamada é redirecionada; por exemplo, para um número 800 ou um número de serviço de cliente.
h323-remote-address	Endereço IP do gateway remoto.
h323-remote-id	Nome DNS, ou hostname definido localmente, do gateway remoto.
h323-return-code	Códigos de retorno são instruções do servidor para o gateway de voz.
h323-setup-time	Data de setup no formato NTP: hora, minutos, segundos, microsegundos, zona horária, dia da semana, mês, dia do mês e ano.
h323-time-and-day	Hora do dia no gateway remoto no formato: hora, minutos, segundos.
h323-voice-quality	Valor representando o ICPIF (impairment/calculated planning impairment factor) da qualidade de voz na conexão fornecida pelos drivers das camadas inferiores (como o processador de sinal digital). Números baixos representam uma melhor qualidade.
hiwater-playout-delay	O maior valor de Voice Playout FIFO Delay durante uma chamada de voz.
in-trunkgroup-label	Contém o label do trunk associado com o grupo de portas de voz através do qual a chamada TDM chegou no gateway.
incoming-area	O texto especifica o identificador do gatekeeper, ou a

VSA	Descrição
	zona ou área, de origem da chamada de voz sobre IP.
in-intrfc-desc	O texto especifica a descrição da porta de voz que recebe a chamada.
incoming-req-uri	A URI requisitada como aparece na linha de requisição, incluindo quaisquer parâmetros de URL.
in-portgrp-id	O texto contém uma descrição associada com a porta física telefônica de entrada que é usada nesse segmento da chamada.
internal-error-code	Identifica a causa de chamadas que falharam.
isup-carrier-id	O atributo CID é gerado pelo cliente RADIUS do gateway e, quando disponível, é enviado para o servidor RADIUS nas mensagens de início e fim de contabilidade para segmentos de chamadas telefônicas.
late-packets	O número de pacotes de voz recebidos que chegaram tarde para serem tocados pelo CODEC durante a chamada.
logical-if-index	O valor de ifIndex da interface lógica através da qual a chamada foi feita. Para meios RDSI, esse seria o ifIndex do canal B utilizado para essa chamada.
lost-packets	O número de pacotes de voz perdidos durante a chamada.
lowater-playout-delay	O menor valor de Voice Playout FIFO Delay durante uma chamada de voz.
Method	Nome do método como definido na linha de requisição.
next-hop-ip	Endereço IP do próximo hop para onde a requisição é encaminhada.
next-hop-dn	O Domain Name (DN) ou Fully Qualified Domain Name (FQDN) para onde a requisição é encaminhada. Quando se utiliza um registro do tipo SRV para resolver o endereço, esse contém o nome do domínio. (Note que isso significa que o FQDN não será incluído). Se apenas uma consulta do tipo A é usada para resolver o endereço IP do próximo hop, então esse é o nome FQDN. Se nenhuma resolução é necessária, significando que o endereço IP foi encontrado em uma entrada estática na URI requisitada, então esse atributo não é incluído na

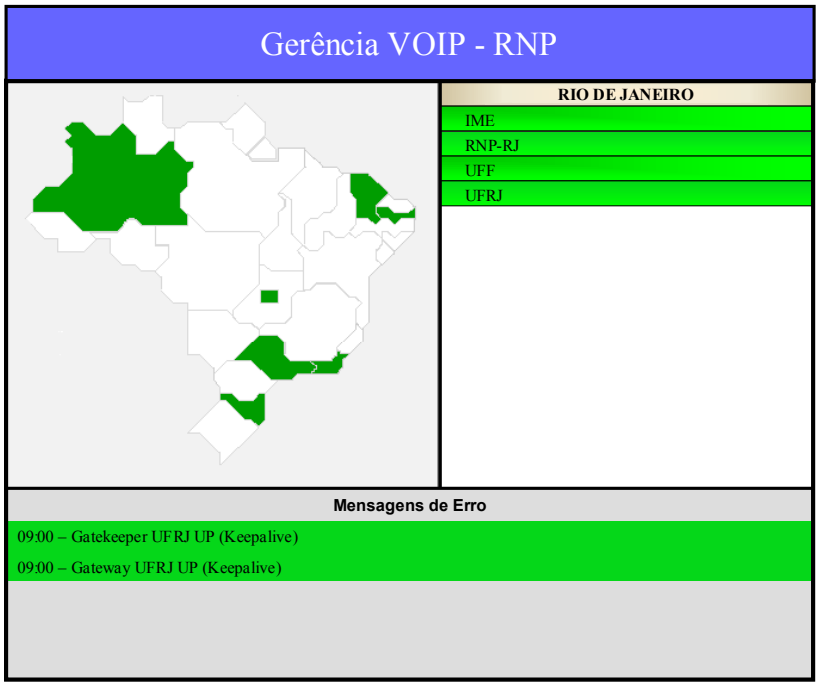
VSA	Descrição
	mensagem de contabilidade.
noise-level	O objeto contém a media de nível de ruído para a chamada. Em Dbm.
ontime-rv-playout	A duração da voz que é tocada a partir de dados recebidos a tempo para essa chamada. Esse valor mais as durações das entradas de GapFills somam a duração total de voz tocada para voz ativa (Total Voice Playout Duration for Active Voice). Em milisegundos.
originating-line-info	O atributo OLI é gerado pelo cliente RADIUS do gateway e, quando disponível, é enviado para o servidor RADIUS nas mensagens de contabilidade início e fim de chamadas telefônicas no segmento.
outgoing-area	O texto especifica o identificador do gatekeeper, ou a zona ou área de destino, da chamada de voz sobre IP sendo originada.
outgoing-req-uri	A URI requisitada que aparece na linha de requisição de saída, incluindo quaisquer parâmentros de URL.
out-carrier-id	O campo de ID de portadora do trunk através do qual as chamadas deixam o gateway, ou o identificador do provedor de serviços de voz da chamada de voz sobre IP que sai.
out-intrfc-desc	O texto especifica a descrição atribuída à porta de saída de voz de uma chamada.
out-portgrp-id	O texto contém uma descrição associada à porta física de telefônica de saída que é usada nesse segmento da chamada.
out-trunkgroup-label	Contém o *label* do *trunk* associado ao grupo de portas de voz, do *gateway*, a partir do qual a chamada TDM é enviada.
peer-address	O número ao qual essa chamada estava conectada. Se o número não está disponível, terá um tamanho igual a zero.
peer-id	É o valor do ID na entrada na tabela do peer para o qual essa chamada foi feita. Se uma entrada na tabela não existe para esse peer, o valor desse objeto será igual a

VSA	Descrição
	zero.
peer-if-index	Esse é o valor do ifIndex da entrada na tabela do peer para onde a chamada foi feita. Se não houver uma entrada na tabela para o peer dessa chamada, o valor desse objeto será igual a zero.
prev-hop-ip	Endereço IP do hop anterior, como visto pelo proxy.
receive-delay	O valor médio do Playout FIFO Delay mais o atraso do decoder durante a chamada de voz.
release-source	Identifica se uma chamada foi liberada pelo originador da chamada, por quem foi chamado, ou por uma fonte interna ou externa.
remote-media-id	Nome DNS do gateway de mídia remoto.
remote-media-address	Endereço IP do gateway de mídia remoto.
remote-media-udp-port	
remote-udp-port	Porta UDP que o sistema remoto escuta, para a qual os pacotes de voz serão transmitidos.
resource-service	Descreve o que o cliente está requisitando do servidor RPMS.
round-trip-delay	O atraso de ida e volta (round trip delay) do pacote de voz entre o sistema local e remoto no backbone IP durante a chamada. Em milisegundos.
session-protocol	Indica qual protocolo de sessão está sendo usado, como o SIP ou o H.323. Sempre igual a “sip” para SIP ou Cisco para H.323.
session-protocol	O objeto especifica o protocolo de sessão a ser usado por chamadas Internet entre o roteador local e remoto no backbone IP.
sip-hdr	Um cabeçalho arbitrário de chamada que foi encontrado na requisição que chegou. Consiste da linha de cabeçalho completa. A inclusão de qualquer cabeçalho em mensagens de contabilidade é controlada por uma diretiva de configuração.
Subscriber	Informação sobre assinante T1/Channel Associated

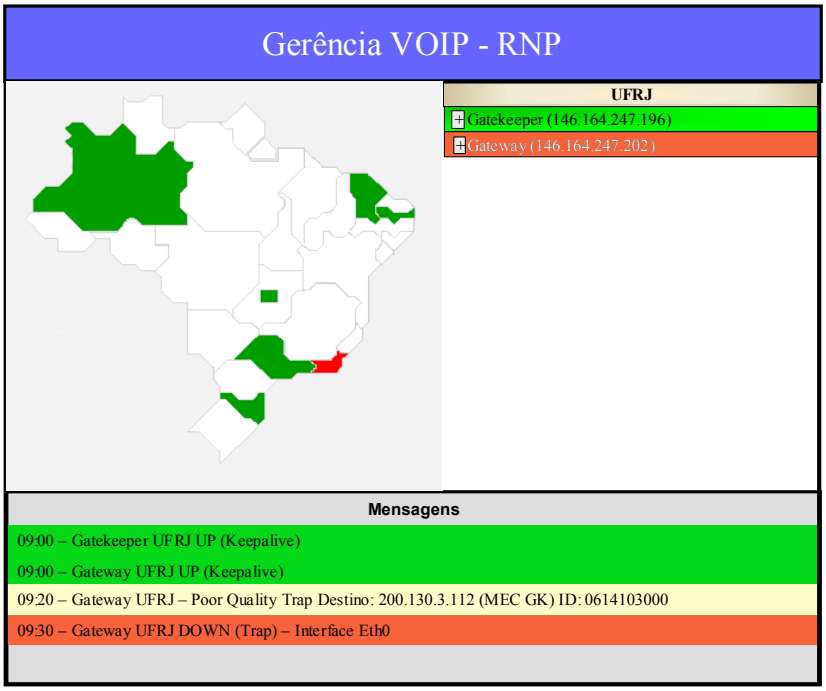
VSA	Descrição
	Signalling (CAS) ou E1/R2
transmission-medium-req	O atributo TMR é gerado pelo cliente RADIUS do gateway e, quando disponível, é enviado para o servidor RADIUS nas mensagens de contabilidade de início e fim de chamadas telefônicas no segmento.
tx-duration	Duração do caminho de transmissão aberto desse ponto até o gateway de voz para a chamada. Em milisegundos.
vad-enable	O objeto indica se o VAD (Voice Activity Detection) está ou não habilitado para a chamada de voz.
voice-tx-duration	Duração dessa ligação. A taxa de utilização de voz (Voice Utilization Rate) pode ser obtida dividindo essa duração por tx-duration. Em milisegundos.

Anexo 3

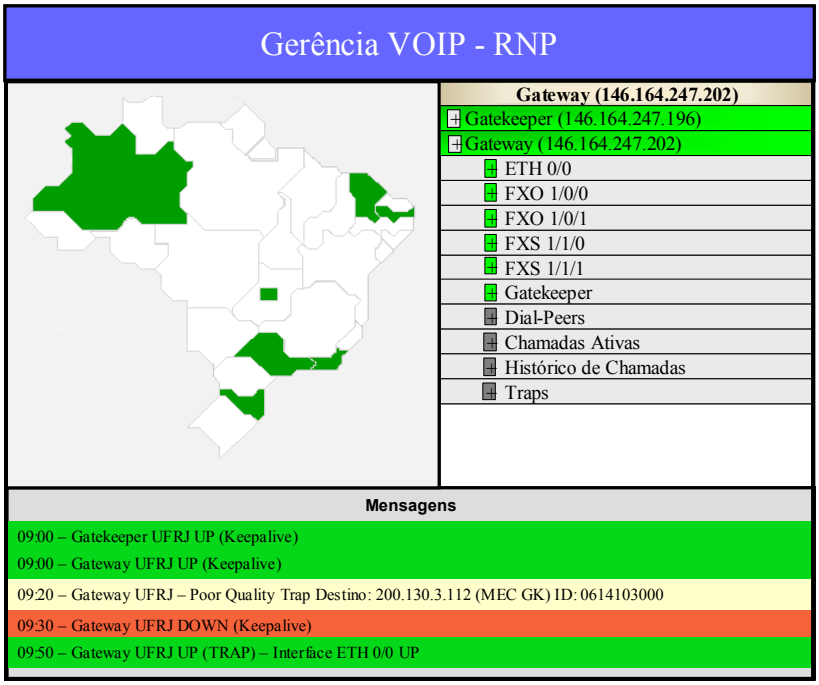
Telas do sistema proposto



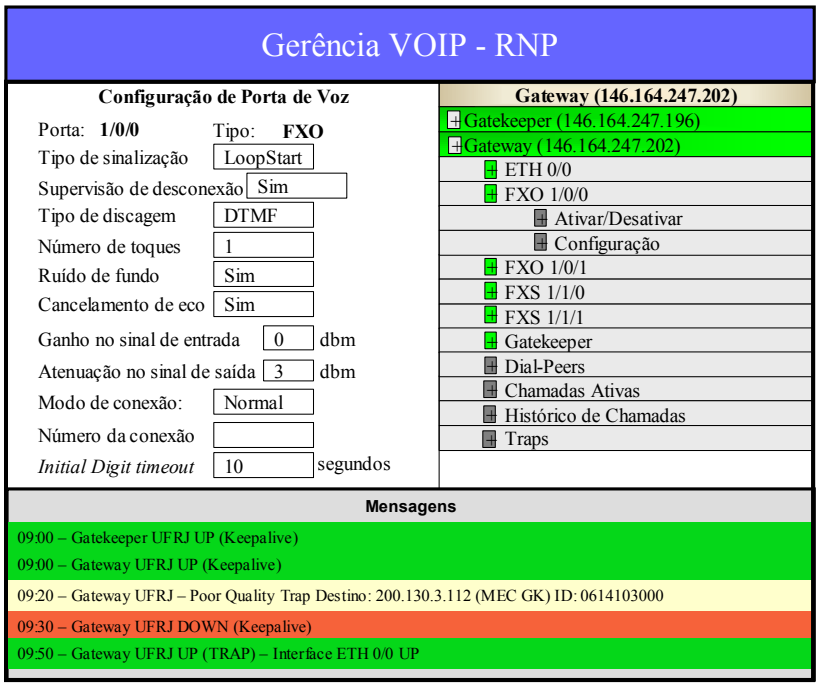
Tela de gerência das instituições por estado



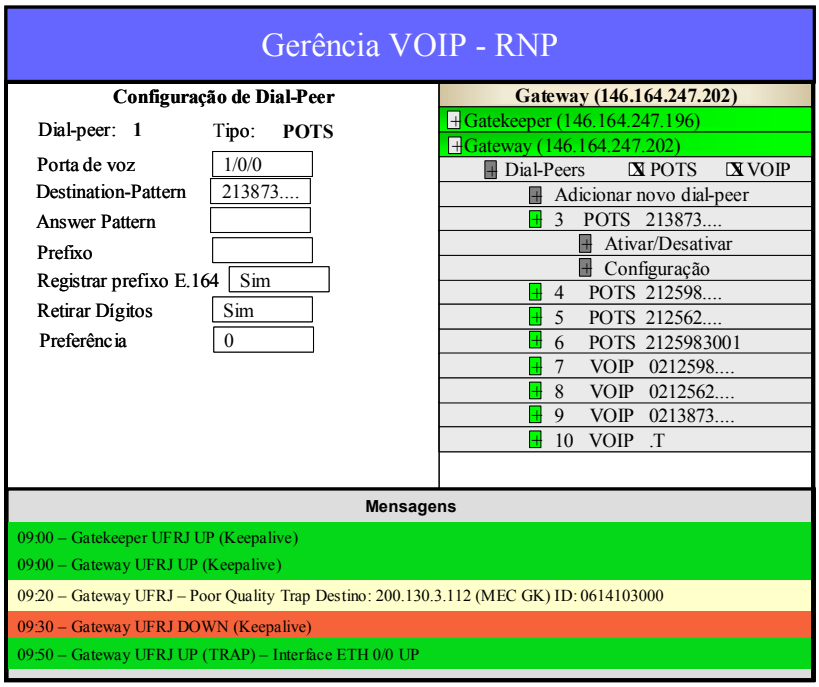
Tela de gerência dos equipamentos por instituição



Tela de monitoração de configuração de *gateways*



Tela de configuração de portas de voz



Tela de configuração de *dial-peer*

Anexo 4

GnuGK: Roteiro *Perl* para a captura de CDRs

```
#!/usr/bin/perl
# sample program that demonstrates how one could attach a
# billing interface to the OpenH323 Gatekeeper via the status port
# use the CDR records for real billing applications !
use strict;

use IO::Socket;

print "THIS IS NO REAL BILLING APPLICATION, JUST A DEMO HOW TO CONNECT TO THE GA
TEKEEPER.\nWRITE YOUR OWB CLIENT TO USE THE CDR MESSAGES!\n";

if (@ARGV != 1) {
        print "usage: billing.pl <gatekeeper_host>\n";
        exit(1);
}

my $gk_host = $ARGV[0];
my $gk_port = 7000;
my %calls,
my %caller;

my $sock = IO::Socket::INET->new(
   PeerAddr => $gk_host,
   PeerPort => $gk_port,
   Proto => 'tcp');
   if (!defined $sock) {
           die "Can't connect to gatekeeper at $gk_host:$gk_port";
   }

while (!$sock->eof()) {
        my $msg = $sock->getline();
        $msg = (split(/;/, $msg))[0];   # remove junk at end of line
        my $msgtype = (split(/\|/, $msg))[0];   # what message type is it ?
        if ($msgtype eq "ACF") {
                my ($calling, $callref, $called) = (split(/\|/, $msg))[2,3,4];
                $caller{$callref} = $calling;
                $calls{$callref} = time();
                print "User $calling started call $callref with $called\n";
       }
       if ($msgtype eq "CDR") {
                my ($callref, $calltime) = (split(/\|/, $msg))[1,2];
                my $initiator = $caller{$callref};
                print "Call $callref ended after $calltime seconds\n";
                print "Charging $initiator for $calltime seconds\n";
       }
}
```

Obs: Roteiro *Perl* fornecido junto com o código-fonte do GNUGK versão 2.0

Anexo 5

FreeRadius - Esquema da tabela Acct (SQL)

```
#
#  db_mysql.sql                      rlm_sql - FreeRADIUS SQL Module       #
#                                                                          #
#     Database schema for MySQL rlm_sql module                             #
#                                                                          #
#     To load:                                                             #
#         mysql -uroot -prootpass radius < db_mysql.sql                    #
#                                                                          #
#                                    Mike Machado <mike@innercite.com>     #
############################################################################
#
# Table structure for table 'radacct'
#

CREATE TABLE radacct (
  RadAcctId bigint(21) NOT NULL auto_increment,
  h323_Conf_Id varchar(48) NOT NULL default '',
  AcctSessionId varchar(32) NOT NULL default '',
  AcctUniqueId varchar(32) NOT NULL default '',
  UserName varchar(64) NOT NULL default '',
  h323_call_type varchar(24) NOT NULL default '',
  h323_setup_time varchar(64) NOT NULL default '0000-00-00 00:00:00',
  h323_connect_time varchar(64) NOT NULL default '0000-00-00 00:00:00',
  h323_disconnect_time varchar(64) NOT NULL default '0000-00-00 00:00:00',
  Realm varchar(64) default '',
  NASIPAddress varchar(15) NOT NULL default '',
  NASPortId int(12) default NULL,
  NASPortType varchar(32) default NULL,
  cisco_NAS_port varchar(24) NOT NULL default '',
  AcctStartTime datetime NOT NULL default '0000-00-00 00:00:00',
  AcctStopTime datetime NOT NULL default '0000-00-00 00:00:00',
  AcctSessionTime int(12) default NULL,
  AcctAuthentic varchar(32) default NULL,
  ConnectInfo_start varchar(32) default NULL,
  ConnectInfo_stop varchar(32) default NULL,
  AcctInputOctets bigint(12) default NULL,
  AcctOutputOctets bigint(12) default NULL,
  h323_disconnect_cause varchar(32) NOT NULL default '',
 h323_voice_quality varchar(24) NOT NULL default '0',
  h323_gw_id varchar(32) NOT NULL default '',
  CalledStationId varchar(50) NOT NULL default '',
  CallingStationId varchar(50) NOT NULL default '',
  AcctTerminateCause varchar(32) NOT NULL default '',
  ServiceType varchar(32) default NULL,
  FramedProtocol varchar(32) default NULL,
  FramedIPAddress varchar(15) NOT NULL default '',
  AcctStartDelay int(12) default NULL,
  AcctStopDelay int(12) default NULL,
  PRIMARY KEY  (RadAcctId),
  KEY UserName (UserName),
  KEY FramedIPAddress (FramedIPAddress),
  KEY AcctSessionId (AcctSessionId),
  KEY AcctUniqueId (AcctUniqueId),
  KEY AcctStartTime (AcctStartTime),
  KEY AcctStopTime (AcctStopTime),
  KEY NASIPAddress (NASIPAddress)
) ;
```

Anexo 6

Informações obtidas de uma chamada H.323 ativa com uso de SNMP

Chamada realizada entre o terminal H.323 (IP: 200.141.82.206) e o telefone 02125983307. O *gatekeeper* (IP: 146.164.247.206) foi utilizado como *H.323 proxy*. O gateway *(IP: 146.164.247.202)* interagia com o PBX através de duas interfaces FXO com indices 8 (FXO 1/0/0) e 9 (FXO 1/0/1). Os *dial-peer* utilizados na conexão tinha índices 41 (POTS) e 58 (VOIP).

Informações coletadas da MIB Dial-Control-MIB (RFC 2128)

callActivePeerAddress.12081.1	octet string	025983399
callActivePeerAddress.12087.1	octet string	2125983307
callActivePeerSubAddress.12081.1	octet string	
callActivePeerSubAddress.12087.1	octet string	
callActivePeerId.12081.1	Integer	1
callActivePeerId.12087.1	Integer	6
callActivePeerIfIndex.12081.1	Integer	58
callActivePeerIfIndex.12087.1	Integer	41
callActiveLogicalIfIndex.12081.1	Integer	0
callActiveLogicalIfIndex.12087.1	Integer	8
callActiveConnectTime.12081.1	Timeticks	0 days 00h 02m 9s.48th
callActiveConnectTime.12087.1	Timeticks	0 days 00h 02m 09s.47th
callActiveCallState.12081.1	Integer	Active
callActiveCallState.12087.1	Integer	Active
callActiveCallOrigin.12081.1	Integer	Answer
callActiveCallOrigin.12087.1	Integer	originate
callActiveChargedUnits.12081.1	Gauge	0
callActiveChargedUnits.12087.1	Gauge	0
callActiveInfoType.12081.1	Integer	speech
callActiveInfoType.12087.1	Integer	speech
callActiveTransmitPackets.12081.1	Gauge	398
callActiveTransmitPackets.12087.1	Gauge	0
callActiveTransmitBytes.12081.1	Gauge	64800
callActiveTransmitBytes.12087.1	Gauge	0
callActiveReceivePackets.12081.1	Gauge	0
callActiveReceivePackets.12087.1	Gauge	415
callActiveReceiveBytes.12081.1	Gauge	0
callActiveReceiveBytes.12087.1	Gauge	67680

Informações coletadas da MIB Cisco-Voice-Dial-Control-MIB

Tabela cvCallActiveTable

cvCallActiveConnectionId.12087.1	F1.3E.23.41.03.EE.18.10.94.BB.00.50.DA.6D.1E.5E
cvCallActiveTxDuration.12087.1	22720
cvCallActiveVoiceTxDuration.12087.1	22790
cvCallActiveFaxTxDuration.12087.1	0
cvCallActiveCoderTypeRate.12087.1	g711ulawr64000
cvCallActiveNoiseLevel.12087.1	0
cvCallActiveACOMLevel.12087.1	20
cvCallActiveOutSignalLevel.12087.1	-82
cvCallActiveInSignalLevel.12087.1	-19
cvCallActiveERLLevel.12087.1	20
cvCallActiveSessionTarget.12087.1	
cvCallActiveImgPageCount.12087.1	0
cvCallActiveEntry.13.12087.1	peixoto
cvCallActiveEntry.14.12087.1	2
cvCallActiveEntry.15.12087.1	51541

#Tabela cvVoIPCallActiveTable

cvVoIPCallActiveConnectionId.12081.1	F1.3E.23.41.03.EE.18.10.94.BB.00.50.DA.6D.1E.5E
cvVoIPCallActiveRemoteIPAddress.12081.1	146.164.247.196
cvVoIPCallActiveRemoteUDPPort.12081.1	5008
cvVoIPCallActiveRoundTripDelay.12081.1	0
cvVoIPCallActiveSelectedQoS.12081.1	bestEffort
cvVoIPCallActiveSessionProtocol.12081.1	cisco
cvVoIPCallActiveSessionTarget.12081.1	
cvVoIPCallActiveOnTimeRvPlayout.12081.1	320
cvVoIPCallActiveGapFillWithSilence.12081.1	10
cvVoIPCallActiveGapFillWithPrediction.12081.1	30
cvVoIPCallActiveGapFillWithInterpolation.120	0
cvVoIPCallActiveGapFillWithRedundancy.12081.1	0
cvVoIPCallActiveHiWaterPlayoutDelay.12081.1	65
cvVoIPCallActiveLoWaterPlayoutDelay.12081.1	64
cvVoIPCallActiveReceiveDelay.12081.1	64
cvVoIPCallActiveVADEnable.12081.1	false
cvVoIPCallActiveCoderTypeRate.12081.1	g711ulawr64000
cvVoIPCallActiveLostPackets.12081.1	0
cvVoIPCallActiveEarlyPackets.12081.1	7
cvVoIPCallActiveLatePackets.12081.1	0
cvVoIPCallActiveEntry.21.12081.1	
cvVoIPCallActiveEntry.22.12081.1	
cvVoIPCallActiveEntry.23.12081.1	1
cvVoIPCallActiveEntry.24.12081.1	146.164.247.196
cvVoIPCallActiveEntry.25.12081.1	40722
cvVoIPCallActiveEntry.26.12081.1	1
cvVoIPCallActiveEntry.27.12081.1	200.141.82.206
cvVoIPCallActiveEntry.28.12081.1	5008

Anexo 7

Histórico de uma chamada H.323 obtido com SNMP

Chamada realizada entre o terminal H.323 (IP: 200.141.82.206) e o telefone 02125983307. O *gatekeeper* (IP: 146.164.247.206) foi utilizado como *H.323 proxy*. O gateway *(IP: 146.164.247.202)* interage com o PBX através de duas interfaces FXO com indices 8 (FXO 1/0/0) e 9 (FXO 1/0/1). Os *dial-peer* utilizados na conexão tinha índices 41 (POTS) e 58 (VOIP).

Informações coletadas da MIB Cisco-Dial-Control-MIB

cCallHistorySetupTime	1	0 days 00h 02m 00s.87th
cCallHistorySetupTime	2	0 days 00h 02m 00s.81th
cCallHistoryPeerAddress	1	2125983307
cCallHistoryPeerAddress	2	025983399
cCallHistoryPeerId	1	6
cCallHistoryPeerId	2	1
cCallHistoryPeerIfIndex	1	41
cCallHistoryPeerIfIndex	2	58
cCallHistoryLogicalIfIndex	1	8 [8]
cCallHistoryLogicalIfIndex	2	0 [0]
cCallHistoryDisconnectCause	1	11
cCallHistoryDisconnectCause	2	1B
cCallHistoryDisconnectText	1	user busy
cCallHistoryDisconnectText	2	destination out of order
cCallHistoryConnectTime	1	0 days 00h 02m 09s.47th
cCallHistoryConnectTime	2	0 days 00h 02m 09s.48th
cCallHistoryDisconnectTime	1	0 days 00h 03m 12s.73th
cCallHistoryDisconnectTime	2	0 days 00h 03m 12s.79th
cCallHistoryCallOrigin	1	Originate
cCallHistoryCallOrigin	2	Answer
cCallHistoryInfoType	1	Speech(2
cCallHistoryInfoType	2	Speech(2
cCallHistoryTransmitPackets	1	13
cCallHistoryTransmitPackets	2	3474
cCallHistoryTransmitBytes	1	3120
cCallHistoryTransmitBytes	2	555840
cCallHistoryReceivePackets	1	3474
cCallHistoryReceivePackets	2	13
cCallHistoryReceiveBytes	1	555840
cCallHistoryReceiveBytes	2	3120
cCallHistoryEntry.20	1	3
cCallHistoryEntry.20	2	3

Informações coletadas da MIB Cisco-Voice-Dial-Control-MIB

Tabela cvCallHistoryTable

cvCallHistoryConnectionId.1	F1.3E.23.41.03.EE.18.10.94.BB.00.50.DA.6D.1E.5E
cvCallHistoryTxDuration.1	10
cvCallHistoryVoiceTxDuration.1	10
cvCallHistoryFaxTxDuration.1	0
cvCallHistoryCoderTypeRate.1	g711ulawr64000
cvCallHistoryNoiseLevel.1	0
cvCallHistoryACOMLevel.1	20
cvCallHistorySessionTarget.1	
cvCallHistoryImgPageCount.1	0
cvCallHistoryEntry.10.1	peixoto
cvCallHistoryEntry.11.1	2

#Tabela cvVoIPCallHistoryTable

cvVoIPCallHistoryConnectionId.2	F1.3E.23.41.03.EE.18.10.94.BB.00.50.DA.6D.1E.5E
cvVoIPCallHistoryRemoteIPAddress.2	146.164.247.196
cvVoIPCallHistoryRemoteUDPPort.2	5008
cvVoIPCallHistoryRoundTripDelay.2	0
cvVoIPCallHistorySelectedQoS.2	bestEffort
cvVoIPCallHistorySessionProtocol.2	cisco
cvVoIPCallHistorySessionTarget.2	
cvVoIPCallHistoryOnTimeRvPlayout.2	320
cvVoIPCallHistoryGapFillWithSilence.2	10
cvVoIPCallHistoryGapFillWithPrediction.2	30
cvVoIPCallHistoryGapFillWithInterpolation.2	0
cvVoIPCallHistoryGapFillWithRedundancy.2	0
cvVoIPCallHistoryHiWaterPlayoutDelay.2	65
cvVoIPCallHistoryLoWaterPlayoutDelay.2	64
cvVoIPCallHistoryReceiveDelay.2	64
cvVoIPCallHistoryVADEnable.2	false
cvVoIPCallHistoryCoderTypeRate.2	g711ulawr64000
cvVoIPCallHistoryIcpif.2	34
cvVoIPCallHistoryLostPackets.2	0
cvVoIPCallHistoryEarlyPackets.2	7
cvVoIPCallHistoryLatePackets.2	0
cvVoIPCallHistoryEntry.22.2	
cvVoIPCallHistoryEntry.23.2	
cvVoIPCallHistoryEntry.24.2	1
cvVoIPCallHistoryEntry.25.2	146.164.247.196
cvVoIPCallHistoryEntry.26.2	40722
cvVoIPCallHistoryEntry.27.2	1
cvVoIPCallHistoryEntry.28.2	200.141.82.206
cvVoIPCallHistoryEntry.29.2	5008